ADVANTECH
Enabling an Intelligent Planet

WISE-DeviceOn

IoT Device Operation Management

User Manual

English v-1.0.18

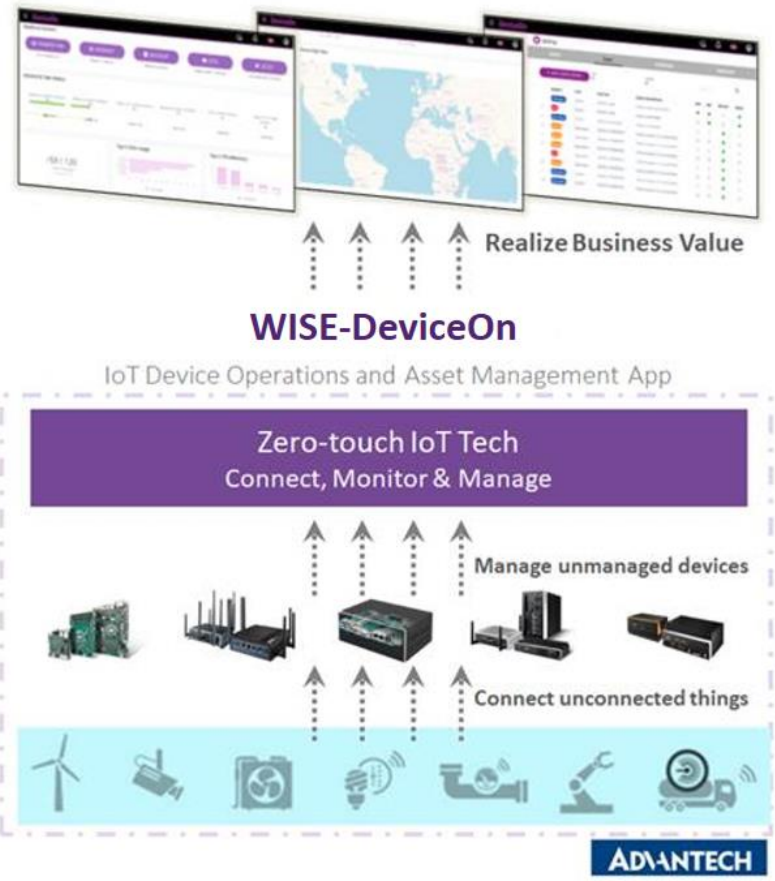
Revision History

Date	Version	Author	Reviewer	Description
2019-12-16	1.0.5	Sephiroth.Wang		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
2020-01-10	1.0.5	Wunhuei.Liou	Sephiroth.Wang	Section 5.3
2020-02-03	1.0.6	Sephiroth.Wang		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		Section 6.10
2020-03-11	1.0.6	Scott.Chang	Sephiroth.Wang	Section 6.3
2020-03-25	1.0.7	Sephiroth.Wang		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		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 development on RISC (Section 5.1.4)
2020-04-21	1.0.11	Listzt.Kao	Sephiroth.Wang	Add plugin development on Android (Section 5.1.5) Modify WISE-DeviceOn -> WISE-DeviceOn
2020-09-02	1.0.12	Sephiroth.Wang		Review all document and update new user interface for v-4.2.3
2020-09-09	1.0.13	Sephiroth.Wang		Add Telegram, Teams, Slack Notification Service (4.3.5 ~ 4.3.7)
2020-09-22	1.0.14	Sephiroth.Wang		Add Linux Agent Onboarding and Re-adjust catalog.
2020-10-27	1.0.15	Sephiroth.Wang		Remove data flow on FAQ and Update HTTPs for WebSocket.
2021-01-26	1.0.16	Sephiroth.Wang		Refactor document for v-4.3.3 released
2021-10-13	1.0.17	Sephiroth.Wang		Refactor document for v-4.4.2 released
2022-01-24	1.0.18	Sephiroth.Wang		Refactor document for v-4.5.2 released

Table of Contents

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.

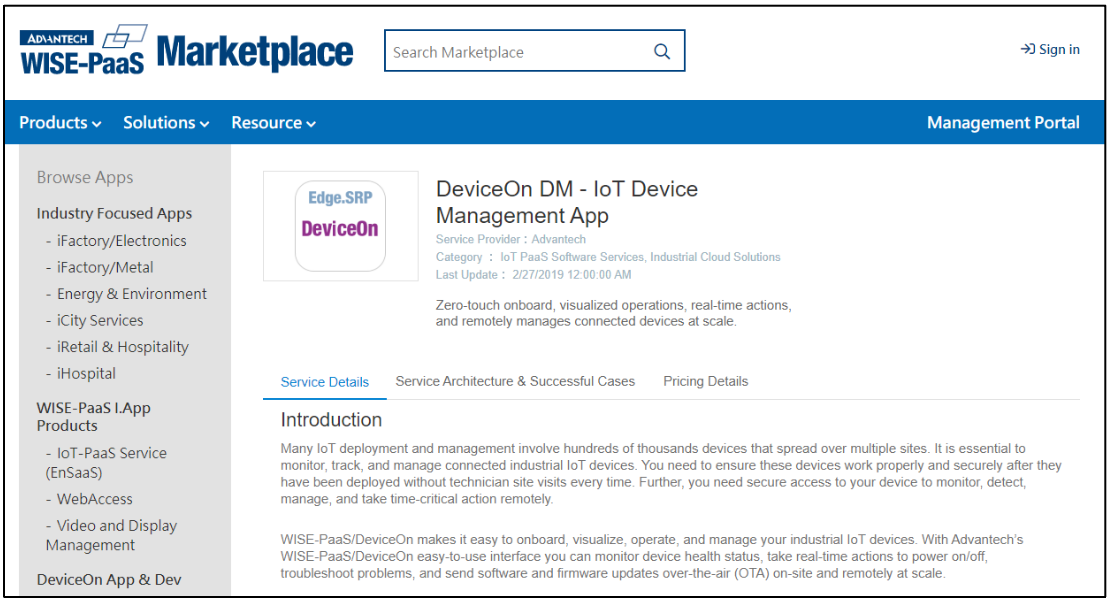

Realize Business Value
WISE-DeviceOn
IoT Device Operations and Asset Management App
Zero-touch IoT Tech
Connect, Monitor & Manage
Manage unmanaged devices
Connect unconnected things
ADVANTECH

With Advantech’s WISE-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-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-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-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-DeviceOn version on the WISE-PaaS Marketplace** and kick-start your new and improved device operations and management experience.



DeviceOn DM - 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.

Introduction

Many IoT deployment and management involve hundreds of thousands devices that spread over multiple sites. It is essential to monitor, track, and manage connected industrial IoT devices. You need to ensure these devices work properly and securely after they have been deployed without technician site visits every time. Further, you need secure access to your device to monitor, detect, manage, and take time-critical action remotely.

WISE-PaaS/DeviceOn makes it easy to onboard, visualize, operate, and manage your industrial IoT devices. With Advantech's WISE-PaaS/DeviceOn easy-to-use interface you can monitor device health status, take real-time actions to power on/off, troubleshoot problems, and send software and firmware updates over-the-air (OTA) on-site and remotely at scale.

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-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 LTSB (LTSB)**

- **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	●	●	●	●	●
	Two-Factor Authentication (2FA)	●	●	●	●	●
	LDAP & Azure AD Domain Service	●	●	●	●	●
	Device Zero-touch Onboarding	●	●	●	●	●
	Device & Device Group Management	●	●	●	●	●
	Device Threshold Detection (Rule-based Engine)	●	●	●	●	●
	Notification & Alert Service (Mail, SMS, LINE, WeChat, WhatsApp, Telegram, Teams, Slack)	●	●	●	●	●
	Device Real-time & Historical Data Monitoring	●	●	●	●	●
	App Store (OTA), Software, Firmware Provisioning	●	●	●	●	●
	Power Control, Terminal, Screenshot, Remote Desktop	●	●	●	◐	◐
	Backup/Recovery, Protection	●	●	●		
	Device Data with Zero-Downtime	●	●	●	●	●
	Process Monitoring & Control (Terminate, Restart, Launch)	●	●	●	●	●
	Container Management (Start, Stop, Monitoring)	●	●	●	●	●
	Operation Management (Batch Control & Statistical Analysis)	●	●	●	●	●
	Audio Volume Control	●	●			
	1-Click to Data Visualization	●	●	●	●	●
	Statics System Report	●	●	●	●	●

	Intel AMT Remote Control and Management	●	●	●		
	Intel IPMI Remote Control and Management	●	●	●		
	Device Map (Open street, Google, Baidu)	●	●	●	●	●
Advantech Hardware Support	Hardware Watchdog Monitoring	◍	●	◍		
	Hardware GPIO Control & Customized	●	●	●	●	●
	Brightness & Backlight Control	●	●	●	●	●
	Hardware Sensor Monitoring	●	●	●	◐	◐
	BIOS Update	●	●	●		
	Advantech Industrial SQ Flash/RAM Remote Management & Monitoring	●	●			
	Advantech iBMC, Out-of-Band Remote Management (Cross-network)	●	●	●		
	Advantech Industrial Display, On-Screen Display (OSD) Management	●	●	●		
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-4.2.x.** The standalone version comprises of IoTHub, database (PostgreSQL and MongoDB), Dashboard (Grafana), Webservices (Tomcat) and DeviceOn core applications.

1.2.1 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 ~ 6102 (v-4.3) 6083 ~ 6183 (v-4.2)

8	Database for MongoDB	27017
9	Database for PostgreSQL	5432
10	FTP Service	2121 [Depends on Installation] (v-4.3)

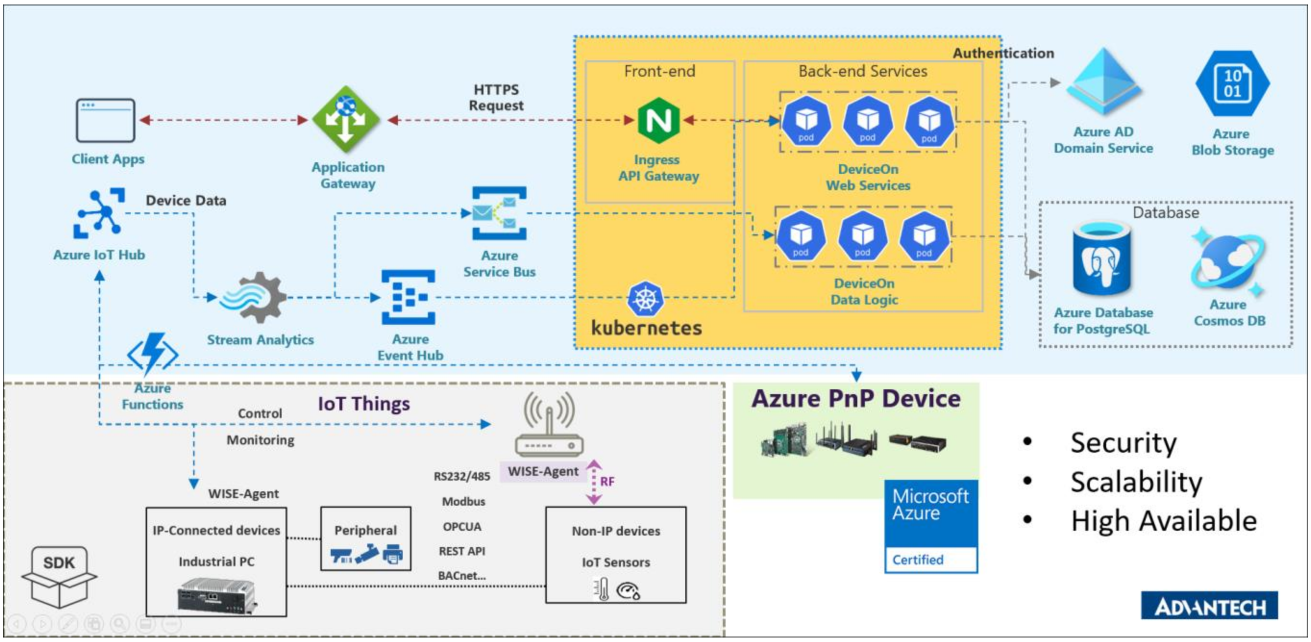
Hardware Minimum Requirements:

- ✓ **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)**

1.2.2 Azure PaaS, Kubernetes (Cloud)

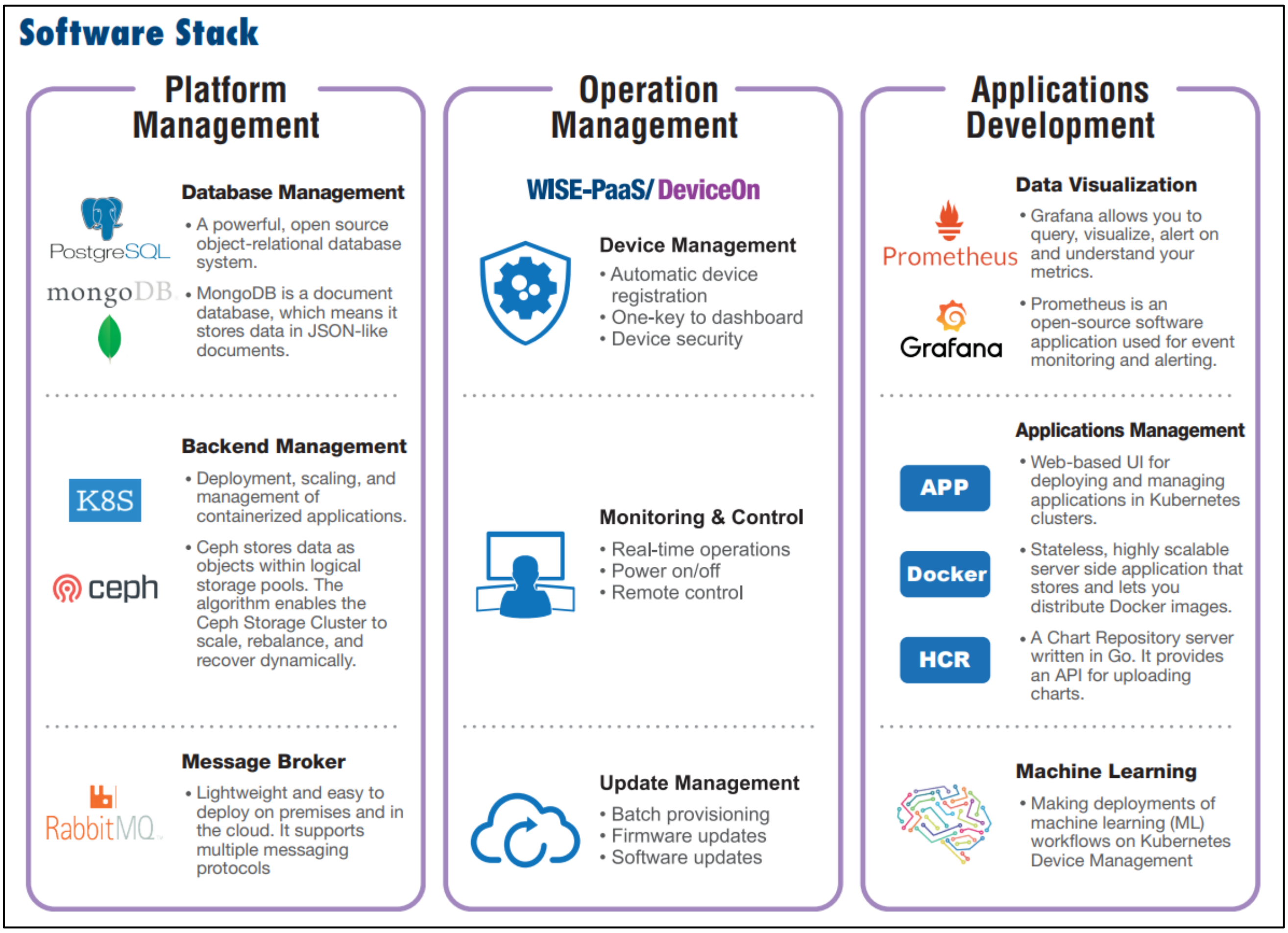
The Azure Kubernetes Service (AKS) makes it easy to deploy a managed Kubernetes cluster to Azure. AKS reduces the complexity and operational overhead of managing Kubernetes by offloading much of that responsibility to Azure. Azure handles critical tasks like health monitoring and maintenance for those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



Software Stack

Platform Management

Database Management

- A powerful, open source object-relational database system.
- MongoDB is a document database, which means it stores data in JSON-like documents.

Backend Management

- Deployment, scaling, and management of containerized applications.
- Ceph stores data as objects within logical storage pools. The algorithm enables the Ceph Storage Cluster to scale, rebalance, and recover dynamically.

Message Broker

- Lightweight and easy to deploy on premises and in the cloud. It supports multiple messaging protocols

Operation Management

WISE-PaaS/ DeviceOn

Device Management

- Automatic device registration
- One-key to dashboard
- Device security

Monitoring & Control

- Real-time operations
- Power on/off
- Remote control

Update Management

- Batch provisioning
- Firmware updates
- Software updates

Applications Development

Data Visualization

- Grafana allows you to query, visualize, alert on and understand your metrics.
- Prometheus is an open-source software application used for event monitoring and alerting.

Applications Management

- Web-based UI for deploying and managing applications in Kubernetes clusters.
- Stateless, highly scalable server side application that stores and lets you distribute Docker images.
- A Chart Repository server written in Go. It provides an API for uploading charts.

Machine Learning

- Making deployments of machine learning (ML) workflows on Kubernetes Device Management

Features:

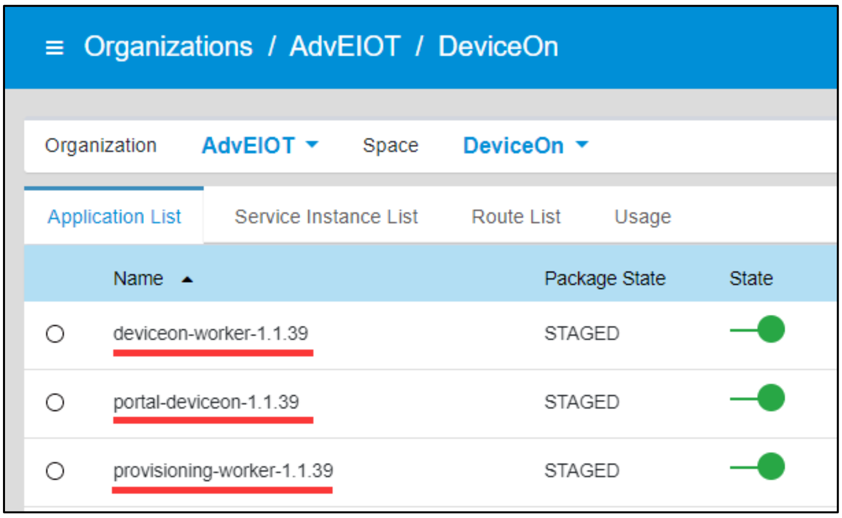
- Integrated solution (HW+SW bundle) for back-end data service and light private cloud
- Pre-configured system: Intel Xeon platform with 32GB RAM, 512GB mSATA SSD including Ubuntu Linux OS
- Open and flexible infrastructure: Kubernetes support, multiple database options, on-demand microservices
- Integrated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

- **WISE-DeviceOn inside for feature-rich IoT Device Management**

1.2.4 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.



	Name ▲	Package State	State
○	deviceon-worker-1.1.39	STAGED	●
○	portal-deviceon-1.1.39	STAGED	●
○	provisioning-worker-1.1.39	STAGED	●

1.3 DeviceOn Agent Version

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 Architecture

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

- **Core Framework** is the main library used to communicate with WISE-PaaS IoTHub or standard MQTT broker and include below components

1. Platform Profiler: describes the target platform (e.g., OS version, SN, Device name, MAC address)
2. Configuration: describes how to connect to MQTT broker (e.g., Credential URL, IoTKey, TLS/SSL settings)
3. Core Manager: integrates and manages the resources and keeps them alive.
4. Core Command: responsible for handling commands that interact with internal components (e.g., rename, update, get capability, auto report start/stop)
5. Plugin SDK: A plugin framework that makes plugin implement more easily.
6. Keep Alive: A component to detect the connection between WISE-Agent and DeviceOn Server.
7. Data Synchronization: kernel plugin that caches and restores data to ensure zero downtime.
8. Rule Engine: kernel plugin that supports the threshold rule check and then sends event or trigger actions
9. Plugin Loader: responsible for loading and managing plugins indicated in **module_config.xml**

- **The plugins** include IPC monitoring (Advantech Hardware, HDD/SSD, Networks, Process…etc.), control function (Backup/Recovery, Protection, Remote Desktop, Terminal…), and sensor protocol collection.

Agent Plugin	Description
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.

Agent Plugin	Description
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
Local Provision Plugin	Similar to UPnP mechanism, provides device fast onboarding on local network.

1.3.2 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 SP1/8/10 32-bit/64-bit**
- ✓ **Ubuntu 16.04, 18.04, 20.04 x64**
- ✓ **CentOS 7.6, 8.2 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

System security is about not only installing and onboarding devices and networks securely but also managing their ongoing operations throughout their lifecycle and identifying and isolating any threats. Industries everywhere are digitizing, which is creating a multitude of new security requirements for the Internet of Things (IoT). End-to-end (E2E) security management will be essential to ensuring security and privacy in the IoT, while simultaneously building strong identities and maintaining trust. As the diversity of IoT services and the number of connected devices continue to increase, the threats to IoT systems are changing and growing even faster.

A comprehensive model of IoT device security, as shown in below structure, the comprehensive IoT module security in an IoT system has three main parts:

A. **Device Security**

DeviceOn leverage **McAfee Embedded Security** software to prevents unauthorized changes and will lock a system down to a known application is an industry, that's an industrial first solution to secure embedded devices.

For disaster recovery, **Acronis** provides users a quick and easy-operated solution to protect data and recover the entire system even when OS crash, effectively reduces down-time cost and lowers the risk of data loss.

B. **Secure Transport**

The server distributed SSL certificates to use SSL/TLS (v-1.3) as an encrypted and secure data transmission channel, and device default enable MQTT-SSL for communication.

- **Topics Isolation & Unique Device IoT Key**

  Topics are specially handled in RabbitMQ. Topics are not public. Access control isolates an activated device to publishing/subscribing only to that device’s topics even though multiple devices will have subscriptions to identically named topics. A device is not allowed to subscribe/publish to another device’s topics.

  Second, in IoT applications, command topics are used to control a device remotely and to acknowledge successful command executions. Unlike telemetry, command topics are not read-only. Commands are a back and forth workflow that can occur **between the cloud and devices**. Because commands are actionable messages, **isolate the MQTT topic for command messages from telemetry topics.**

- **Use x.509 Certificates to Authenticate Edge Device**

  DeviceOn supports x.509 certificate authentication for use with a secure TLS/SSL connection. The x.509 edge device authentication **allows device to authenticate to servers with certificates rather than with a username and password.**

- **Use TPM + x.509 Certificates to Provide Higher Security**

  The solution that we integrate on DeviceOn for Azure (Enterprise Edition), leverage Azure IoT Edge and TPM 2.0 to offer secure authentication and private key protected.

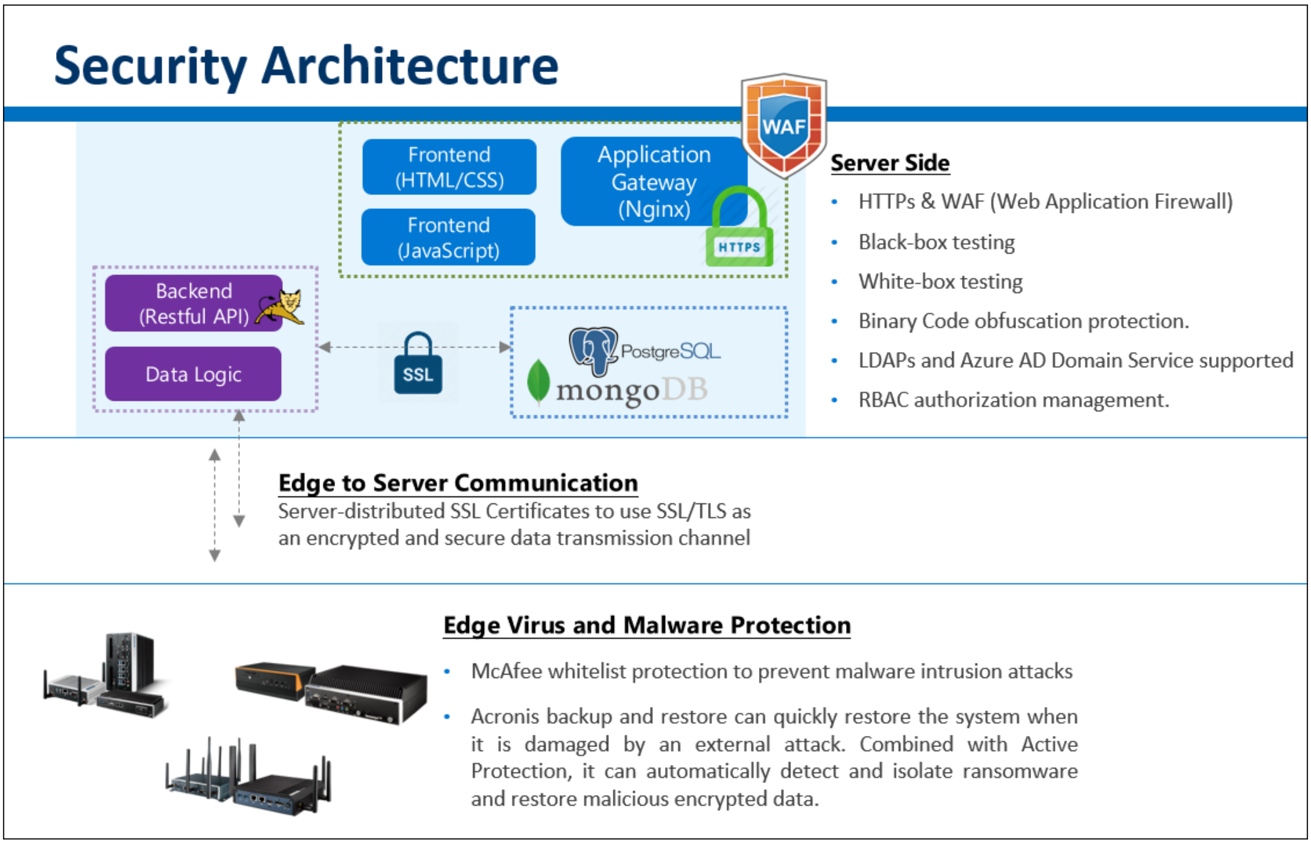
  TPM, also known as ISO/IEC 11889, is a standard for securely generating and storing cryptographic keys. TPM also refers to a virtual or physical I/O device that interacts with modules that implement the standard. A TPM device can exist as discrete hardware, integrated hardware, a firmware-based module, or a software-based module.

C. Secure Cloud Service

The cloud service components include Tomcat as a web server that provide an HTTPS protocol and backend APIs services, each connection between backend and database adopt SSL encryption, and enforce password policies, refer to Section 1.4.2 for details. Second, for advanced attack, such as SQL injection, XXC, local and remote file vulnerabilities, the **Nginx+Naxsi** to achieve Web Application firewall (WAF) protection.

All DeviceOn services pass through famous vulnerability tools (refer to Section 1.4.3) to ensure security for your it IoT solutions, and the binary uses **ProGuard** code obfuscation protection.

The APIs authentication not only uses JWT (JSON Web Tokens) to hide/encrypt sensitive data, but, integrate LDAP & Azure AD Domain Service for secure.



Security Architecture

Server Side

- HTTPs & WAF (Web Application Firewall)
- Black-box testing
- White-box testing
- Binary Code obfuscation protection.
- LDAPs and Azure AD Domain Service supported
- RBAC authorization management.

Edge to Server Communication

Server-distributed SSL Certificates to use SSL/TLS as an encrypted and secure data transmission channel

Edge Virus and Malware Protection

- McAfee whitelist protection to prevent malware intrusion attacks
- Acronis backup and restore can quickly restore the system when it is damaged by an external attack. Combined with Active Protection, it can automatically detect and isolate ransomware and restore malicious encrypted data.

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/TLS 1.3**

  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 Vulnerability Scanning Tools

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

- **OWASP ZAP**

  The OWASP Zed Attack Proxy (ZAP) is one of the world’s most popular free security tools and is actively maintained by hundreds of international volunteers*. It can help you automatically find security vulnerabilities in your web applications while you are developing and testing your applications. It's also a great tool for experienced pen testers to use for manual security testing.

- **Skipfish**

  Skipfish is an active web application security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

  Key features:

  ✓ High speed: pure C code, highly optimized HTTP handling, minimal CPU footprint – easily achieving 2000 requests per second with responsive targets.

  ✓ Ease of use: heuristics to support a variety of quirky web frameworks and mixed-technology sites, with automatic learning capabilities, on-the-fly wordlist creation, and form auto completion.

  ✓ Cutting-edge security logic: high quality, low false positive, differential security checks, capable of spotting a range of subtle flaws, including blind injection vectors.

- **Nikto**

  Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

- **W3af**

  w3af is a **Web Application Attack and Audit Framework**. The project's goal is to create a framework to help you secure your web applications by finding and exploiting all web application vulnerabilities.

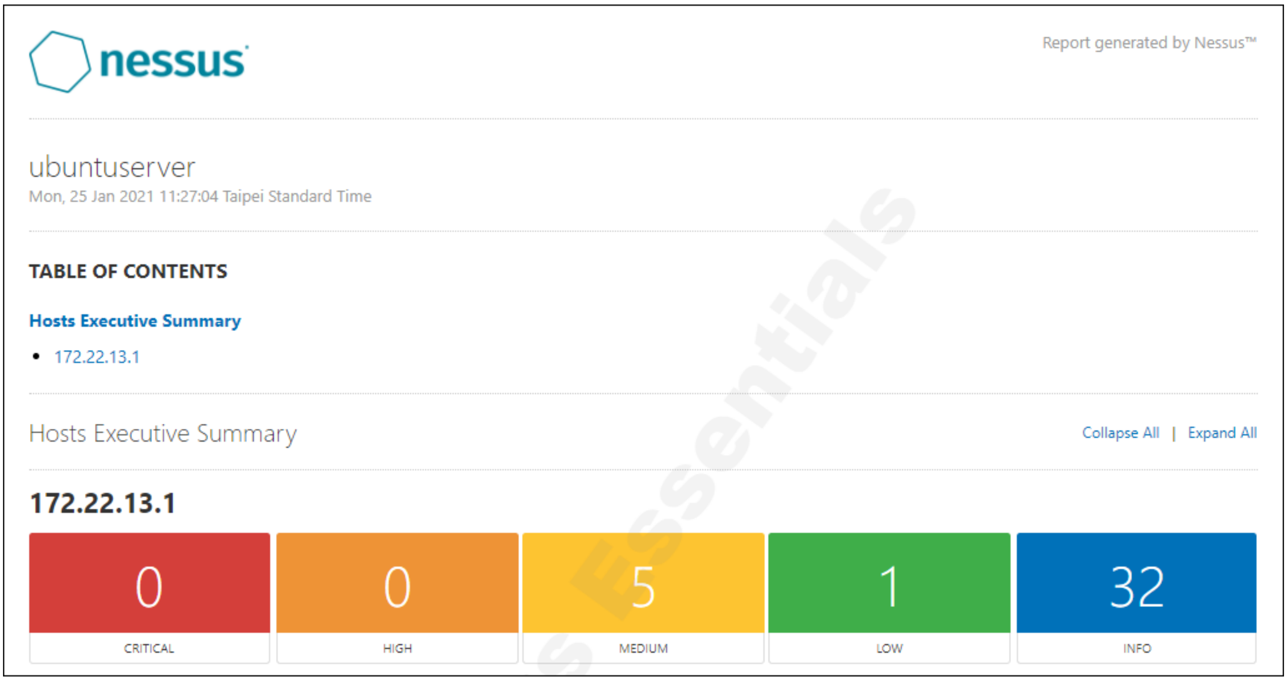
- **Arachni**

  Arachni is a fully featured web security scanning tool, it is based on ruby framework. It is an open source, modular and high-performance tool. It comes with both command line interface as well as web based gui interface, it is highly versatile tool for security scanning purpose. It supports almost all of the popular web application such as HTML5, Java Script and AJAX etc, additionally it is enables with multi user-multi platform collaboration. It allows you to generate reports in desired format (.txt, XML, HTML).

1.4.4 Third-Party Vulnerability Fixed and Updates

- OpenJRE (v-1.8.0_292-1)
  CVE-2021-2161, CVE-2021-2163
- Tomcat (v-9.0.50)
  CVE-2021-33037, CVE-2021-30640, CVE-2021-30639, CVE-2020-9484, CVE-2021-25329, CVE-2021-25122
- RabbitMQ (v-3.8.19), Erlang 24
  CVE-2021-32719, CVE-2021-32718, CVE-2021-22116, CVE-2021-22117
- PostgreSQL (v-10.17)
  CVE-2021-32027, CVE-2021-32028, CVE-2021-32029
- MongoDB (v-4.2.15)
- Grafana (v-7.3.10)
  CVE-2021-28146, CVE-2021-28147, CVE-2021-28148

1.4.5 Scanned Report



nessus

Report generated by Nessus™

ubuntuserver
Mon, 25 Jan 2021 11:27:04 Taipei Standard Time

TABLE OF CONTENTS

Hosts Executive Summary

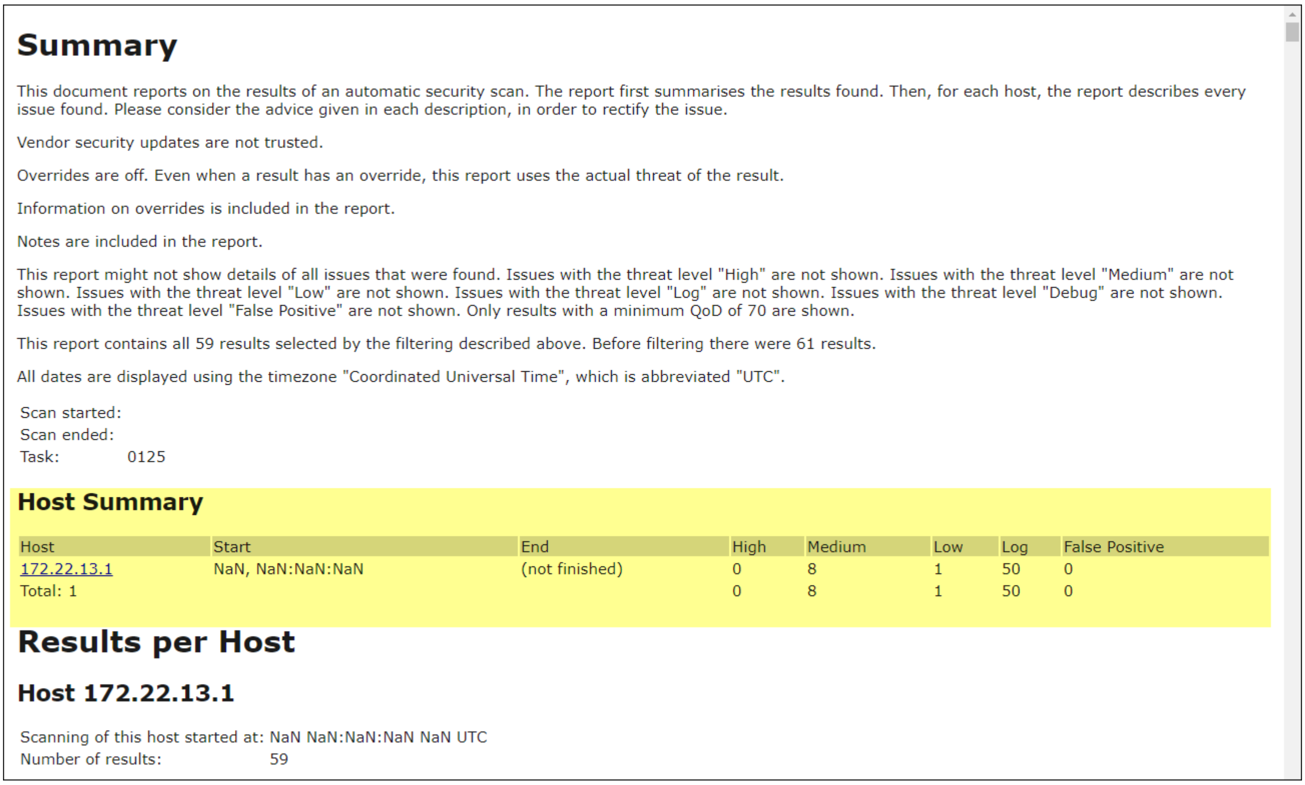
- 172.22.13.1

Hosts Executive Summary

Collapse All | Expand All

172.22.13.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	5	1	32



Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Vendor security updates are not trusted.

Overrides are off. Even when a result has an override, this report uses the actual threat of the result.

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found. Issues with the threat level "High" are not shown. Issues with the threat level "Medium" are not shown. Issues with the threat level "Low" are not shown. Issues with the threat level "Log" are not shown. Issues with the threat level "Debug" are not shown. Issues with the threat level "False Positive" are not shown. Only results with a minimum QoD of 70 are shown.

This report contains all 59 results selected by the filtering described above. Before filtering there were 61 results.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started:
Scan ended:
Task: 0125

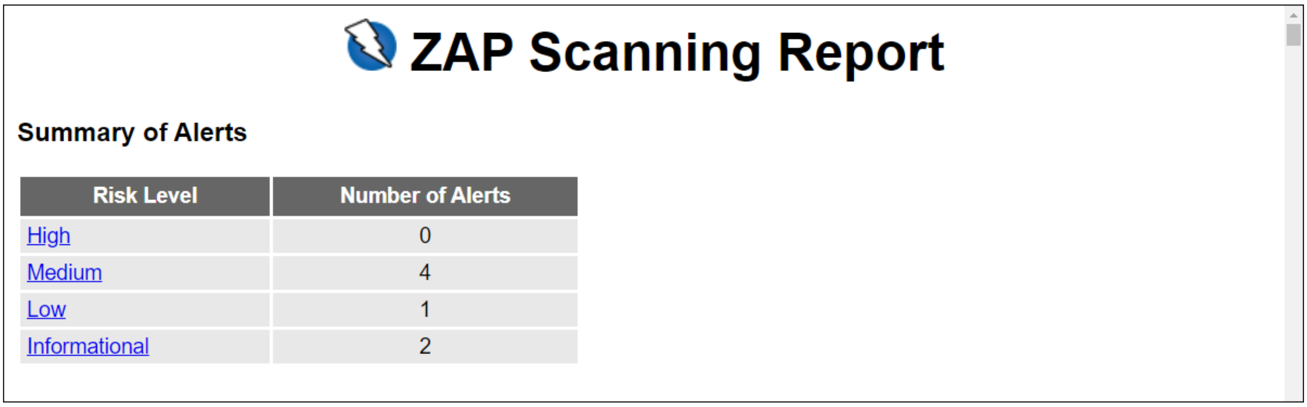
Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
172.22.13.1	NaN, NaN:NaN:NaN	(not finished)	0	8	1	50	0
Total: 1			0	8	1	50	0

Results per Host

Host 172.22.13.1

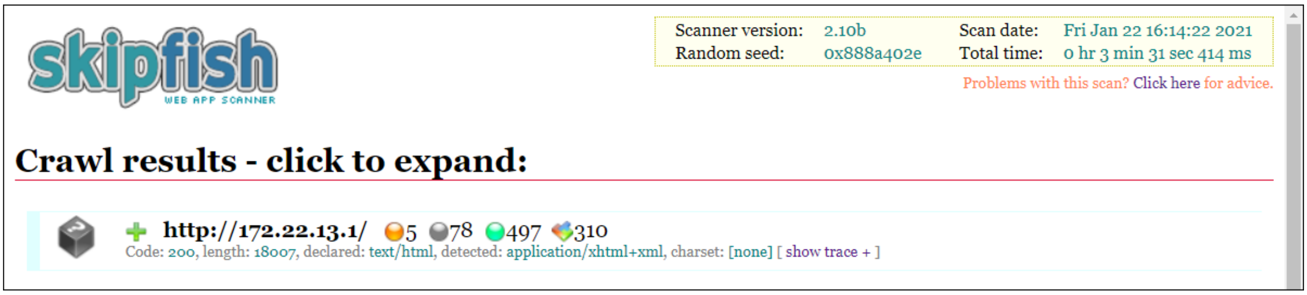
Scanning of this host started at: NaN NaN:NaN:NaN NaN UTC
Number of results: 59



ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	1
Informational	2



Scanner version:	2.10b	Scan date:	Fri Jan 22 16:14:22 2021
Random seed:	0x888a402e	Total time:	0 hr 3 min 31 sec 414 ms

Problems with this scan? Click here for advice.

Crawl results - click to expand:

http://172.22.13.1/ ●5 ●78 ●497 310
Code: 200, length: 18007, declared: text/html, detected: application/xhtml+xml, charset: [none] [show trace +]

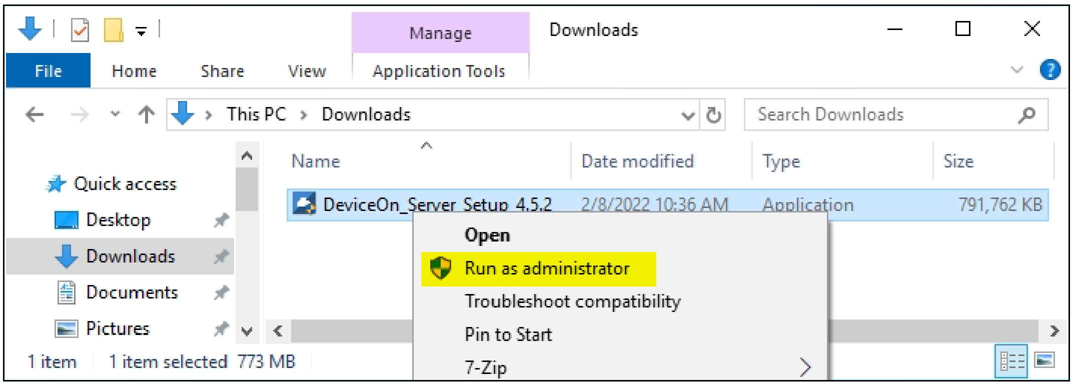
2. Getting Started

2.1 DeviceOn Cloud Installation

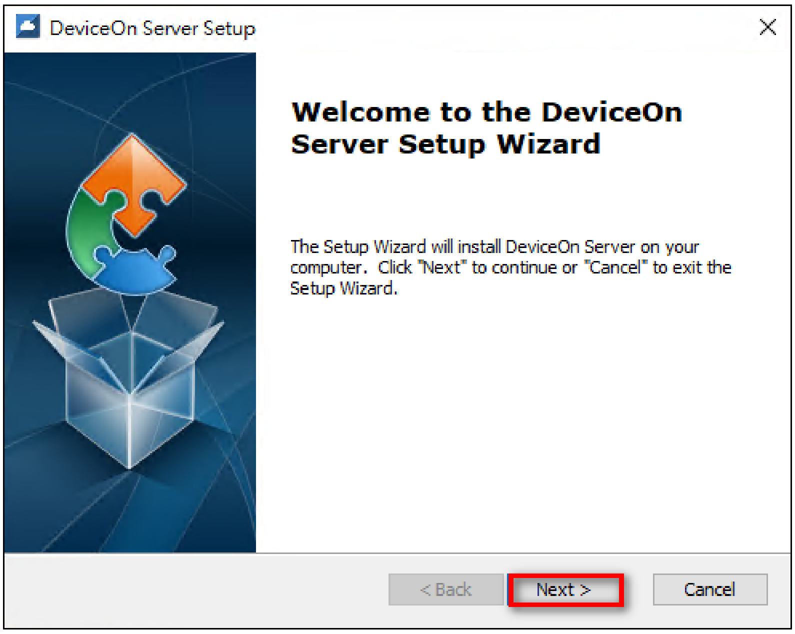
2.1.1 Setup Standalone Version (On-premise)

Step 1: Install the DeviceOn package on your system

Copy the installation file (**DeviceOn_Server_Setup_4.5.x.exe**) to your target system and run it as administrator.



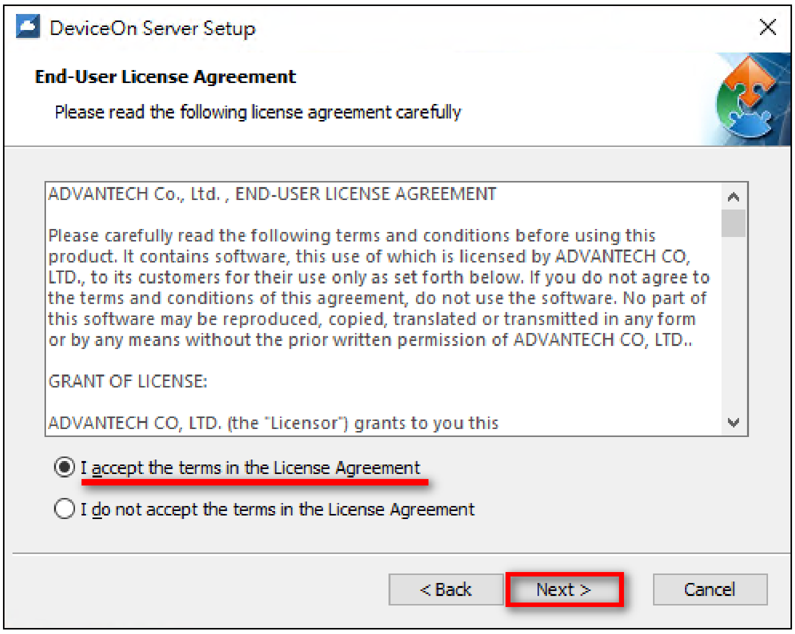
Click “**Next”** to start the installation process.



Welcome to the DeviceOn Server Setup Wizard

The Setup Wizard will install DeviceOn Server on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

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


DeviceOn Server Setup

End-User License Agreement

Please read the following license agreement carefully

ADVANTECH Co., Ltd. , END-USER LICENSE AGREEMENT

Please carefully read the following terms and conditions before using this product. It contains software, this use of which is licensed by ADVANTECH CO, LTD., to its customers for their use only as set forth below. If you do not agree to the terms and conditions of this agreement, do not use the software. No part of this software may be reproduced, copied, translated or transmitted in any form or by any means without the prior written permission of ADVANTECH CO, LTD..

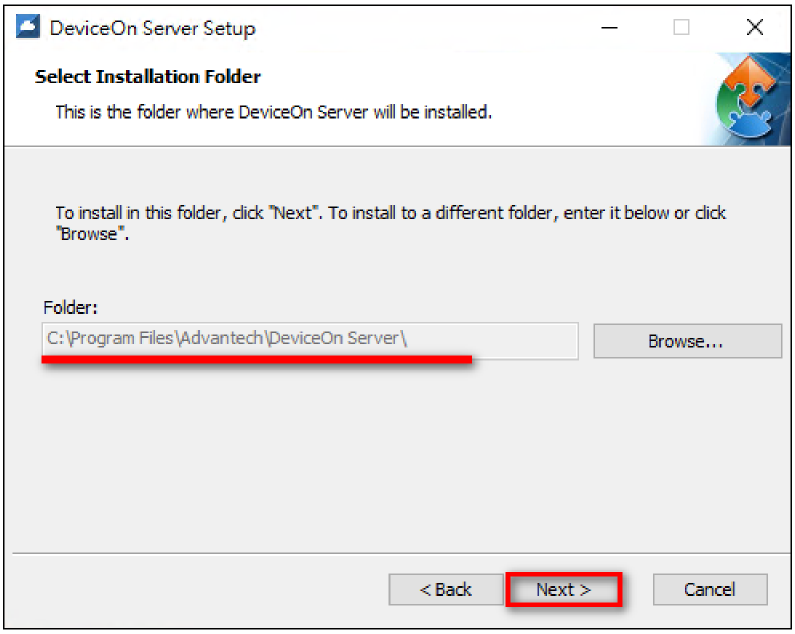
GRANT OF LICENSE:

ADVANTECH CO, LTD. (the "Licensor") grants to you this

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

Select the "**Installation Folder**" for DeviceOn Server and click "**Next**"


DeviceOn Server Setup

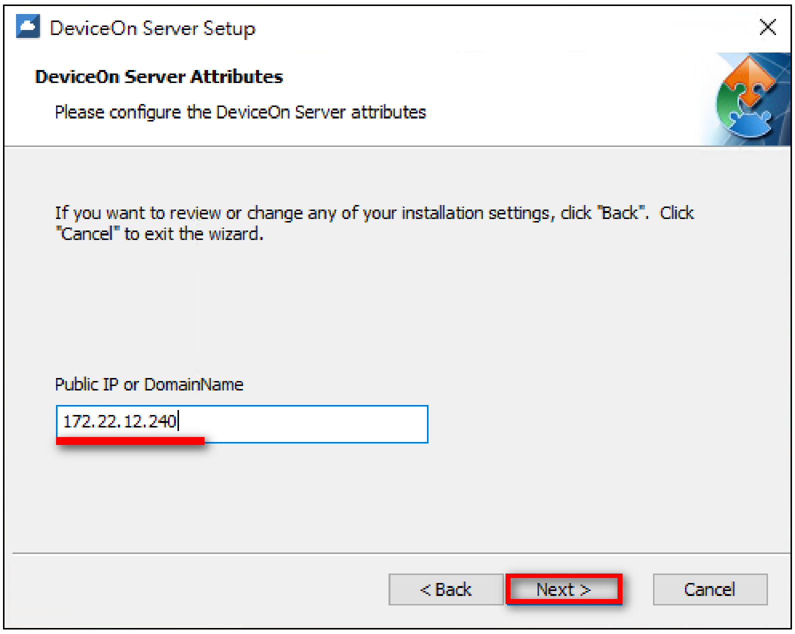
Select Installation Folder

This is the folder where DeviceOn Server will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\Advantech\DeviceOn Server\

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.



DeviceOn Server Setup

DeviceOn Server Attributes

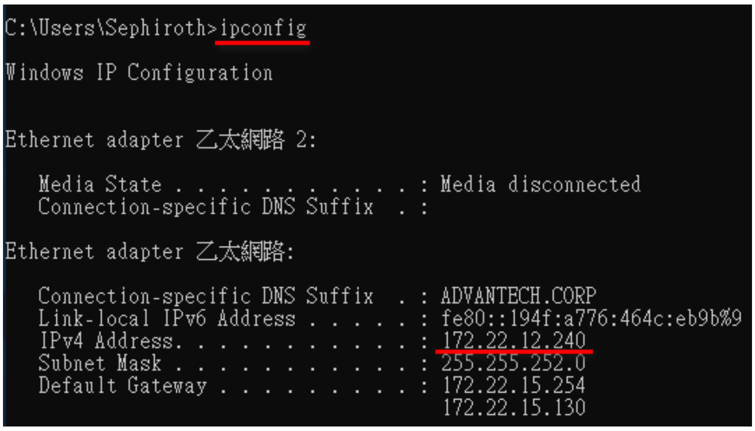
Please configure the DeviceOn Server attributes

If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Public IP or DomainName

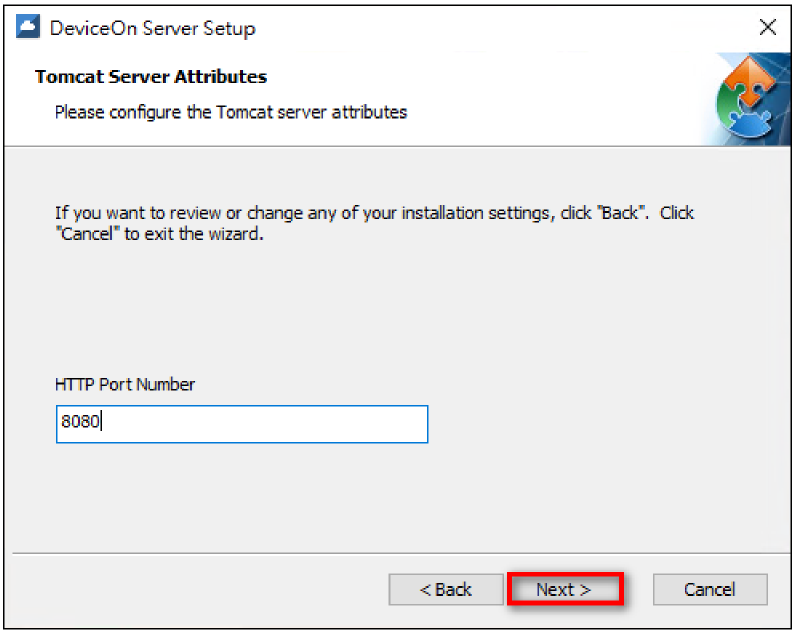
172.22.12.240

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**”.



DeviceOn Server Setup

Tomcat Server Attributes

Please configure the Tomcat server attributes

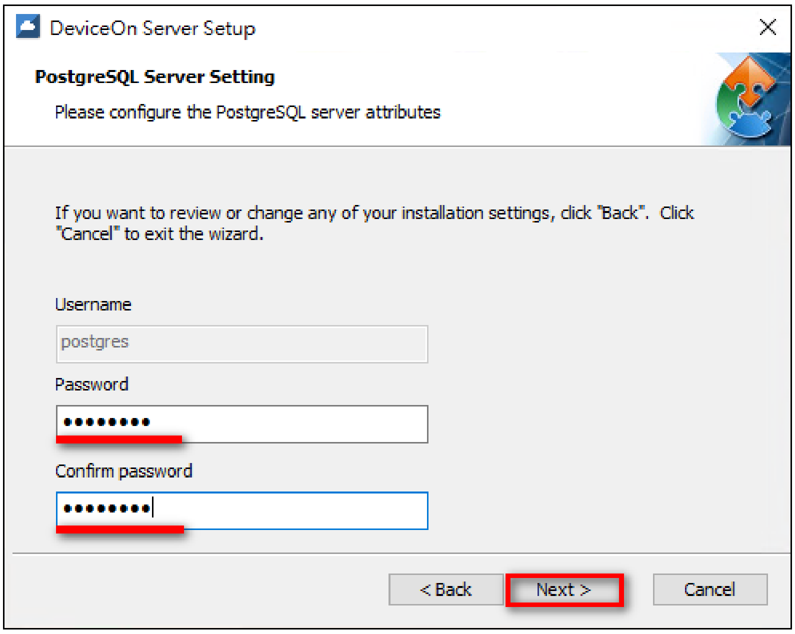
If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

HTTP Port Number: 8080

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)



DeviceOn Server Setup

PostgreSQL Server Setting

Please configure the PostgreSQL server attributes

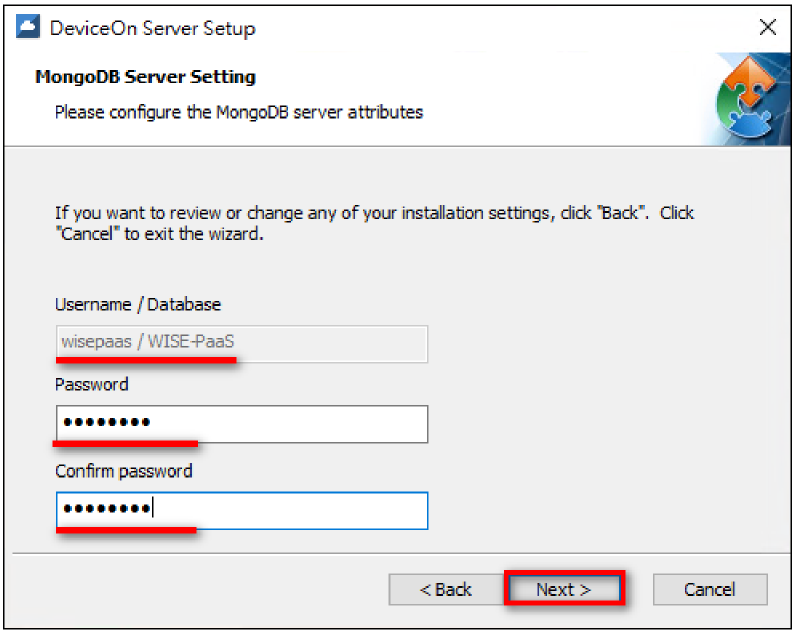
If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Username: postgres

Password: ••••••••

Confirm password: ••••••••

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.



MongoDB Server Setting

Please configure the MongoDB server attributes

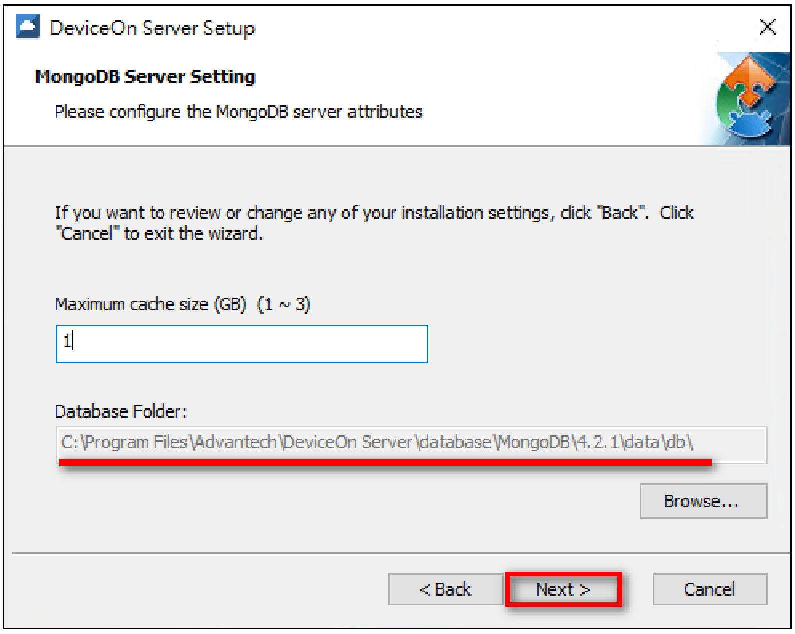
If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Username / Database: wisepaas / WISE-PaaS

Password: ••••••••

Confirm password: ••••••••

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 referend to the official documentation.



MongoDB Server Setting

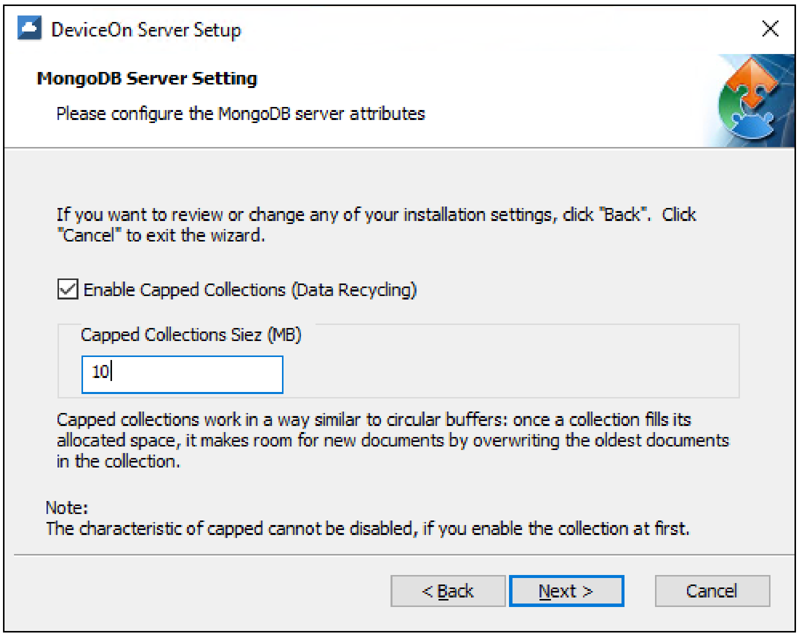
Please configure the MongoDB server attributes

If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Maximum cache size (GB) (1 ~ 3): 1

Database Folder: C:\Program Files\Advantech\DeviceOn Server\database\MongoDB\4.2.1\data\db\

In order to avoid the hard disk space being used up by device data, the MongoDB provide a capped mechanism, that 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. **Please note, the characteristic of capped cannot be disable, if you enable the collection at first.**



DeviceOn Server Setup

MongoDB Server Setting

Please configure the MongoDB server attributes

If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

☑ Enable Capped Collections (Data Recycling)

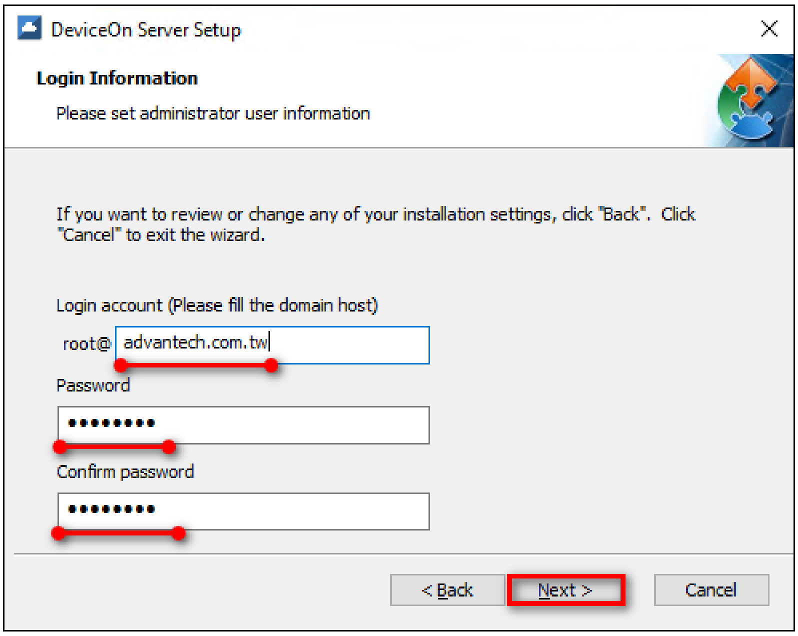
Capped Collections Siez (MB)

10

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.

Note:
The characteristic of capped cannot be disabled, if you enable the collection at first.

Configure the password and suffix domain of the root account (dummy name “root@”) 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.



DeviceOn Server Setup

Login Information

Please set administrator user information

If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Login account (Please fill the domain host)

root@ advantech.com.tw

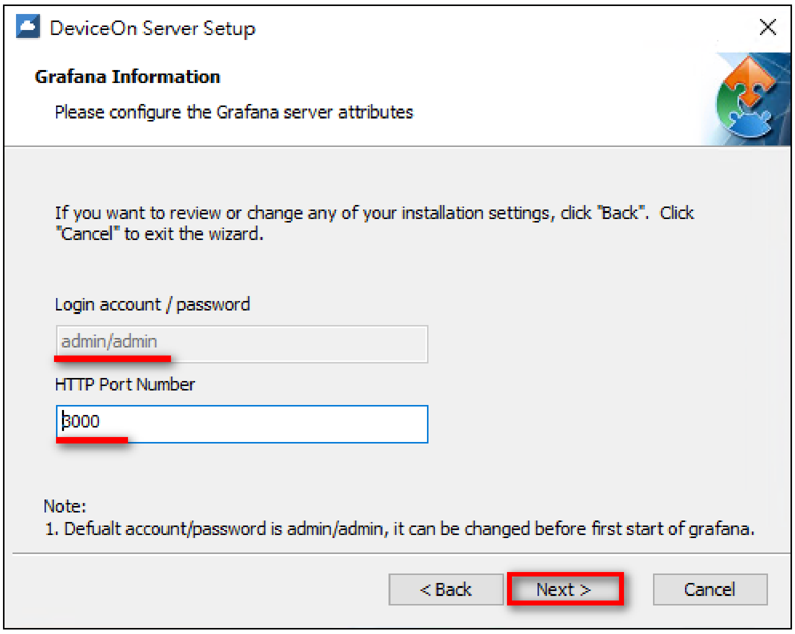
Password

••••••••

Confirm password

••••••••

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


DeviceOn Server Setup

Grafana Information

Please configure the Grafana server attributes

If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Login account / password

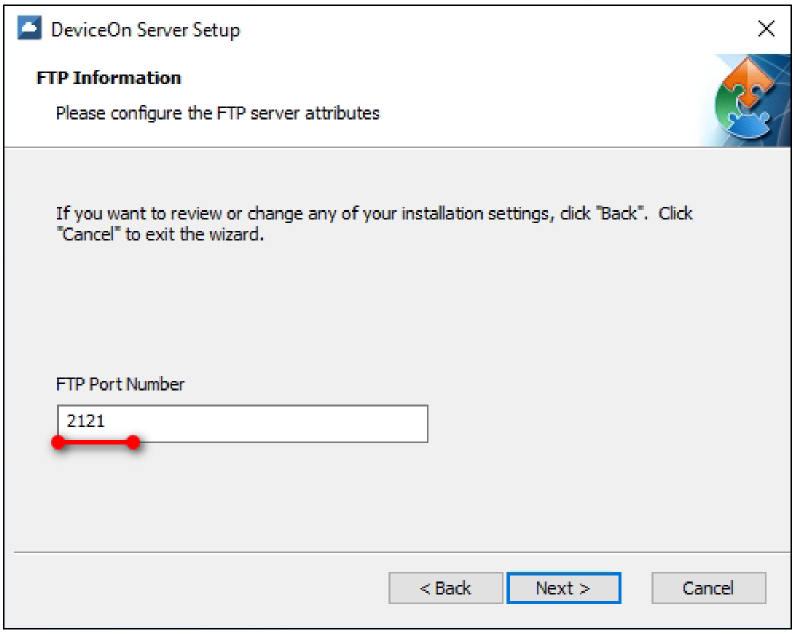
admin/admin

HTTP Port Number

3000

Note:
1. Defualt account/password is admin/admin, it can be changed before first start of grafana.

Set up the FTP service port for OTA default storage, the default port is 2121, but you can select any other port as long as it does not conflict with any other application or service. Click “**Next**”.


DeviceOn Server Setup

FTP Information

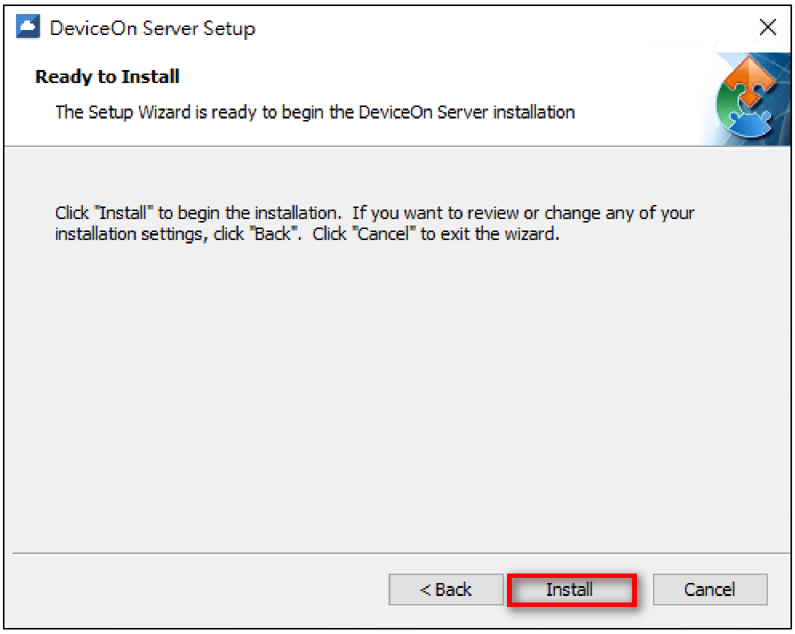
Please configure the FTP server attributes

If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

FTP Port Number

2121

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



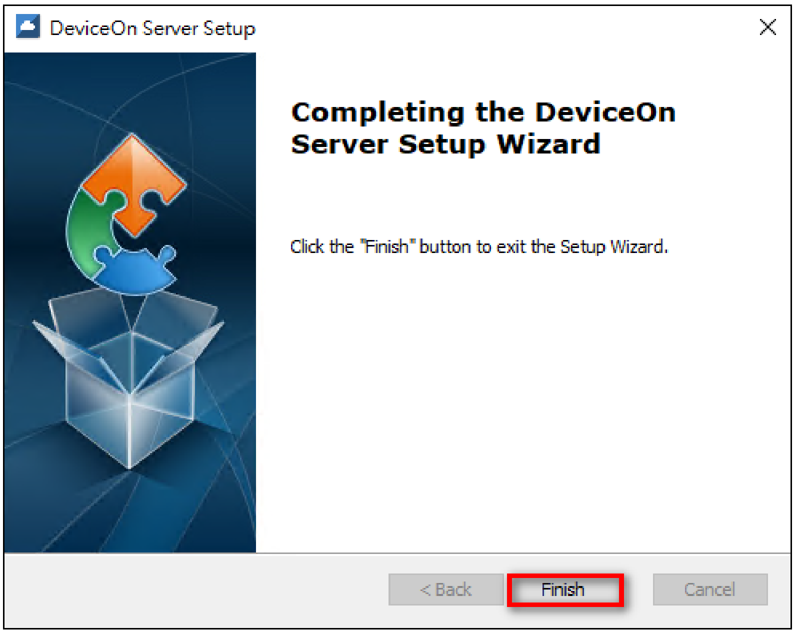
DeviceOn Server Setup

Ready to Install

The Setup Wizard is ready to begin the DeviceOn Server installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

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



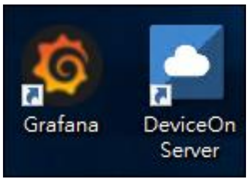
DeviceOn Server Setup

Completing the DeviceOn Server Setup Wizard

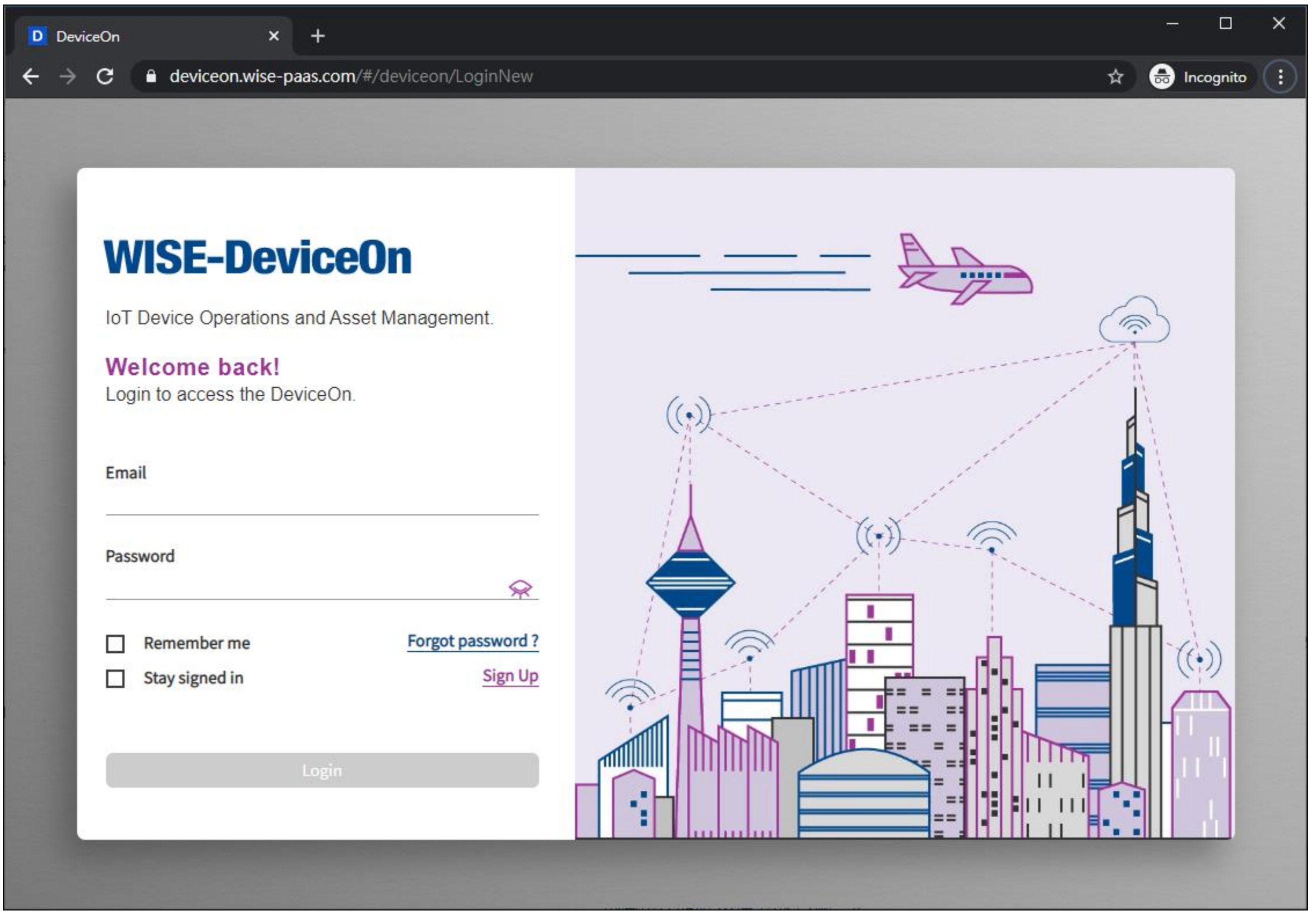
Click the "Finish" button to exit the Setup Wizard.

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.



WISE-DeviceOn

IoT Device Operations and Asset Management.

Welcome back!

Login to access the DeviceOn.

Email

Password

□ Remember me

□ Stay signed in

Forgot password ?

Sign Up

Login

2.1.2 Setup 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_4.5.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_4.5.x.run**" so that the installer as an executable file under Ubuntu Linux.

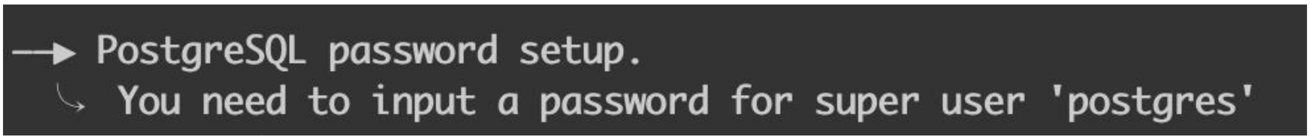
Step 4: Running the installer

Change your working directory to where the installer is and run "**./ DeviceOn_Server_Ubuntu 18.04_x64_4.5.x.run** ". You may need to run "**sudo ./ DeviceOn_Server_Ubuntu 18.04_x64_4.5.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:

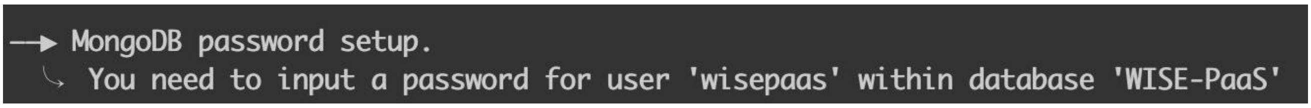
A. The password of user "**postgres**" to login PostgreSQL database.



```
—▶ 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.

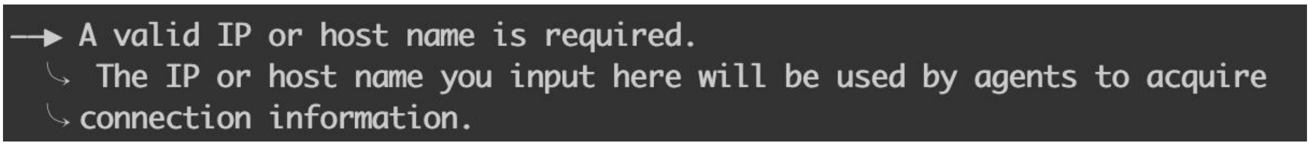
B. The password of user "**wisepaas**" to login MongoDB database.



```
—▶ 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.

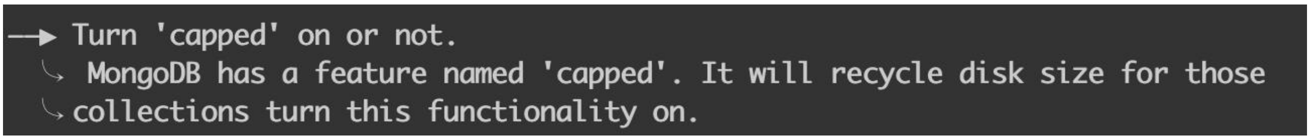
C. The valid IP or host name of the target host.



```
—▶ 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.
```

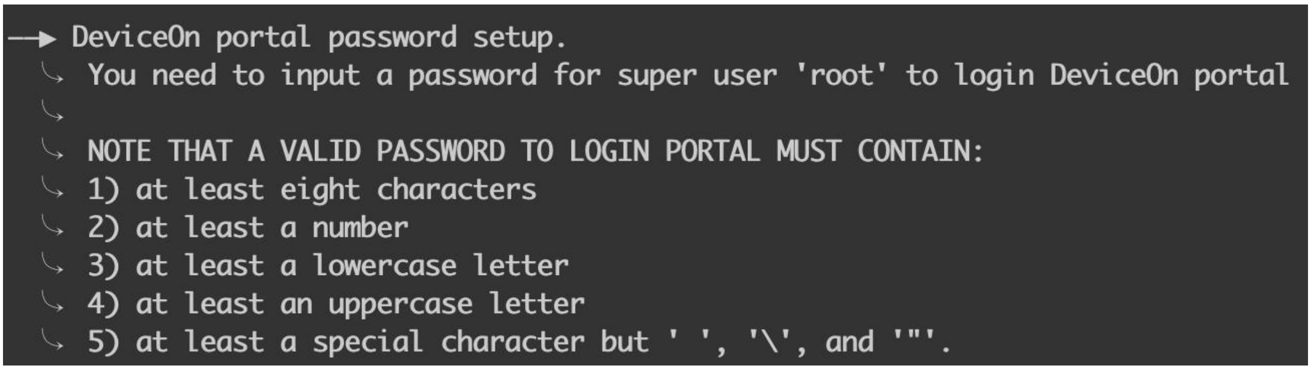
When you run into this step the question shows like above. Just input “**yes**” or “**no**” to enable or disable “capped” functionality. If you answer “yes”, a subsequent question followed to ask you “how much capped size, in MB, to be used? “. Just input the size, in MB, you want to use in “capped” 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.

2.1.3 Deploy DeviceOn for Azure (Enterprise Edition)

Prerequisites

To achieve the goal to deploy WISE-DeviceOn, some resources must be acquired and preconditions must be met as well.

- An active Azure subscription.
- An **Azure CLI** installed on your laptop, please refer to Azure documentation to download and

setup. The Azure CLI is available to install in Windows, macOS and Linux environments. It can also be run in a Docker container and Azure Cloud Shell.

Second option, if you don't want to install Azure CLI, you can also adopt **Azure Cloud Shell**, please refer to Microsoft documentation.

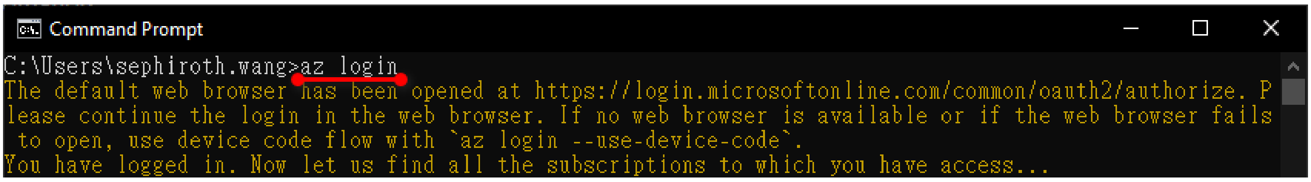
Step 1: Obtain the following three parameters for deployment

- Application ID
- Password (Client Secrets)
- Tenant ID

A. Sign into your Azure account through Azure CLI

Use any way you prefer to open a Command Prompt and enter

```
az login
```



```
C:\Users\sephiroth.wang>az login
The default web browser has been opened at https://login.microsoftonline.com/common/oauth2/authorize. P
lease continue the login in the web browser. If no web browser is available or if the web browser fails
 to open, use device code flow with `az login --use-device-code`.
You have logged in. Now let us find all the subscriptions to which you have access...
```

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.

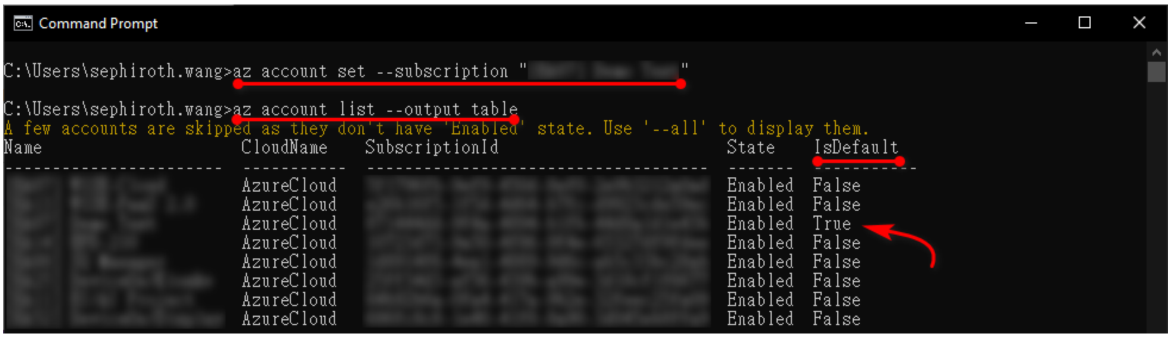
B. Select your Subscription

After you login, the terminal console will list all subscriptions, please select the subscription that you would like to deploy.

```
az account set --subscription <SUBSCRIPTION_NAME>
```

If you don't know which subscriptions you have, you can use below command to list all the subscriptions and determine whether the subscription has been selected according to isDefault.

```
az account list --output table
```

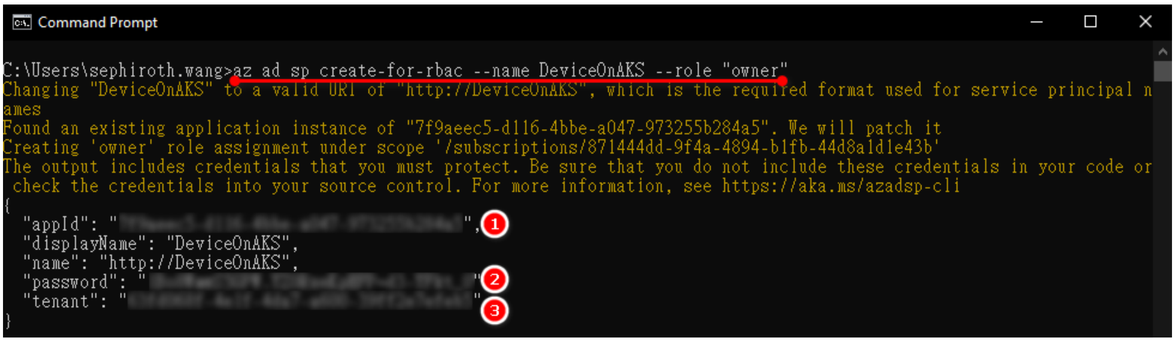


```
C:\Users\sephiroth.wang>az account set --subscription "[redacted]"

C:\Users\sephiroth.wang>az account list --output table
A few accounts are skipped as they don't have 'Enabled' state. Use '--all' to display them.
Name                    CloudName    SubscriptionId                        State     IsDefault
----------------------  -----------  ------------------------------------  --------  -----------
[redacted]              AzureCloud   [redacted]                            Enabled   False
[redacted]              AzureCloud   [redacted]                            Enabled   False
[redacted]              AzureCloud   [redacted]                            Enabled   True
[redacted]              AzureCloud   [redacted]                            Enabled   False
[redacted]              AzureCloud   [redacted]                            Enabled   False
[redacted]              AzureCloud   [redacted]                            Enabled   False
[redacted]              AzureCloud   [redacted]                            Enabled   False
[redacted]              AzureCloud   [redacted]                            Enabled   False
```

C. Select your Subscription

The last step to create a service principal and generate these parameters. (**1. Application ID, 2. Password and 3. Tenant ID**)

```
az ad sp create-for-rbac --name <SERVICE_PRINCIPAL_NAME> --role "owner"
```



```
C:\Users\sephiroth.wang>az ad sp create-for-rbac --name DeviceOnAKS --role "owner"
Changing "DeviceOnAKS" to a valid URI of "http://DeviceOnAKS", which is the required format used for service principal n
ames
Found an existing application instance of "7f9aeec5-d116-4bbe-a047-973255b284a5". We will patch it
Creating 'owner' role assignment under scope '/subscriptions/871444dd-9f4a-4894-b1fb-44d8a1d1e43b'
The output includes credentials that you must protect. Be sure that you do not include these credentials in your code or
 check the credentials into your source control. For more information, see https://aka.ms/azadsp-cli
{
  "appId": "[redacted]",
  "displayName": "DeviceOnAKS",
  "name": "http://DeviceOnAKS",
  "password": "[redacted]"
  "tenant": "[redacted]"
}
```

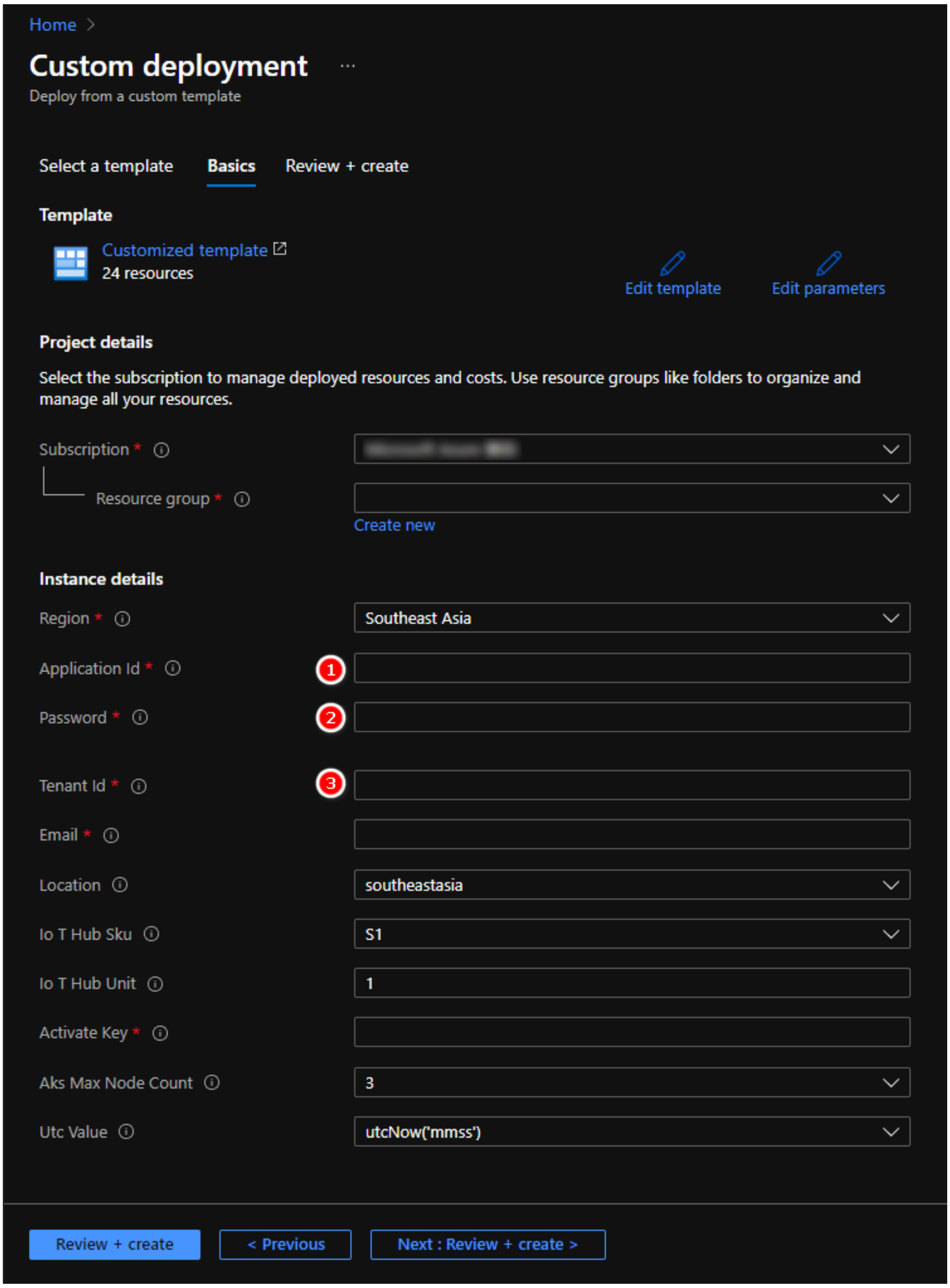
If you want to further limit the scope of service principle to resource group, please try to create the resource group, and then use the following command to limit.

```
az ad sp create-for-rbac --name <SERVICE_PRINCIPAL_NAME> --role "owner" --scopes /subscriptions/{SubID}/resourceGroups/{ResourceGroup1}
```

Step 2: Deploy WISE-DeviceOn via Custom Template

Deploy to Azure

A. This will open the Azure Portal (portal.azure.com) in your subscription and create the required resources.



Home >

Custom deployment ···

Deploy from a custom template

Select a template | **Basics** | Review + create

Template

Customized template
24 resources

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	[redacted]
Resource group *	
	Create new

Instance details

Region *	Southeast Asia
Application Id * ①	
Password * ②	
Tenant Id * ③	
Email *	
Location	southeastasia
Io T Hub Sku	S1
Io T Hub Unit	1
Activate Key *	
Aks Max Node Count	3
Utc Value	utcNow('mmss')

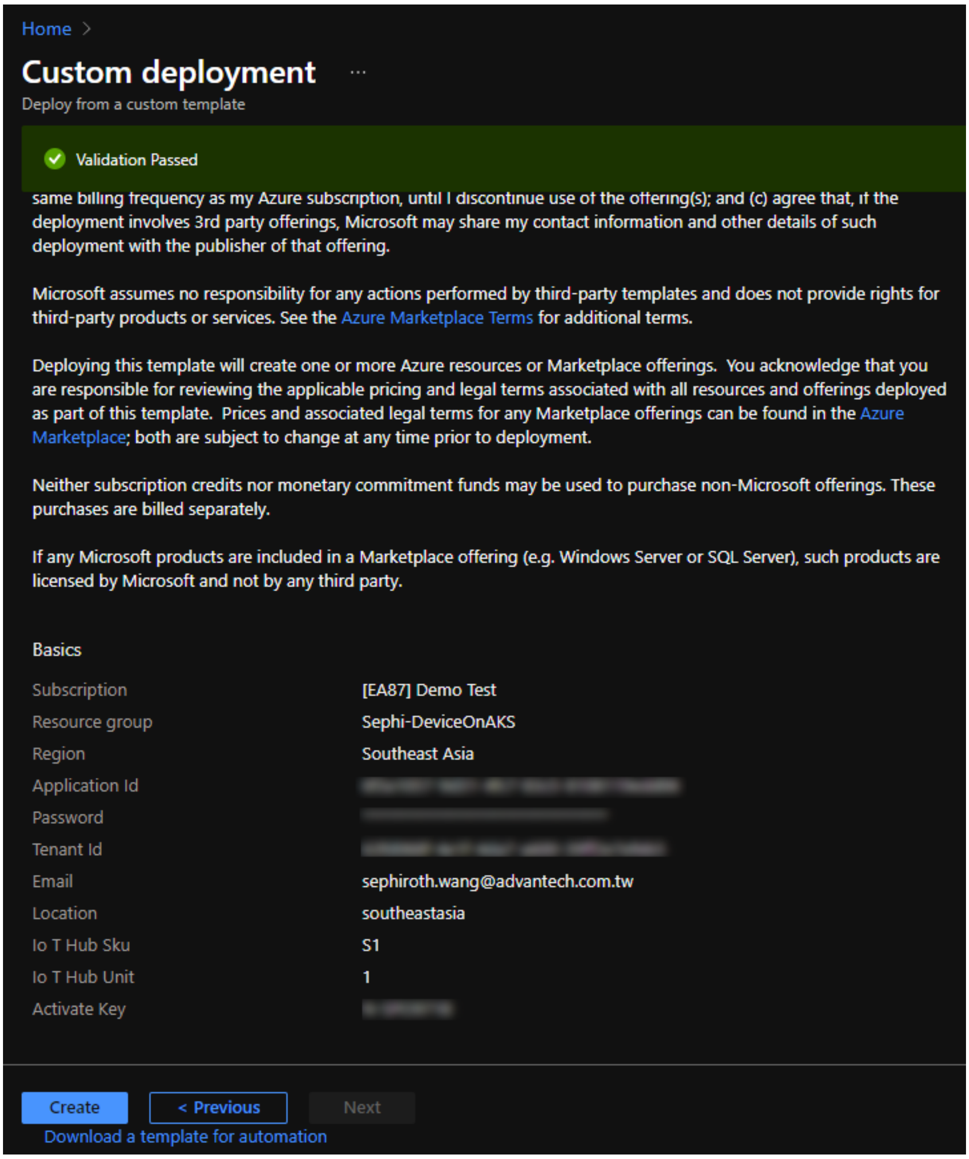
B. Enter the following values:

Name	Value
Resource Group	Select the resource group name you created in the last section.
Region	Select a location for the resource group. For example, Southeast Asia.
Application Id	The application Id is obtained from Step 1.

Name	**Value**
Password	The password is obtained from Step 1.
Tenant Id	The tenant Id is obtained from Step 1.
Email	After deployment, the result/progress will be sent to this email
Location	Enter the location name according to the data center. for examle, Asia East(**eastasia**), Asia Southeast(**southeastasia**), Japan East(**japaneast**), US East(**eastus**), Europe North(**northeurope**)
IoTHub Sku	S1/S2/S3, the default is **S1**, you could adjust the tier from Azure Portal, if need.
IoTHub Unit	default is 1
Activate Key	Advantech hardware connection, enter **N/A** (free support for 1000 Advantech devices), or please contact us to purchase license key for Non-Advantech devices.
AKS Max Node Count	Maximum number of Kubernetes nodes to auto-scaling
UTC Value	Fix value for generating unique string

C. Select **Review + create**

D. Validation and start to create.



Custom deployment ...

Deploy from a custom template

✓ Validation Passed

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.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the Azure Marketplace Terms for additional terms.

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the Azure Marketplace; both are subject to change at any time prior to deployment.

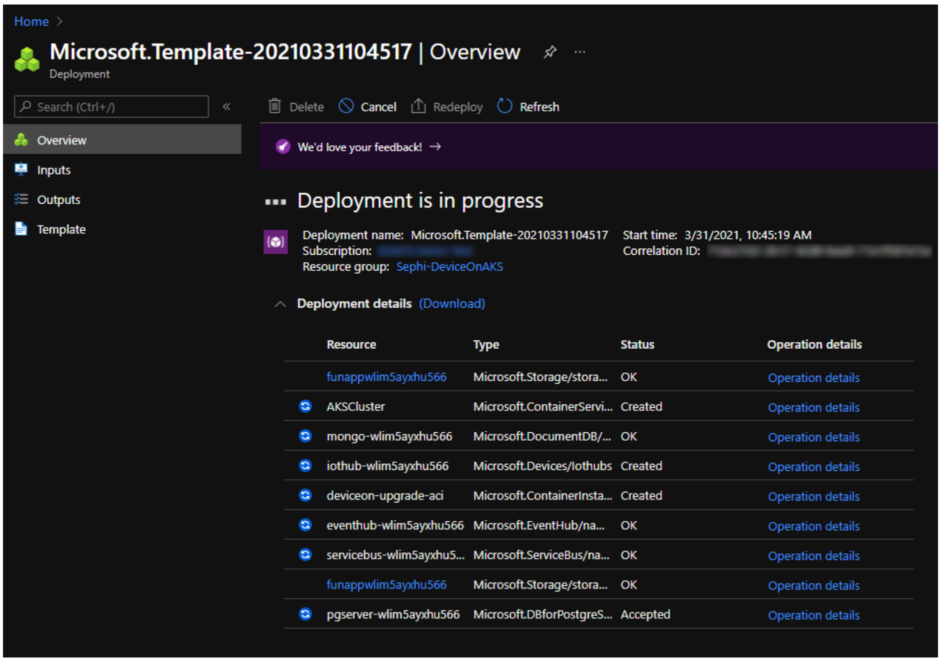
Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.

If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Basics

Subscription	[EA87] Demo Test
Resource group	Sephi-DeviceOnAKS
Region	Southeast Asia
Application Id	[redacted]
Password	[redacted]
Tenant Id	[redacted]
Email	sephiroth.wang@advantech.com.tw
Location	southeastasia
Io T Hub Sku	S1
Io T Hub Unit	1
Activate Key	[redacted]

E. The entire deployment process takes about **30 minutes**. After completion, you will receive a mail notification. The content of the mail includes the DeviceOn web **Service IP** and login **Account password**.

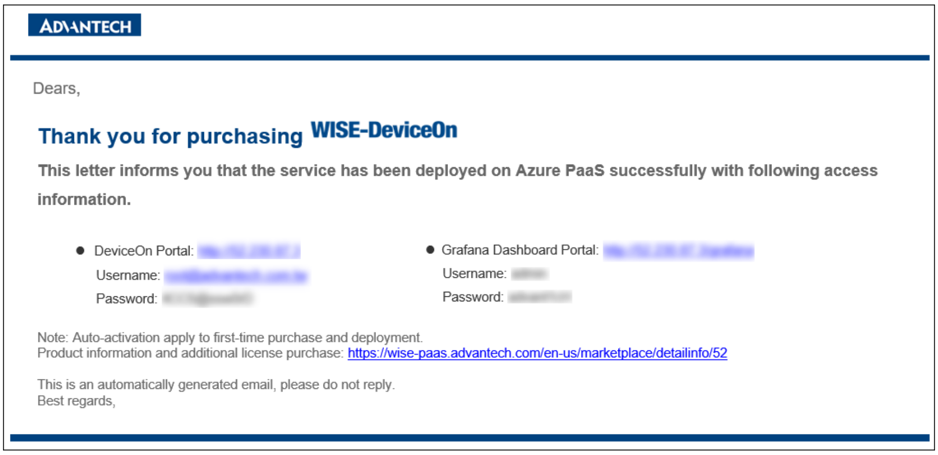


Deployment is in progress

Deployment name: Microsoft.Template-20210331104517
Subscription: [redacted]
Resource group: Sephi-DeviceOnAKS
Start time: 3/31/2021, 10:45:19 AM
Correlation ID: [redacted]

Deployment details (Download)

Resource	Type	Status	Operation details
funappwlim5ayxhu566	Microsoft.Storage/stora...	OK	Operation details
AKSCluster	Microsoft.ContainerServi...	Created	Operation details
mongo-wlim5ayxhu566	Microsoft.DocumentDB/...	OK	Operation details
iothub-wlim5ayxhu566	Microsoft.Devices/Iothubs	Created	Operation details
deviceon-upgrade-aci	Microsoft.ContainerInsta...	Created	Operation details
eventhub-wlim5ayxhu566	Microsoft.EventHub/na...	OK	Operation details
servicebus-wlim5ayxhu5...	Microsoft.ServiceBus/na...	OK	Operation details
funappwlim5ayxhu566	Microsoft.Storage/stora...	OK	Operation details
pgserver-wlim5ayxhu566	Microsoft.DBforPostgreS...	Accepted	Operation details



ADVANTECH

Dears,

Thank you for purchasing WISE-DeviceOn

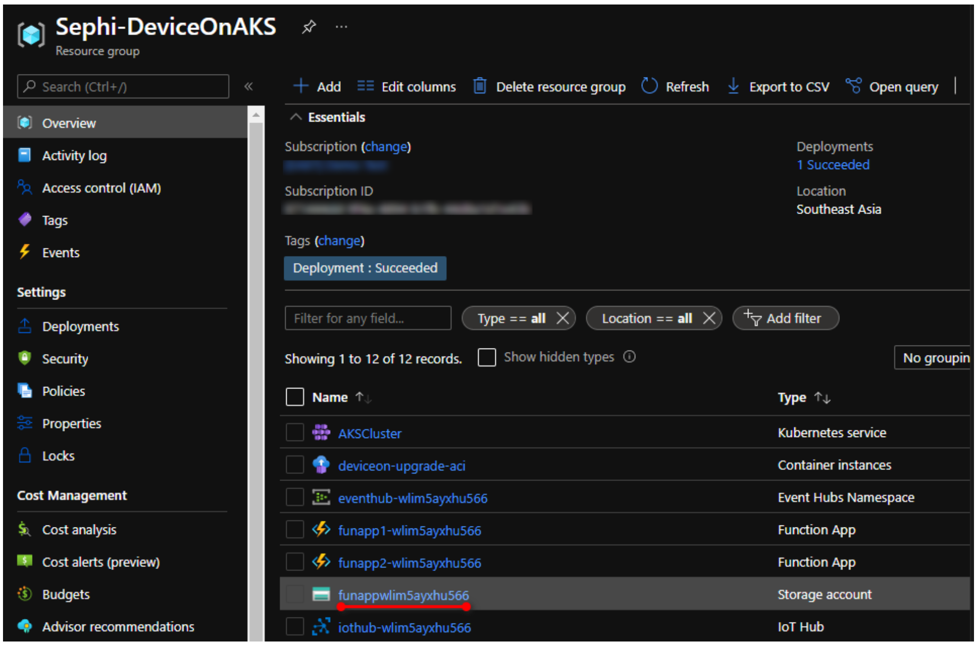
This letter informs you that the service has been deployed on Azure PaaS successfully with following access information.

- DeviceOn Portal: [redacted]
  Username: [redacted]
  Password: [redacted]
- Grafana Dashboard Portal: [redacted]
  Username: [redacted]
  Password: [redacted]

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,

Assuming that your mail is intercepted/block or not received due to mail server filters, we will synchronously write this information to the **Azure Blob Log** container. Go to your **resource group** (you entered at the stage of deployment) **storage account -> container -> Log -> ServerInformation.log**. If the container has not been created, please wait a few minutes for initialization.



Subscription (change)
[redacted]

Subscription ID
[redacted]

Tags (change)
Deployment : Succeeded

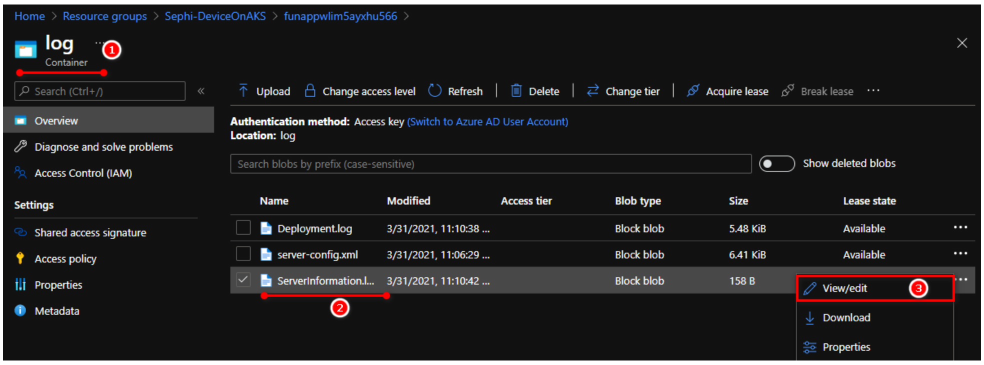
Deployments
1 Succeeded

Location
Southeast Asia

Filter for any field... | Type == all | Location == all | Add filter

Showing 1 to 12 of 12 records. □ Show hidden types | No groupin

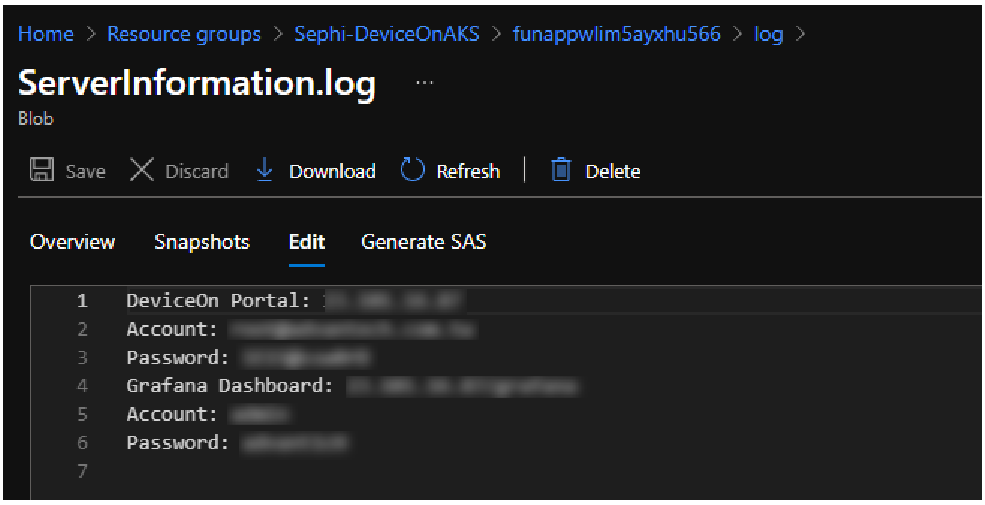
Name	Type
AKSCluster	Kubernetes service
deviceon-upgrade-aci	Container instances
eventhub-wlim5ayxhu566	Event Hubs Namespace
funapp1-wlim5ayxhu566	Function App
funapp2-wlim5ayxhu566	Function App
funappwlim5ayxhu566	Storage account
iothub-wlim5ayxhu566	IoT Hub



Authentication method: Access key (Switch to Azure AD User Account)
Location: log

Search blobs by prefix (case-sensitive) | Show deleted blobs

Name	Modified	Access tier	Blob type	Size	Lease state
Deployment.log	3/31/2021, 11:10:38 ...		Block blob	5.48 KiB	Available
server-config.xml	3/31/2021, 11:06:29 ...		Block blob	6.41 KiB	Available
ServerInformation.l...	3/31/2021, 11:10:42 ...		Block blob	158 B	



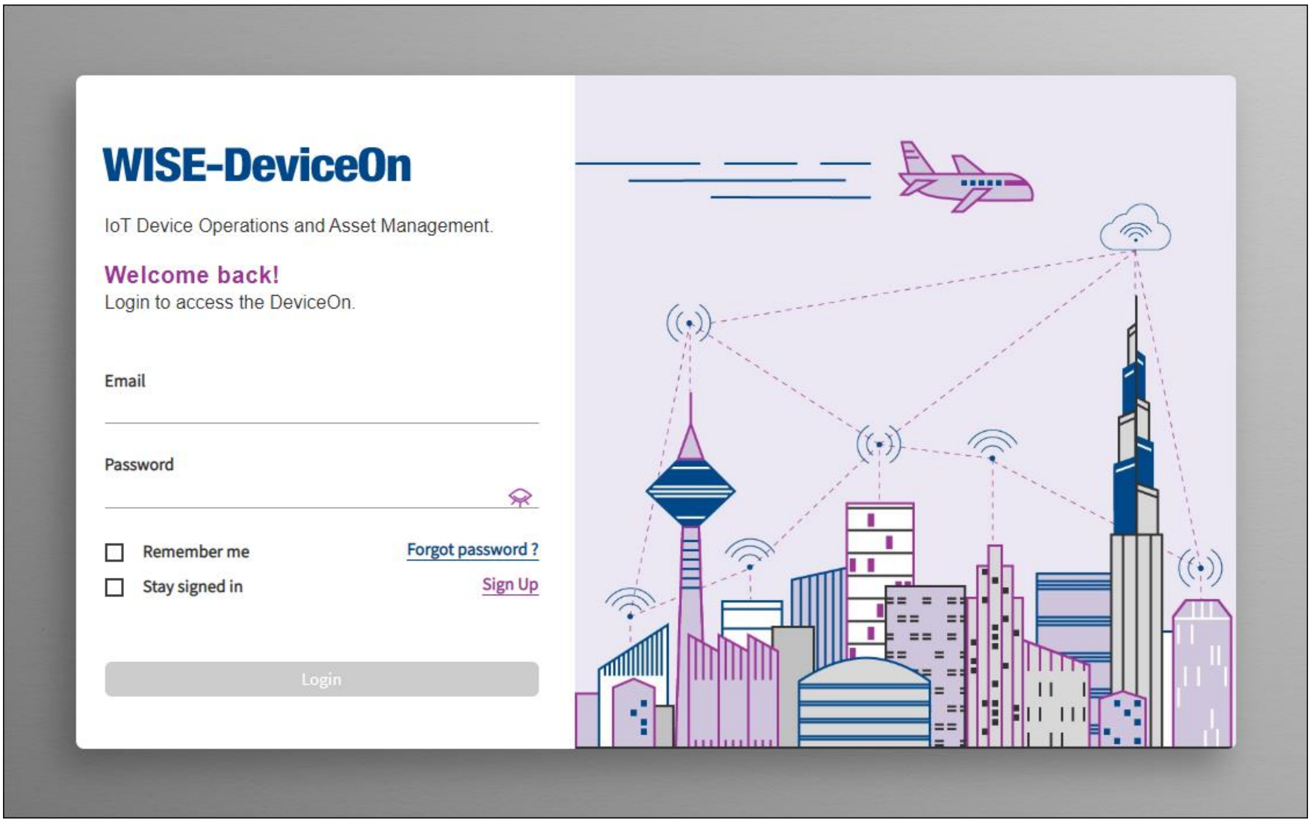
```
DeviceOn Portal: [redacted]
Account: [redacted]
Password: [redacted]
Grafana Dashboard: [redacted]
Account: [redacted]
Password: [redacted]

```

F. There are two resource group generated on your subscription, one is you entered at the stage of deployment, which include the services such as: AKS, IoT Hub, EventHub, Stream Analytics, Cosmos DB, PostgreSQL…etc. Another resource group name prefix name starts with MC_, that contains AKS VM node.

2.2 DeviceOn Client Installation

2.2.1 Setup Device Onboarding (Windows)

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



WISE-DeviceOn

IoT Device Operations and Asset Management.

Welcome back!

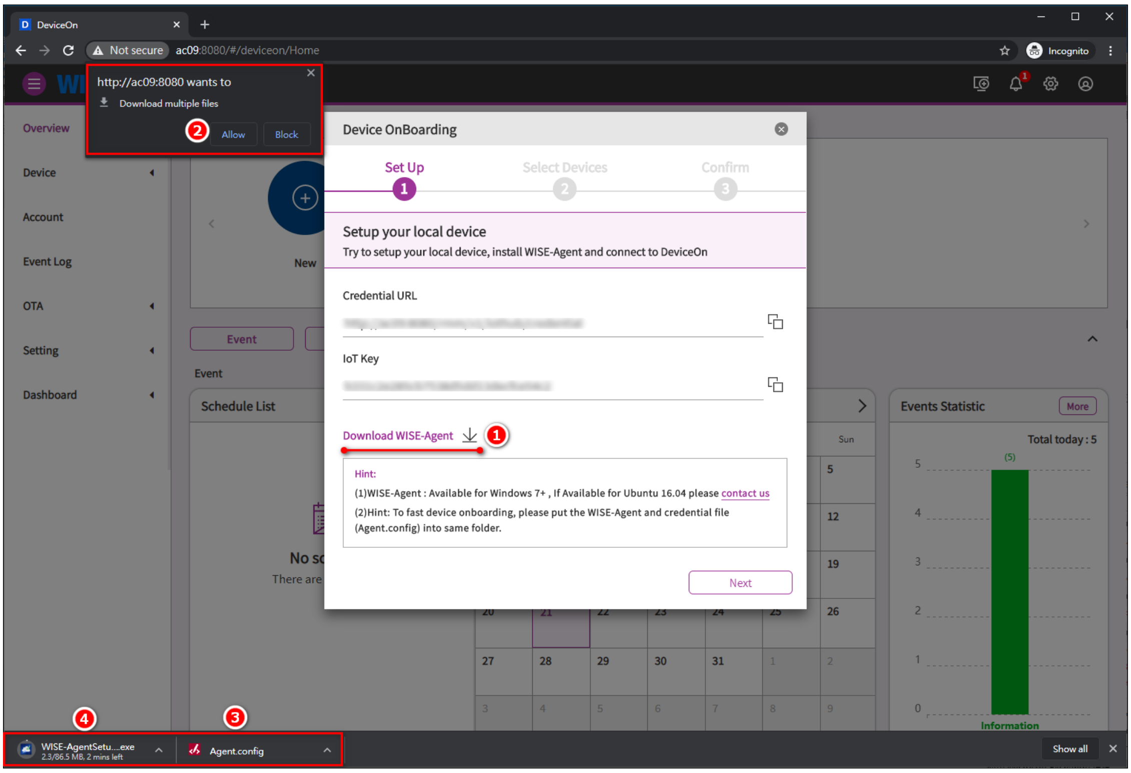
Login to access the DeviceOn.

Email

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**)



Device OnBoarding

Set Up 1 — Select Devices 2 — Confirm 3

Setup your local device

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

Credential URL

[redacted]

IoT Key

[redacted]

Download WISE-Agent

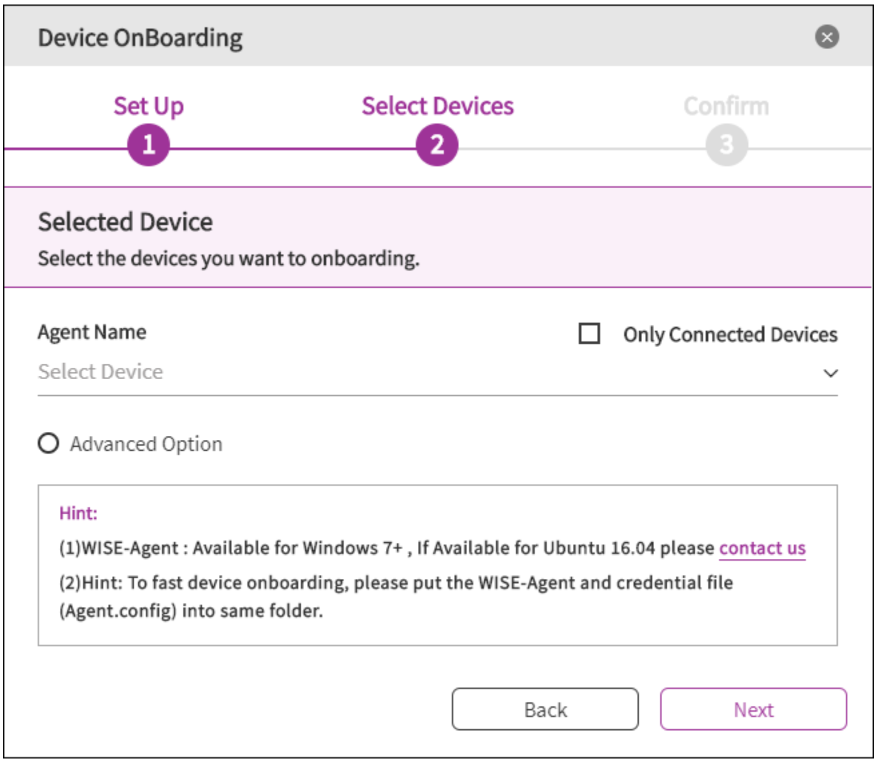
Hint:

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

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

Next

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



Device OnBoarding

Set Up 1 — Select Devices 2 — Confirm 3

Selected Device

Select the devices you want to onboarding.

Agent Name

□ Only Connected Devices

Select Device

○ Advanced Option

Hint:

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

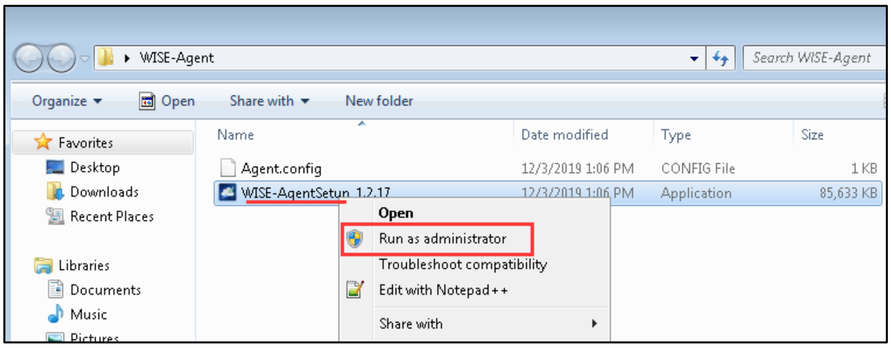
(2)Hint: To fast device onboarding, please put the WISE-Agent and credential file (Agent.config) into same folder.

Back

Next

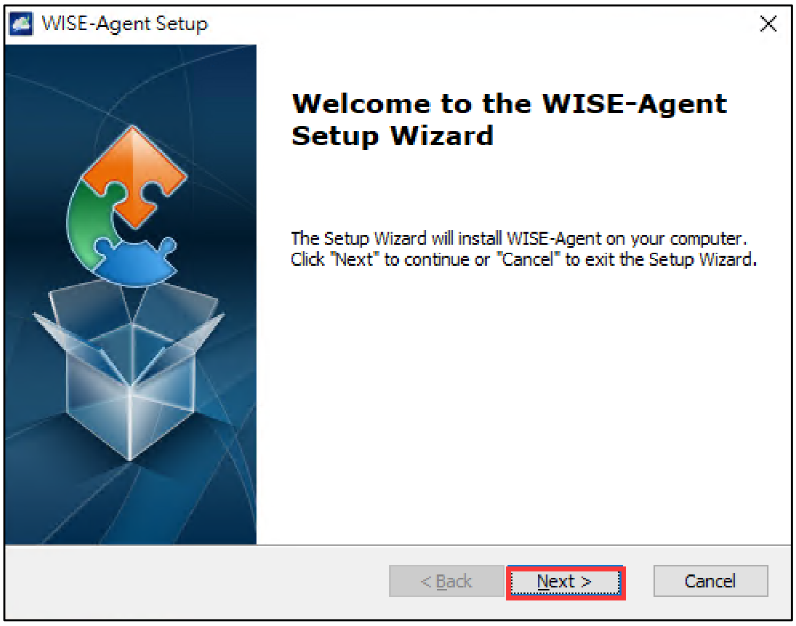
Step 3: Set up Your Local Device

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.



Name	Date modified	Type	Size
Agent.config	12/3/2019 1:06 PM	CONFIG File	1 KB
WISE-AgentSetup_1.2.17	12/3/2019 1:06 PM	Application	85,633 KB

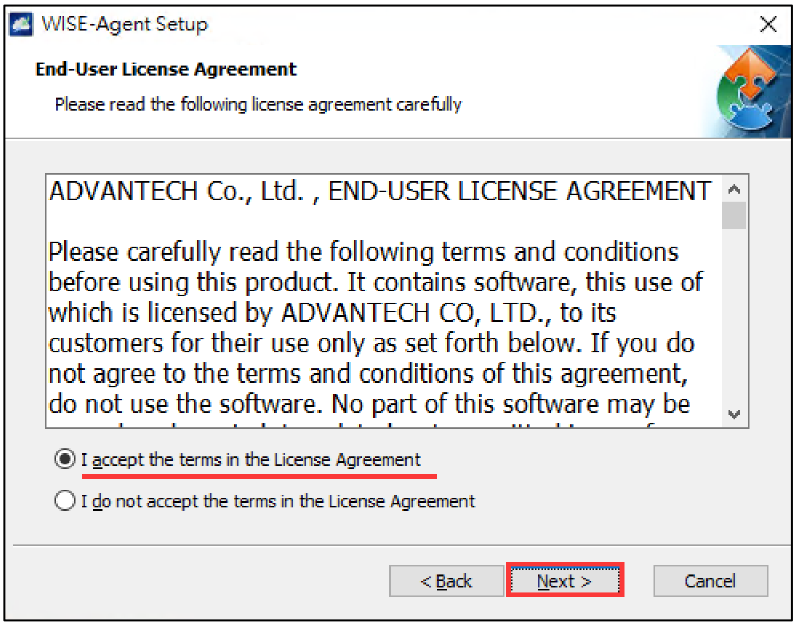
Click “**Next”** to set up the WISE-Agent program.



Welcome to the WISE-Agent Setup Wizard

The Setup Wizard will install WISE-Agent on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

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



End-User License Agreement

Please read the following license agreement carefully

ADVANTECH Co., Ltd. , END-USER LICENSE AGREEMENT

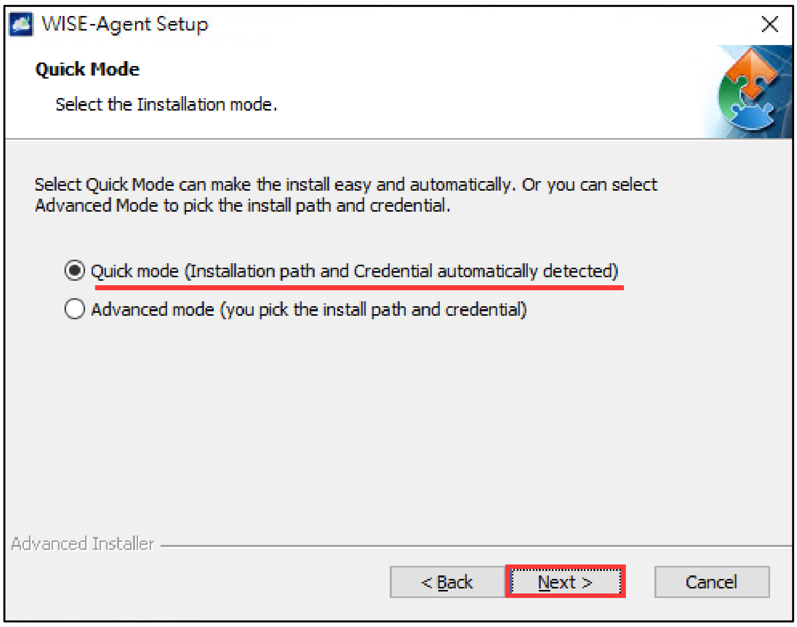
Please carefully read the following terms and conditions before using this product. It contains software, this use of which is licensed by ADVANTECH CO, LTD., to its customers for their use only as set forth below. If you do not agree to the terms and conditions of this agreement, do not use the software. No part of this software may be

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

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:



WISE-Agent Setup

Quick Mode

Select the Installation mode.

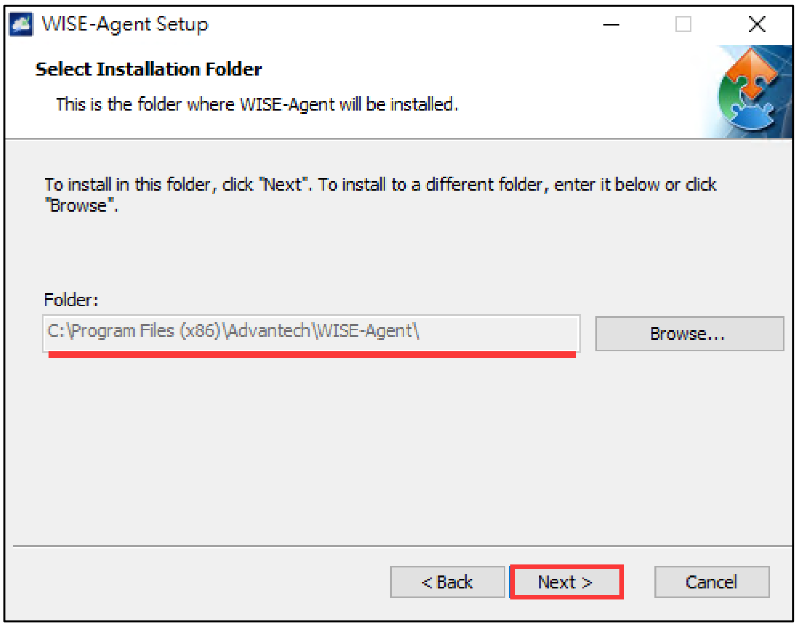
Select Quick Mode can make the install easy and automatically. Or you can select Advanced Mode to pick the install path and credential.

● Quick mode (Installation path and Credential automatically detected)

○ Advanced mode (you pick the install path and credential)

Advanced Mode:

Select the Installation folder for WISE-Agent



WISE-Agent Setup

Select Installation Folder

This is the folder where WISE-Agent will be installed.

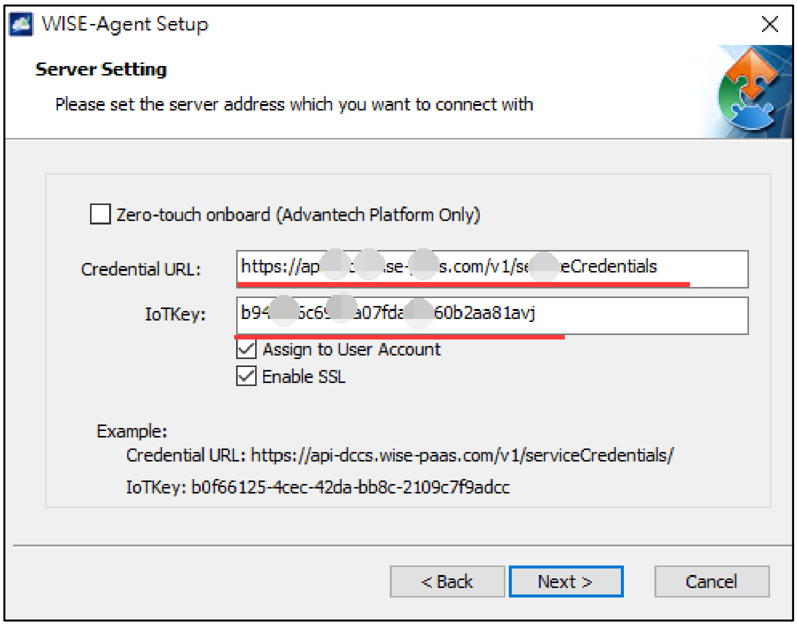
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:

C:\Program Files (x86)\Advantech\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.*



Server Setting

Please set the server address which you want to connect with

□ Zero-touch onboard (Advantech Platform Only)

Credential URL: https://ap[redacted]se-[redacted]s.com/v1/se[redacted]eCredentials

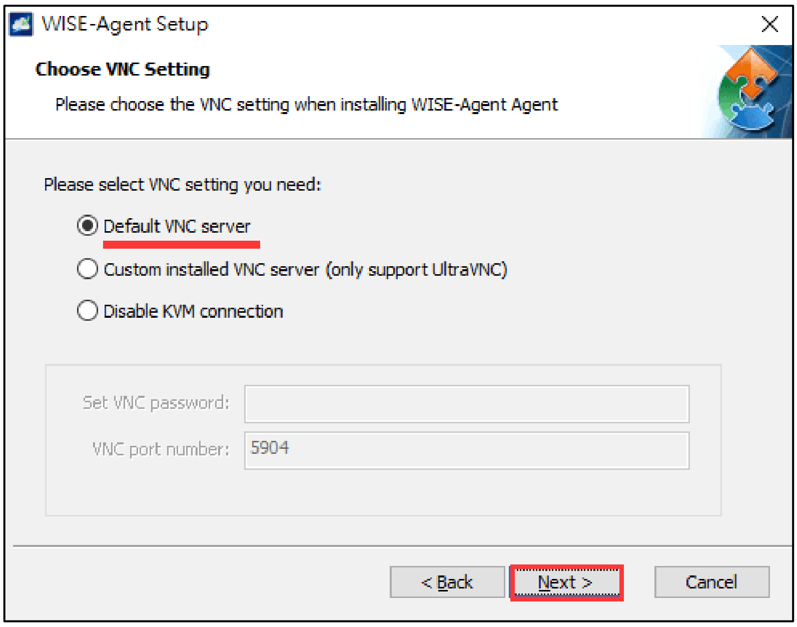
IoTKey: b94[redacted]5c6[redacted]a07fda[redacted]60b2aa81avj

☑ Assign to User Account

☑ Enable SSL

Example:
Credential URL: https://api-dccs.wise-paas.com/v1/serviceCredentials/
IoTKey: b0f66125-4cec-42da-bb8c-2109c7f9adcc

WISE-Agent supports remote desktop through built-in UltraVNC. You can manually specific 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".



Choose VNC Setting

Please choose the VNC setting when installing WISE-Agent Agent

Please select VNC setting you need:

● Default VNC server

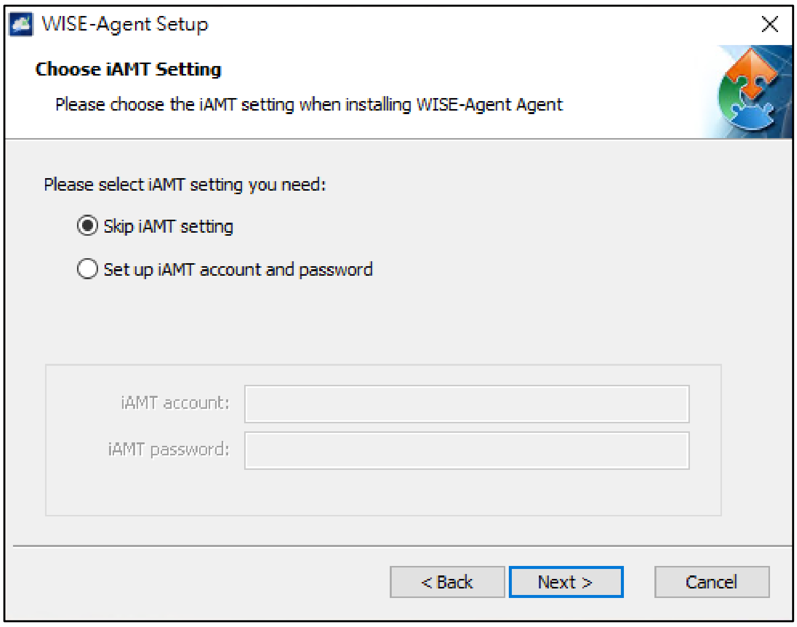
○ Custom installed VNC server (only support UltraVNC)

○ Disable KVM connection

Set VNC password:

VNC port number: 5904

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.



WISE-Agent Setup

Choose iAMT Setting

Please choose the iAMT setting when installing WISE-Agent Agent

Please select iAMT setting you need:

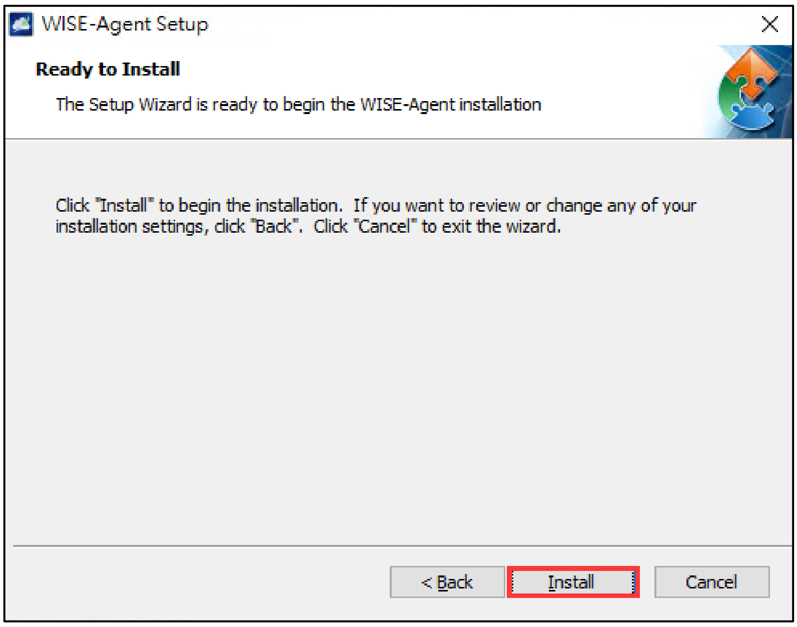
● Skip iAMT setting

○ Set up iAMT account and password

iAMT account:

iAMT password:

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



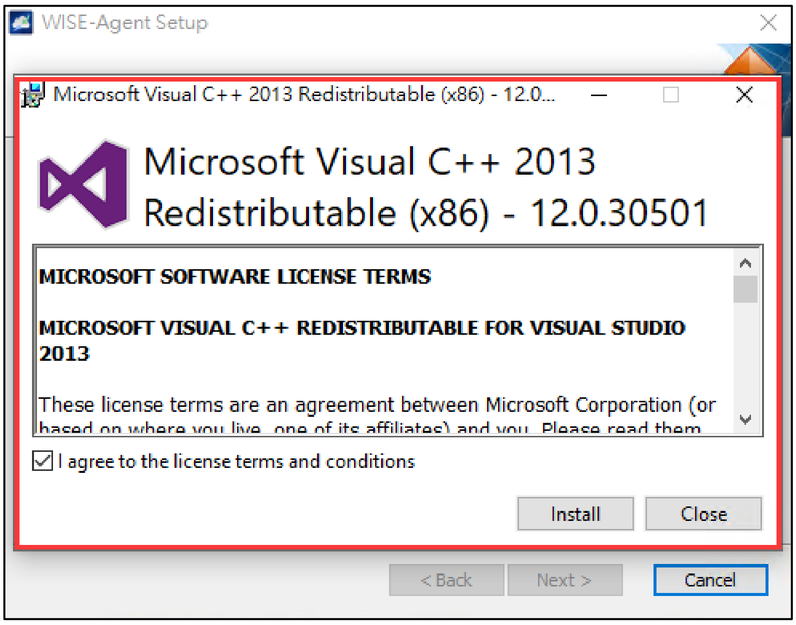
WISE-Agent Setup

Ready to Install

The Setup Wizard is ready to begin the WISE-Agent installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

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.



Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501

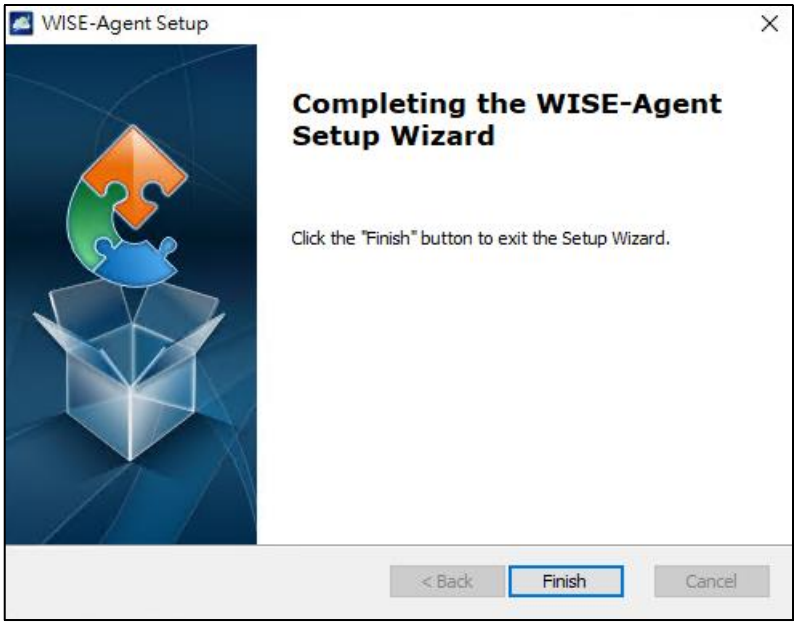
MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT VISUAL C++ REDISTRIBUTABLE FOR VISUAL STUDIO 2013

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them

☑ I agree to the license terms and conditions

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

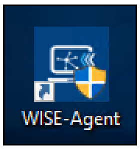


Completing the WISE-Agent Setup Wizard

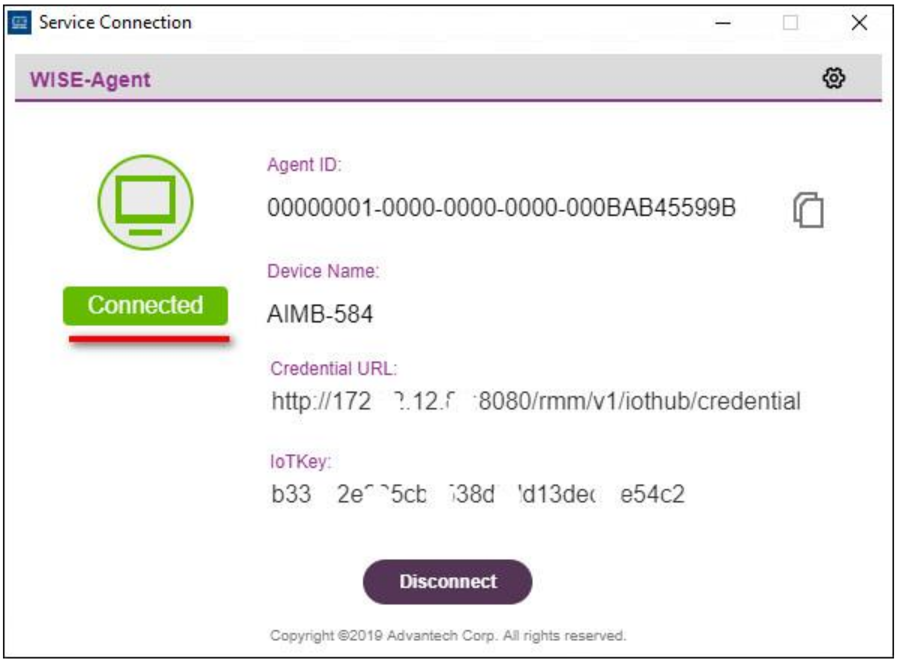
Click the "Finish" button to exit the Setup Wizard.

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, Microsoft Azure) or on premise (standalone server version) depending on deployment scenario. Then, please click the “Connect” button to try to reconnect.



Service Connection

WISE-Agent

Connected

Agent ID:
00000001-0000-0000-0000-000BAB45599B

Device Name:
AIMB-584

Credential URL:
http://172 ?.12.f 8080/rmm/v1/iothub/credential

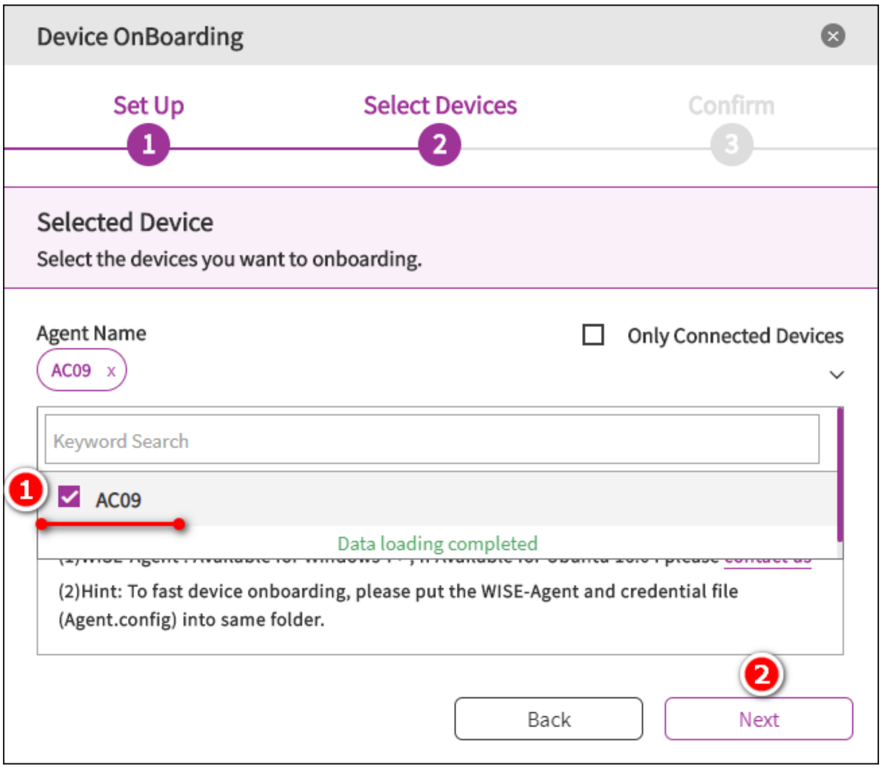
IoTKey:
b33 2e 5cb 38d d13de e54c2

Disconnect

Copyright ©2019 Advantech Corp. All rights reserved.

Step 5: Grouping Your Devices

Once the device connects, to device grouping page, where the device group for these devices can be selected.



Device OnBoarding

Selected Device

Select the devices you want to onboarding.

Agent Name

AC09 x

□ Only Connected Devices

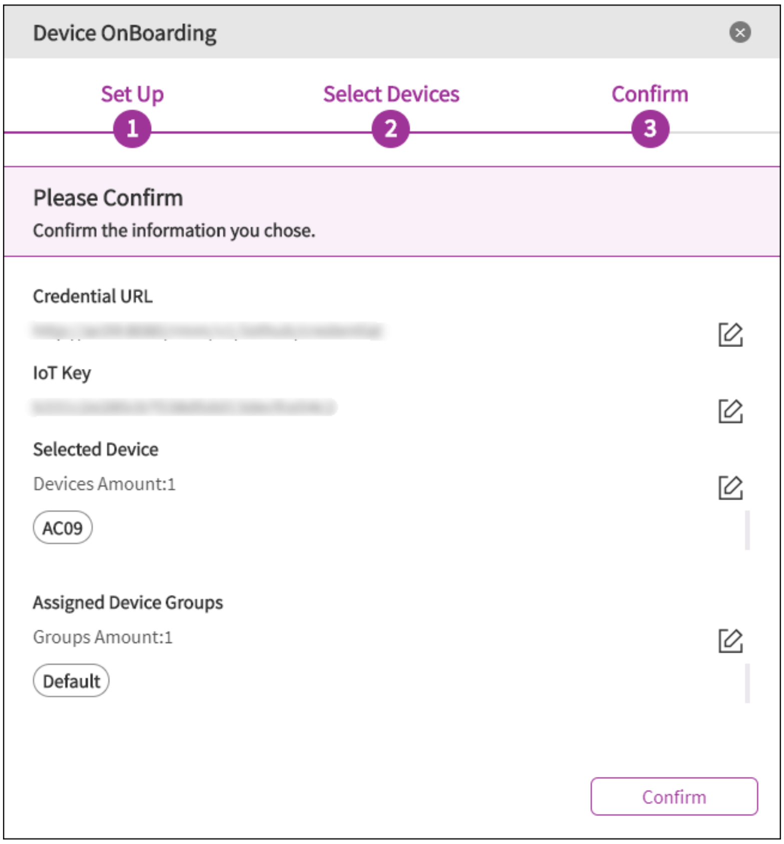
Keyword Search

1 ☑ AC09

Data loading completed

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

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.



Device OnBoarding

Please Confirm

Confirm the information you chose.

Credential URL

[redacted]

IoT Key

[redacted]

Selected Device

Devices Amount:1

AC09

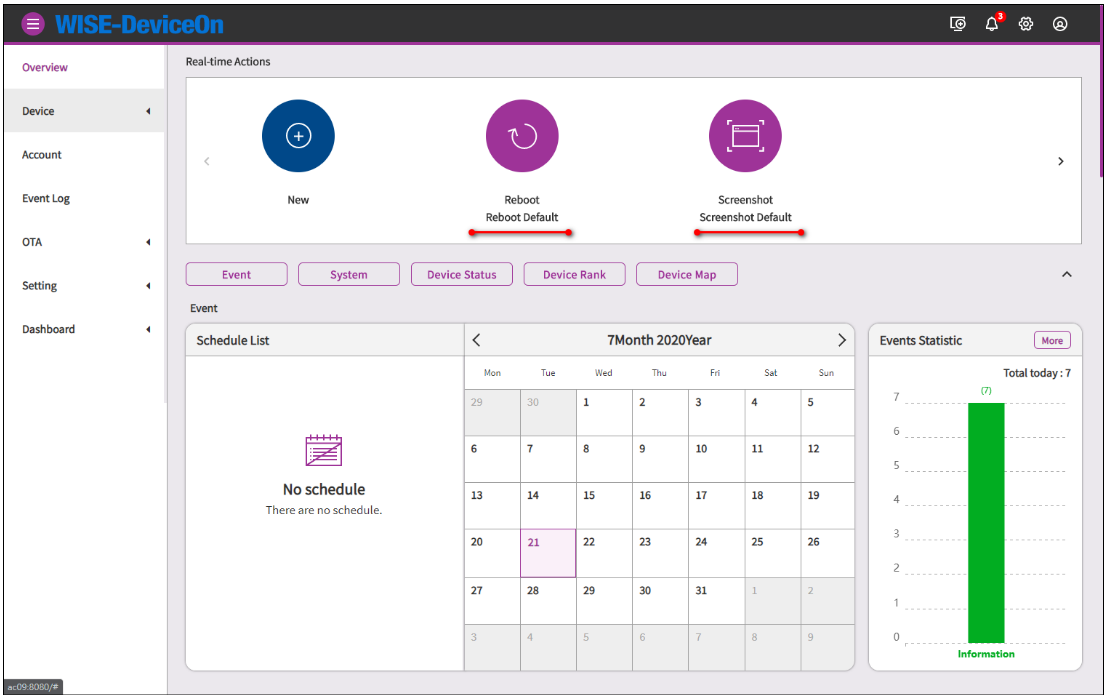
Assigned Device Groups

Groups Amount:1

Default

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.



2.2.2 Setup Device Onboarding (Linux)

We also provide an installer for Ubuntu Linux (one of the most popular Linux distribution). This section will guide you how to install WISE-Agent on Ubuntu Linux. Note here that:

The WISE-Agent Ubuntu Linux installer is named something like "**wise-agent-Ubuntu 18.04 x86_64-1.x.x.0.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

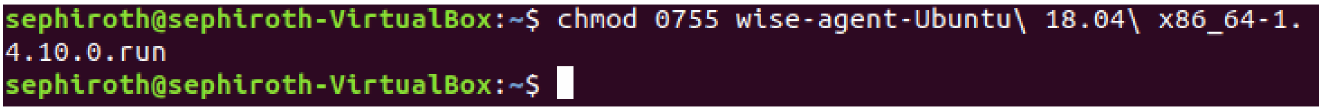
The installer runs in CLI (Command Line Interface) mode. As such, open a terminal preferable for you.

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

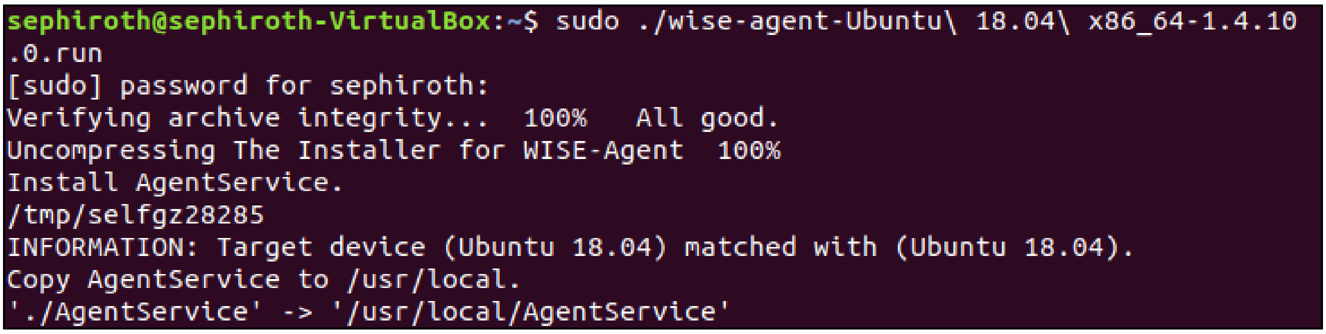
In the terminal, run "**chmod 0755 wise-agent-Ubuntu 18.04 x86_64-1.x.x.0.run**" so that the installer as an executable file under Ubuntu Linux.



```
sephiroth@sephiroth-VirtualBox:~$ chmod 0755 wise-agent-Ubuntu\ 18.04\ x86_64-1.
4.10.0.run
sephiroth@sephiroth-VirtualBox:~$ █
```

Step 4: Running the installer

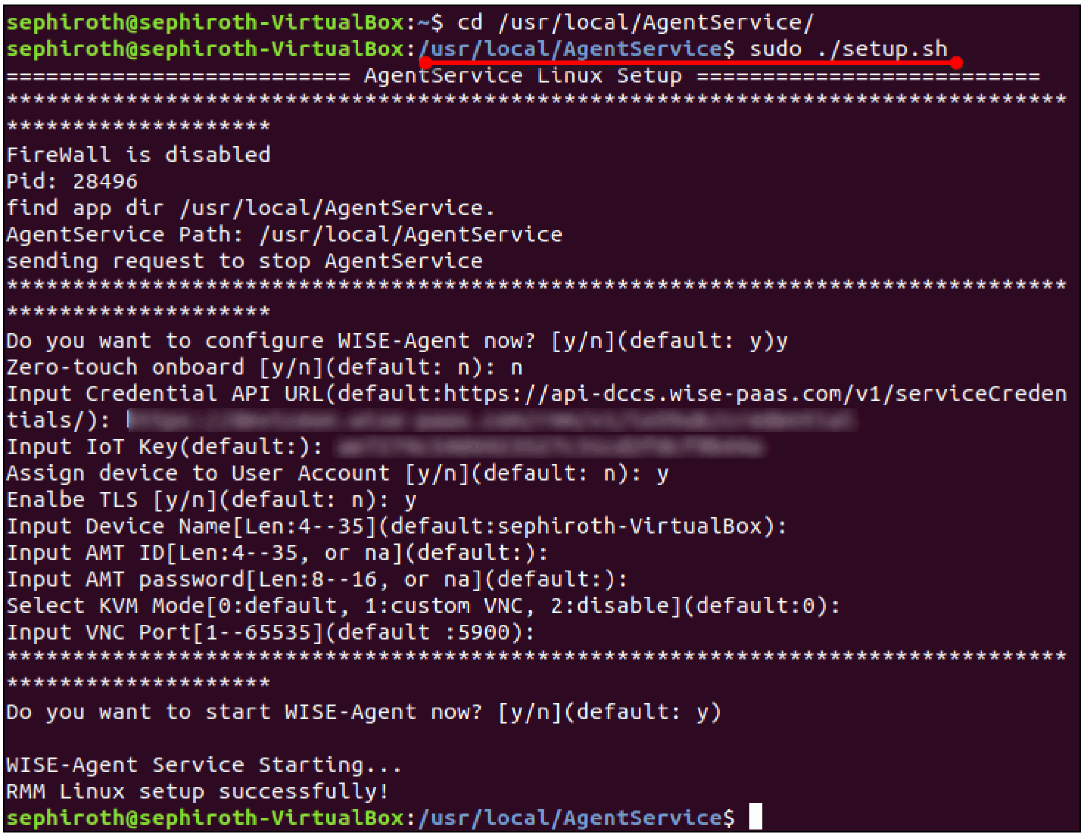
Change your working directory to where the installer is and run "**./wise-agent-Ubuntu 18.04 x86_64-1.x.x.0.run** ". You may need to run "**sudo ./wise-agent-Ubuntu 18.04 x86_64-1.x.x.0.run**" to acquire higher privileges if you were logged in as a normal user.



```
sephiroth@sephiroth-VirtualBox:~$ sudo ./wise-agent-Ubuntu\ 18.04\ x86_64-1.4.10
.0.run
[sudo] password for sephiroth:
Verifying archive integrity...  100%   All good.
Uncompressing The Installer for WISE-Agent  100%
Install AgentService.
/tmp/selfgz28285
INFORMATION: Target device (Ubuntu 18.04) matched with (Ubuntu 18.04).
Copy AgentService to /usr/local.
'./AgentService' -> '/usr/local/AgentService'
```

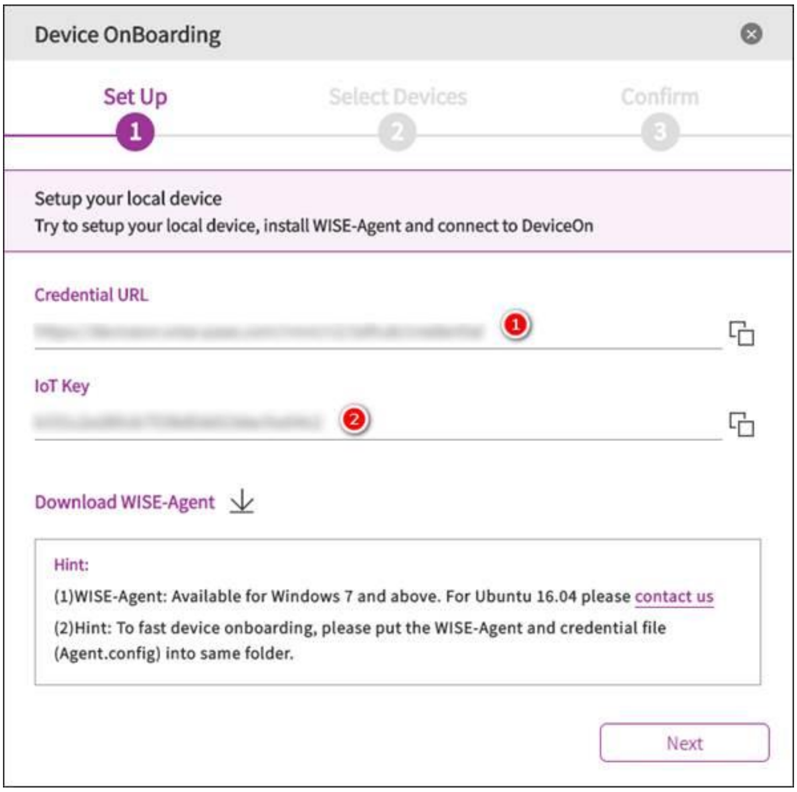
Step 5: Start WISE-Agent and Connect to DeviceOn

Change your directory to **/usr/local/AgentService** and run **sudo ./setup.sh** to answer connection information, such as credential URL, IoTKey, Device Name and etc.



```
sephiroth@sephiroth-VirtualBox:~$ cd /usr/local/AgentService/
sephiroth@sephiroth-VirtualBox:/usr/local/AgentService$ sudo ./setup.sh
========================= AgentService Linux Setup =========================
********************************************************************************
********************
FireWall is disabled
Pid: 28496
find app dir /usr/local/AgentService.
AgentService Path: /usr/local/AgentService
sending request to stop AgentService
********************************************************************************
********************
Do you want to configure WISE-Agent now? [y/n](default: y)y
Zero-touch onboard [y/n](default: n): n
Input Credential API URL(default:https://api-dccs.wise-paas.com/v1/serviceCreden
tials/): [redacted]
Input IoT Key(default:): [redacted]
Assign device to User Account [y/n](default: n): y
Enalbe TLS [y/n](default: n): y
Input Device Name[Len:4--35](default:sephiroth-VirtualBox):
Input AMT ID[Len:4--35, or na](default:):
Input AMT password[Len:8--16, or na](default:):
Select KVM Mode[0:default, 1:custom VNC, 2:disable](default:0):
Input VNC Port[1--65535](default :5900):
********************************************************************************
********************
Do you want to start WISE-Agent now? [y/n](default: y)

WISE-Agent Service Starting...
RMM Linux setup successfully!
sephiroth@sephiroth-VirtualBox:/usr/local/AgentService$
```

1. Zero-touch onboard is a zero-configuration and quick connection mode for a special purpose. The default is disabled (n).
2. Enter **Credential URL** and **IoT Key** that information could retrieve from the DeviceOn portal.



Device OnBoarding

Setup your local device

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

Credential URL: [redacted]

IoT Key: [redacted]

Download WISE-Agent

Hint:

(1)WISE-Agent: Available for Windows 7 and above. For Ubuntu 16.04 please contact us

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

3. Assign device to User Account: You can bind the target device into a “Default” group in your account on the portal automatically
4. Enable TLS: Turn ON/OFF the TLS/SSL mode.
5. Input Device Name: Give your device name and show it on the portal.
6. Input AMT ID and password: If your device support Intel AMT, please enter AMT ID and Password to enable these functions.
7. Select KVM Mode [0:**default**, 1:**Custom VNC**, 2:**disable**]: User can use our default VNC to support the Remote Desktop function by entering 0 and give a listen port if you don’t want to use the default port. Second, select **Custom Mode**, if they already have a VNC server by entering 1 and provide the listen port and password. To disable the KVM function by entering 2.

When you run into this step the question shows like above, device is connected and under your account.

3. DeviceOn User Interface & Functions

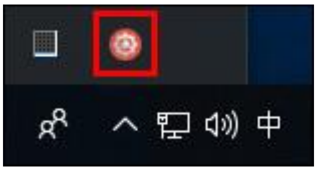
3.1 DeviceOn Server (Standalone)

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.

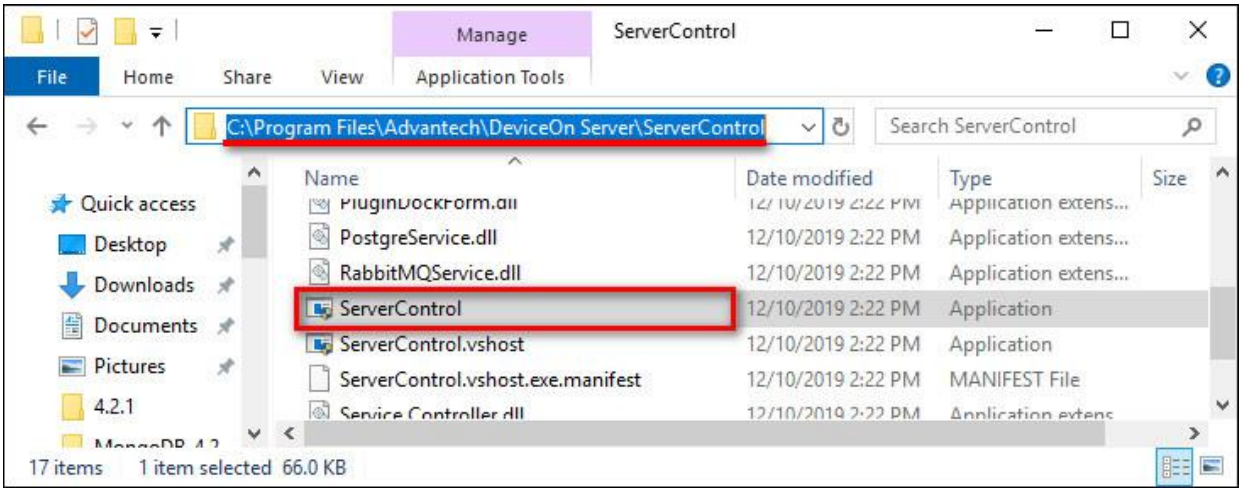
The following section (3.1.1) introduces the “Standalone Server Control” tool that allows to monitor and enable/disable DeviceOn core components. The watchdog service is explained in section 3.1.2.

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:

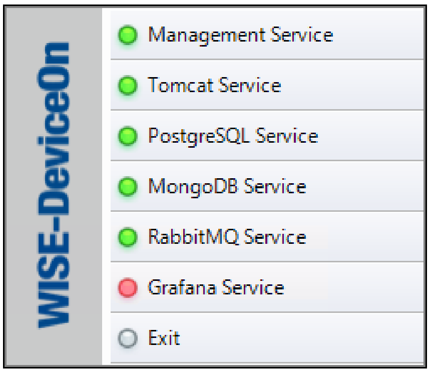


C:\Program Files\Advantech\DeviceOn Server\ServerControl

Name	Date modified	Type	Size
PluginDockForm.dll	12/10/2019 2:22 PM	Application extens...	
PostgreService.dll	12/10/2019 2:22 PM	Application extens...	
RabbitMQService.dll	12/10/2019 2:22 PM	Application extens...	
ServerControl	12/10/2019 2:22 PM	Application	
ServerControl.vshost	12/10/2019 2:22 PM	Application	
ServerControl.vshost.exe.manifest	12/10/2019 2:22 PM	MANIFEST File	
Service Controller.dll	12/10/2019 2:22 PM	Application extens	

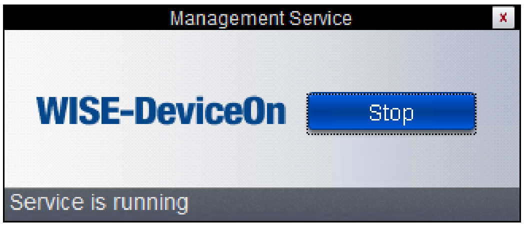
17 items 1 item selected 66.0 KB

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

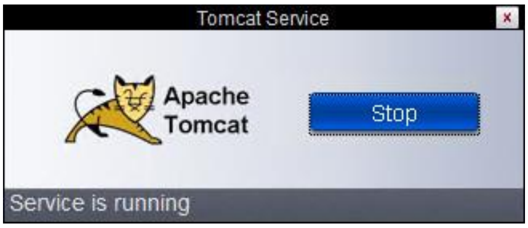
The “Management” service includes the DeviceOn backend core function and consists of two Java processes (DeviceOn and Provisioning Worker) that handle messages and process OTA traffic between the client and server. Click “Stop” to stop the management service.



Service is running

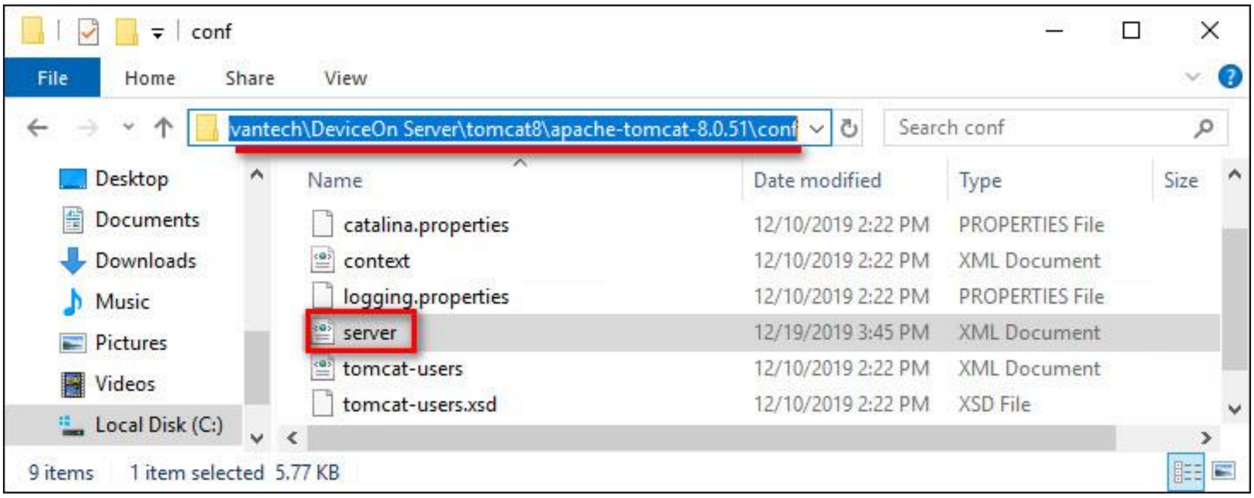
- Tomcat Service

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



Service is running

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



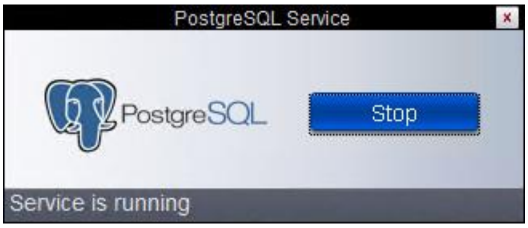
vantech\DeviceOn Server\tomcat8\apache-tomcat-8.0.51\conf

Name	Date modified	Type	Size
catalina.properties	12/10/2019 2:22 PM	PROPERTIES File	
context	12/10/2019 2:22 PM	XML Document	
logging.properties	12/10/2019 2:22 PM	PROPERTIES File	
server	12/19/2019 3:45 PM	XML Document	
tomcat-users	12/10/2019 2:22 PM	XML Document	
tomcat-users.xsd	12/10/2019 2:22 PM	XSD File	

9 items 1 item selected 5.77 KB

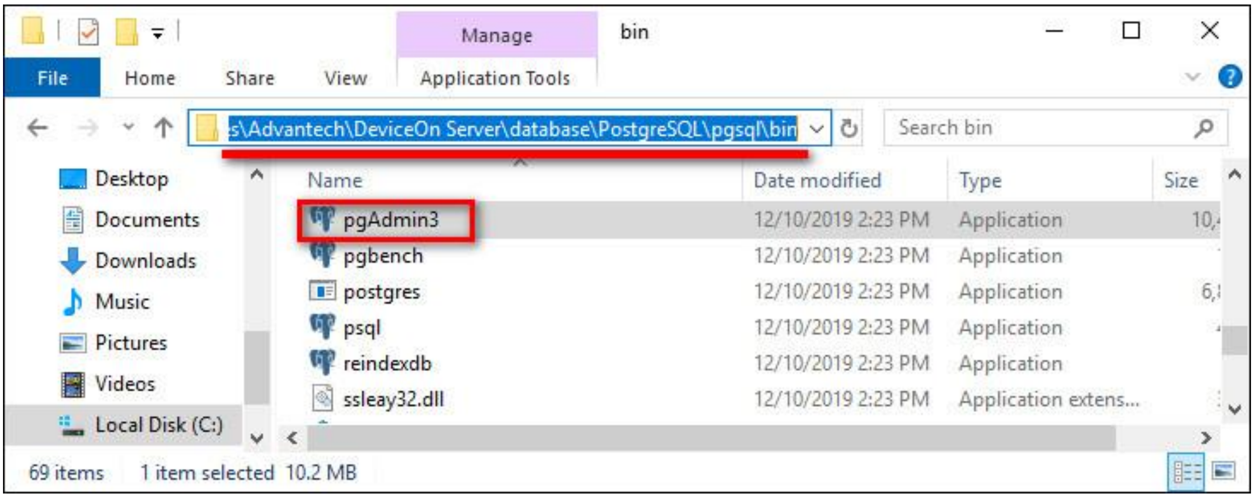
- PostgreSQL Service

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



Service is running

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.



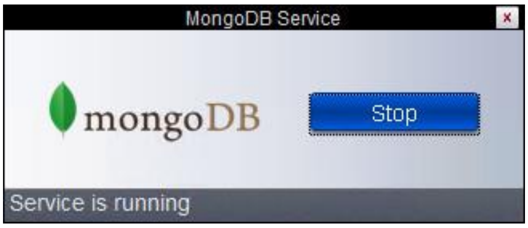
s\Advantech\DeviceOn Server\database\PostgreSQL\pgsql\bin

Name	Date modified	Type	Size
pgAdmin3	12/10/2019 2:23 PM	Application	10,
pgbench	12/10/2019 2:23 PM	Application	
postgres	12/10/2019 2:23 PM	Application	6,
psql	12/10/2019 2:23 PM	Application	
reindexdb	12/10/2019 2:23 PM	Application	
ssleay32.dll	12/10/2019 2:23 PM	Application extens...	

69 items 1 item selected 10.2 MB

- MongoDB Service

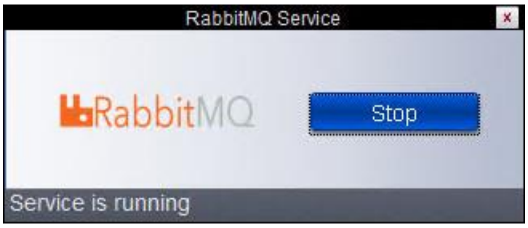
To process sensor data from client devices, DeviceOn leverages MongoDB to provide better performance and compression rates than relational databases. Click “**Stop**” to stop the MongoDB service.



Service is running

- RabbitMQ Service

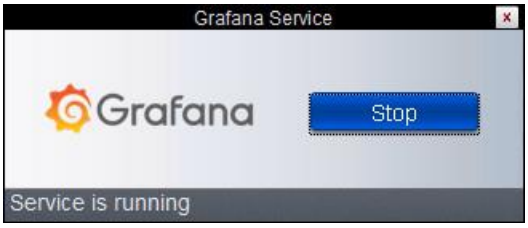
RabbitMQ is one of the most popular open-source message brokers, and is used as “IoT Hub” to exchange messages between the server and client devices. Click “**Stop**” to stop the RabbitMQ service.



Service is running

- Grafana Service

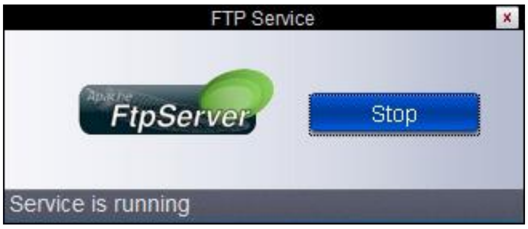
Grafana is a popular framework that allows you to query, visualize and alert on data from various data sources. DeviceOn supports a simple JSON API that as can be used as data source in Grafana, effectively making all DeviceOn data available to Grafana. Click “**Stop**” to stop the Grafana service.



Service is running

- FTP Service

To remote deploy the application to edge device via OTA, DeviceOn build-in a FTP service (Apache FTP) as a default storage. The Apache FtpServer is a 100% pure Java FTP server. It’s designed to be a complete and portable FTP server engine solution based on currently available open protocols. FtpServer can be run standalone as a Windows service or Unix/Linux daemon or embedded into a Java application.

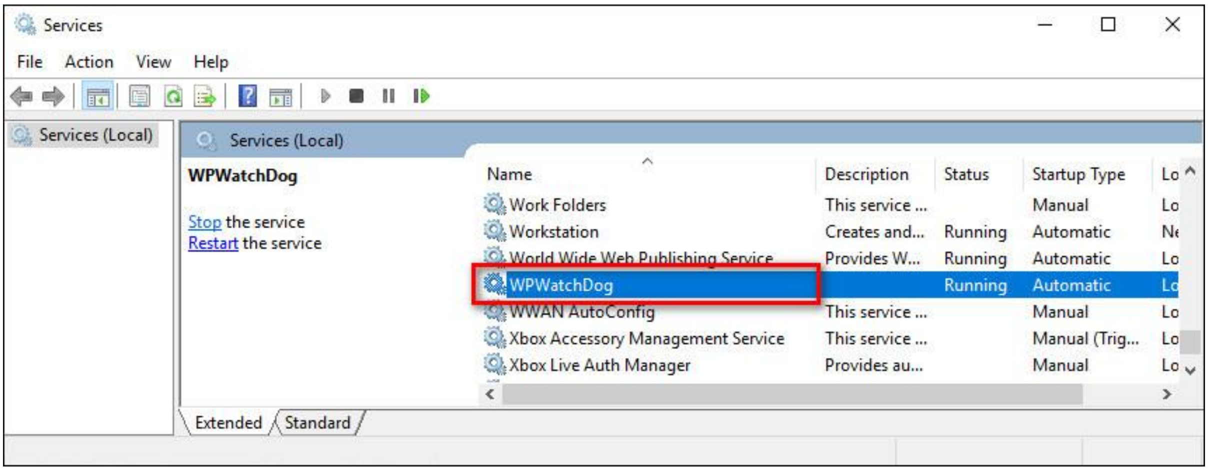


Service is running

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.



WPWatchDog

Stop the service
Restart the service

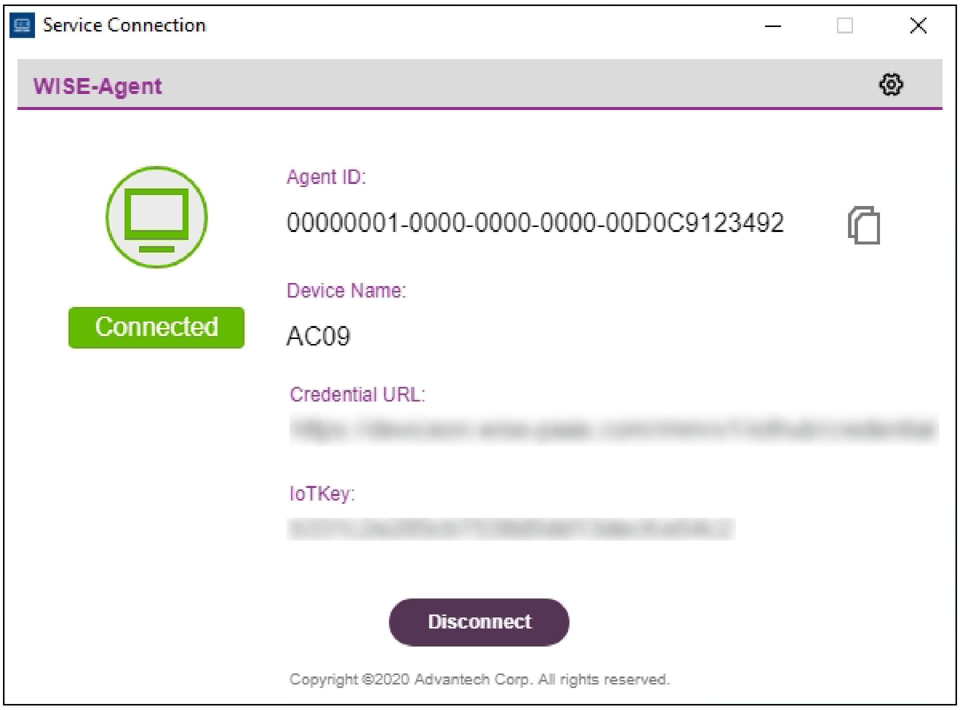
Name	Description	Status	Startup Type	Lo
Work Folders	This service ...		Manual	Lo
Workstation	Creates and...	Running	Automatic	Ne
World Wide Web Publishing Service	Provides W...	Running	Automatic	Lo
WPWatchDog		Running	Automatic	Lo
WWAN AutoConfig	This service ...		Manual	Lo
Xbox Accessory Management Service	This service ...		Manual (Trig...	Lo
Xbox Live Auth Manager	Provides au...		Manual	Lo

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 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 2.2.1** to install WISE-Agent. After launching the WISE-Agent user interface, it will provide an overview of the connection status, device information (Agent ID, Device Name) as well as connection credentials (Credential URL, IoTKey).



Agent ID:
00000001-0000-0000-0000-00D0C9123492

Device Name:
AC09

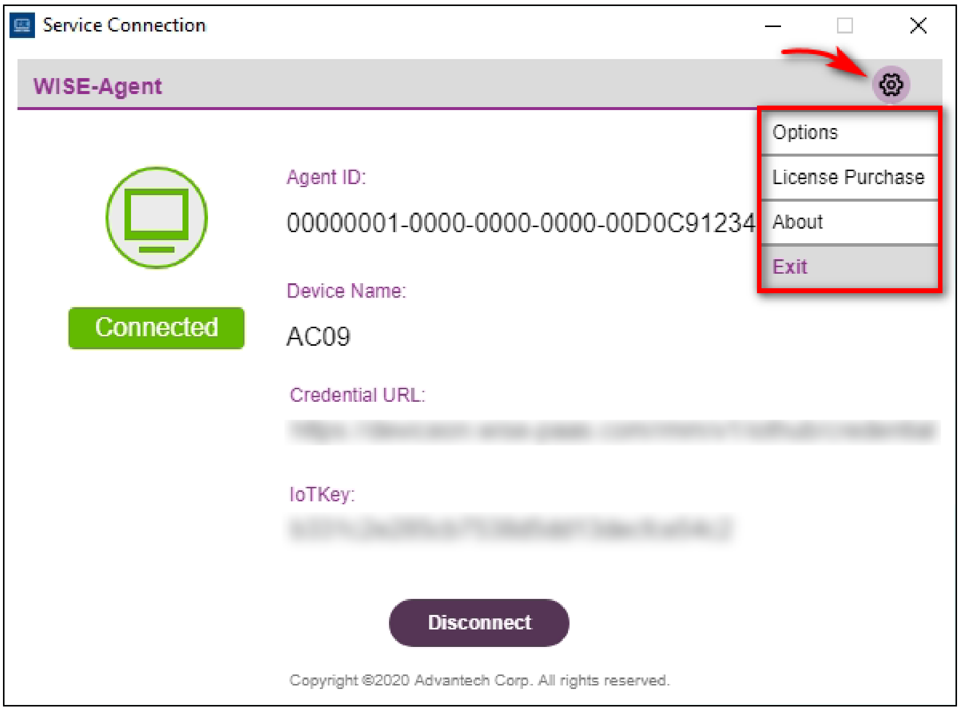
Credential URL:
[redacted]

IoTKey:
[redacted]

Copyright ©2020 Advantech Corp. All rights reserved.

- **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**”.



Agent ID:
00000001-0000-0000-0000-00D0C91234

Device Name:
AC09

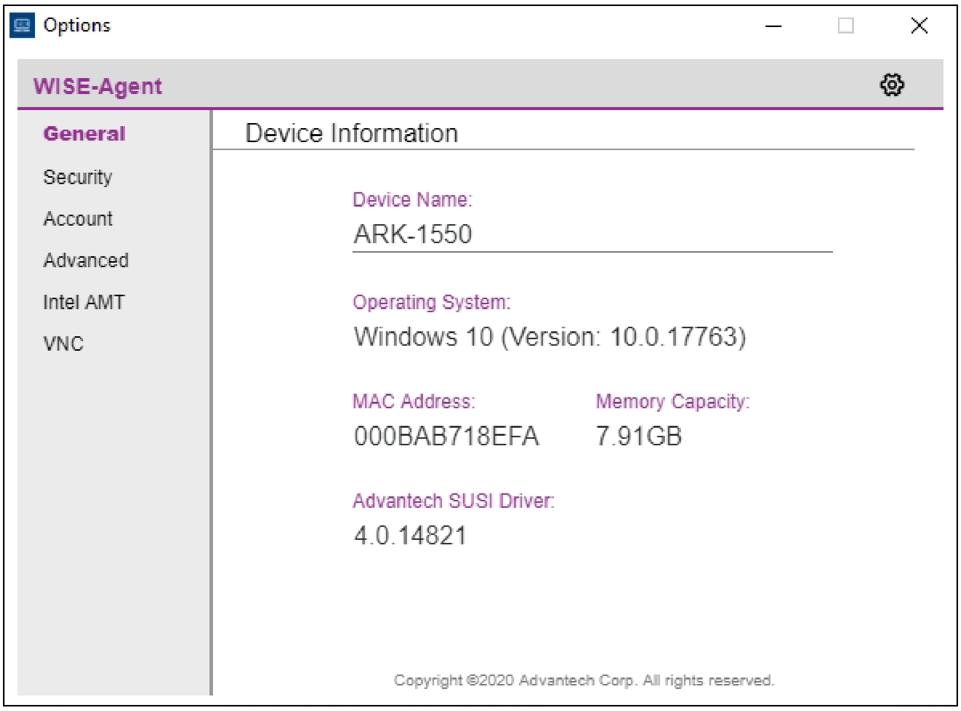
Credential URL:
[redacted]

IoTKey:
[redacted]

Copyright ©2020 Advantech Corp. All rights reserved.

- 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.



Device Information

Device Name:
ARK-1550

Operating System:
Windows 10 (Version: 10.0.17763)

MAC Address:
000BAB718EFA

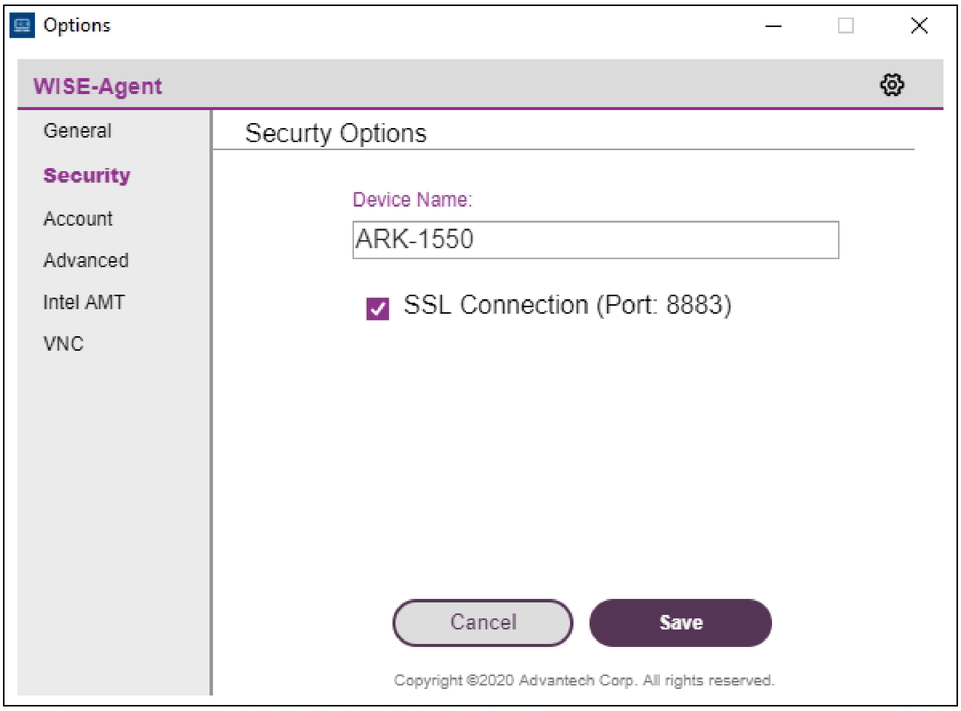
Memory Capacity:
7.91GB

Advantech SUSI Driver:
4.0.14821

Copyright ©2020 Advantech Corp. All rights reserved.

- 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**.



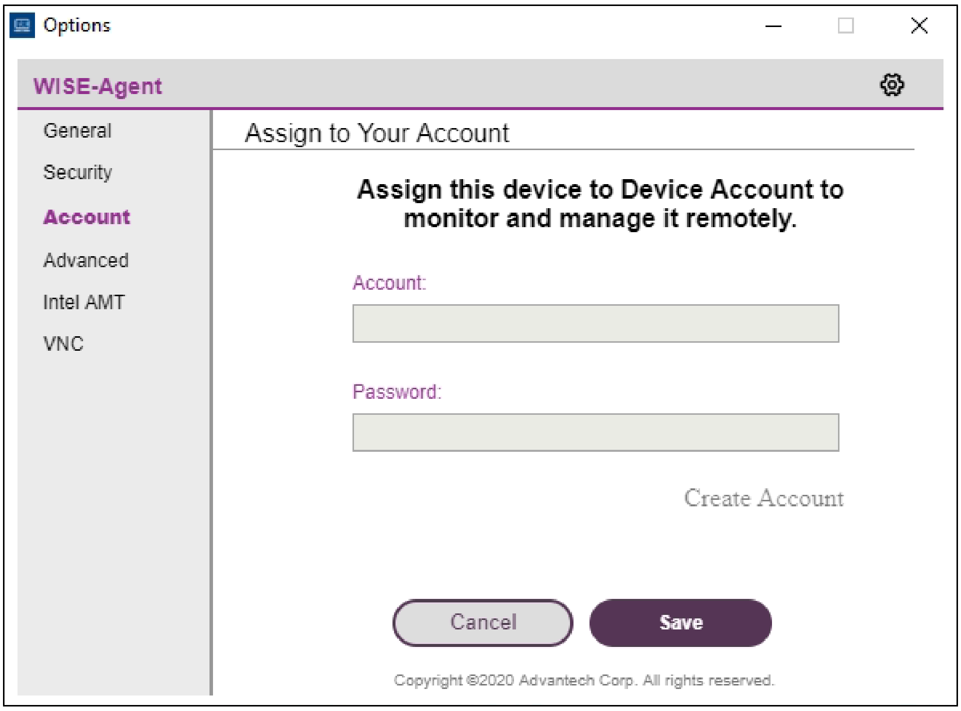
Device Name: ARK-1550

☑ SSL Connection (Port: 8883)

Copyright ©2020 Advantech Corp. All rights reserved.

- 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 got to the “Advanced” tab and select “Trial Account”.



Assign to Your Account

Assign this device to Device Account to monitor and manage it remotely.

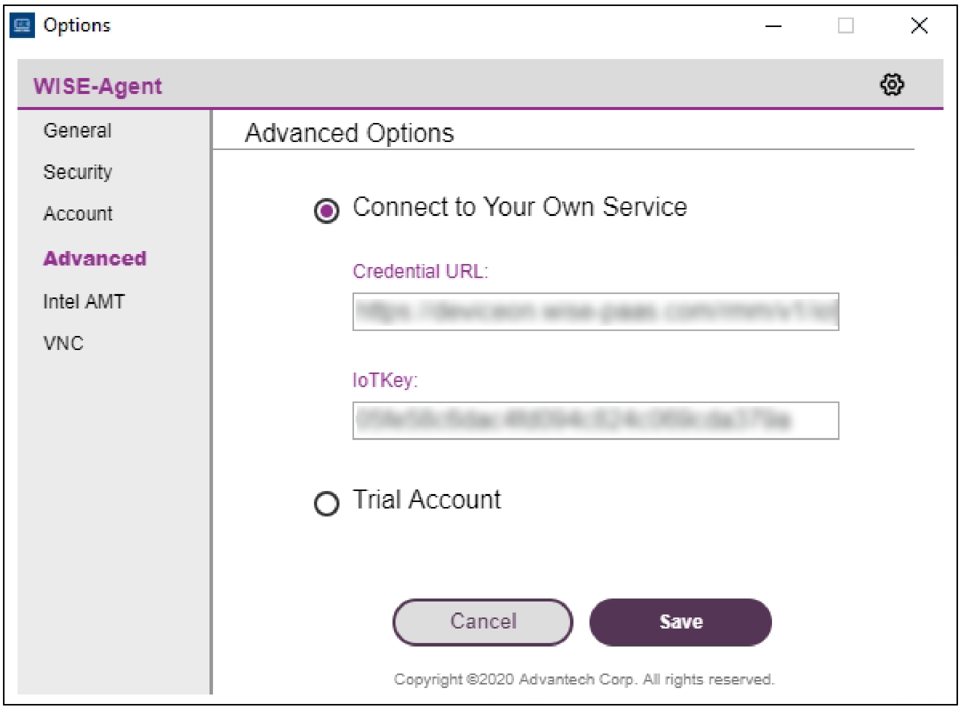
Account:

Password:

Copyright ©2020 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 2.2.1** on information how to obtain those.



Advanced Options

● Connect to Your Own Service

Credential URL: [redacted]

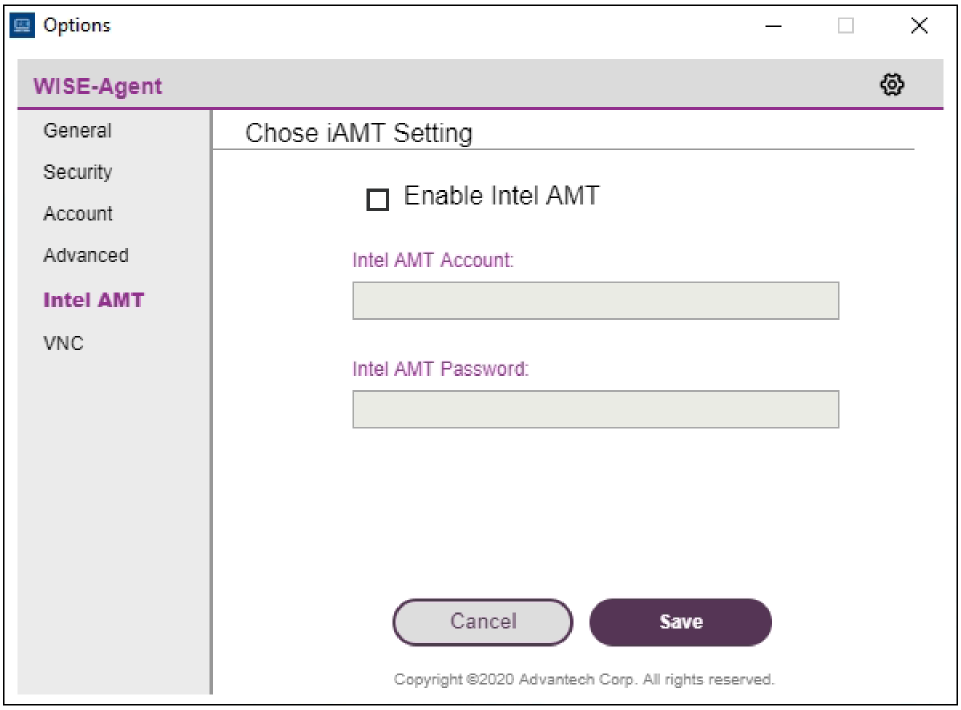
IoTKey: [redacted]

○ Trial Account

Copyright ©2020 Advantech Corp. All rights reserved.

- Option -> **Intel AMT**

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.



Chose iAMT Setting

□ Enable Intel AMT

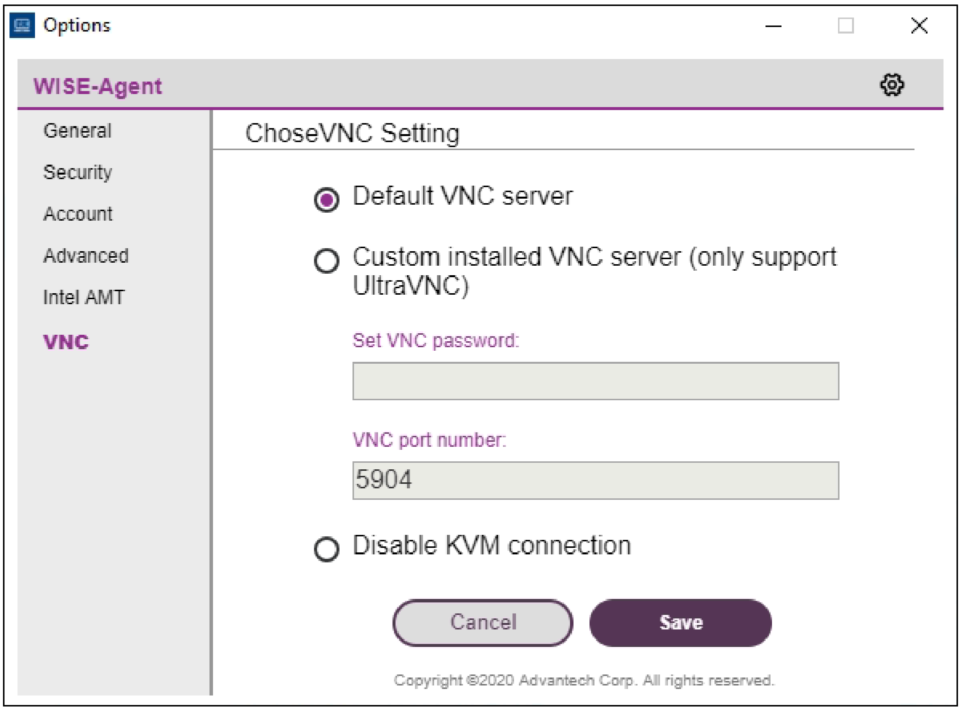
Intel AMT Account:

Intel AMT Password:

Copyright ©2020 Advantech Corp. All rights reserved.

- Option -> **VNC**

WISE-Agent supports remote desktop through built-in UltraVNC. You can manually specific the location of your own UltraVNC installation if preferred (Custom installed VNC server). If you do not want the remote desktop feature to be available, please select "Disable KVM Connection".



Options

WISE-Agent

ChoseVNC Setting

● Default VNC server

○ Custom installed VNC server (only support UltraVNC)

Set VNC password:

VNC port number: 5904

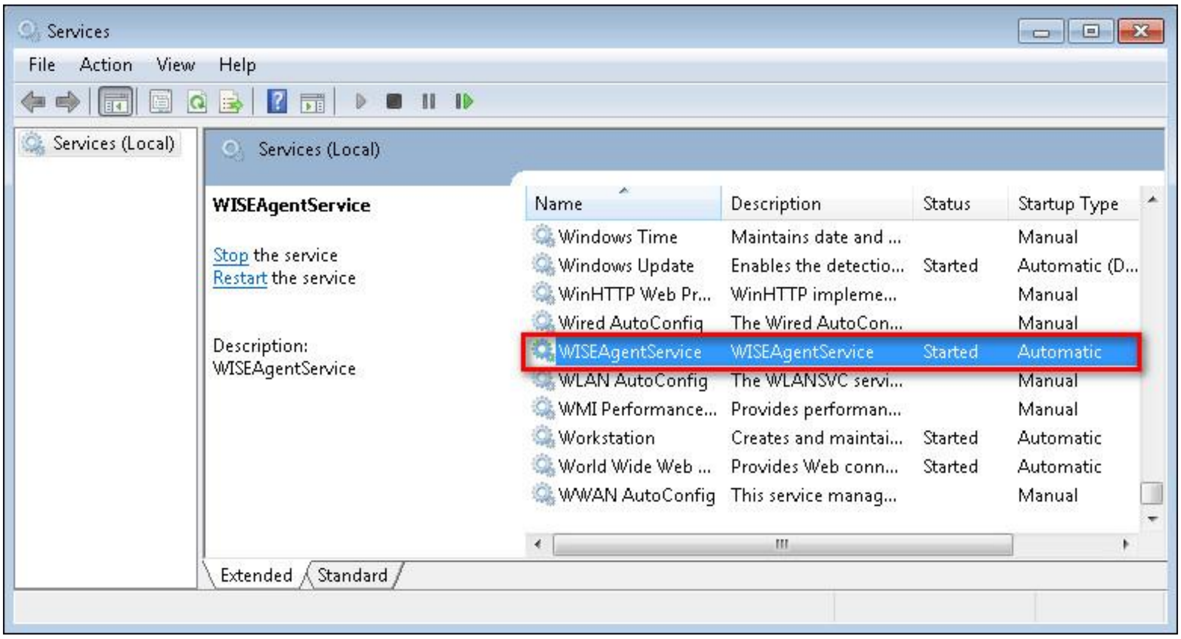
○ Disable KVM connection

Copyright ©2020 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.



WISEAgentService

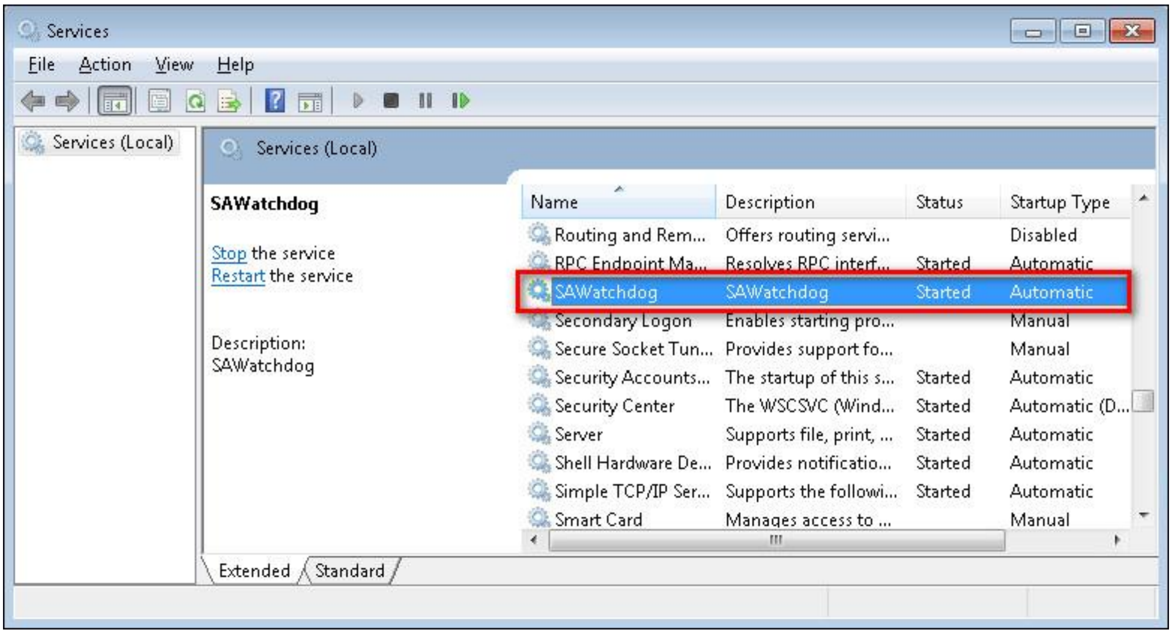
Stop the service
Restart the service

Description:
WISEAgentService

Name	Description	Status	Startup Type
Windows Time	Maintains date and ...		Manual
Windows Update	Enables the detectio...	Started	Automatic (D...
WinHTTP Web Pr...	WinHTTP impleme...		Manual
Wired AutoConfig	The Wired AutoCon...		Manual
WISEAgentService	WISEAgentService	Started	Automatic
WLAN AutoConfig	The WLANSVC servi...		Manual
WMI Performance...	Provides performan...		Manual
Workstation	Creates and maintai...	Started	Automatic
World Wide Web ...	Provides Web conn...	Started	Automatic
WWAN AutoConfig	This service manag...		Manual

- Watchdog Service

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



SAWatchdog

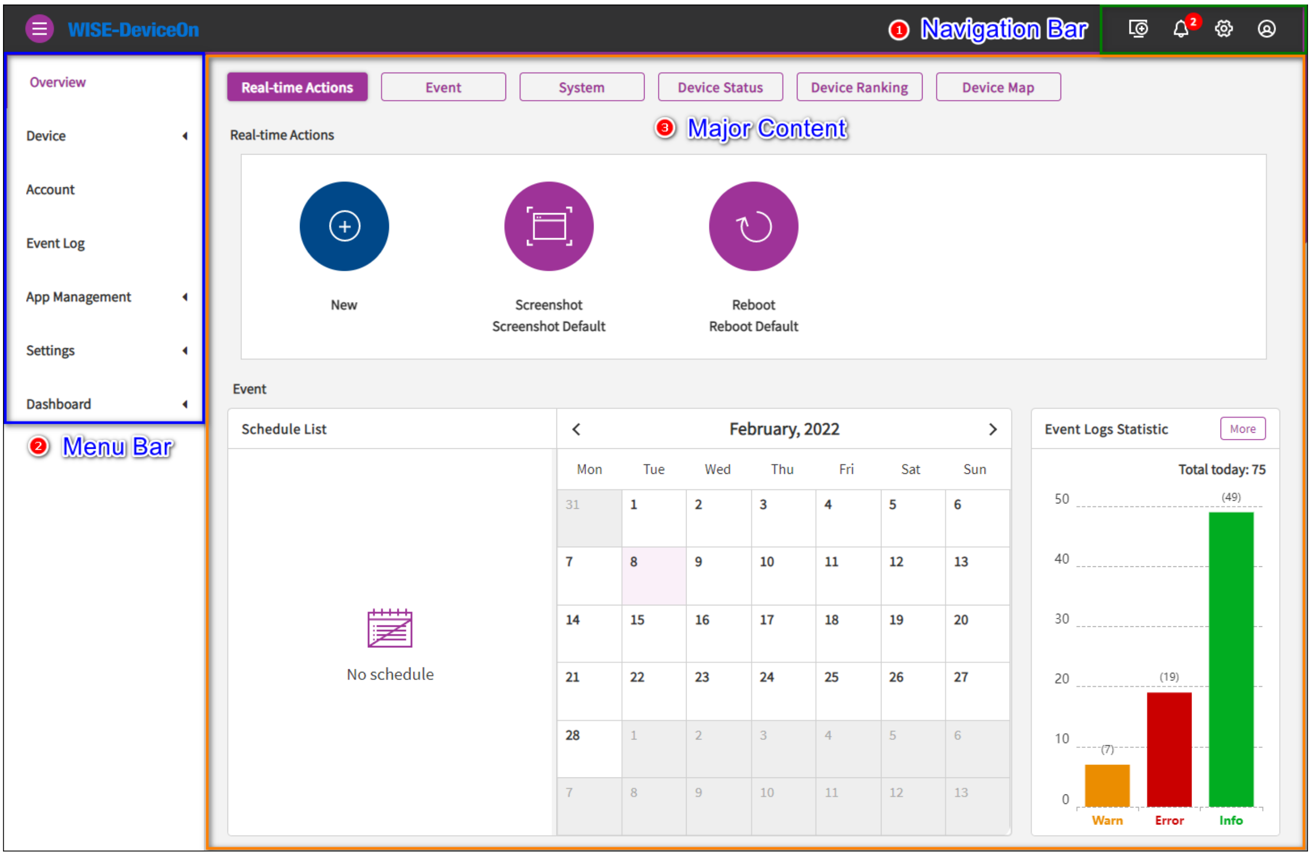
Stop the service
Restart the service

Description:
SAWatchdog

Name	Description	Status	Startup Type
Routing and Rem...	Offers routing servi...		Disabled
RPC Endpoint Ma...	Resolves RPC interf...	Started	Automatic
SAWatchdog	SAWatchdog	Started	Automatic
Secondary Logon	Enables starting pro...		Manual
Secure Socket Tun...	Provides support fo...		Manual
Security Accounts...	The startup of this s...	Started	Automatic
Security Center	The WSCSVC (Wind...	Started	Automatic (D...
Server	Supports file, print, ...	Started	Automatic
Shell Hardware De...	Provides notificatio...	Started	Automatic
Simple TCP/IP Ser...	Supports the followi...	Started	Automatic
Smart Card	Manages access to ...		Manual

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.

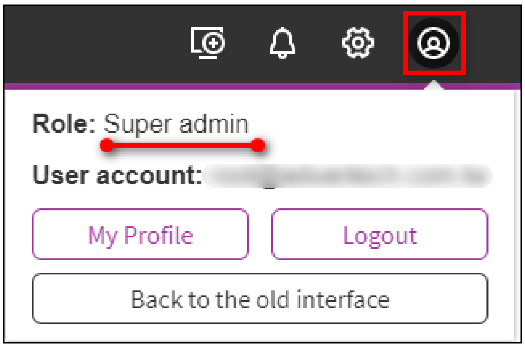


Mon	Tue	Wed	Thu	Fri	Sat	Sun
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

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.

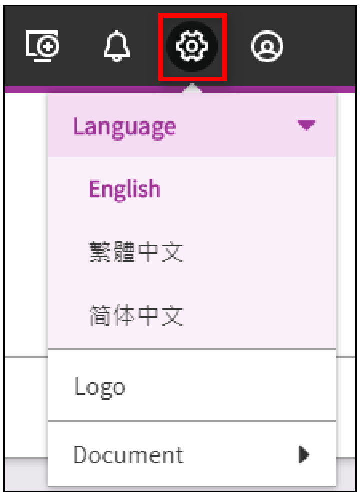


Role: Super admin

User account: [redacted]

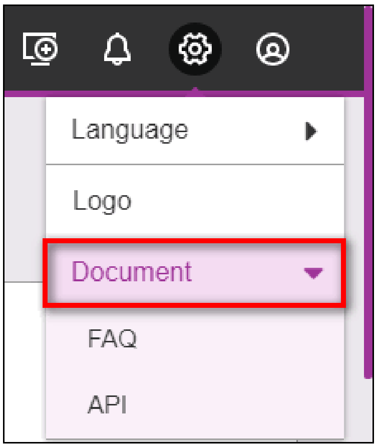
- Languages

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.

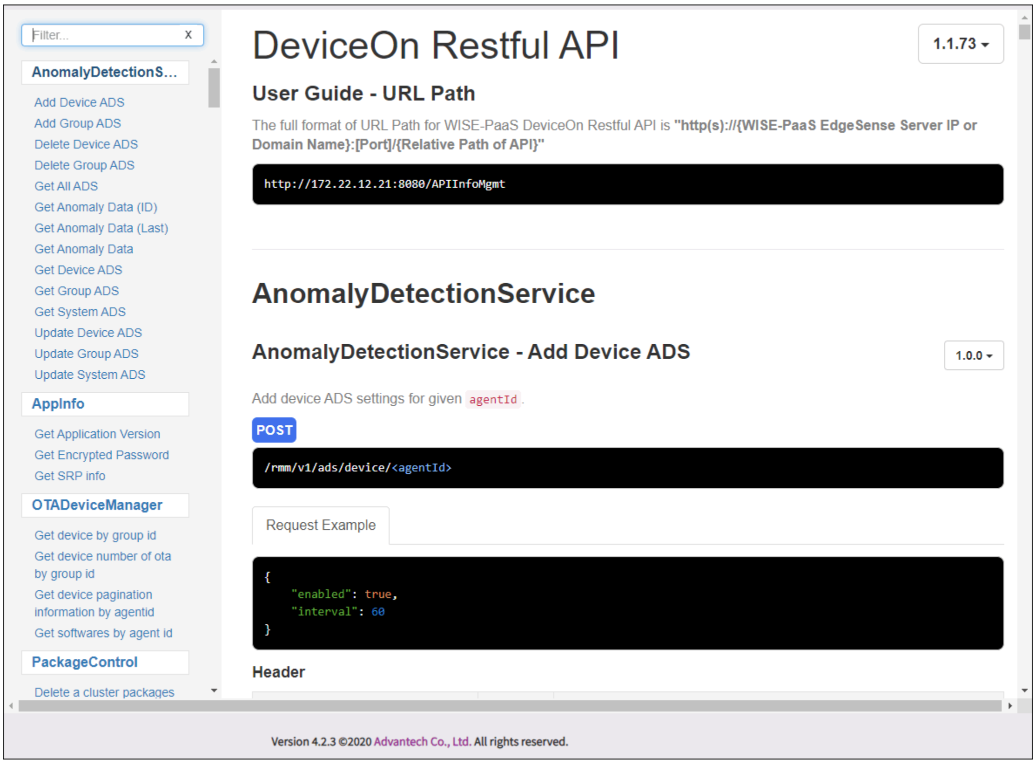


- Document (FAQ & API Reference)

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 Restful API

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}"**

```
http://172.22.12.21:8080/APIInfoMgmt
```

AnomalyDetectionService

AnomalyDetectionService - Add Device ADS

Add device ADS settings for given `agentId`.

```
/rmm/v1/ads/device/<agentId>
```

```
{
    "enabled": true,
    "interval": 60
}
```

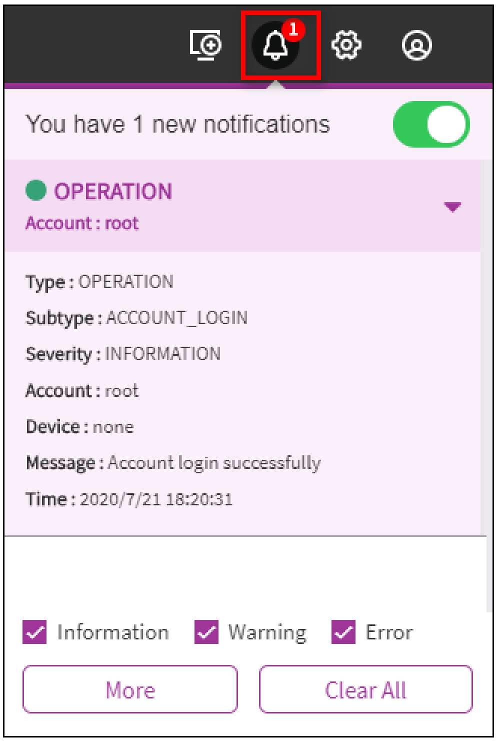
Header

Version 4.2.3 ©2020 Advantech Co., Ltd. All rights reserved.

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)

- 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**)


You have 1 new notifications

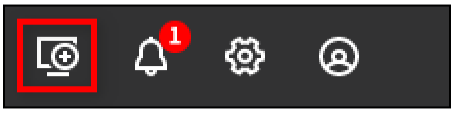
OPERATION
Account : root

Type : OPERATION
Subtype : ACCOUNT_LOGIN
Severity : INFORMATION
Account : root
Device : none
Message : Account login successfully
Time : 2020/7/21 18:20:31

☑ Information ☑ Warning ☑ Error

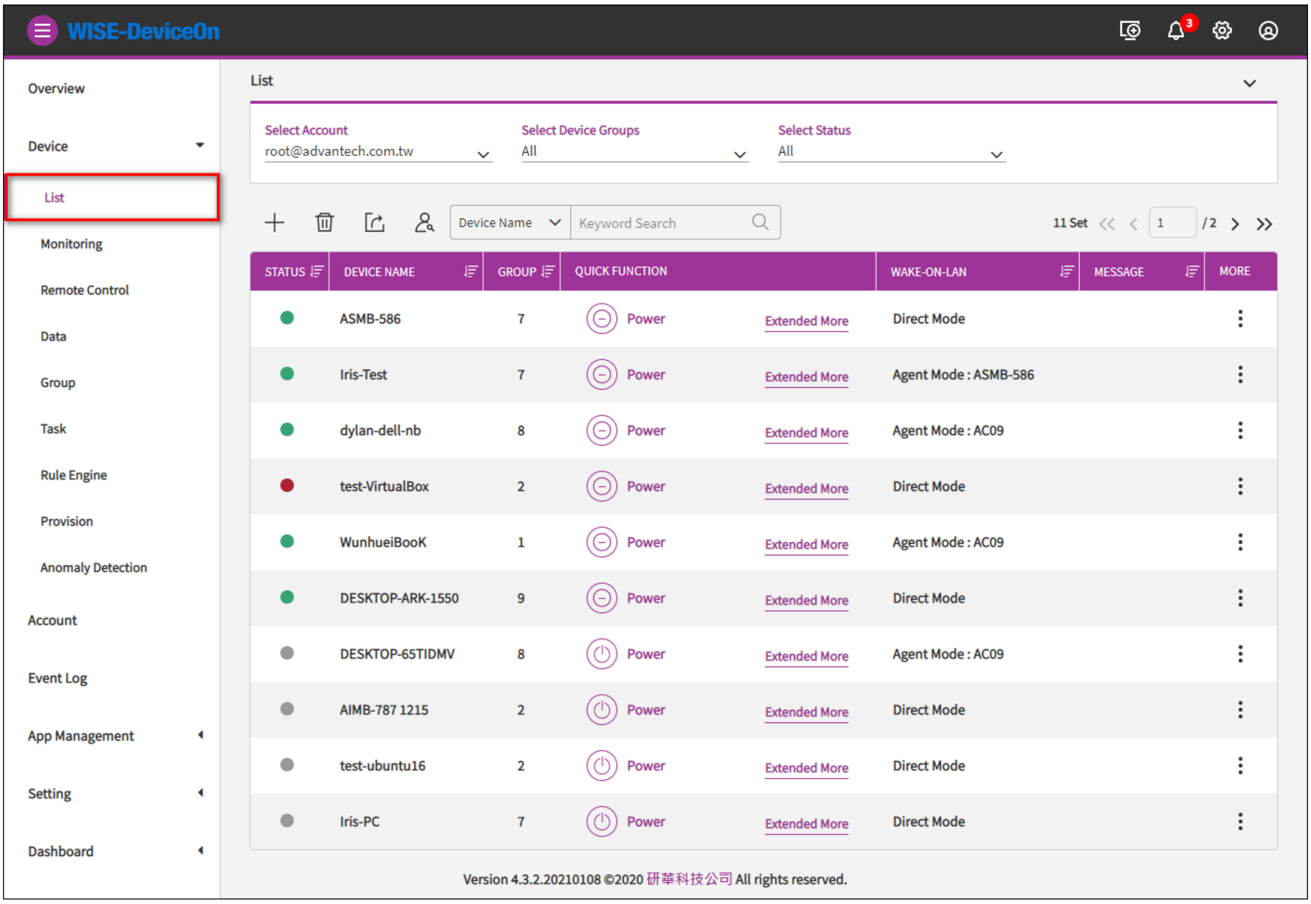
- Device Onboarding

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.



3.3.1 Device Management

After your device onboarding, you could view, edit device basic information, remote control, and retrieve sensor data on your devices. Eight sub items under Device, Device List contain device name, upgrade status, power management and etc. Device Monitoring to give device loading at present. To remote diagnostic and debug through Remote Control. Next, all of plugin sensor data from Device Data. To grouping your device through the Device Group. Rule Engine to set a threshold rule for your devices data in real-time. For advanced configuration, such as WoL, System Backup/Recovery and Protection via Device Provisioning. The last, one of AI solution to detect device screen status on Anomaly Detection.



List

Select Account: root@advantech.com.tw
Select Device Groups: All
Select Status: All

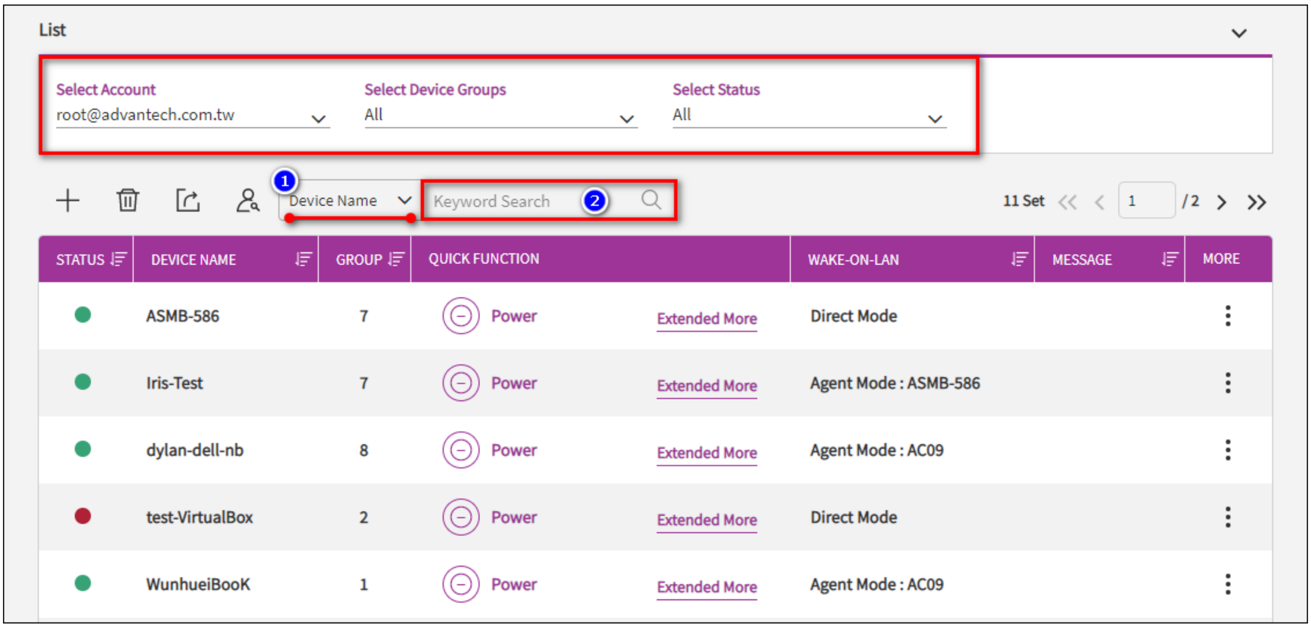
Device Name | Keyword Search | 11 Set | 1 /2

STATUS	DEVICE NAME	GROUP	QUICK FUNCTION		WAKE-ON-LAN	MESSAGE	MORE
●	ASMB-586	7	Power	Extended More	Direct Mode		⋮
●	Iris-Test	7	Power	Extended More	Agent Mode : ASMB-586		⋮
●	dylan-dell-nb	8	Power	Extended More	Agent Mode : AC09		⋮
●	test-VirtualBox	2	Power	Extended More	Direct Mode		⋮
●	WunhueiBooK	1	Power	Extended More	Agent Mode : AC09		⋮
●	DESKTOP-ARK-1550	9	Power	Extended More	Direct Mode		⋮
●	DESKTOP-65TIDMV	8	Power	Extended More	Agent Mode : AC09		⋮
●	AIMB-787 1215	2	Power	Extended More	Direct Mode		⋮
●	test-ubuntu16	2	Power	Extended More	Direct Mode		⋮
●	Iris-PC	7	Power	Extended More	Direct Mode		⋮

Version 4.3.2.20210108 ©2020 研華科技公司 All rights reserved.

- 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, Status** or **Keyword**.



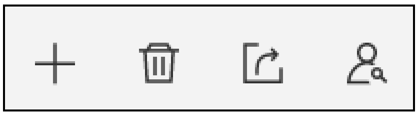
List

Select Account: root@advantech.com.tw
Select Device Groups: All
Select Status: All

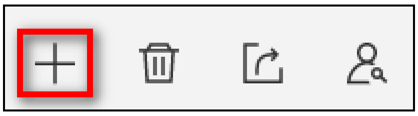
Device Name | Keyword Search | 11 Set | 1 /2

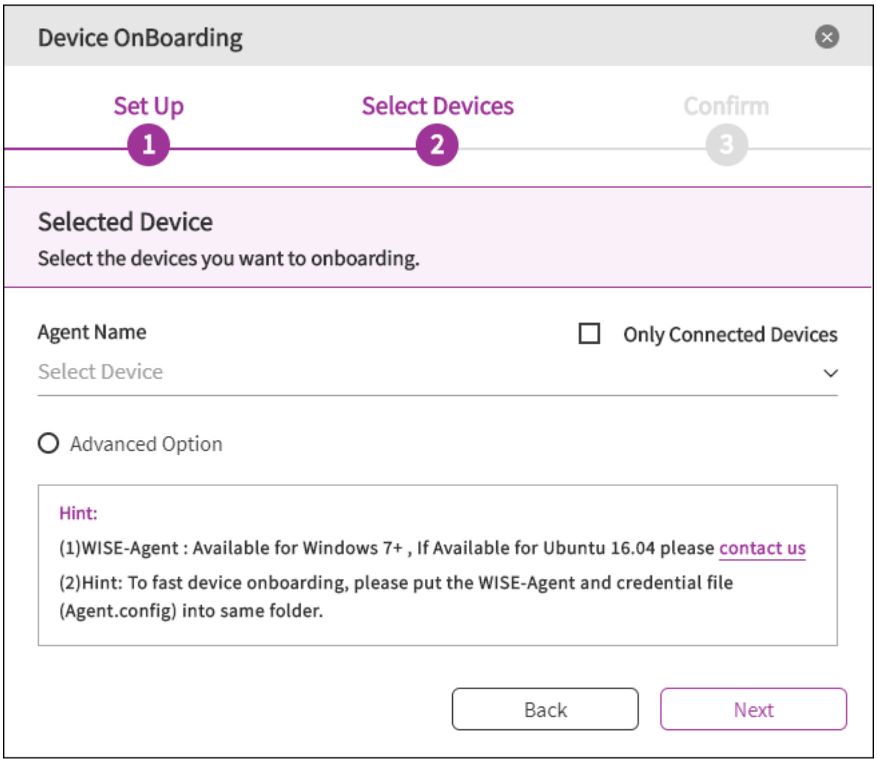
STATUS	DEVICE NAME	GROUP	QUICK FUNCTION		WAKE-ON-LAN	MESSAGE	MORE
●	ASMB-586	7	Power	Extended More	Direct Mode		⋮
●	Iris-Test	7	Power	Extended More	Agent Mode : ASMB-586		⋮
●	dylan-dell-nb	8	Power	Extended More	Agent Mode : AC09		⋮
●	test-VirtualBox	2	Power	Extended More	Direct Mode		⋮
●	WunhueiBooK	1	Power	Extended More	Agent Mode : AC09		⋮

Here is action bar for add, remove, export and search 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.





Device OnBoarding

Selected Device

Select the devices you want to onboarding.

Agent Name

□ Only Connected Devices

Select Device

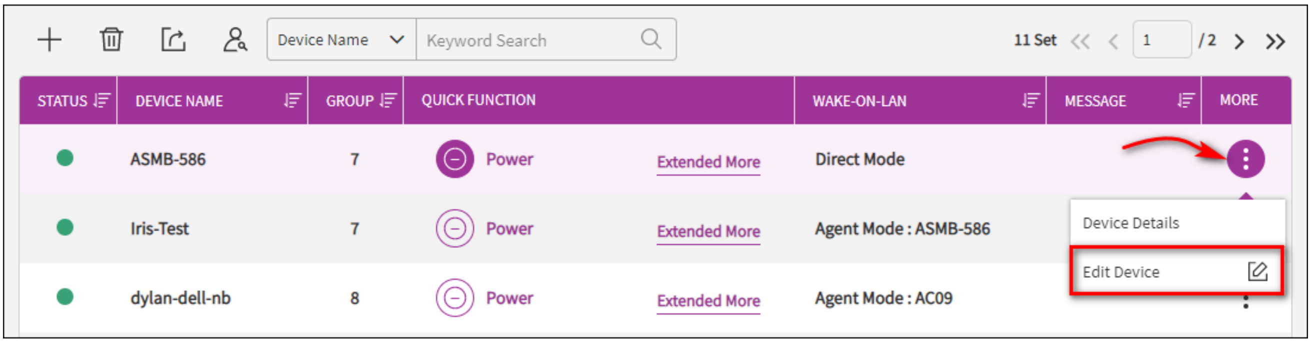
○ Advanced Option

Hint:

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

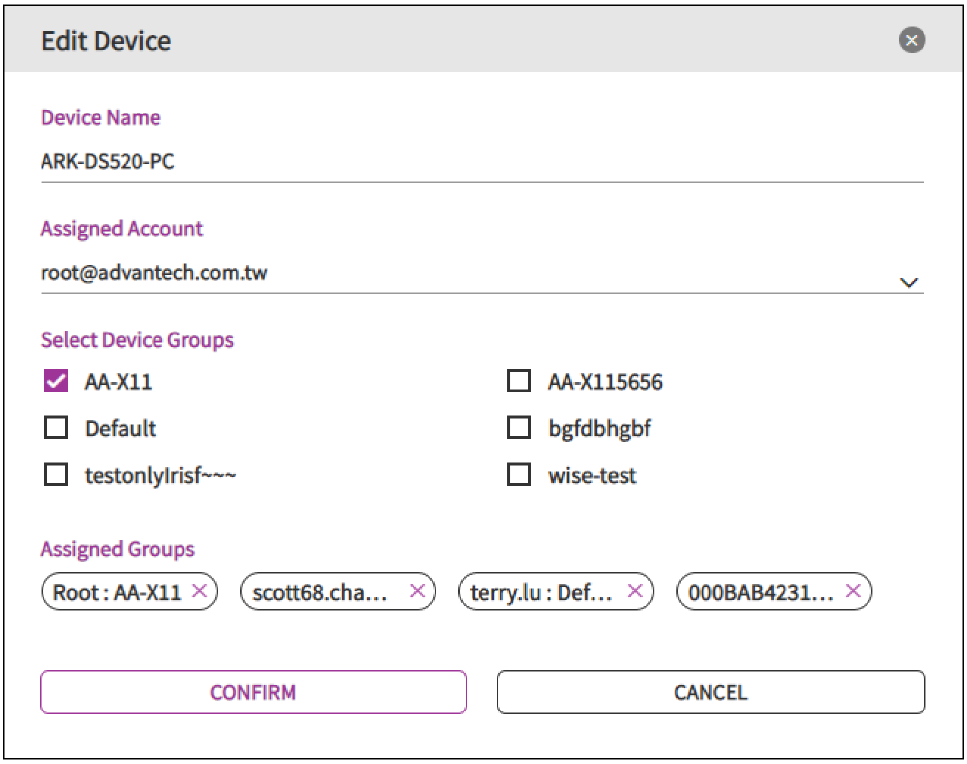
(2)Hint: To fast device onboarding, please put the WISE-Agent and credential file (Agent.config) into same folder.

Click the more icon to display "**Edit**" options on each device list.



STATUS	DEVICE NAME	GROUP	QUICK FUNCTION		WAKE-ON-LAN	MESSAGE	MORE
●	ASMB-586	7	Power	Extended More	Direct Mode		⋮
●	Iris-Test	7	Power	Extended More	Agent Mode : ASMB-586		
●	dylan-dell-nb	8	Power	Extended More	Agent Mode : AC09		⋮

You could edit device name, assign to different accounts, device groups in "**Edit Device**"



Edit Device

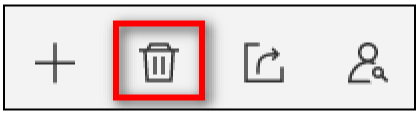
Device Name
ARK-DS520-PC

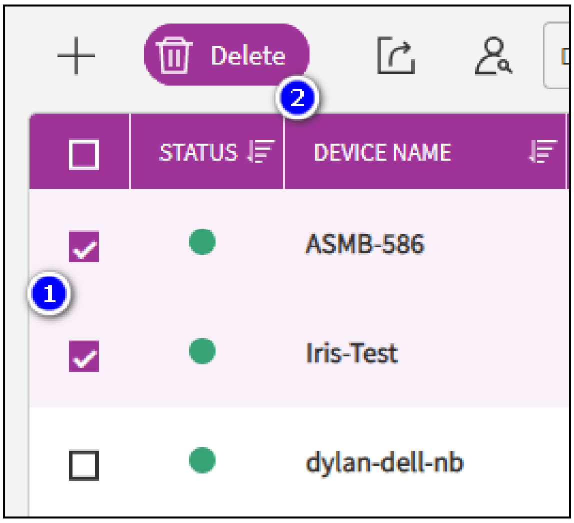
Assigned Account
root@advantech.com.tw

Select Device Groups
☑ AA-X11 ☐ AA-X115656
☐ Default ☐ bgfdbhgbf
☐ testonlylrisf~~~ ☐ wise-test

Assigned Groups
Root : AA-X11 × scott68.cha… × terry.lu : Def… × 000BAB4231… ×

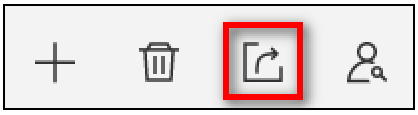
Click the delete icon to display “**Delete**” options on each device list, pick up the checkbox and confirm to delete these devices.

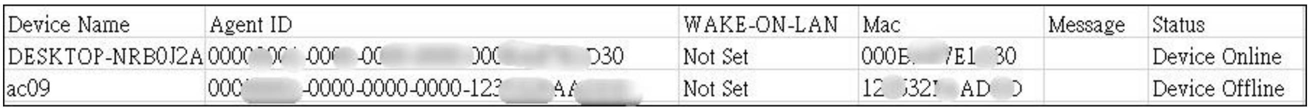




☐	STATUS	DEVICE NAME
☑	●	ASMB-586
☑	●	Iris-Test
☐	●	dylan-dell-nb

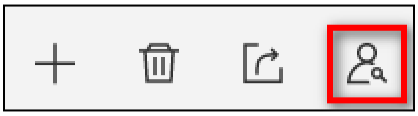
Click on export icon to export devices that in the table as CSV file.

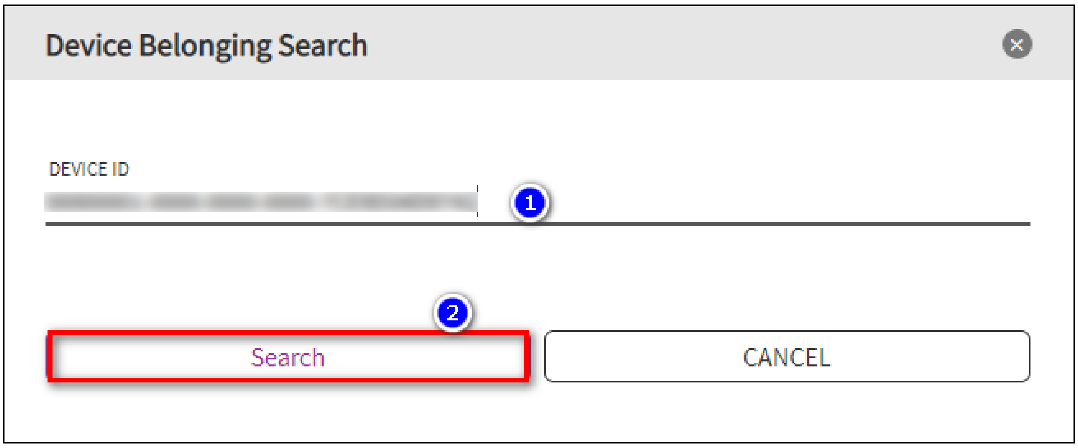




Device Name	Agent ID	WAKE-ON-LAN	Mac	Message	Status
DESKTOP-NRB0J2A	000[redacted]00[redacted]00[redacted]D30	Not Set	000B[redacted]7E1[redacted]30		Device Online
ac09	000[redacted]-0000-0000-0000-123[redacted]AA[redacted]	Not Set	12[redacted]32[redacted]AD[redacted]D		Device Offline

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.



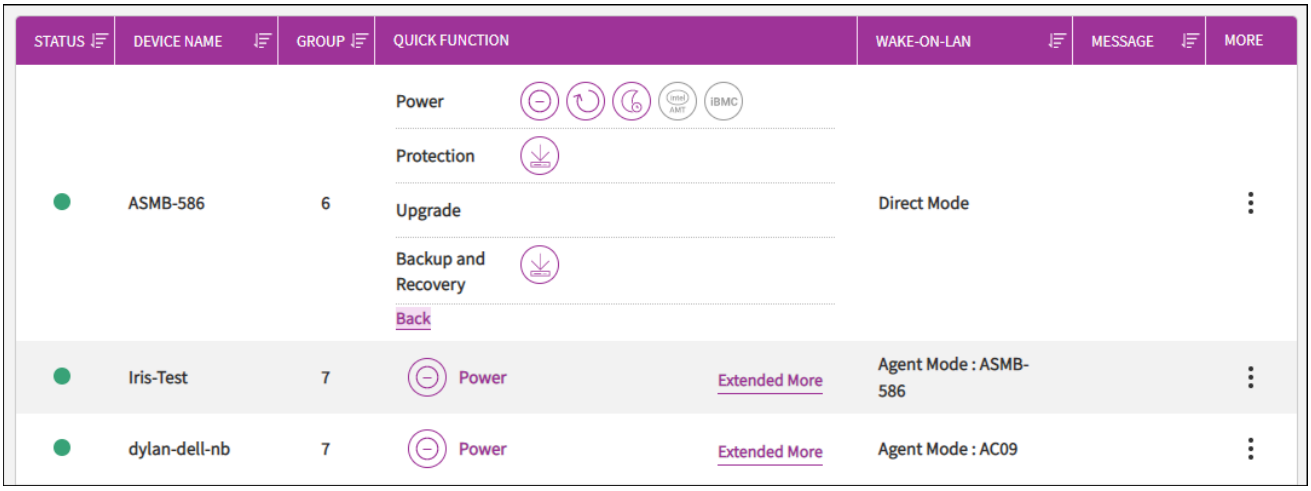


Device Belonging Search

DEVICE ID

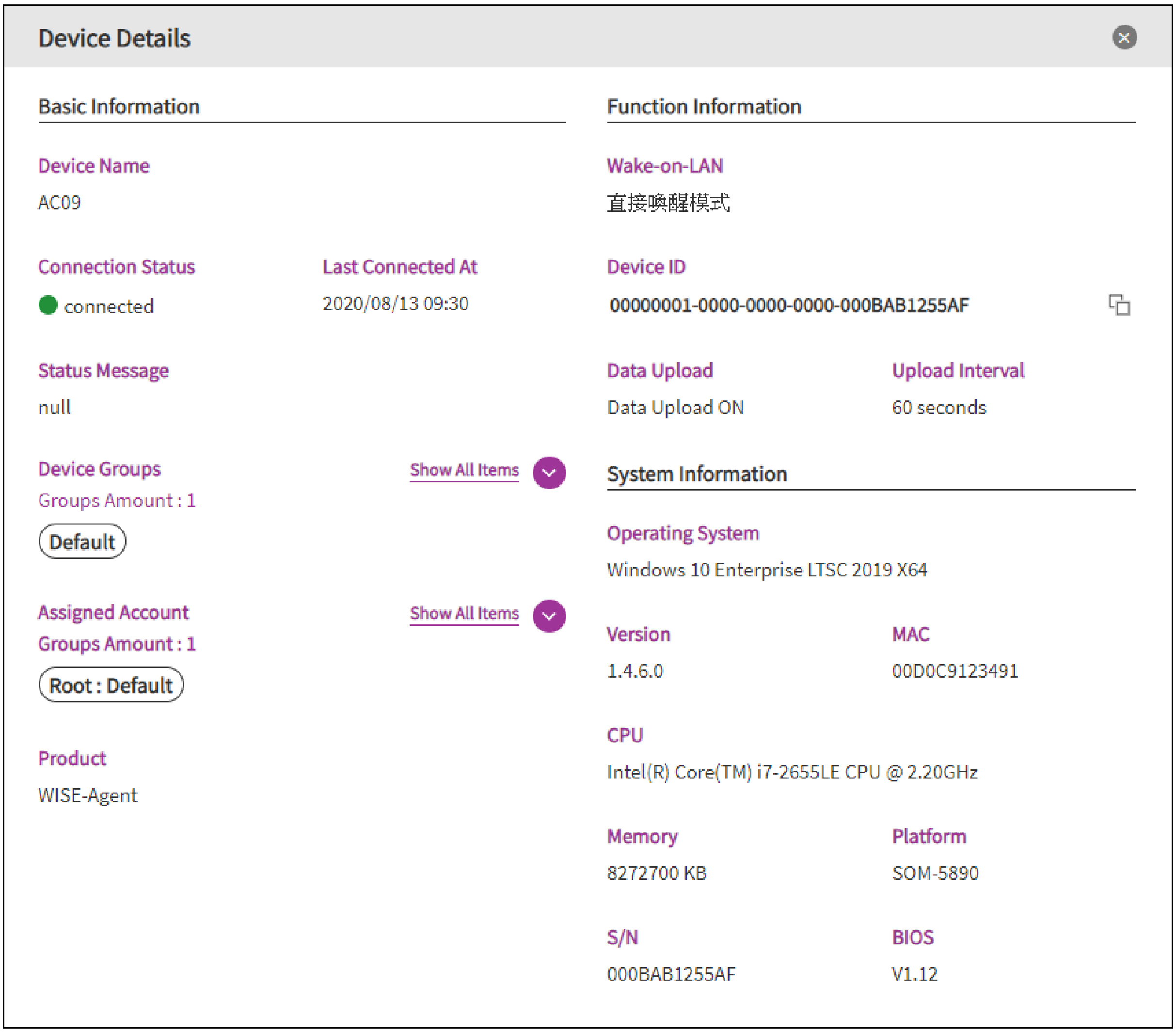
[redacted]

You cloud do lots of remote action on the device.



STATUS	DEVICE NAME	GROUP	QUICK FUNCTION	WAKE-ON-LAN	MESSAGE	MORE
●	ASMB-586	6	Power Protection Upgrade Backup and Recovery Back	Direct Mode		⋮
●	Iris-Test	7	Power Extended More	Agent Mode : ASMB-586		⋮
●	dylan-dell-nb	7	Power Extended More	Agent Mode : AC09		⋮

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



Device Details

Basic Information

Device Name
AC09

Connection Status
● connected

Last Connected At
2020/08/13 09:30

Status Message
null

Device Groups
Groups Amount : 1
Default

Assigned Account
Groups Amount : 1
Root : Default

Product
WISE-Agent

Function Information

Wake-on-LAN
直接喚醒模式

Device ID
00000001-0000-0000-0000-000BAB1255AF

Data Upload
Data Upload ON

Upload Interval
60 seconds

System Information

Operating System
Windows 10 Enterprise LTSC 2019 X64

Version
1.4.6.0

MAC
00D0C9123491

CPU
Intel(R) Core(TM) i7-2655LE CPU @ 2.20GHz

Memory
8272700 KB

Platform
SOM-5890

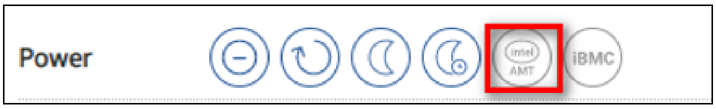
S/N
000BAB1255AF

BIOS
V1.12

- ✧ **Group**: Number of groups for the devices, for example, the device could belong to multiple groups.
- ✧ **Quick Functions**: Including **Power Management**, **System Protection**, **Upgrade** WISE-Agent and **System Backup/Recovery**.

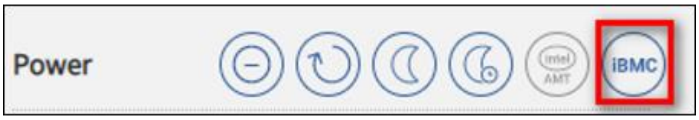
  The power management supports **On/Off**, **Restart**, **Sleep** and **hibernate**, the actions depend on your device supported. These functions adopt software mechanism, and most of the industrial PC, personal laptop supported.

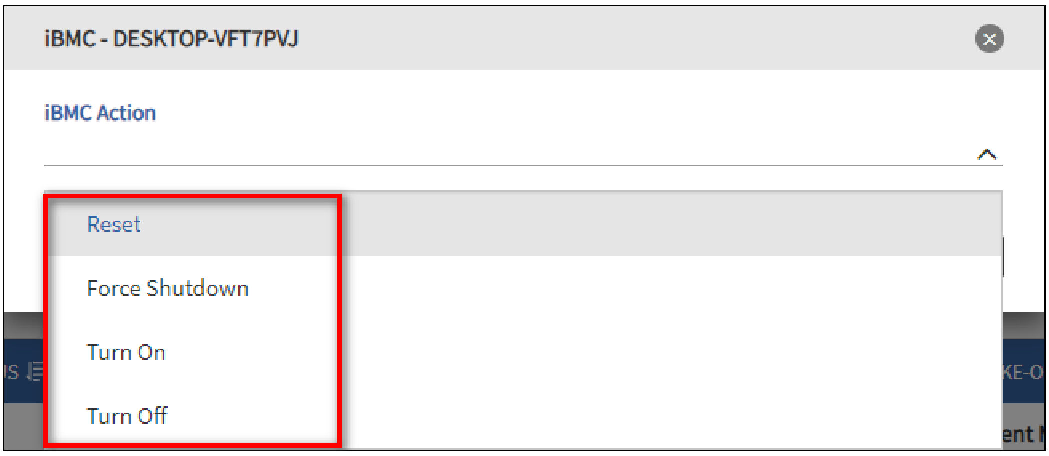
  Moreover, DeviceOn integrate Intel AMT (Intel Active Management Technology) for power device **up**, **reboot** and **hardware reset**. Please make sure you enable the AMT function and configured on your WISE-Agent with AMT credential.



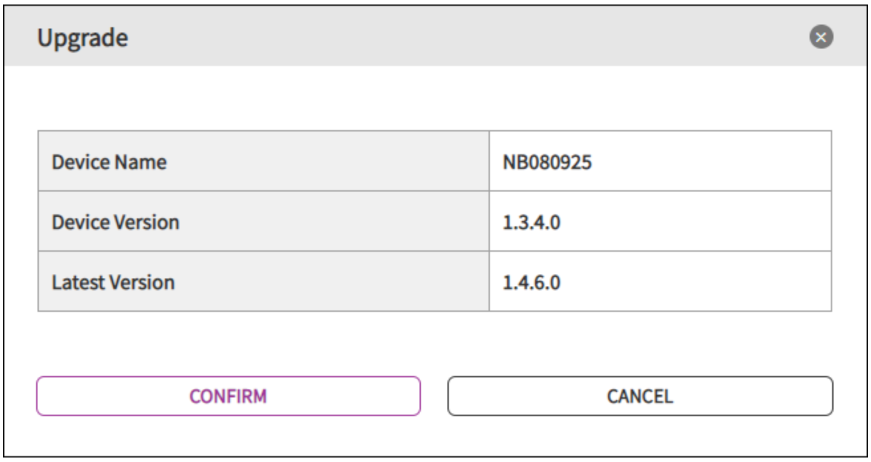
Next advanced power option is Advantech developed a mini-Baseboard Management

Controller named **iBMC** to provide out of band management. When the main system is abnormal or powered down, it can be powered on remotely and executed across networks, whether in public cloud or private.





Second, protection is 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. Next, for the WISE-Agent upgrade, if there is new version released by Advantech, it will check and show the icon automatically.



Device Name	NB080925
Device Version	1.3.4.0
Latest Version	1.4.6.0

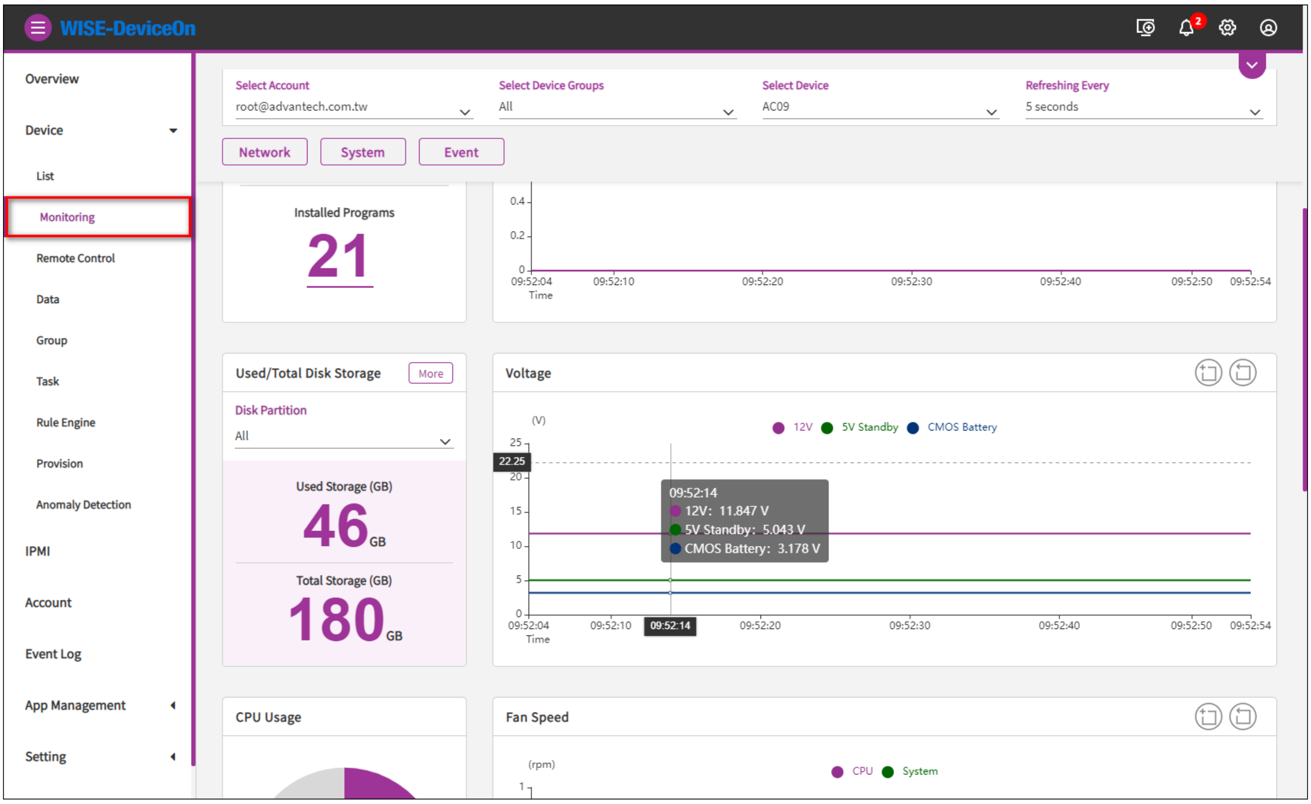
Fourth, System Backup/Recovery is power-by Acronis to backup/recovery device runtime system partition. Please go to **Setting** -> **Provision**-> **Backup/Recovery** to install first.

- **Wake-On-LAN**: Wake-On-LAN mode for device, three modes 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.



Select Account: root@advantech.com.tw

Select Device Groups: All

Select Device: AC09

Refreshing Every: 5 seconds

Installed Programs
21

Used/Total Disk Storage

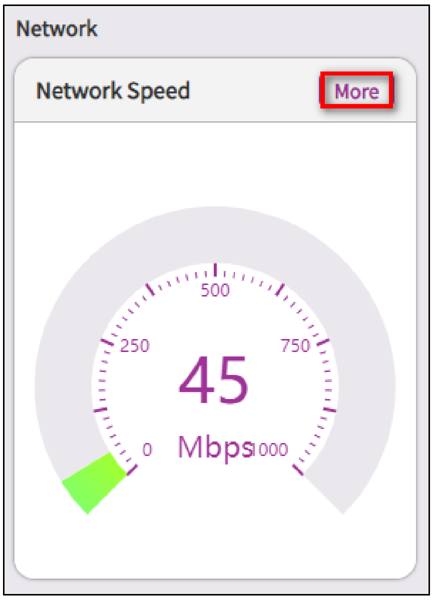
Disk Partition: All

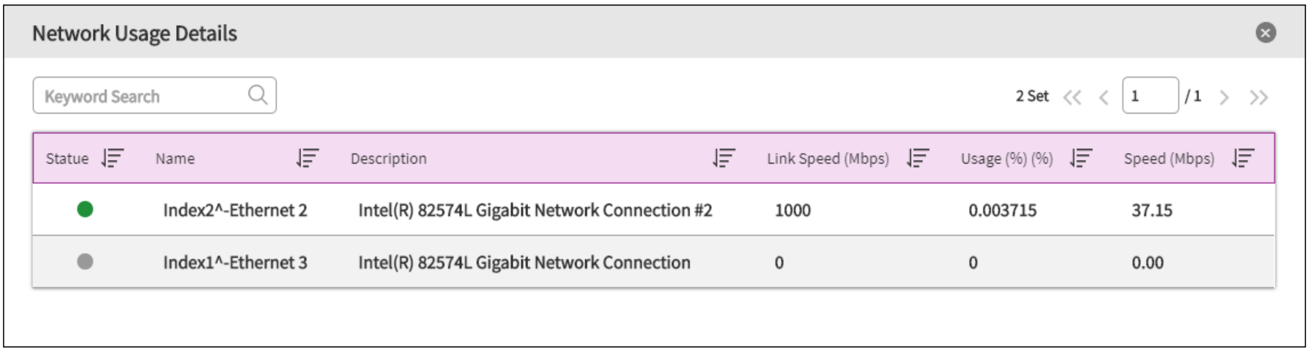
Used Storage (GB)
46 GB

Total Storage (GB)
180 GB

09:52:14
12V: 11.847 V
5V Standby: 5.043 V
CMOS Battery: 3.178 V

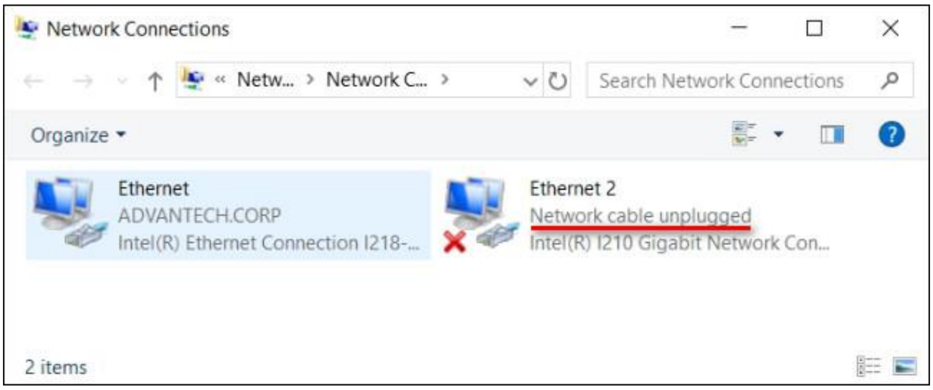
Some of devices support multiple network cards, especial industrial PC. Click on the network button to retrieve others.





Statue	Name	Description	Link Speed (Mbps)	Usage (%) (%)	Speed (Mbps)
●	Index2^-Ethernet 2	Intel(R) 82574L Gigabit Network Connection #2	1000	0.003715	37.15
●	Index1^-Ethernet 3	Intel(R) 82574L Gigabit Network Connection	0	0	0.00

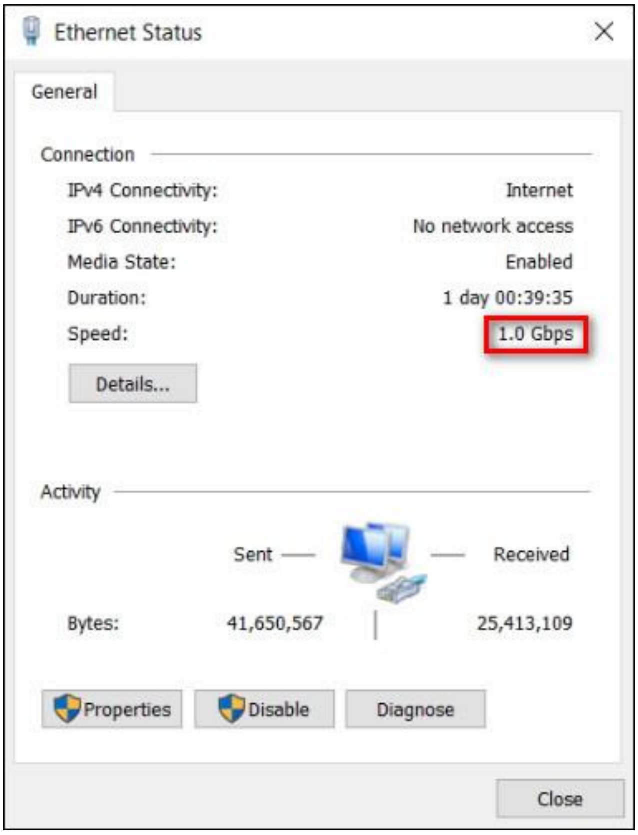
- ✧ **Name**: Name of network card
- ✧ **Description**: network description
- ✧ **State**: Network connected or disconnected, for example, ethernet cable plugin or not.



Ethernet
ADVANTECH.CORP
Intel(R) Ethernet Connection I218-...

Ethernet 2
Network cable unplugged
Intel(R) I210 Gigabit Network Con...

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



Ethernet Status

Connection

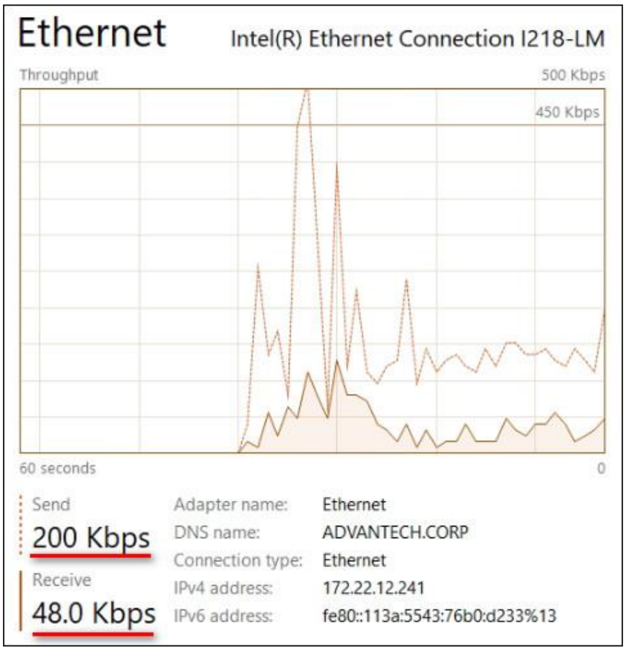
IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 1 day 00:39:35
Speed: 1.0 Gbps

Activity

Sent — — Received

Bytes: 41,650,567 | 25,413,109

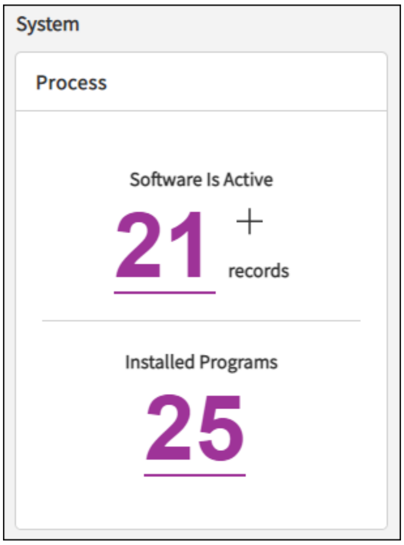
- ✧ **Usage:** Network current usage, **Speed/Link Speed**.
- ✧ **Speed (MBPS):** Send plus receive data rate.



Send
200 Kbps
Receive
48.0 Kbps

Adapter name: Ethernet
DNS name: ADVANTECH.CORP
Connection type: Ethernet
IPv4 address: 172.22.12.241
IPv6 address: fe80::113a:5543:76b0:d233%13

Click on **Software Process** to show **current user process** list, if your device system not login, the result might be zero. Also, click on “**Installed Programs**” to check the programs on the device.



System

Process

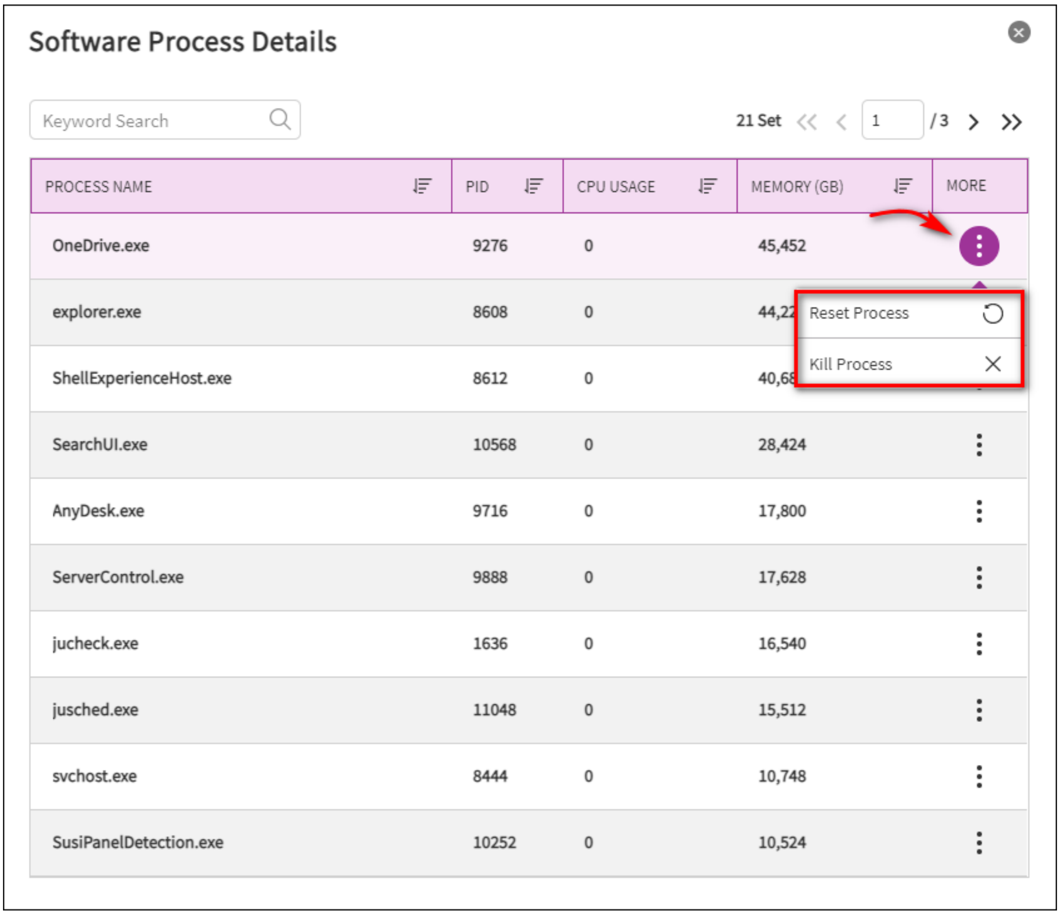
Software Is Active

21 + records

Installed Programs

25

Click on the more option to restart or terminal your specific process.



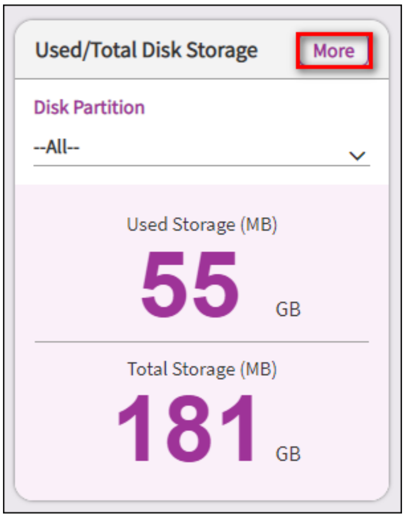
Software Process Details

Keyword Search

21 Set 1 /3

PROCESS NAME	PID	CPU USAGE	MEMORY (GB)	MORE
OneDrive.exe	9276	0	45,452	⋮
explorer.exe	8608	0	44,22	Reset Process
ShellExperienceHost.exe	8612	0	40,68	Kill Process
SearchUI.exe	10568	0	28,424	⋮
AnyDesk.exe	9716	0	17,800	⋮
ServerControl.exe	9888	0	17,628	⋮
jucheck.exe	1636	0	16,540	⋮
jusched.exe	11048	0	15,512	⋮
svchost.exe	8444	0	10,748	⋮
SusiPanelDetection.exe	10252	0	10,524	⋮

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, refer to the official page.

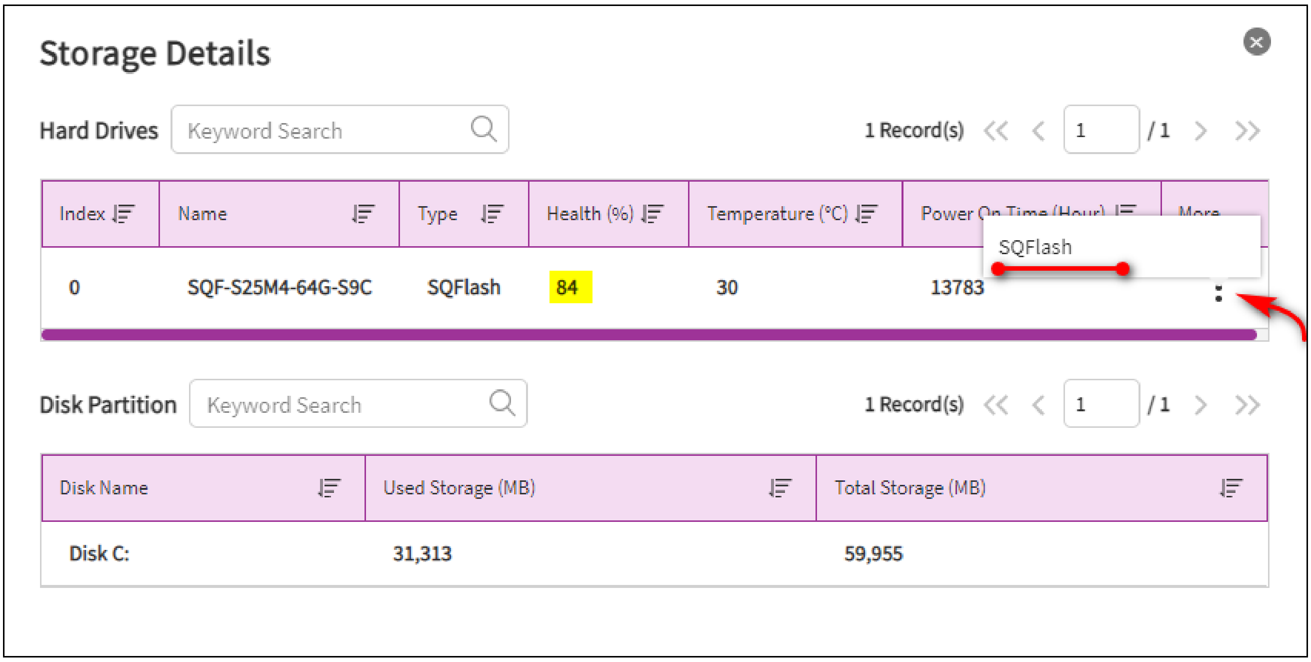


Used/Total Disk Storage

Disk Partition: --All--

Used Storage (MB)
55 GB

Total Storage (MB)
181 GB



Storage Details

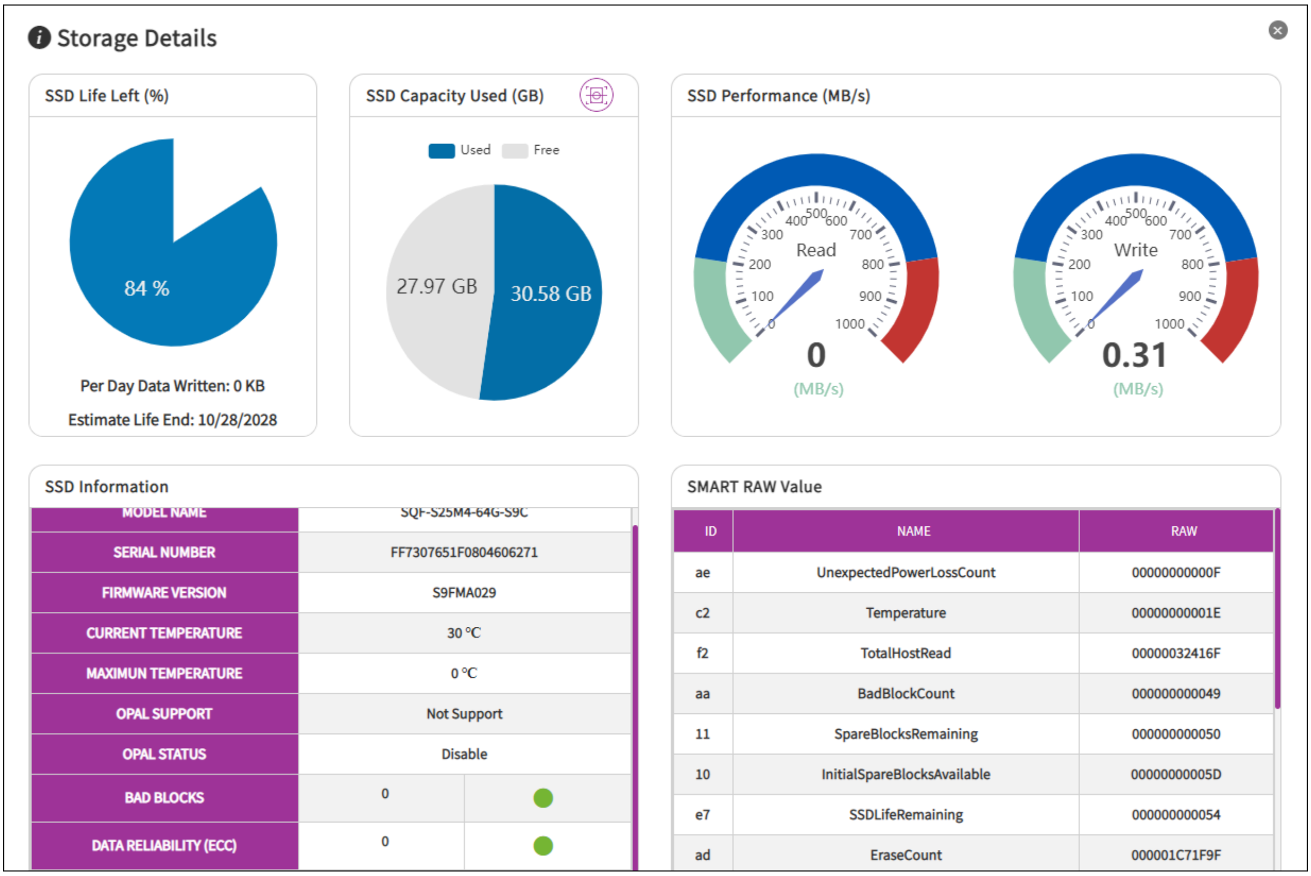
Hard Drives

Index	Name	Type	Health (%)	Temperature (°C)	Power On Time (Hour)	More
0	SQF-S25M4-64G-S9C	SQFlash	84	30	13783	⋮

Disk Partition

Disk Name	Used Storage (MB)	Total Storage (MB)
Disk C:	31,313	59,955

For Advantech industrial SQ Flash, we provide advanced information, such as SSD performance, per day host & NAND Data Volume, Estimate life End, self-check and so on.



Storage Details

SSD Life Left (%)

Per Day Data Written: 0 KB

Estimate Life End: 10/28/2028

SSD Capacity Used (GB)

SSD Performance (MB/s)

SSD Information

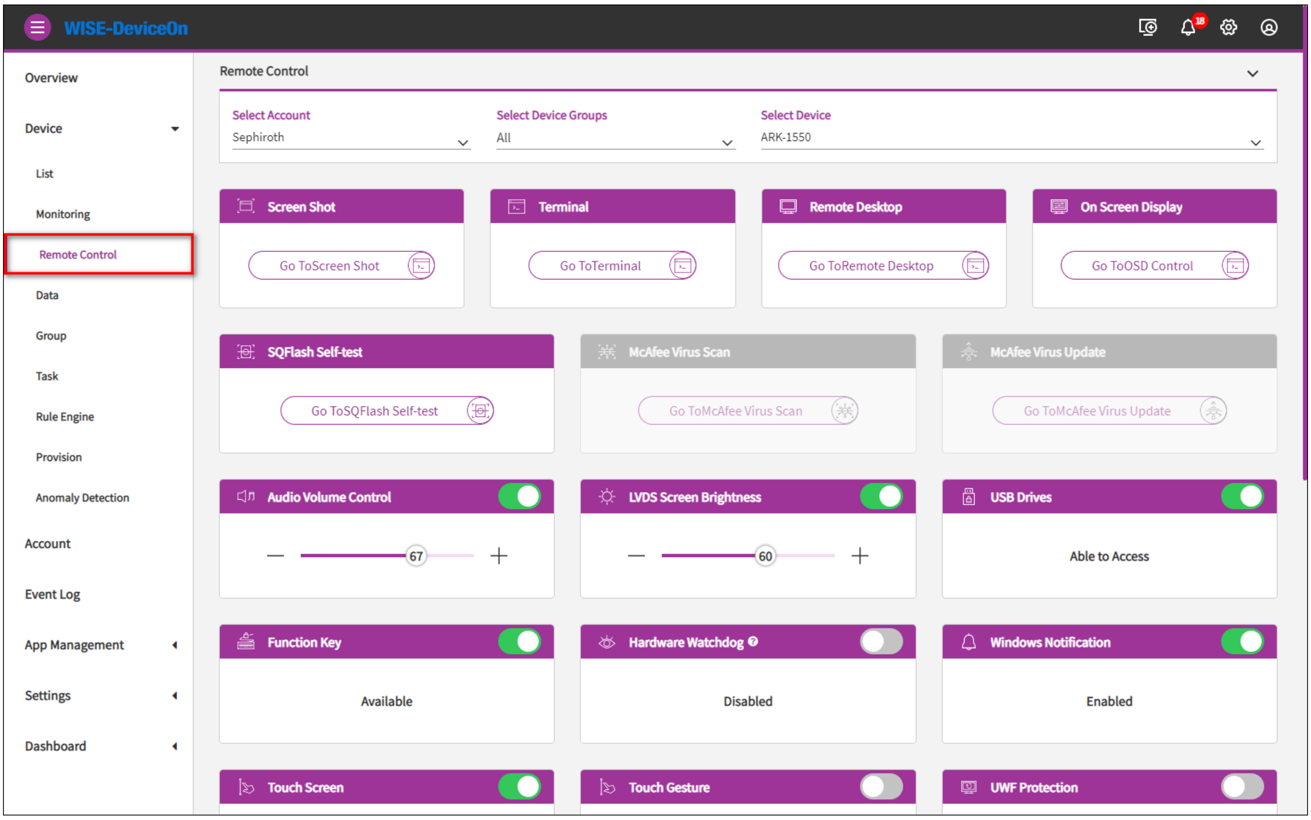
MODEL NAME	SQF-S25M4-64G-S9C	
SERIAL NUMBER	FF7307651F0804606271	
FIRMWARE VERSION	S9FMA029	
CURRENT TEMPERATURE	30 °C	
MAXIMUN TEMPERATURE	0 °C	
OPAL SUPPORT	Not Support	
OPAL STATUS	Disable	
BAD BLOCKS	0	●
DATA RELIABILITY (ECC)	0	●

SMART RAW Value

ID	NAME	RAW
ae	UnexpectedPowerLossCount	0000000000F
c2	Temperature	0000000001E
f2	TotalHostRead	00000032416F
aa	BadBlockCount	000000000049
11	SpareBlocksRemaining	000000000050
10	InitialSpareBlocksAvailable	00000000005D
e7	SSDLifeRemaining	000000000054
ad	EraseCount	000001C71F9F

- 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.



Select Account: Sephiroth

Select Device Groups: All

Select Device: ARK-1550

Audio Volume Control: 67

LVDS Screen Brightness: 60

USB Drives: Able to Access

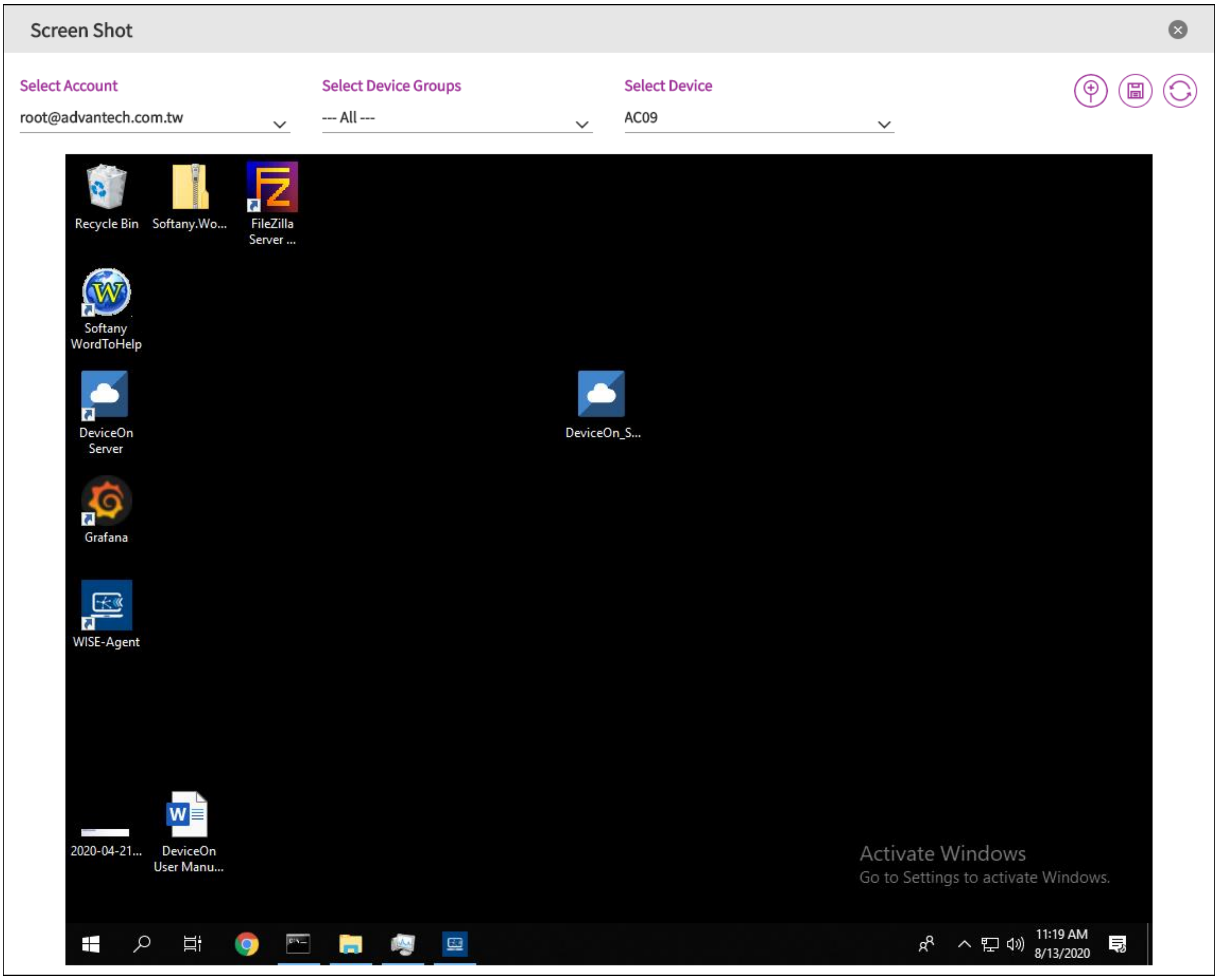
Function Key: Available

Hardware Watchdog: Disabled

Windows Notification: Enabled

[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 “**The OS of device is not logged in**”

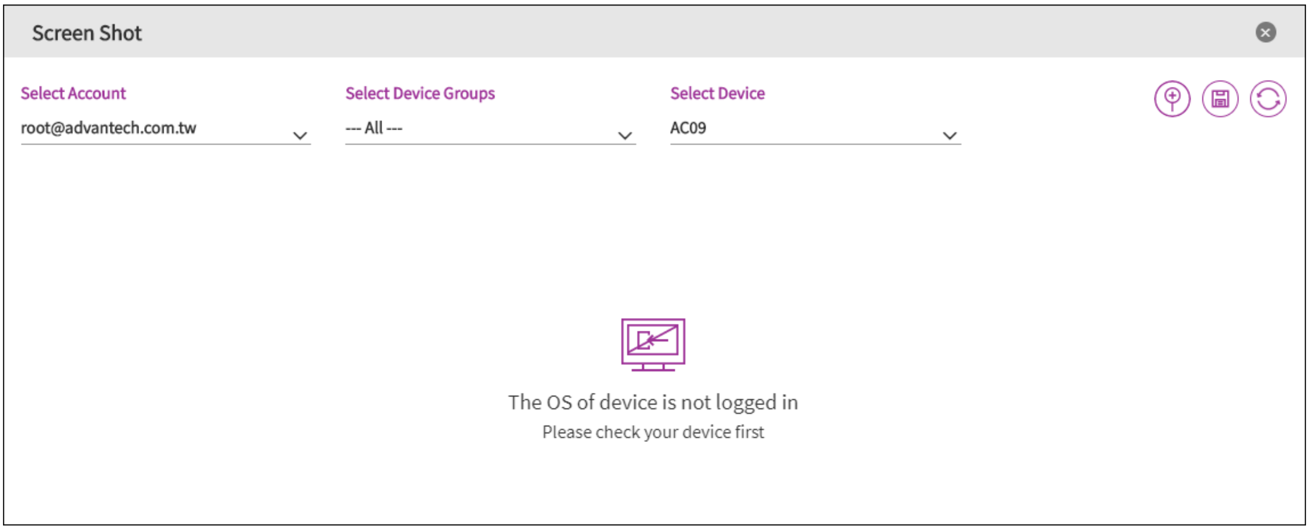


Screen Shot

Select Account: root@advantech.com.tw

Select Device Groups: --- All ---

Select Device: AC09



Screen Shot

Select Account: root@advantech.com.tw

Select Device Groups: --- All ---

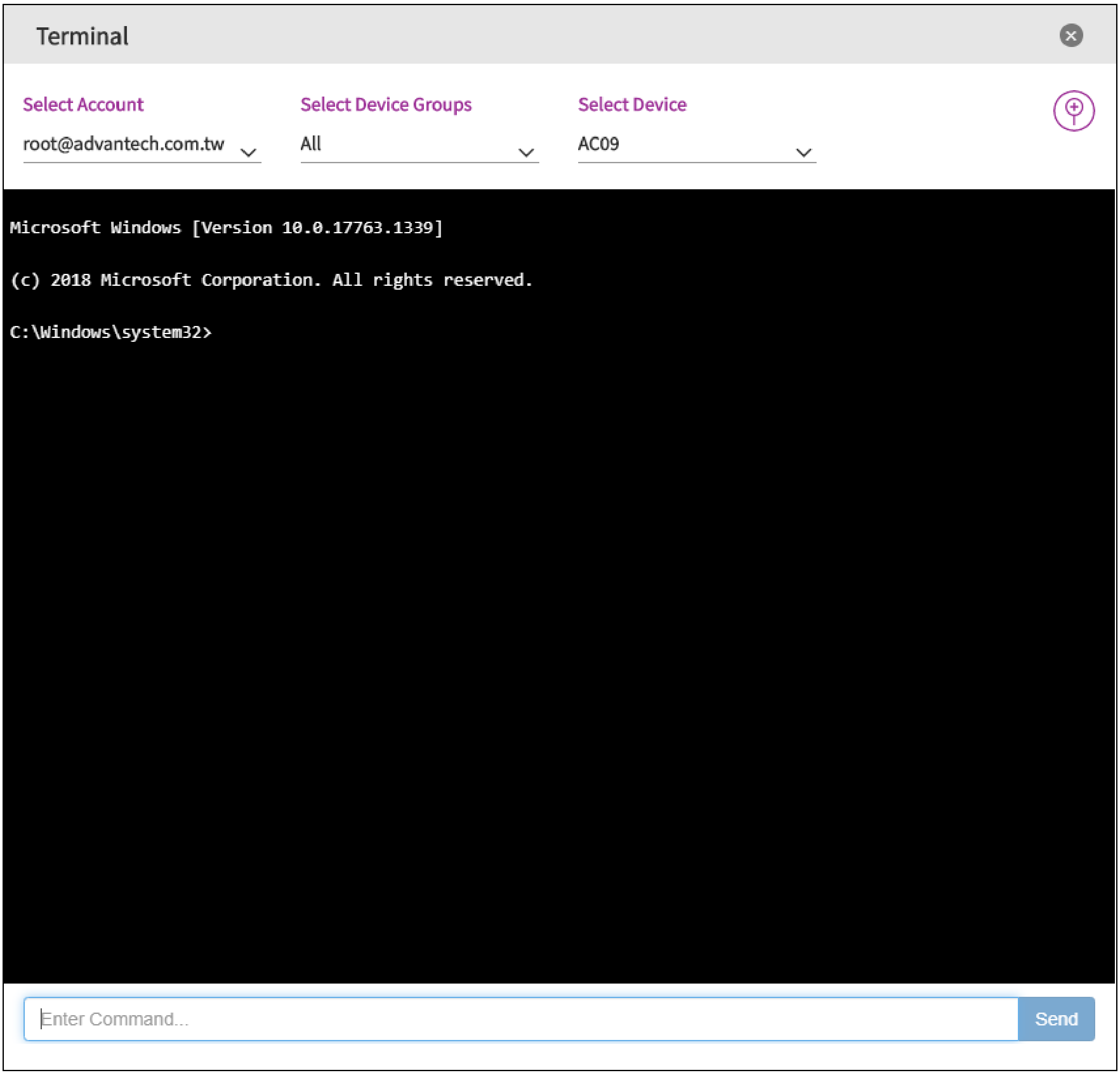
Select Device: AC09

The OS of device is not logged in

Please check your device first

[Terminal]

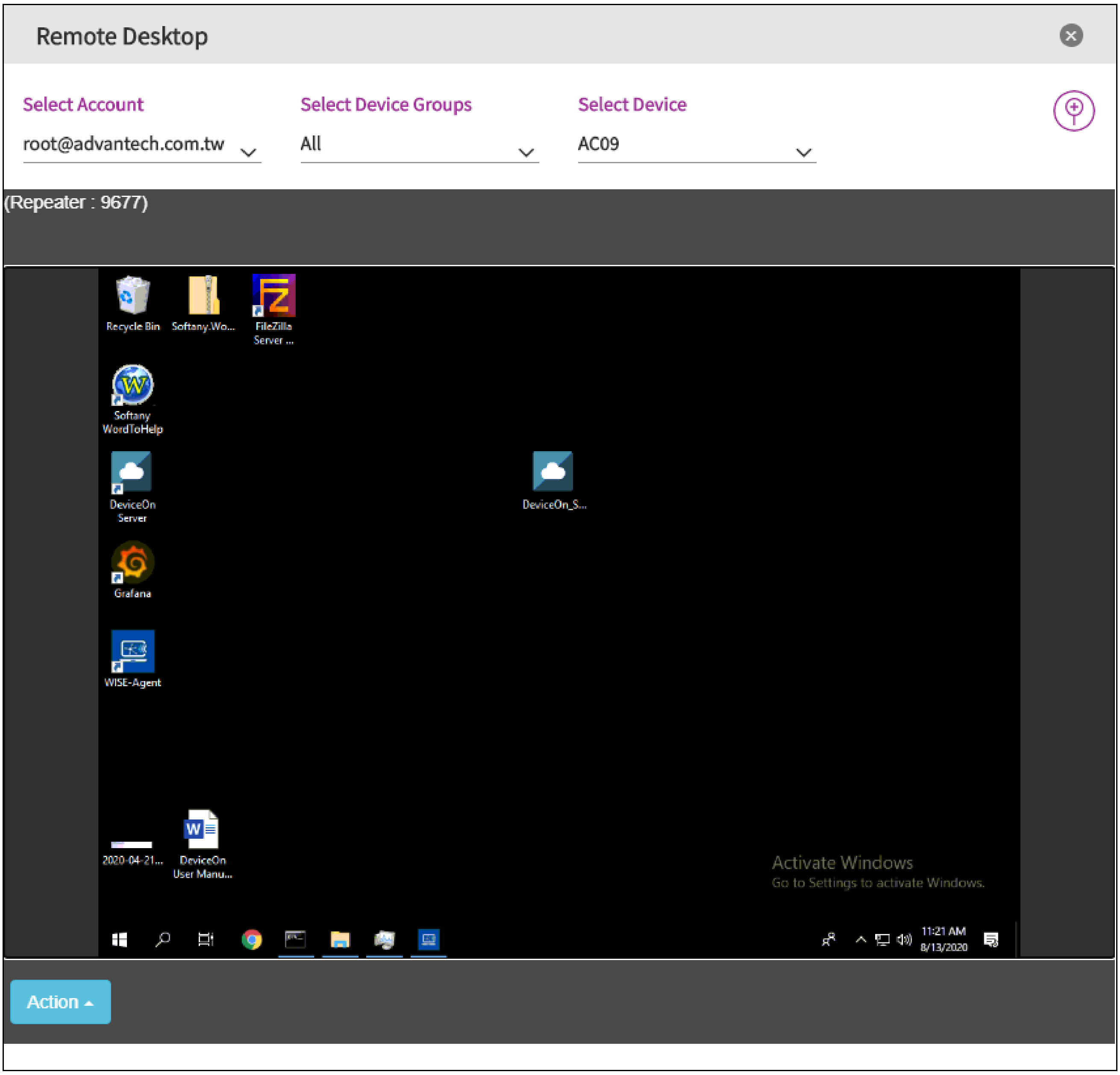
To terminal support any command to your devices, for instance, realize your device IP, traceroute the network or copy/view file on the device.



```
Microsoft Windows [Version 10.0.17763.1339]

(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

[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. Please make sure your web client port (outbound) is allow within (**6083~6102**), and target device outbound port, **5501**.



Remote Desktop

Select Account: root@advantech.com.tw

Select Device Groups: All

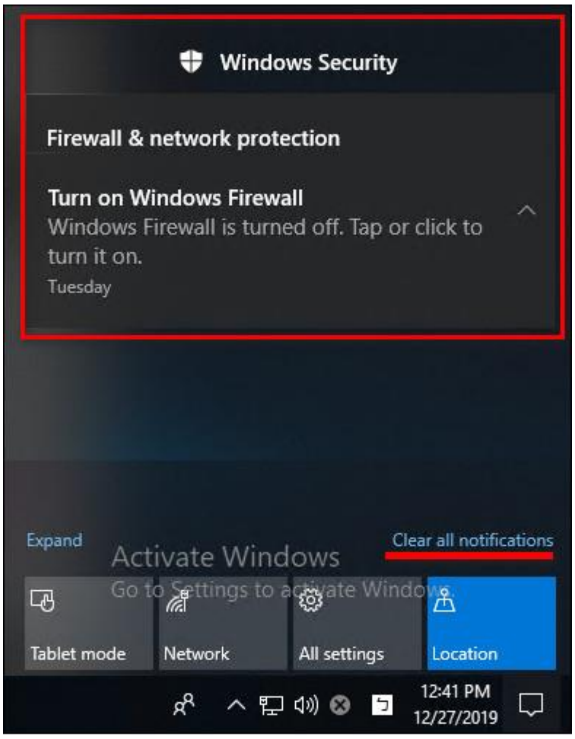
Select Device: AC09

(Repeater : 9677)

[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.



Windows Security

Firewall & network protection

Turn on Windows Firewall
Windows Firewall is turned off. Tap or click to turn it on.
Tuesday

[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, GPIO** 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.

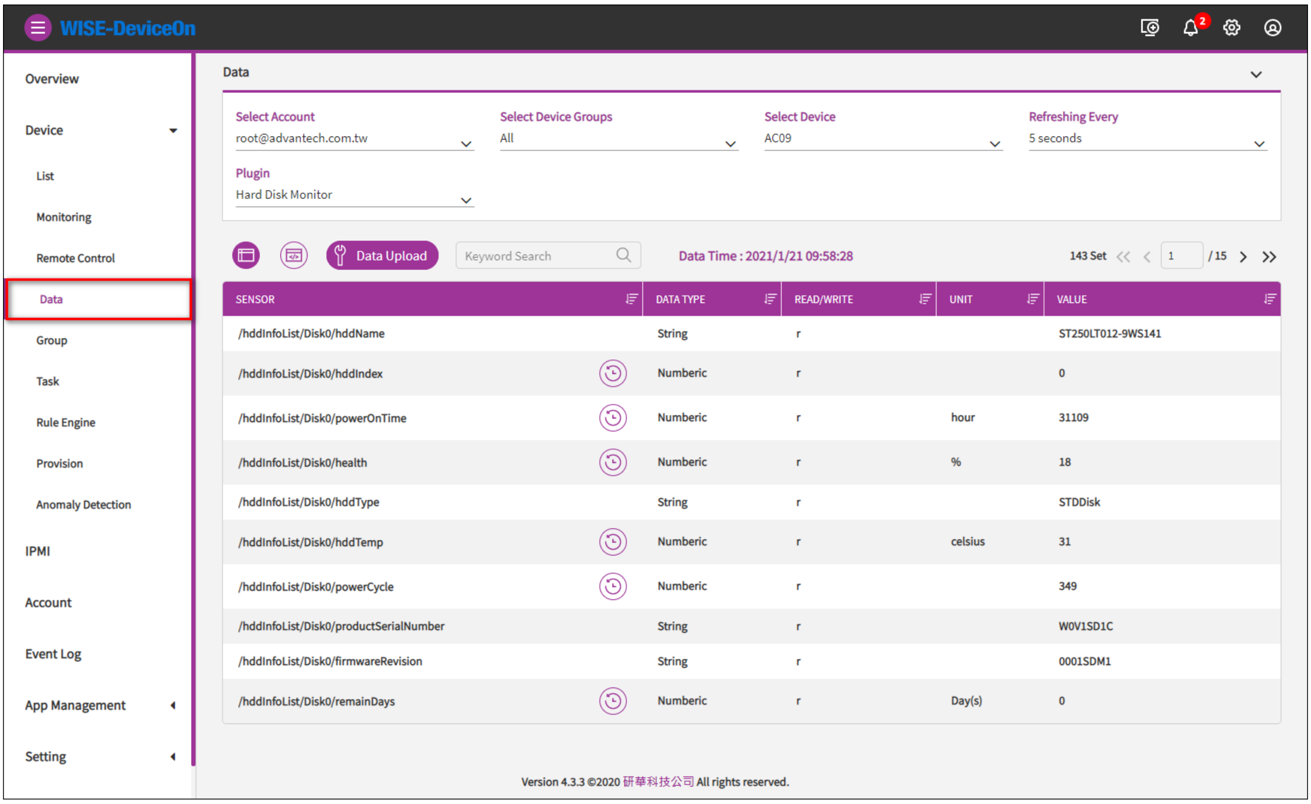
[**On Screen Display**]: Adjust monitor (brightness, color temperature, resolution, …etc.), especially support on Advantech Industrial Display.

[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 called 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.



Select Account: root@advantech.com.tw
Select Device Groups: All
Select Device: AC09
Refreshing Every: 5 seconds
Plugin: Hard Disk Monitor

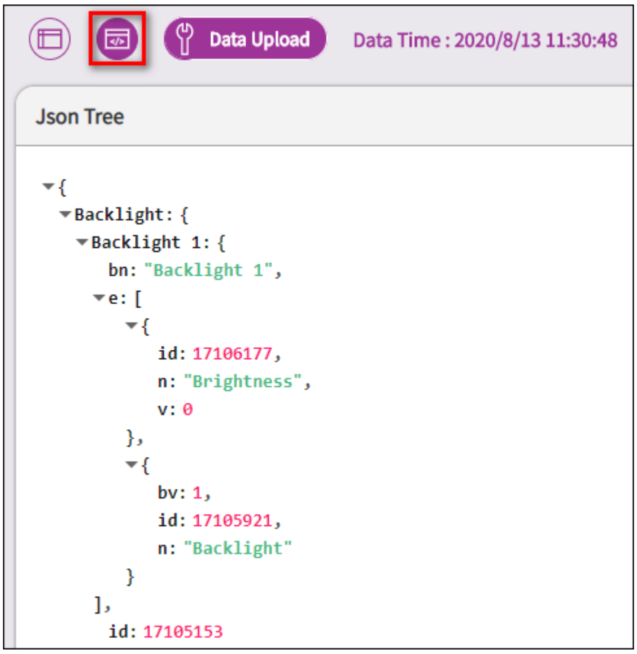
Data Time : 2021/1/21 09:58:28

143 Set 1 / 15

SENSOR	DATA TYPE	READ/WRITE	UNIT	VALUE
/hddInfoList/Disk0/hddName	String	r		ST250LT012-9WS141
/hddInfoList/Disk0/hddIndex	Numberic	r		0
/hddInfoList/Disk0/powerOnTime	Numberic	r	hour	31109
/hddInfoList/Disk0/health	Numberic	r	%	18
/hddInfoList/Disk0/hddType	String	r		STDDisk
/hddInfoList/Disk0/hddTemp	Numberic	r	celsius	31
/hddInfoList/Disk0/powerCycle	Numberic	r		349
/hddInfoList/Disk0/productSerialNumber	String	r		W0V1SD1C
/hddInfoList/Disk0/firmwareRevision	String	r		0001SDM1
/hddInfoList/Disk0/remainDays	Numberic	r	Day(s)	0

Version 4.3.3 ©2020 研華科技公司 All rights reserved.

The default display is table mode, you could switch to JSON format through the icon.

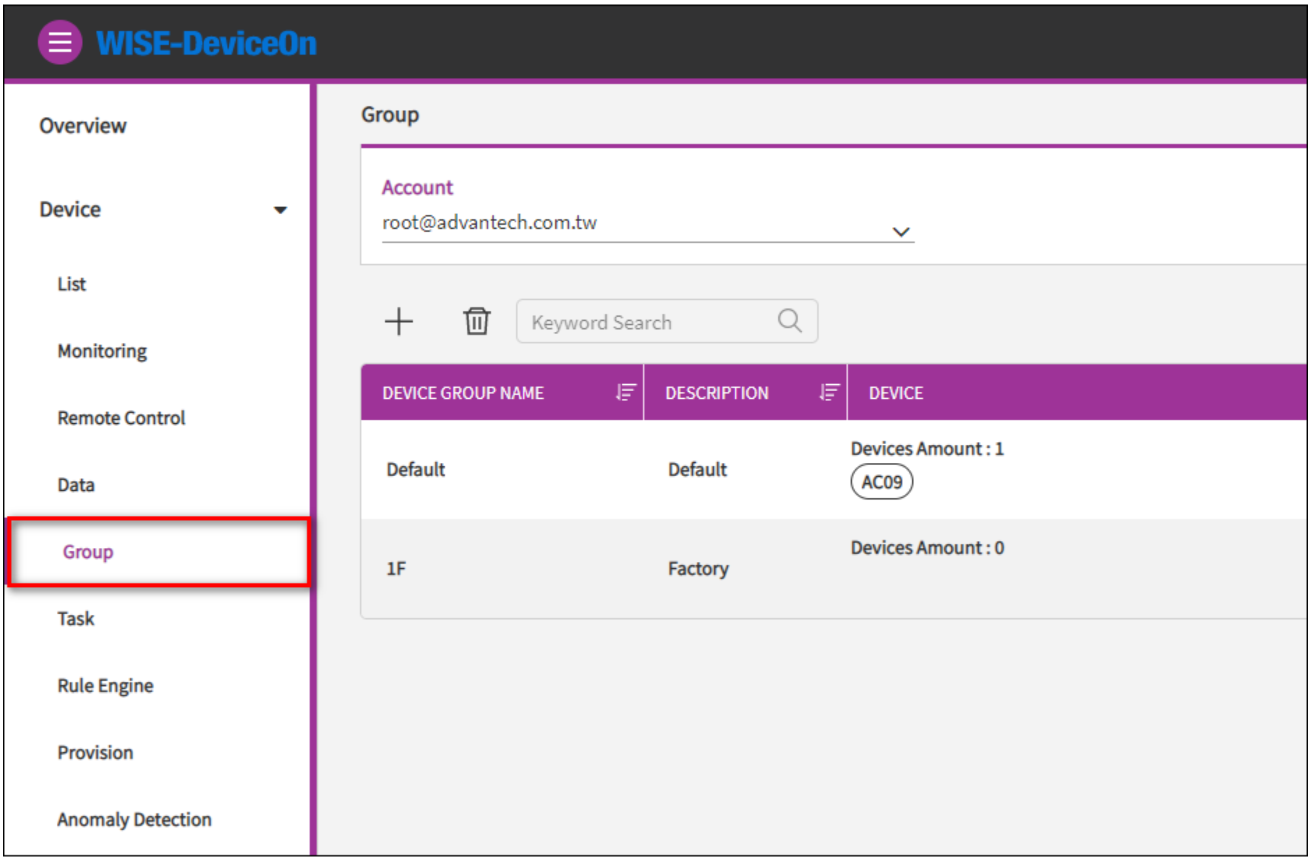


Data Time : 2020/8/13 11:30:48

```
{
  Backlight: {
    Backlight 1: {
      bn: "Backlight 1",
      e: [
        {
          id: 17106177,
          n: "Brightness",
          v: 0
        },
        {
          bv: 1,
          id: 17105921,
          n: "Backlight"
        }
      ],
      id: 17105153
```

- Device Group

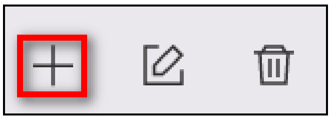
Every account could group their device into different groups to manage, for example, device over different floor on the building. User could create 1F, 2F group to easy management.

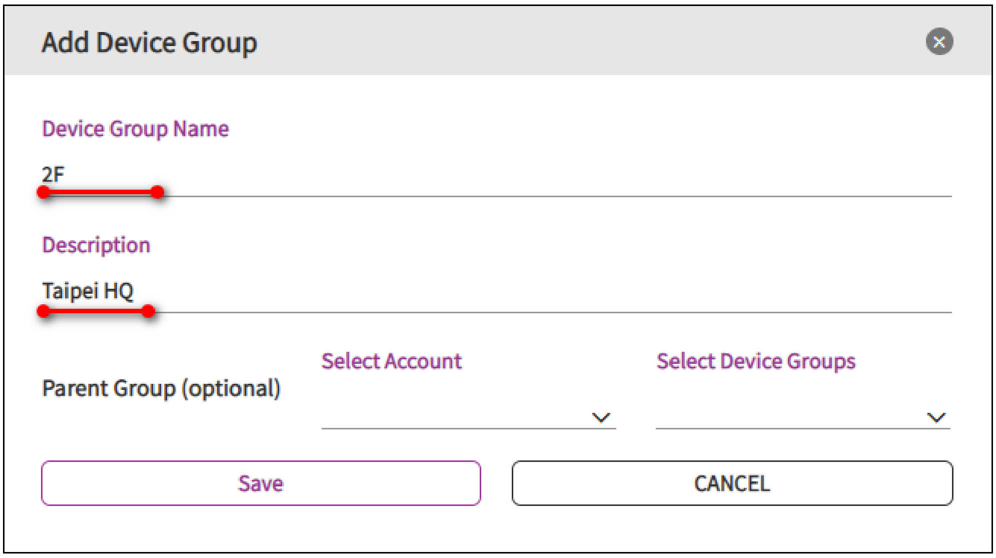


Account: root@advantech.com.tw

DEVICE GROUP NAME	DESCRIPTION	DEVICE
Default	Default	Devices Amount : 1 AC09
1F	Factory	Devices Amount : 0

Click on the icon to add “**Device Group**”. The option to configure the parent group, that’s means share the device group to parent group owner.





Add Device Group

Device Group Name

2F

Description

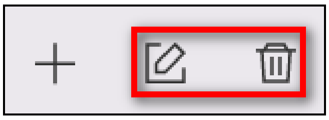
Taipei HQ

Parent Group (optional)

Select Account

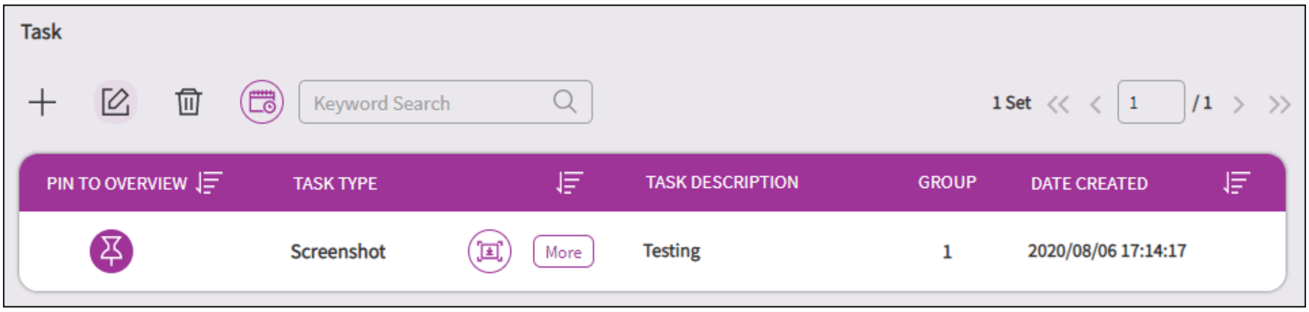
Select Device Groups

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



- Task

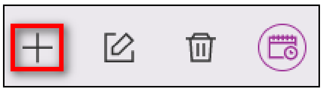
The real-time actions on the overview that are defined, created on here, you could add a new task and pin to overview. These tasks are binding to personal account, cannot view, edit, and delete others.



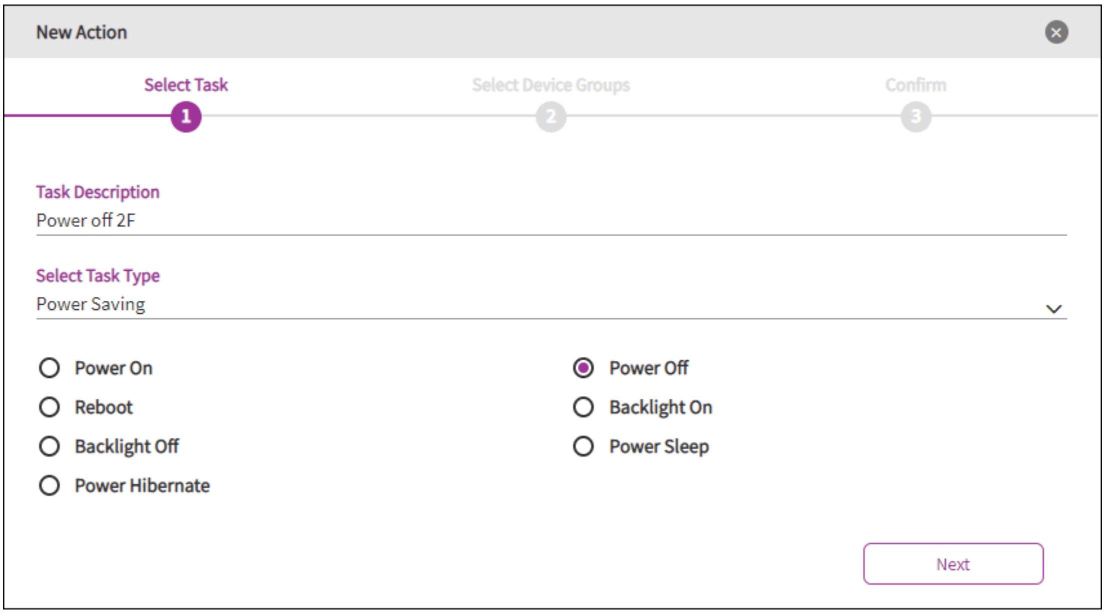
Task

PIN TO OVERVIEW	TASK TYPE		TASK DESCRIPTION	GROUP	DATE CREATED
	Screenshot	More	Testing	1	2020/08/06 17:14:17

Click on the icon to add action.



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



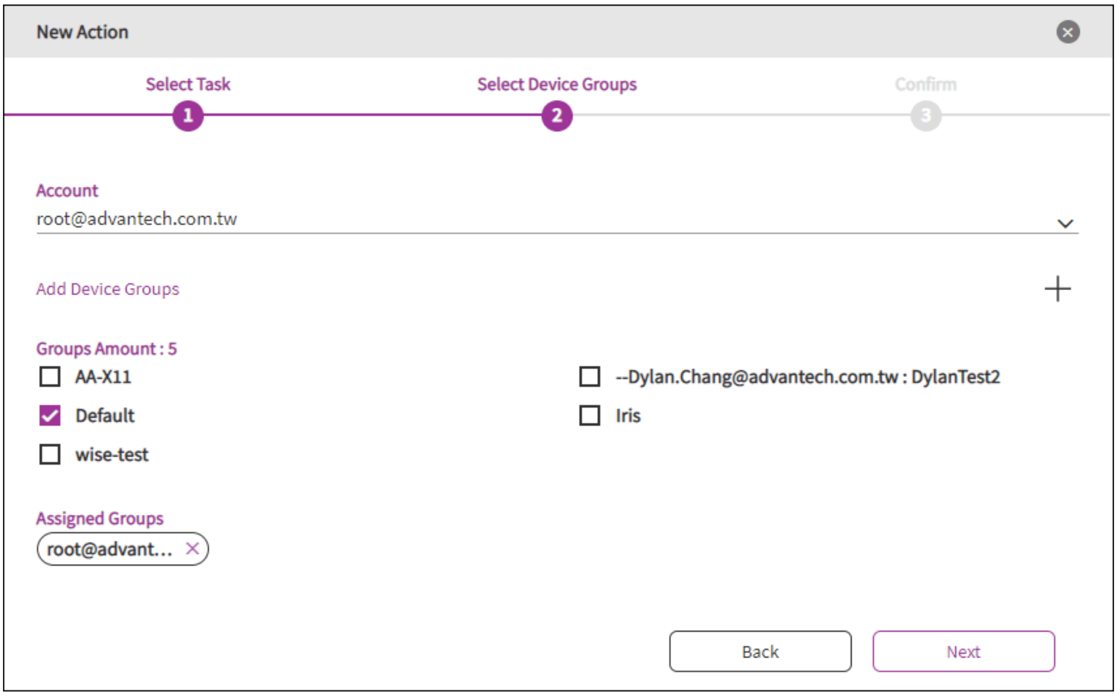
New Action

Task Description
Power off 2F

Select Task Type
Power Saving

○ Power On
○ Reboot
○ Backlight Off
○ Power Hibernate
● Power Off
○ Backlight On
○ Power Sleep

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



New Action

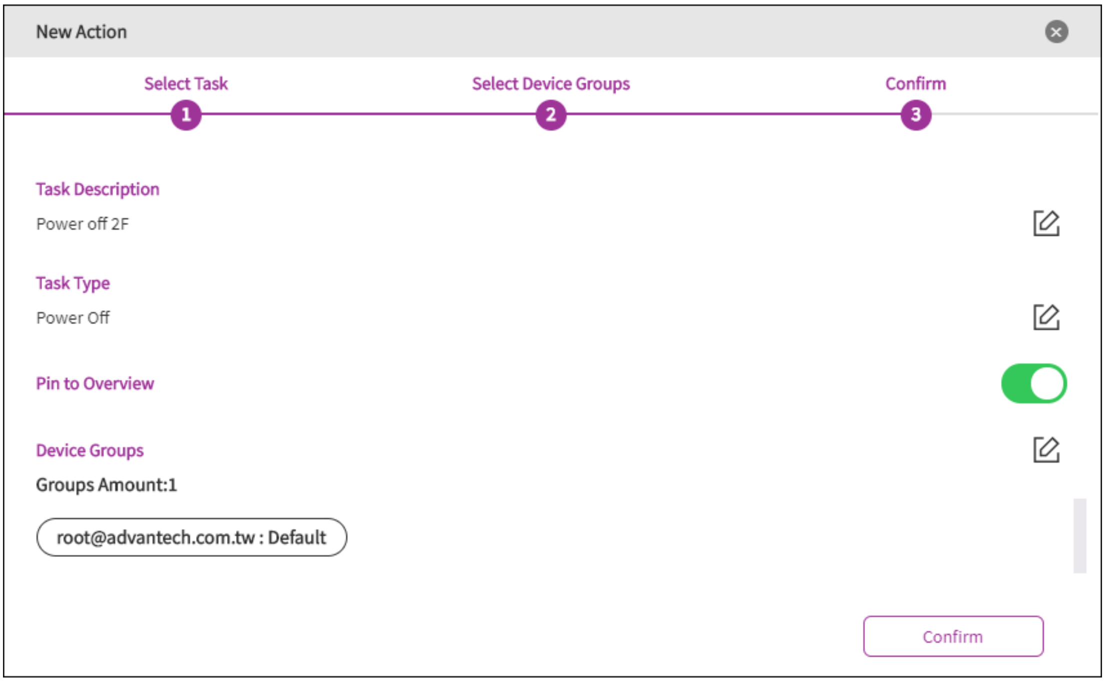
Account
root@advantech.com.tw

Add Device Groups

Groups Amount : 5
□ AA-X11
☑ Default
□ wise-test
□ --Dylan.Chang@advantech.com.tw : DylanTest2
□ Iris

Assigned Groups
root@advant... ×

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



Task Description
Power off 2F

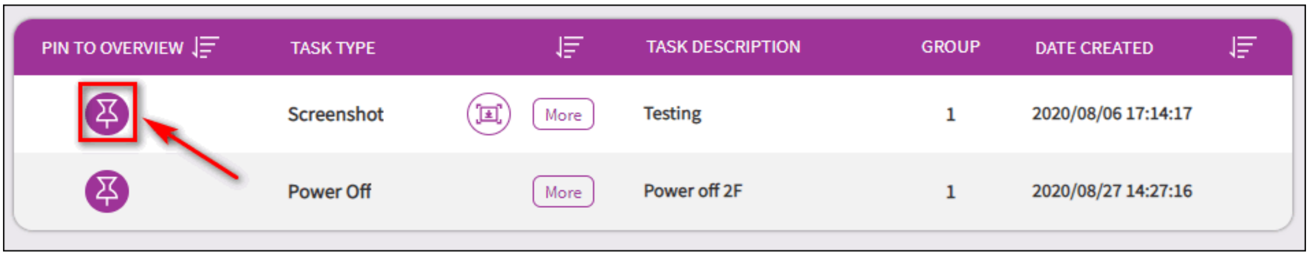
Task Type
Power Off

Pin to Overview

Device Groups
Groups Amount:1

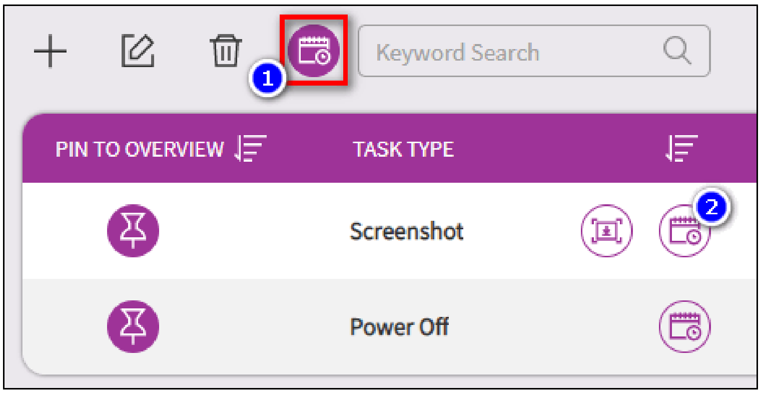
root@advantech.com.tw : Default

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.



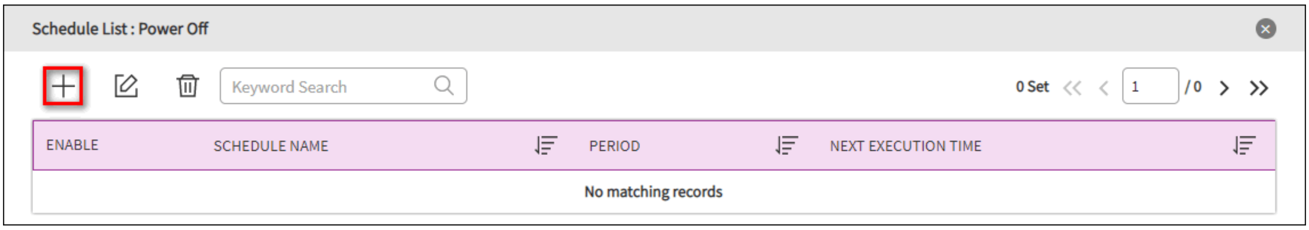
PIN TO OVERVIEW	TASK TYPE		TASK DESCRIPTION	GROUP	DATE CREATED
	Screenshot	More	Testing	1	2020/08/06 17:14:17
	Power Off	More	Power off 2F	1	2020/08/27 14:27:16

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



PIN TO OVERVIEW	TASK TYPE
	Screenshot
	Power Off

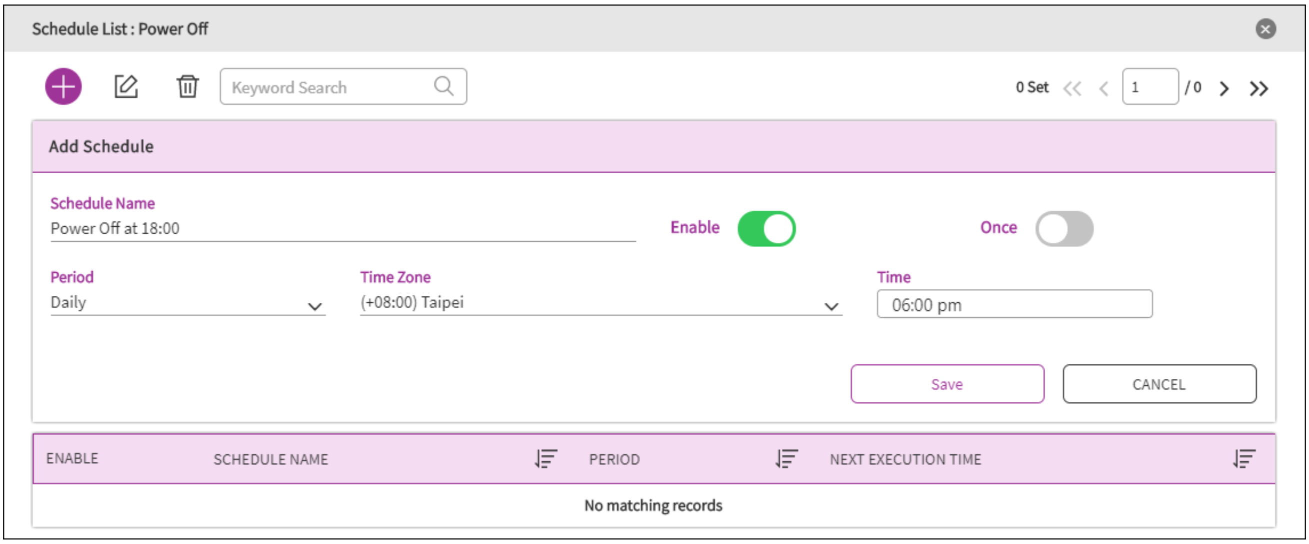
Enter to schedule list for all actions and click on add icon to create new schedule.


Schedule List : Power Off

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 subdivisons 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.


Schedule List : Power Off

Add Schedule

Schedule Name: Power Off at 18:00

Enable: on

Once: off

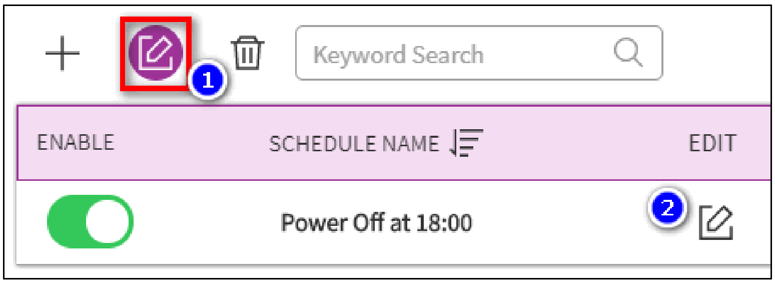
Period: Daily

Time Zone: (+08:00) Taipei

Time: 06:00 pm

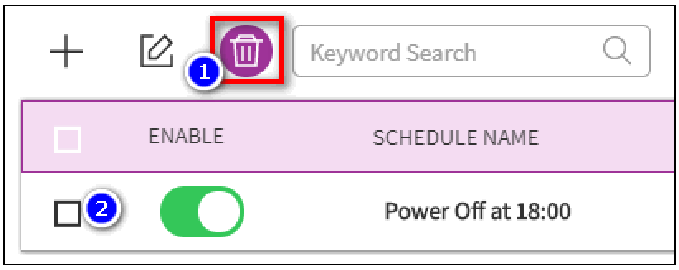
No matching records

Click on the edit icon to adjust schedule item.



Power Off at 18:00

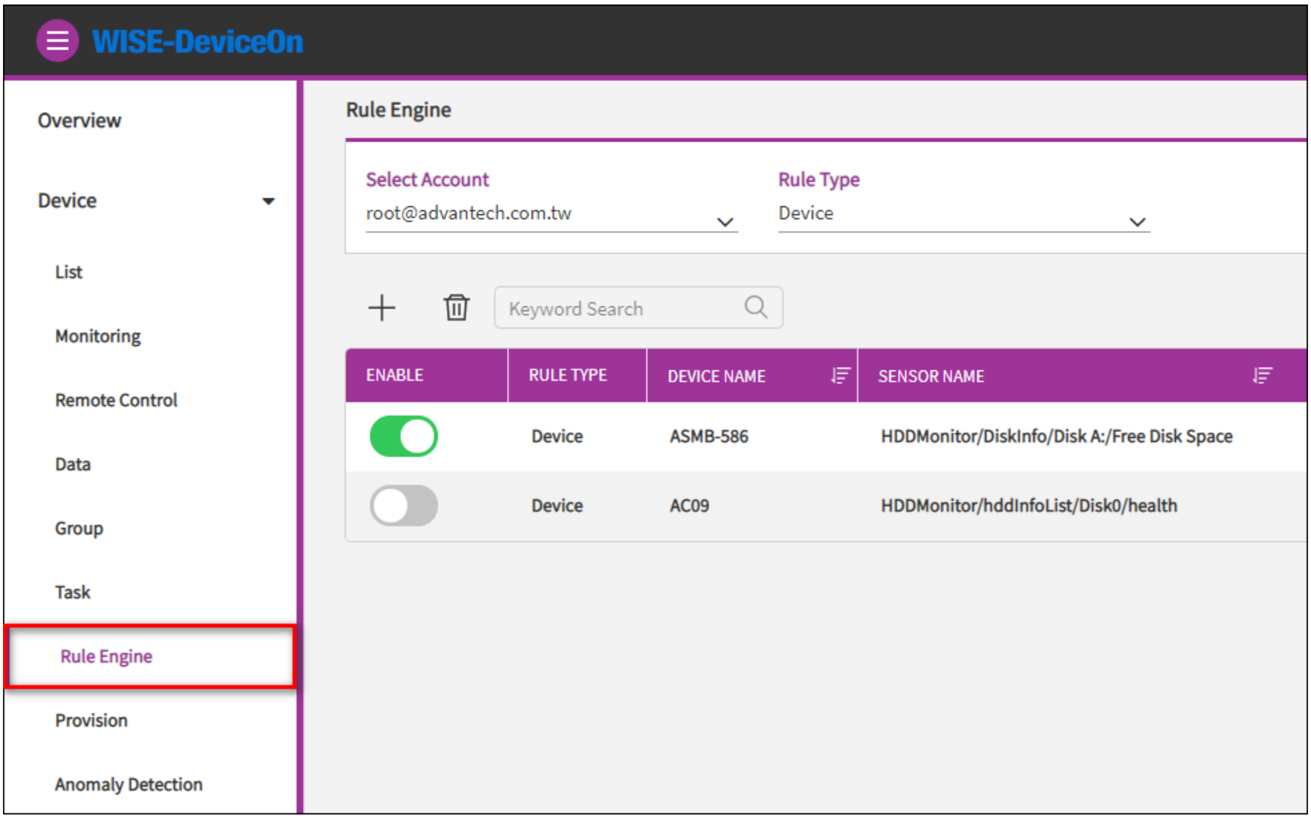
Click on the delete icon to delete schedule item.



□	ENABLE	SCHEDULE NAME
□	🟩	Power Off at 18:00

- 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.



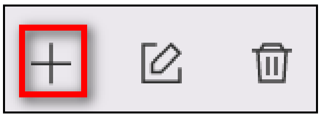
Rule Engine

Select Account: root@advantech.com.tw

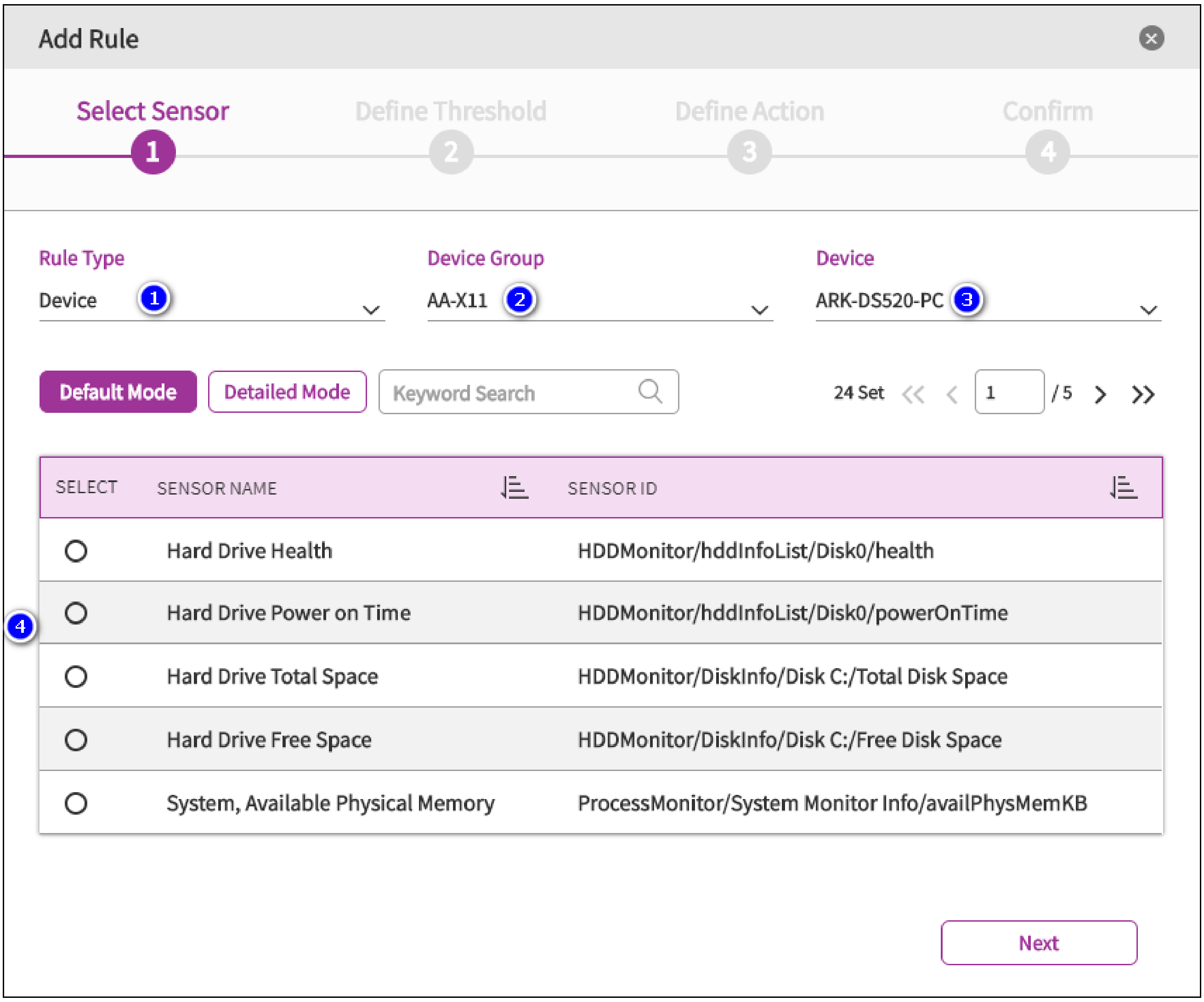
Rule Type: Device

ENABLE	RULE TYPE	DEVICE NAME	SENSOR NAME
🟩	Device	ASMB-586	HDDMonitor/DiskInfo/Disk A:/Free Disk Space
○	Device	AC09	HDDMonitor/hddInfoList/Disk0/health

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**.



Rule Type: Device

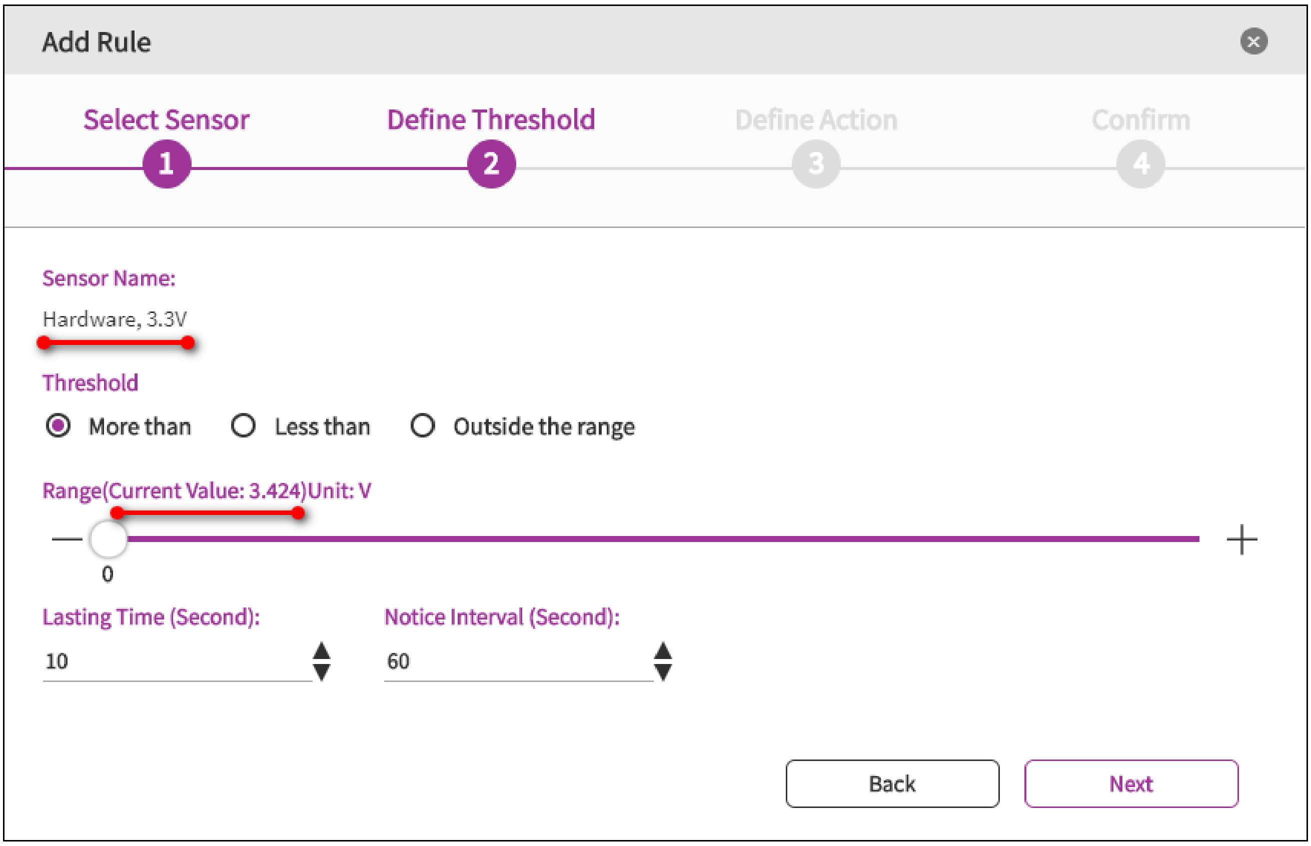
Device Group: AA-X11

Device: ARK-DS520-PC

SELECT	SENSOR NAME	SENSOR ID
○	Hard Drive Health	HDDMonitor/hddInfoList/Disk0/health
○	Hard Drive Power on Time	HDDMonitor/hddInfoList/Disk0/powerOnTime
○	Hard Drive Total Space	HDDMonitor/DiskInfo/Disk C:/Total Disk Space
○	Hard Drive Free Space	HDDMonitor/DiskInfo/Disk C:/Free Disk Space
○	System, Available Physical Memory	ProcessMonitor/System Monitor Info/availPhysMemKB

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.



Sensor Name:
Hardware, 3.3V

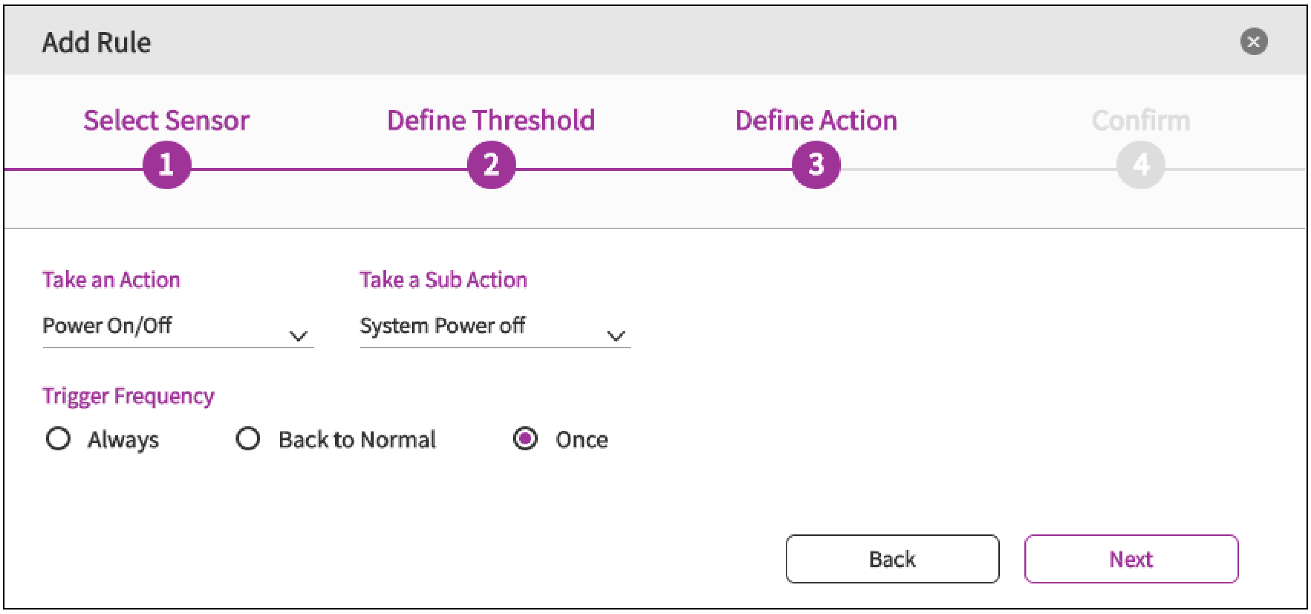
Threshold
● More than ○ Less than ○ Outside the range

Range(Current Value: 3.424)Unit: V
0

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.

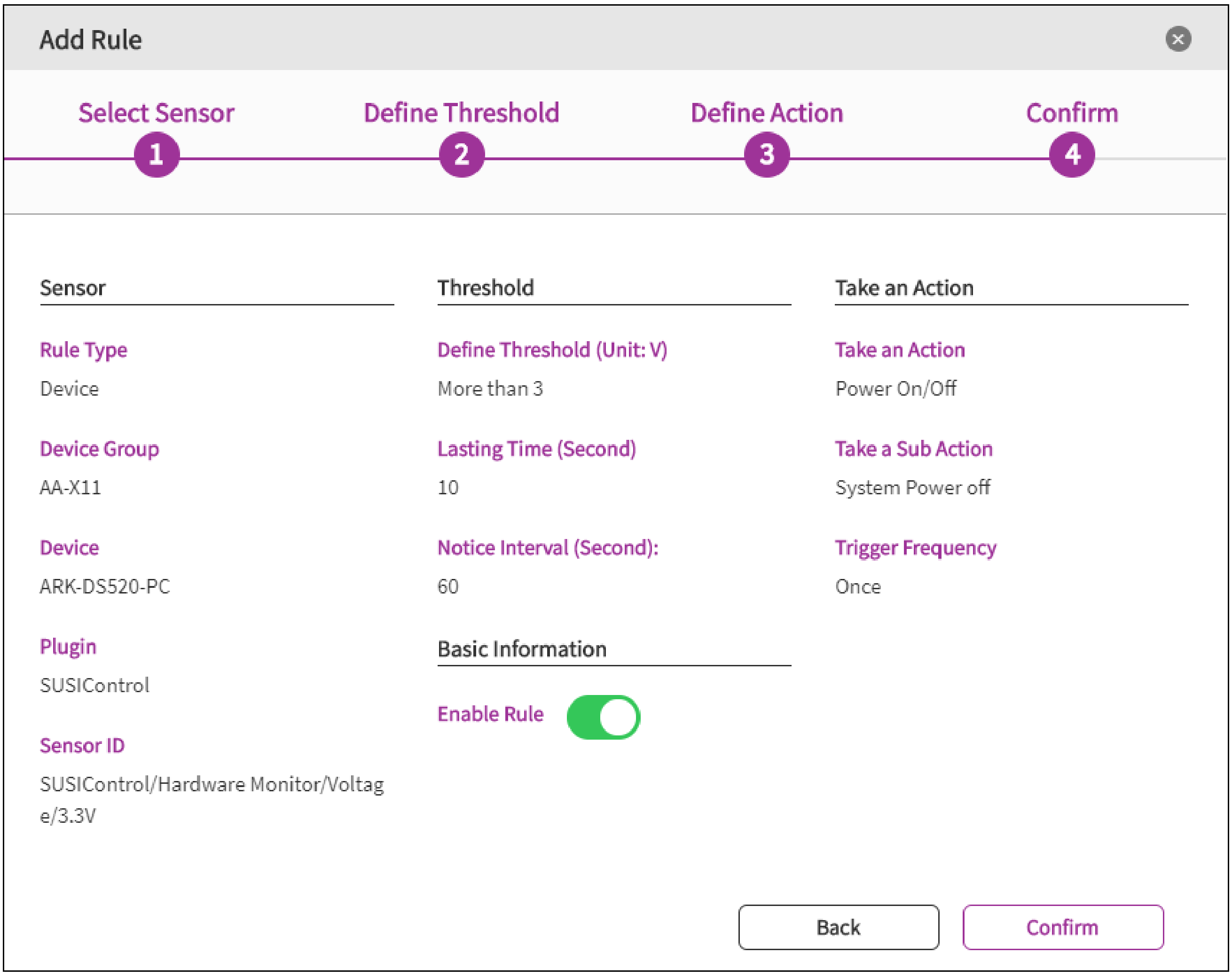


Take an Action: Power On/Off

Take a Sub Action: System Power off

Trigger Frequency
○ Always ○ Back to Normal ● Once

Confirm the rule setting and click confirm.



Add Rule

Sensor

Rule Type
Device

Device Group
AA-X11

Device
ARK-DS520-PC

Plugin
SUSIControl

Sensor ID
SUSIControl/Hardware Monitor/Voltage/3.3V

Threshold

Define Threshold (Unit: V)
More than 3

Lasting Time (Second)
10

Notice Interval (Second):
60

Basic Information

Enable Rule

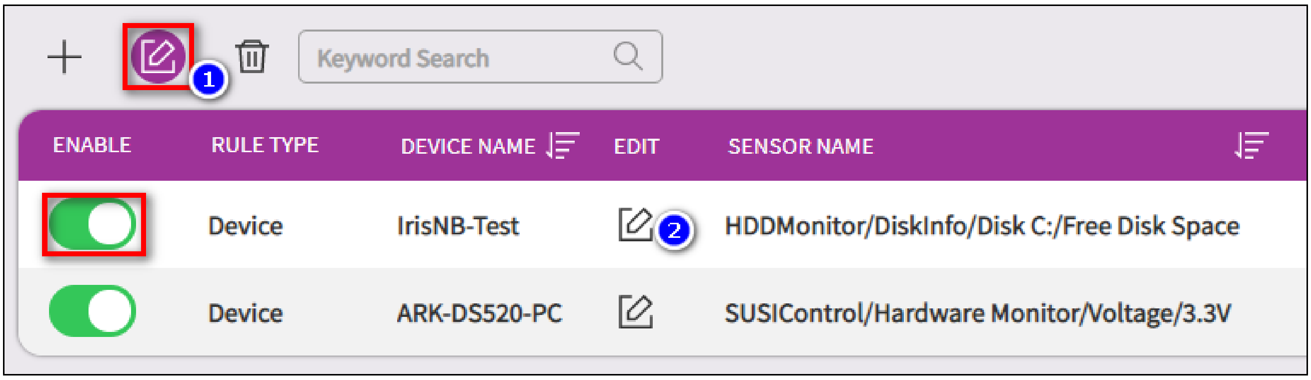
Take an Action

Take an Action
Power On/Off

Take a Sub Action
System Power off

Trigger Frequency
Once

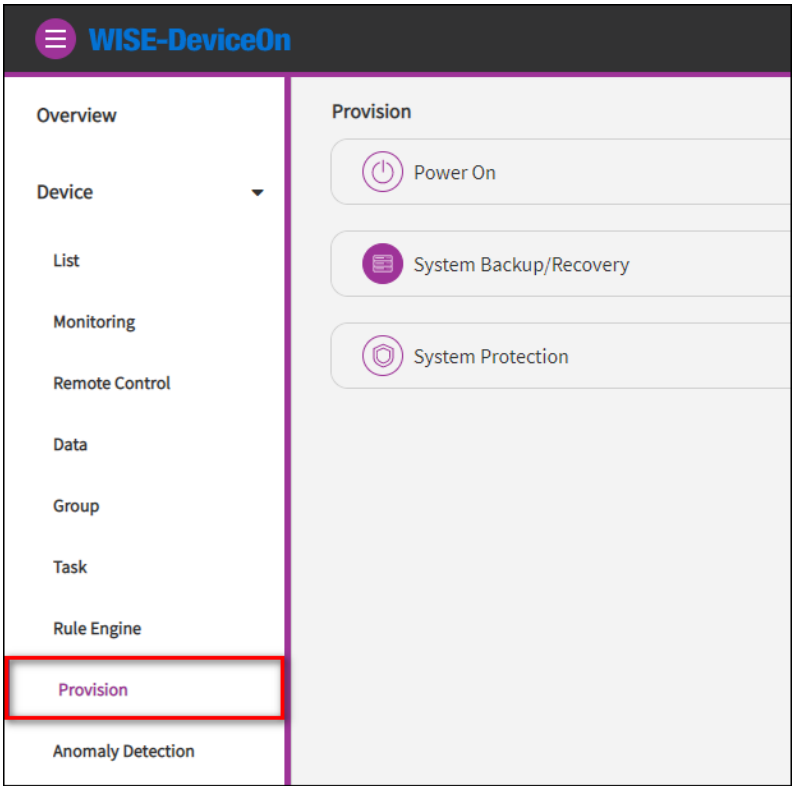
The rule list shown as below, user could edit or disable through the switch.



ENABLE	RULE TYPE	DEVICE NAME	EDIT	SENSOR NAME
●	Device	IrisNB-Test		HDDMonitor/DiskInfo/Disk C:/Free Disk Space
●	Device	ARK-DS520-PC		SUSIControl/Hardware Monitor/Voltage/3.3V

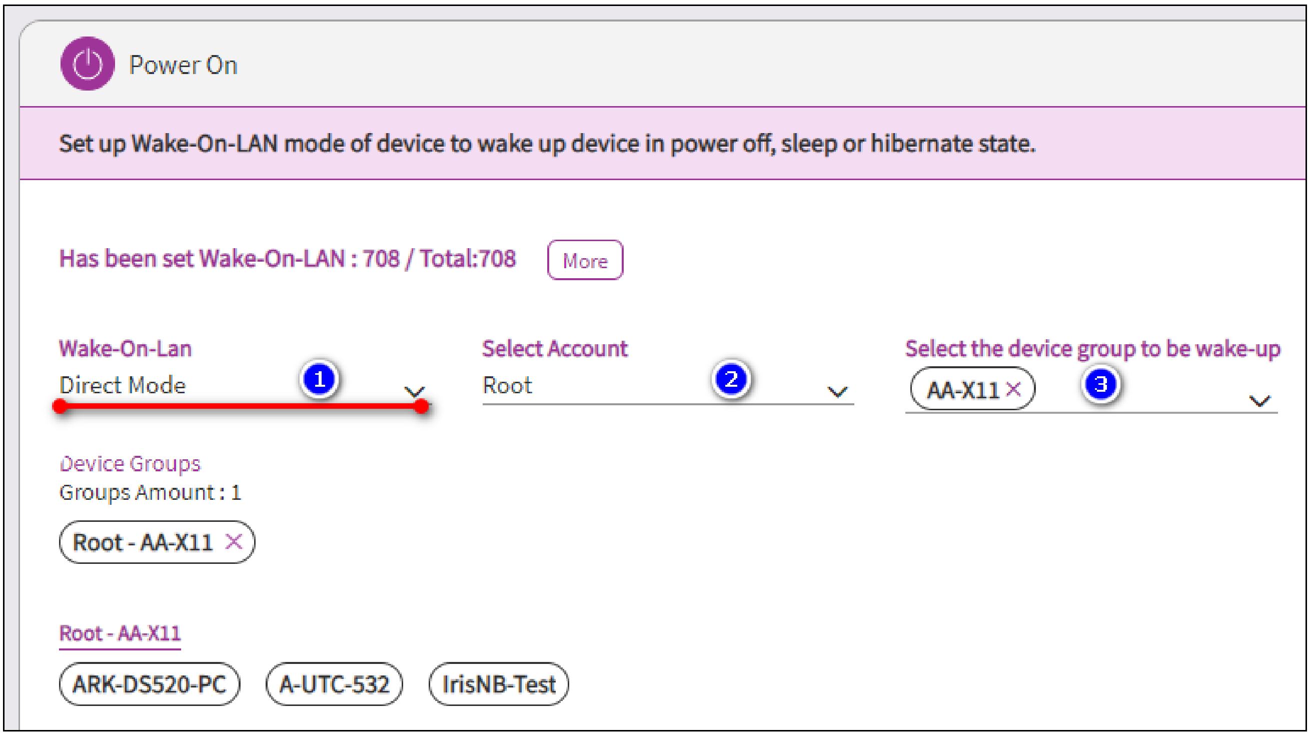
- Provision

For device provision, 3 types of 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.



✧ 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 On

Set up Wake-On-LAN mode of device to wake up device in power off, sleep or hibernate state.

Has been set Wake-On-LAN : 708 / Total:708 More

Wake-On-Lan: Direct Mode

Select Account: Root

Select the device group to be wake-up: AA-X11

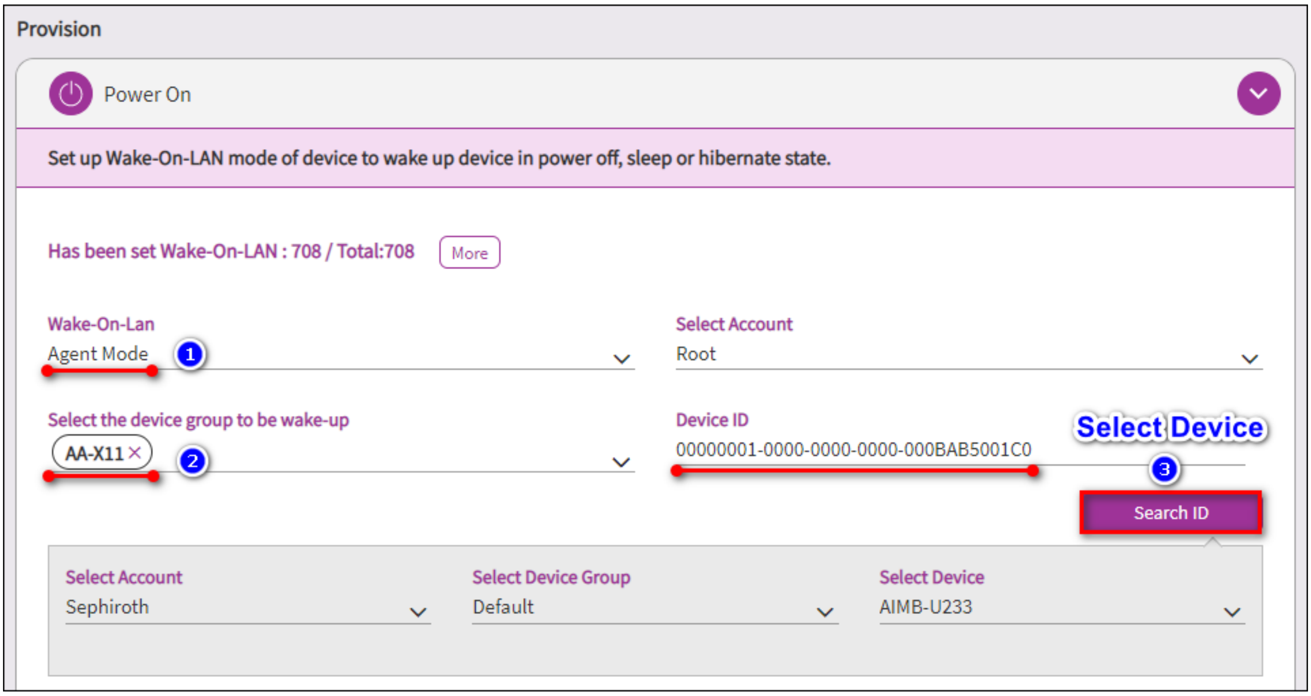
Device Groups
Groups Amount : 1

Root - AA-X11

Root - AA-X11

ARK-DS520-PC A-UTC-532 IrisNB-Test

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.



Provision

Power On

Set up Wake-On-LAN mode of device to wake up device in power off, sleep or hibernate state.

Has been set Wake-On-LAN : 708 / Total:708

Wake-On-Lan: Agent Mode

Select Account: Root

Select the device group to be wake-up: AA-X11

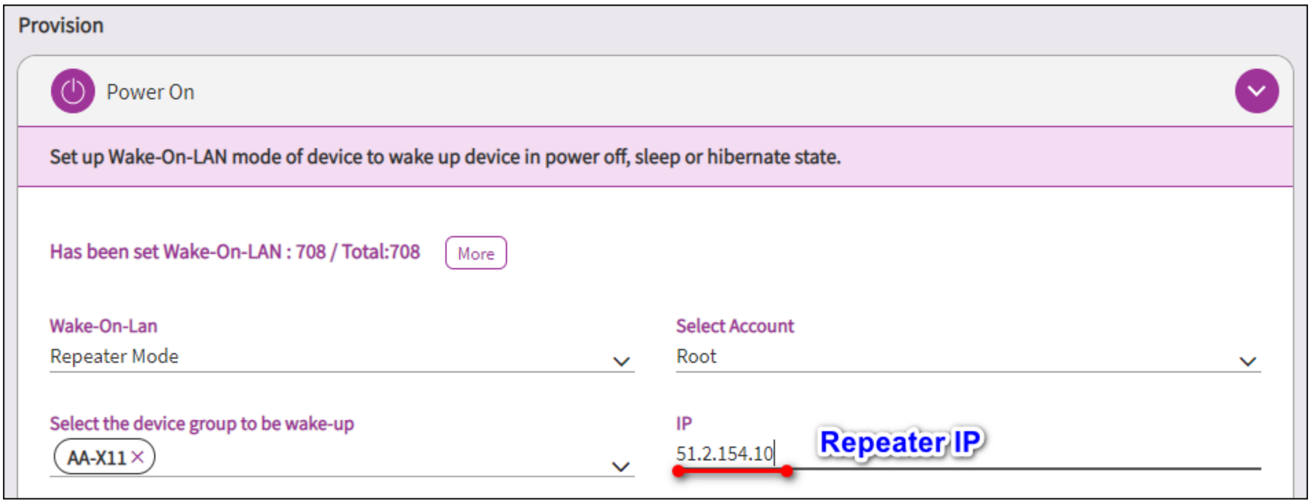
Device ID: 00000001-0000-0000-0000-000BAB5001C0

Select Account: Sephiroth

Select Device Group: Default

Select Device: AIMB-U233

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.



Provision

Power On

Set up Wake-On-LAN mode of device to wake up device in power off, sleep or hibernate state.

Has been set Wake-On-LAN : 708 / Total:708

Wake-On-Lan: Repeater Mode

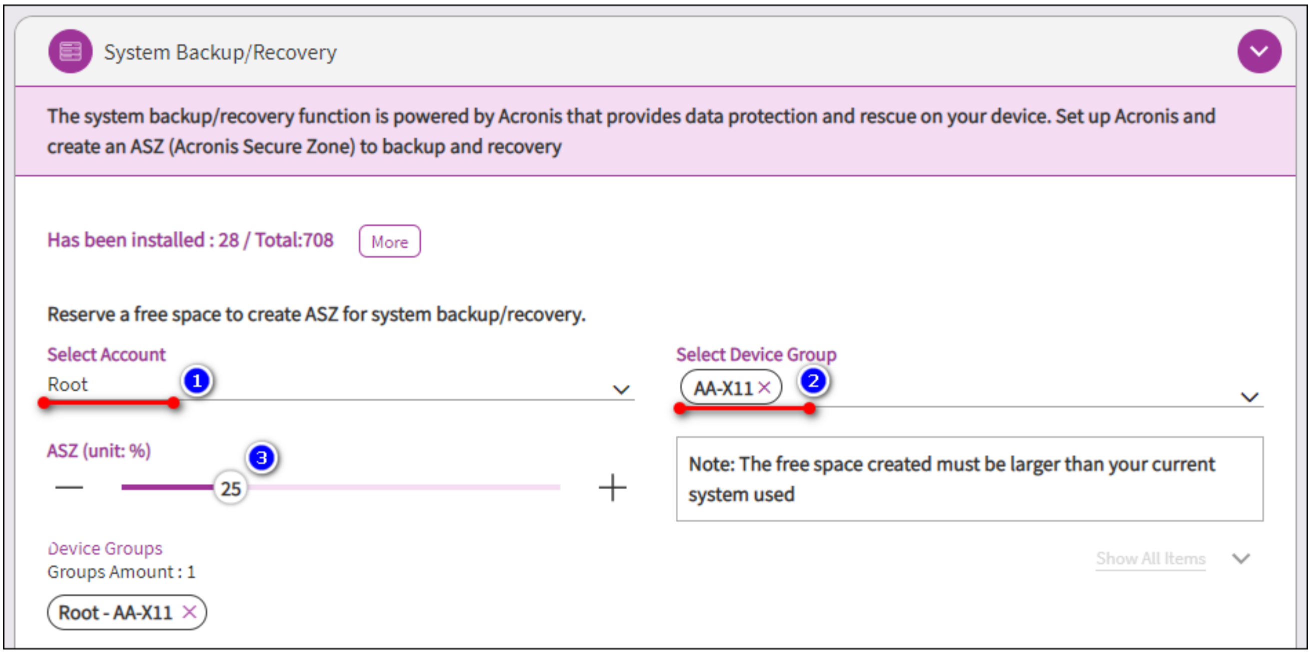
Select Account: Root

Select the device group to be wake-up: AA-X11

IP: 51.2.154.10

- ✧ System Backup/Recovery

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.



System Backup/Recovery

The system backup/recovery function is powered by Acronis that provides data protection and rescue on your device. Set up Acronis and create an ASZ (Acronis Secure Zone) to backup and recovery

Has been installed : 28 / Total:708 More

Reserve a free space to create ASZ for system backup/recovery.

Select Account: Root 1

Select Device Group: AA-X11 2

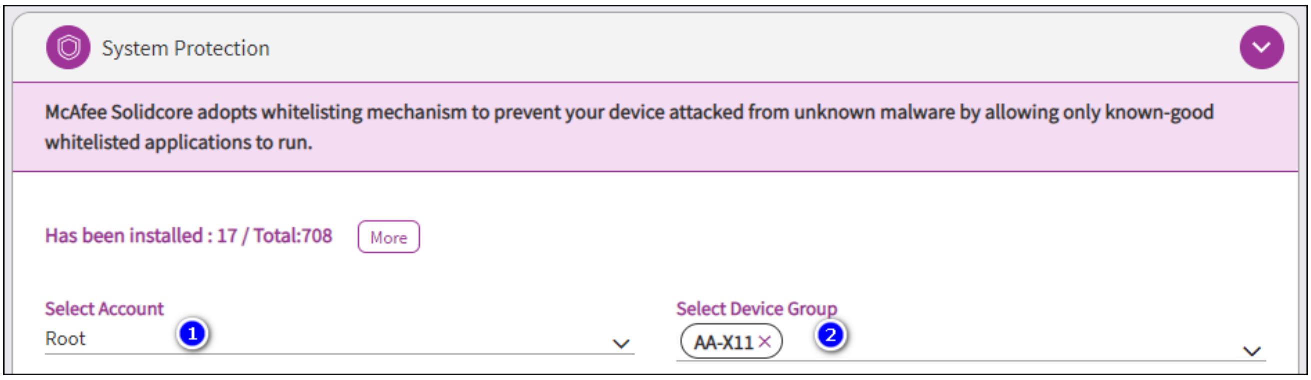
ASZ (unit: %) 3: 25

Note: The free space created must be larger than your current system used

Device Groups
Groups Amount : 1
Root - AA-X11

✧ System Protection

Select the device group to install.



System Protection

McAfee Solidcore adopts whitelisting mechanism to prevent your device attacked from unknown malware by allowing only known-good whitelisted applications to run.

Has been installed : 17 / Total:708 More

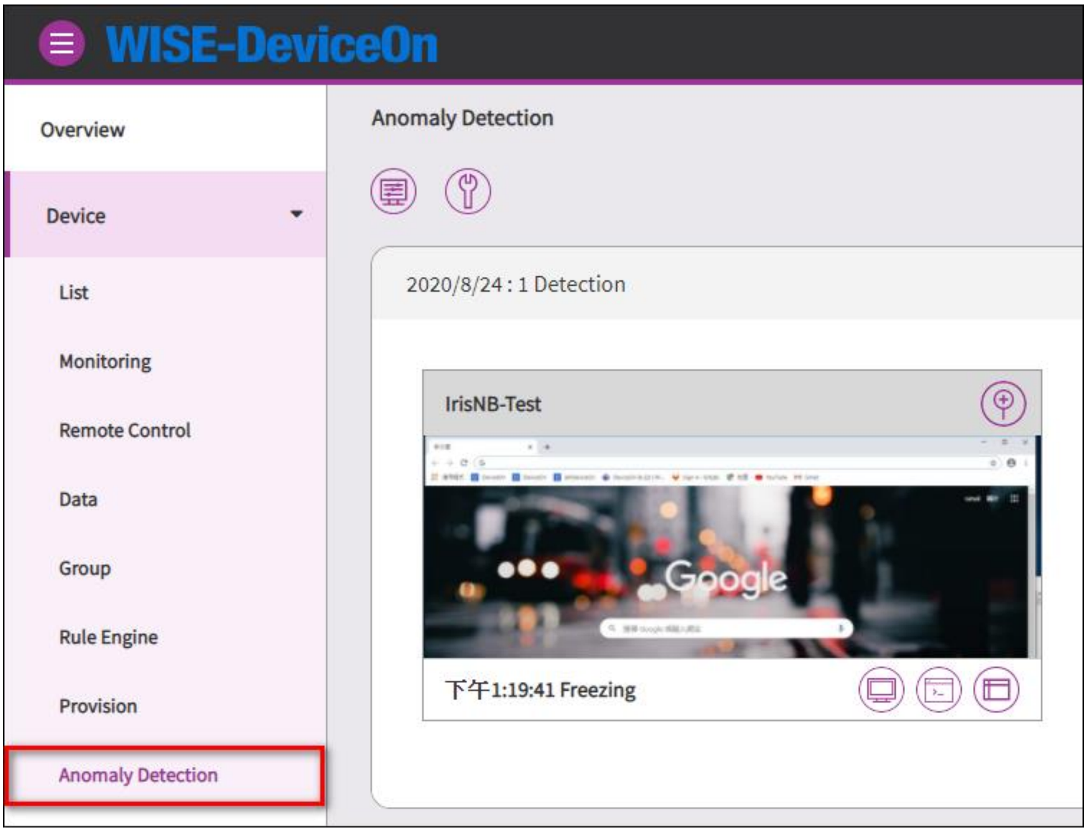
Select Account: Root 1

Select Device Group: AA-X11 2

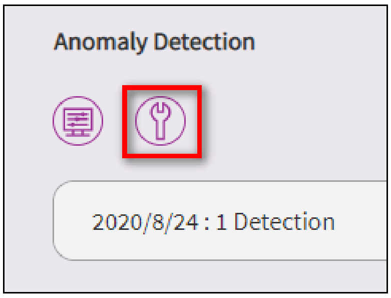
- Anomaly Detection

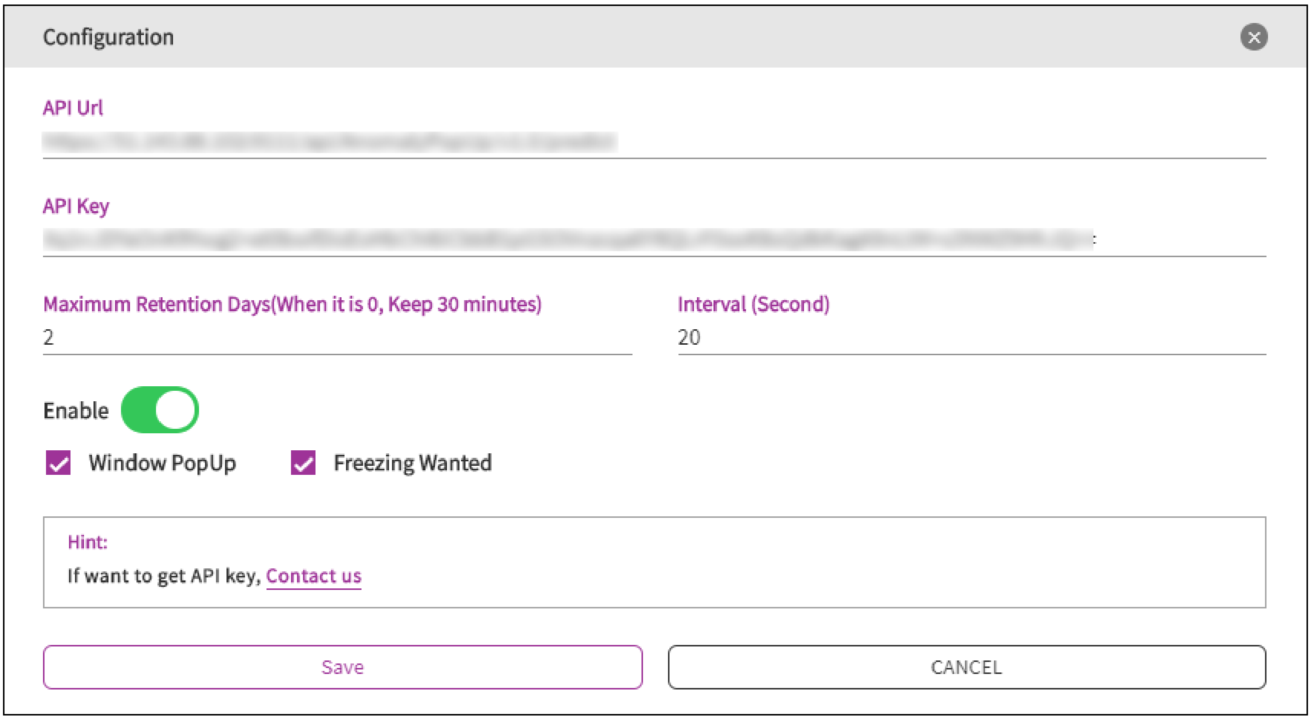
DeviceOn ADS is one of the services that combines anomaly detection algorithm and DeviceOn function. It not only gives customers the high accuracy identification of the error message when advertising is getting interruption but also provides the IoT device remote monitoring and management. Leverage with Azure Custom Vision to continually train the algorithm in order to overcome various errors pop-up under real field.

Before to detect your anomaly screen, please make sure your device is logged in to capture screen status.



Click on the configuration icon to enter API URL and Key.





Configuration

API Url
[redacted]

API Key
[redacted]

Maximum Retention Days(When it is 0, Keep 30 minutes)
2

Interval (Second)
20

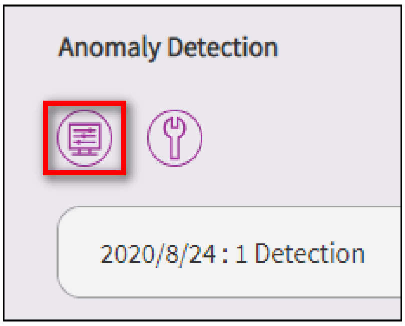
Enable

☑ Window PopUp ☑ Freezing Wanted

Hint:
If want to get API key, Contact us

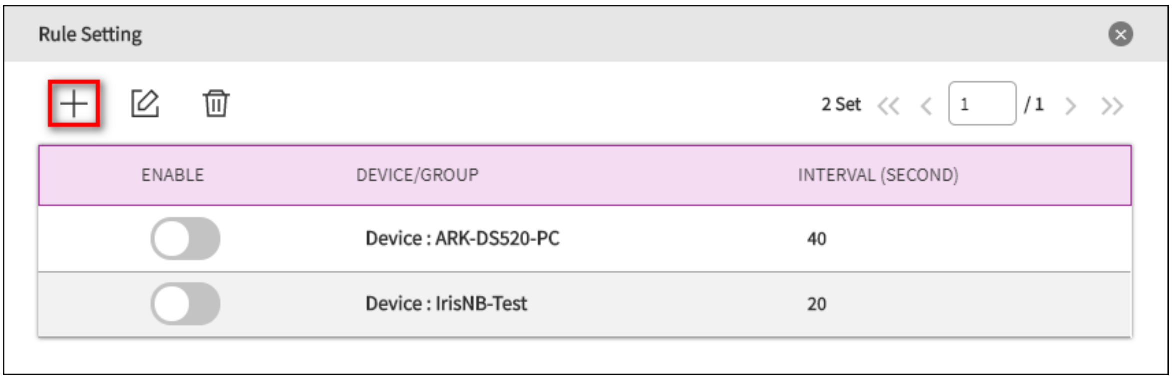
- ✧ API URL & Key: Please contact us for AI machine URL and Key, otherwise, deploy total package from Azure Marketplace.
- ✧ Maximum Retention Days: Maximum retention days for the warning images.
- ✧ Interval: Minimal interval to detect devices screen.
- ✧ Window Popup: Enable to detect popup window on the devices.
- ✧ Freezing Wanted: Enable to detect freezing window on the devices.

Click on the rule icon to enable detection rules.



Anomaly Detection

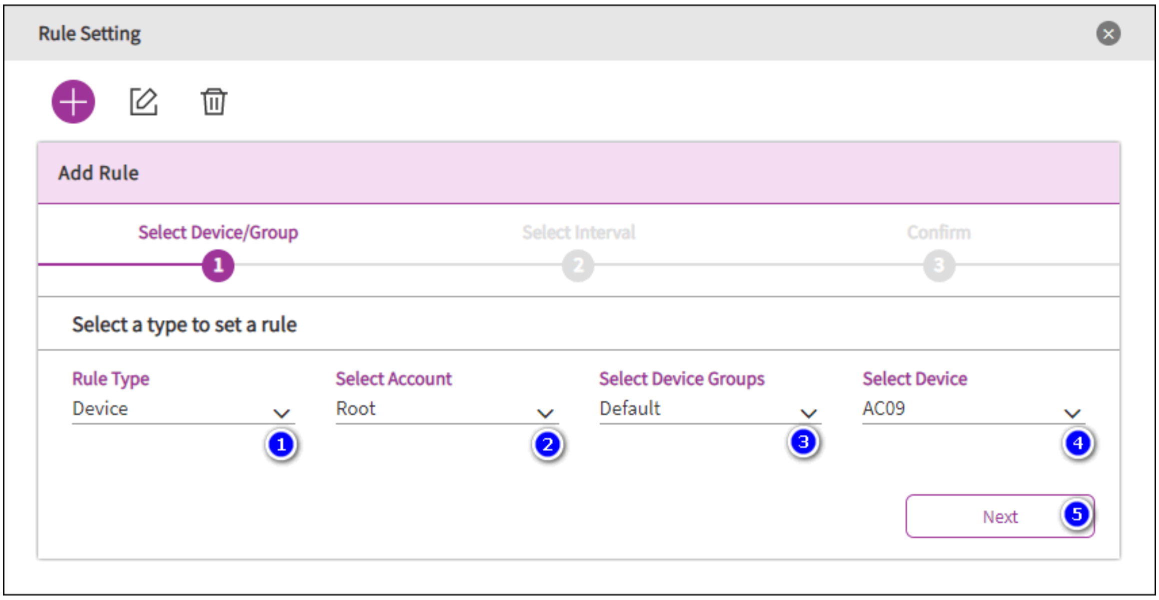
2020/8/24 : 1 Detection



Rule Setting

ENABLE	DEVICE/GROUP	INTERVAL (SECOND)
○	Device : ARK-DS520-PC	40
○	Device : IrisNB-Test	20

Click on the “+” icon to create anomaly rule, select to your device or device group



Rule Setting

Add Rule

Select Device/Group · Select Interval · Confirm

Select a type to set a rule

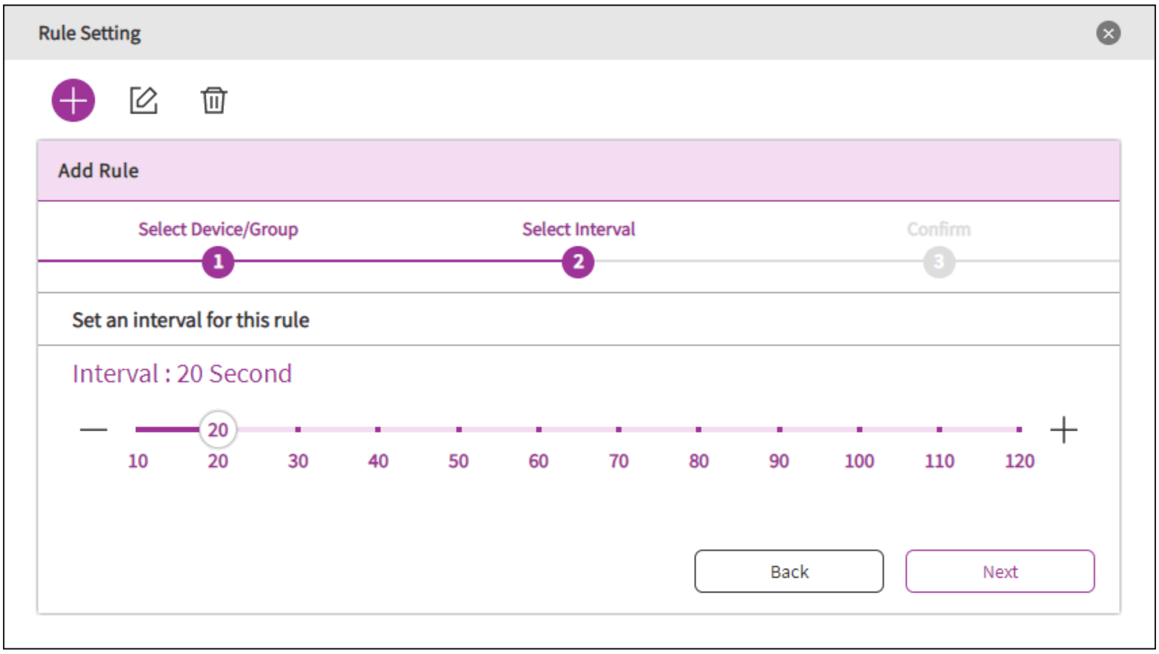
Rule Type: Device (1)

Select Account: Root (2)

Select Device Groups: Default (3)

Select Device: AC09 (4)

Set the detection interval of the rule, the interval cannot be less than the configuration.



Rule Setting

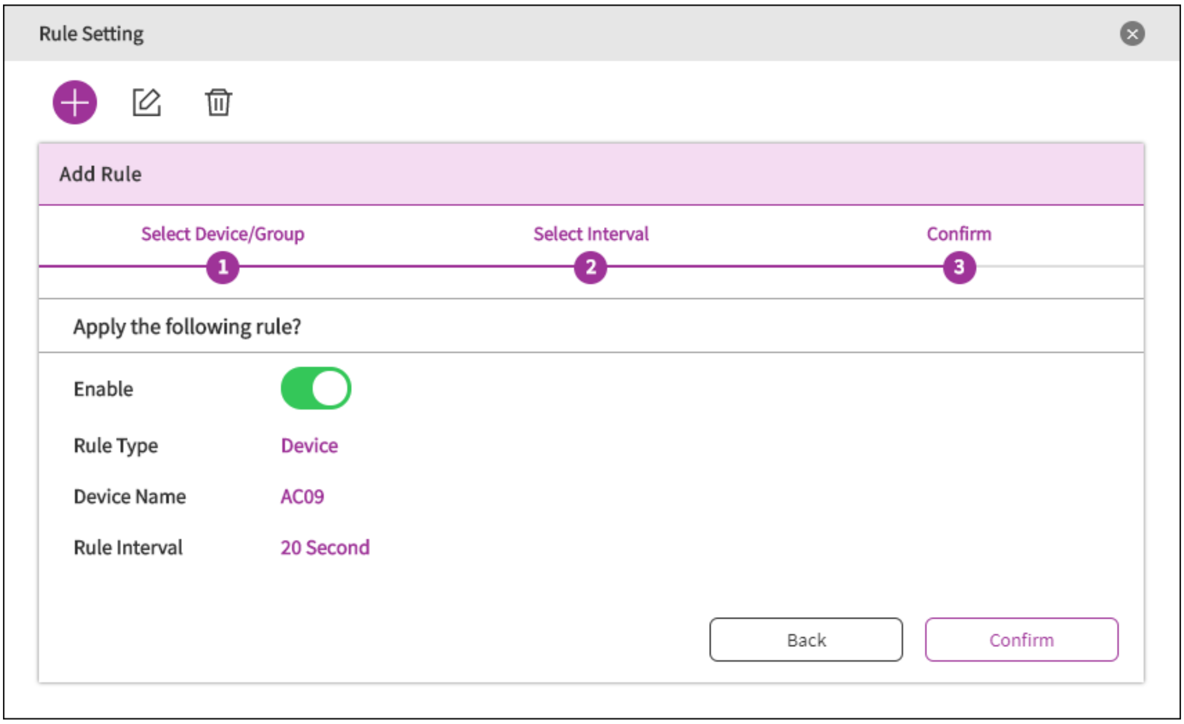
Add Rule

Select Device/Group · Select Interval · Confirm

Set an interval for this rule

Interval : 20 Second

Confirm the rule and enable it.



Rule Setting

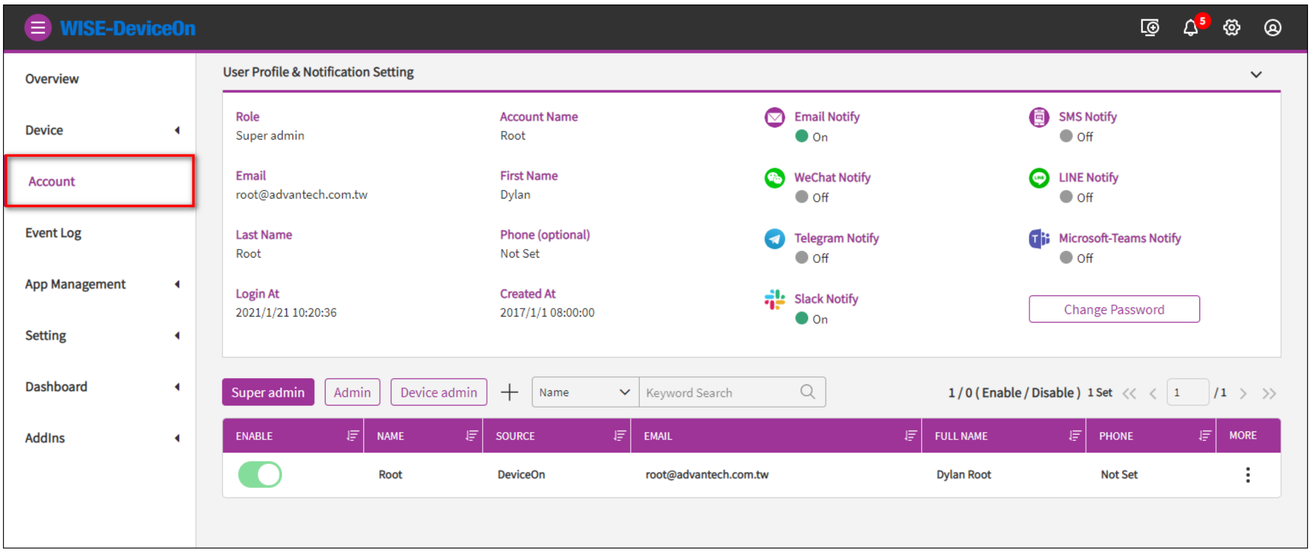
Add Rule

Apply the following rule?

Enable	
Rule Type	Device
Device Name	AC09
Rule Interval	20 Second

3.3.2 **Account Management**

The first step to manage device is login to DeviceOn, therefore, you could start to invite, edit other accounts on this page. The user profile shows your account information and person alert service, such as Email, SMS, WeChat, LINE, Telegram, Slack and Teams status.

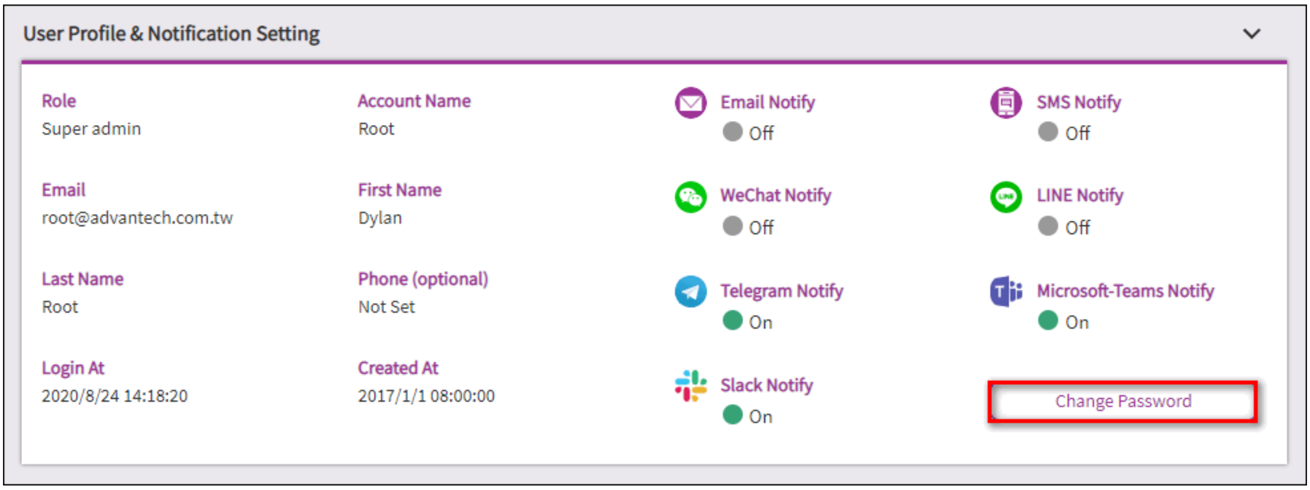


User Profile & Notification Setting

Role: Super admin
Account Name: Root
Email Notify: On
SMS Notify: Off
Email: root@advantech.com.tw
First Name: Dylan
WeChat Notify: Off
LINE Notify: Off
Last Name: Root
Phone (optional): Not Set
Telegram Notify: Off
Microsoft-Teams Notify: Off
Login At: 2021/1/21 10:20:36
Created At: 2017/1/1 08:00:00
Slack Notify: On

ENABLE	NAME	SOURCE	EMAIL	FULL NAME	PHONE	MORE
	Root	DeviceOn	root@advantech.com.tw	Dylan Root	Not Set	⋮

To change your password, please click on the "Change Password" on the profile.



User Profile & Notification Setting

Role
Super admin

Account Name
Root

Email
root@advantech.com.tw

First Name
Dylan

Last Name
Root

Phone (optional)
Not Set

Login At
2020/8/24 14:18:20

Created At
2017/1/1 08:00:00

Email Notify ● Off

SMS Notify ● Off

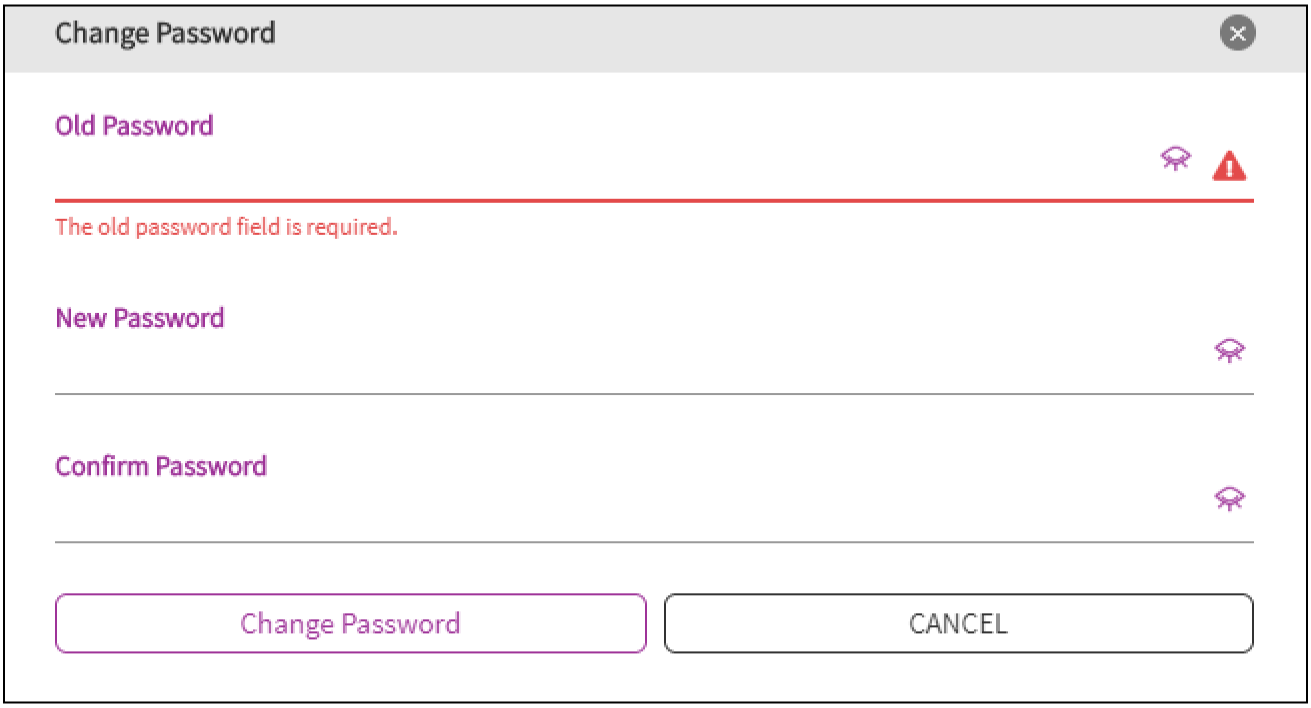
WeChat Notify ● Off

LINE Notify ● Off

Telegram Notify ● On

Microsoft-Teams Notify ● On

Slack Notify ● On



Change Password

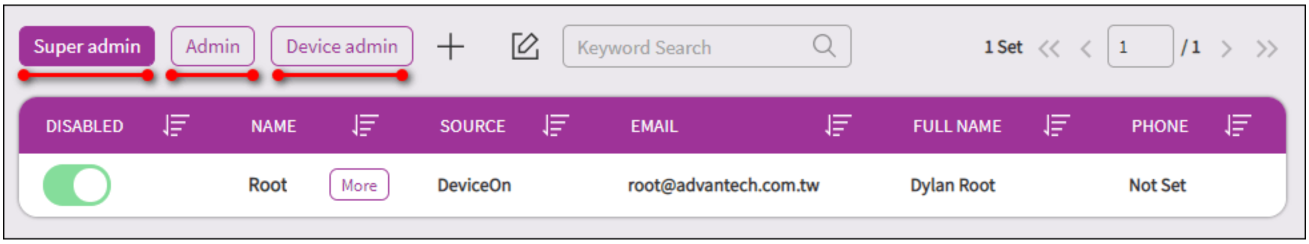
Old Password

The old password field is required.

New Password

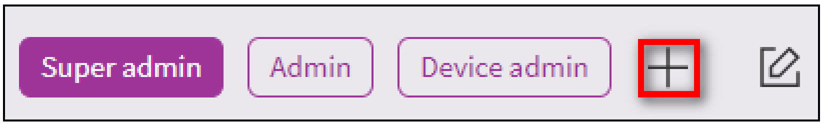
Confirm Password

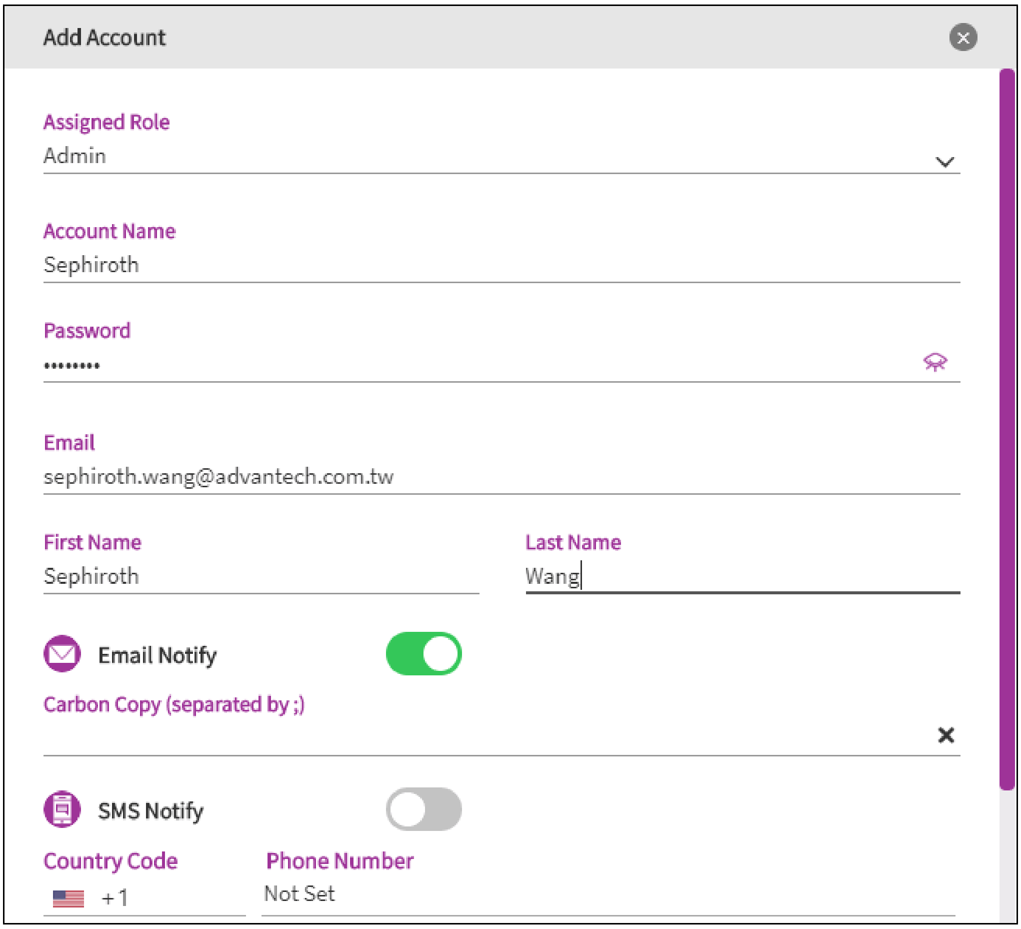
Every account belongs to a role, you could switch the tab to invite/view and edit account. There are 3 roles in the DeviceOn system. One is “**Super Admin**”, only one account in the system belongs to “**Super Admin**”. The other role is “**Admin**” and “**Device Admin**”. For detail role permission,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



DISABLED	NAME		SOURCE	EMAIL	FULL NAME	PHONE
●	Root	More	DeviceOn	root@advantech.com.tw	Dylan Root	Not Set

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 ;)

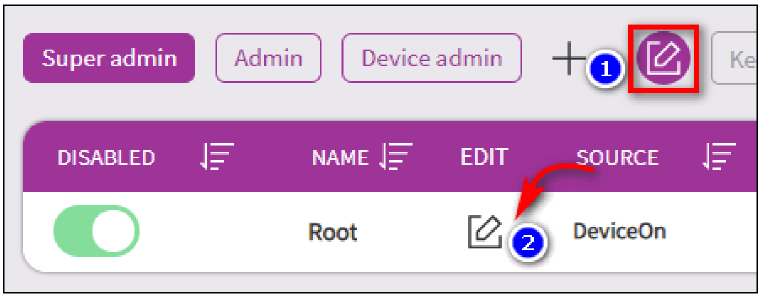
SMS Notify: off

Country Code: +1

Phone Number: Not Set

Enter your account, role, password, etc. to create an account. If the user would receive notify from device, system alert, please enable these alert services on “**Mail**”, “**SMS**”, “**WeChat**”, “**LINE**”, “**Telegram**”, “**Teams**” and “**Slack**”. 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.



DISABLED	NAME	EDIT	SOURCE
on	Root		DeviceOn

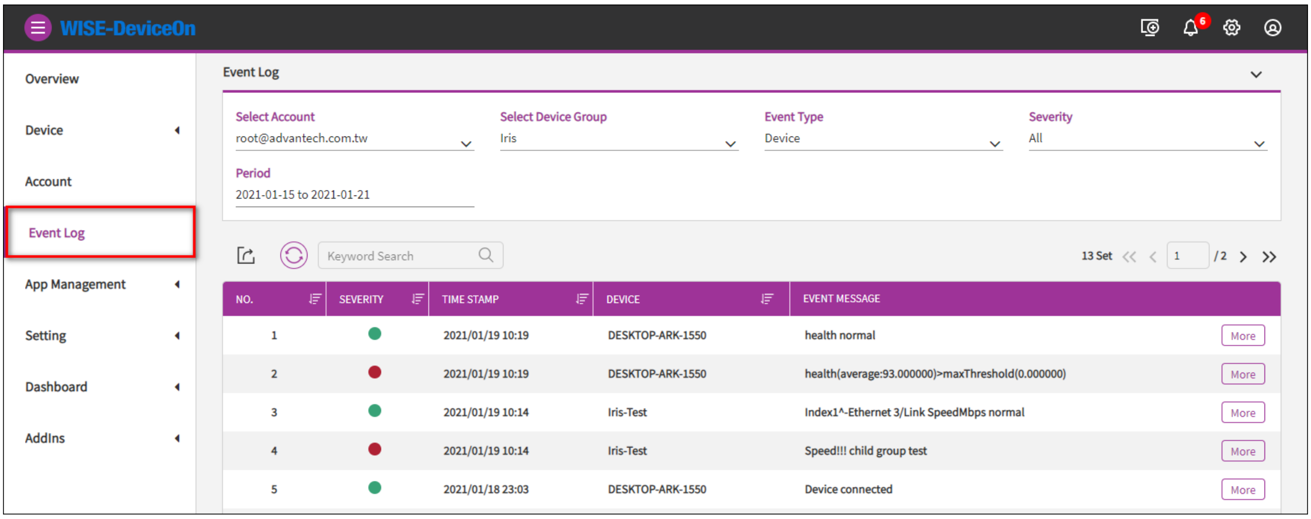
3.3.3 Event Logs

Device management is complex with device log and user behaver. 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:

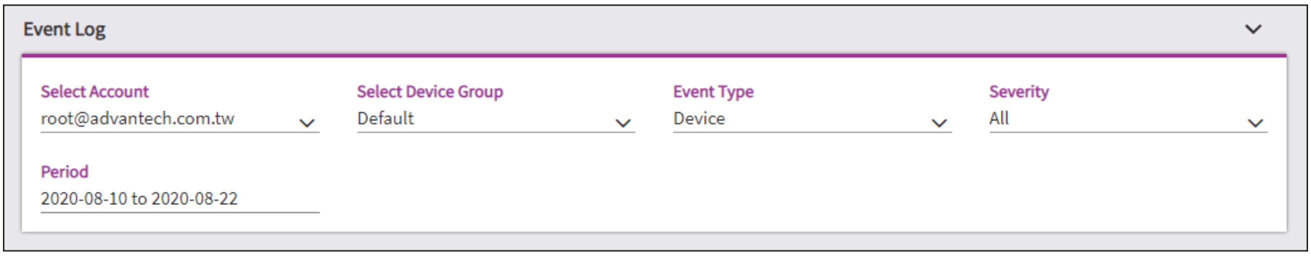
- Operation logs provide information about DeviceOn resource CREATE, UPDATE and DELETE operation, like set device power off, update device name or delete account.
- Device logs provide information about events raised as device side resources, like connected, disconnected, over the threshold,
- System logs 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 IoTHub queue and provides concise alerts.



Select Account: root@advantech.com.tw
Select Device Group: Iris
Event Type: Device
Severity: All
Period: 2021-01-15 to 2021-01-21

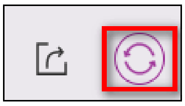
NO.	SEVERITY	TIME STAMP	DEVICE	EVENT MESSAGE	
1	🟢	2021/01/19 10:19	DESKTOP-ARK-1550	health normal	More
2	🔴	2021/01/19 10:19	DESKTOP-ARK-1550	health(average:93.000000)>maxThreshold(0.000000)	More
3	🟢	2021/01/19 10:14	Iris-Test	Index1^-Ethernet 3/Link SpeedMbps normal	More
4	🔴	2021/01/19 10:14	Iris-Test	Speed!!! child group test	More
5	🟢	2021/01/18 23:03	DESKTOP-ARK-1550	Device connected	More

There are three types 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.

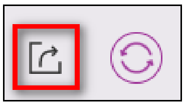


Select Account: root@advantech.com.tw
Select Device Group: Default
Event Type: Device
Severity: All
Period: 2020-08-10 to 2020-08-22

Click on the icon to refresh event log by manual.



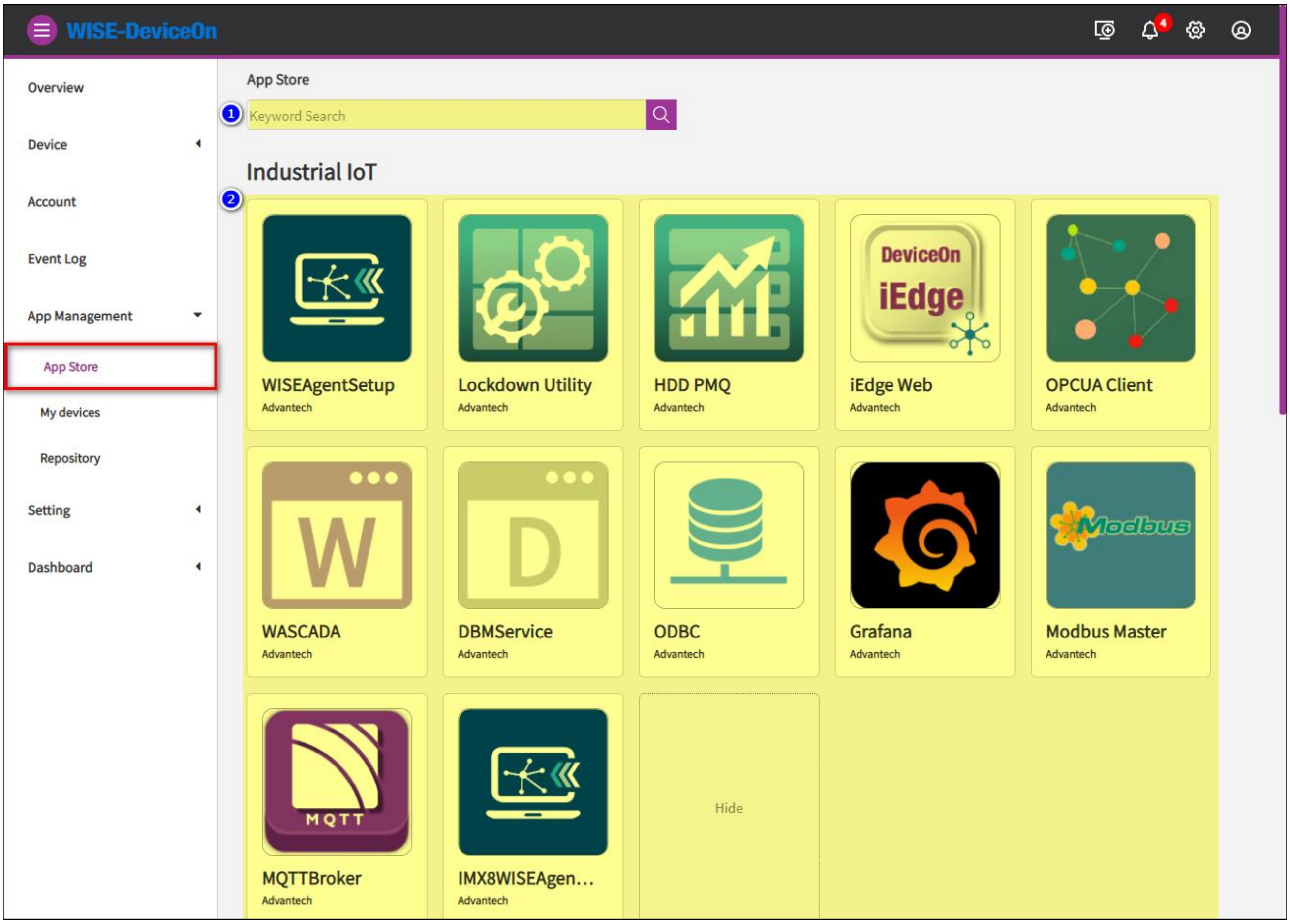
Click on export icon to export devices that in the table as CSV file.



3.3.4 App Management (Enhancement OTA)

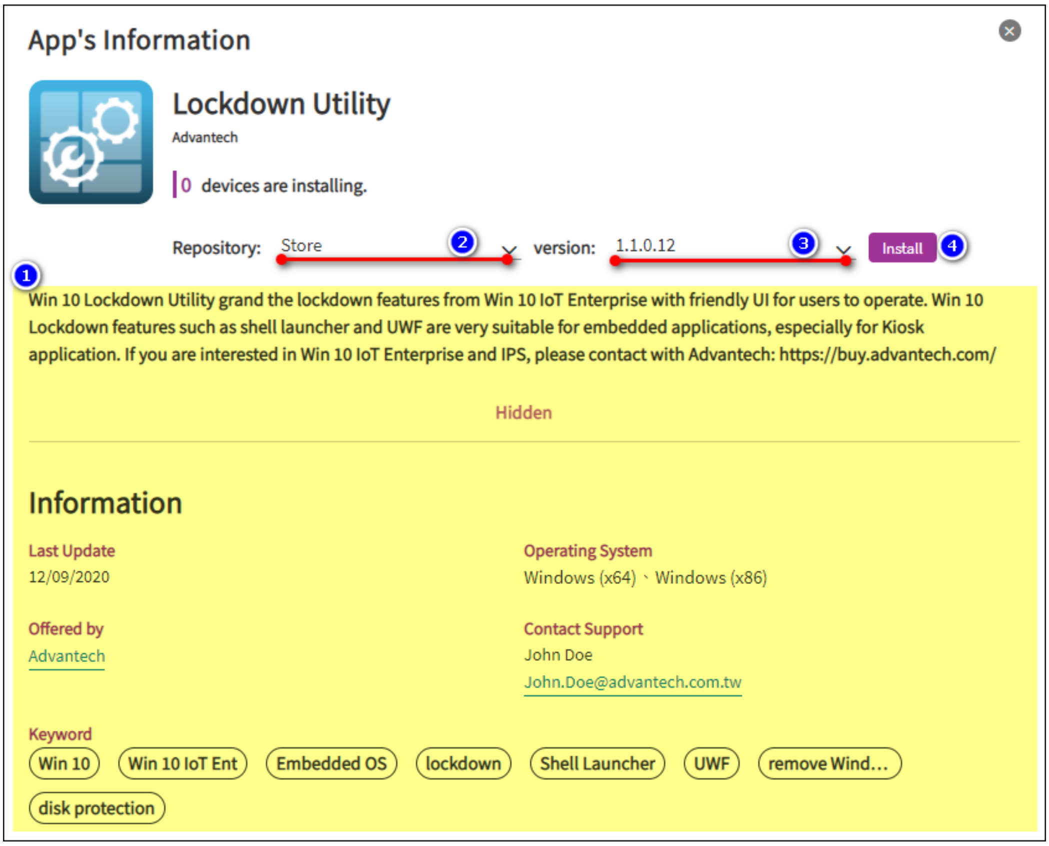
App Store is an enhanced OTA software update feature which presented in a familiar mobile management user interface to provide users with the ability to manage their own exclusive applications and deploy them to remote devices in a simple way. App Store is divided into two modes of operation. IT administrators could use WISE-DeviceOn portal to customize, upload, manage apps and schedule installation to designated devices, which we call the manager mode. Second, in the client mode, the App Store application is built-in the device side, and the device can instantly update the applications.

- App Store



1. **Keyword Search**: Input keyword to search apps.
2. **App List**: View all apps, grouping by category. Click to open a window to present App Information.

[Application Information]



App's Information

Lockdown Utility

Advantech

0 devices are installing.

Repository: Store

version: 1.1.0.12

Win 10 Lockdown Utility grand the lockdown features from Win 10 IoT Enterprise with friendly UI for users to operate. Win 10 Lockdown features such as shell launcher and UWF are very suitable for embedded applications, especially for Kiosk application. If you are interested in Win 10 IoT Enterprise and IPS, please contact with Advantech: https://buy.advantech.com/

Hidden

Information

Last Update
12/09/2020

Operating System
Windows (x64) 、Windows (x86)

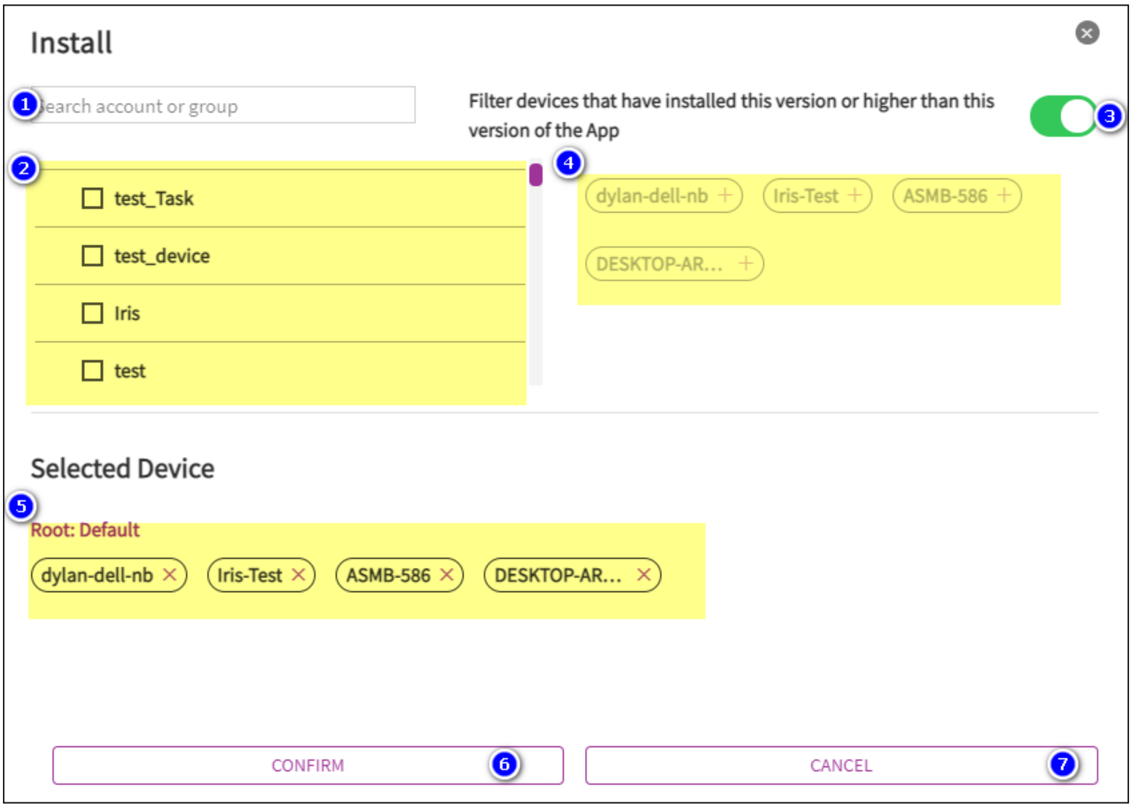
Offered by
Advantech

Contact Support
John Doe
John.Doe@advantech.com.tw

Keyword
Win 10 | Win 10 IoT Ent | Embedded OS | lockdown | Shell Launcher | UWF | remove Wind... | disk protection

1. **Information**: Including all information about the app.
   - A. *Description*: Description text of app. Hidden in default, click [**More**] to show all.
   - B. *Last Update*: Last update date of app.
   - C. *Operating System*: The app's support operating system. It is relevant to version, might have different platforms between versions.
   - D. *Offered by*: The provider company of app. Click on it to show more information of the company, and all apps belongs to the company.
   - E. *Contact Support*: Contact person of the app.
   - F. *Keyword*: Keyword list of the app. Manager can search app by these keywords.
2. **Repository**: The file holder of the app. Select one of repositories to decide where app downloads from and getting app's Version list.
3. **Version**: The version number of the app.
4. **Install**: After select Repository and Version, click Install button to open the Install dialog, where manager can select Devices/Groups to run installation.

[Install]

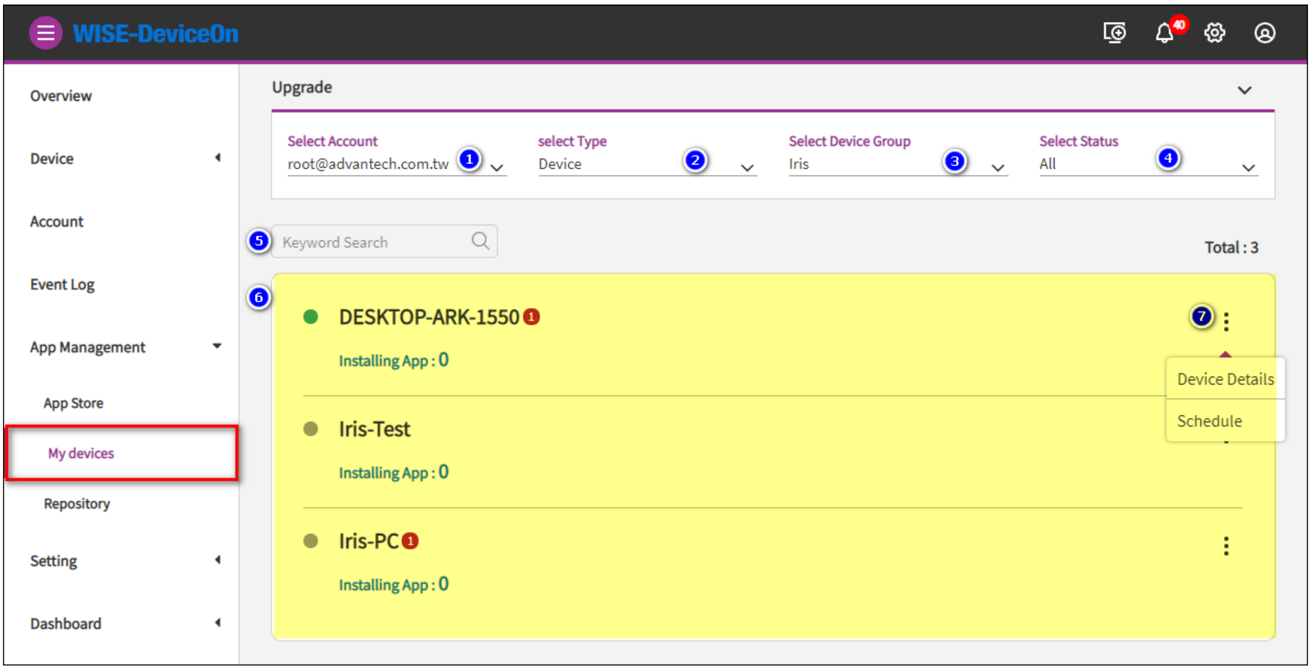


1. **Search account or group**: Input keyword to search account or group. It is useful when there are a lot of accounts below.
2. **Accounts and Device Groups**: List accounts, and Device Groups under each account. Check the Device Group will add all installable devices of the Device Group to Selected Device.
3. **Filter devices**: Turn On/Off the filter.
   - If switch-on: Device List shows devices which does not install the version of the app.
   - If switch-off: Device List shows devices which does not install the version of the app, and devices have installed app's version is the same or beyond manager selected version. Default is "On" to prevent manager duplicating installing app with the same version.
4. **Device List**: Devices can install the app will list in this area. Click the plus sign + will add the device to Selected Device.
5. **Selected Device**: Devices list here will install the app.
6. **CONFIRM**: Execute installation of the app to selected devices.
7. **CANCEL**: Cancel this operation, back to previous step.

- My Devices

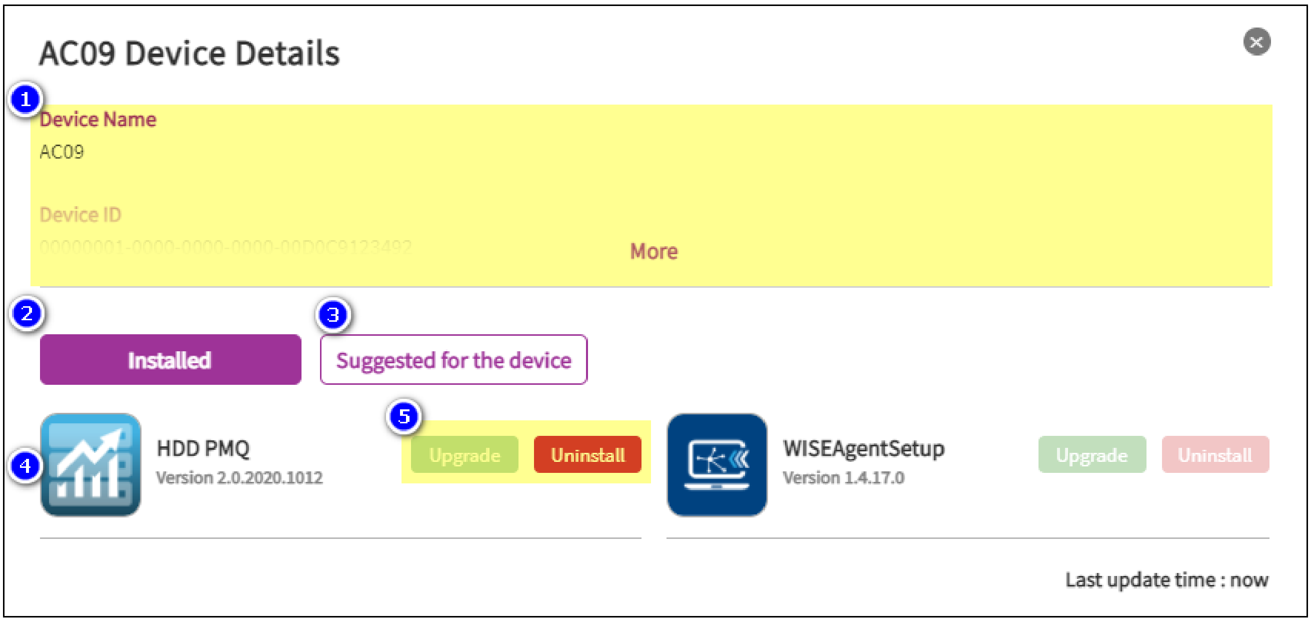
Specify a device to control app upgrade, install, uninstall, and set schedule of certain app maintenance. Also, schedule can be added to Device Group, control multiple devices by pre-defined group.

[Device List]



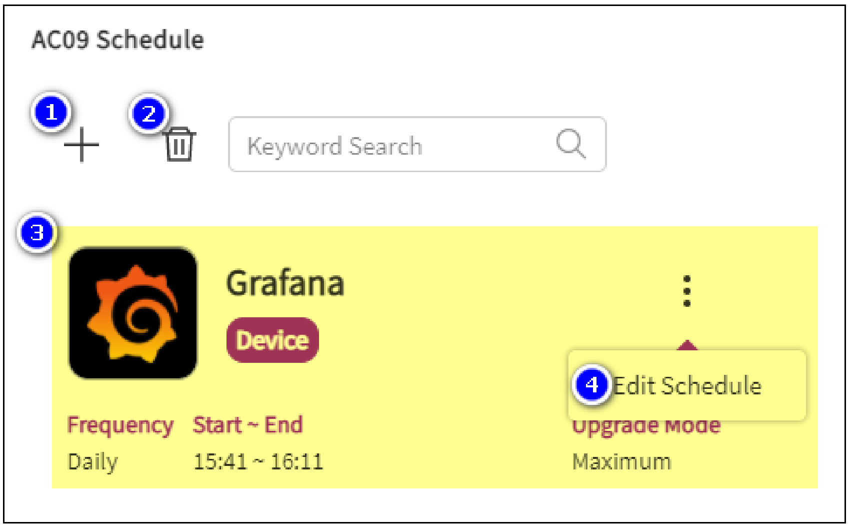
1. **Select Account**: Select an account which owns device, manager want to control.
2. **Select Type**: Select Device to retrieve device list or select Device Group to retrieve device group list. Changing this option will affect result of list below.
3. **Select Device Group**: Select a device group to retrieve device under the group.
4. **Select Status**: Select device connect status.
5. **Keyword Search**: Input keyword to search match device.
6. **Device List**: Match conditions' device list here.
7. **Open Menu**: Click to open menu.

[Device Details]

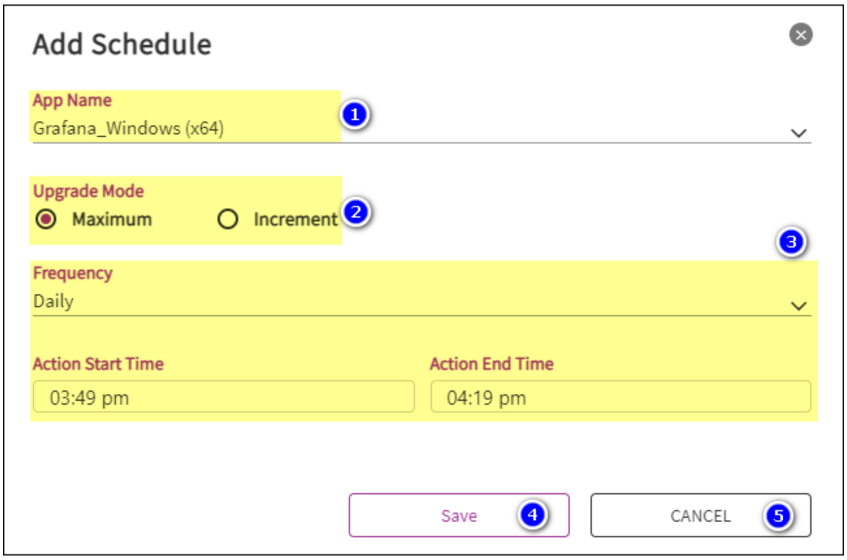


1. **Device Information**: Information of the device, click More to view full content
2. **Installed**: Show installed app of the device.
3. **Installed App**: Installed apps list.
4. **Suggested for the device**: Not installed apps list, or installed app has newer version.
5. **App Control Button**: Enabled button is colorful, otherwise button is fade-out.
   5.1. *Upgrade*: The app can upgrade to newer version.
   5.2. *Uninstall*: The app support uninstall ability; manager can uninstall the app online.

[Device Schedule]



1. **Add Schedule**: Open a dialog to add schedule setting.


Add Schedule

App Name: Grafana_Windows (x64)

Upgrade Mode: ● Maximum ○ Increment

Frequency: Daily

Action Start Time: 03:49 pm

Action End Time: 04:19 pm

1.1. *App Name*: Select an application and OS to upgrade.

1.2. *Upgrade Mode*: Decide how to upgrade when there are multiple versions beyond the app installed in the device currently. **Maximum** mode will upgrade to the latest version directly. **Increment** mode will upgrade from next version to the latest version by ascending sorted version.

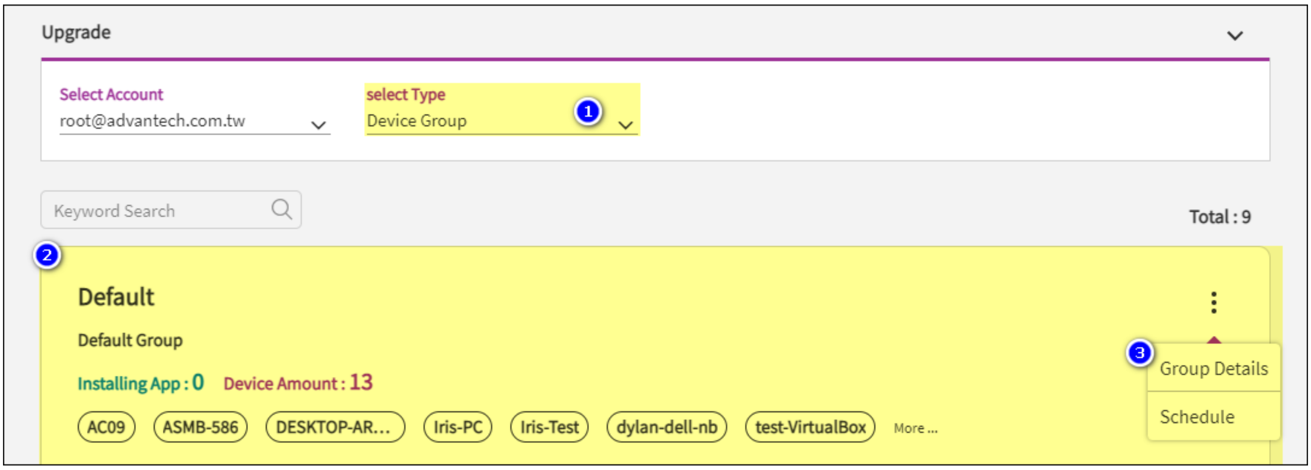
1.3. *Execute Frequency*: Schedule executing frequency. By changing frequency option to set relevant setting. DeviceOn provide **Daily**, **Weekly**, **Monthly**, and **Once** to fit variable schedule needing.

1.4. *Save*: Click to save schedule setting.

1.5. *Cancel*: Discard changes and close this dialog.

2. **Remove Schedule**: Switch to remove mode, select schedules which manager want to remove, then click this button again to remove selected schedule.
3. **Schedule List**: List schedules of the device. And the setting detail of schedule.
4. **Edit Schedule**: Open a dialog to change schedule upgrade mode, executing frequency and timing.

[Device Group List]



Upgrade

Select Account: root@advantech.com.tw

select Type: Device Group

Total : 9

Default

Default Group

Installing App : 0 Device Amount : 13

1. **Select Type**: Select Device Group to retrieve device group list or select Device to retrieve device list. Changing this option will affect result of list below.
2. **Device Group List**: Device groups are managed by Select Account will list here.
3. **Open Menu**: Click to open menu.

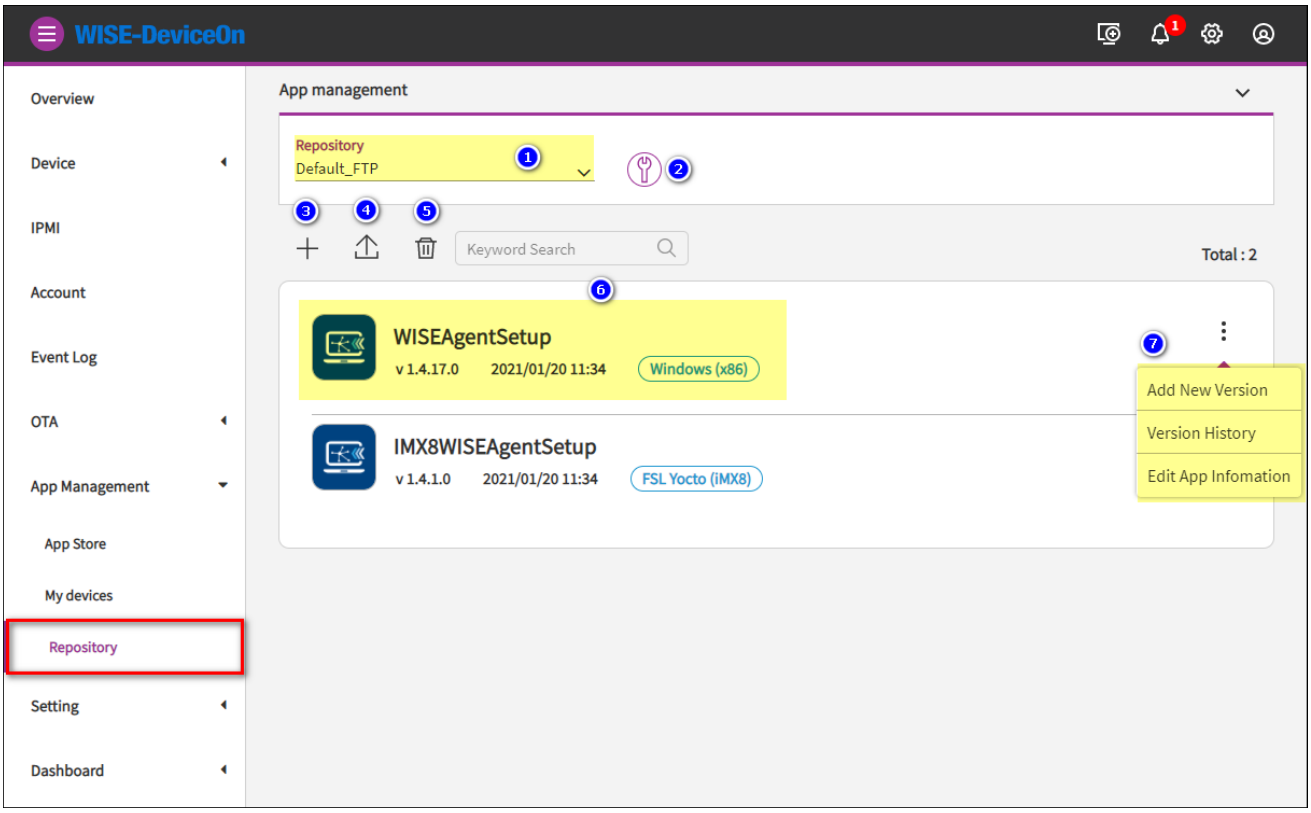
3.1. *Group Details*: Open a dialog shows device group relevant information. e.g. group description, list of devices under the device group.

3.2. *Group Schedule*: Setting schedule to the device group. UI and setting are all the same with Device Schedule. And, the schedule setting will apply to devices in the group, which are able to install/upgrade app.

- Repository

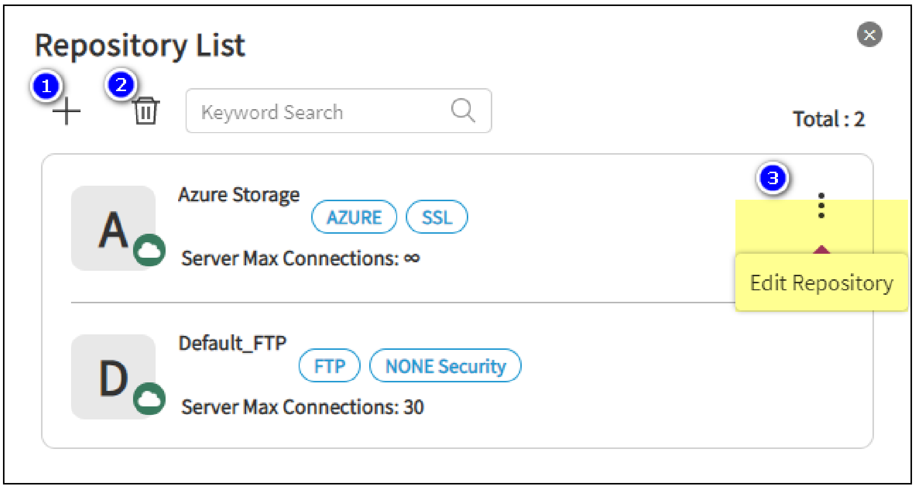
Repository management, and app management. Repository is where apps package file upload to. Repository support several protocols, e.g., **Azure Blob**, **Amazon S3**, and **FTP**. Manager can create preferred repository or using built-in Default-FTP provided by DeviceOn. Upload app package file, maintaining versions of app, or modify app's description data, icon. Also, manager can wrap your own app via online tool.

[Repository Overview]



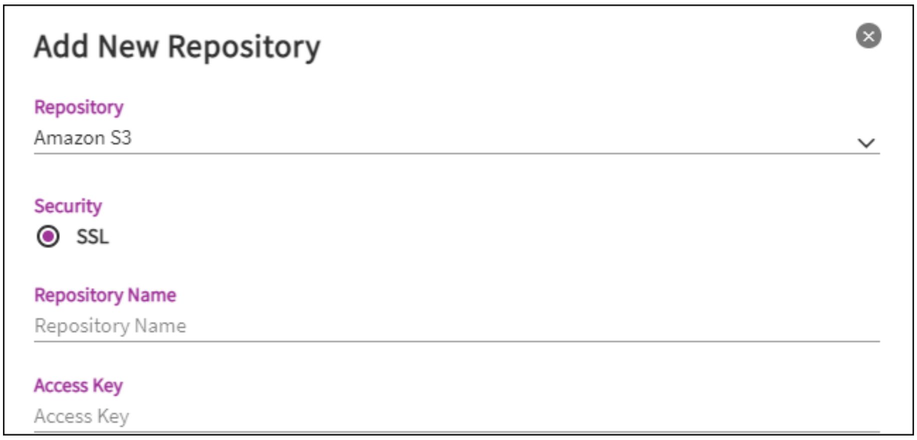
1. **Repository List**: All repository's list here. Select an option to show apps in the repository.
2. **Edit Repository List**: Open a dialog to manage repository.
3. **Add App**: Open **Online Wrap Tool** to build an app.
4. **Upload App**: Upload app package files which are created by **Online Wrap Tool**.
5. **Remove App**: Switch to remove mode, select app which manager want to remove, then click this button again to remove selected app.
6. **App**: The app brief information. E.g. latest version number, update date, and support OS.
7. **Menu**: Open a menu shows **Add New Version, Version History, Edit App Information**.

[Repository Management]



1. **Add New Repository**: Open a dialog to add a repository, depending on selected repository type

to enter relevant parameters.



Add New Repository

Repository
Amazon S3

Security
● SSL

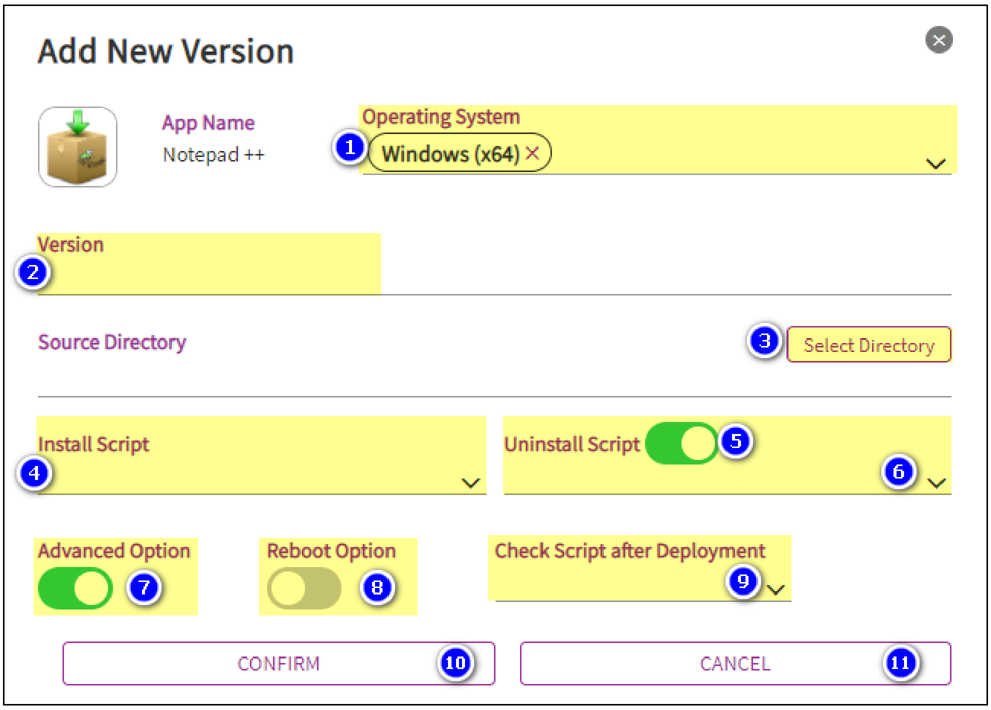
Repository Name
Repository Name

Access Key
Access Key

2. **Remove Repository**: Switch to remove mode, select repository which manager want to remove, then click this button again to remove selected repository.
3. **Edit Repository**: Open a dialog to edit selected repository setting.

[App Management]

1. **Add New Version**



Add New Version

App Name
Notepad ++

Operating System
Windows (x64)

Version

Source Directory

1.1. *Operating System*: Select OS of the version can install.

1.2. *Version*: Version number. 3 or 4 digits and separated by dot(.). For example: 1.0.0 or 1.2.3.4

1.3. *Select Directory*: Select a directory to upload, which contains files are necessary for installing the app.

1.4. *Install Script*: Select a runnable script file for executing installation.

1.5. *Uninstall Option*: Switch On/Off to determine this version’s app can uninstall or not.

1.6. *Uninstall Script*: Select a runnable script file for executing uninstallation.

1.7. *Advanced Option*: Switch On/Off to show/hide more option.

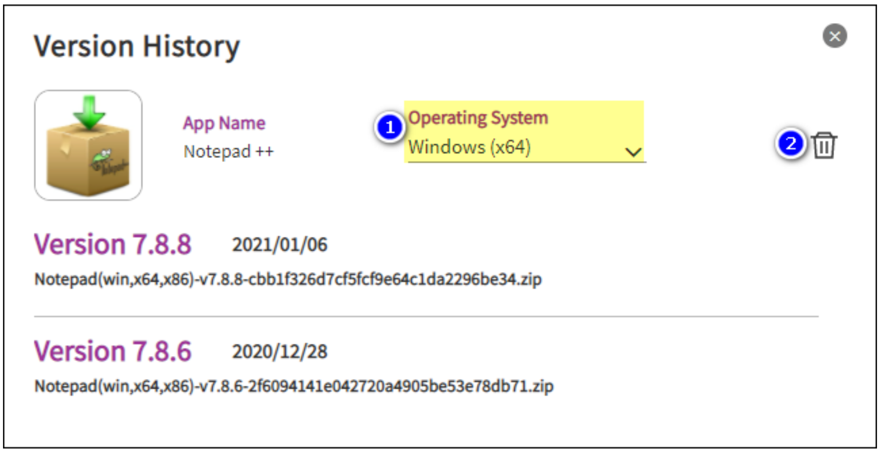
1.8. *Reboot Option*: Switch On/Off to determine this version's app need reboot after installation or not.

1.9. *Check Script*: Select a runnable script file for executing checking result of installation is successful or failed. The script file must return "0", that means success, and all other value will be took as fail.

1.10. *CONFIRM*: After reviewing settings above, then click this button to start upload

1.11. *CANCEL*: Discard changes and close this dialog.

2. Version History



Version History

App Name
Notepad ++

Operating System
Windows (x64)

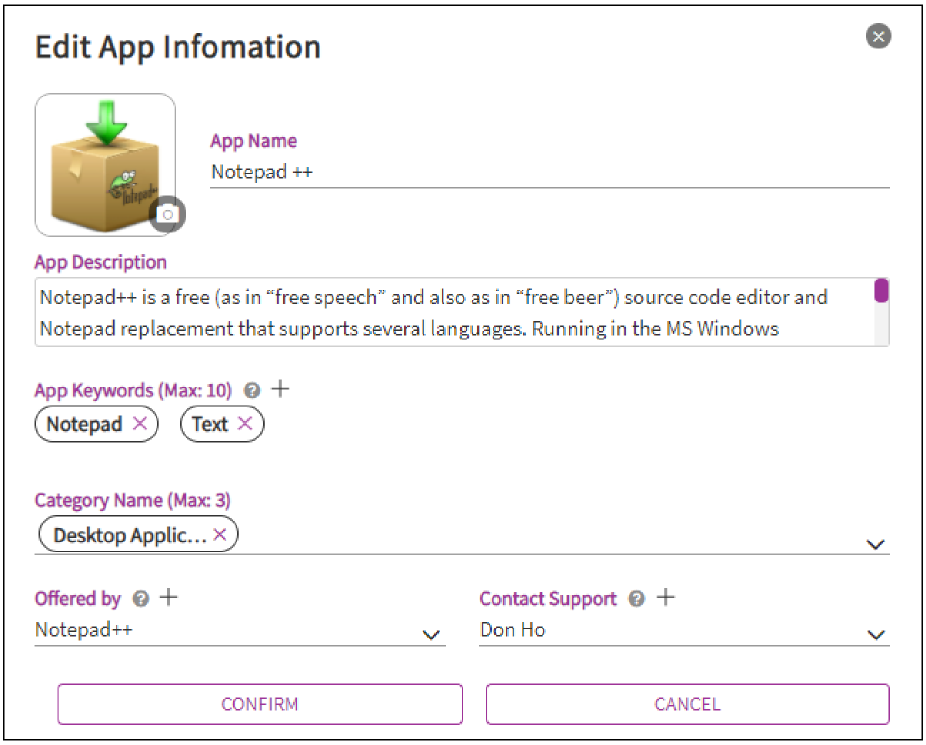
Version 7.8.8 2021/01/06
Notepad(win,x64,x86)-v7.8.8-cbb1f326d7cf5fcf9e64c1da2296be34.zip

Version 7.8.6 2020/12/28
Notepad(win,x64,x86)-v7.8.6-2f6094141e042720a4905be53e78db71.zip

2.1. *Operating System*: Show all support operating system in list. By selecting different item in the list to show versions it owns.

2.2. *Remove Version*: Switch to remove mode, select version which manager want to remove, then click this button again to remove selected version.

3. Edit App Information



Edit App Infomation

App Name: Notepad ++

App Description: Notepad++ is a free (as in "free speech" and also as in "free beer") source code editor and Notepad replacement that supports several languages. Running in the MS Windows

App Keywords (Max: 10): Notepad, Text

Category Name (Max: 3): Desktop Applic...

Offered by: Notepad++

Contact Support: Don Ho

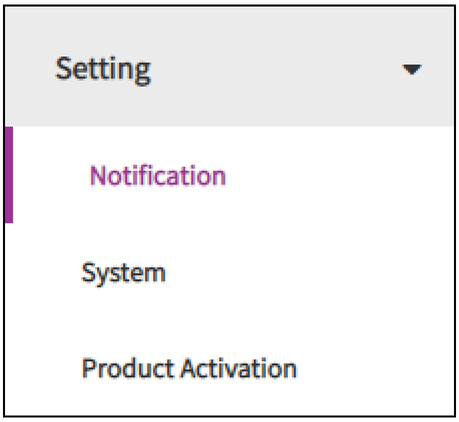
Manager can edit the app's descripting data, changing icon, provider, and contact information. Click CONFIRM to apply setting. Or, click CANCEL to discard change and close dialog.

[Wrap Your Application]

Refer to Hand-On Labs, **Section 4.2.**

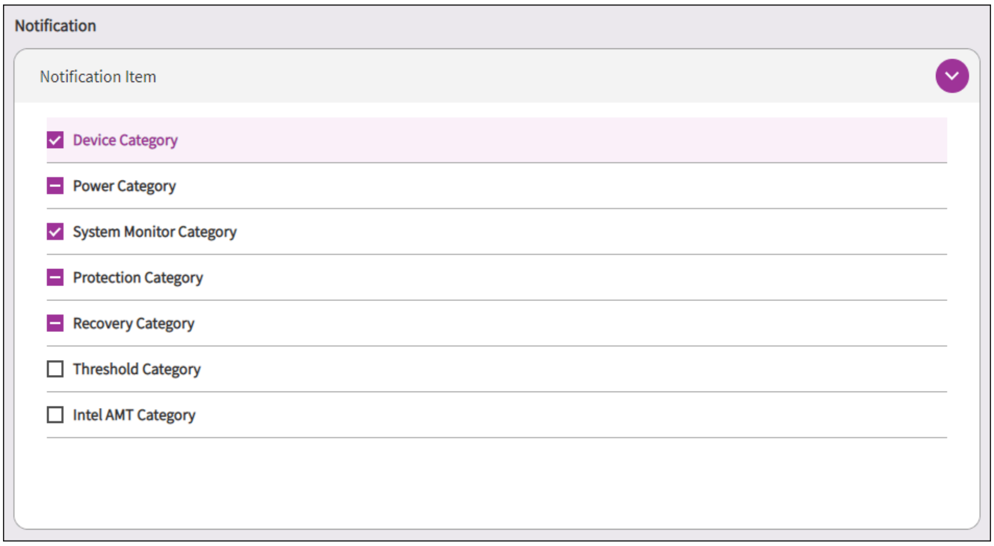
3.3.5 System Configuration

A System Configuration define advanced setting include "**Notification & Event Alert**", "**System UI**" and "**Product Activation**. These setting 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.



- Notification & Event Alert

Here are seven notification services, include tradition service (SMS, Email) and popular social media (LINE, WeChat, Telegram, Microsoft Teams, Slack), if you select the event log type on "**Notification Item**", 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**.



Notification

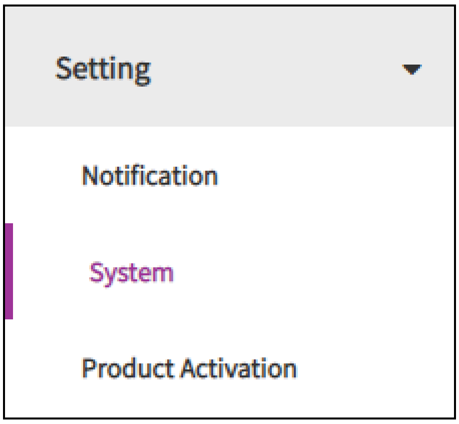
Notification Item

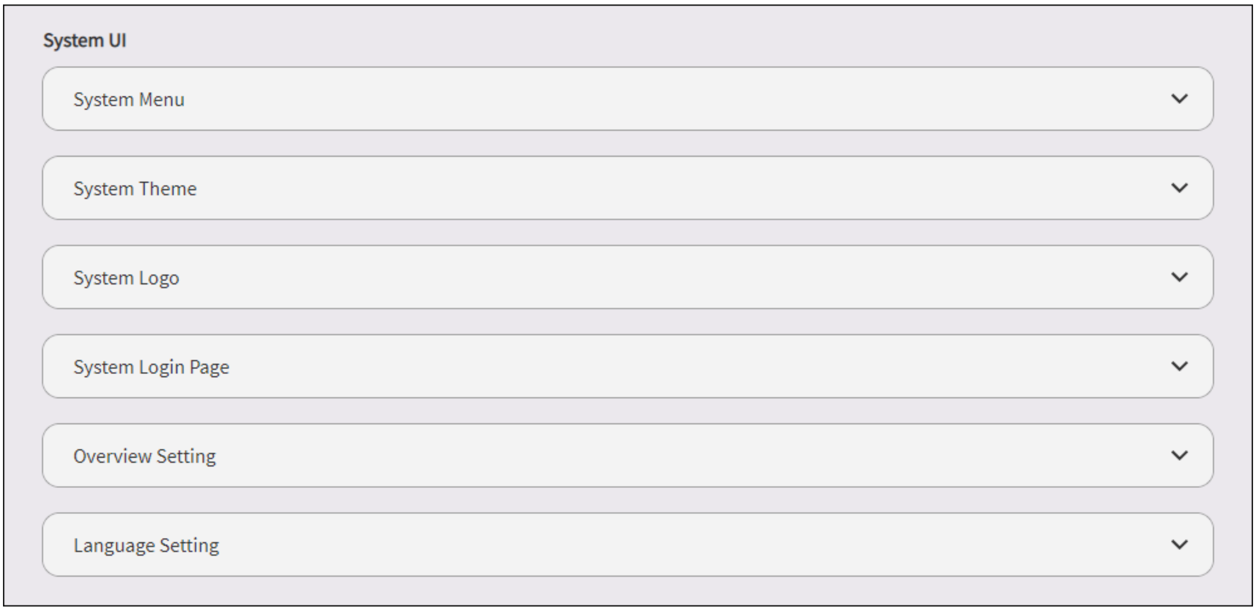
☑ Device Category
⊟ Power Category
☑ System Monitor Category
⊟ Protection Category
⊟ Recovery Category
☐ Threshold Category
☐ Intel AMT Category

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

- System User Interface

DeviceOn provide an option to customize menu item, theme, logo and user could by setting up the user interface to meet their needs.





System UI

System Menu

System Theme

System Logo

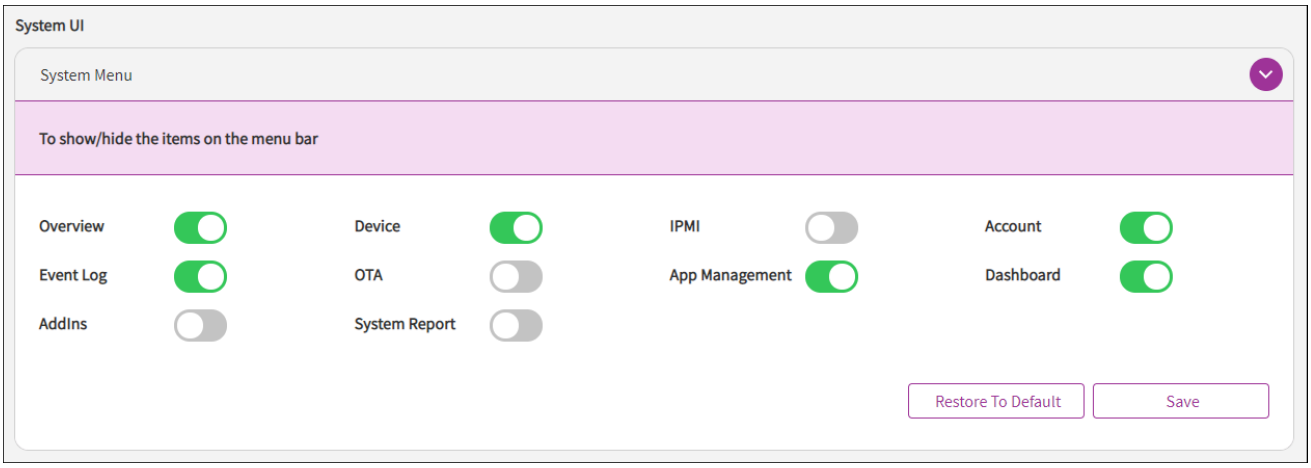
System Login Page

Overview Setting

Language Setting

✧ System Menu: To show/hide the items on the menu bar

The default setting does not include “**IPMI**”, “**OTA**” (Replaced by **App Management**), “**Addins**” and “**System Report**”, the “**AddIns**” is used to customized UI page or embed specific website page to integrate with DeviceOn.



System UI

System Menu

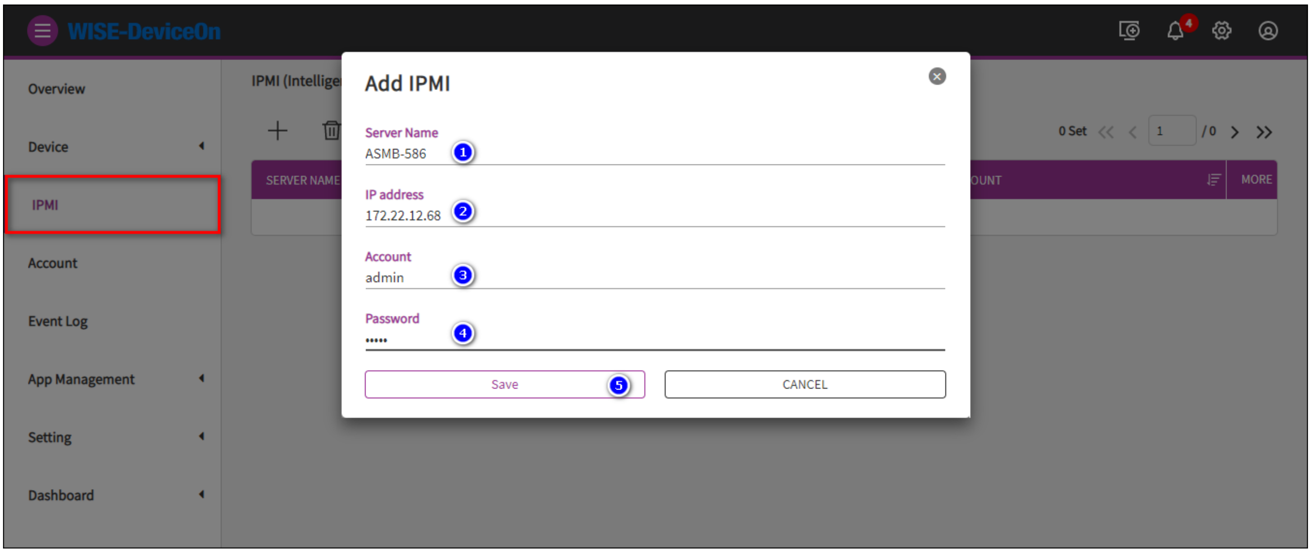
To show/hide the items on the menu bar

Overview	☑	Device	☑	IPMI	☐	Account	☑
Event Log	☑	OTA	☐	App Management	☑	Dashboard	☑
AddIns	☐	System Report	☐				

➢ [IPMI]

The Intelligent Platform Management Interface (IPMI) is a standardized message-based hardware management interface. At the core of the IPMI is a hardware chip that is known as the Baseboard Management Controller (BMC), or Management Controller (MC). DeviceOn integrate standard functions as below to retrieve device status and power management.

- Sensors (“sensor” and “sdr” related commands) --- practically using all the IPMI sensors as data source in DeviceOn
- SEL (System Event Log)
- power on/off/graceful shutdown/cycle as well as reset commands



Add IPMI

Server Name
ASMB-586 1

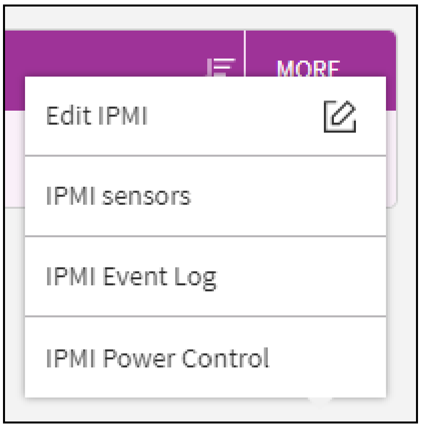
IP address
172.22.12.68 2

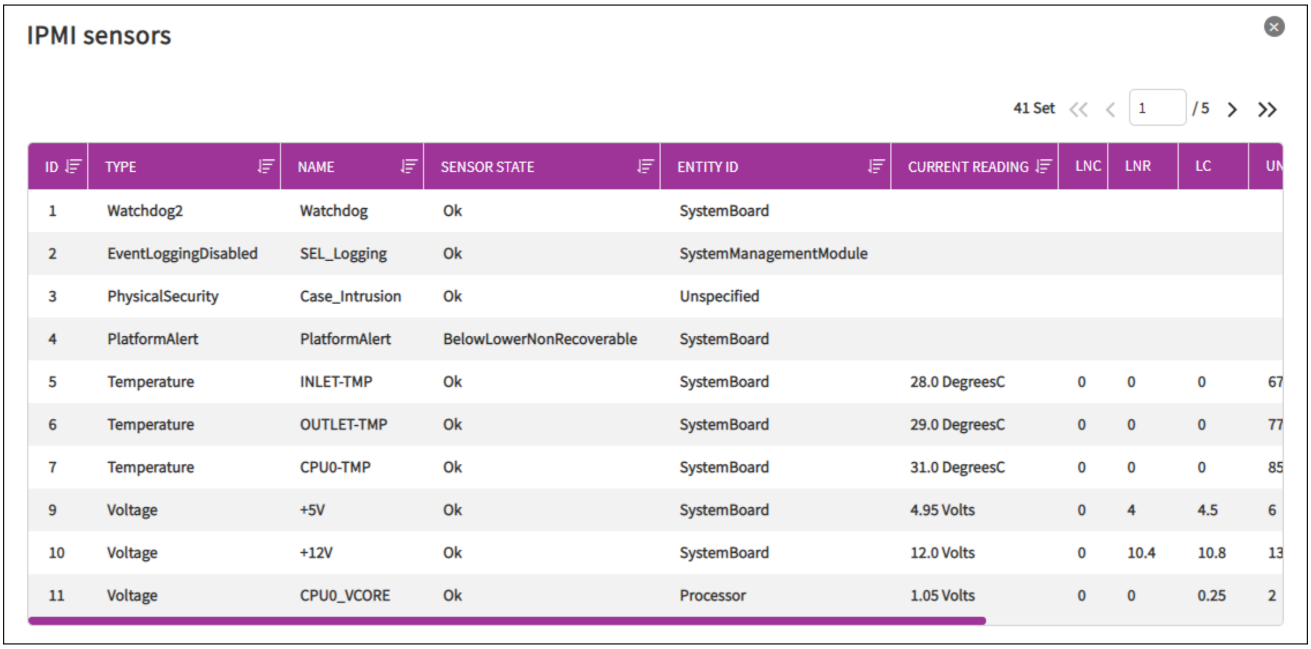
Account
admin 3

Password
••••• 4

Save 5 | CANCEL

Click on more option to view the device sensor, event log and power control.





IPMI sensors

41 Set 1 / 5

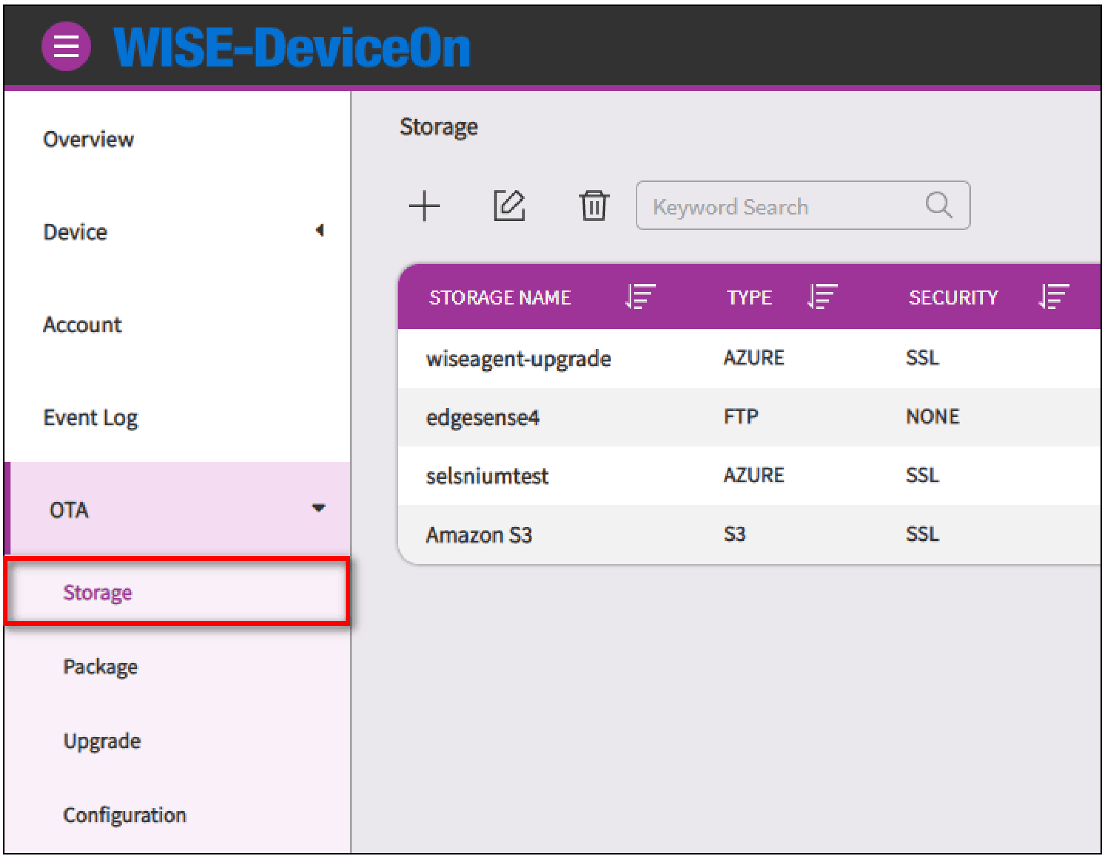
ID	TYPE	NAME	SENSOR STATE	ENTITY ID	CURRENT READING	LNC	LNR	LC	UN
1	Watchdog2	Watchdog	Ok	SystemBoard					
2	EventLoggingDisabled	SEL_Logging	Ok	SystemManagementModule					
3	PhysicalSecurity	Case_Intrusion	Ok	Unspecified					
4	PlatformAlert	PlatformAlert	BelowLowerNonRecoverable	SystemBoard					
5	Temperature	INLET-TMP	Ok	SystemBoard	28.0 DegreesC	0	0	0	67
6	Temperature	OUTLET-TMP	Ok	SystemBoard	29.0 DegreesC	0	0	0	77
7	Temperature	CPU0-TMP	Ok	SystemBoard	31.0 DegreesC	0	0	0	85
9	Voltage	+5V	Ok	SystemBoard	4.95 Volts	0	4	4.5	6
10	Voltage	+12V	Ok	SystemBoard	12.0 Volts	0	10.4	10.8	13
11	Voltage	CPU0_VCORE	Ok	Processor	1.05 Volts	0	0	0.25	2

- **[OTA] Deprecated, Replaced by App Store**

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.

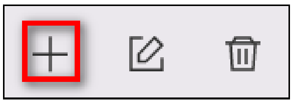
- Storage

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 NAME	TYPE	SECURITY
wiseagent-upgrade	AZURE	SSL
edgesense4	FTP	NONE
selsniumtest	AZURE	SSL
Amazon S3	S3	SSL

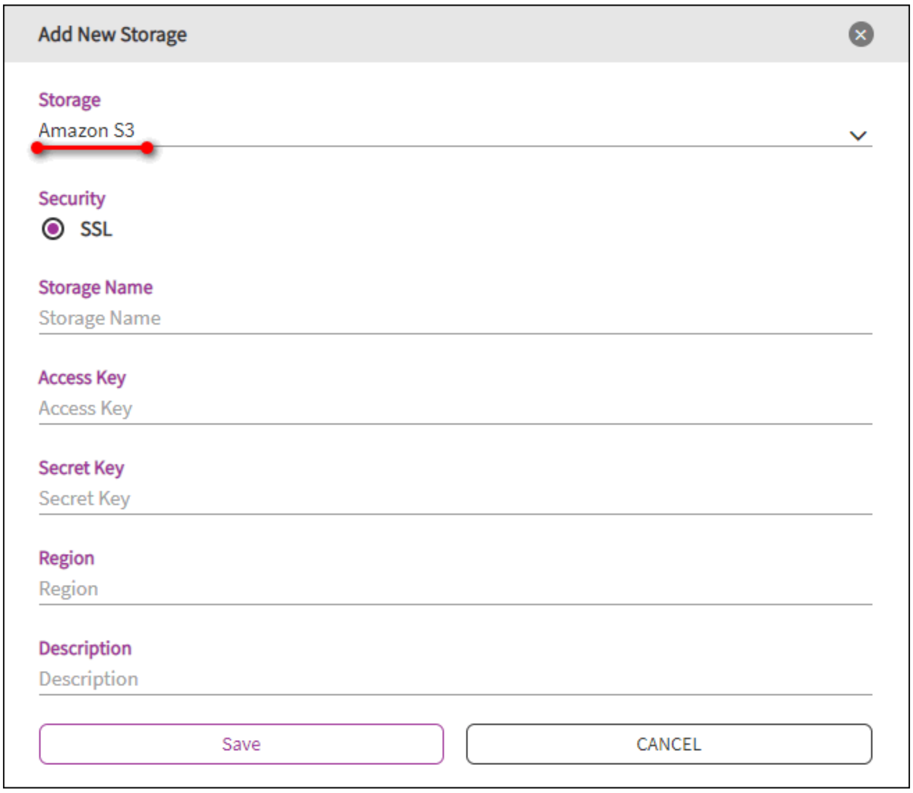
Click on add icon to add new storage.



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: Storage Name

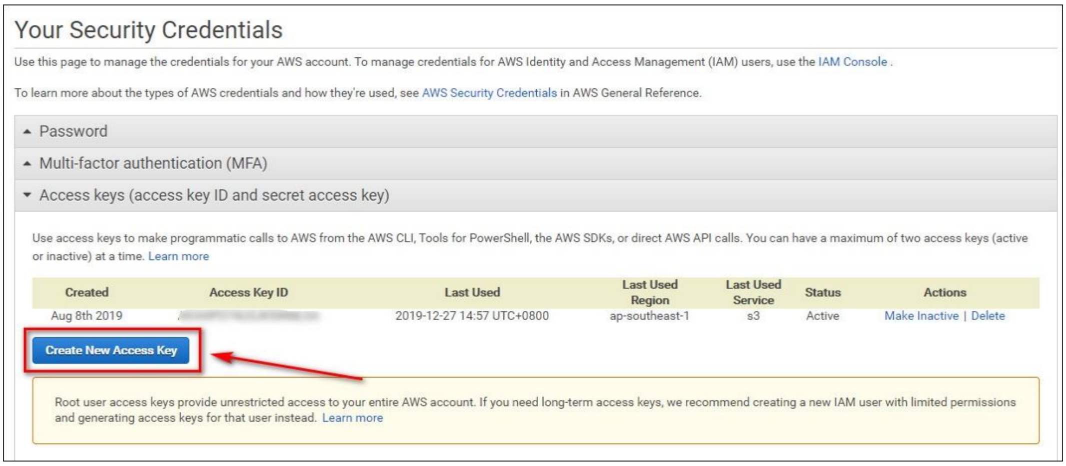
Access Key: Access Key

Secret Key: Secret Key

Region: Region

Description: Description

- ✧ 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 .

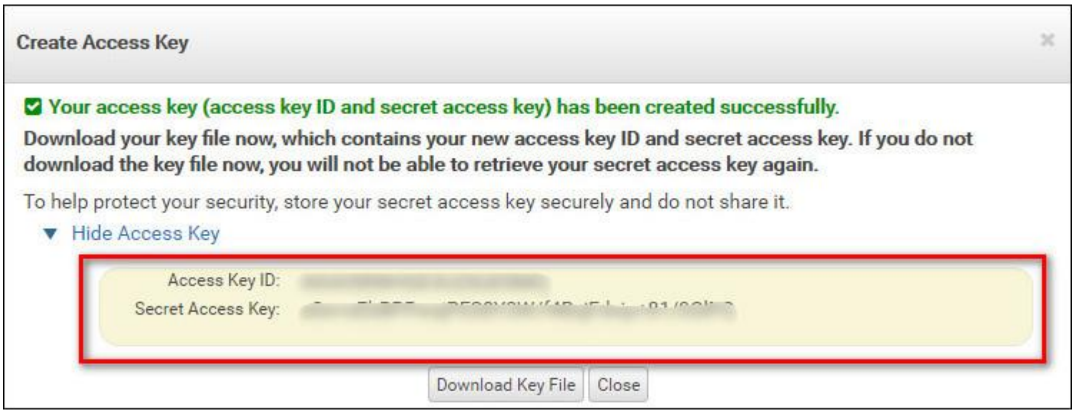
To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

▴ 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

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.

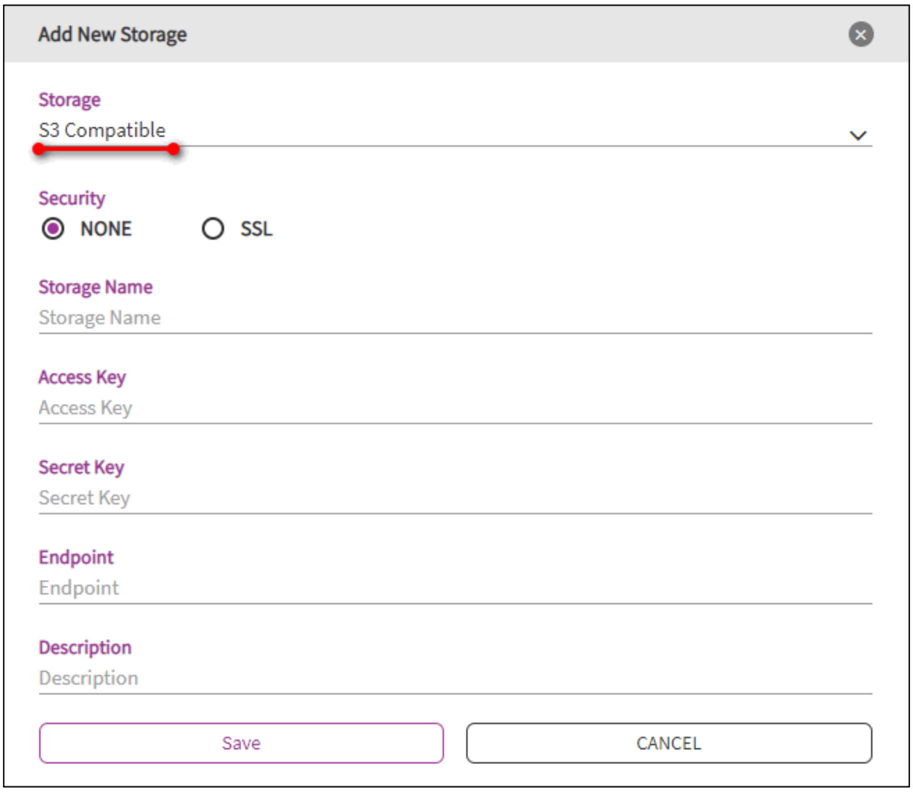
To help protect your security, store your secret access key securely and do not share it.

▼ Hide Access Key

Access Key ID: [redacted]
Secret Access Key: [redacted]

[**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: Storage Name

Access Key: Access Key

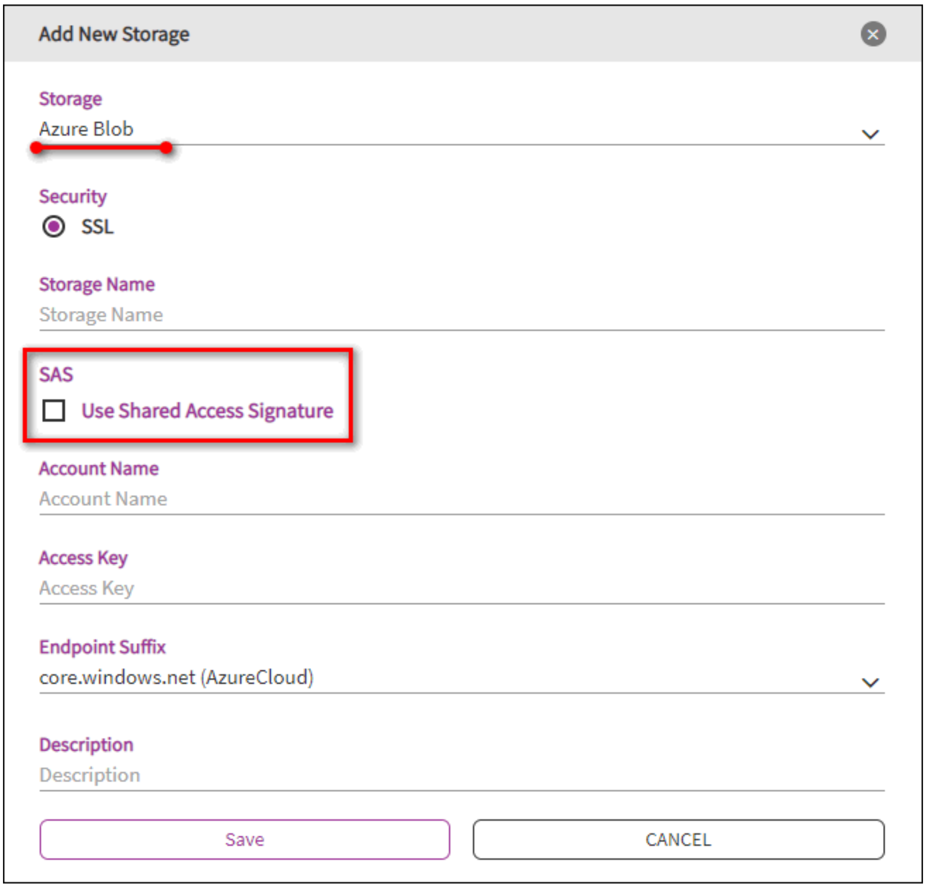
Secret Key: Secret Key

Endpoint: Endpoint

Description: 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
Storage Name

SAS
□ Use Shared Access Signature

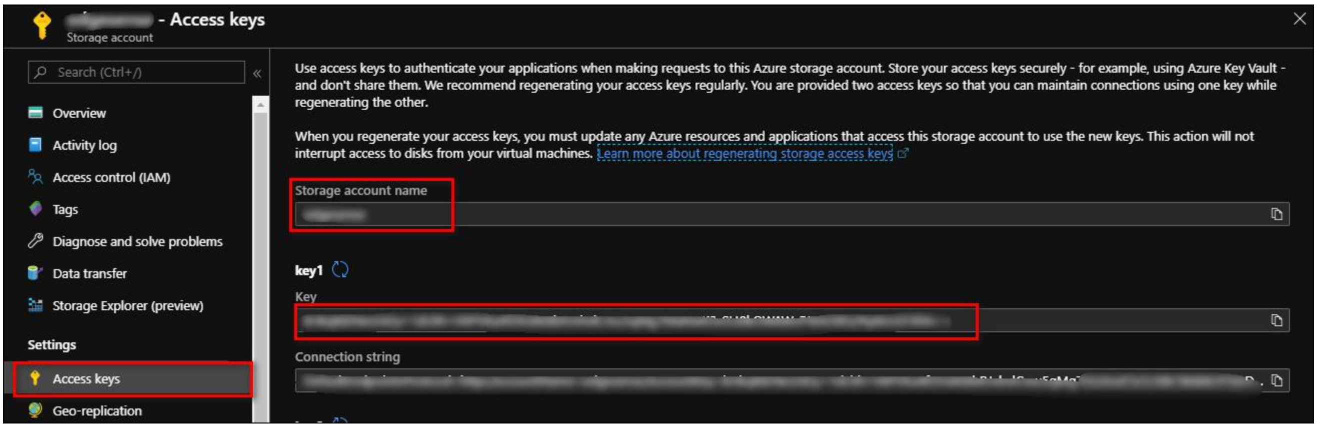
Account Name
Account Name

Access Key
Access Key

Endpoint Suffix
core.windows.net (AzureCloud)

Description
Description

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



[redacted] - Access keys
Storage account

Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. Learn more about regenerating storage access keys

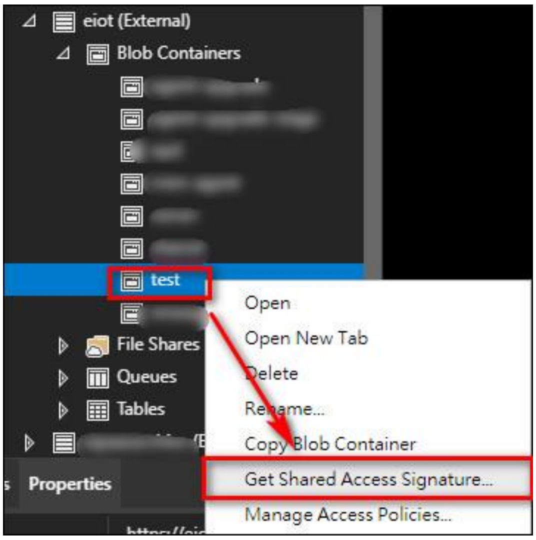
Storage account name
[redacted]

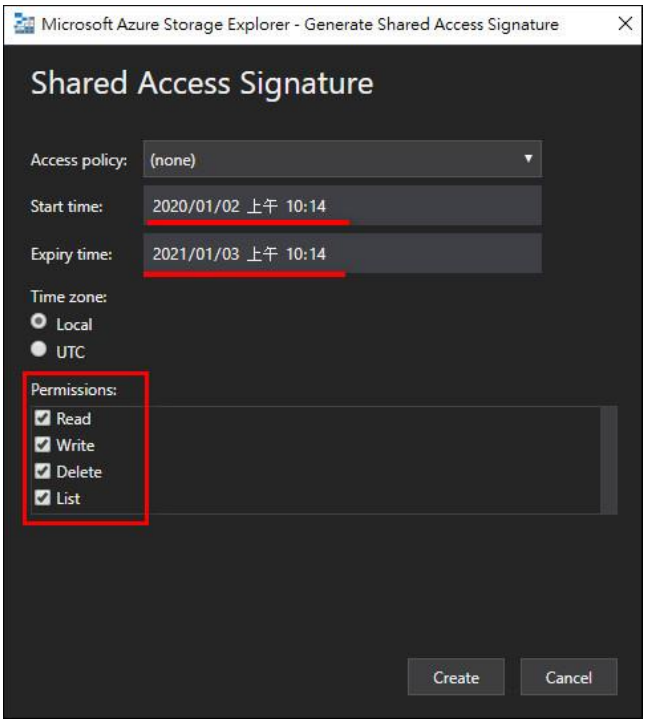
key1

Key
[redacted]

Connection string
[redacted]

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





Microsoft Azure Storage Explorer - Generate Shared Access Signature

Shared Access Signature

Access policy: (none)

Start time: 2020/01/02 上午 10:14

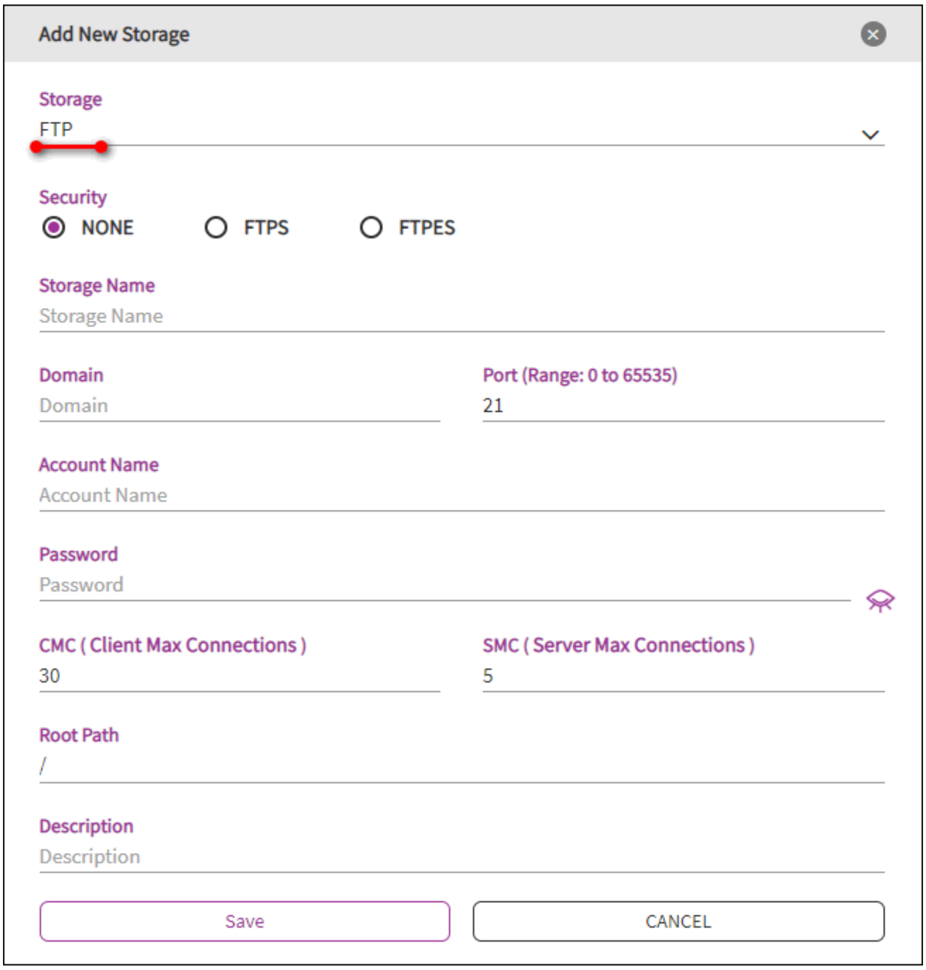
Expiry time: 2021/01/03 上午 10:14

Time zone:
● Local
○ UTC

Permissions:
☑ Read
☑ Write
☑ Delete
☑ List

[**FTP**]

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



Add New Storage

Storage: FTP

Security: ● NONE ○ FTPS ○ FTPES

Storage Name: Storage Name

Domain: Domain

Port (Range: 0 to 65535): 21

Account Name: Account Name

Password: Password

CMC (Client Max Connections): 30

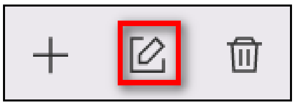
SMC (Server Max Connections): 5

Root Path: /

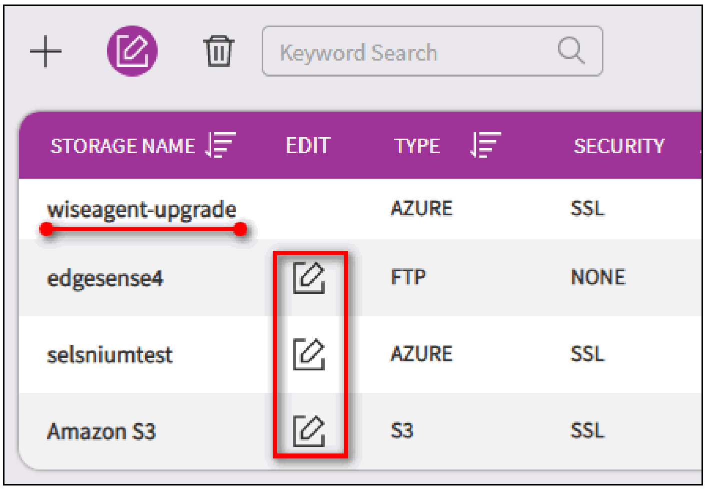
Description: Description

- ✧ **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.

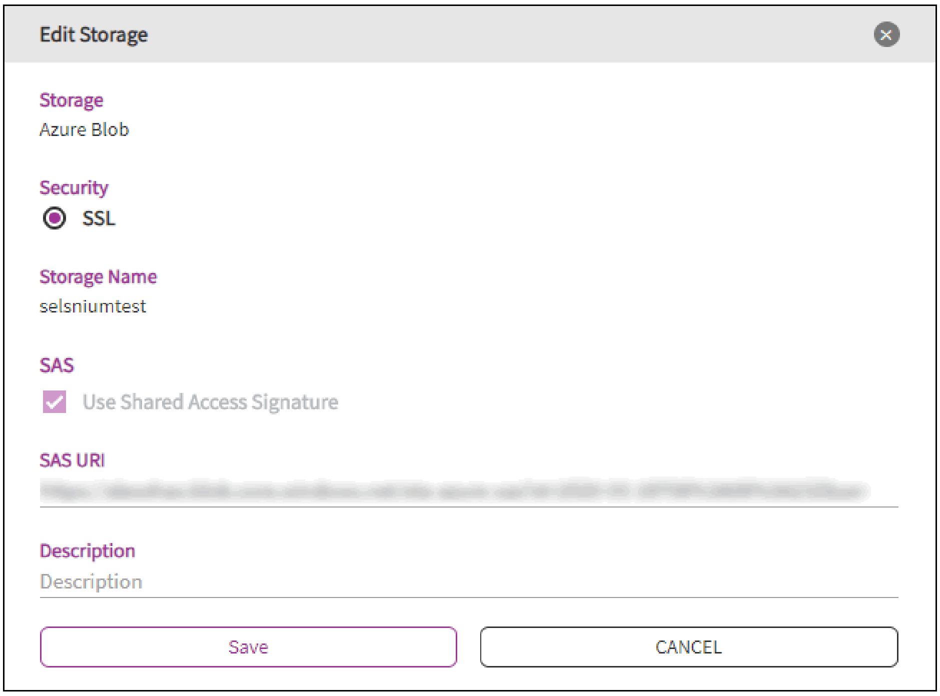
Click on edit icon to adjust a storage.



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



STORAGE NAME	EDIT	TYPE	SECURITY
wiseagent-upgrade		AZURE	SSL
edgesense4	✎	FTP	NONE
selsniumtest	✎	AZURE	SSL
Amazon S3	✎	S3	SSL



Edit Storage

Storage
Azure Blob

Security
● SSL

Storage Name
selsniumtest

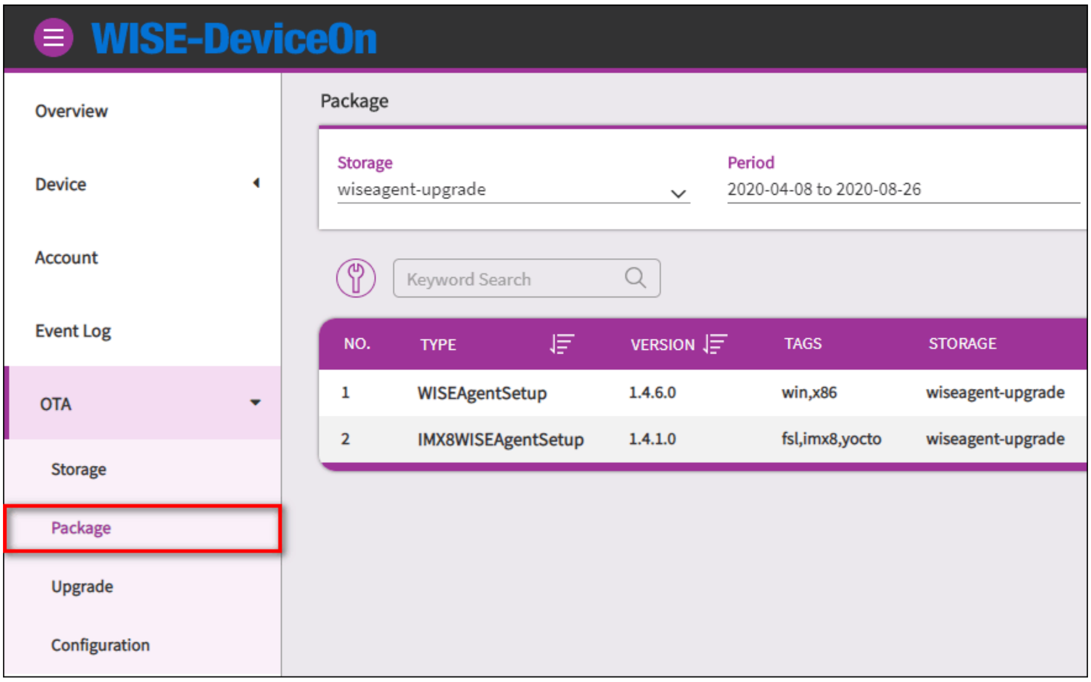
SAS
☑ Use Shared Access Signature

SAS URI

Description
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.



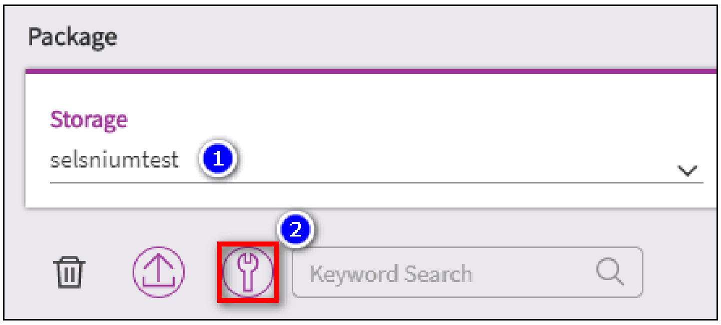
Package

Storage
wiseagent-upgrade

Period
2020-04-08 to 2020-08-26

NO.	TYPE	VERSION	TAGS	STORAGE
1	WISEAgentSetup	1.4.6.0	win,x86	wiseagent-upgrade
2	IMX8WISEAgentSetup	1.4.1.0	fsl,imx8,yocto	wiseagent-upgrade

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

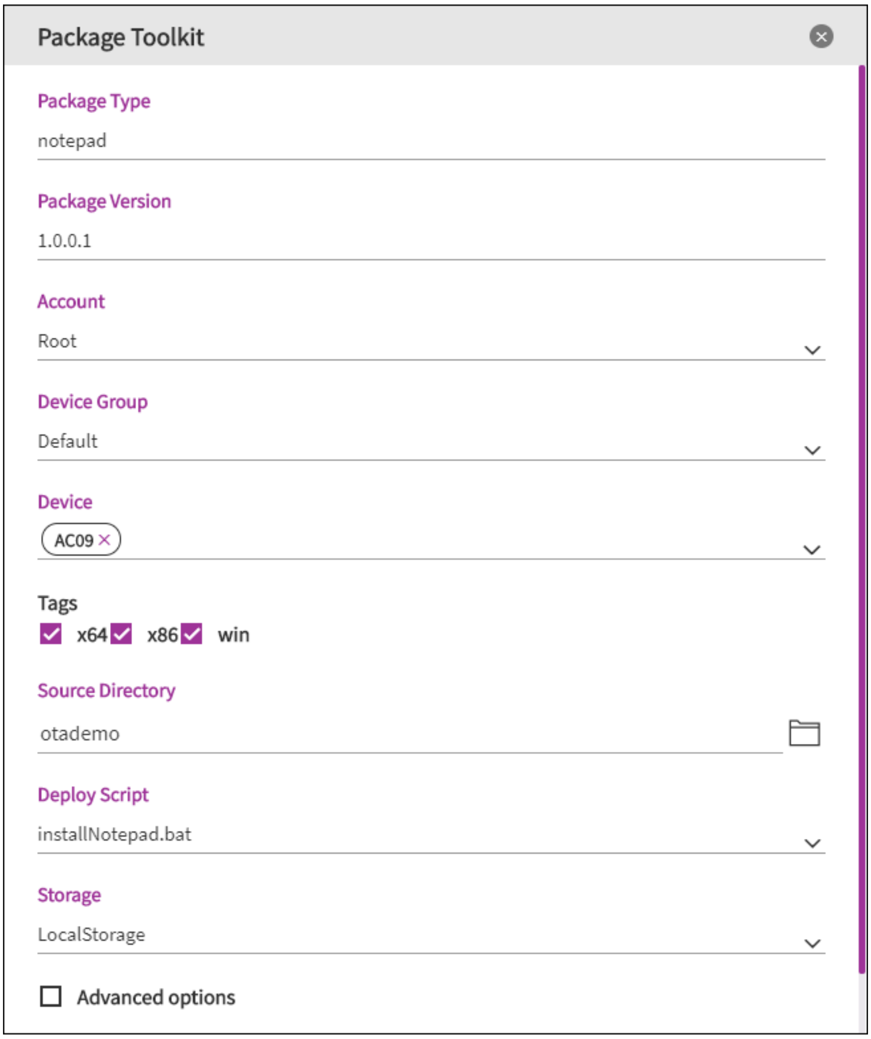


Prepare your software, configuration and installation script first, gives below information. The operation system and architecture might be different. Therefore, to determine the OTA package be deployed on which devices, please pick-up the “**Tag Name**” on “**Supported Arch**”. All “**Tags**” must match 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
Default

Device
AC09 ×

Tags
☑ x64 ☑ x86 ☑ win

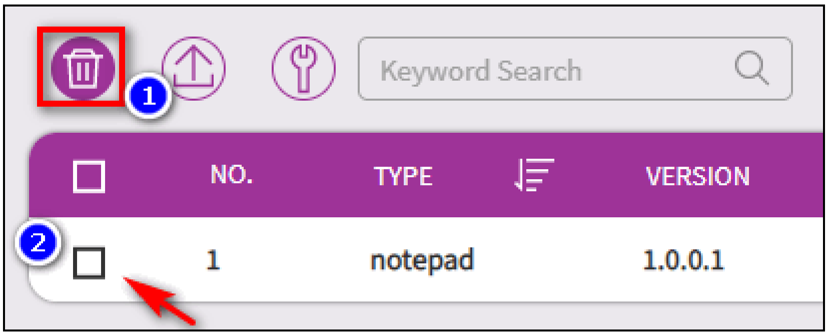
Source Directory
otademo

Deploy Script
installNotepad.bat

Storage
LocalStorage

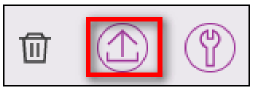
□ Advanced options

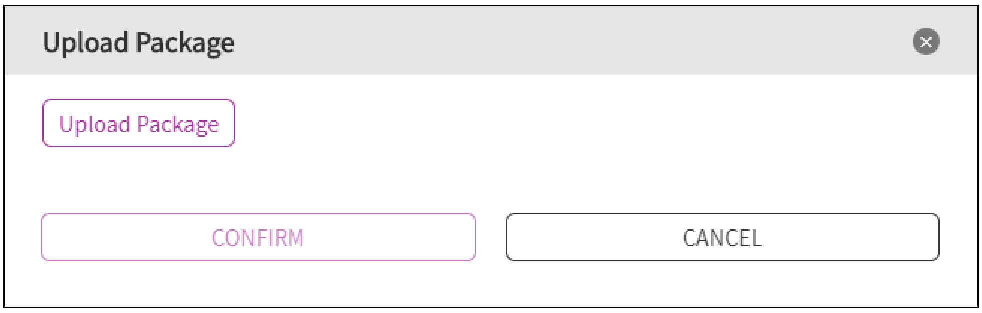
Click on the delete icon to delete your OTA package.



□	NO.	TYPE	VERSION
□	1	notepad	1.0.0.1

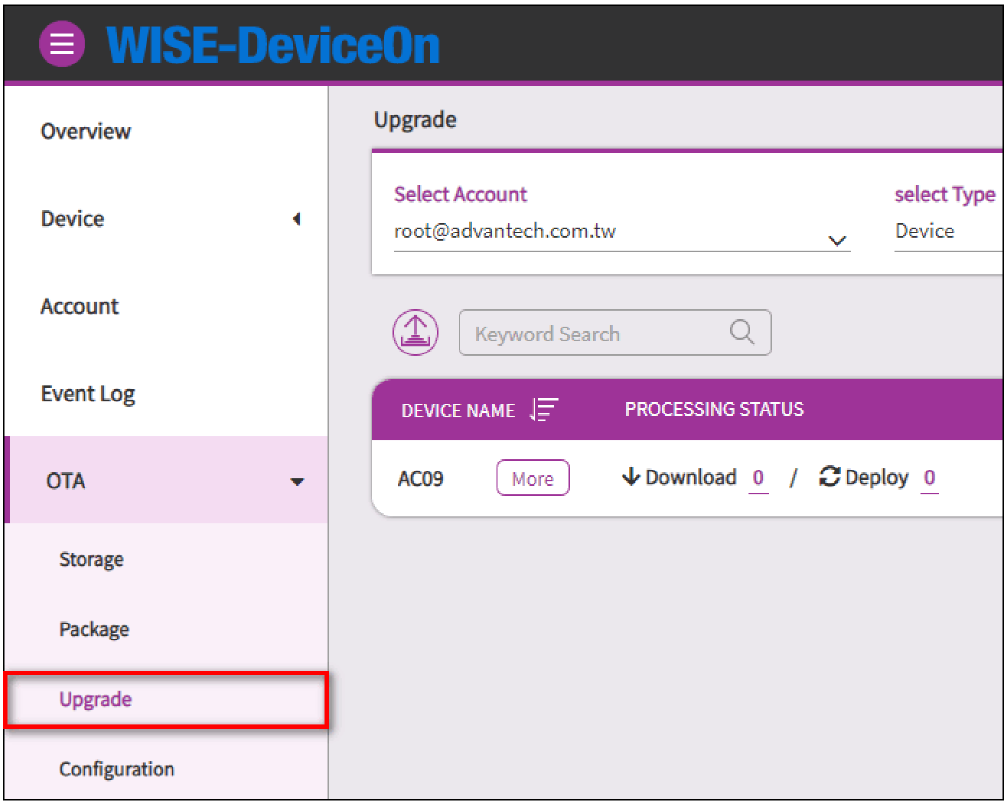
Click on the upload icon to upload your OTA package.



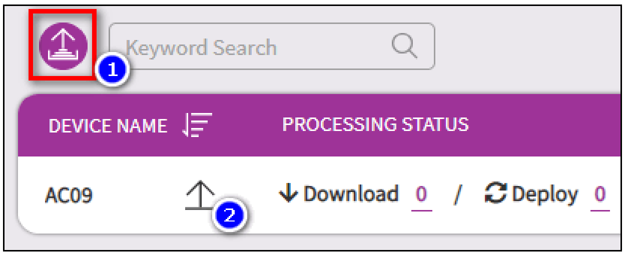


- Upgrade

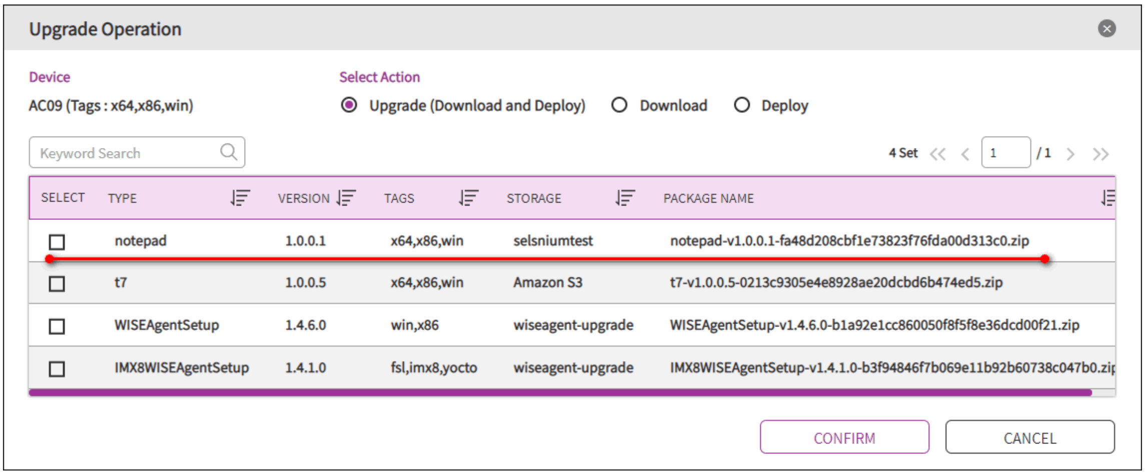
On the upgrade tab, start to select your device or device group and pick-up your OTA package that you upload before. On the device list to configure schedule, check the result status and program list that installed.



Click on upgrade icon to select OTA package.



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
AC09 (Tags : x64,x86,win)

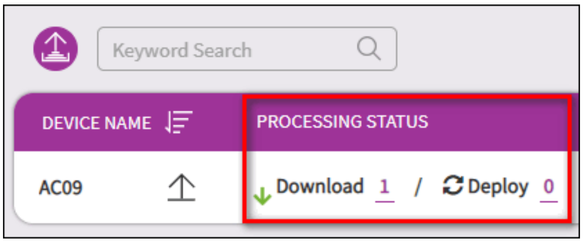
Select Action
● Upgrade (Download and Deploy) ○ Download ○ Deploy

Keyword Search

4 Set << < 1 /1 > >>

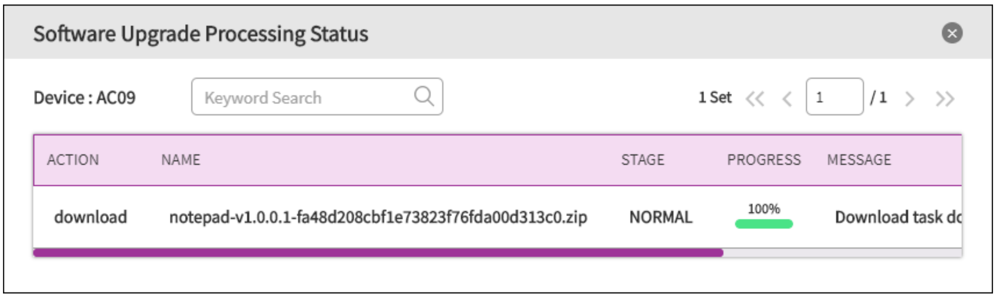
SELECT	TYPE	VERSION	TAGS	STORAGE	PACKAGE NAME
□	notepad	1.0.0.1	x64,x86,win	selsniumtest	notepad-v1.0.0.1-fa48d208cbf1e73823f76fda00d313c0.zip
□	t7	1.0.0.5	x64,x86,win	Amazon S3	t7-v1.0.0.5-0213c9305e4e8928ae20dcbd6b474ed5.zip
□	WISEAgentSetup	1.4.6.0	win,x86	wiseagent-upgrade	WISEAgentSetup-v1.4.6.0-b1a92e1cc860050f8f5f8e36dcd00f21.zip
□	IMX8WISEAgentSetup	1.4.1.0	fsl,imx8,yocto	wiseagent-upgrade	IMX8WISEAgentSetup-v1.4.1.0-b3f94846f7b069e11b92b60738c047b0.zip

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



Keyword Search

DEVICE NAME		PROCESSING STATUS
AC09		Download 1 / Deploy 0



Software Upgrade Processing Status

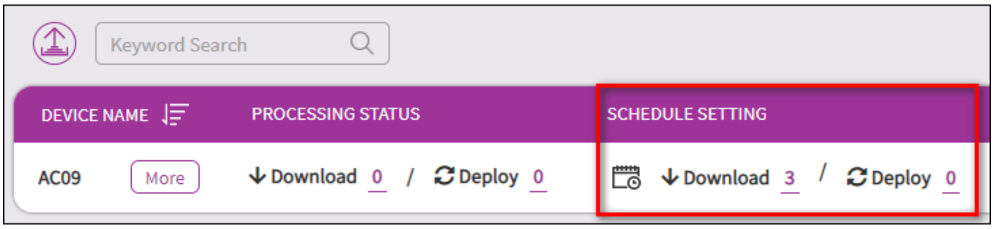
Device : AC09

Keyword Search

1 Set << < 1 /1 > >>

ACTION	NAME	STAGE	PROGRESS	MESSAGE
download	notepad-v1.0.0.1-fa48d208cbf1e73823f76fda00d313c0.zip	NORMAL	100%	Download task dc

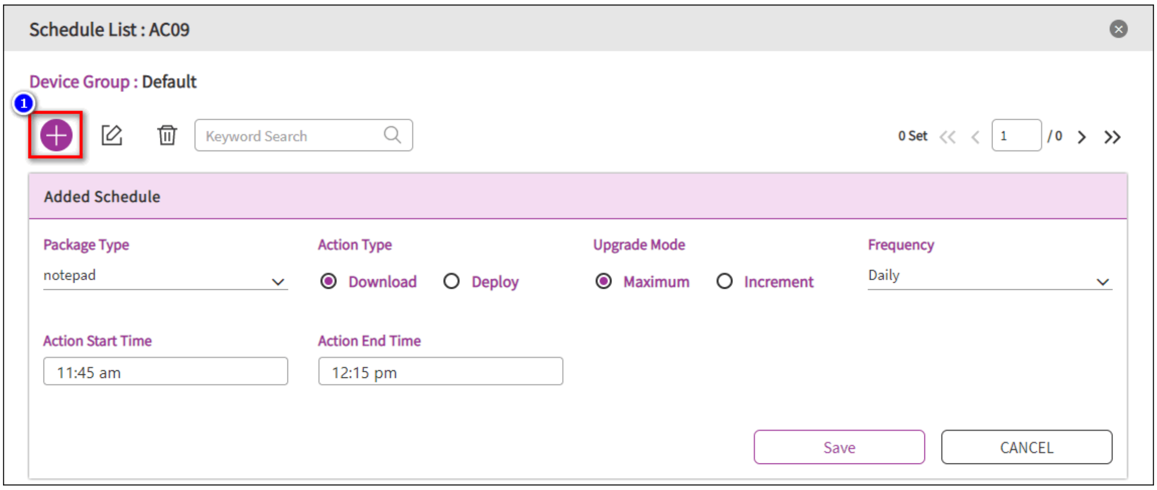
To avoid burst download on large number of devices upgrade at the same time, user could add schedule to check and upgrade by schedule.



Keyword Search

DEVICE NAME		PROCESSING STATUS	SCHEDULE SETTING
AC09	More	Download 0 / Deploy 0	Download 3 / Deploy 0

Click on add icon to create a schedule.



Schedule List : AC09

Device Group : Default

0 Set 1 / 0

Added Schedule

Package Type: notepad

Action Type: ● Download ○ Deploy

Upgrade Mode: ● Maximum ○ Increment

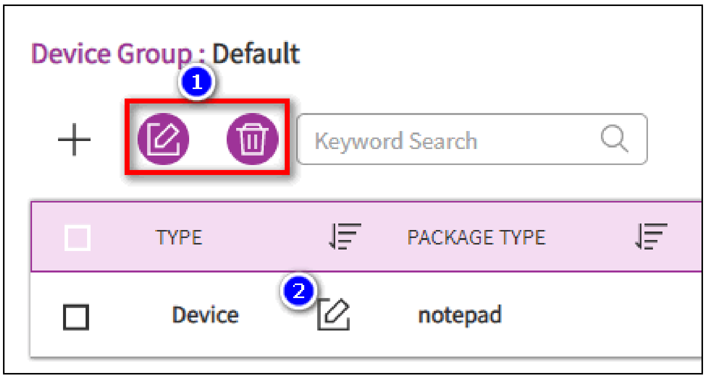
Frequency: Daily

Action Start Time: 11:45 am

Action End Time: 12:15 pm

- ✧ 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.

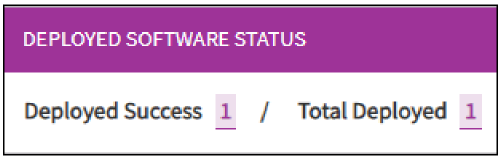
Click on edit icon to modify, delete OTA schedule.



Device Group : Default

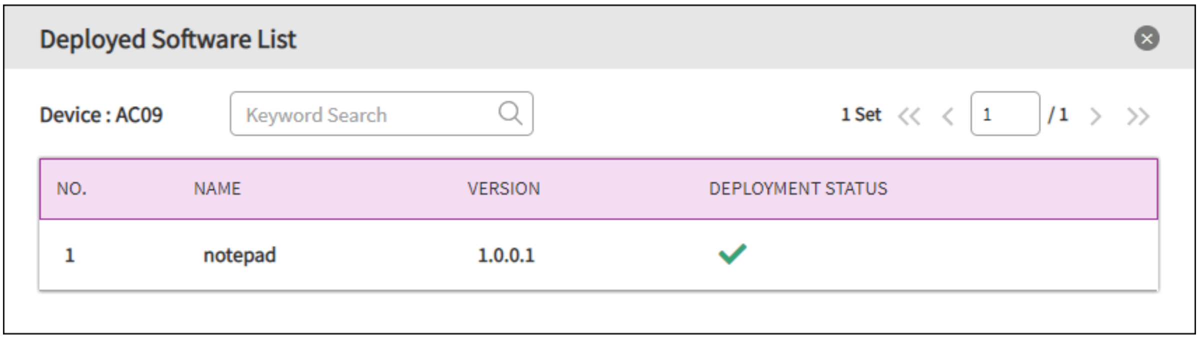
□	TYPE	PACKAGE TYPE
□	Device	notepad

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



DEPLOYED SOFTWARE STATUS

Deployed Success 1 / Total Deployed 1

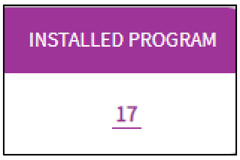


Deployed Software List

Device : AC09

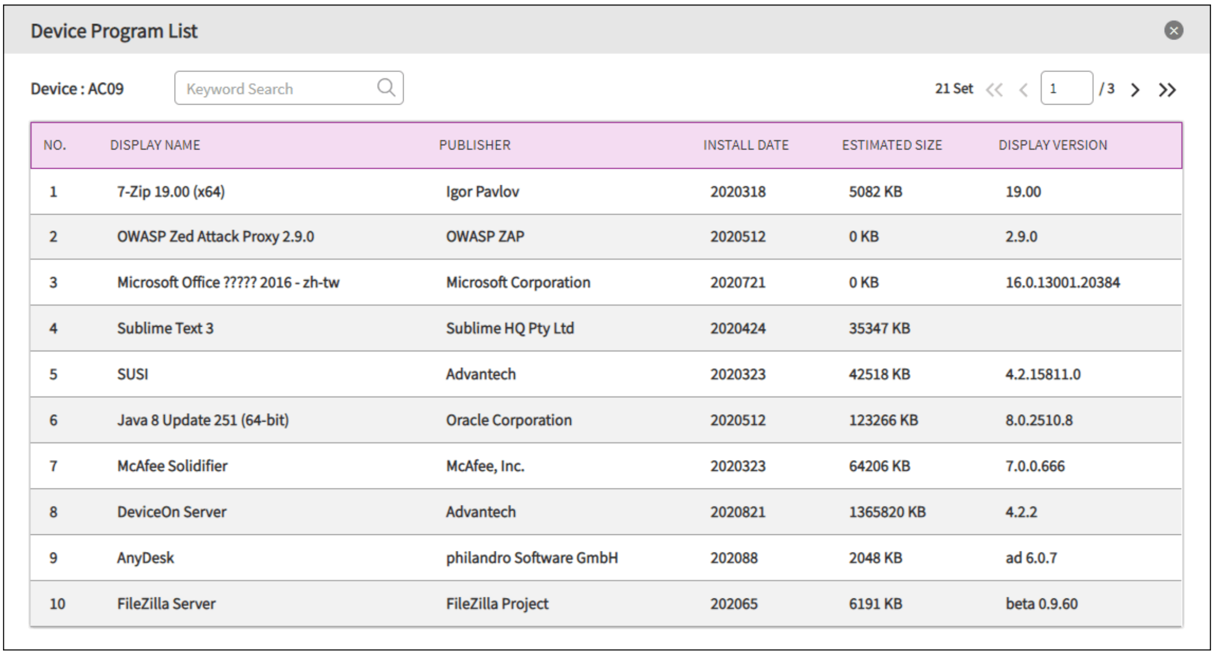
NO.	NAME	VERSION	DEPLOYMENT STATUS
1	notepad	1.0.0.1	✓

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



INSTALLED PROGRAM

17

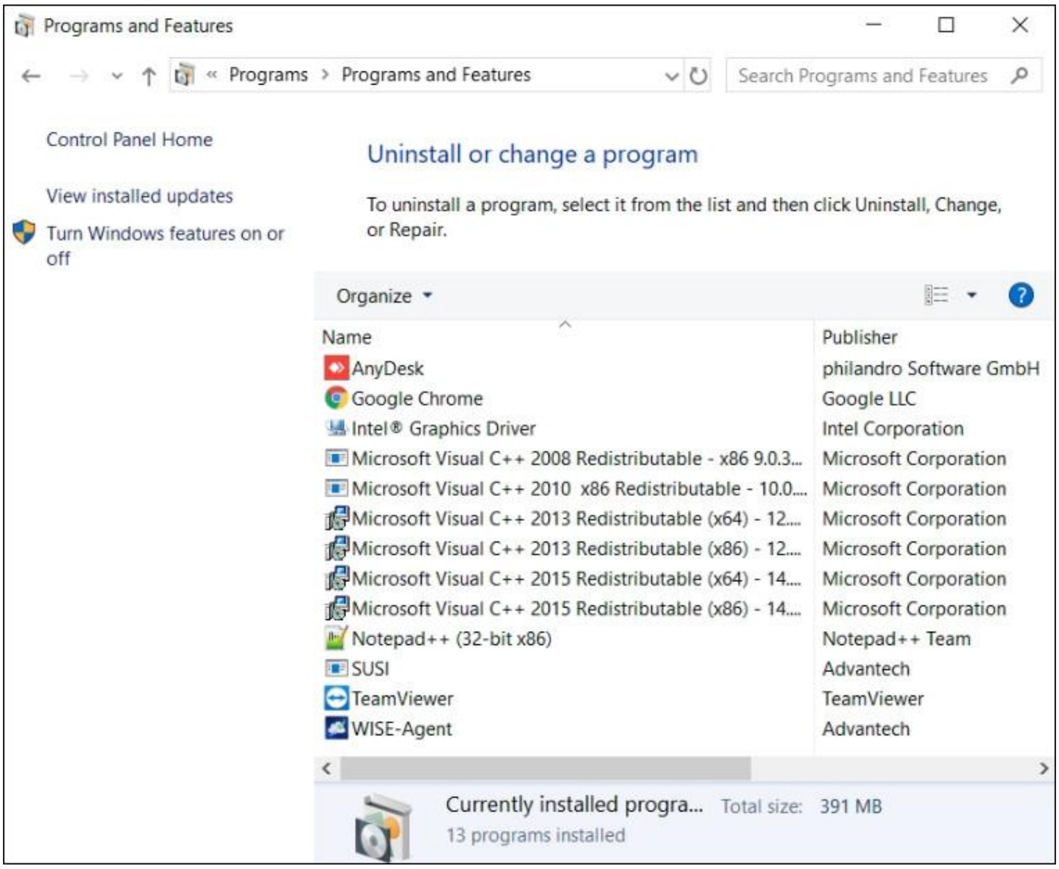


Device Program List

Device : AC09

NO.	DISPLAY NAME	PUBLISHER	INSTALL DATE	ESTIMATED SIZE	DISPLAY VERSION
1	7-Zip 19.00 (x64)	Igor Pavlov	2020318	5082 KB	19.00
2	OWASP Zed Attack Proxy 2.9.0	OWASP ZAP	2020512	0 KB	2.9.0
3	Microsoft Office ????? 2016 - zh-tw	Microsoft Corporation	2020721	0 KB	16.0.13001.20384
4	Sublime Text 3	Sublime HQ Pty Ltd	2020424	35347 KB	
5	SUSI	Advantech	2020323	42518 KB	4.2.15811.0
6	Java 8 Update 251 (64-bit)	Oracle Corporation	2020512	123266 KB	8.0.2510.8
7	McAfee Solidifier	McAfee, Inc.	2020323	64206 KB	7.0.0.666
8	DeviceOn Server	Advantech	2020821	1365820 KB	4.2.2
9	AnyDesk	philandro Software GmbH	202088	2048 KB	ad 6.0.7
10	FileZilla Server	FileZilla Project	202065	6191 KB	beta 0.9.60

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



Programs and Features
« Programs › Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾

Uninstall or change a program

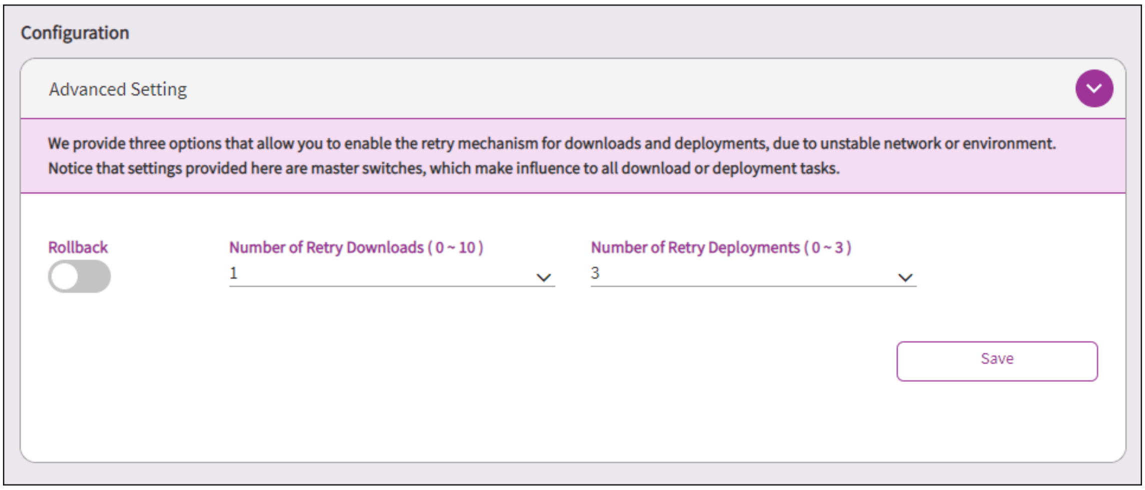
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher
AnyDesk	philandro Software GmbH
Google Chrome	Google LLC
Intel® Graphics Driver	Intel Corporation
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...	Microsoft Corporation
Microsoft Visual C++ 2010 x86 Redistributable - 10.0....	Microsoft Corporation
Microsoft Visual C++ 2013 Redistributable (x64) - 12....	Microsoft Corporation
Microsoft Visual C++ 2013 Redistributable (x86) - 12....	Microsoft Corporation
Microsoft Visual C++ 2015 Redistributable (x64) - 14....	Microsoft Corporation
Microsoft Visual C++ 2015 Redistributable (x86) - 14....	Microsoft Corporation
Notepad++ (32-bit x86)	Notepad++ Team
SUSI	Advantech
TeamViewer	TeamViewer
WISE-Agent	Advantech

Currently installed progra... Total size: 391 MB
13 programs installed

- Configuration

There are three options for OTA to deploy your package, one is “**Rollback**” that means if a new version deploys failed, and the WISE-Agent would try the best to rollback to previous version that successfully. But there is a perquisite, 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 successfully deployment as possible.



We provide three options that allow you to enable the retry mechanism for downloads and deployments, due to unstable network or environment. Notice that settings provided here are master switches, which make influence to all download or deployment tasks.

Rollback: off

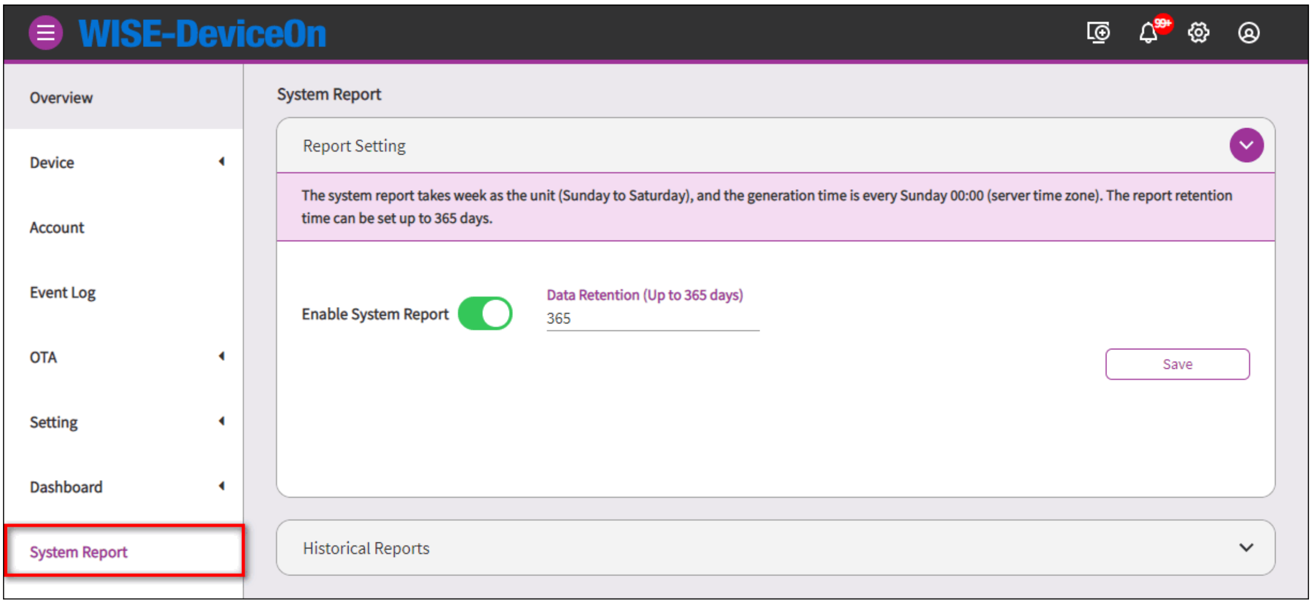
Number of Retry Downloads (0 ~ 10): 1

Number of Retry Deployments (0 ~ 3): 3

[System Report]

Second, if the System Report be enabled will appears to the menu item. The system report takes week as the unit (Sunday to Saturday), and the generation time is every Sunday 00:00 (server time zone).

The report retention time can be set up to 365 days.

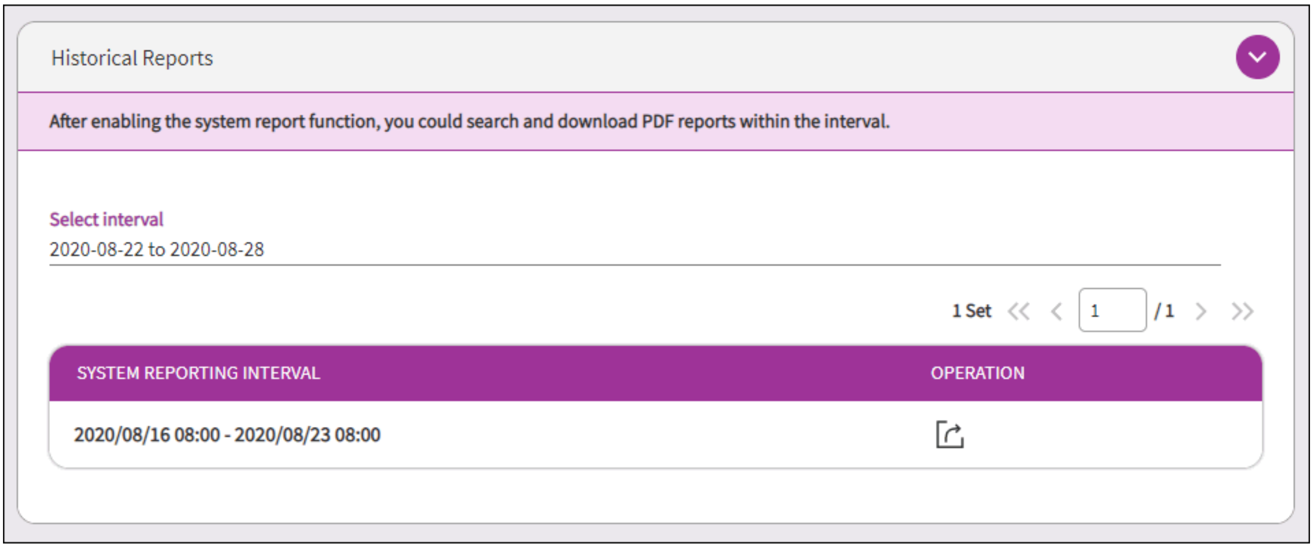


The system report takes week as the unit (Sunday to Saturday), and the generation time is every Sunday 00:00 (server time zone). The report retention time can be set up to 365 days.

Enable System Report

Data Retention (Up to 365 days)
365

After enabling the system report function, you could search and download PDF reports within the interval.



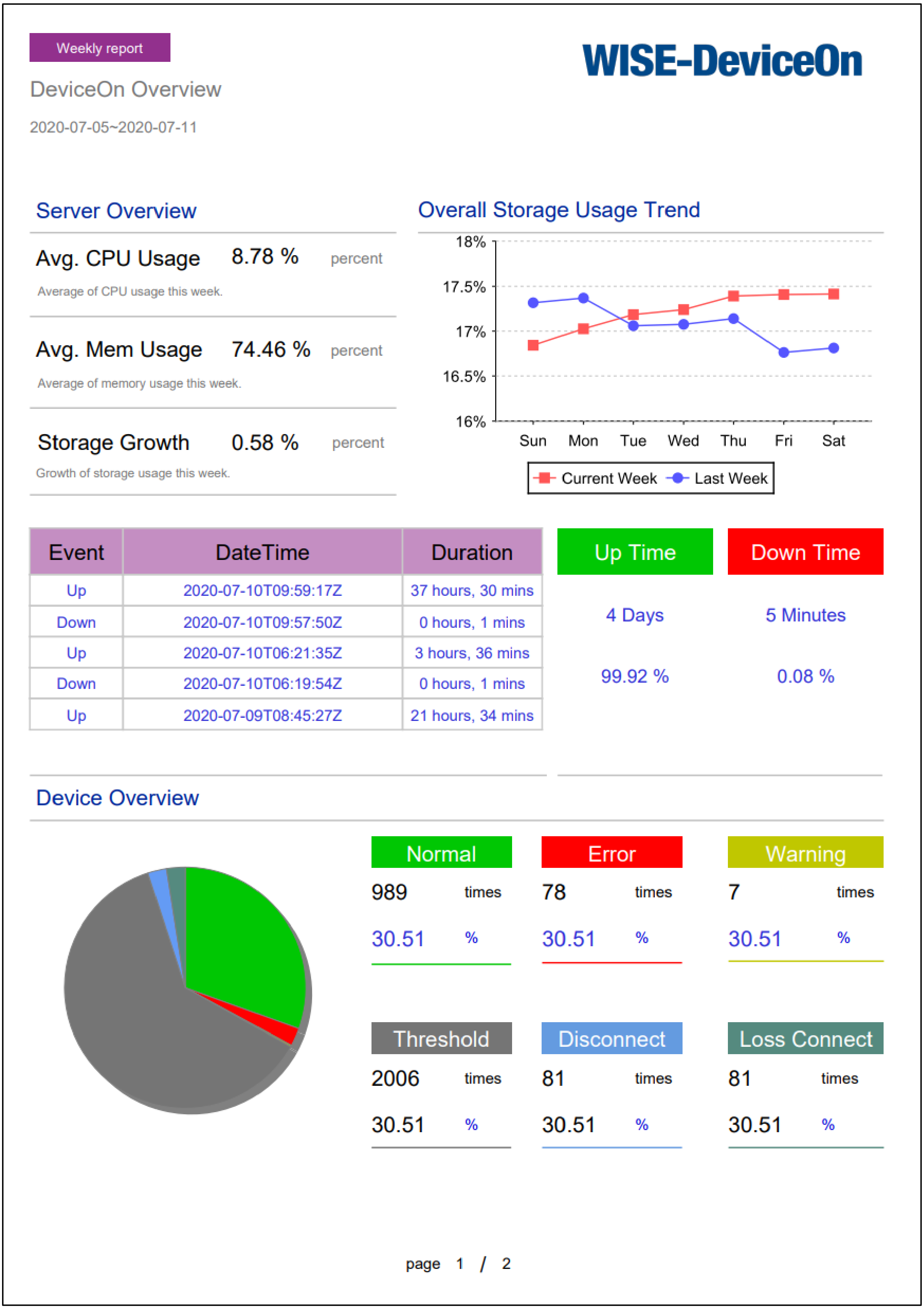
After enabling the system report function, you could search and download PDF reports within the interval.

Select interval
2020-08-22 to 2020-08-28

1 Set << < 1 /1 > >>

SYSTEM REPORTING INTERVAL	OPERATION
2020/08/16 08:00 - 2020/08/23 08:00	

From the system report, you may realize the whole status, including server uptime, downtime and managed devices healthy for the pass week.



Weekly report

WISE-DeviceOn

DeviceOn Overview

2020-07-05~2020-07-11

Server Overview

Avg. CPU Usage	8.78 %	percent
Average of CPU usage this week.		
Avg. Mem Usage	74.46 %	percent
Average of memory usage this week.		
Storage Growth	0.58 %	percent
Growth of storage usage this week.		

Overall Storage Usage Trend

Event	DateTime	Duration
Up	2020-07-10T09:59:17Z	37 hours, 30 mins
Down	2020-07-10T09:57:50Z	0 hours, 1 mins
Up	2020-07-10T06:21:35Z	3 hours, 36 mins
Down	2020-07-10T06:19:54Z	0 hours, 1 mins
Up	2020-07-09T08:45:27Z	21 hours, 34 mins

Up Time	Down Time
4 Days	5 Minutes
99.92 %	0.08 %

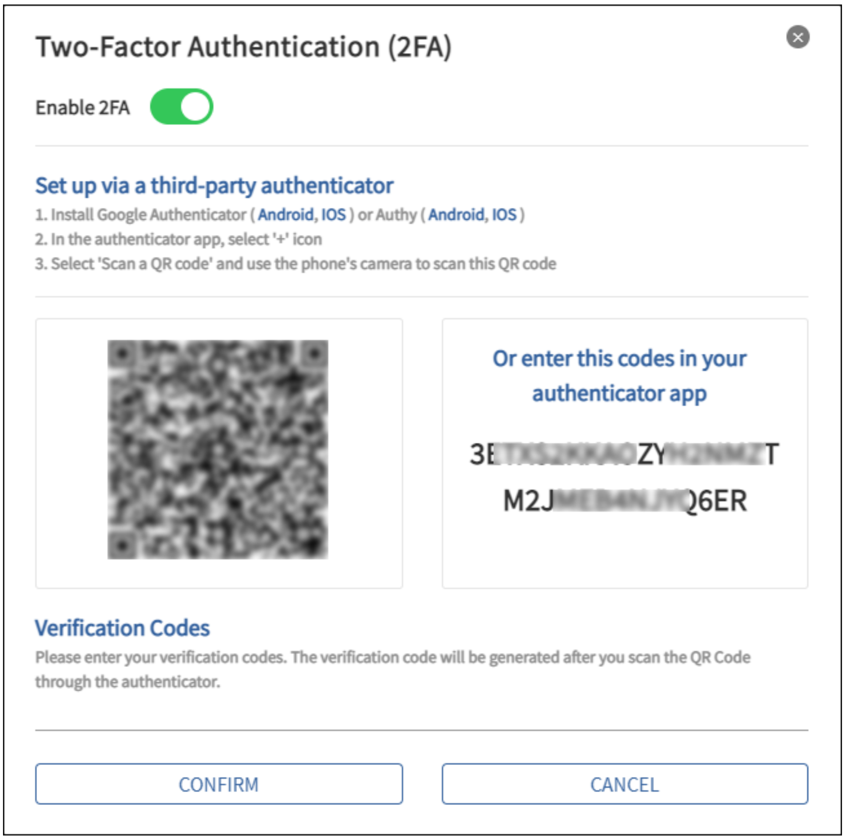
Device Overview

Normal		Error		Warning	
989	times	78	times	7	times
30.51	%	30.51	%	30.51	%

Threshold		Disconnect		Loss Connect	
2006	times	81	times	81	times
30.51	%	30.51	%	30.51	%

page 1 / 2

- **System Theme**: Select the theme style of the system
- **System Logo**: Product logo customized, supported formats: GIF, PNG, JPEG/JPG. We recommend the image with a height is less than 55 pixels.
- **System Login Page**: Login page customized, supported formats: PNG, JPEG/JPG. We recommend the image with a resolution is less than 860x840 pixels.
- **Overview Setting**: To show/hide the functions on the overview
- **Language Setting**: Set display language, (English, Traditional Chinese and Simplified Chinese)
- **Server Time Zone**: Set the server time zone, which only affects the event log time of the notification message.
- **Account Registration**: Enable account registration, users can sign up an account in the login page, the default role is the device administrator.
- **Two-Factor Authentication**: Two-factor authentication (2FA) is an extra layer of security used when logging into websites or apps. With 2FA, you must log in with your username and password and provide another form of authentication that only you know or have access to. If you prefer to use an authenticator app for two-step verification, here are a few common authenticator apps that can be found in your mobile device app store:
  - **Google Authenticator**
  - **Microsoft Authenticator**
  - **Authy**
  - **LastPass Authenticator**



Two-Factor Authentication (2FA)

Enable 2FA

Set up via a third-party authenticator

1. Install Google Authenticator (Android, IOS) or Authy (Android, IOS)
2. In the authenticator app, select '+' icon
3. Select 'Scan a QR code' and use the phone's camera to scan this QR code

Or enter this codes in your authenticator app

3E[redacted]ZY[redacted]T
M2J[redacted]Q6ER

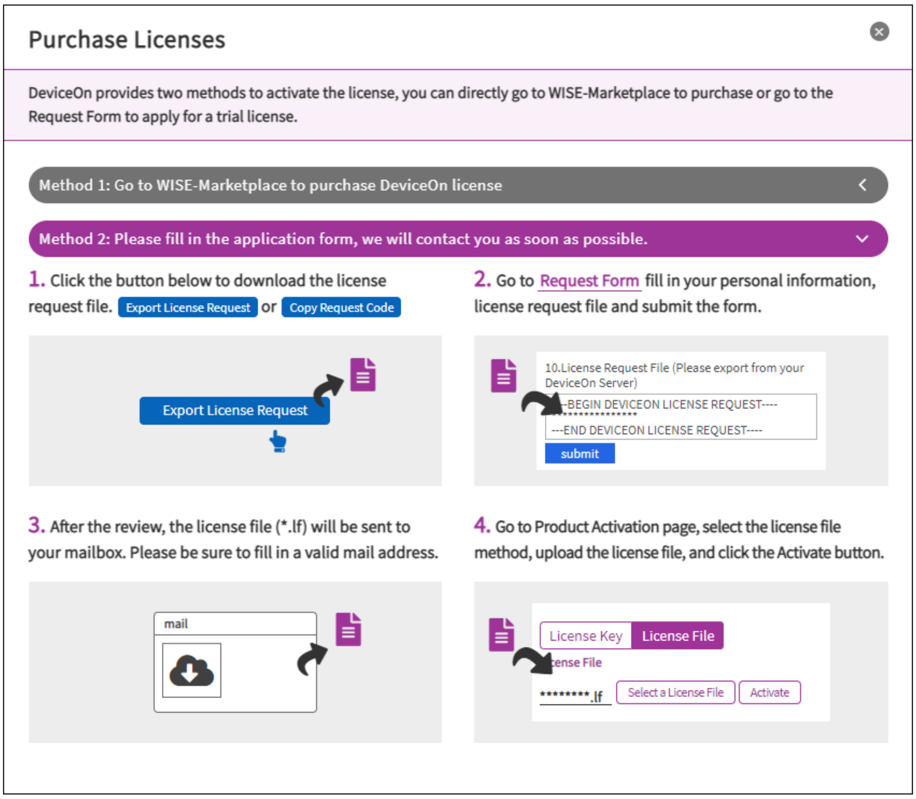
Verification Codes

Please enter your verification codes. The verification code will be generated after you scan the QR Code through the authenticator.

- ✧ **LDAP**: Configure LDAP Server Setting
- ✧ **X.509 Certificate**: DeviceOn supports x.509 certificate authentication for use with a secure **TLS/SSL** connection. The x.509 edge device authentication allows device to authenticate to servers with certificates rather than with a username and password.
- ✧ **Remote Storage (SMB/CIFS)**: Support for remote device system backup to SMB/CIFS instead of a local drive, and recovery from SMB. For instance, a user could generate a golden operation system image, then restore to hundry of device in a factory, if needed. You also can leverage Azure file to mount a SMB on your remote system to achieve cloud backup.
- ✧ **Data Export**: The data export help to dump your sensor data as **CSV** or **JSON** format and upload to your cold storage, such as **Azure Blob**, **AWS S3** and **FTP** for advance data ingestion and learning through third-party. The generation time is every Sunday.
- ✧ **Webhook**: In addition to the existing event notification via social media services (LINE, WeChat, Teams, Slack, Telegram), it also supports the integration of third-party APIs via Webhook. Such as Microsoft Dynamics 365 Field services.
- ✧ **Syslog**: Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the type of system generating the message, and is assigned a severity level. DeviceOn may use syslog for system management and security auditing as well as general informational, analysis, and debugging messages.
- ✧ **App Management** -> **Offered by**: App developer or company.
- ✧ **App Management** -> **Contact Support**: App developer and contact mail.

- Product Activation

Starting from **Version 4.5**, we have adjusted the license mechanism, DeviceOn provides two methods to activate the license, you can directly go to **WISE-Marketplace** to purchase or go to the **Request Form** to apply for a trial license. After you apply, the product team will review your request then send back the license file.



Purchase Licenses

DeviceOn provides two methods to activate the license, you can directly go to WISE-Marketplace to purchase or go to the Request Form to apply for a trial license.

Method 1: Go to WISE-Marketplace to purchase DeviceOn license

Method 2: Please fill in the application form, we will contact you as soon as possible.

1. Click the button below to download the license request file. Export License Request or Copy Request Code

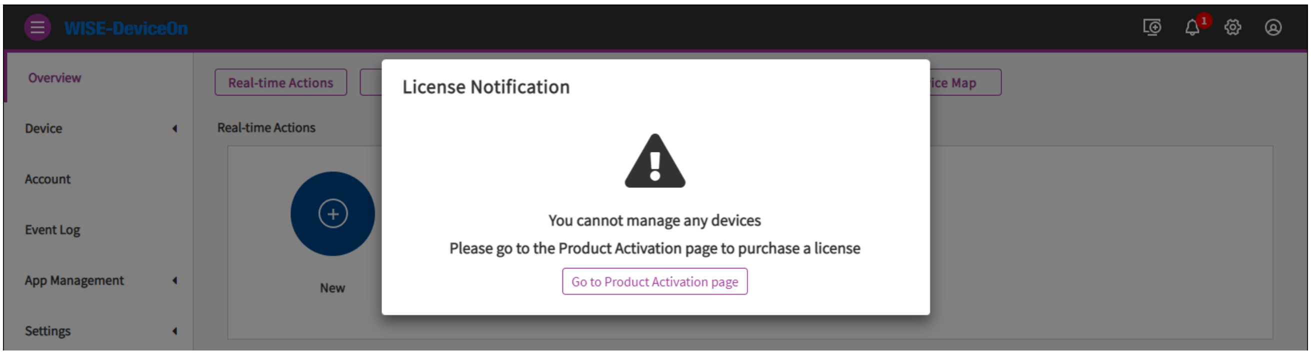
2. Go to Request Form fill in your personal information, license request file and submit the form.

3. After the review, the license file (*.lf) will be sent to your mailbox. Please be sure to fill in a valid mail address.

4. Go to Product Activation page, select the license file method, upload the license file, and click the Activate button.

Export License Request
10.License Request File (Please export from your DeviceOn Server)
----BEGIN DEVICEON LICENSE REQUEST----
----END DEVICEON LICENSE REQUEST----
submit
mail
License Key
License File
ense File
********.lf
Select a License File
Activate

When you log in for the first time, you will be prompted that you do not have any license to manage the device, please purchase or apply for a license first.

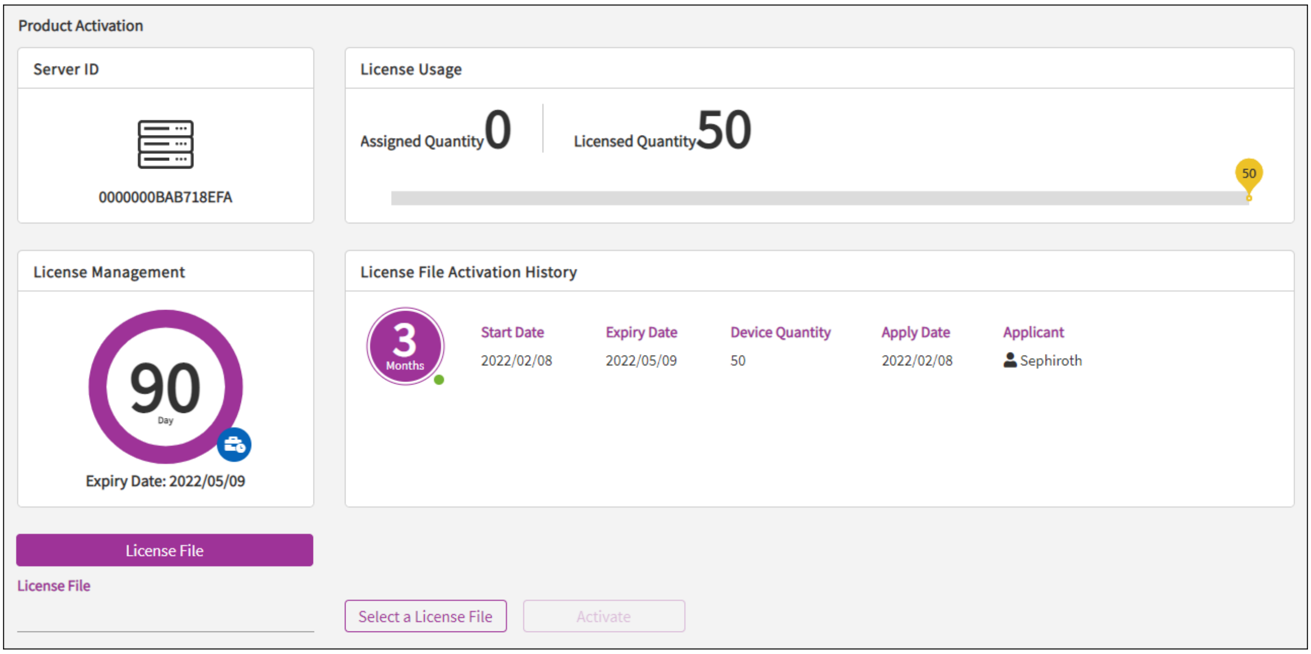


License Notification

You cannot manage any devices
Please go to the Product Activation page to purchase a license

After obtaining the License key or File, the license status and record of the server will be displayed after import. Note that the **License Key** is the old mechanism. After converting to the new mechanism (**License File**), we no longer support the old.

- New License Flow
- Purchase a License from WISE-Marketplace



Product Activation

Server ID

0000000BAB718EFA

License Usage

Assigned Quantity 0 | Licensed Quantity 50

License Management

90 Day

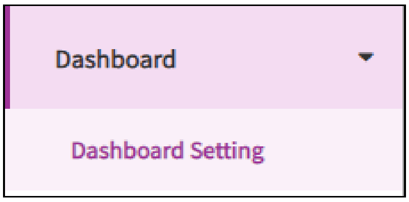
Expiry Date: 2022/05/09

License File Activation History

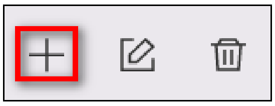
	Start Date	Expiry Date	Device Quantity	Apply Date	Applicant
3 Months	2022/02/08	2022/05/09	50	2022/02/08	Sephiroth

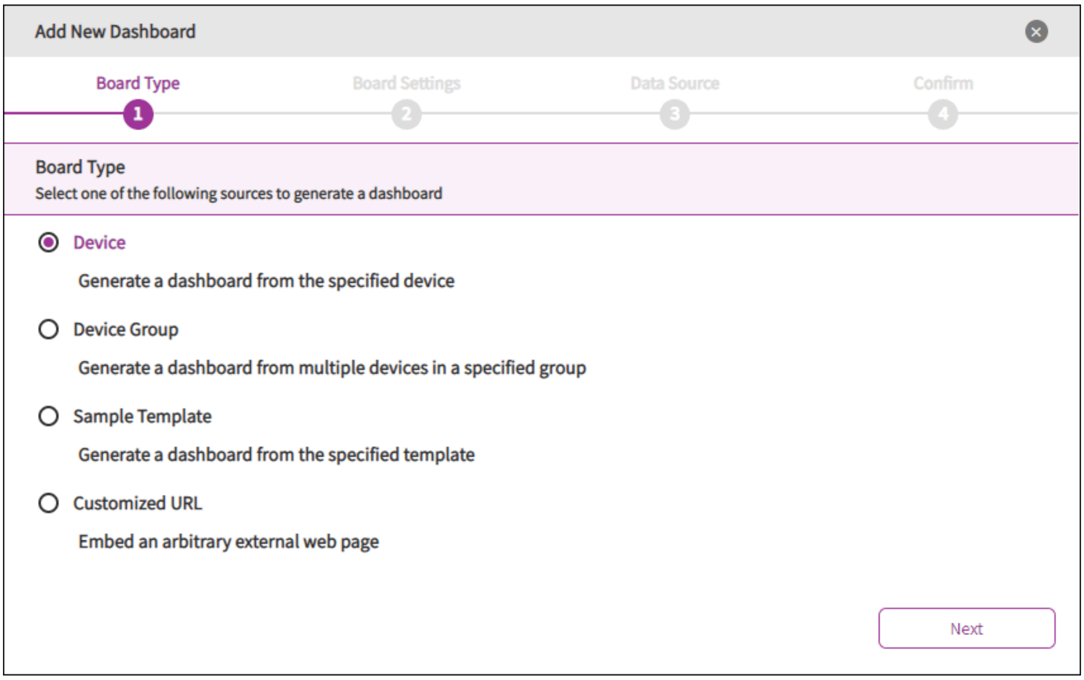
3.3.6 Dashboard

The DeviceOn not only native support and build-in Grafana for data visualize, but fully integrate and simplified procedure to 1-Click to generate a 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.



Click on the “+” icon to create dashboard item.





Add New Dashboard

Board Type
Select one of the following sources to generate a dashboard

● Device
Generate a dashboard from the specified device

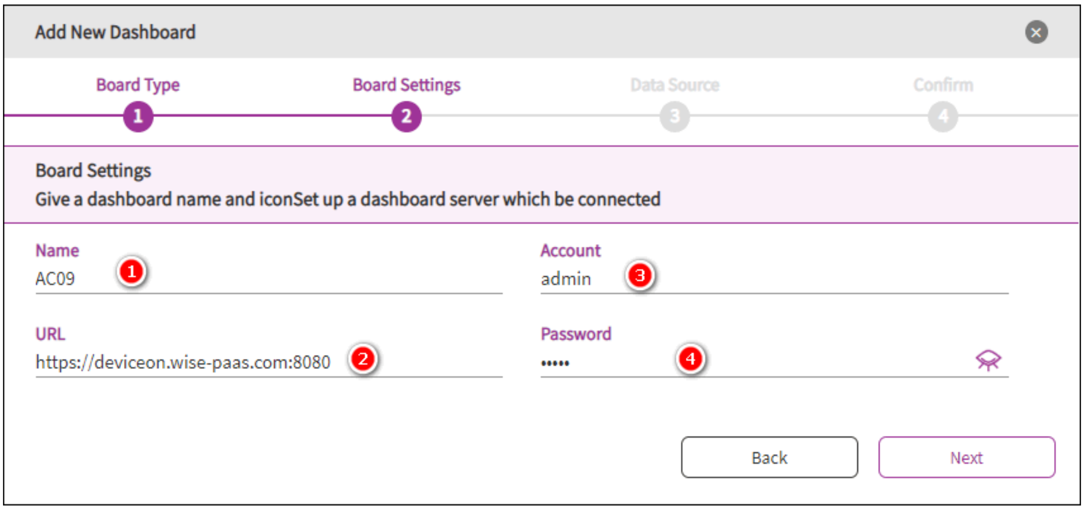
○ Device Group
Generate a dashboard from multiple devices in a specified group

○ Sample Template
Generate a dashboard from the specified template

○ Customized URL
Embed an arbitrary external web page

Here, DeviceOn support 4 types of board, select one of method to generate your dashboard. Device, device group, mode or select our default template to generate. Last, embed an arbitrary external web page.

Enter your board name, Grafana URL, account and password. (Default account and password is “**admin**”)



Add New Dashboard

Board Settings
Give a dashboard name and iconSet up a dashboard server which be connected

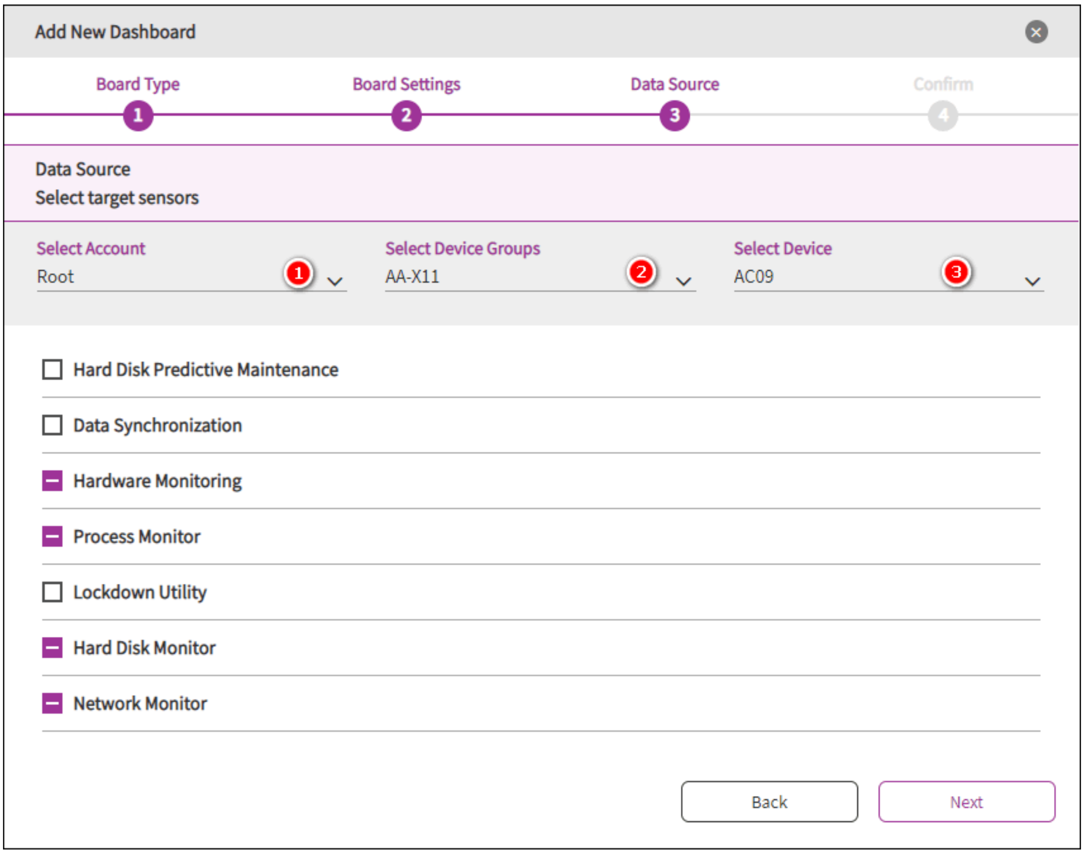
Name 1: AC09

Account 3: admin

URL 2: https://deviceon.wise-paas.com:8080

Password 4: •••••

Select target sensor from the device and click next.



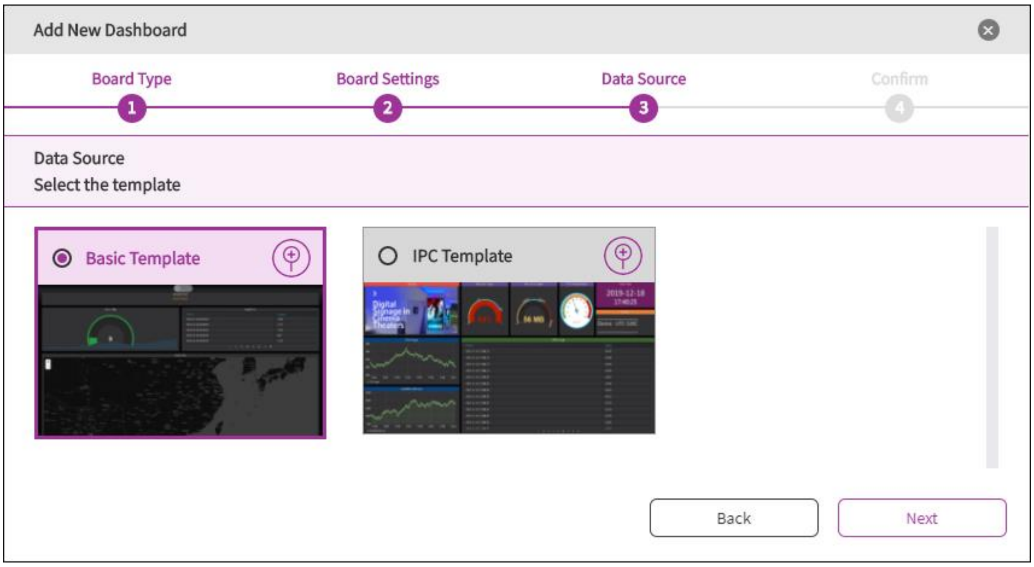
Add New Dashboard

Data Source
Select target sensors

Select Account: Root
Select Device Groups: AA-X11
Select Device: AC09

- □ Hard Disk Predictive Maintenance
- □ Data Synchronization
- ▬ Hardware Monitoring
- ▬ Process Monitor
- □ Lockdown Utility
- ▬ Hard Disk Monitor
- ▬ Network Monitor

(Device Method)



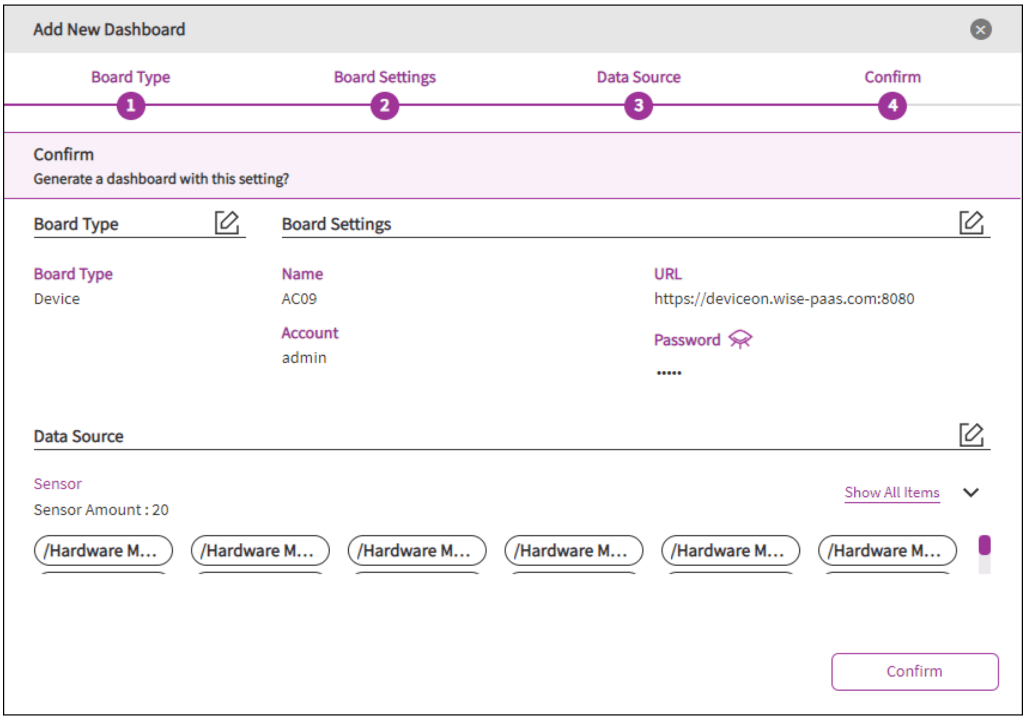
Add New Dashboard

Data Source
Select the template

● Basic Template
○ IPC Template

(Template Method)

Confirm the result and information and start to generate.



Confirm
Generate a dashboard with this setting?

Board Type

Board Type
Device

Board Settings

Name
AC09

URL
https://deviceon.wise-paas.com:8080

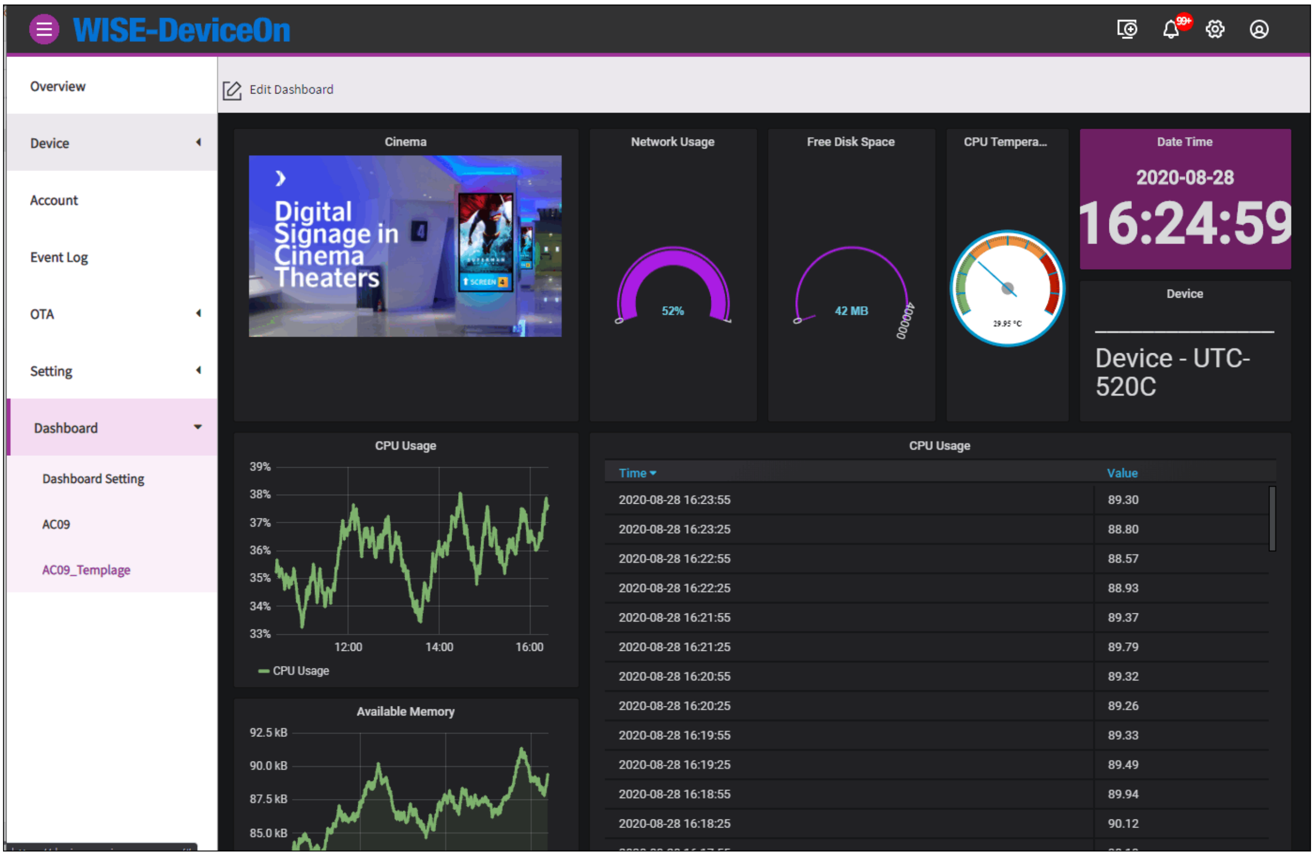
Account
admin

Password
•••••

Data Source

Sensor
Sensor Amount : 20

After that, the board be generated on the menu item.



CPU Usage

Time	Value
2020-08-28 16:23:55	89.30
2020-08-28 16:23:25	88.80
2020-08-28 16:22:55	88.57
2020-08-28 16:22:25	88.93
2020-08-28 16:21:55	89.37
2020-08-28 16:21:25	89.79
2020-08-28 16:20:55	89.32
2020-08-28 16:20:25	89.26
2020-08-28 16:19:55	89.33
2020-08-28 16:19:25	89.49
2020-08-28 16:18:55	89.94
2020-08-28 16:18:25	90.12

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:

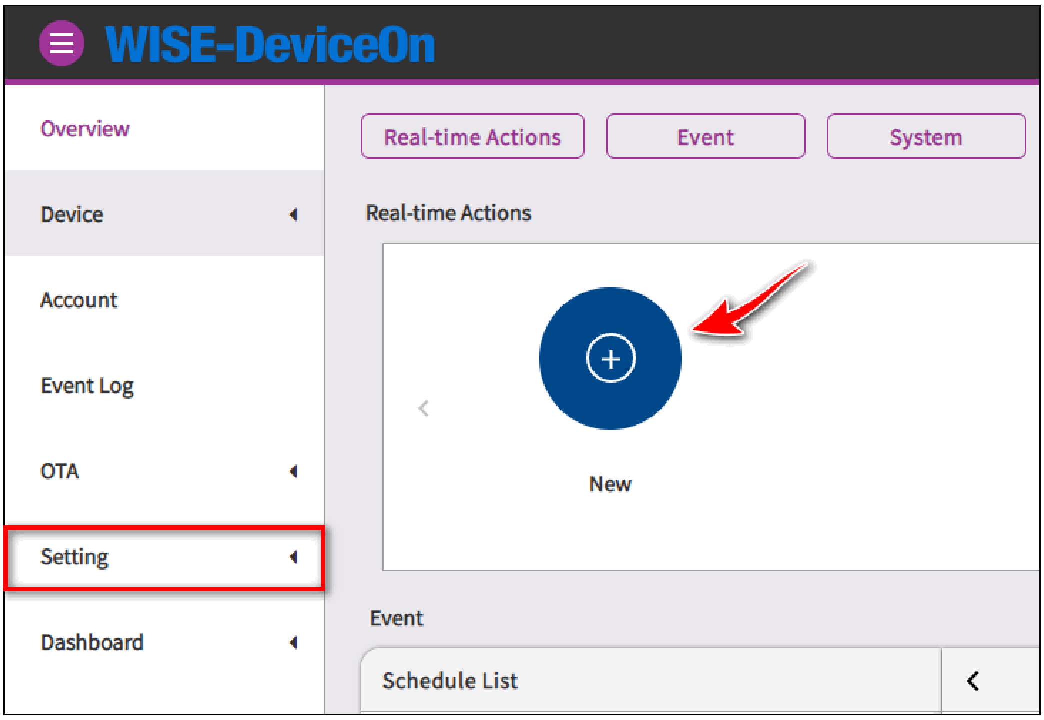
- Learn how to create a real-time action on demand.
- Know of what actions DeviceOn provides.
- Have an action named **"MyTask"** and pinned into your **"Overview"** page, that can reboot devices belong to group **"Default"**.

4.1.1 Prerequisite

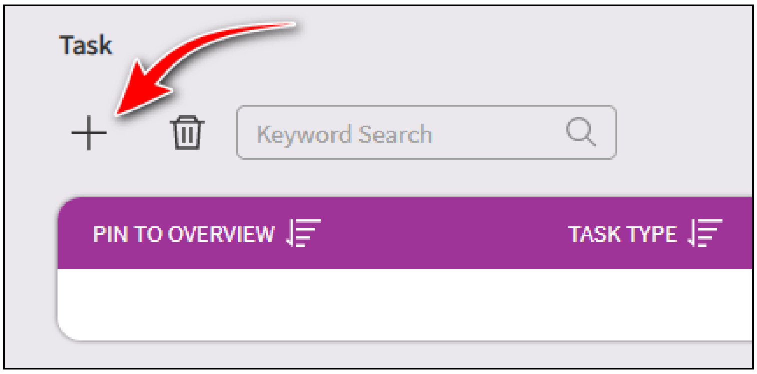
- A running DeviceOn server.
- A device that installed WISE-Agent connects to DeviceOn server.

4.1.2 Step-by-Step

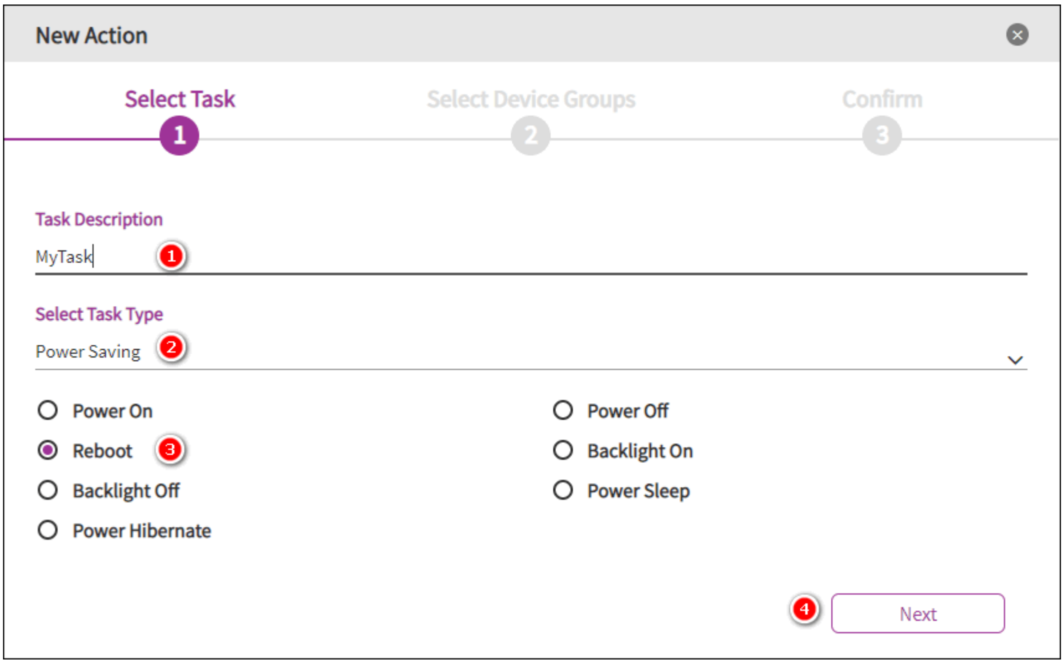
Step 1: To create a real-time action, click the **"New"** icon in **"Overview"**. Alternate, click **"Setting"** from the menu populated in left hand side.



Step 2: Either way you use in step 1, it leads you into the **"Add Task"** page. Click the **"+"** symbol.



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

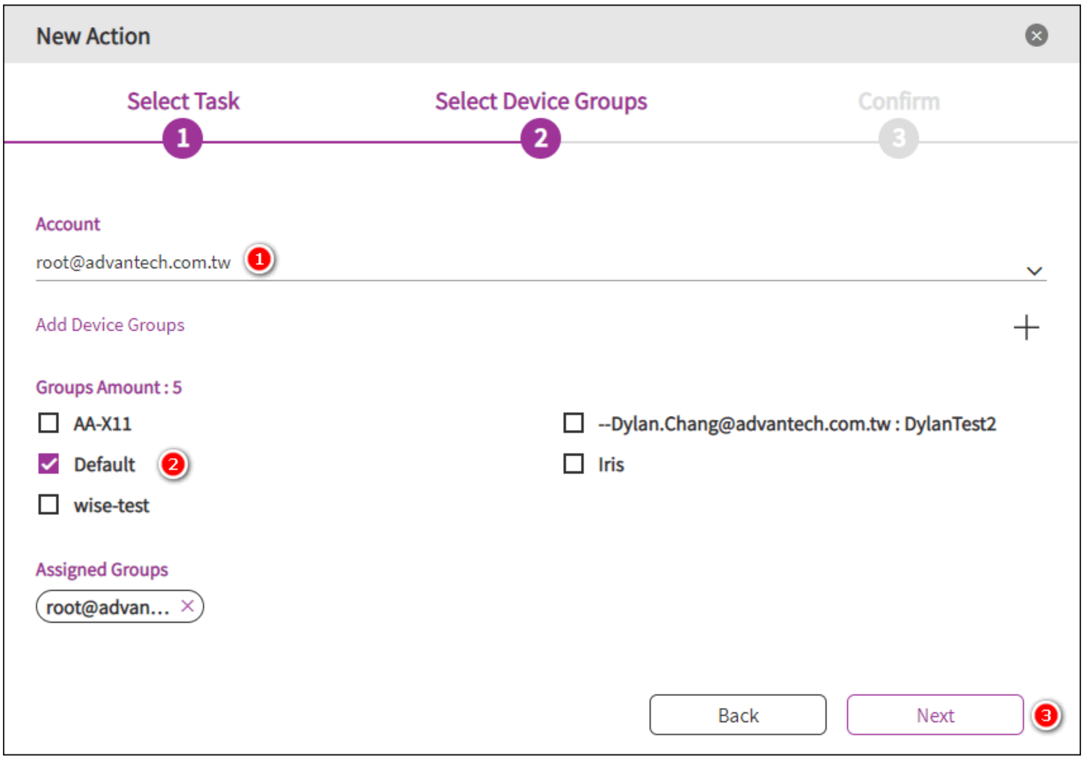


Task Description
MyTask 1

Select Task Type
Power Saving 2

○ Power On
○ Power Off
● Reboot 3
○ Backlight On
○ Backlight Off
○ Power Sleep
○ Power Hibernate

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


New Action

Account

root@advantech.com.tw

Add Device Groups

Groups Amount : 5

☐ AA-X11

☑ Default

☐ wise-test

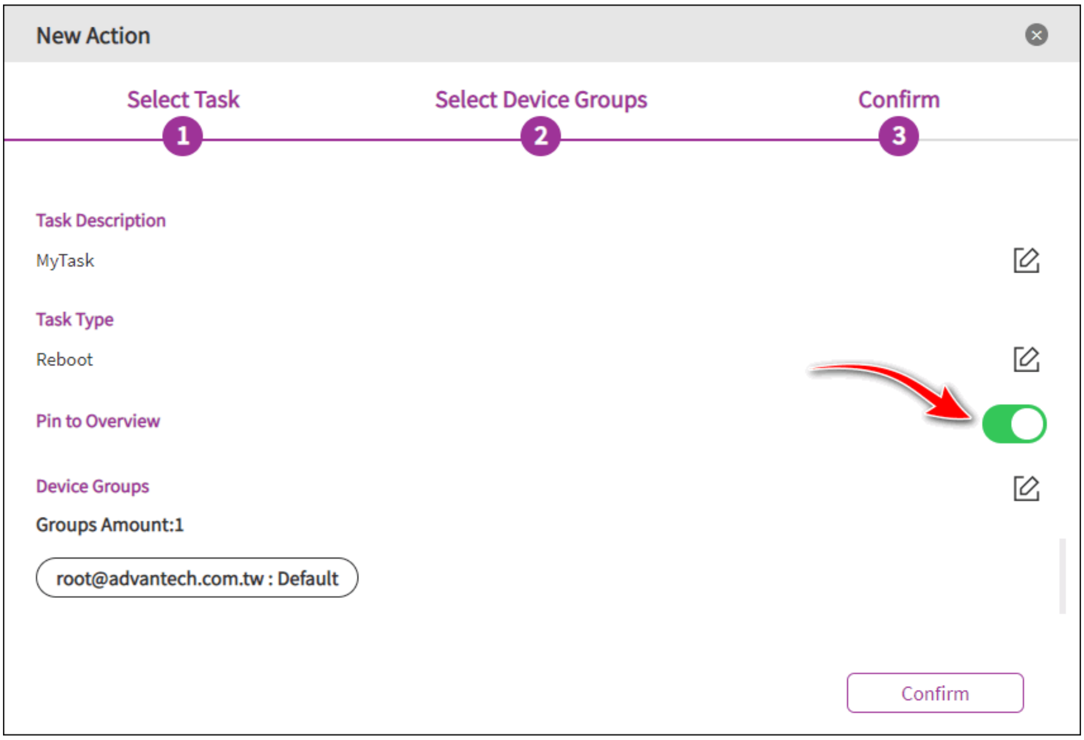
☐ --Dylan.Chang@advantech.com.tw : DylanTest2

☐ Iris

Assigned Groups

root@advan… ✕

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.


New Action

Task Description

MyTask

Task Type

Reboot

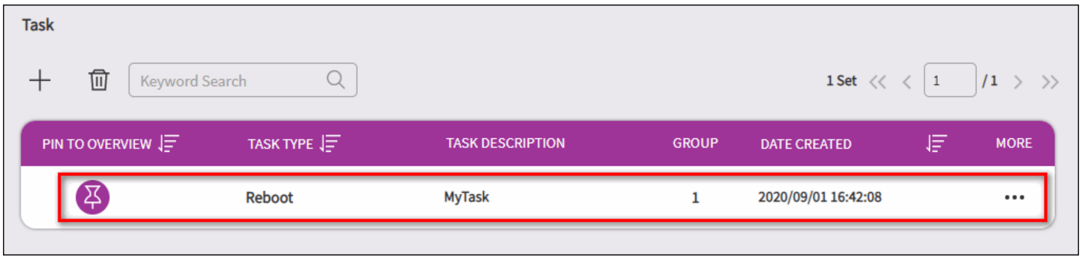
Pin to Overview

Device Groups

Groups Amount:1

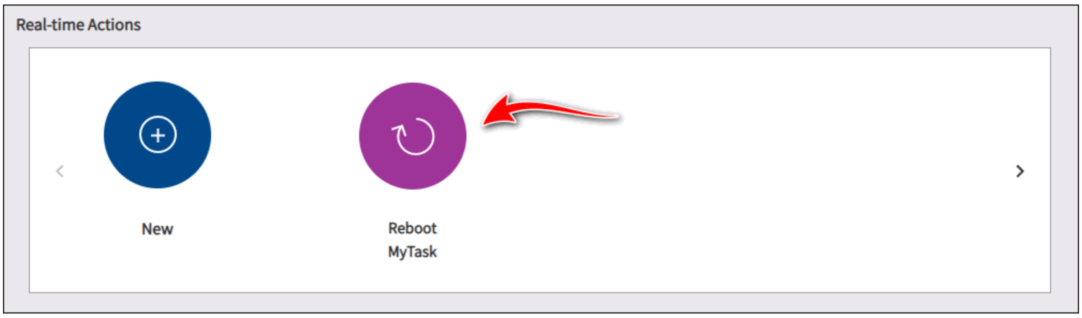
root@advantech.com.tw : Default

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



Task

PIN TO OVERVIEW	TASK TYPE	TASK DESCRIPTION	GROUP	DATE CREATED	MORE
	Reboot	MyTask	1	2020/09/01 16:42:08	•••



Real-time Actions

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 Upload an App to Your App Store

App Store is another powerful feature DeviceOn provides. Users can install software application onto a device remotely, or even many devices broadly. This lab guides you how to accomplish upload and wrap your application to on-premise App Store. And, after this lab, you should:

- Learn how to wrap 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 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 App Store. For Windows it can be batch file or power shell, while for Ubuntu it may be shell scripts.

4.2.2 Step-by-Step

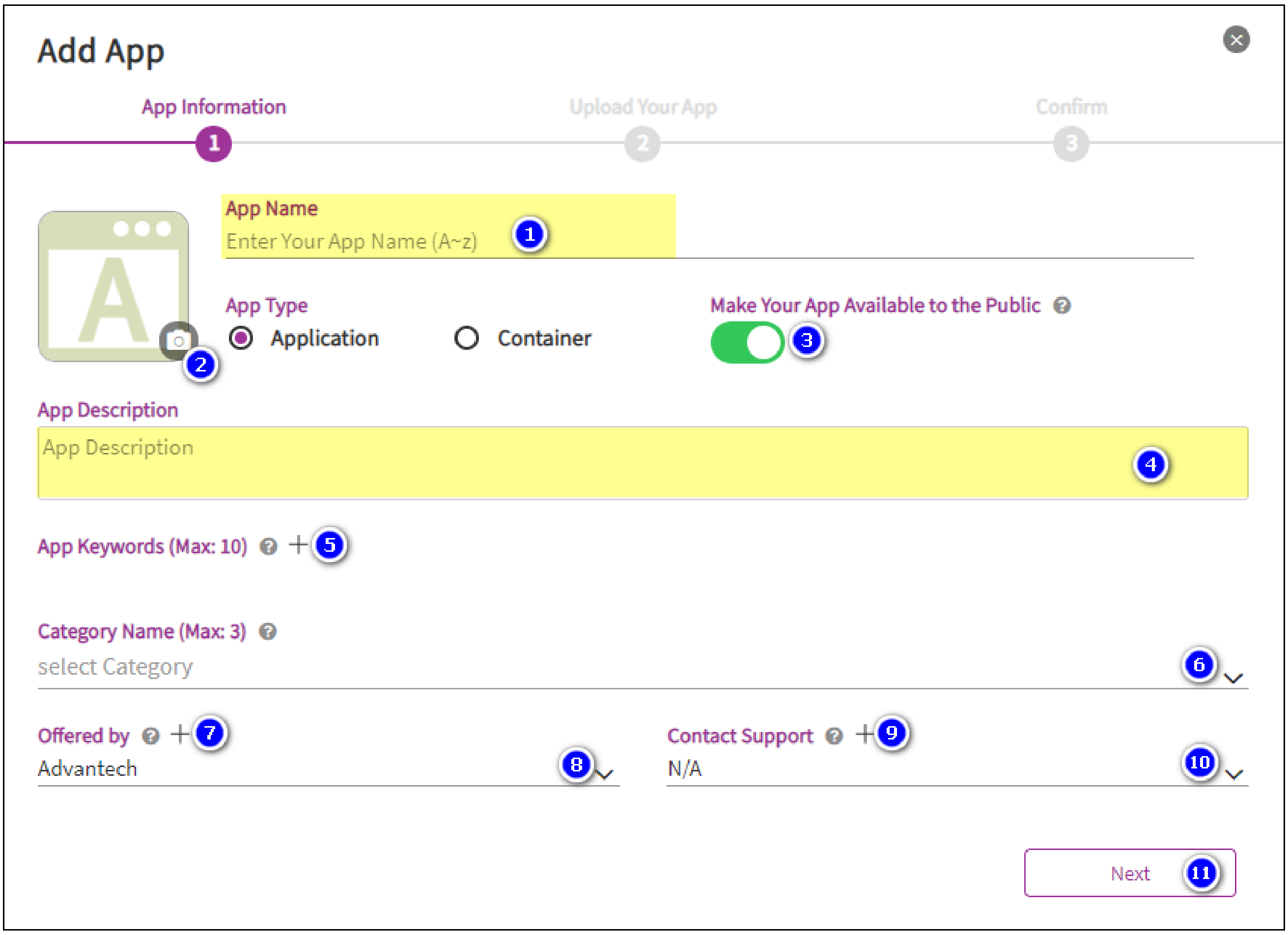
Step 1: Preparation

What should we prepare for an App:

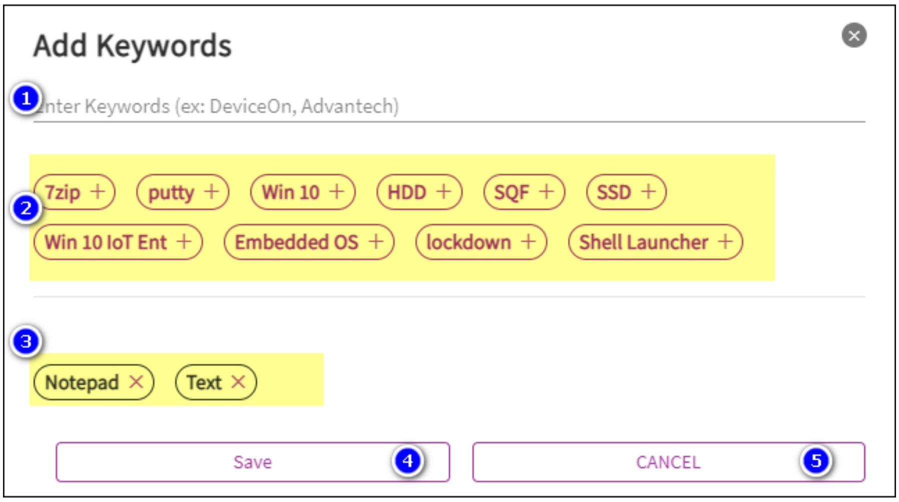
1. **Name**: The public name of app that you want to present to users.
2. **App**: App files for installing to device. There are two necessary files, installer and install script file. In windows, installer may be MSI or EXE, and install script file may be BAT. If the app need to run uninstallation, you need to prepare one more script file for uninstalling.
3. **Icon**: A well-design icon image makes app looks more professional.
4. **Description**: Detailed description text will help user knows the app more.
5. **Keywords**: Accurate keyword can lead user to the app via searching tool, making higher visibility.
6. **Category**: The same with keywords, and more. Category will directly show in app store's first page.
7. **Provider**: The provider is company, or organization who owns the app. The same provider's app will display together under provider's page. Please prepare a logo image, website URL, and description about provider.
8. **Contact**: Providing contact information to users. Let user could send feedback to help app's growth. Please prepare name of contact, and e-mail address.

Note: Image specification: A squared image, in JPG, PNG, GIF formatted file. Recommendation size is 400 x 400 pixel. And smaller than 1 MB(Megabytes)

Step 1: Given an App Information



1. **Name**: The public name of the app.
2. **Icon**: Click to upload an image as app's icon.
3. **Is Public**: Switch to turn On/Off share property to the app. If turn On, other account can install this app to their device. If turn Off, only the account who upload this app can retrieve the app. Note: The property cannot be modified later.
4. **Description**: Text information about the app.
5. **Add Keywords**: Open a dialog to set keywords. At most 10 keywords are acceptable.



5.1. *Enter Keywords*: Input keywords and it will display in keyword candidate list. Manager can input a comma-separated string contains multiple keywords at once. For example: "**Editor**, **Text**" will be two items in keyword candidate list "**Editor**", "**Text**".

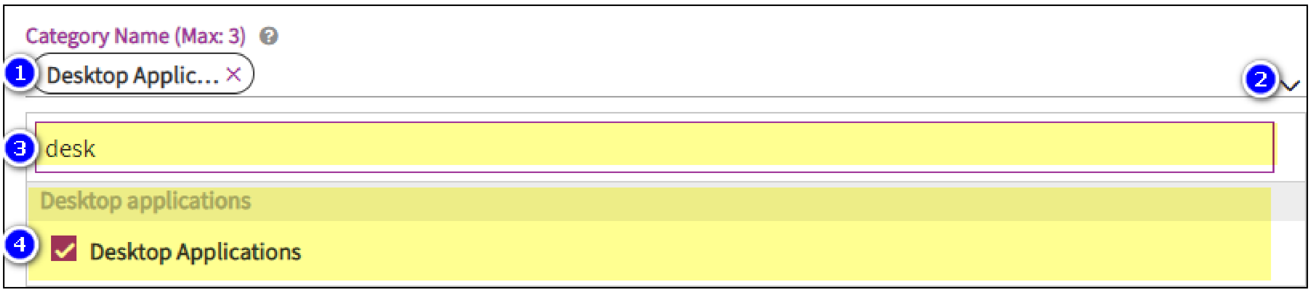
5.2. *Keyword Candidate List*: Shows extant keywords or taking apart from string input above. Click plus sign (+) in the keyword item to add to Keyword List.

5.3. *Keyword List*: Shows manager selected keywords. Click cross sign (x) in the keyword item to remove it from **Keyword List**.

5.4. *Save*: Save keywords in **Keyword List**.

5.5. *Cancel*: Discard change and close dialog.

6. **Category Name**: Select fitting category in drop-down list.



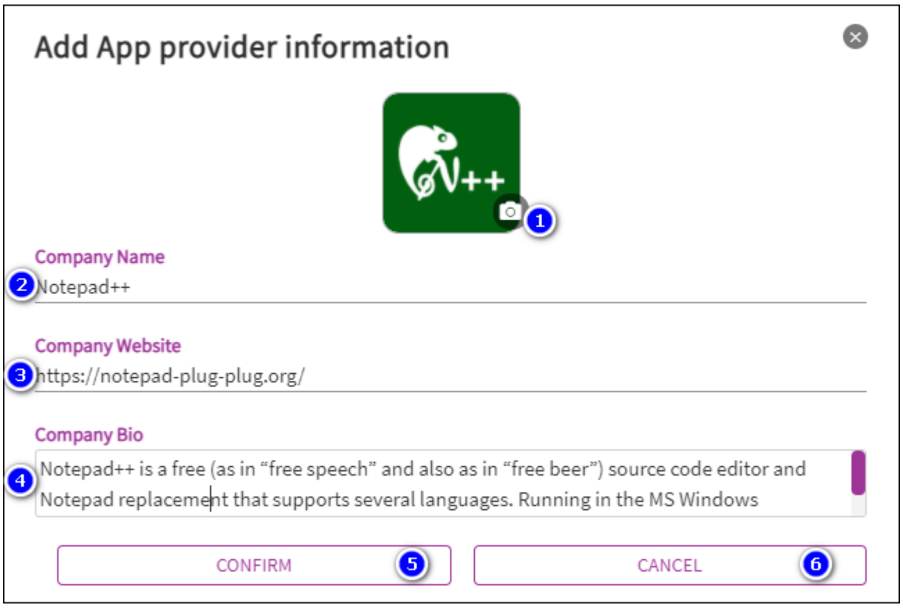
6.1. *Category List*: Selected category list. Click cross sign (x) in the category item to remove it from **Category List**.

6.2. *Open*: Open **Category Candidate List**.

6.3. *Search*: Enter keyword to filter matching category in **Category Candidate List**.

6.4. *Category Candidate List*: All categories list, click on suitable category to add to **Category List**

7. **Add Provider**: If provider not found in provider list, manager can add one here.



Add App provider information

Company Name
Notepad++

Company Website
https://notepad-plug-plug.org/

Company Bio
Notepad++ is a free (as in "free speech" and also as in "free beer") source code editor and Notepad replacement that supports several languages. Running in the MS Windows

7.1. *Logo*: Upload an image as company's logo.

7.2. *Company Name*: The name of company

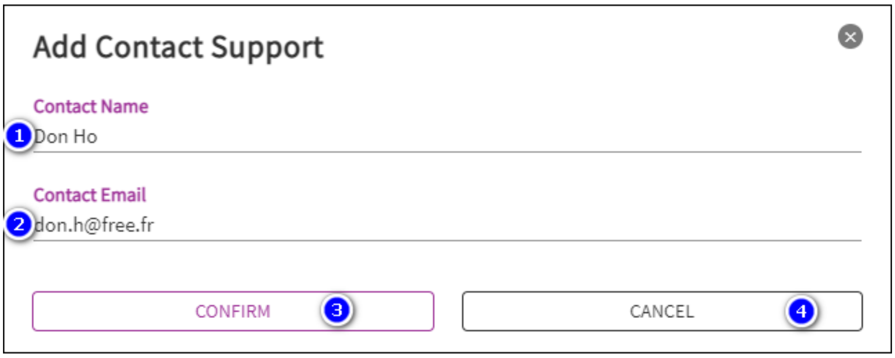
7.3. *Company Website*: URL of website.

7.4. *Company Bio*: Text description of company.

7.5. *CONFIRM*: Save to database and can be found in **Select Provider**.

7.6. *CANCEL*: Discard change and close dialog.

8. **Select Provider**: Select a provider in extant provider list.
9. **Add Contact**: If contact not found in contact list, manager can add one here.



Add Contact Support

Contact Name
1 Don Ho

Contact Email
2 don.h@free.fr

9.1. *Contact Name*: Name of contact.

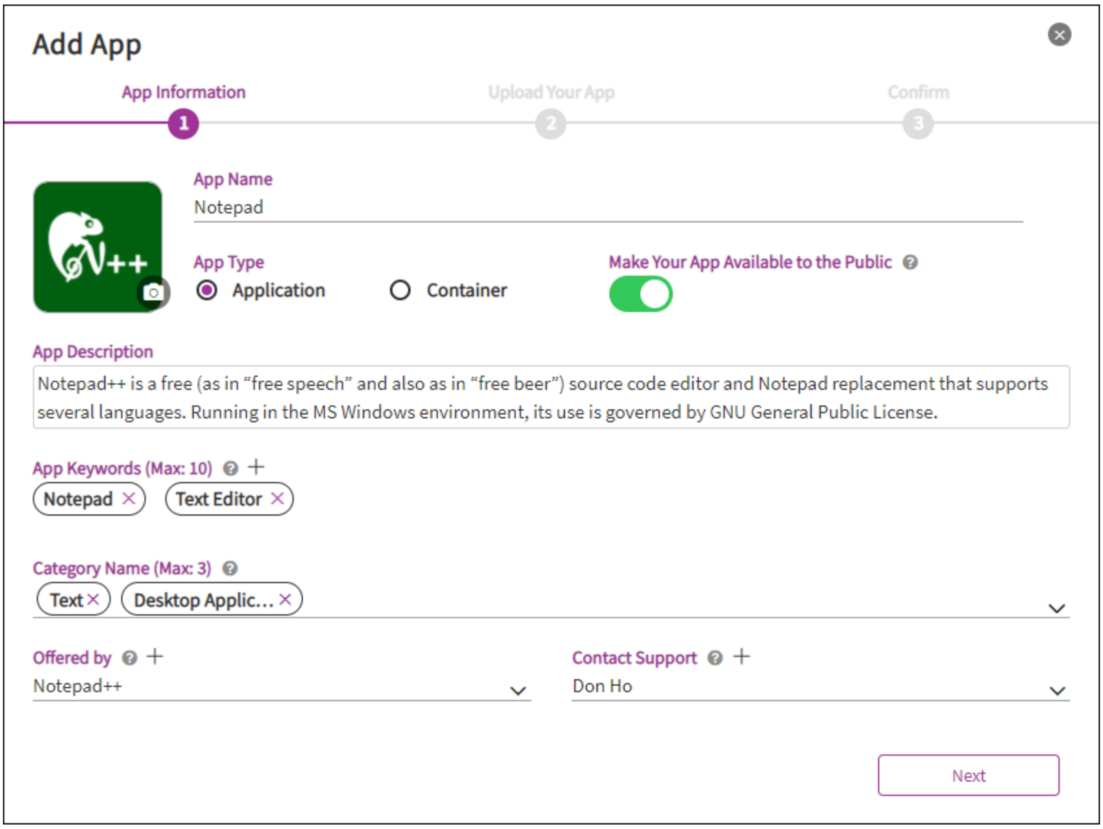
9.2. *Contact Email*: Email of contact.

9.3. *CONFIRM*: Save to database and can be found in Select Contact.

9.4. *CANCEL*: Discard change and close dialog.

10. **Contact Support**: Select a contact in extant contact list.
11. **Next**: To next step.

The result similar as below sample of step 1.



Add App

App Name
Notepad

App Type
● Application ○ Container

Make Your App Available to the Public
On

App Description
Notepad++ is a free (as in “free speech” and also as in “free beer”) source code editor and Notepad replacement that supports several languages. Running in the MS Windows environment, its use is governed by GNU General Public License.

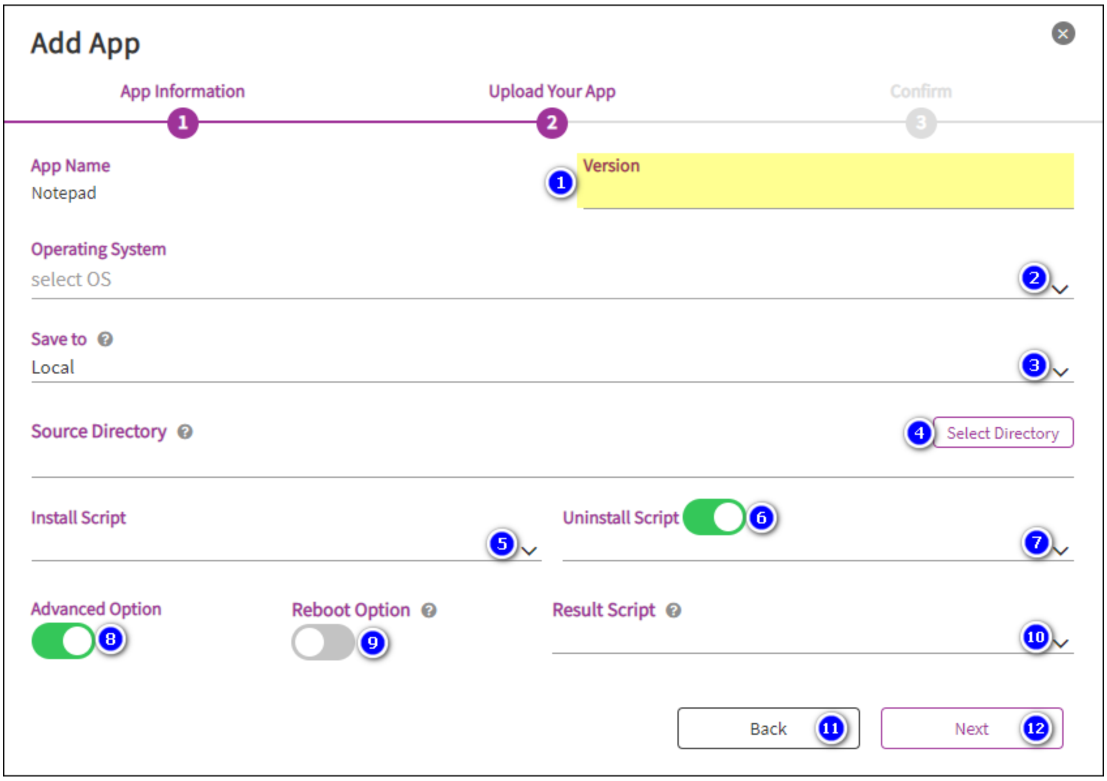
App Keywords (Max: 10)
Notepad ✕ Text Editor ✕

Category Name (Max: 3)
Text ✕ Desktop Applic... ✕

Offered by
Notepad++

Contact Support
Don Ho

Step 2: Upload your App



Add App

App Name
Notepad

Version

Operating System
select OS

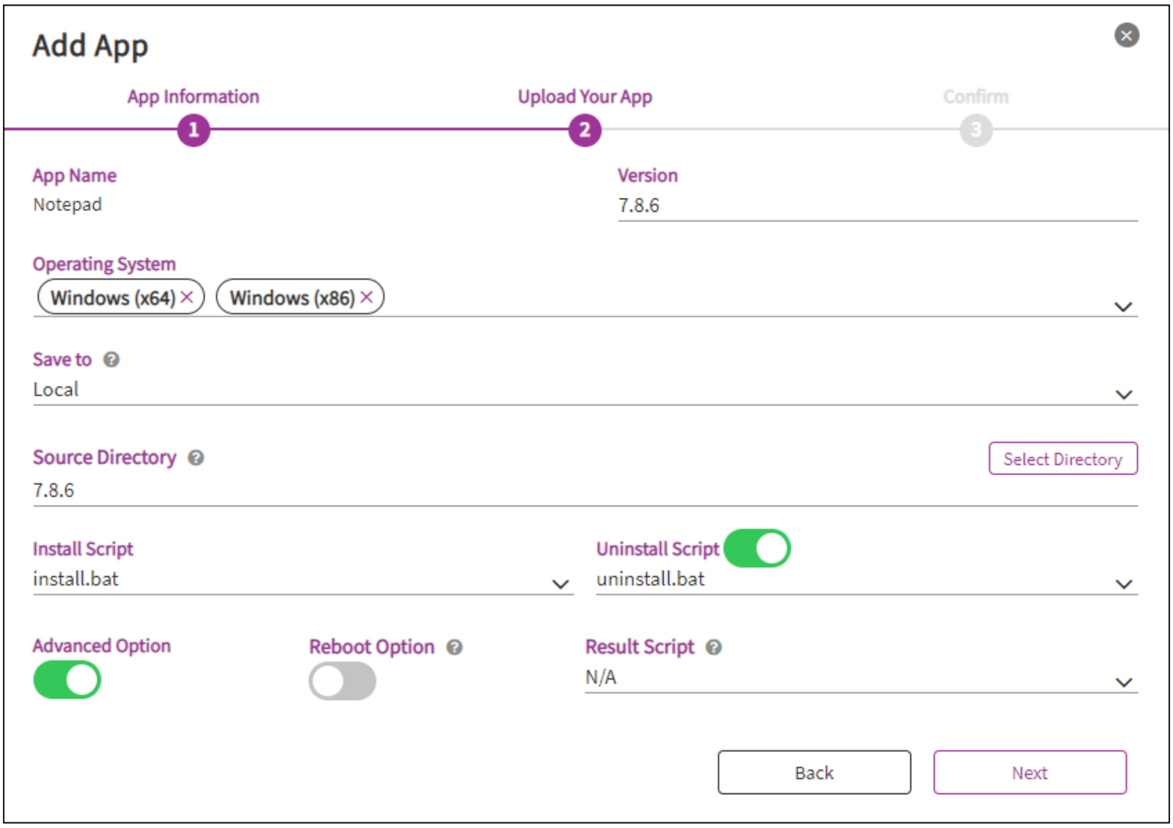
Save to
Local

Source Directory

1. **Version**: App’s version number. 3 or 4 digits and separated by dot(.). For example: 1.0.0 or 1.2.3.4
2. **Operating System**: Select OS of the app can install. Multiple OS are acceptable.
3. **Save to**: Select an option where app package file will save after Step 3. Confirm. [**Local**] means

there will be two zip files download to your local machine, please save it properly, and uploading to specific repository by **Upload App** from **[Repository Name]** means **Online Wrap Tool** will upload app package files to the repository directly.

4. **Select Directory**: Select a directory to upload, which contains files are necessary for installing the app.
5. **Install Script**: Select a runnable script file for executing installation.
6. **Uninstall Option**: Switch On/Off to determine this version's app can uninstall or not.
7. **Uninstall Script**: Select a runnable script file for executing uninstallation.
8. **Advanced Option**: Switch On/Off to show/hide more option.
9. **Reboot Option**: Switch On/Off to determine this version's app need reboot after installation or not.
10. **Result Script**: Select a runnable script file for executing checking result of installation is successful or failed. The script file must return "0", that means success, and all other value will be took as fail.
11. **Back**: Back to previous step.
12. **Next**: To next step.



Add App

App Name
Notepad

Version
7.8.6

Operating System
Windows (x64) ✕ Windows (x86) ✕

Save to
Local

Source Directory
7.8.6

Install Script
install.bat

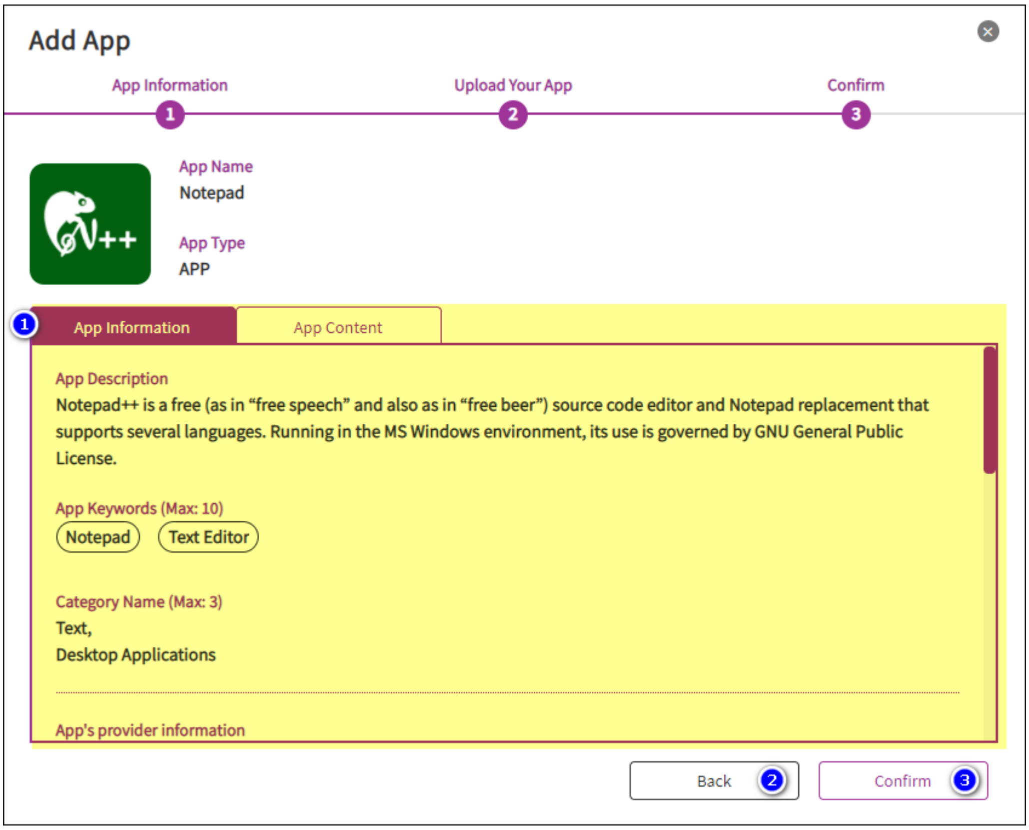
Uninstall Script
uninstall.bat

Advanced Option

Reboot Option

Result Script
N/A

Step 3: Confirm



Add App

App Description
Notepad++ is a free (as in "free speech" and also as in "free beer") source code editor and Notepad replacement that supports several languages. Running in the MS Windows environment, its use is governed by GNU General Public License.

App Keywords (Max: 10)
Notepad
Text Editor

Category Name (Max: 3)
Text,
Desktop Applications

App's provider information

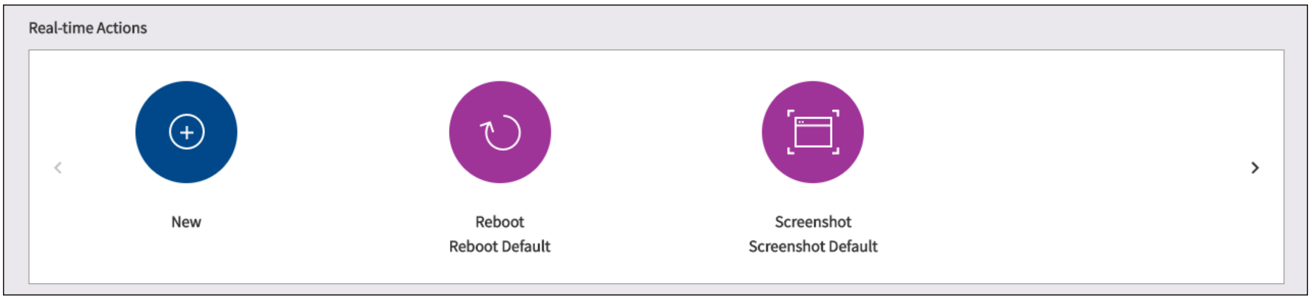
1. **App Information/Content**: Display all data entered in previous steps, please check again before you click **Confirm**.
2. **Back**: Back to previous step.
3. **Confirm**: After checking **App Information/Content**, click Confirm to finish this tool.
   Note: Depending on selected option of **Step 2: Save To**, you will save two zip files or waiting a while for uploading app package files.

4.2.3 DeviceOn Overview

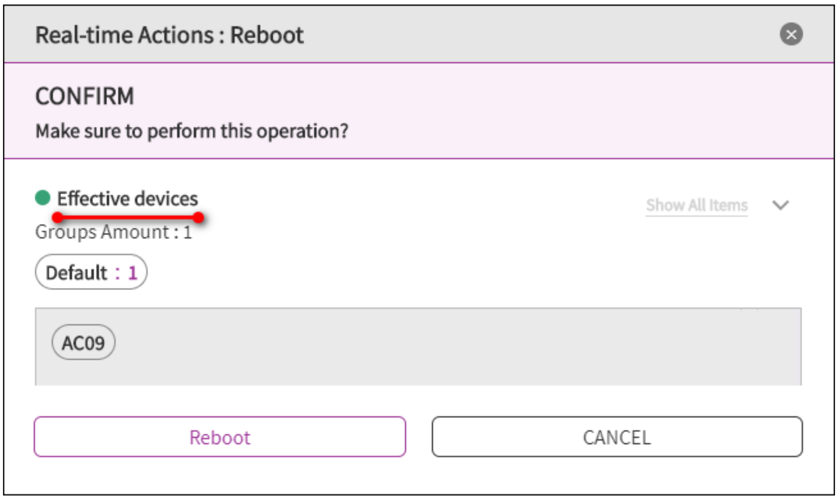
The overview provides quick access to real-time statistics for your managed devices. This information helps to monitor overall status as well as identifying high risk devices. Currently the overview includes Real-time Action, Scheduled Tasks, System Analysis, Device Ranking, and Device Map.

- 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).


Real-time Actions : Reboot

CONFIRM

Make sure to perform this operation?

Effective devices

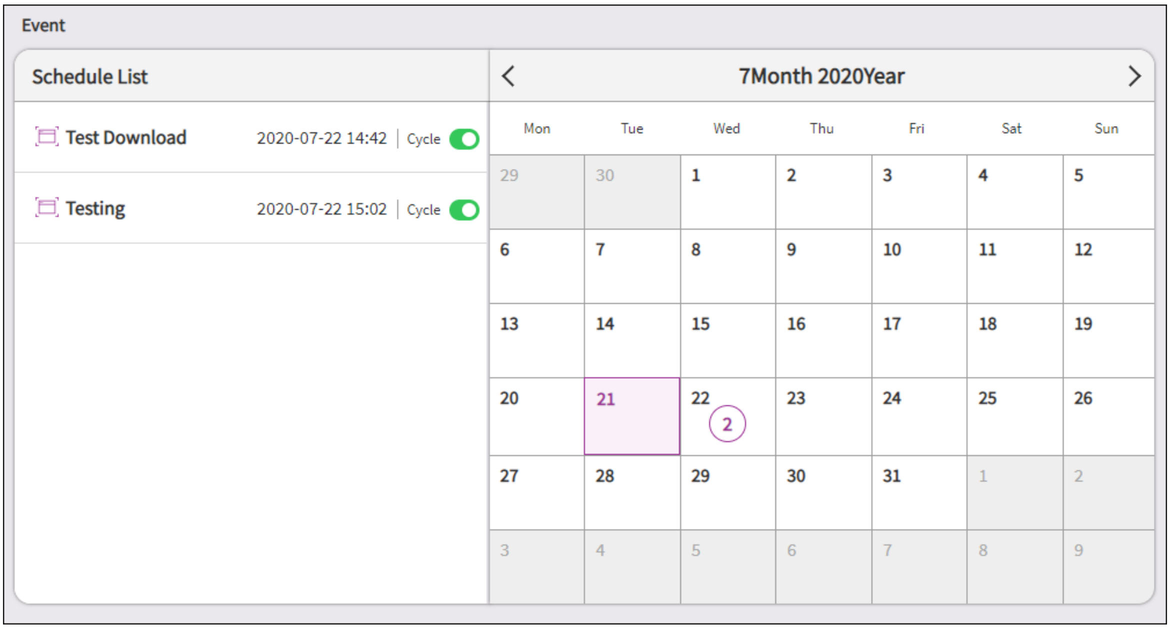
Groups Amount : 1

Default : 1

AC09

- 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.


Event

Schedule List

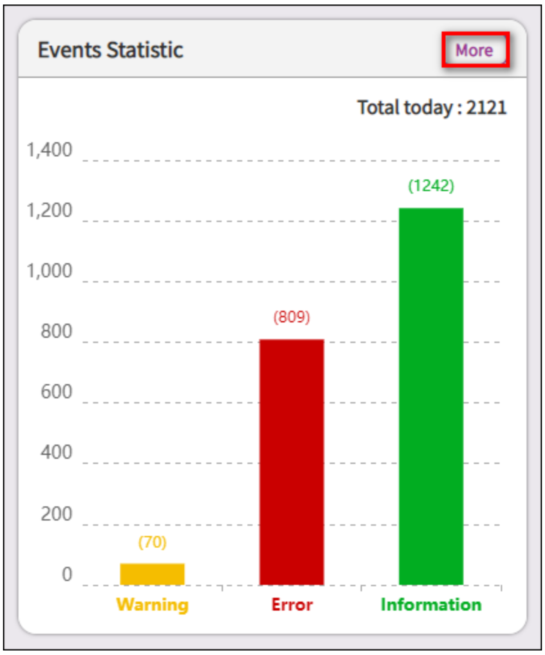
Test Download	2020-07-22 14:42	Cycle
Testing	2020-07-22 15:02	Cycle

7Month 2020Year

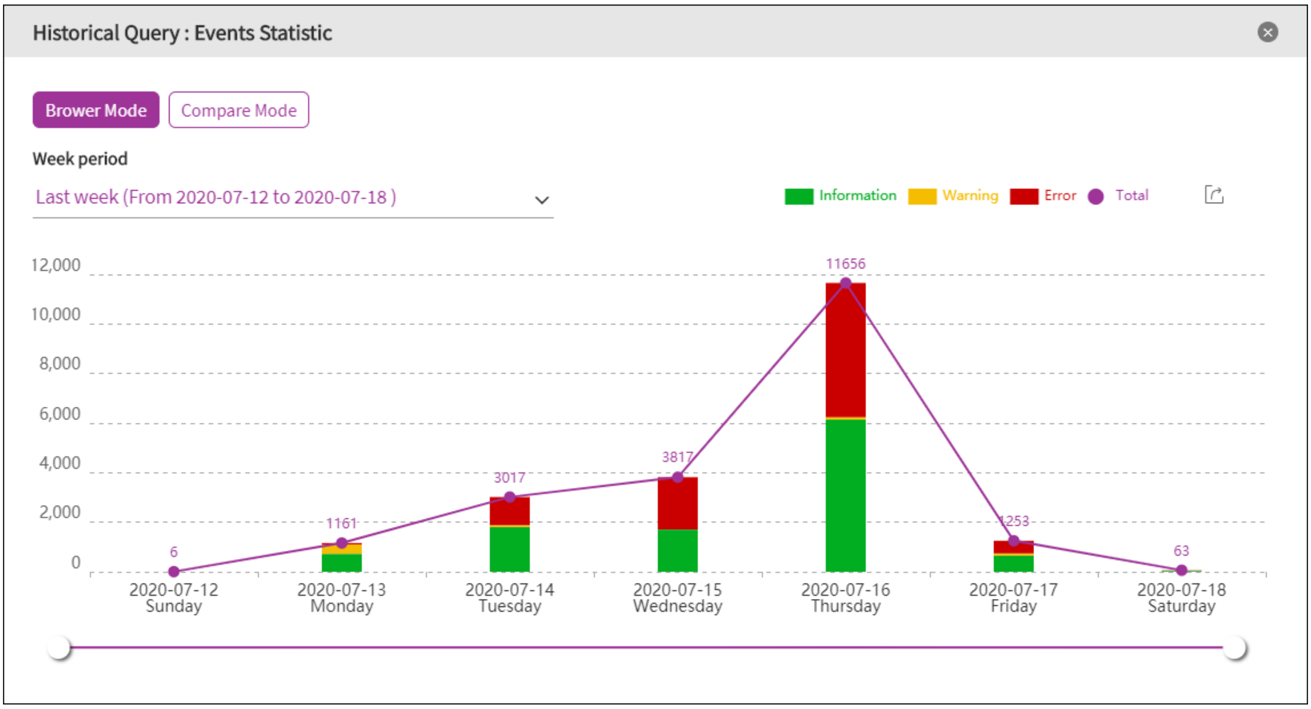
Mon	Tue	Wed	Thu	Fri	Sat	Sun
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22 2	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

- Event Log Statistic

There are three levels of event log on DeviceOn system, such as **Warning**, **Error**, and **Information**. Gives a summary and statistic result for current day. Click on the bar char to redirect **Event Log** tab to check detail log information.

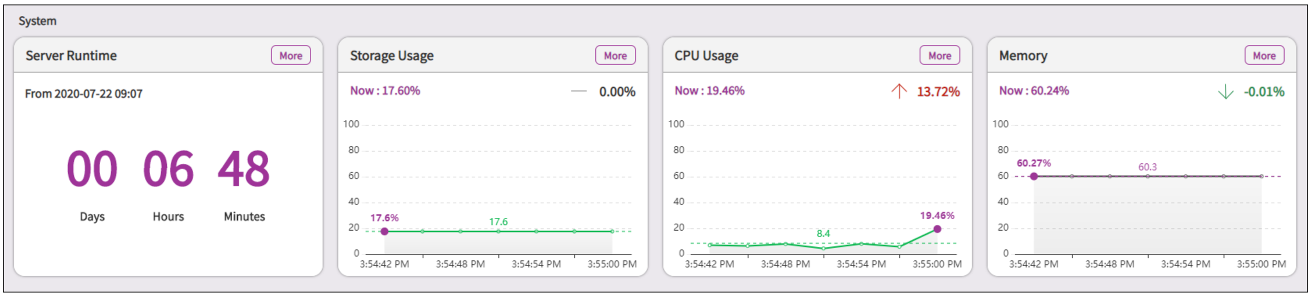


For historical data, please click on "**More**" to compare the daily, weekly result.



- System

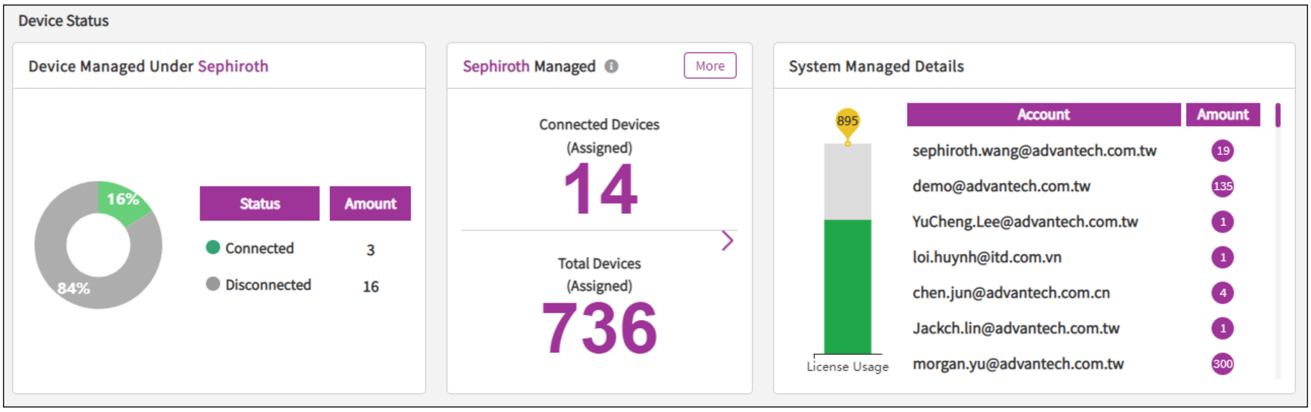
The system is focus on DeviceOn server loading and usage, including storage, CPU and Memory. The administrator could realize the real-time server uptime, downtime through the overview and based on the matrix to scale cloud performance.



- Devices Status

Shows the total devices of current account and DeviceOn system managed.

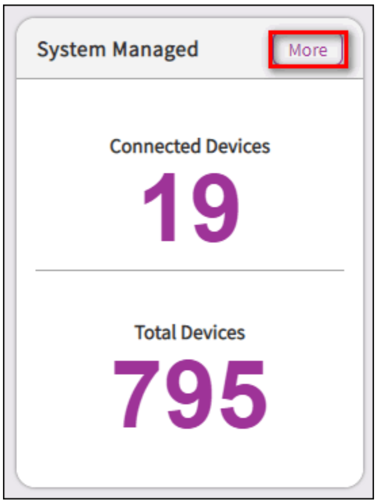
Shows the number of currently online devices as well as total number of managed devices (assigned to account).



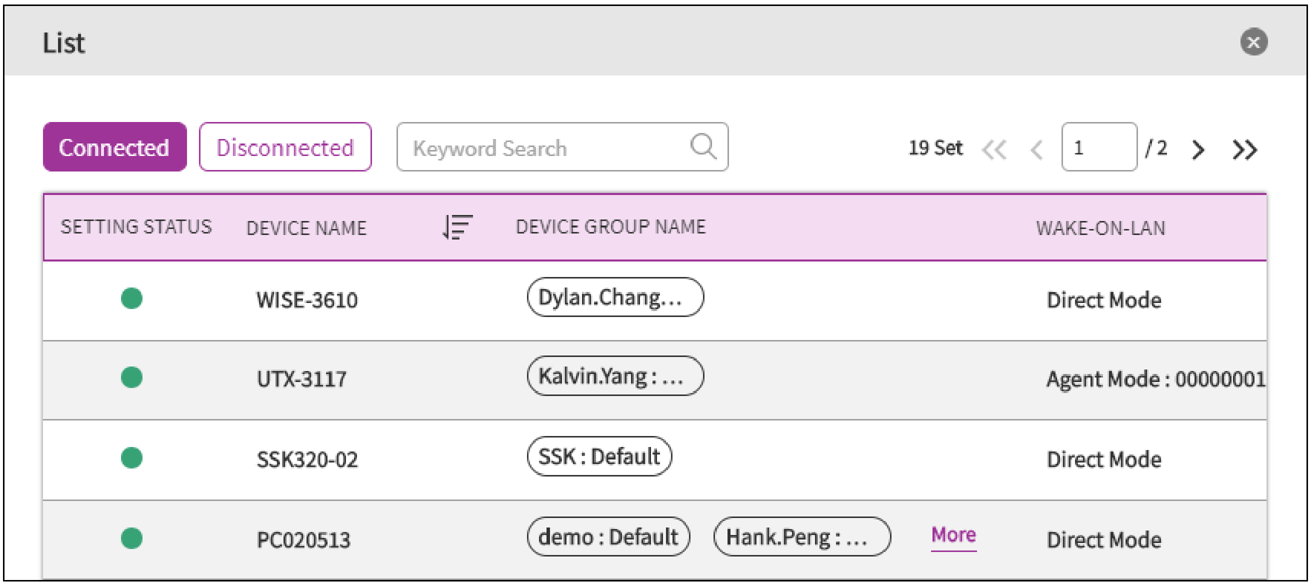
Status	Amount
● Connected	3
● Disconnected	16

Account	Amount
sephiroth.wang@advantech.com.tw	19
demo@advantech.com.tw	135
YuCheng.Lee@advantech.com.tw	1
loi.huynh@itd.com.vn	1
chen.jun@advantech.com.cn	4
Jackch.lin@advantech.com.tw	1
morgan.yu@advantech.com.tw	300

Click on the more information on system managed to show the number of currently online devices as well as total number of managed devices.



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



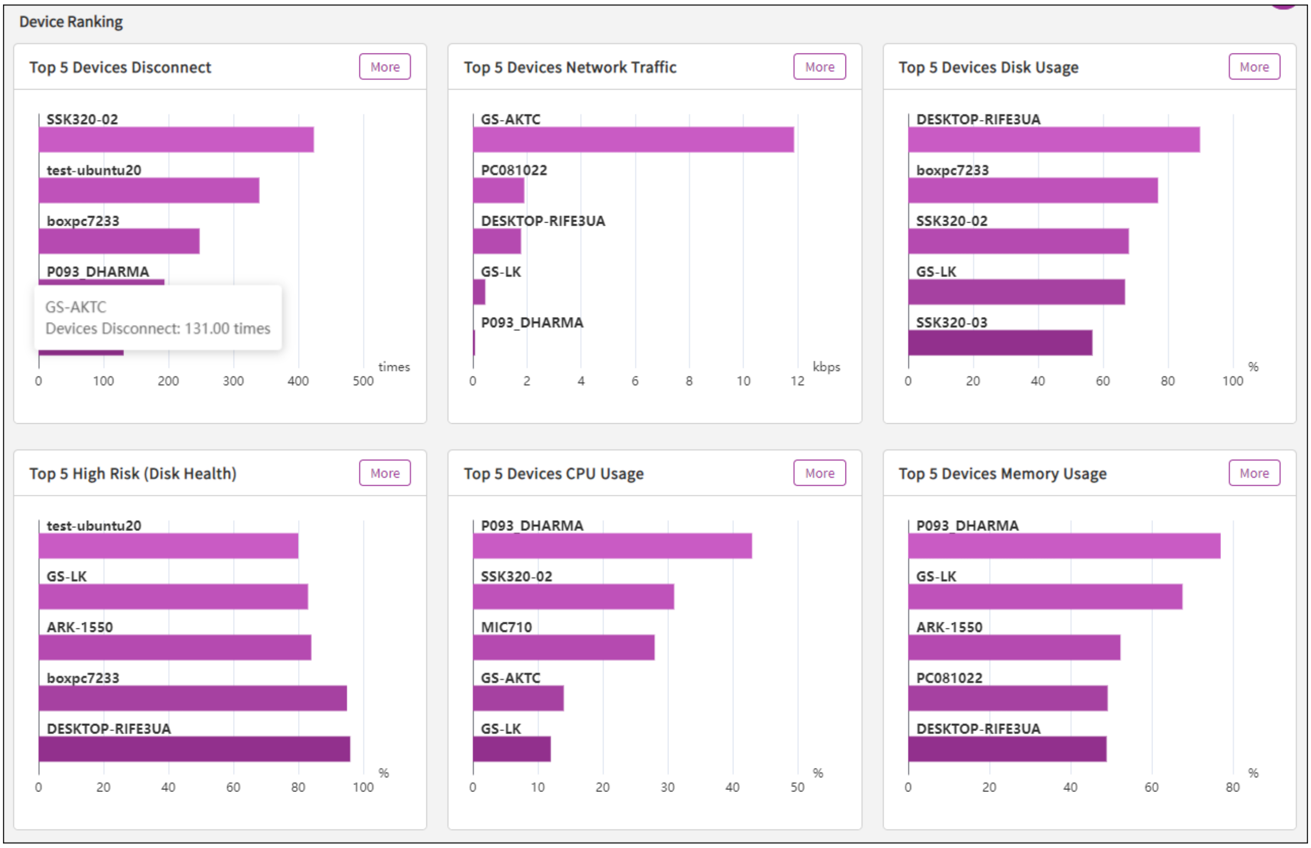
List

Connected | Disconnected | Keyword Search | 19 Set | 1 /2

SETTING STATUS	DEVICE NAME	DEVICE GROUP NAME	WAKE-ON-LAN
●	WISE-3610	Dylan.Chang...	Direct Mode
●	UTX-3117	Kalvin.Yang : ...	Agent Mode : 00000001
●	SSK320-02	SSK : Default	Direct Mode
●	PC020513	demo : Default Hank.Peng : ... More	Direct Mode

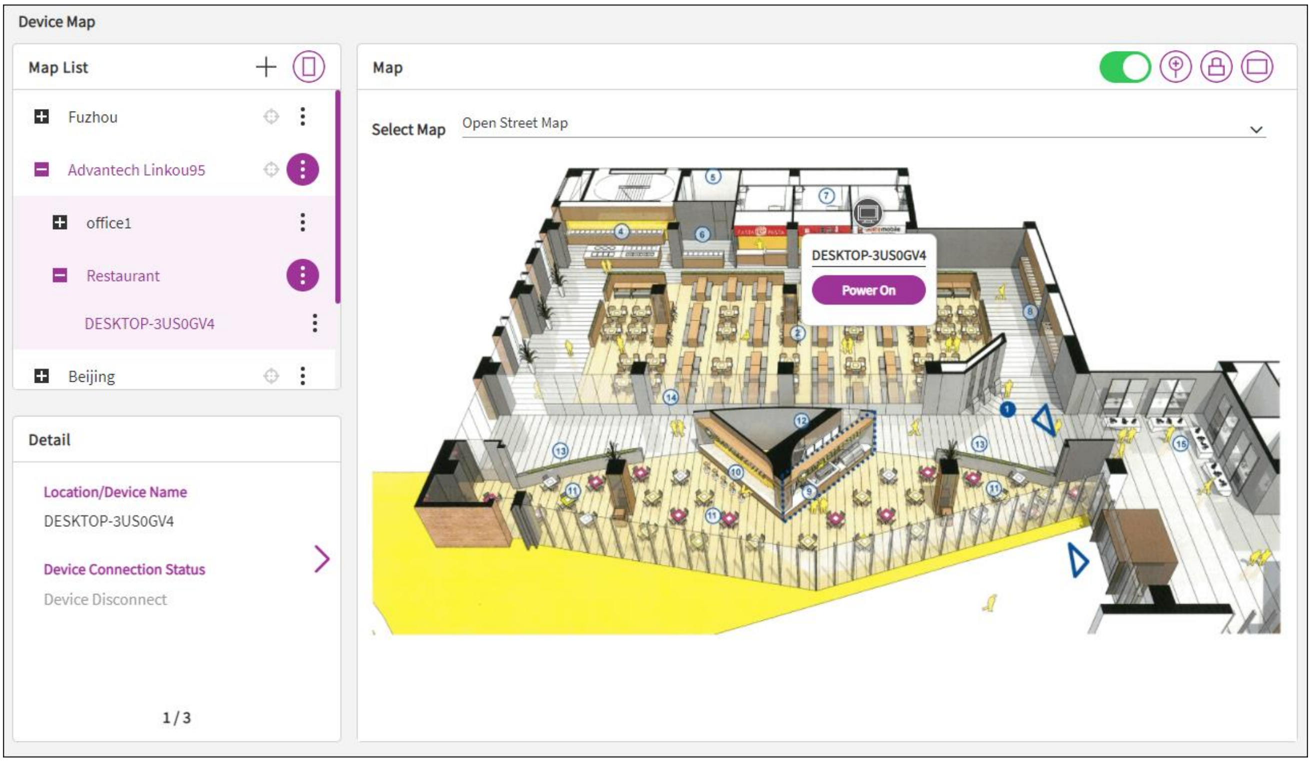
- Top 5 (High-Risk) Statistic

DeviceOn leverages six common sensor types to identify potential high-risk devices. Those sensors are device disconnects, network traffic, disk usage, disk health, CPU usage and memory usage. This “top 5” overview allows to quickly identify potential issues and fix or replace the systems to avoid unexpected downtime.



- Device Map (**OpenStreetMap/Google Map/Baidu Map**)

DeviceOn offers support for maps (latitude and longitude-based position) or floor plans to visualize the location of managed devices. User could define their location on the map and place the device to the area (floor plans).



Location/Device Name: DESKTOP-3US0GV4

Device Connection Status: Device Disconnect

Select Map: Open Street Map

For on-premises and without public network environment, you could try to download an offline OpenStreet map and place into right place.

Step 1: Download OpenStreetMap data for your region (.osm.pbf)

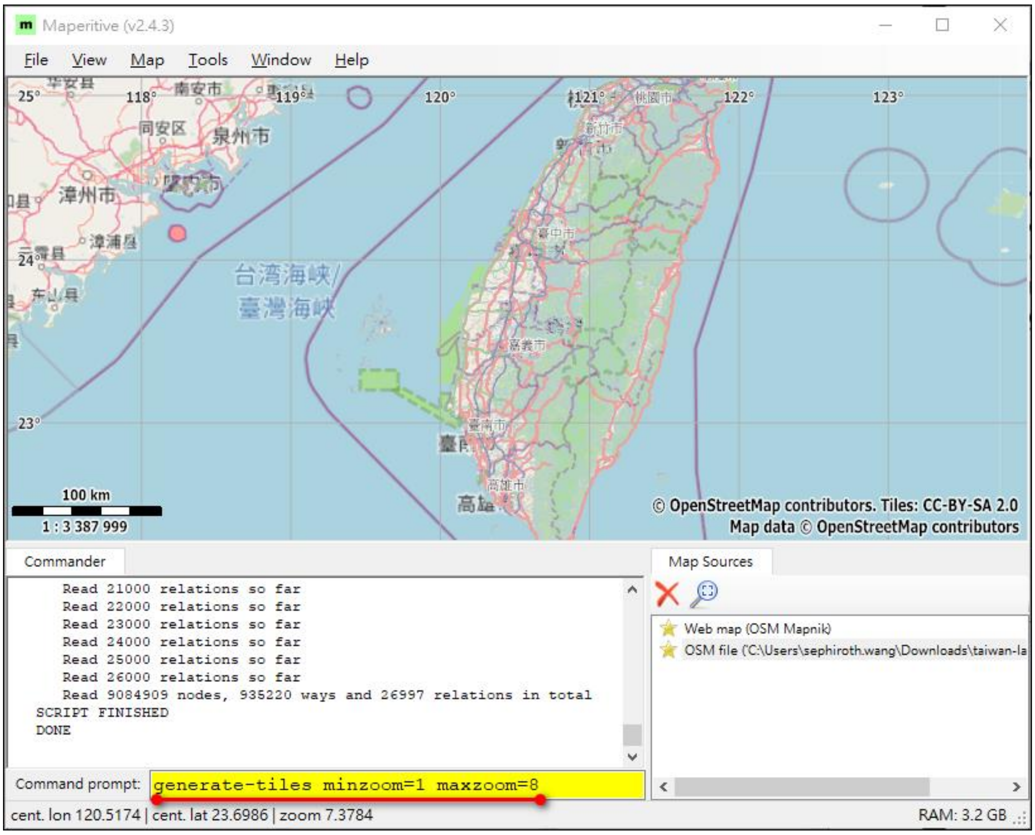
Step 2: Convert and process OpenStreetMap file (.osm.pbf to .osm) via Osmconvert

```
osmconvert.exe <YOUR_REGION>.osm.pbf --out-osm -o=<YOUR_REGION>.osm_01.osm
```

Step 3: Adopt Maperitive for drawing maps based on OpenStreetMap

- Open the .osm file that generated from Step 2 through Mapertive.
- Generates tiles from the zoom level 1 up to the zoom level 8. (REF)

```
generate-tiles minzoom=1 maxzoom=8
```


Maperitive (v2.4.3)
File View Map Tools Window Help
100 km
1 : 3 387 999
© OpenStreetMap contributors. Tiles: CC-BY-SA 2.0
Map data © OpenStreetMap contributors
Commander
Map Sources

```
    Read 21000 relations so far
    Read 22000 relations so far
    Read 23000 relations so far
    Read 24000 relations so far
    Read 25000 relations so far
    Read 26000 relations so far
    Read 9084909 nodes, 935220 ways and 26997 relations in total
 SCRIPT FINISHED
 DONE
```

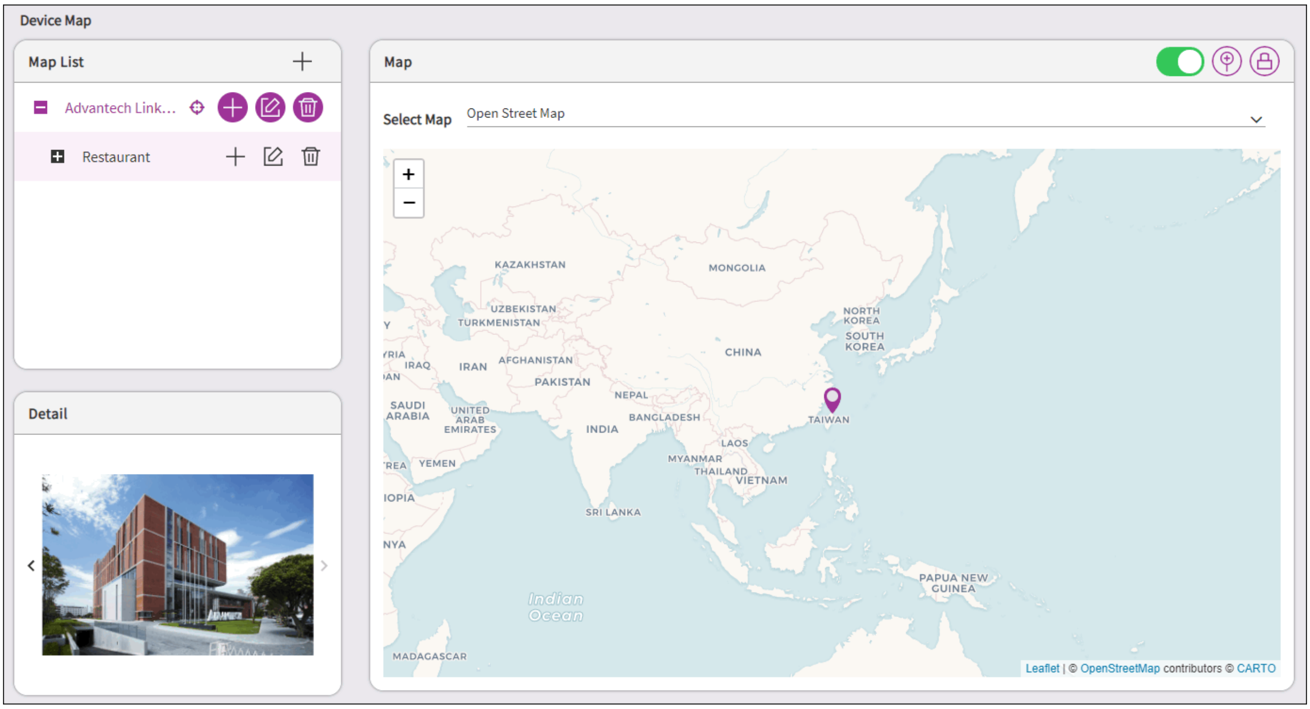
Web map (OSM Mapnik)
OSM file (C:\Users\sephiroth.wang\Downloads\taiwan-la

Command prompt: `generate-tiles minzoom=1 maxzoom=8`

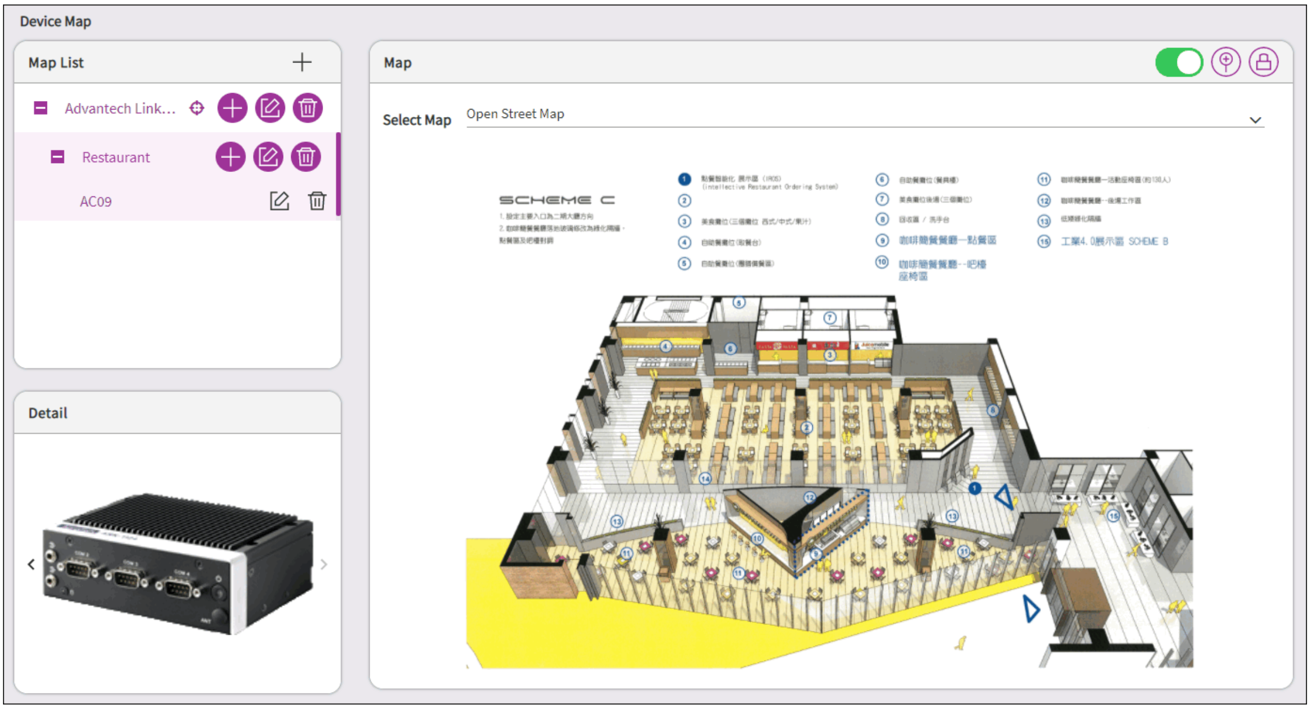
cent. lon 120.5174 | cent. lat 23.6986 | zoom 7.3784 RAM: 3.2 GB

- Copy the all folder and tiles.json that generated under "./Maperitive/Titles" to DeviceOn Server path (/portal/static/offlineMap/OpenStreetMap/Tiles)

Note: Be careful when specifying zoom levels. Each zoom level needs about four times as many tiles as the previous one, so you can very quickly reach pretty large numbers of tiles which can take a very long time to generate and require a lot of disk space.



Select Map: Open Street Map



Select Map: Open Street Map

4.3 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:

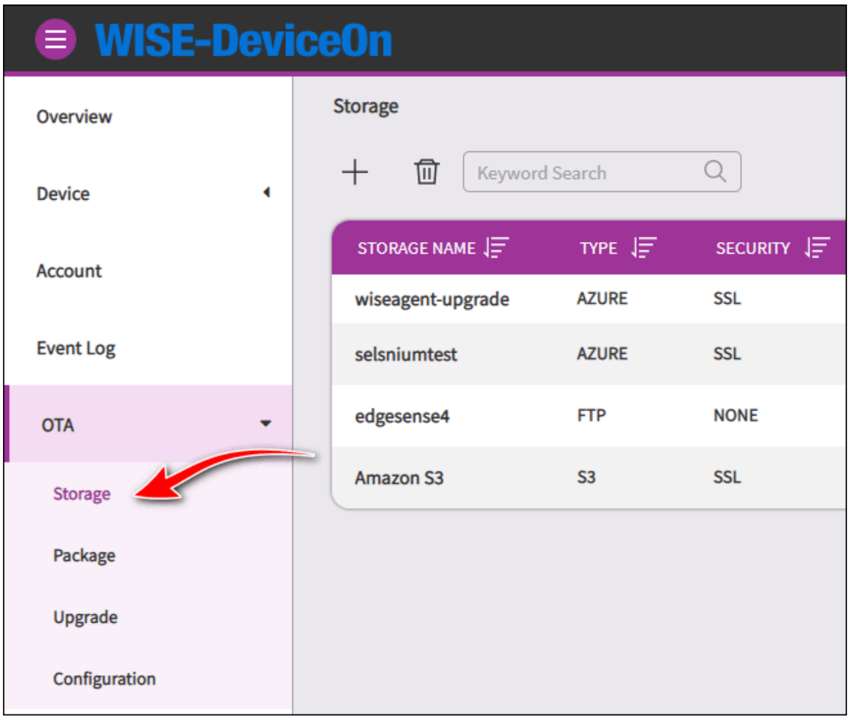
- Learn how to remote provisioning your software via OTA on demand.
- Learn how to package your software for remote provisioning.
- Have the NotePad++, a popular and famous text editor, populated within the target device.

4.3.1 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.

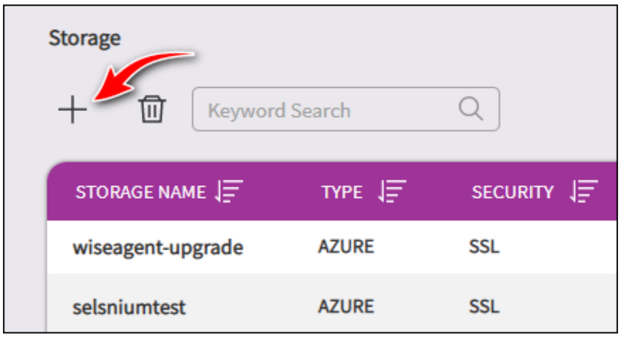
4.3.2 Step-by-Step

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



STORAGE NAME	TYPE	SECURITY
wiseagent-upgrade	AZURE	SSL
selsniumtest	AZURE	SSL
edgesense4	FTP	NONE
Amazon S3	S3	SSL

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.



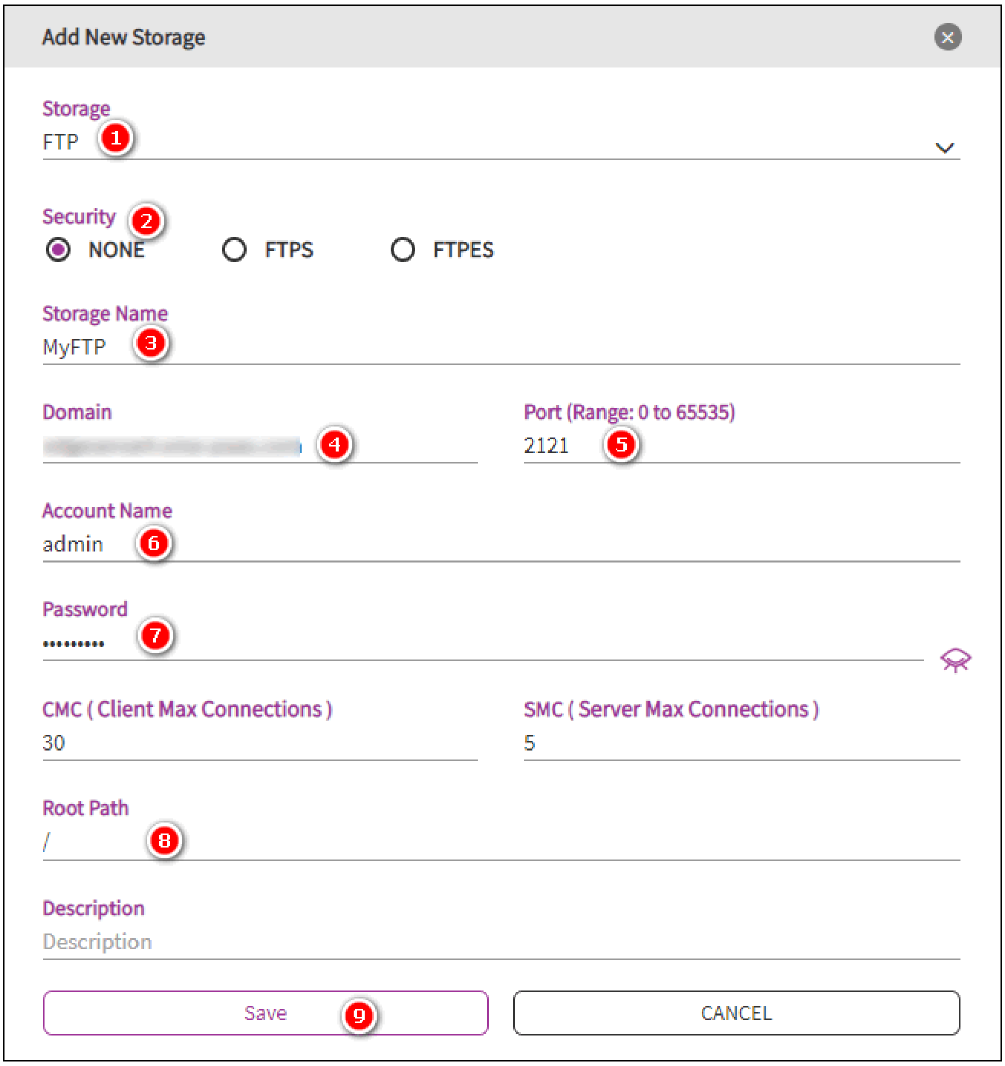
STORAGE NAME	TYPE	SECURITY
wiseagent-upgrade	AZURE	SSL
selsniumtest	AZURE	SSL

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
[redacted] ④

Port (Range: 0 to 65535)
2121 ⑤

Account Name
admin ⑥

Password
••••••••• ⑦

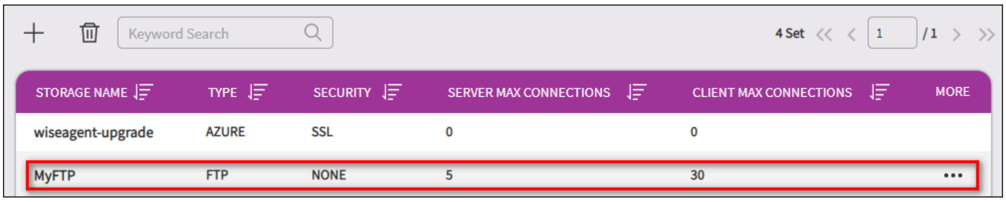
CMC (Client Max Connections)
30

SMC (Server Max Connections)
5

Root Path
/ ⑧

Description
Description

Save ⑨ CANCEL

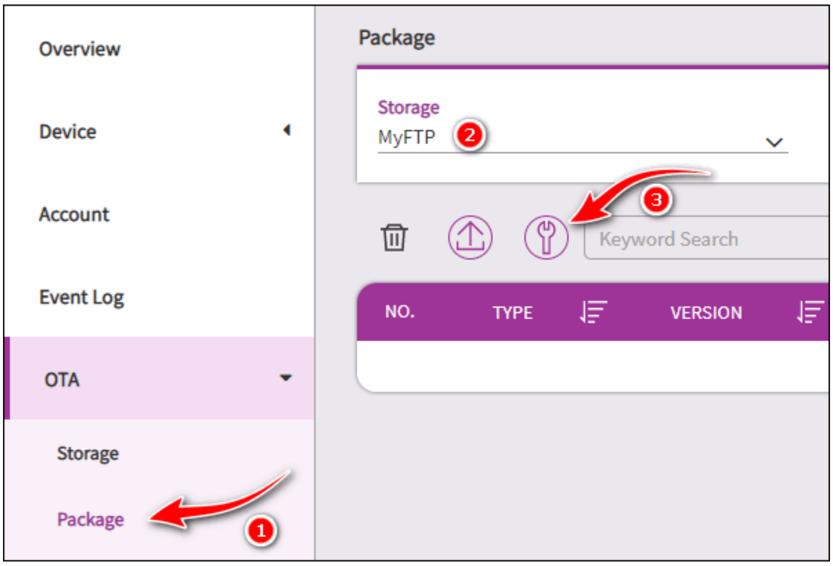


STORAGE NAME	TYPE	SECURITY	SERVER MAX CONNECTIONS	CLIENT MAX CONNECTIONS	MORE
wiseagent-upgrade	AZURE	SSL	0	0	
MyFTP	FTP	NONE	5	30	•••

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.

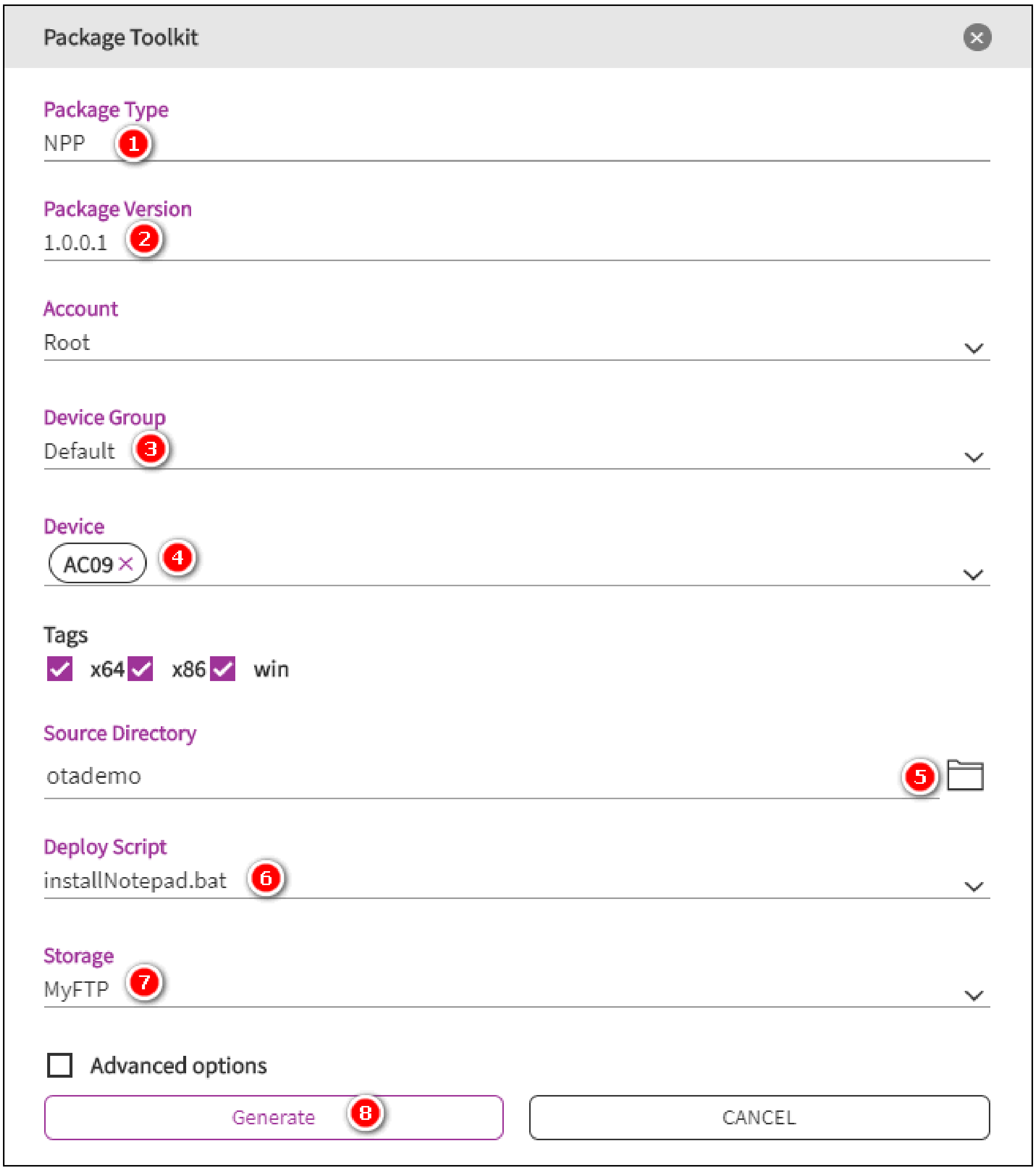
1. Create a new folder names **"NPP"** in, say, your desktop.
2. Move the downloaded file **"npp.7.8.2.Installer.exe"** into.
3. Create a new file **"install.bat",** contains only **start /wait npp.7.8.2.Installer.exe /S**, inside. This command, per its document in official web site, installs the downloaded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

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



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.



Package Toolkit

Package Type
NPP

Package Version
1.0.0.1

Account
Root

Device Group
Default

Device
AC09 ×

Tags
☑ x64 ☑ x86 ☑ win

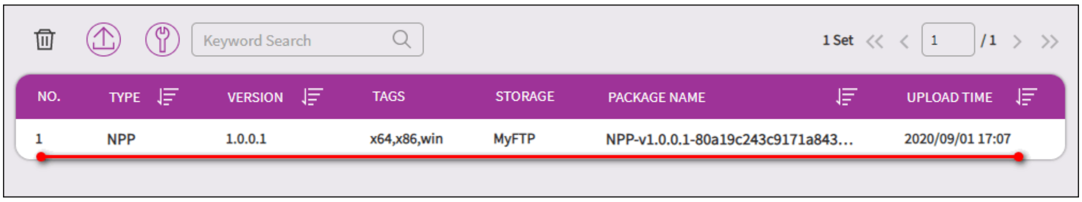
Source Directory
otademo

Deploy Script
installNotepad.bat

Storage
MyFTP

□ Advanced options

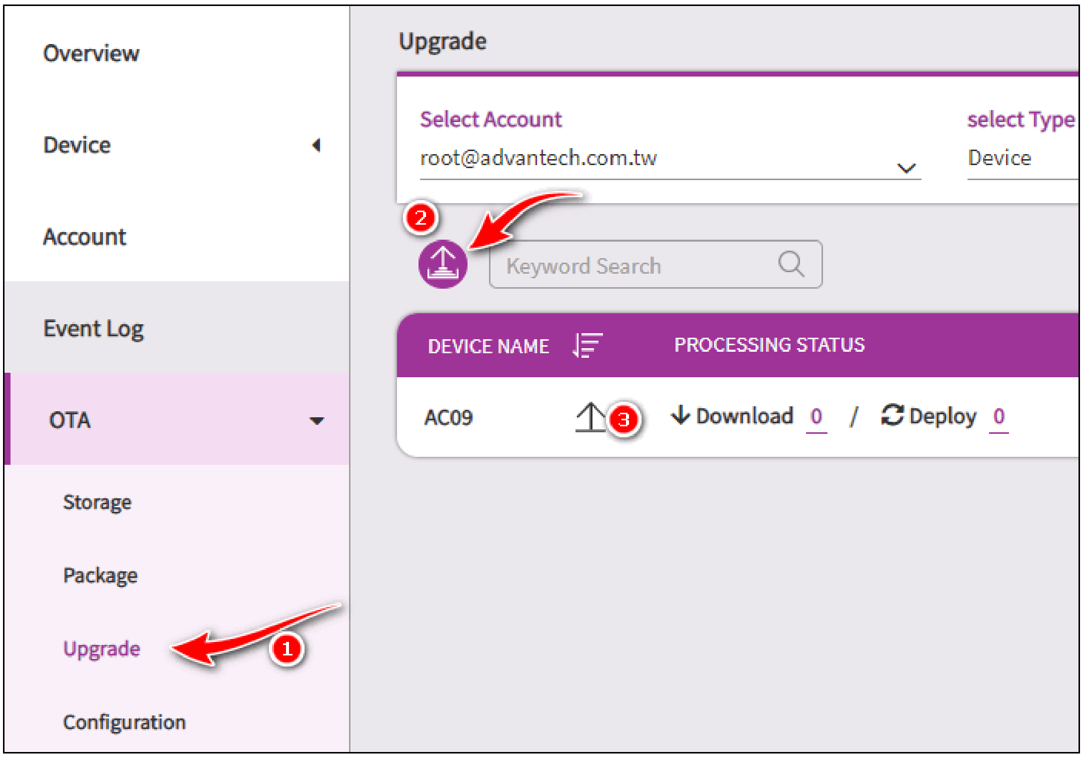
Step 7: Now, in **"Package"** page, a new one table row represents the **"NPP"** package has been added.



Keyword Search　　1 Set　1 /1

NO.	TYPE	VERSION	TAGS	STORAGE	PACKAGE NAME	UPLOAD TIME
1	NPP	1.0.0.1	x64,x86,win	MyFTP	NPP-v1.0.0.1-80a19c243c9171a843...	2020/09/01 17:07

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.



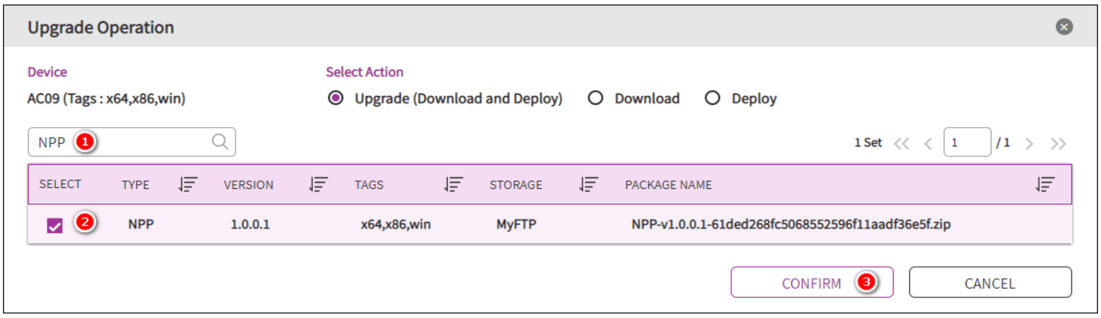
Upgrade

Select Account: root@advantech.com.tw

select Type: Device

DEVICE NAME	PROCESSING STATUS
AC09	↓ Download 0 / ↻ Deploy 0

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 **"FONFIRM"** button.



Upgrade Operation

Device: AC09 (Tags : x64,x86,win)

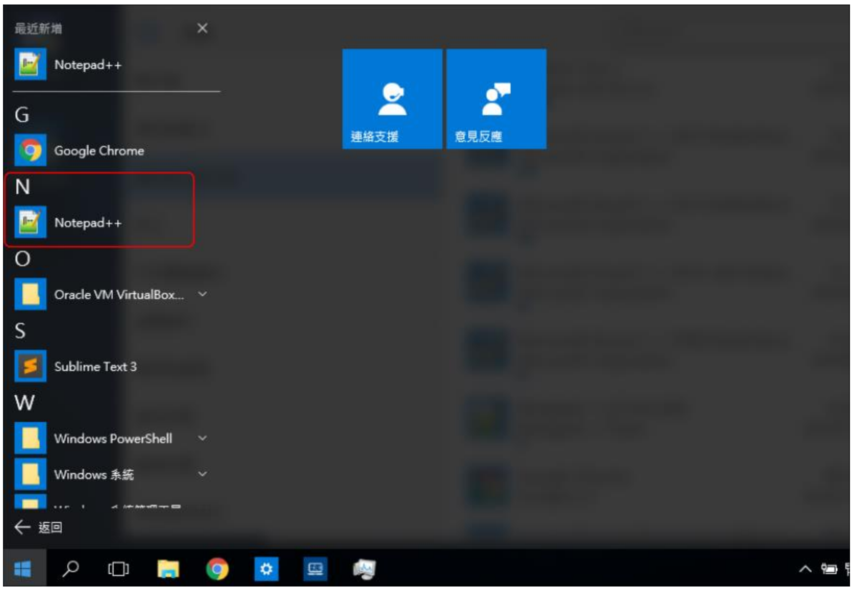
Select Action: ● Upgrade (Download and Deploy) ○ Download ○ Deploy

NPP

1 Set 1 /1

SELECT	TYPE	VERSION	TAGS	STORAGE	PACKAGE NAME
☑	NPP	1.0.0.1	x64,x86,win	MyFTP	NPP-v1.0.0.1-61ded268fc5068552596f11aadf36e5f.zip

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



4.4 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.

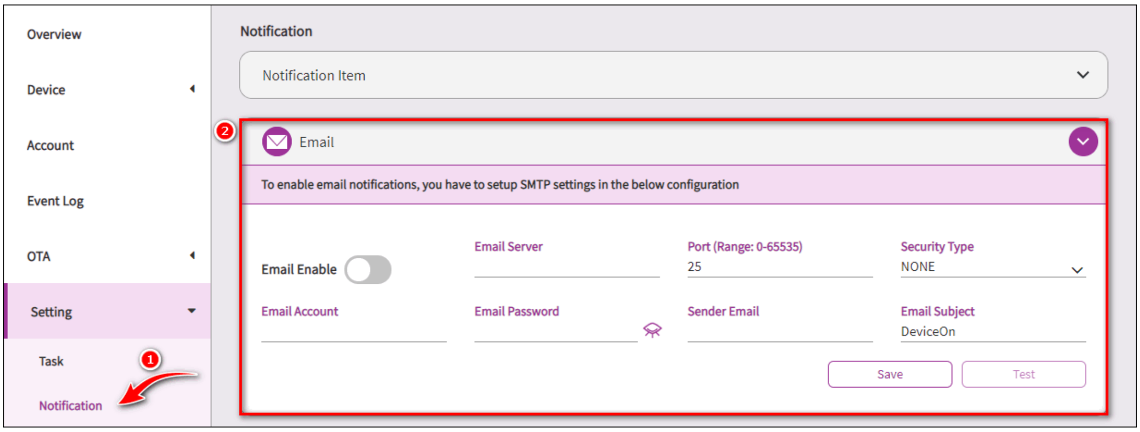
4.4.1 Prerequisite

- 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.

4.4.2 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"**. Click **"EMail"** bar to open settings regarding email notification service.

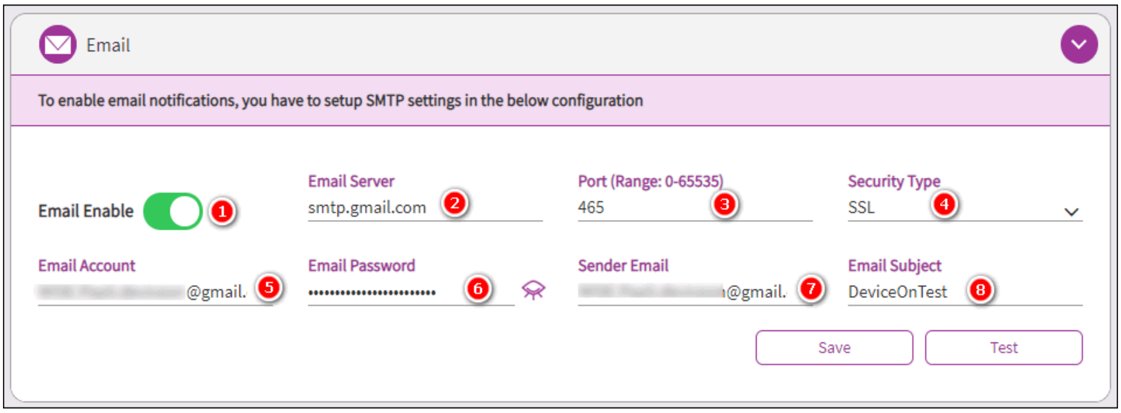


To enable email notifications, you have to setup SMTP settings in the below configuration

Email Enable
Email Server:
Port (Range: 0-65535): 25
Security Type: NONE
Email Account:
Email Password:
Sender Email:
Email Subject: DeviceOn

Step 2: 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.

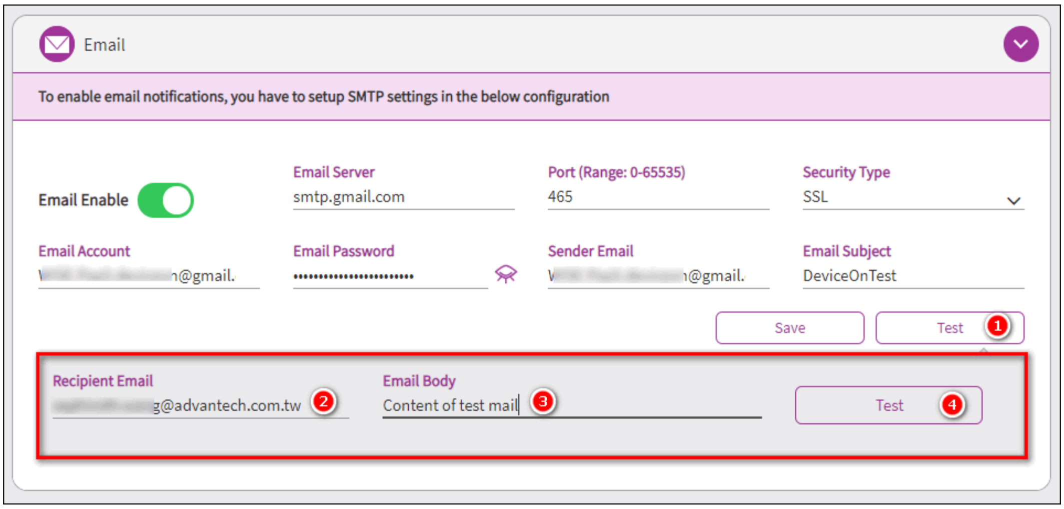


To enable email notifications, you have to setup SMTP settings in the below configuration

Email Enable
Email Server: smtp.gmail.com
Port (Range: 0-65535): 465
Security Type: SSL
Email Account: [redacted]@gmail.
Email Password: ••••••••••••••••••••••••
Sender Email: [redacted]@gmail.
Email Subject: DeviceOnTest

Step 3: 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.



Email

To enable email notifications, you have to setup SMTP settings in the below configuration

Email Enable

Email Server: smtp.gmail.com

Port (Range: 0-65535): 465

Security Type: SSL

Email Account: [redacted]@gmail.

Email Password: ••••••••••••••••••••••••

Sender Email: [redacted]@gmail.

Email Subject: DeviceOnTest

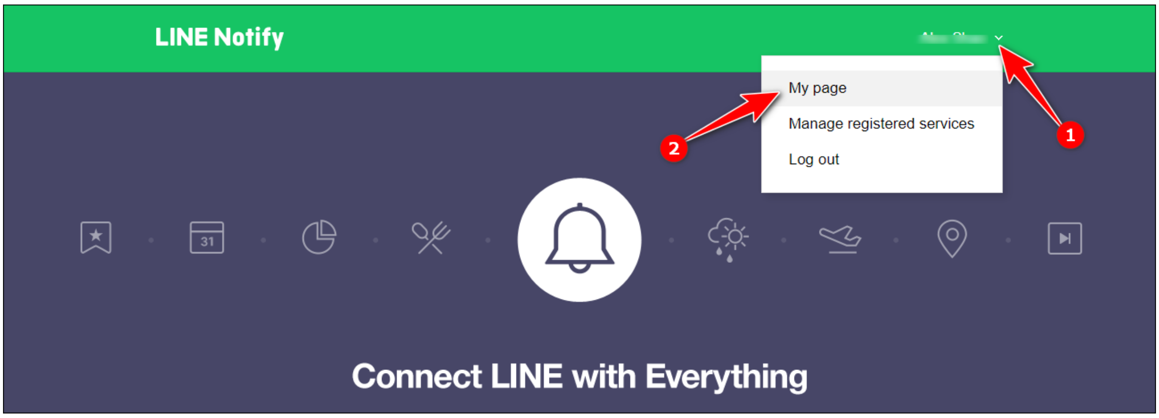
Recipient Email: [redacted]g@advantech.com.tw

Email Body: Content of test mail

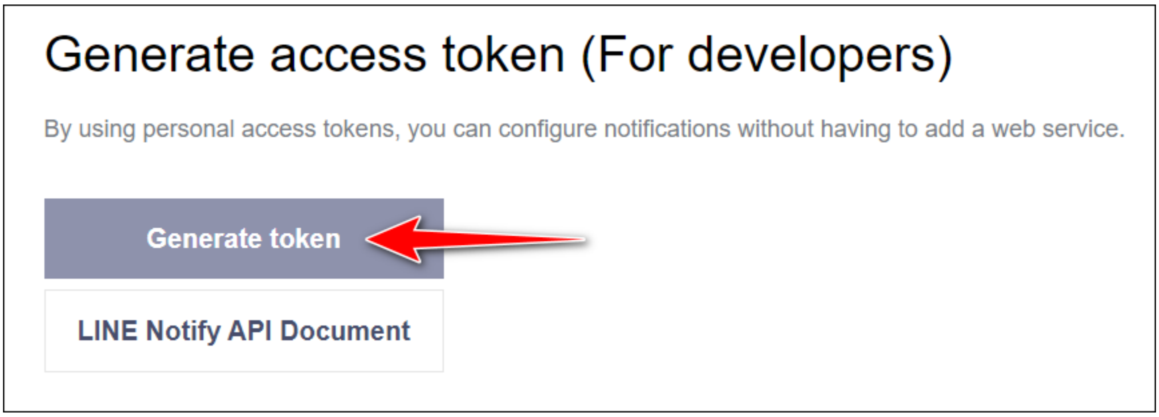
Step 4: Click **“Save”** on the bottom right of the page that shows in step 2 to keep all settings and enable email notification service.

4.4.3 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.



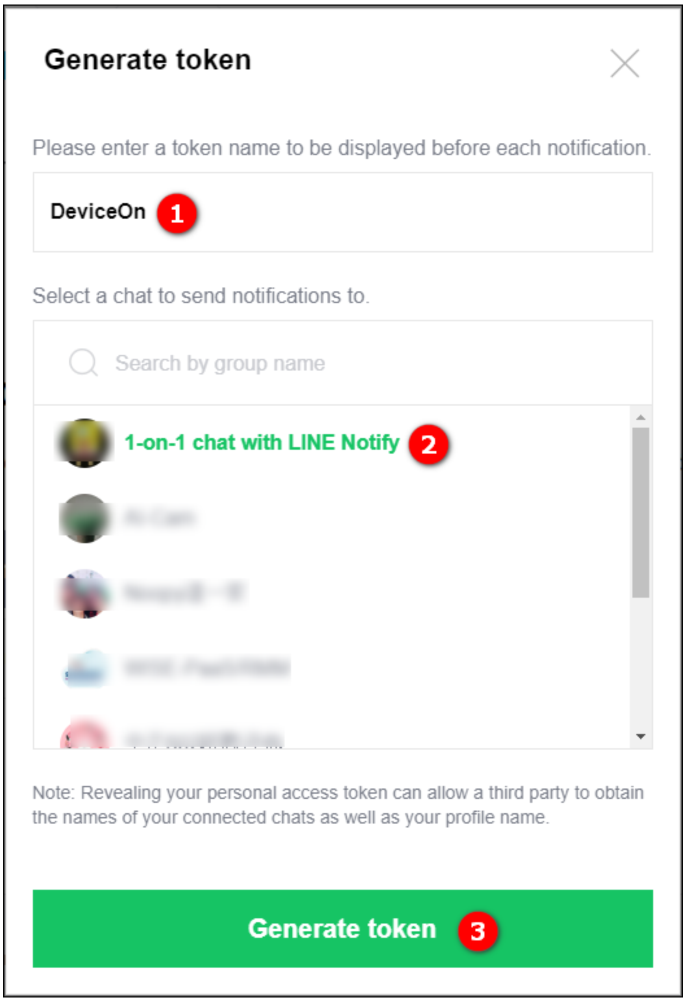
Step 2: Click **“Generate token”** under **“Generate access token (For developers)”**. It pops up the **“Generate token”** dialog.



Generate access token (For developers)

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

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

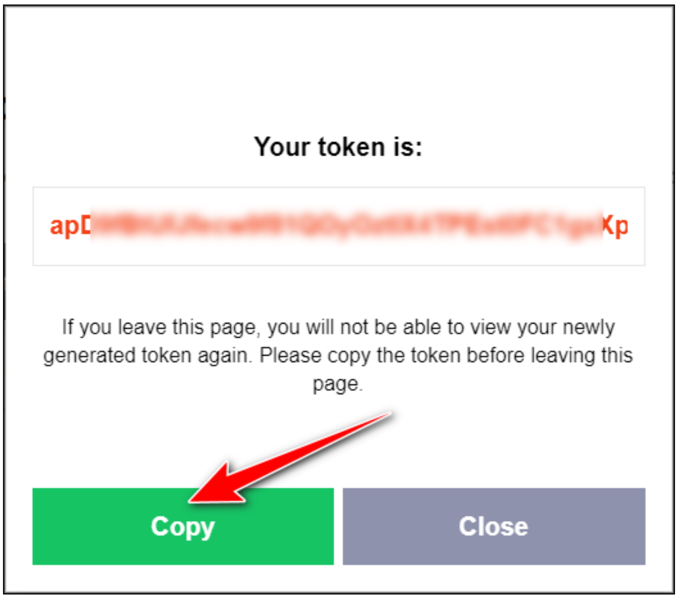
Please enter a token name to be displayed before each notification.

DeviceOn 1

Select a chat to send notifications to.

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.

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.

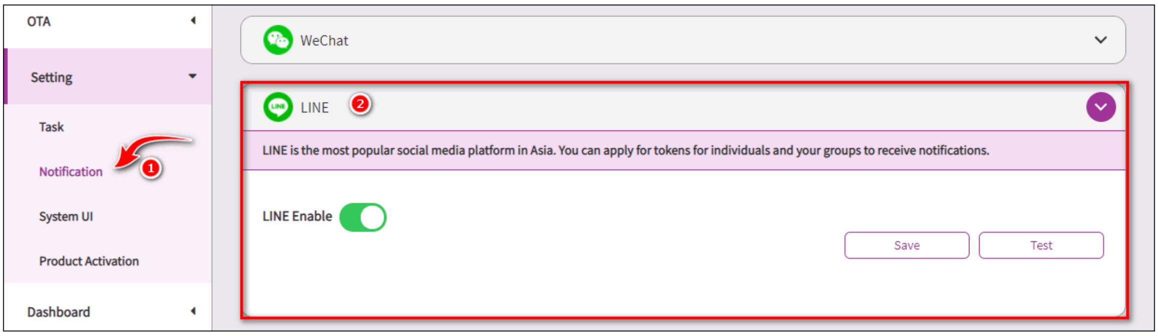


Your token is:

apD[redacted]Xp

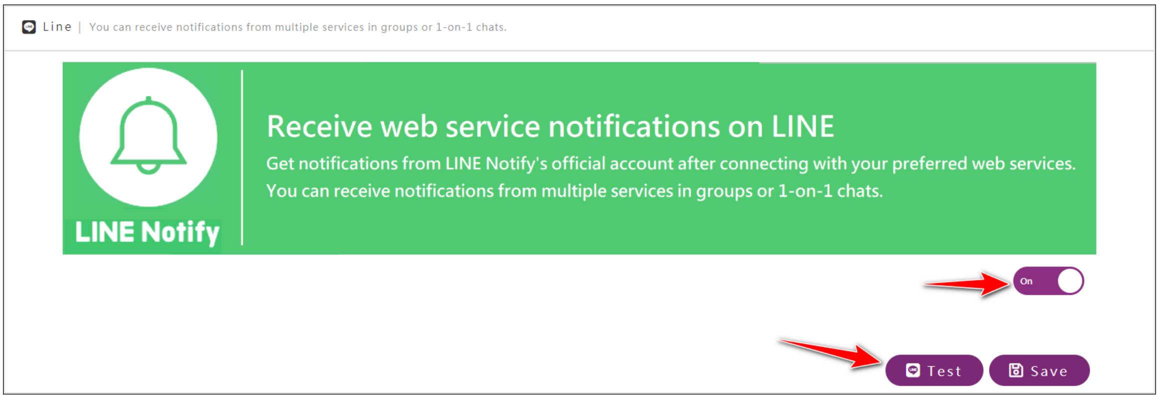
If you leave this page, you will not be able to view your newly generated token again. Please copy the token before leaving this page.

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.



LINE is the most popular social media platform in Asia. You can apply for tokens for individuals and your groups to receive notifications.

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

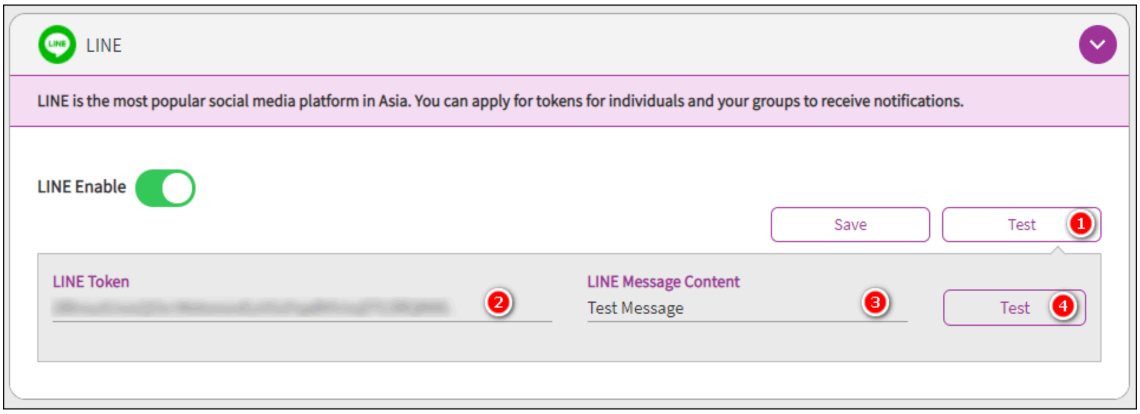


Line | You can receive notifications from multiple services in groups or 1-on-1 chats.

Receive web service notifications on LINE

Get notifications from LINE Notify's official account after connecting with your preferred web services. You can receive notifications from multiple services in groups or 1-on-1 chats.

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.



LINE is the most popular social media platform in Asia. You can apply for tokens for individuals and your groups to receive notifications.

LINE Enable

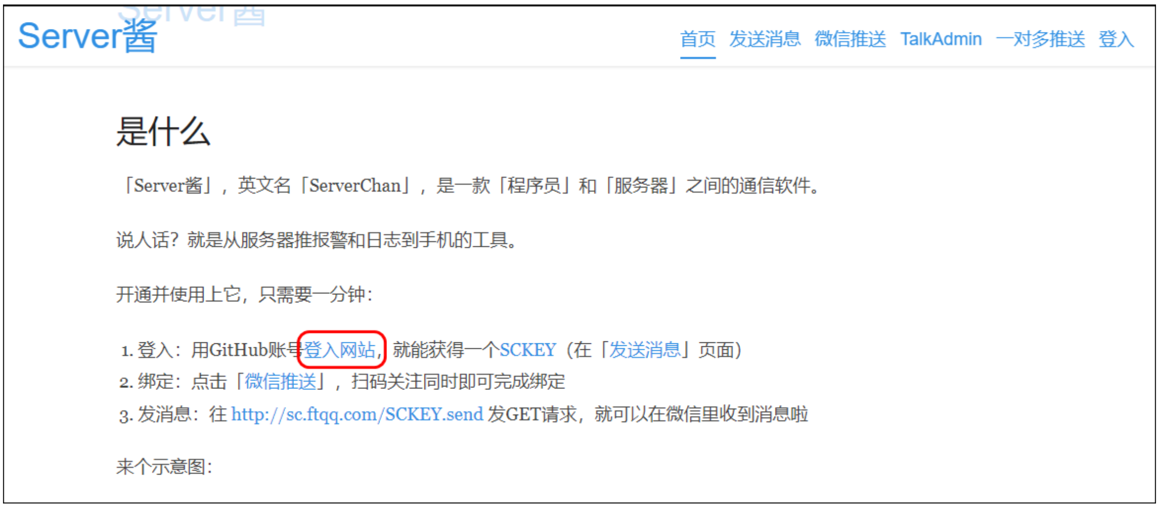
LINE Token: [redacted]

LINE Message Content: Test Message

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

4.4.4 Steps to Set Event Notification Service – WeChat

Step 1: Go to http://sc.ftqq.com/3.version. Click "登入网站" hyperlink.



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。

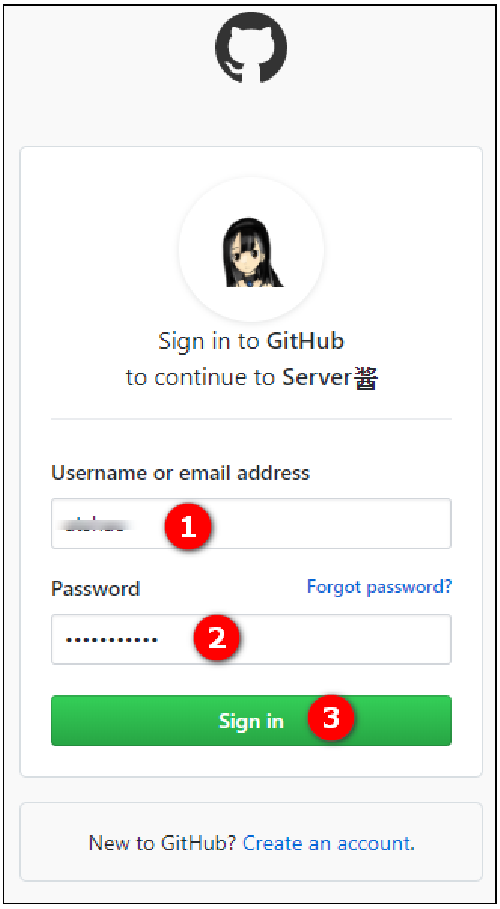
说人话？就是从服务器推报警和日志到手机的工具。

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.



Sign in to GitHub
to continue to Server酱

Username or email address

[redacted]

Password

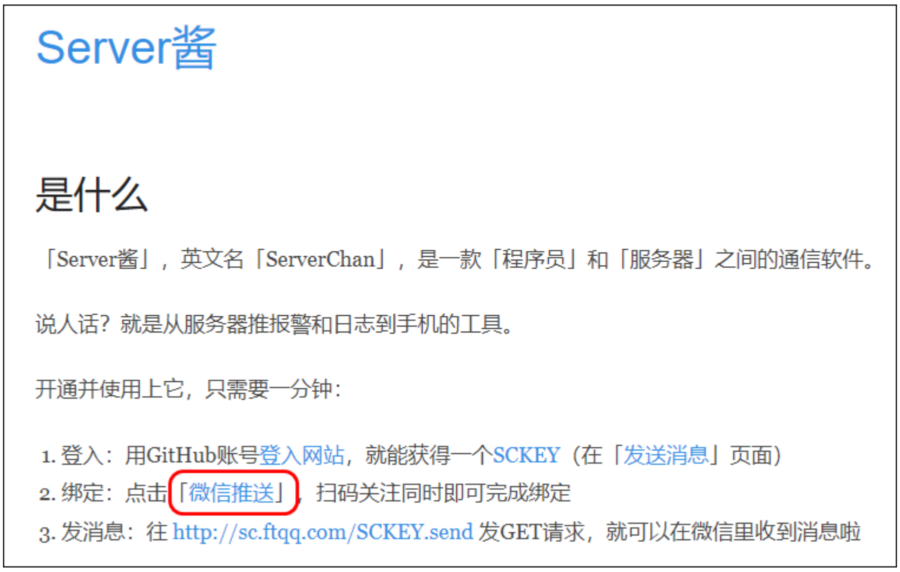
Forgot password?

•••••••••••

Sign in

New to GitHub? Create an account.

Step 3: Click “微信推送” hyperlink.



Server酱

是什么

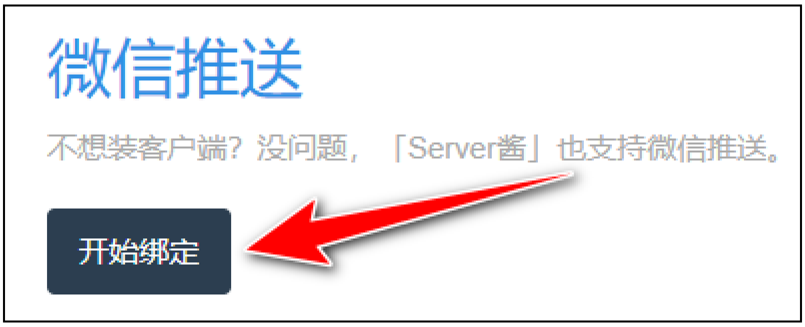
「Server酱」，英文名「ServerChan」，是一款「程序员」和「服务器」之间的通信软件。

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

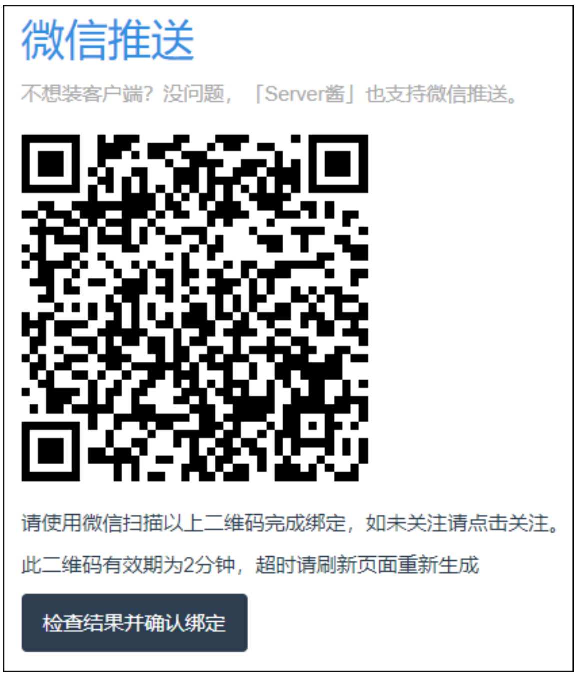
Step 4: Click “开始绑定”. It opens a QR code image.



微信推送

不想装客户端？没问题，「Server酱」也支持微信推送。

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.



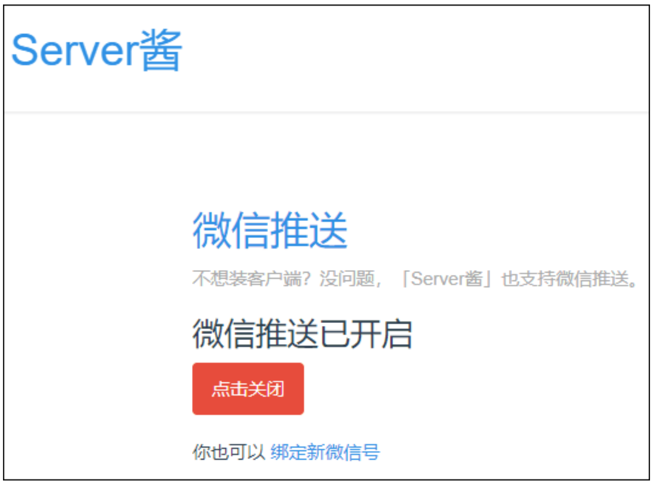
微信推送

不想装客户端？没问题，「Server酱」也支持微信推送。

请使用微信扫描以上二维码完成绑定，如未关注请点击关注。

此二维码有效期为2分钟，超时请刷新页面重新生成

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



Server酱

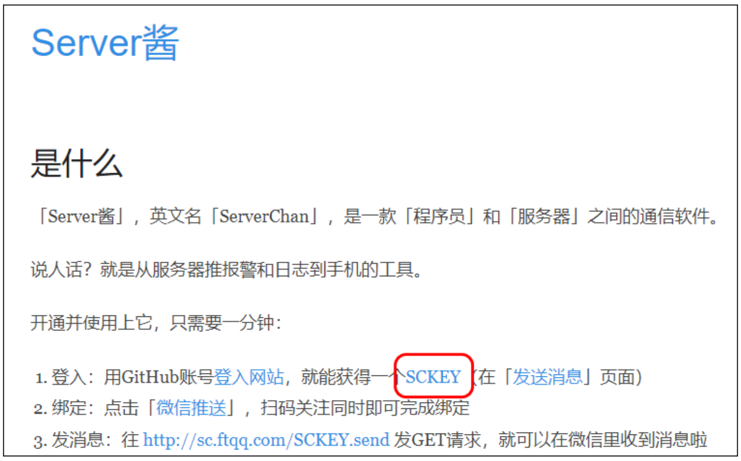
微信推送

不想装客户端？没问题，「Server酱」也支持微信推送。

微信推送已开启

你也可以 绑定新微信号

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



Server酱

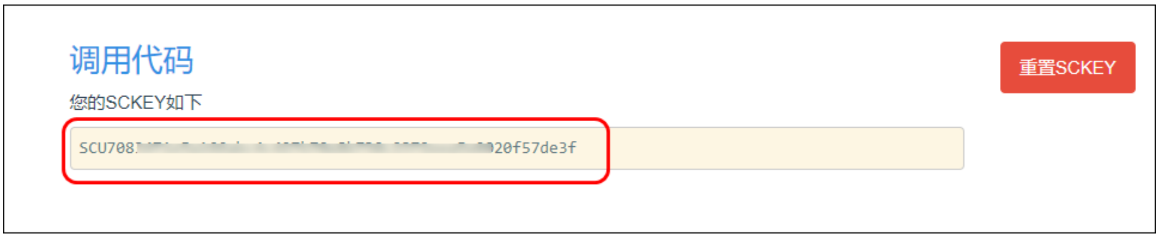
是什么

「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

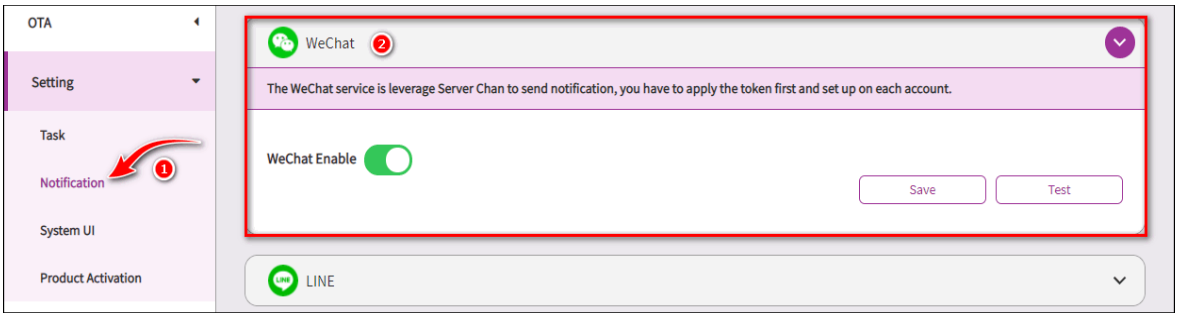


调用代码

您的SCKEY如下

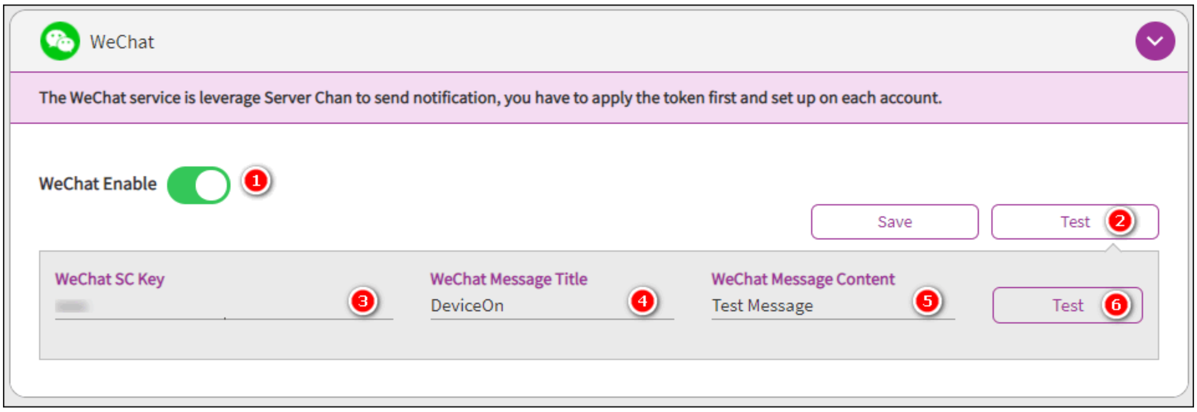
SCU708[redacted]020f57de3f

Step 8: Now switch your browser to DeviceOn portal. Click **“Setting”** menu on the left-hand side, then **“Notification”**, and **“WeChat”** to open settings regarding WeChat event notification service.



The WeChat service is leverage Server Chan to send notification, you have to apply the token first and set up on each account.

Step 9: Toggle **“On/Off”** switch to enable this feature. Click **“Test”** to show the test dialog up. 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.



The WeChat service is leverage Server Chan to send notification, you have to apply the token first and set up on each account.

WeChat Enable

WeChat SC Key: [redacted]

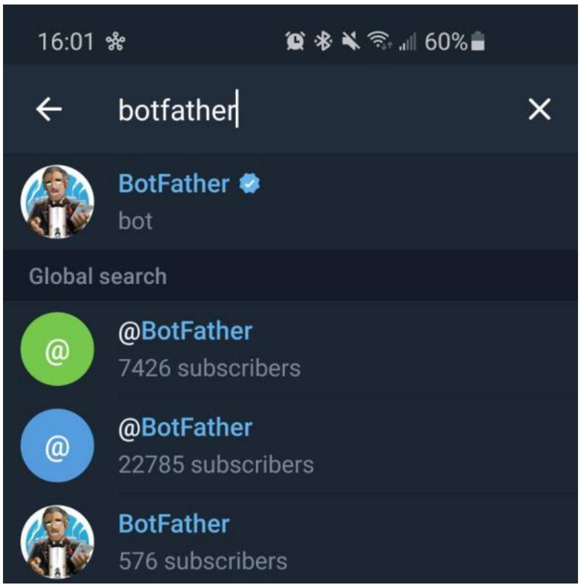
WeChat Message Title: DeviceOn

WeChat Message Content: Test Message

Step 10: Click **"Save"** button that shows in step 9 to keep your settings and enable WeChat event notification service.

4.4.5 Steps to Set Event Notification Service – Telegram

Step 1: Search "BotFather" and start to chat on your Telegram App.

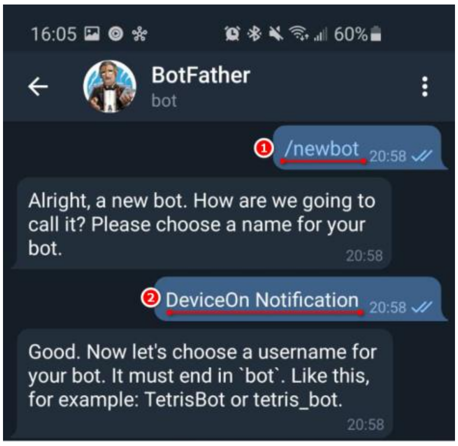


Step 2: Create a new bot and generate an **authorization token**.

Use the **/newbot** command to create a new bot. The BotFather will ask you for a name and username, then generate an authorization token for your new bot. The name of your bot is displayed in contact details and elsewhere.

The Username is a short name, to be used in mentions and t.me links. Usernames are 5-32 characters long and are case insensitive, but may only include Latin characters, numbers, and underscores. Your bot's username must end in '**bot**', e.g. 'tetris_bot' or 'TetrisBot'.

The token is a string along the lines of 110201543:AAHdqTcvCH1vGWJxfSeofSAs0K5PALDsaw that is required to authorize the bot and send requests to the Bot API. Keep your token secure and store it safely, it can be used by anyone to control your bot.

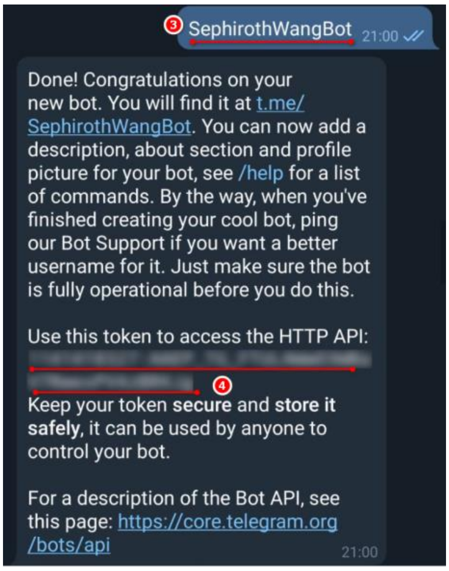


1 /newbot 20:58

Alright, a new bot. How are we going to call it? Please choose a name for your bot. 20:58

2 DeviceOn Notification 20:58

Good. Now let's choose a username for your bot. It must end in `bot`. Like this, for example: TetrisBot or tetris_bot. 20:58



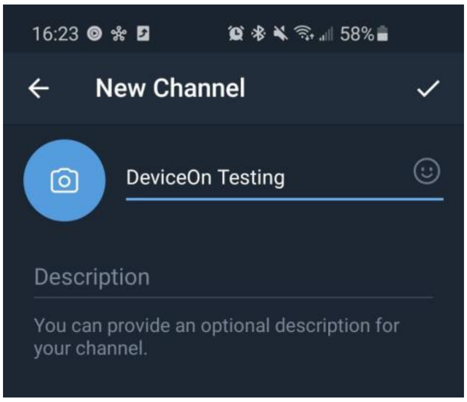
3 SephirothWangBot 21:00

Done! Congratulations on your new bot. You will find it at t.me/SephirothWangBot. You can now add a description, about section and profile picture for your bot, see /help for a list of commands. By the way, when you've finished creating your cool bot, ping our Bot Support if you want a better username for it. Just make sure the bot is fully operational before you do this.

Use this token to access the HTTP API:
[redacted] 4
Keep your token **secure** and **store it safely**, it can be used by anyone to control your bot.

For a description of the Bot API, see this page: https://core.telegram.org/bots/api 21:00

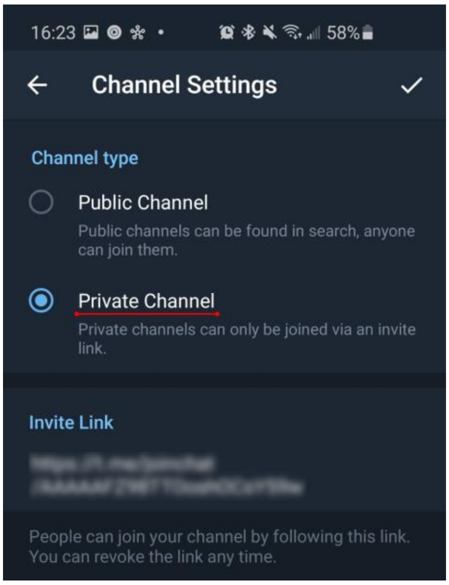
Step 2: Create your private channel on Telegram



DeviceOn Testing

Description

You can provide an optional description for your channel.



Channel type

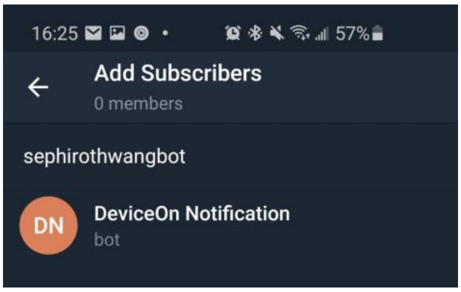
○ Public Channel
Public channels can be found in search, anyone can join them.

● Private Channel
Private channels can only be joined via an invite link.

Invite Link
[redacted]

People can join your channel by following this link. You can revoke the link any time.

Step 3: Invite your bot into the channel.

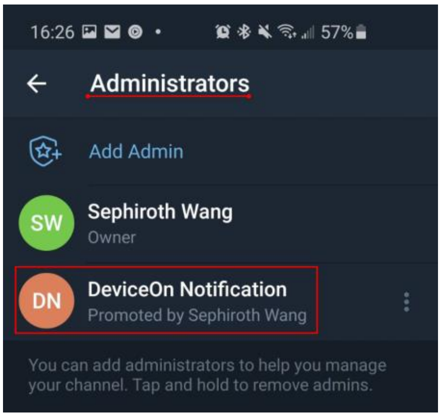


Add Subscribers
0 members

sephirothwangbot

DN DeviceOn Notification
bot

Step 4: Set your bot as “**Administrators**”



16:26 57%

Administrators

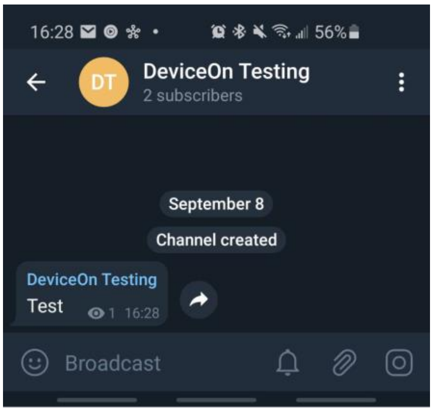
Add Admin

SW Sephiroth Wang
Owner

DN DeviceOn Notification
Promoted by Sephiroth Wang

You can add administrators to help you manage your channel. Tap and hold to remove admins.

Step 5: Enter any txt message in the channel.



16:28 56%

DT DeviceOn Testing
2 subscribers

September 8

Channel created

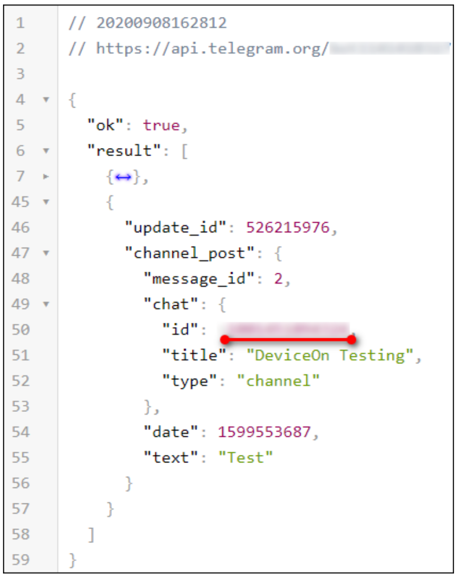
DeviceOn Testing
Test 1 16:28

Broadcast

Step 6: Retrieve the **chat id** via below URL with your authorization token (Step 2).

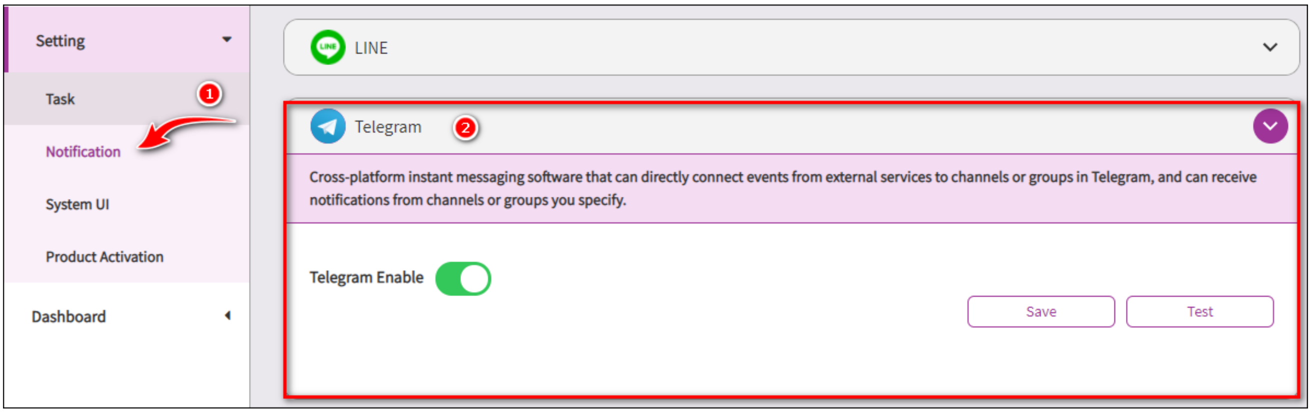
⇨ https://api.telegram.org/bot**TOKEN**/getUpdates

The response that include your chat id as below example.



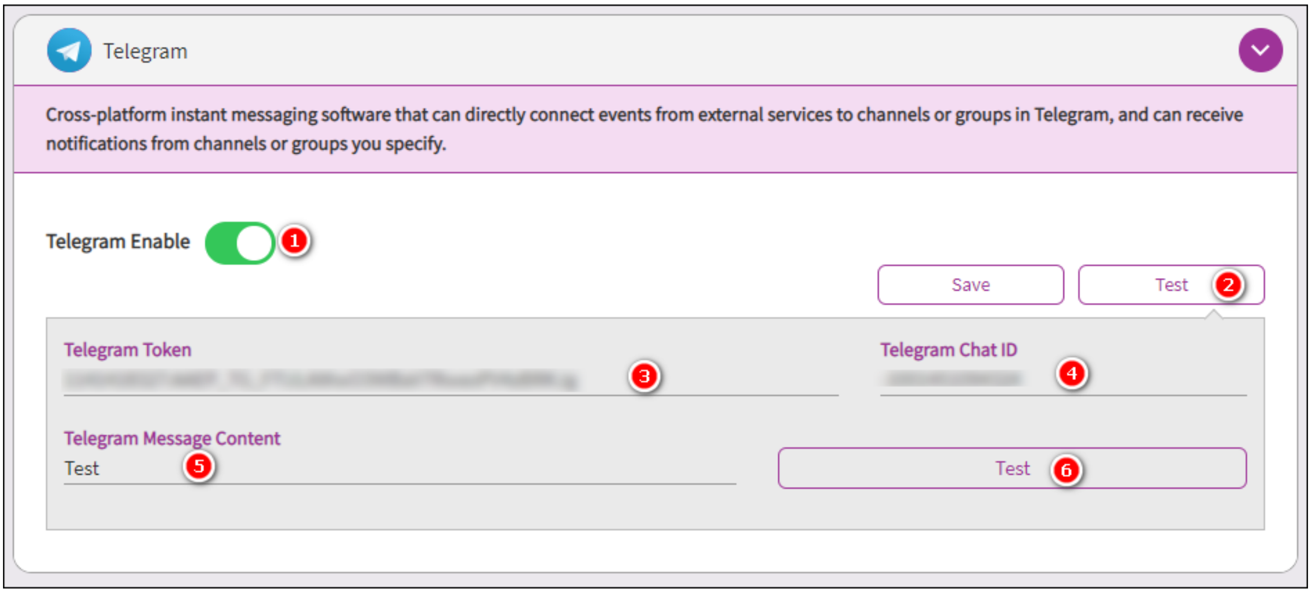
```
// 20200908162812
// https://api.telegram.org/[redacted]

{
  "ok": true,
  "result": [
    {↔},
    {
      "update_id": 526215976,
      "channel_post": {
        "message_id": 2,
        "chat": {
          "id": [redacted]
          "title": "DeviceOn Testing",
          "type": "channel"
        },
        "date": 1599553687,
        "text": "Test"
      }
    }
  ]
}
```

Step 7: Now switch your browser to DeviceOn portal. Click **"Setting"** menu on the left-hand side, then **"Notification"**, and **"Telegram"** to open settings regarding Telegram event notification service.



Cross-platform instant messaging software that can directly connect events from external services to channels or groups in Telegram, and can receive notifications from channels or groups you specify.

Step 8: Toggle **"On/Off"** switch to enable this feature. Click **"Test"** to show the test dialog up. Paste the copied Token and chat id, copied in step 2 and step 6. Give a title to the second field **"Telegram Message Content"**. Write some message content to the last field **"Test"**. And click **"Test"** to see if it works or not.



Cross-platform instant messaging software that can directly connect events from external services to channels or groups in Telegram, and can receive notifications from channels or groups you specify.

Telegram Token: [redacted]

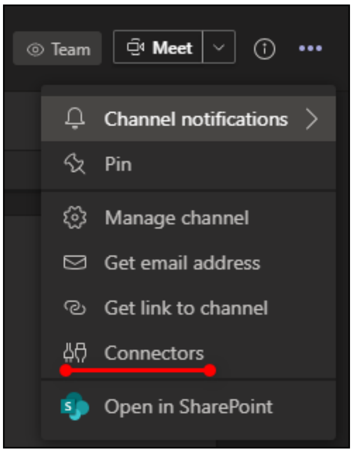
Telegram Chat ID: [redacted]

Telegram Message Content: Test

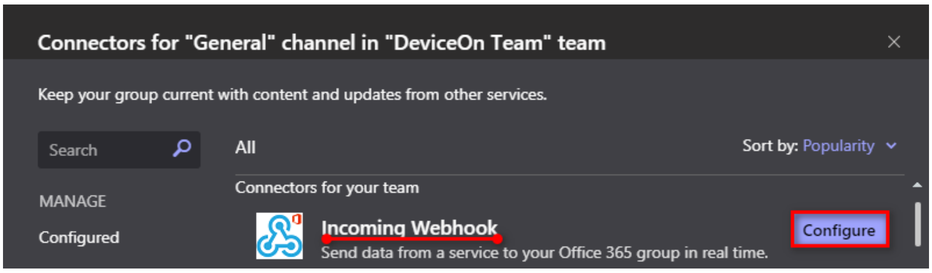
Step 10: Click **"Save"** button that shows in step 8 to keep your settings and enable Telegram event notification service.

4.4.6 Steps to Set Event Notification Service – Microsoft Teams

Step 1: In the function menu of the channel where you want to send the message, select...(Other), and select the connector in the menu.

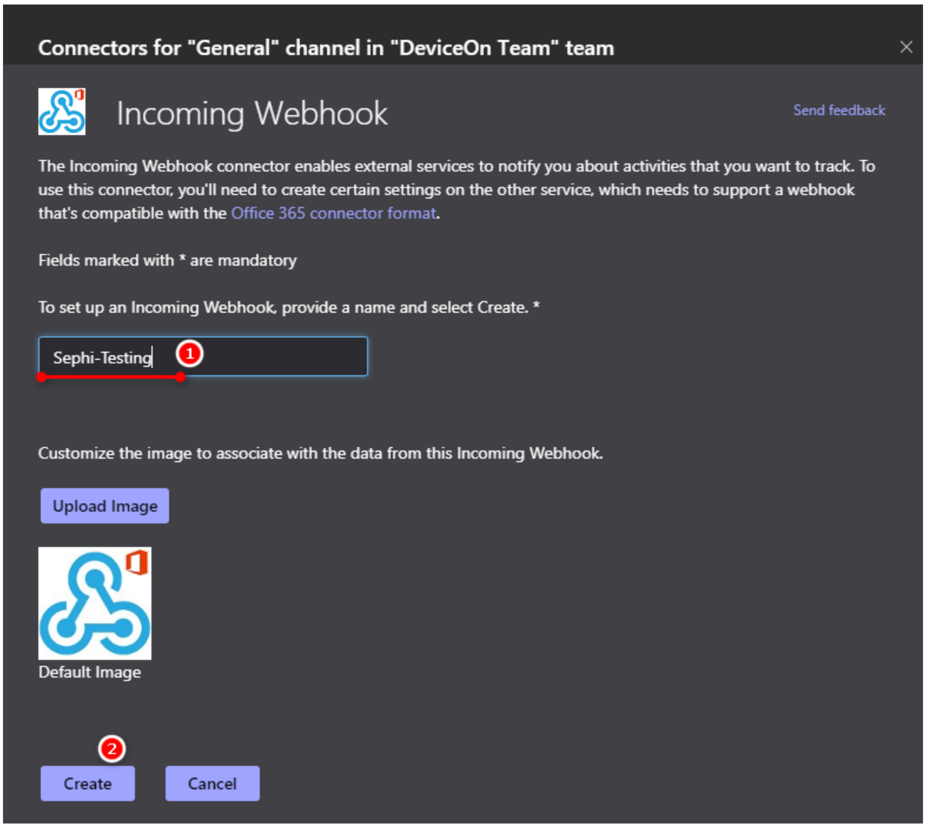


Step 2: Select “Incoming Webhook”


Connectors for "General" channel in "DeviceOn Team" team

Keep your group current with content and updates from other services.

Step 3: Give this connector a name, then press the create button


Connectors for "General" channel in "DeviceOn Team" team

Incoming Webhook

Send feedback

The Incoming Webhook connector enables external services to notify you about activities that you want to track. To use this connector, you'll need to create certain settings on the other service, which needs to support a webhook that's compatible with the Office 365 connector format.

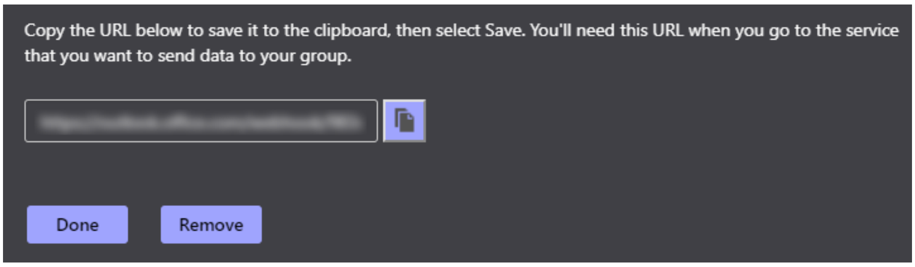
Fields marked with * are mandatory

To set up an Incoming Webhook, provide a name and select Create. *

Sephi-Testing

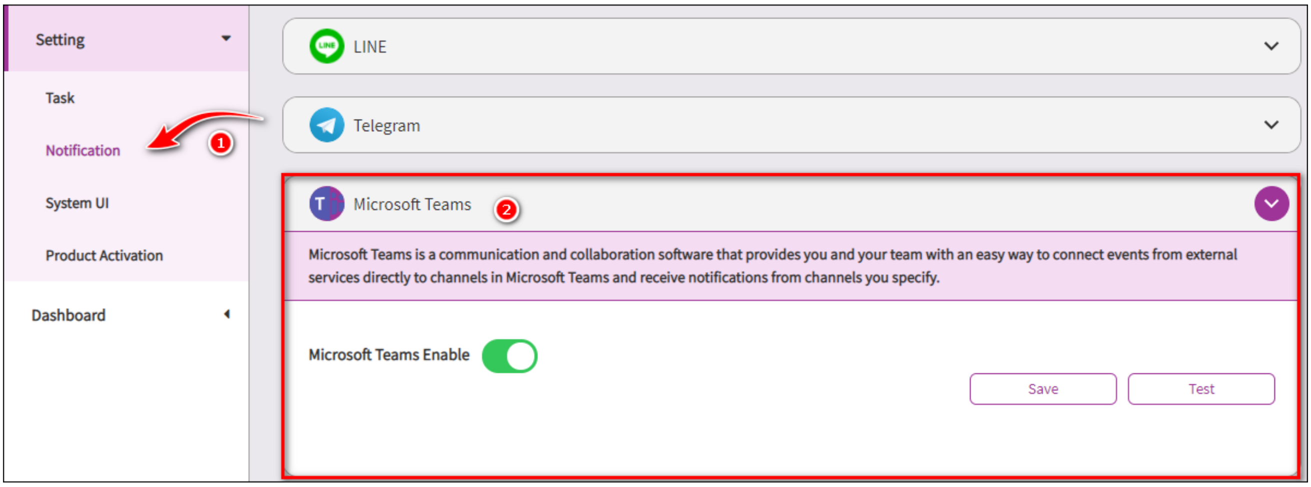
Customize the image to associate with the data from this Incoming Webhook.

Step 4: At this time, a set of URLs will appear, which are used to transfer message. After copying, press the “**Done**” button.



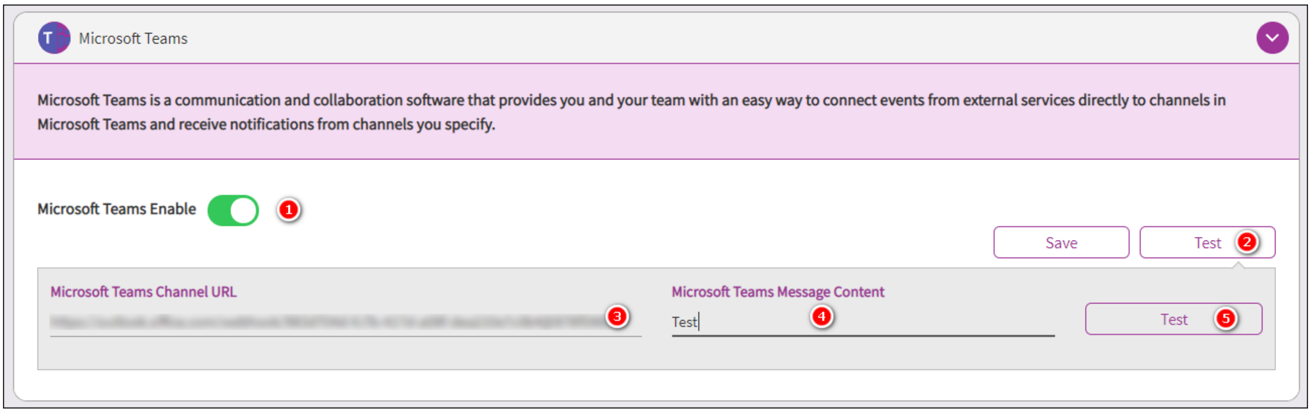
Copy the URL below to save it to the clipboard, then select Save. You'll need this URL when you go to the service that you want to send data to your group.

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



Microsoft Teams is a communication and collaboration software that provides you and your team with an easy way to connect events from external services directly to channels in Microsoft Teams and receive notifications from channels you specify.

Step 6: Toggle **“On/Off”** switch to enable this feature. Click **“Test”** to show the test dialog up. Paste the URL, copied in step 4. Give a title to the second field **“Microsoft Teams Message Content”**. Write some message content to the last field **“Test”**. And click **“Test”** to see if it works or not.

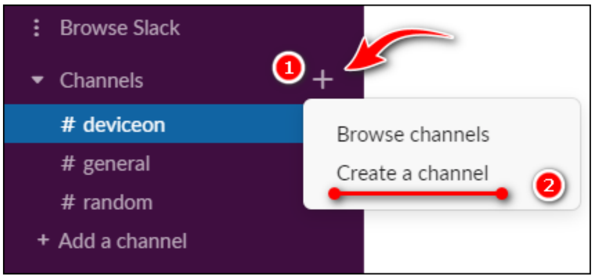


Microsoft Teams is a communication and collaboration software that provides you and your team with an easy way to connect events from external services directly to channels in Microsoft Teams and receive notifications from channels you specify.

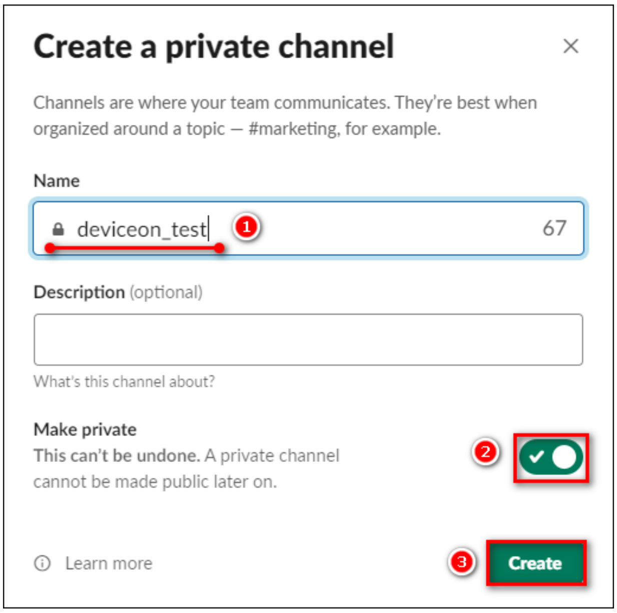
Step 7: Click **“Save”** button that shows in step 6 to keep your settings and enable Microsoft Teams event notification service.

4.4.7 Steps to Set Event Notification Service – Slack

Step 1: Create your channel on your Slack.



Step 2: Give this channel name and set as private.


Create a private channel

Channels are where your team communicates. They're best when organized around a topic — #marketing, for example.

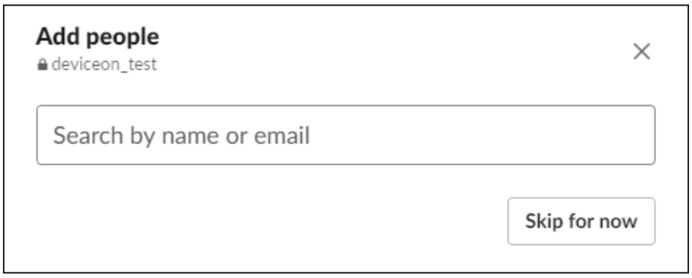
Name: deviceon_test (67)

Description (optional)

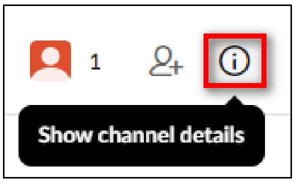
What's this channel about?

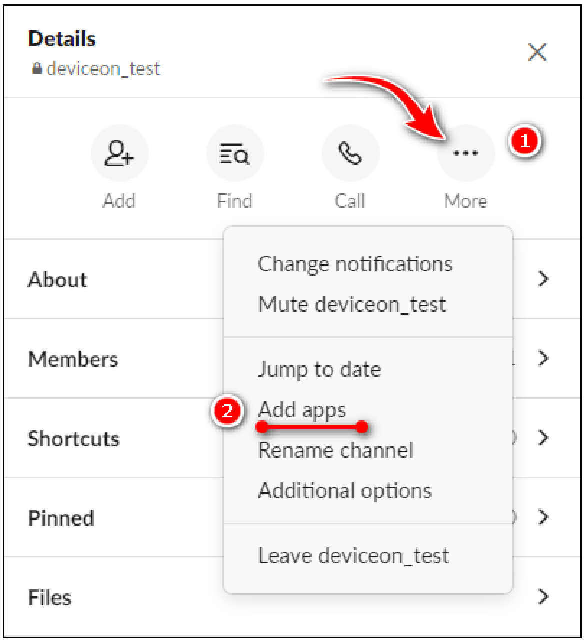
Make private
This can't be undone. A private channel cannot be made public later on.

Step 3: Skip or add your member into channel.

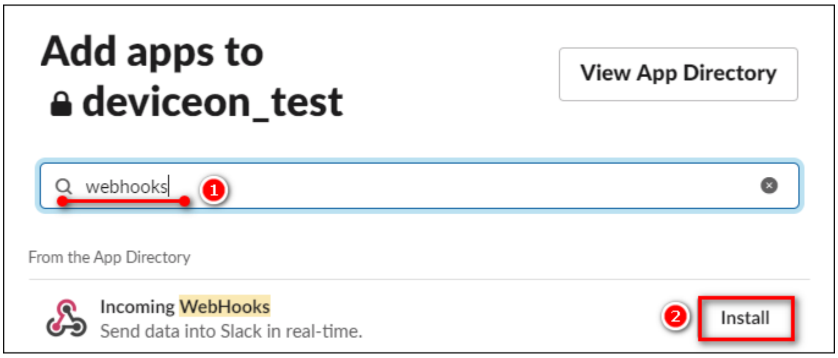

Add people
deviceon_test

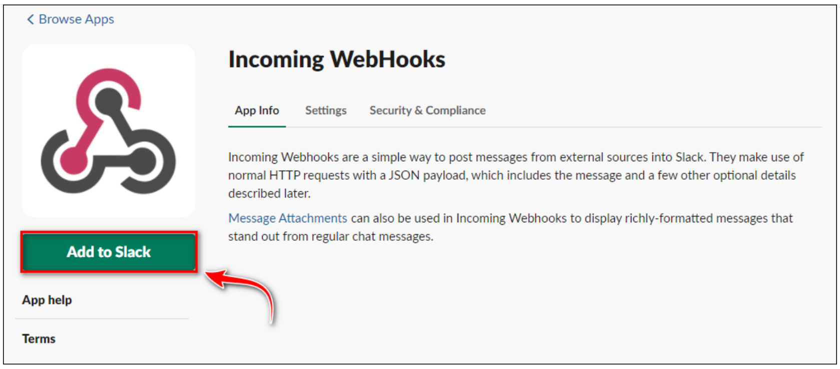
Step 4: After logging in to slack, there will be a row of menus on the right, click "**Apps**" to expand the sub-menu, and then click "**Add Apps**"





Step 5: A search box will appear, type "**webhooks**" and you will see the first result is "**Incoming WebHooks**", then click to install and “**Add to Slack**”.

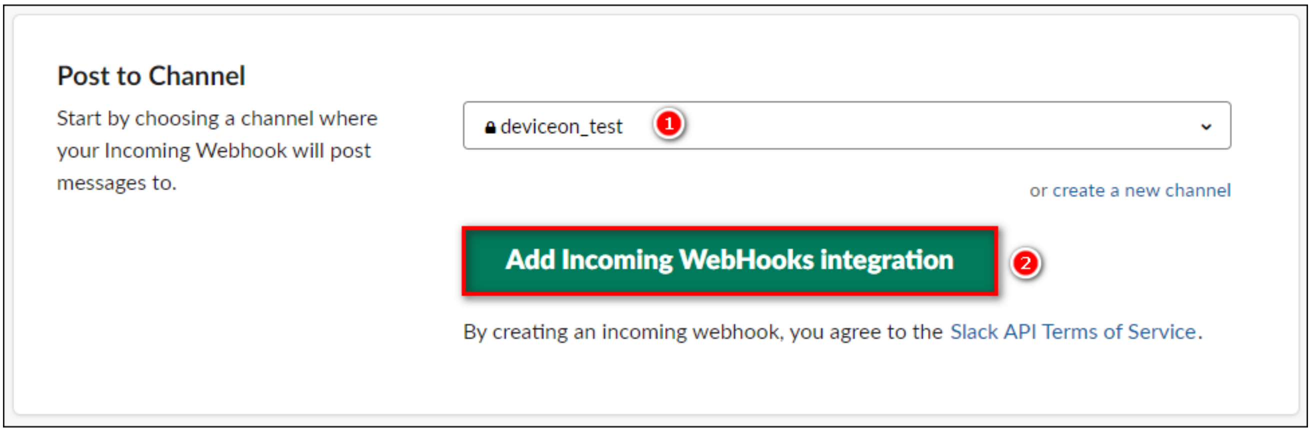




Incoming Webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details described later.

Message Attachments can also be used in Incoming Webhooks to display richly-formatted messages that stand out from regular chat messages.

Step 6: Click "**Add to Slack**", and a menu will appear asking which channel to install on. After selecting it, click "Incoming WebHooks integration".



Post to Channel

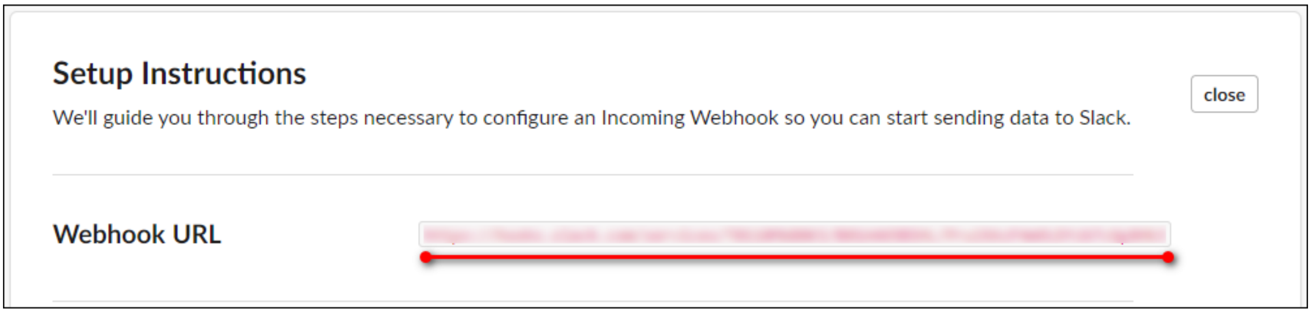
Start by choosing a channel where your Incoming Webhook will post messages to.

deviceon_test ①

or create a new channel

By creating an incoming webhook, you agree to the Slack API Terms of Service.

Step 7: After installation, you will enter the setting page of incoming webhooks. The first line of the page "**Webhook URL**" is the most important. We can send out automatic notification messages as long as we post to this url.

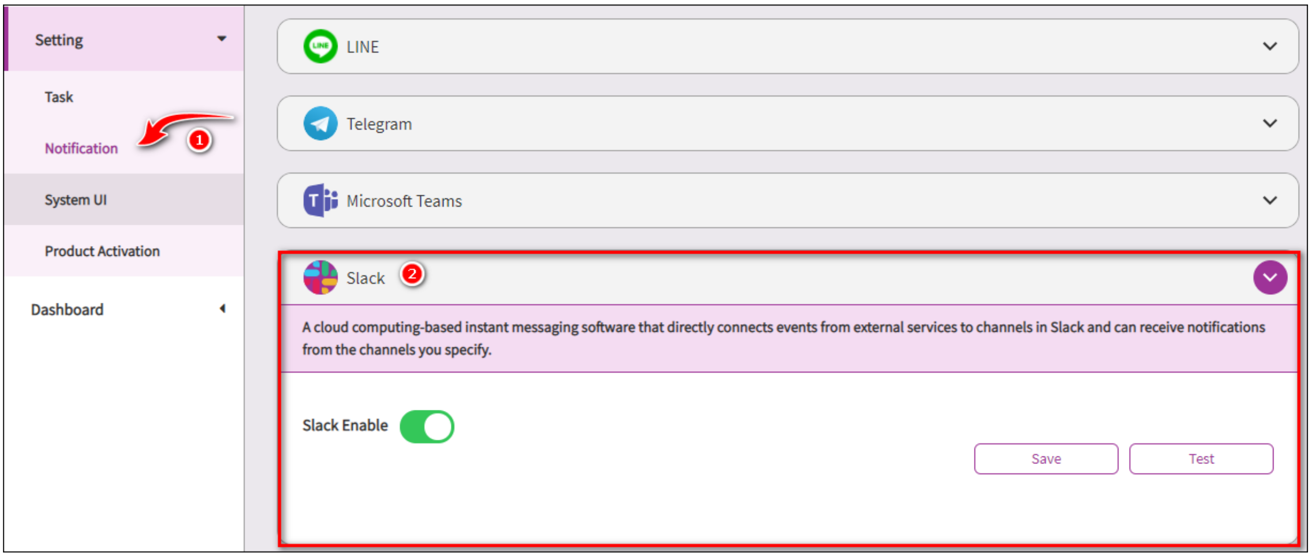


Setup Instructions

We'll guide you through the steps necessary to configure an Incoming Webhook so you can start sending data to Slack.

Webhook URL [redacted]

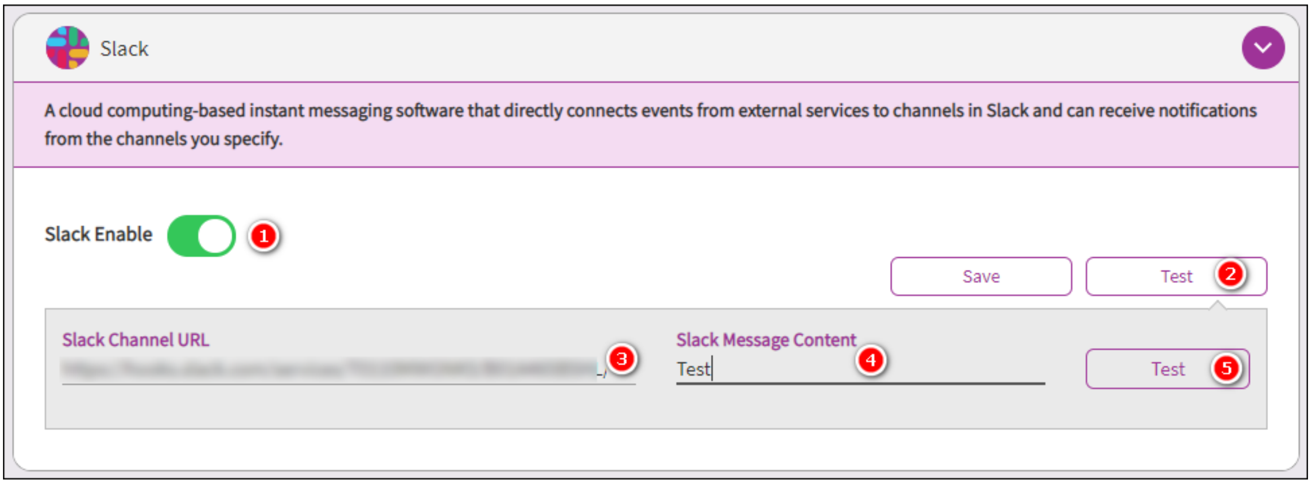
Step 8: Now switch your browser to DeviceOn portal. Click **“Setting”** menu on the left-hand side, then **“Notification”**, and **“Slack”** to open settings regarding Slack event notification service.



A cloud computing-based instant messaging software that directly connects events from external services to channels in Slack and can receive notifications from the channels you specify.

Slack Enable

Step 9: Toggle **“On/Off”** switch to enable this feature. Click **“Test”** to show the test dialog up. Paste the URL, copied in step 4. Give a title to the second field **“Slack Message Content”**. Write some message content to the last field **“Test”**. And click **“Test”** to see if it works or not.



Slack

A cloud computing-based instant messaging software that directly connects events from external services to channels in Slack and can receive notifications from the channels you specify.

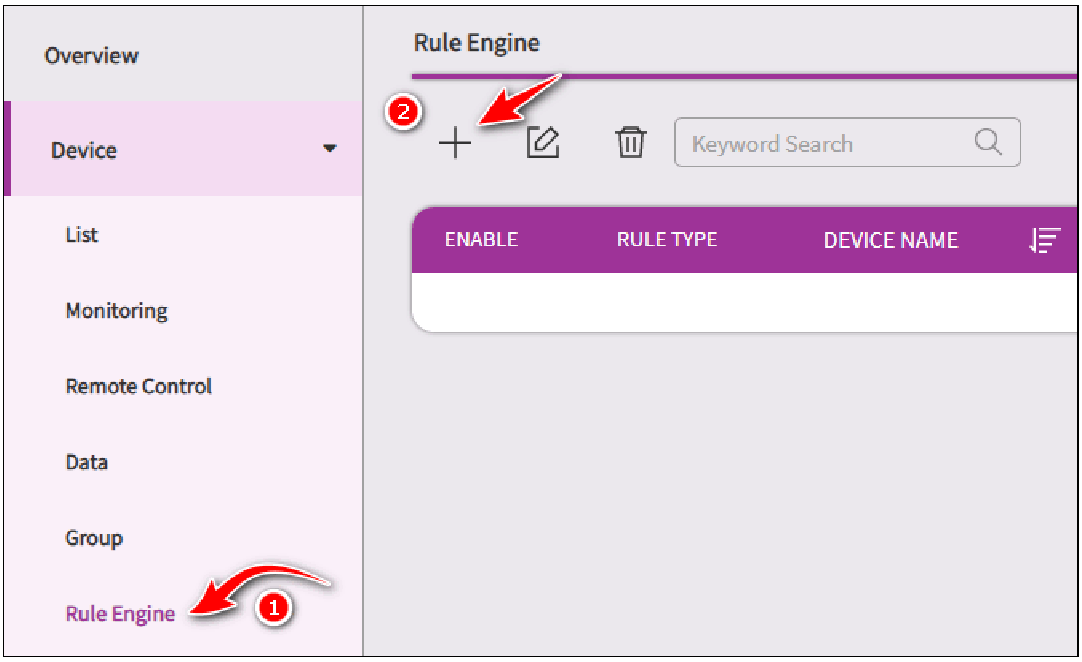
Slack Enable 1

Slack Channel URL [redacted] 3

Slack Message Content 4
Test

4.4.8 Steps to Set Thresholds to a Device

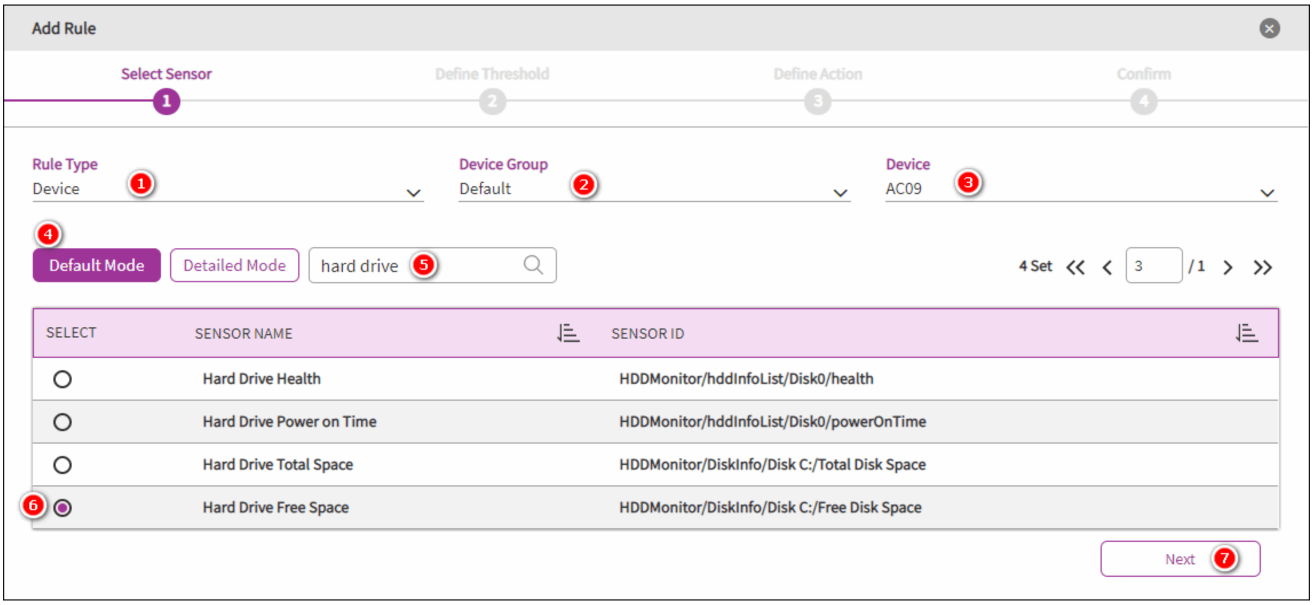
Step 1: Click **"Setting"** menu on the left-hand side of DeviceOn portal and, then, **"Rule Engine",** click the plus (+) sign to enter **"Rule Engine"** page.



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 drive"** 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.

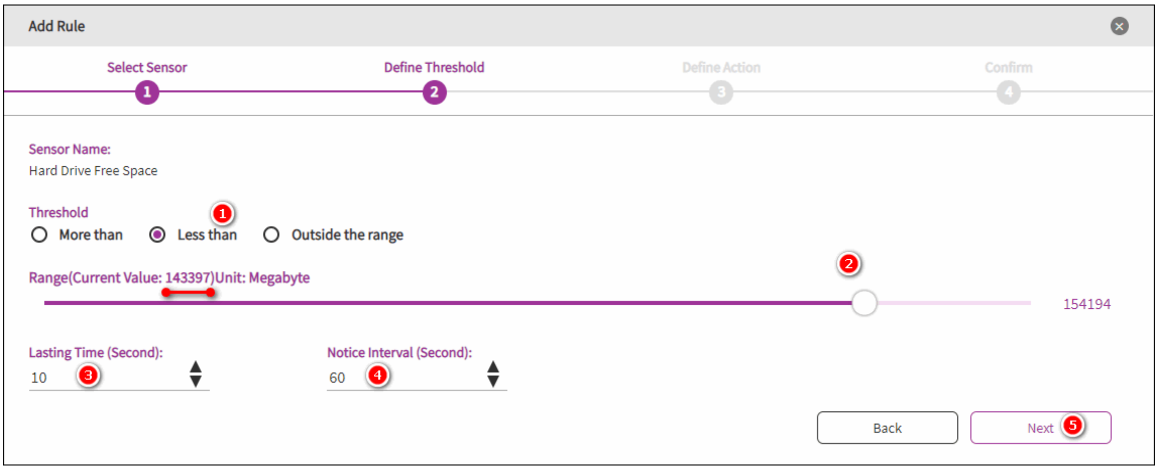


Rule Type: Device
Device Group: Default
Device: AC09
Search: hard drive

SELECT	SENSOR NAME	SENSOR ID
○	Hard Drive Health	HDDMonitor/hddInfoList/Disk0/health
○	Hard Drive Power on Time	HDDMonitor/hddInfoList/Disk0/powerOnTime
○	Hard Drive Total Space	HDDMonitor/DiskInfo/Disk C:/Total Disk Space
●	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.



Sensor Name:
Hard Drive Free Space

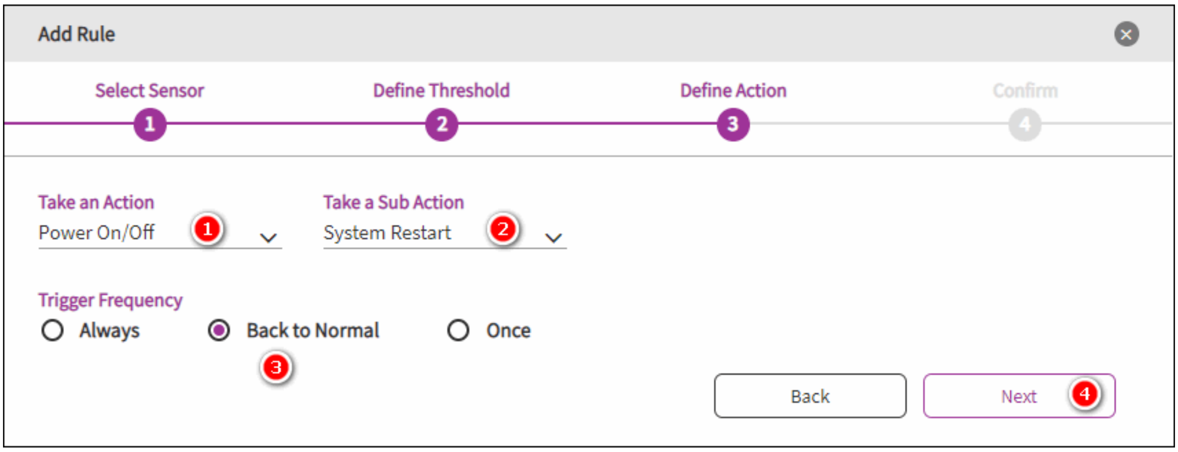
Threshold
○ More than ● Less than ○ Outside the range

Range(Current Value: 143397)Unit: Megabyte

Lasting Time (Second): 10

Notice Interval (Second): 60

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.



Add Rule

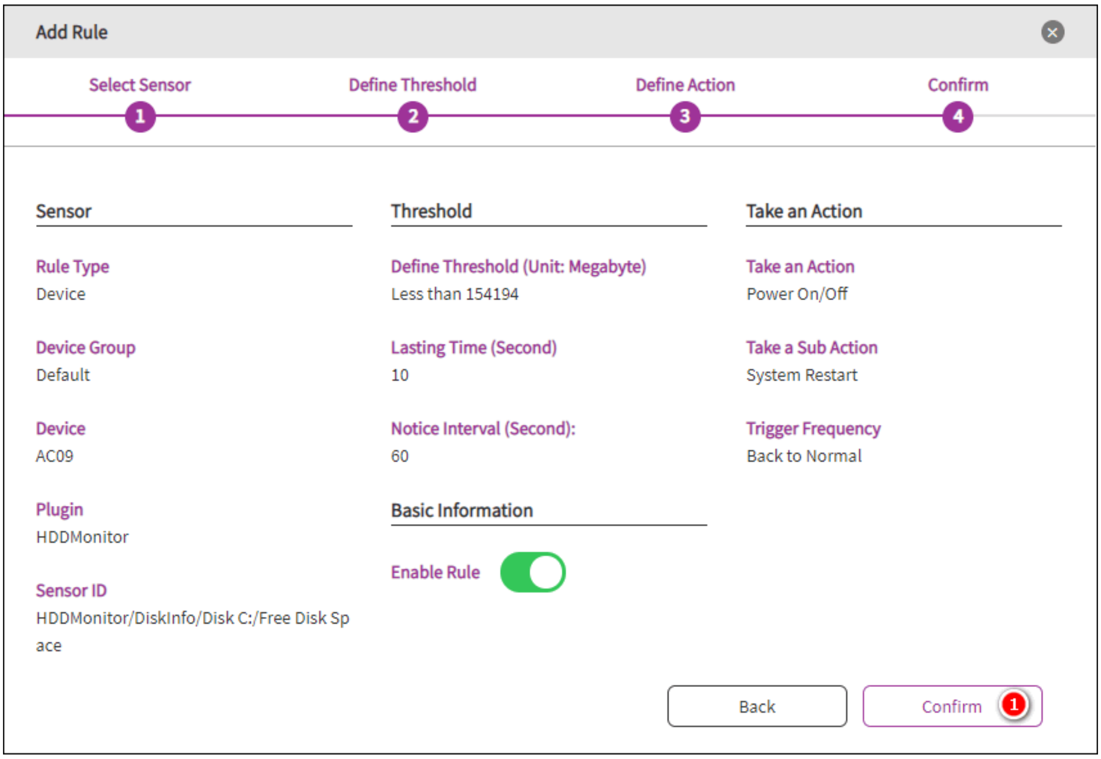
Select Sensor 1 — Define Threshold 2 — Define Action 3 — Confirm 4

Take an Action: Power On/Off 1

Take a Sub Action: System Restart 2

Trigger Frequency: ○ Always ● Back to Normal 3 ○ Once

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.



Add Rule

Select Sensor 1 — Define Threshold 2 — Define Action 3 — Confirm 4

Sensor

Rule Type: Device

Device Group: Default

Device: AC09

Plugin: HDDMonitor

Sensor ID: HDDMonitor/DiskInfo/Disk C:/Free Disk Space

Threshold

Define Threshold (Unit: Megabyte): Less than 154194

Lasting Time (Second): 10

Notice Interval (Second):: 60

Basic Information

Enable Rule: ●

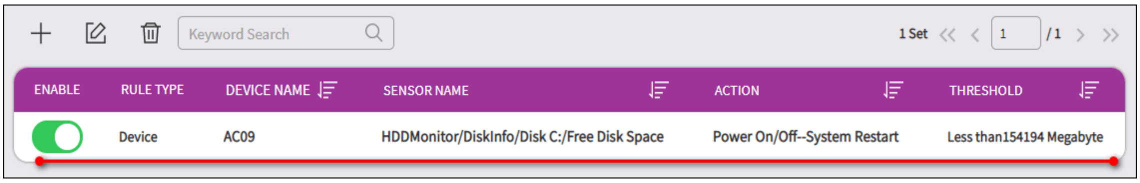
Take an Action

Take an Action: Power On/Off

Take a Sub Action: System Restart

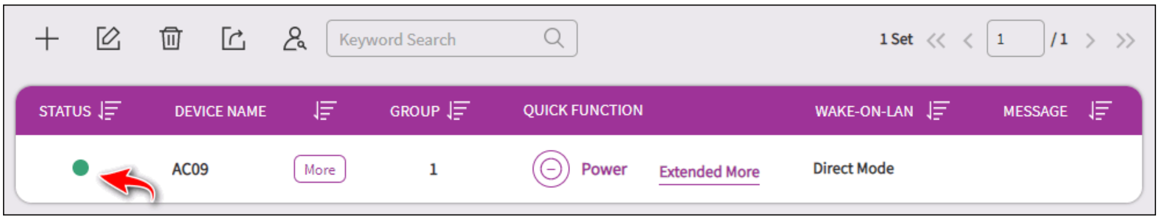
Trigger Frequency: Back to Normal

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



ENABLE	RULE TYPE	DEVICE NAME	SENSOR NAME	ACTION	THRESHOLD
●	Device	AC09	HDDMonitor/DiskInfo/Disk C:/Free Disk Space	Power On/Off--System Restart	Less than154194 Megabyte

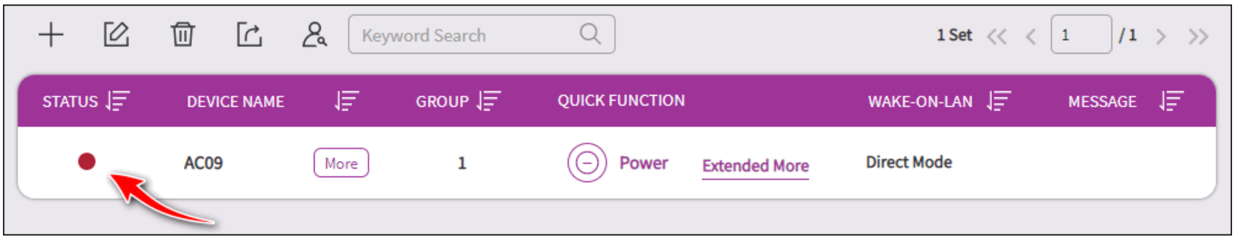
Step 9: Click **"Device"** menu item on left hand side of DeviceOn portal. You can see a green circle represents the target device accordingly.



Keyword Search | 1 Set | 1 | /1

STATUS	DEVICE NAME		GROUP	QUICK FUNCTION		WAKE-ON-LAN	MESSAGE
●	AC09	More	1	Power	Extended More	Direct Mode	

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.



Keyword Search | 1 Set | 1 | /1

STATUS	DEVICE NAME		GROUP	QUICK FUNCTION		WAKE-ON-LAN	MESSAGE
●	AC09	More	1	Power	Extended More	Direct Mode	

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.

4.5 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.

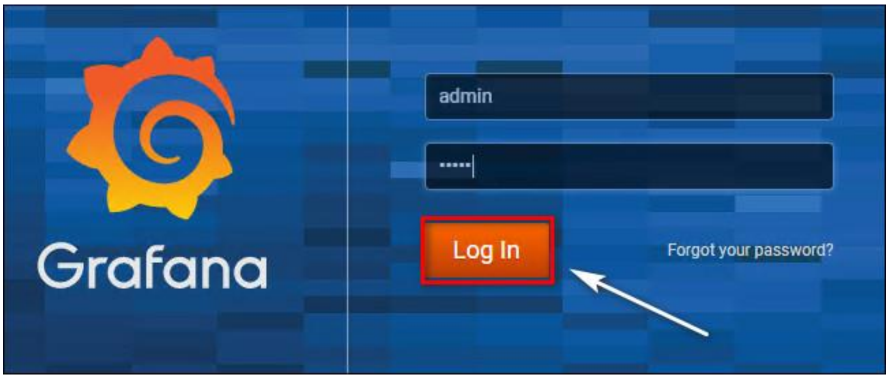
4.5.1 Prerequisite

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

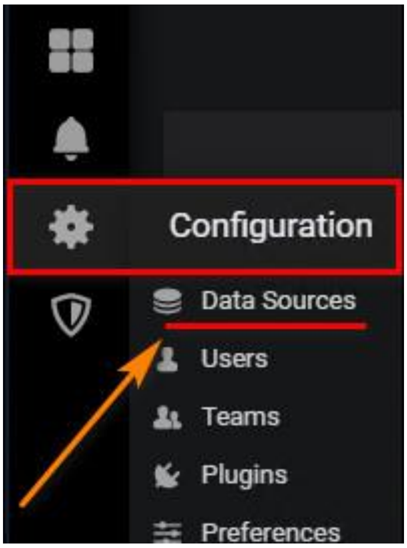
4.5.2 Step-by-Step

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

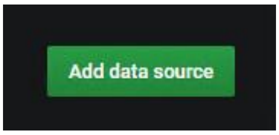
Step 2: Login to Grafana portal with your account, password (Default: admin/admin)

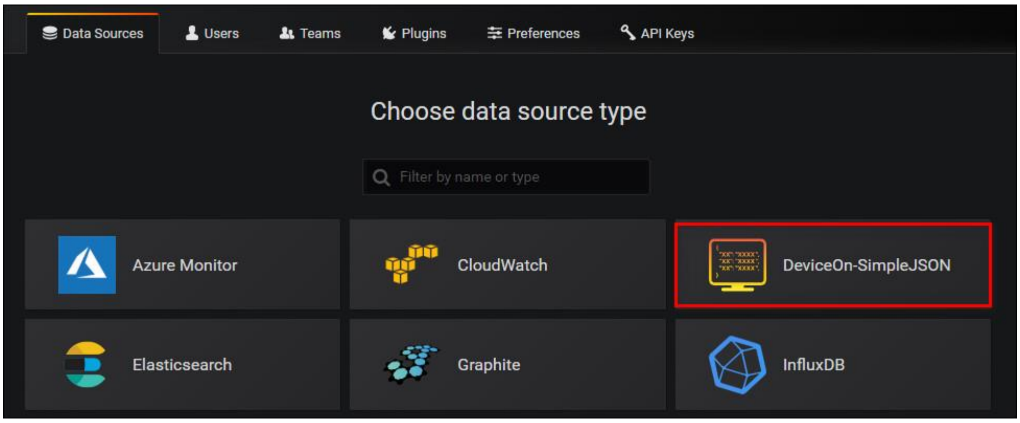


Step 3: Create a data source to access DeviceOn SimpleJson API.



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





Choose data source type

Filter by name or type

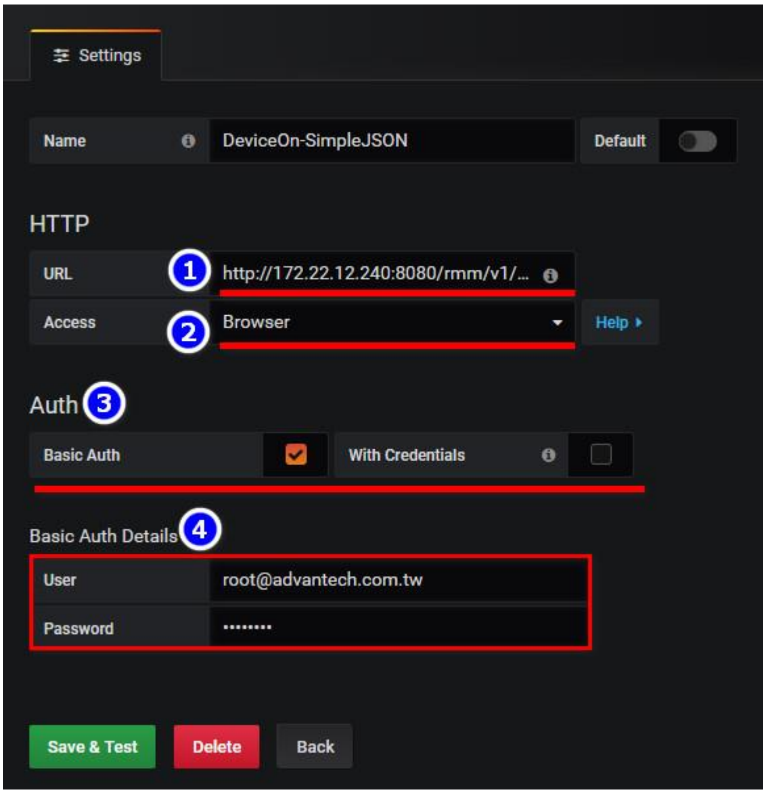
Step 4: Given below parameters for data source plugin to retrieve device data from DeviceOn APIs.

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

Access: Browser

Auth: Basic Auth (Support on prefecture version)

Basic Auth: DeviceOn Account & Password



Name: DeviceOn-SimpleJSON
Default

HTTP

1 URL: http://172.22.12.240:8080/rmm/v1/...
2 Access: Browser
Help ▸

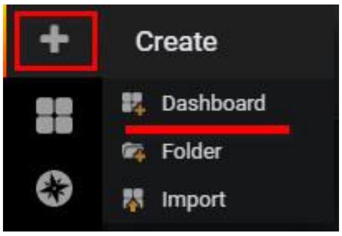
Auth 3

Basic Auth ☑
With Credentials □

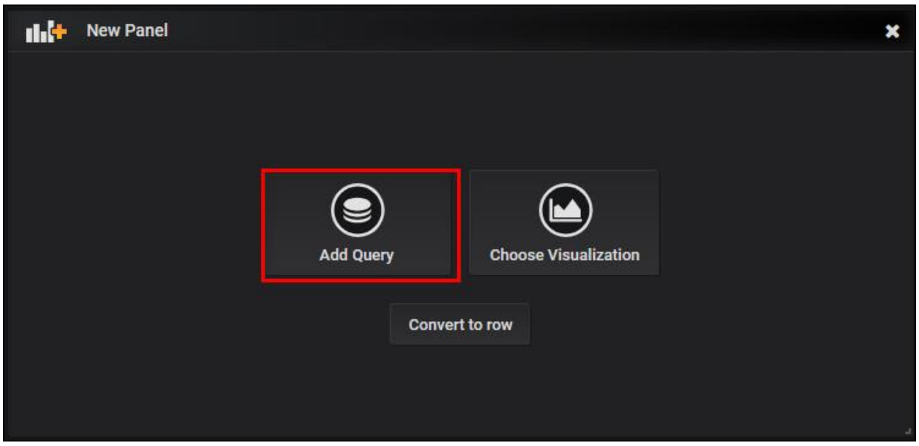
Basic Auth Details 4

User: root@advantech.com.tw
Password: ••••••••

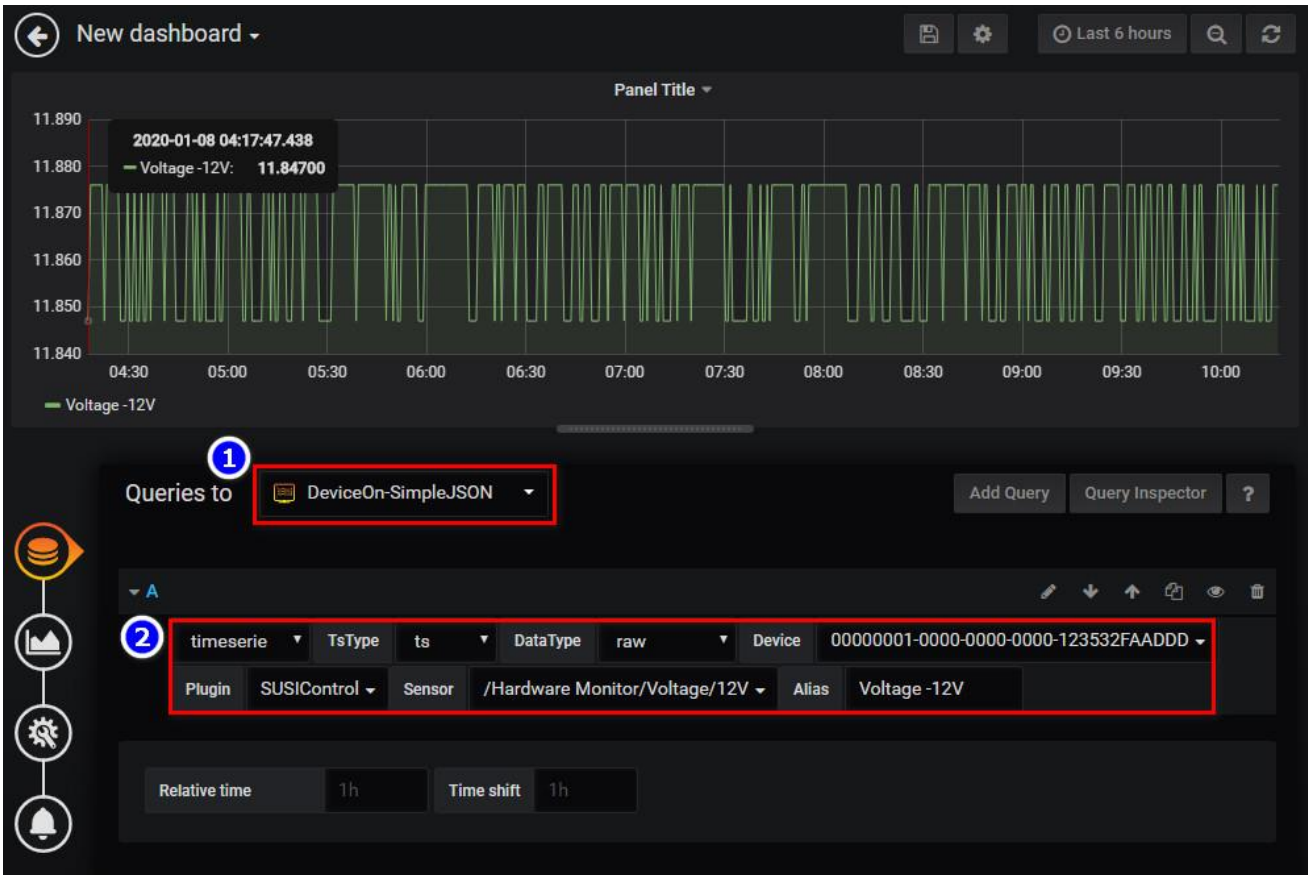
Step 5: Create a dashboard to visualize your device data.



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).



Queries to DeviceOn-SimpleJSON

timeserie | TsType ts | DataType raw | Device 00000001-0000-0000-0000-123532FAADDD

Plugin SUSIControl | Sensor /Hardware Monitor/Voltage/12V | Alias Voltage -12V

Relative time 1h | Time shift 1h

4.6 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:

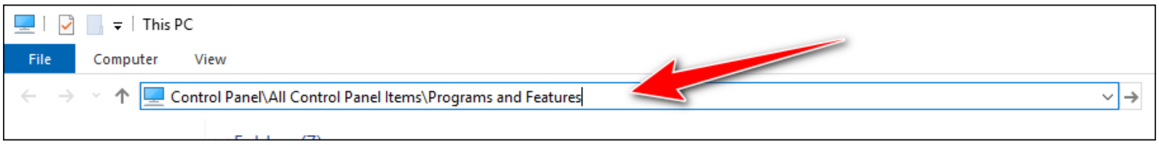
- Learn how to enable **“Keyboard Filter”** and **“Unified Write Filter”** (a.k.a. UWF) in Windows lockdown features.
- Know what lockdown features can be controlled via DeviceOn portal.

4.6.1 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.

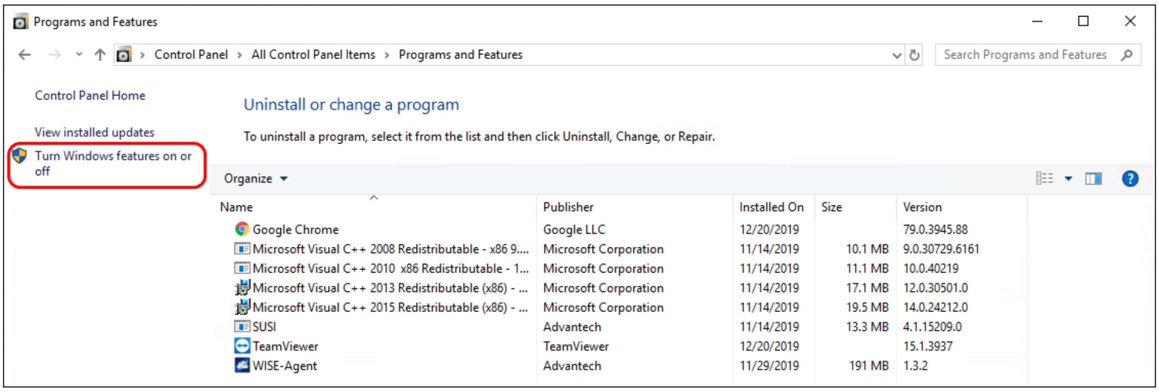
4.6.2 Step-by-Step

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.



Control Panel\All Control Panel Items\Programs and Features

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

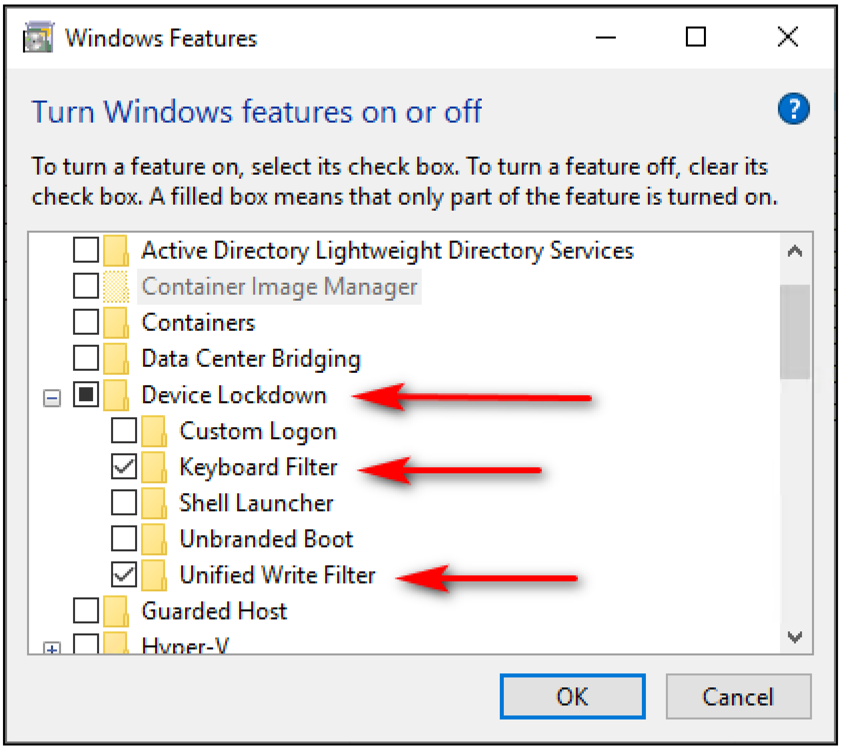

Programs and Features
Control Panel › All Control Panel Items › Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
Google Chrome	Google LLC	12/20/2019		79.0.3945.88
Microsoft Visual C++ 2008 Redistributable - x86 9....	Microsoft Corporation	11/14/2019	10.1 MB	9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable - 1...	Microsoft Corporation	11/14/2019	11.1 MB	10.0.40219
Microsoft Visual C++ 2013 Redistributable (x86) - ...	Microsoft Corporation	11/14/2019	17.1 MB	12.0.30501.0
Microsoft Visual C++ 2015 Redistributable (x86) - ...	Microsoft Corporation	11/14/2019	19.5 MB	14.0.24212.0
SUSI	Advantech	11/14/2019	13.3 MB	4.1.15209.0
TeamViewer	TeamViewer	12/20/2019		15.1.3937
WISE-Agent	Advantech	11/29/2019	191 MB	1.3.2

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”**.



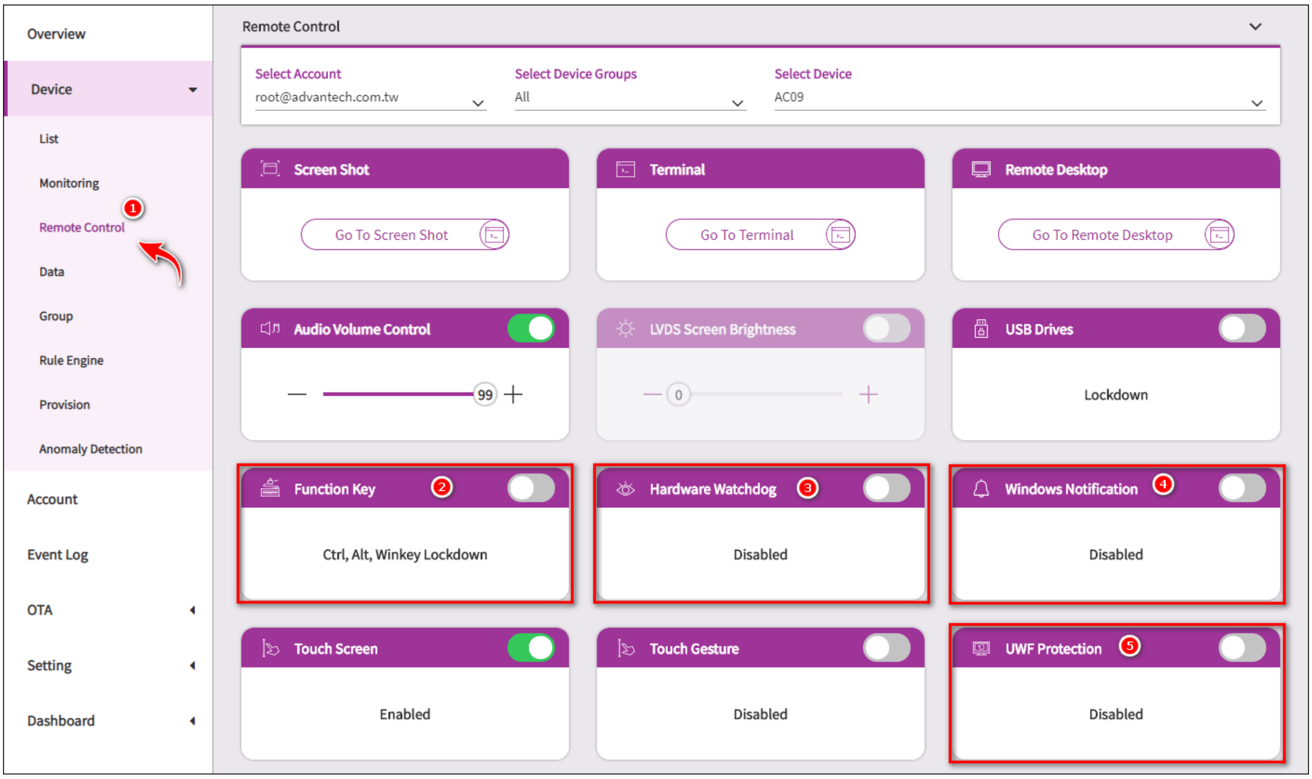
Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ Active Directory Lightweight Directory Services
- □ Container Image Manager
- □ Containers
- □ Data Center Bridging
- ■ Device Lockdown
  - □ Custom Logon
  - ☑ Keyboard Filter
  - □ Shell Launcher
  - □ Unbranded Boot
  - ☑ Unified Write Filter
- □ Guarded Host
- □ Hyper-V

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.



Select Account: root@advantech.com.tw
Select Device Groups: All
Select Device: AC09

Audio Volume Control: 99
LVDS Screen Brightness: 0
USB Drives: Lockdown
Function Key [2]: Ctrl, Alt, Winkey Lockdown
Hardware Watchdog [3]: Disabled
Windows Notification [4]: Disabled
Touch Screen: Enabled
Touch Gesture: Disabled
UWF Protection [5]: Disabled

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.

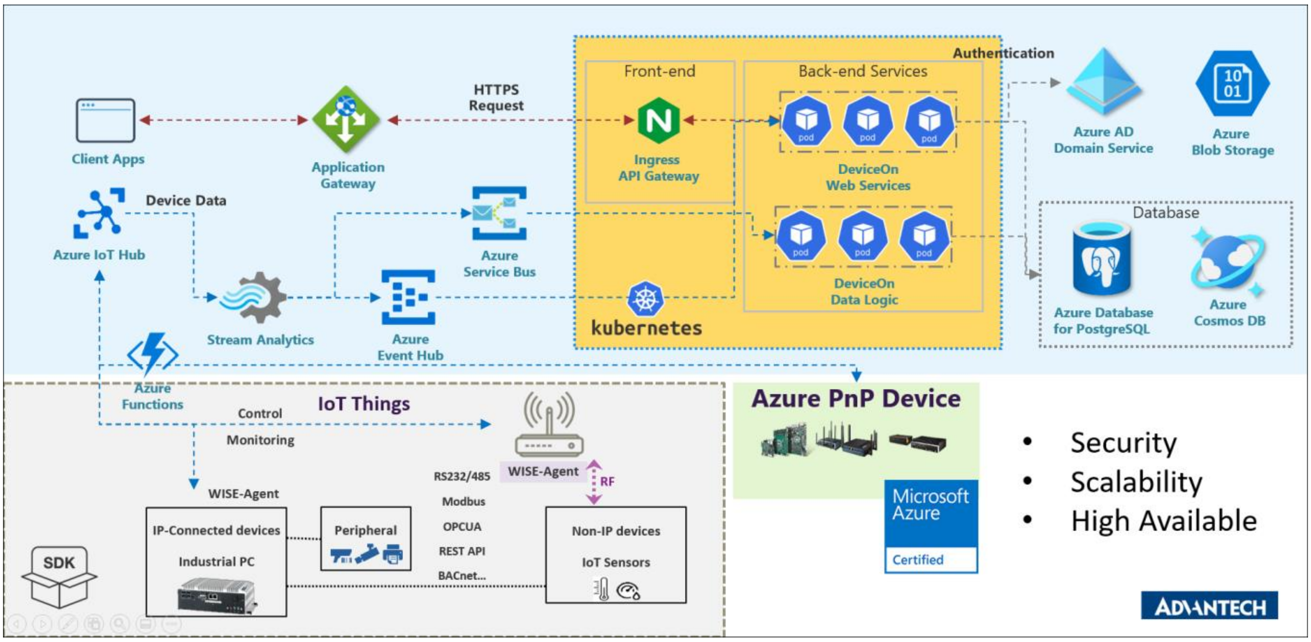
4.7 How to Deploy & Manage DeviceOn on AKS

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-DeviceOn. Second, how to serve **1k, 10k, 100k** or **millions** of devices in a system and ensure the data is secure.

Today more than ever, privacy is of critical importance in the technology industry. Microsoft has an enduring commitment to protect data privacy, not as an afterthought, but built into Microsoft Azure from the ground up. Microsoft designed Azure with industry-leading security controls, compliance tools, and privacy policies to safeguard your data in the cloud, including the categories of personal data identified by the GDPR. These also help you comply with other important global and regional privacy standards such as ISO/IEC 27018, EU-U.S. Privacy Shield, EU Model Clauses, HIPAA/HITECH, and HITRUST.

When you build on Azure's secure foundation, you accelerate your move to the cloud by achieving compliance more readily, allowing you to enable privacy-sensitive cloud scenarios.

Learn more on the Service Trust Portal about how Microsoft can help you meet GDPR requirements.
Read more about our steadfast commitment to privacy at Microsoft.



4.7.1 Prerequisite

To achieve the goal to deploy WISE-DeviceOn, some resources must be acquired, and preconditions must be met as well.

- An active Azure subscription.
- An **Azure CLI** installed on your laptop, please refer to Azure documentation to download and setup. The Azure CLI is available to install in Windows, macOS and Linux environments. It can also be run in a Docker container and Azure Cloud Shell.
- Second option, if you don't want to install Azure CLI, you can also adopt **Azure Cloud Shell**, please refer to Microsoft documentation.
- A WISE-DeviceOn ARM template prepared.

4.7.2 Steps to Deploy DeviceOn to AKS by Manual

This document tries to describe, and guide you, how to deploy WISE-DeviceOn on Azure cloud. The version is focused on Azure PaaS components to integrate to provide security, scalability, and high availability. Microsoft Azure provides lots of cloud services with security, scalability and high available. Based on Azure PaaS solutions, DeviceOn could focus on functionalities for device management and data acquisition. We fully integrate with below services:

- Azure Application Gateway (WAF protection and traffic load balancer), Optional
- Kubernetes (Container Management)
- Azure AD (Authentication), Optional
- Cosmos DB, Azure PostgreSQL (Database)
- Azure Function, IoTHub (Secure Device Connection)

- Stream Analytics, Event Hub, Service Bus (Message Bus and Filter)

When you build on Azure's secure foundation, you accelerate your move to the cloud by achieving compliance more readily, allowing you to enable privacy-sensitive cloud scenarios, such as financial and health service, with confidence.

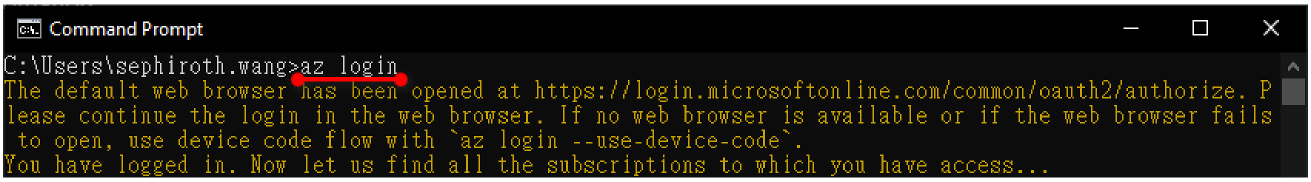
Step 1: Obtain the following three parameters for deployment.

- Application ID
- Password (Client Secrets)
- Tenant ID

1. Sign into your Azure account through Azure CLI

Use any way you prefer to open a Command Prompt and enter

```
az login
```



```
C:\Users\sephiroth.wang>az login
The default web browser has been opened at https://login.microsoftonline.com/common/oauth2/authorize. P
lease continue the login in the web browser. If no web browser is available or if the web browser fails
 to open, use device code flow with `az login --use-device-code`.
You have logged in. Now let us find all the subscriptions to which you have access...
```

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.

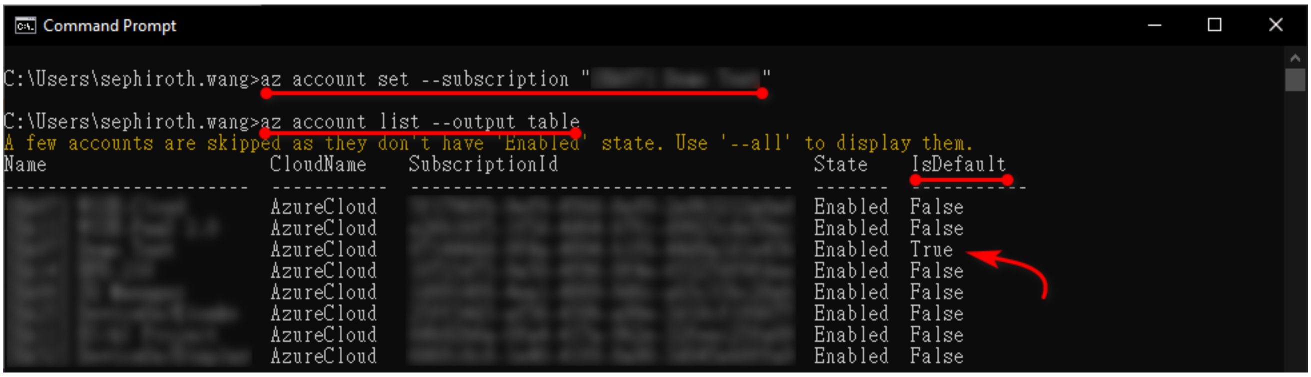
2. Select your Subscription.

After you login, the terminal console will list all subscriptions, please select the subscription that you would like to deploy.

```
az account set --subscription <SUBSCRIPTION_NAME>
```

If you do not know which subscriptions you have, you can use below command to list all the subscriptions and determine whether the subscription has been selected according to **isDefault**.

```
az account list --output table
```

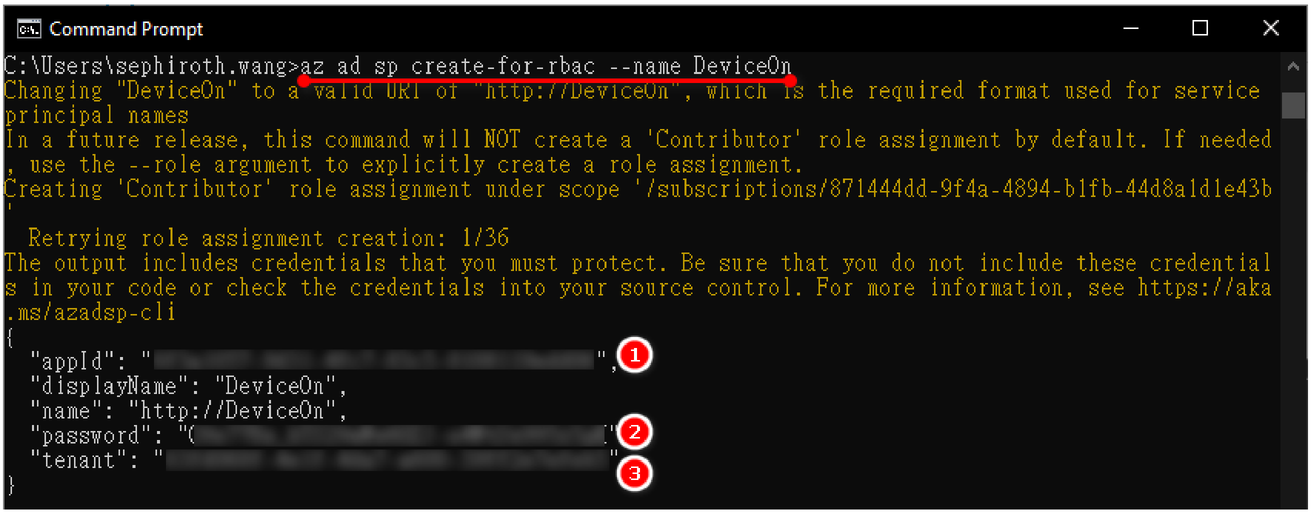


```
C:\Users\sephiroth.wang>az account set --subscription "[redacted]"

C:\Users\sephiroth.wang>az account list --output table
A few accounts are skipped as they don't have 'Enabled' state. Use '--all' to display them.
Name                    CloudName    SubscriptionId                        State    IsDefault
----------------------  -----------  ------------------------------------  -------  -----------
[redacted]              AzureCloud   [redacted]                            Enabled  False
                        AzureCloud                                         Enabled  False
                        AzureCloud                                         Enabled  True
                        AzureCloud                                         Enabled  False
                        AzureCloud                                         Enabled  False
                        AzureCloud                                         Enabled  False
                        AzureCloud                                         Enabled  False
                        AzureCloud                                         Enabled  False
```

3. Create a service principal.

The last step to create a service principal and generate these parameters. (1. **Application ID**, 2. **Password** and 3. **Tenant ID**)

```
az ad sp create-for-rbac --name <SERVICE_PRINCIPAL_NAME>
```

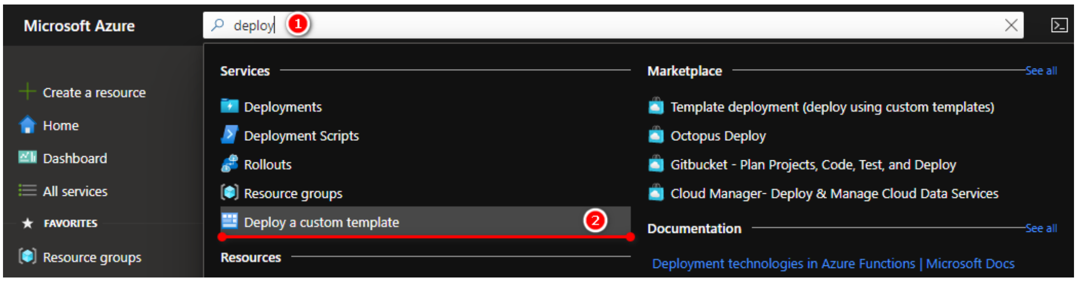


```
C:\Users\sephiroth.wang>az ad sp create-for-rbac --name DeviceOn
Changing "DeviceOn" to a valid URI of "http://DeviceOn", which is the required format used for service
principal names
In a future release, this command will NOT create a 'Contributor' role assignment by default. If needed
, use the --role argument to explicitly create a role assignment.
Creating 'Contributor' role assignment under scope '/subscriptions/871444dd-9f4a-4894-b1fb-44d8a1d1e43b
'
  Retrying role assignment creation: 1/36
The output includes credentials that you must protect. Be sure that you do not include these credential
s in your code or check the credentials into your source control. For more information, see https://aka
.ms/azadsp-cli
{
  "appId": "[redacted]",
  "displayName": "DeviceOn",
  "name": "http://DeviceOn",
  "password": "([redacted]",
  "tenant": "[redacted]"
}
```

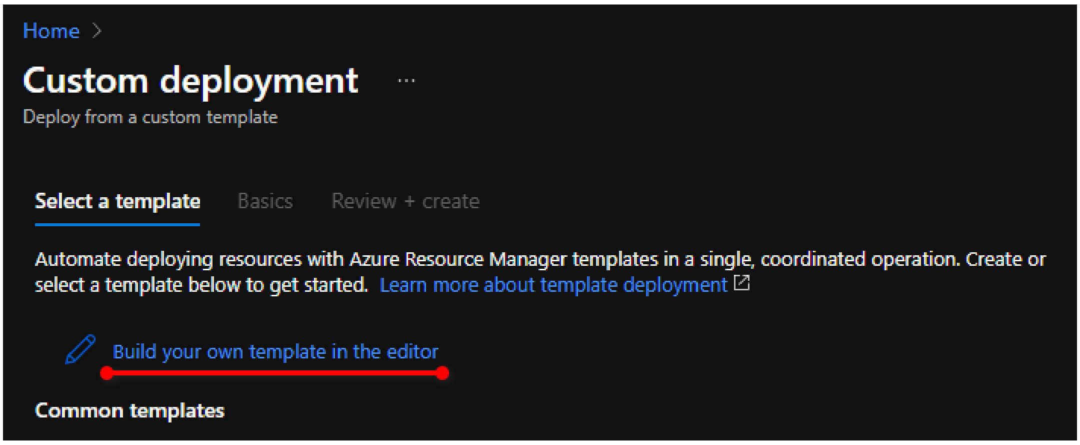
Step 2: Obtain the following three parameters for deployment.

Let's start the deployment. After you log in to the Azure portal, adopt **Deploy a custom template** to deploy the service automatically.

1. From the Azure portal menu, in the search box, type **deploy**, and then select **Deploy a custom template**.



2. Select **Build your own template in the editor**.



Home >

Custom deployment ...

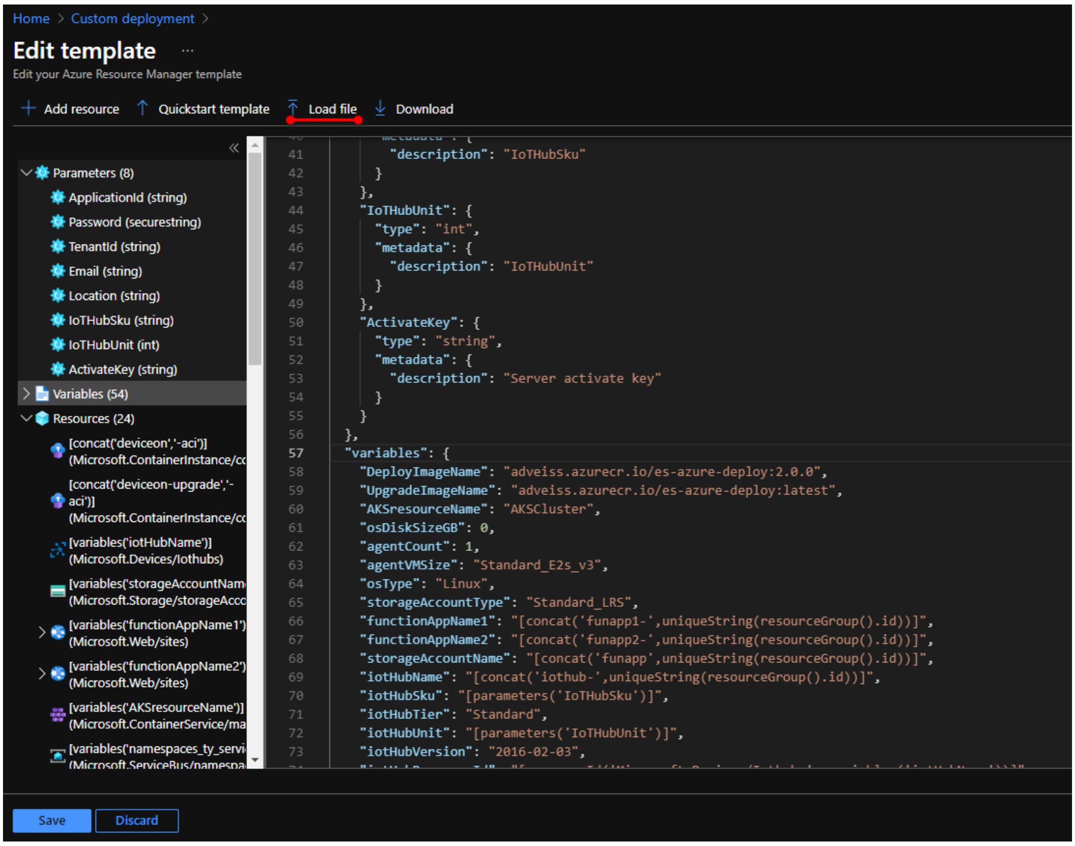
Deploy from a custom template

Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Create or select a template below to get started. Learn more about template deployment

Build your own template in the editor

Common templates

3. Select Load file, and then follow the instructions to load DeviceOn_Template.json or copy/paste the json content to the editor.



Home > Custom deployment >

Edit template ...

Edit your Azure Resource Manager template

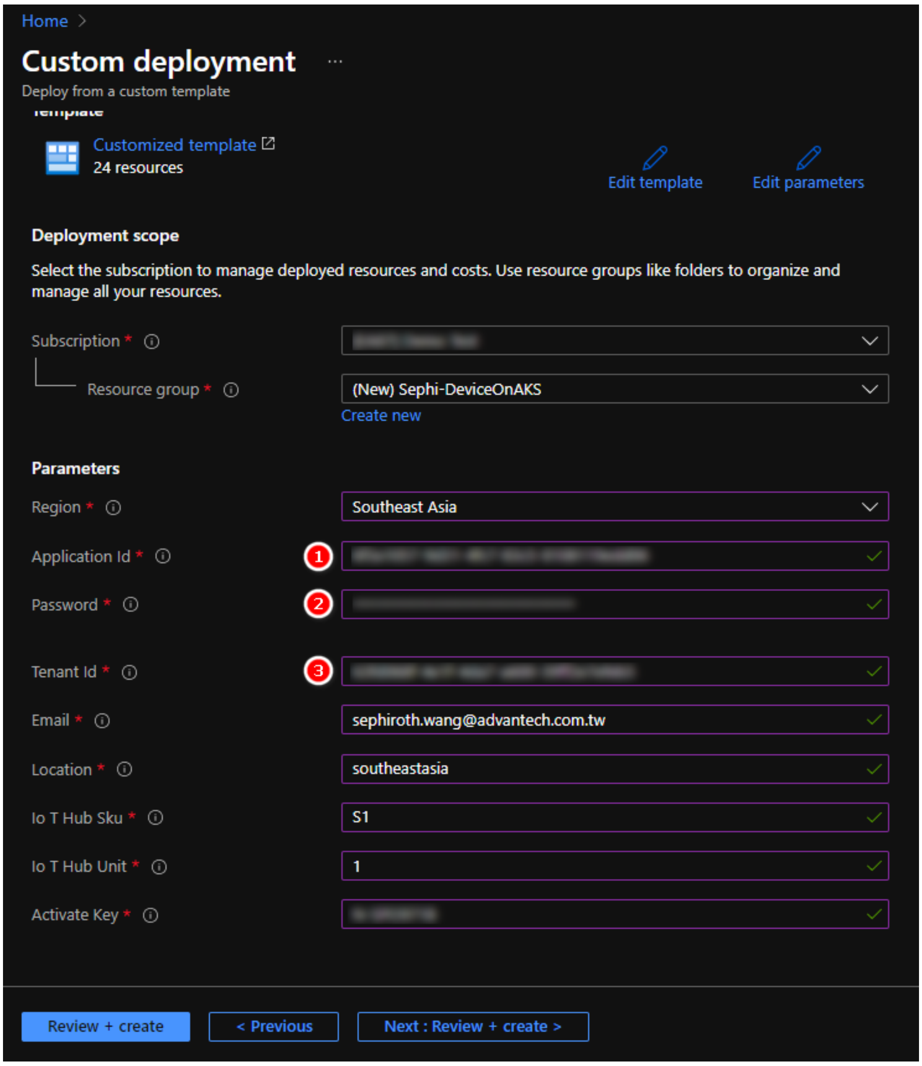
Add resource
Quickstart template
Load file
Download
Parameters (8)
ApplicationId (string)
Password (securestring)
TenantId (string)
Email (string)
Location (string)
IoTHubSku (string)
IoTHubUnit (int)
ActivateKey (string)
Variables (54)
Resources (24)
[concat('deviceon','-aci')] (Microsoft.ContainerInstance/cc
[concat('deviceon-upgrade','-aci')] (Microsoft.ContainerInstance/cc
[variables('iotHubName')] (Microsoft.Devices/Iothubs)
[variables('storageAccountNam (Microsoft.Storage/storageAcco
[variables('functionAppName1') (Microsoft.Web/sites)
[variables('functionAppName2') (Microsoft.Web/sites)
[variables('AKSresourceName')] (Microsoft.ContainerService/ma
[variables('namespaces_ty_servi (Microsoft.ServiceBus/namespa
Save
Discard

```
          "description": "IoTHubSku"
        }
      },
      "IoTHubUnit": {
        "type": "int",
        "metadata": {
          "description": "IoTHubUnit"
        }
      },
      "ActivateKey": {
        "type": "string",
        "metadata": {
          "description": "Server activate key"
        }
      }
    },
    "variables": {
      "DeployImageName": "adveiss.azurecr.io/es-azure-deploy:2.0.0",
      "UpgradeImageName": "adveiss.azurecr.io/es-azure-deploy:latest",
      "AKSresourceName": "AKSCluster",
      "osDiskSizeGB": 0,
      "agentCount": 1,
      "agentVMSize": "Standard_E2s_v3",
      "osType": "Linux",
      "storageAccountType": "Standard_LRS",
      "functionAppName1": "[concat('funapp1-',uniqueString(resourceGroup().id))]",
      "functionAppName2": "[concat('funapp2-',uniqueString(resourceGroup().id))]",
      "storageAccountName": "[concat('funapp',uniqueString(resourceGroup().id))]",
      "iotHubName": "[concat('iothub-',uniqueString(resourceGroup().id))]",
      "iotHubSku": "[parameters('IoTHubSku')]",
      "iotHubTier": "Standard",
      "iotHubUnit": "[parameters('IoTHubUnit')]",
      "iotHubVersion": "2016-02-03",
```

4. Select **Save**.
5. Enter the following values:

Name	Value
Resource Group	Select the resource group name you created in the last section.

Name	**Value**
Region	Select a location for the resource group. For example, Southeast Asia.
Application Id	The application Id is obtained from Step 1.
Password	The password is obtained from Step 1.
Tenant Id	The tenant Id is obtained from Step 1.
Email	After deployment, the result/progress will be sent to this email
Location	Enter the location name according to the data center. for examle, Asia East(**eastasia**), Asia Southeast(**southeastasia**), Japan East(**japaneast**), US East(**eastus**), Europe North(**northeurope**)
IoTHub SKU	S1/S2/S3, the default is **S1**, you could adjust the tier from Azure Poral if need.
IoTHub Unit	default is 1
Activate Key	Advantech hardware connection, enter **N/A** (free support for 1000 Advantech devices), or please contact us to purchase license key for Non-Advantech devices.



Deployment scope

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : [redacted]

Resource group * : (New) Sephi-DeviceOnAKS

Create new

Parameters

Region * : Southeast Asia

Application Id * : 1 [redacted]

Password * : 2 [redacted]

Tenant Id * : 3 [redacted]

Email * : sephiroth.wang@advantech.com.tw

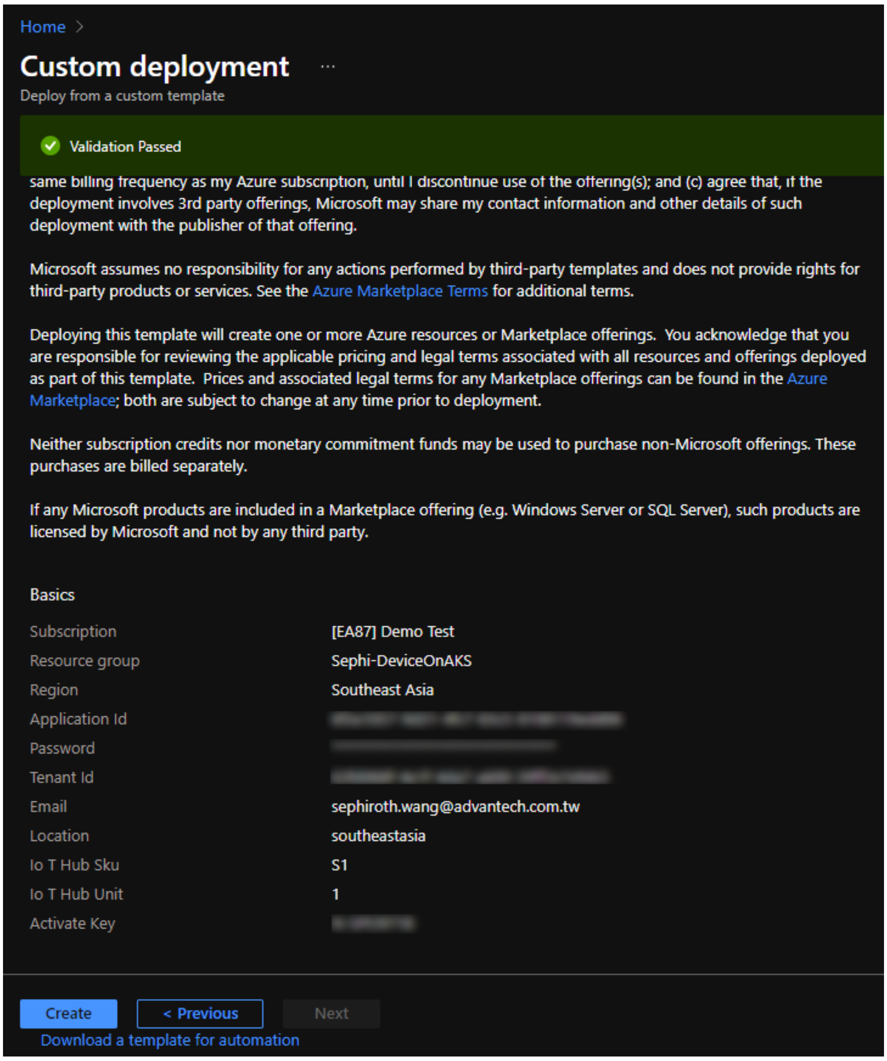
Location * : southeastasia

Io T Hub Sku * : S1

Io T Hub Unit * : 1

Activate Key * : [redacted]

6. Select **Review + create**
7. Validation and start to create.



Home >

Custom deployment ...

Deploy from a custom template

✓ Validation Passed

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.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the Azure Marketplace Terms for additional terms.

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the Azure Marketplace; both are subject to change at any time prior to deployment.

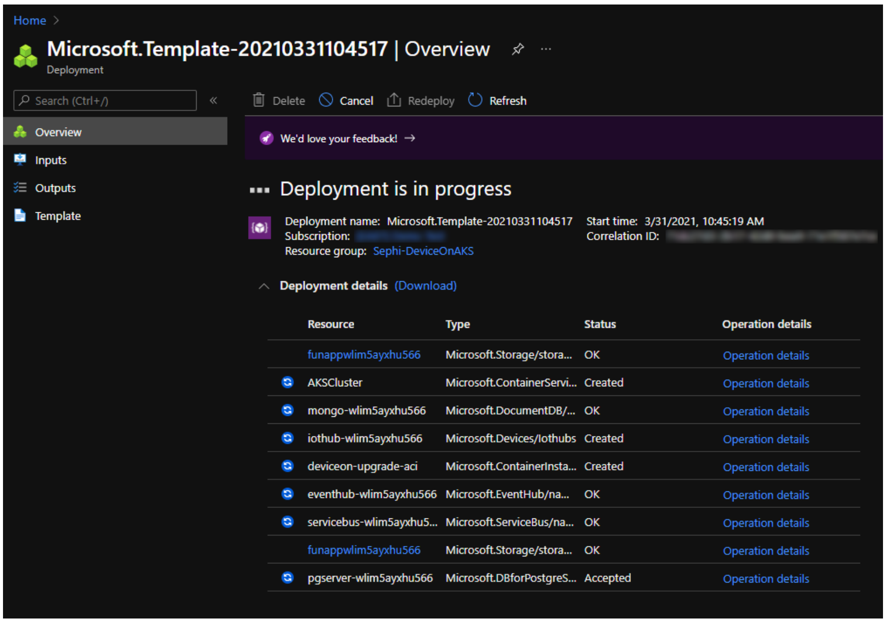
Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.

If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Basics

Subscription	[EA87] Demo Test
Resource group	Sephi-DeviceOnAKS
Region	Southeast Asia
Application Id	[redacted]
Password	[redacted]
Tenant Id	[redacted]
Email	sephiroth.wang@advantech.com.tw
Location	southeastasia
Io T Hub Sku	S1
Io T Hub Unit	1
Activate Key	[redacted]

8. The entire deployment process takes about 30 minutes. After completion, you will receive a mail notification. The content of the mail includes the DeviceOn web Service IP and login Account password.



Home >

Microsoft.Template-20210331104517 | Overview

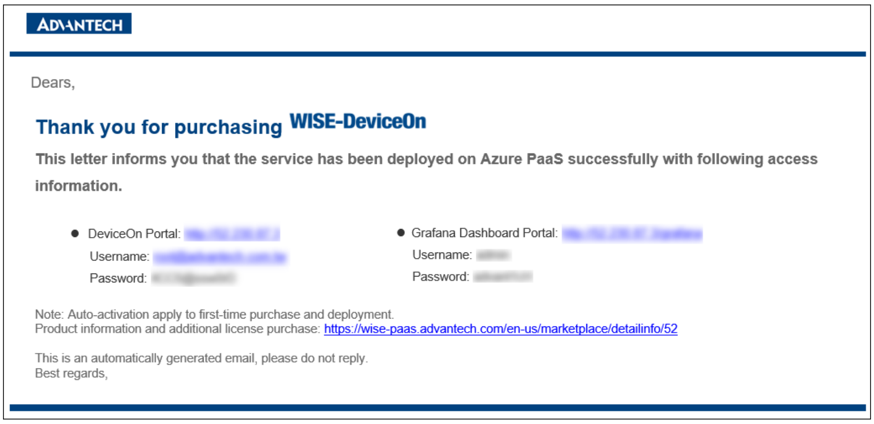
Deployment

Deployment is in progress

Deployment name: Microsoft.Template-20210331104517
Subscription: [redacted]
Resource group: Sephi-DeviceOnAKS
Start time: 3/31/2021, 10:45:19 AM
Correlation ID: [redacted]

Deployment details (Download)

Resource	Type	Status	Operation details
funappwlim5ayxhu566	Microsoft.Storage/stora...	OK	Operation details
AKSCluster	Microsoft.ContainerServi...	Created	Operation details
mongo-wlim5ayxhu566	Microsoft.DocumentDB/...	OK	Operation details
iothub-wlim5ayxhu566	Microsoft.Devices/Iothubs	Created	Operation details
deviceon-upgrade-aci	Microsoft.ContainerInsta...	Created	Operation details
eventhub-wlim5ayxhu566	Microsoft.EventHub/na...	OK	Operation details
servicebus-wlim5ayxhu5...	Microsoft.ServiceBus/na...	OK	Operation details
funappwlim5ayxhu566	Microsoft.Storage/stora...	OK	Operation details
pgserver-wlim5ayxhu566	Microsoft.DBforPostgreS...	Accepted	Operation details



ADVANTECH

Dears,

Thank you for purchasing WISE-DeviceOn

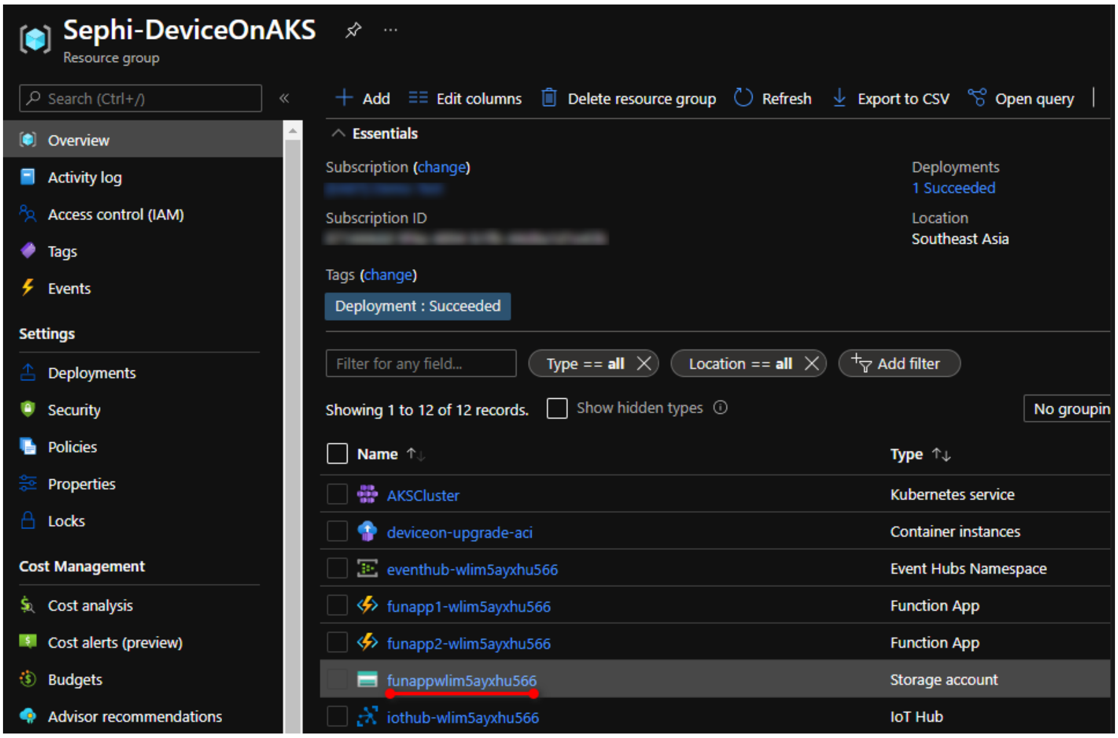
This letter informs you that the service has been deployed on Azure PaaS successfully with following access information.

- DeviceOn Portal: [redacted]
  Username: [redacted]
  Password: [redacted]
- Grafana Dashboard Portal: [redacted]
  Username: [redacted]
  Password: [redacted]

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,

Assuming that your mail is intercepted/block or not received due to mail server filters, we will synchronously write this information to the **Azure Blob Log** container. Go to your **resource group** (you entered at the stage of deployment) **storage account -> container -> Log -> ServerInformation.log**. If the container has not been created, please wait a few minutes for initialization.



Sephi-DeviceOnAKS
Resource group

Essentials

Subscription (change)
[redacted]

Subscription ID
[redacted]

Deployments
1 Succeeded

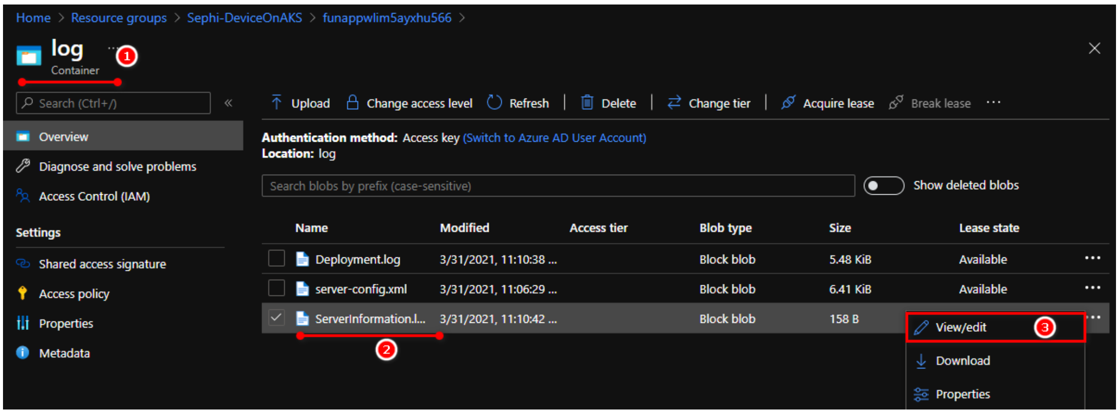
Location
Southeast Asia

Tags (change)
Deployment : Succeeded

Filter for any field... Type == all Location == all Add filter

Showing 1 to 12 of 12 records. □ Show hidden types

Name	Type
AKSCluster	Kubernetes service
deviceon-upgrade-aci	Container instances
eventhub-wlim5ayxhu566	Event Hubs Namespace
funapp1-wlim5ayxhu566	Function App
funapp2-wlim5ayxhu566	Function App
funappwlim5ayxhu566	Storage account
iothub-wlim5ayxhu566	IoT Hub

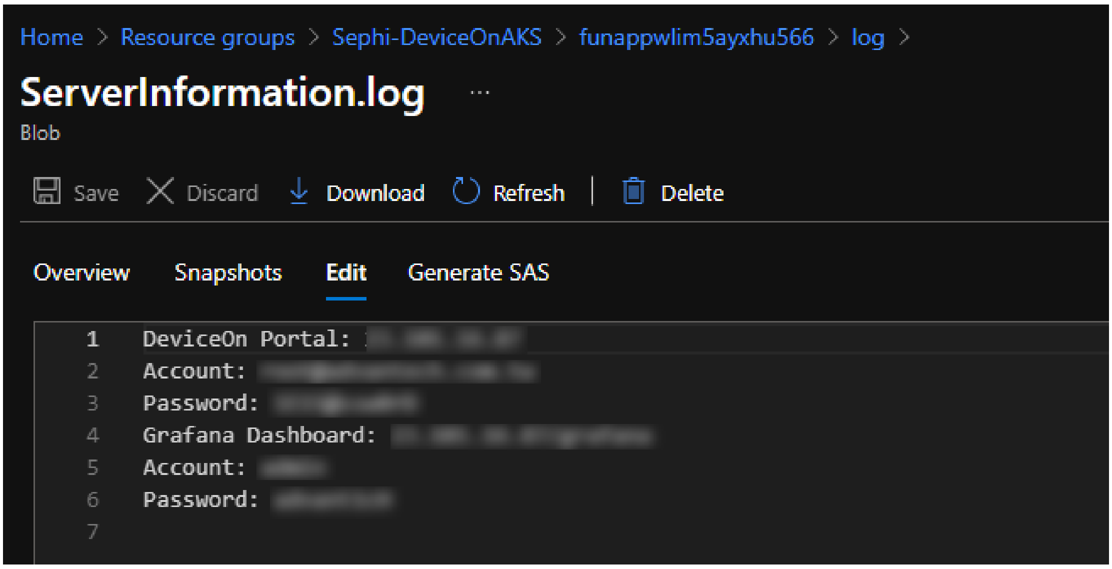


Home > Resource groups > Sephi-DeviceOnAKS > funappwlim5ayxhu566 >

log
Container

Authentication method: Access key (Switch to Azure AD User Account)
Location: log

Name	Modified	Access tier	Blob type	Size	Lease state
Deployment.log	3/31/2021, 11:10:38 ...		Block blob	5.48 KiB	Available
server-config.xml	3/31/2021, 11:06:29 ...		Block blob	6.41 KiB	Available
ServerInformation.l...	3/31/2021, 11:10:42 ...		Block blob	158 B	


Home > Resource groups > Sephi-DeviceOnAKS > funappwlim5ayxhu566 > log >
ServerInformation.log ···
Blob
Save
Discard
Download
Refresh
Delete
Overview
Snapshots
Edit
Generate SAS

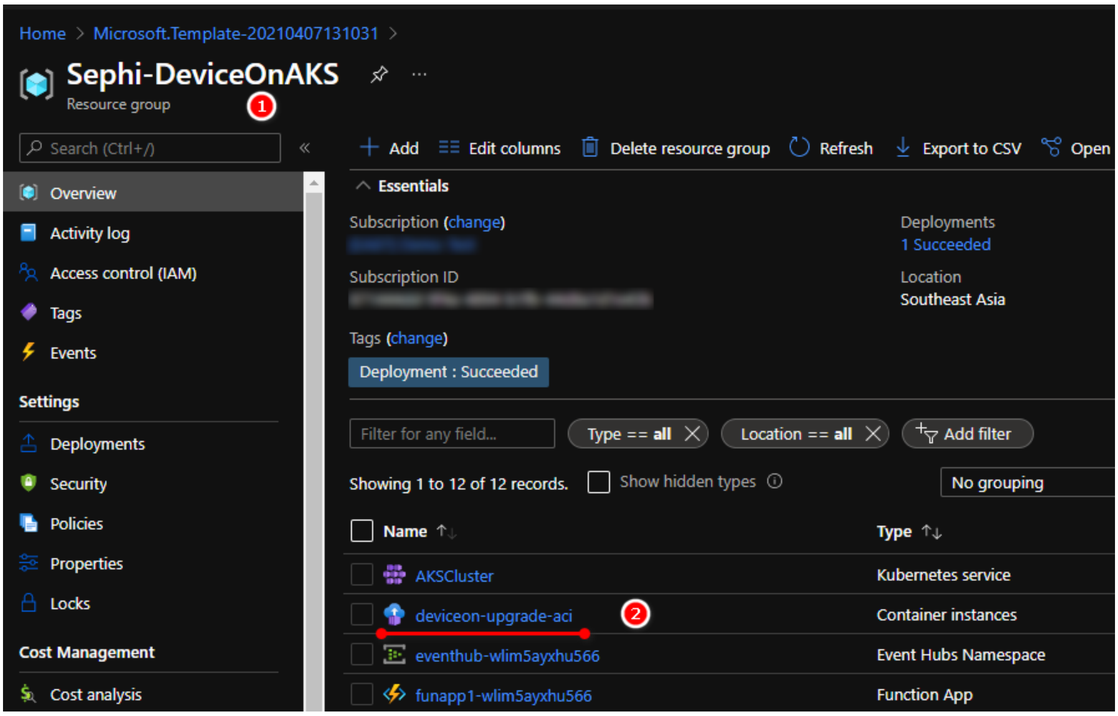
```
DeviceOn Portal: [redacted]
Account: [redacted]
Password: [redacted]
Grafana Dashboard: [redacted]
Account: [redacted]
Password: [redacted]
```

9. There are two resource group generated on your subscription, one is you entered at the stage of deployment, which include the services such as: AKS, IoTHub, EventHub, Stream Analytics, CosmosDB, PostgreSQL…etc. Another resource group name prefix name starts with **MC_**, that contains AKS VM node.

4.7.3 Steps to Upgrade DeviceOn

Step 1: Login to Azure Portal and Redirect to Your Resource Group

Select deviceon-upgrade-aci



Subscription (change): [redacted]

Subscription ID: [redacted]

Tags (change): Deployment : Succeeded

Deployments: 1 Succeeded

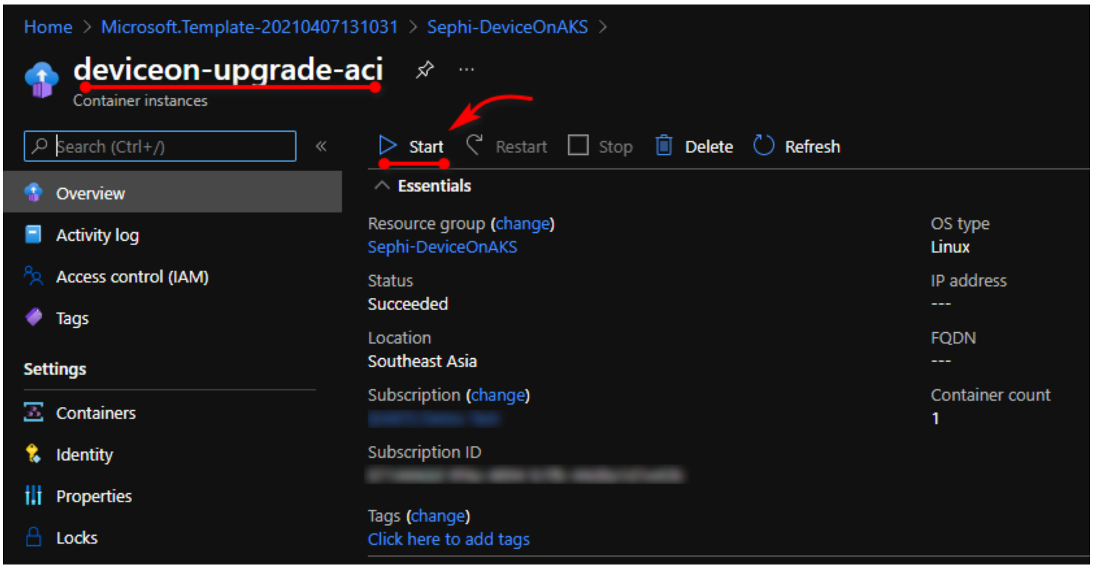
Location: Southeast Asia

Showing 1 to 12 of 12 records.

Name	Type
AKSCluster	Kubernetes service
deviceon-upgrade-aci	Container instances
eventhub-wlim5ayxhu566	Event Hubs Namespace
funapp1-wlim5ayxhu566	Function App

Step 2: Run the Azure Container Instance

Click **Start** button to check and upgrade DeviceOn container to the latest version.



Resource group (change)
Sephi-DeviceOnAKS

Status
Succeeded

Location
Southeast Asia

Subscription (change)
[redacted]

Subscription ID
[redacted]

Tags (change)
Click here to add tags

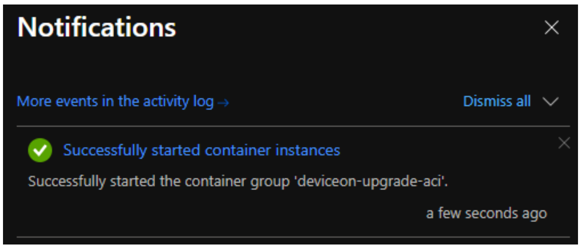
OS type
Linux

IP address

FQDN

Container count
1

After running, the service (**deviceon-upgrade-aci**) will automatically check and update the DeviceOn in your AKS. At the end, this service will stop.



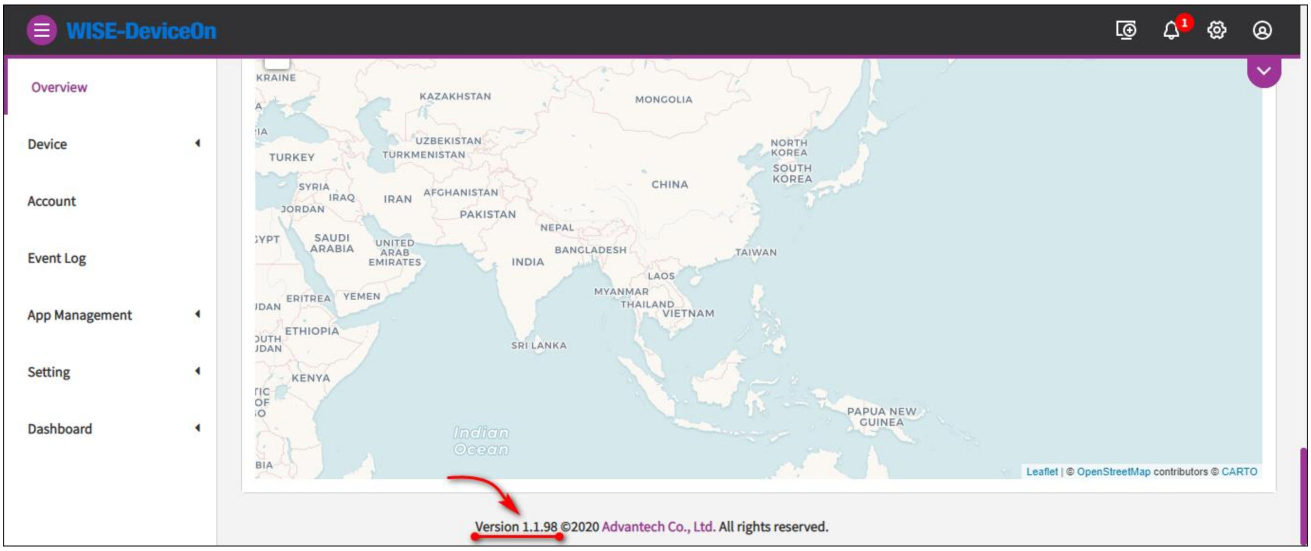
Successfully started container instances

Successfully started the container group 'deviceon-upgrade-aci'.

a few seconds ago

Step 3: Check your DeviceOn Verison

Please go to your DeviceOn portal to confirm the version updated. If the version has not changed, it means that it is the latest version.

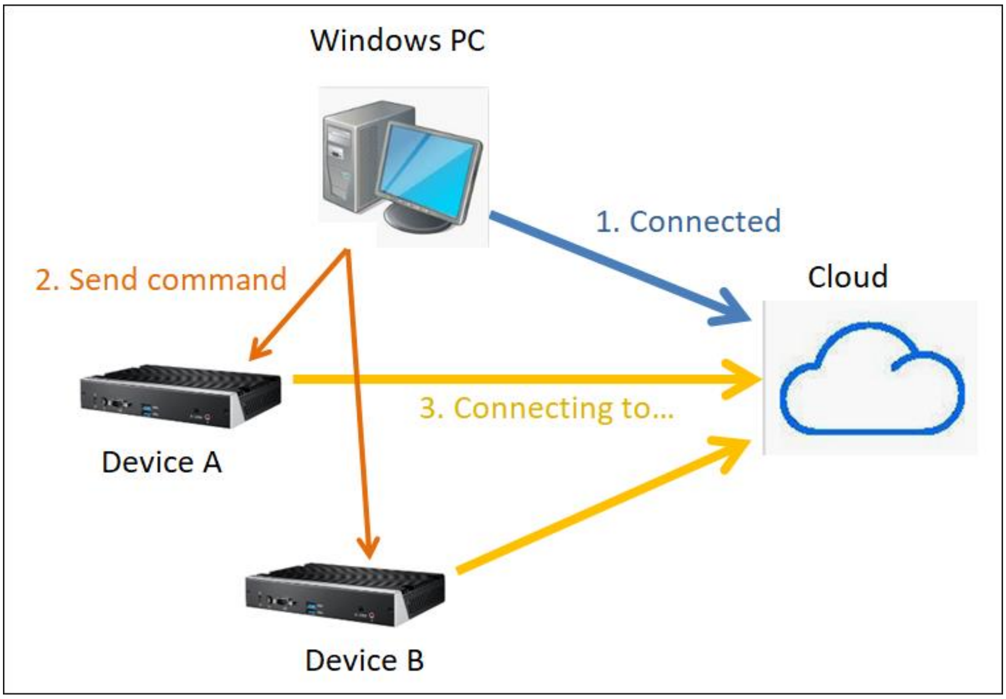


Version 1.1.98 ©2020 Advantech Co., Ltd. All rights reserved.

4.8 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.



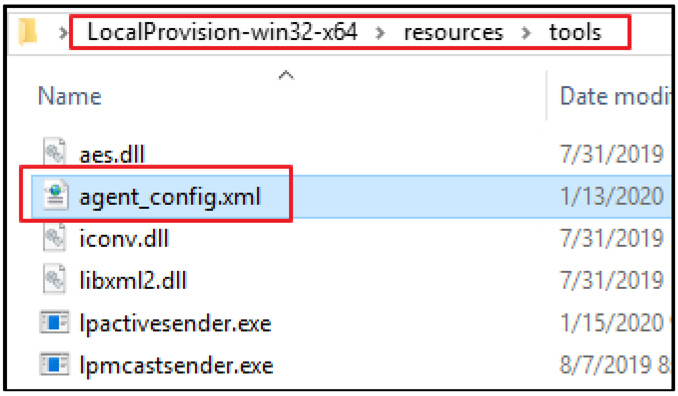
4.8.1 Prerequisite

- 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.

4.8.2 Steps to Local Provisioning

Step 1: Download and unzip the local provision GUI tool.

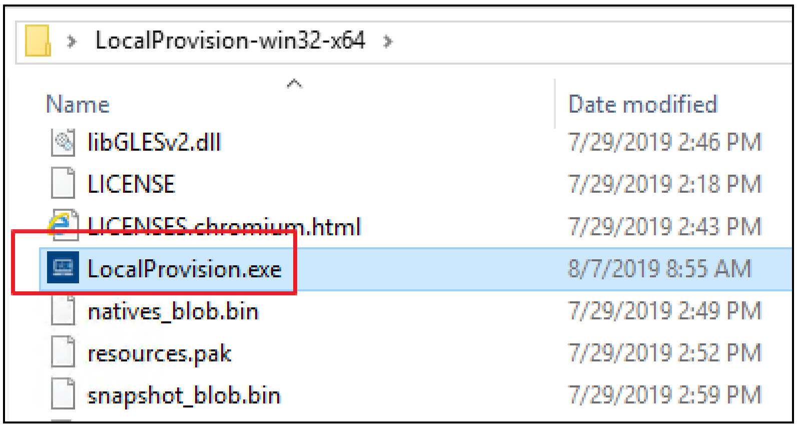
Step 2: Place valid "**agnet_config.xml**" file (with correct Credential URL and IoT Key) to "**GUI tool\resources\tools**" folder



LocalProvision-win32-x64 › resources › tools

Name	Date modi
aes.dll	7/31/2019
agent_config.xml	1/13/2020
iconv.dll	7/31/2019
libxml2.dll	7/31/2019
lpactivesender.exe	1/15/2020
lpmcastsender.exe	8/7/2019 8

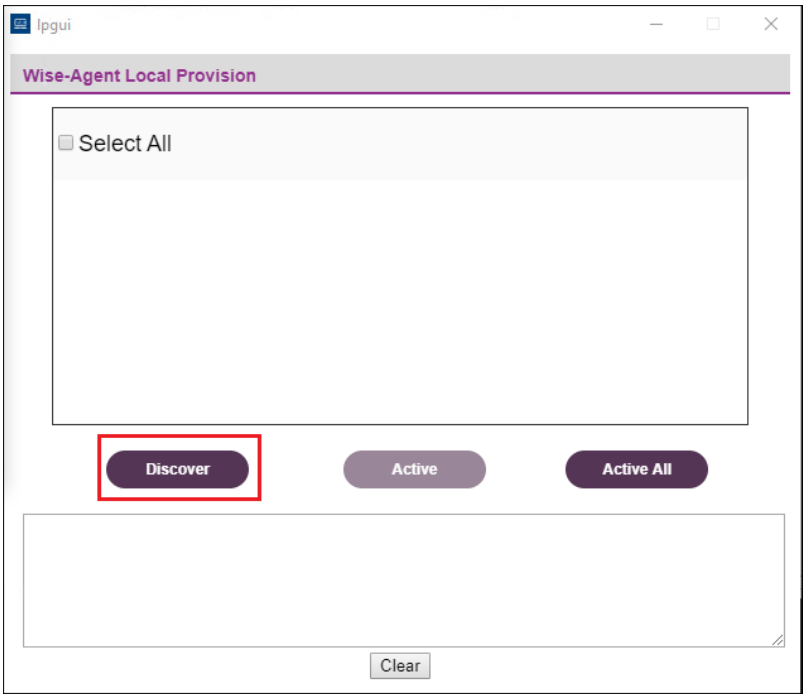
Step 3: Double click "**LocalProvision.exe**"



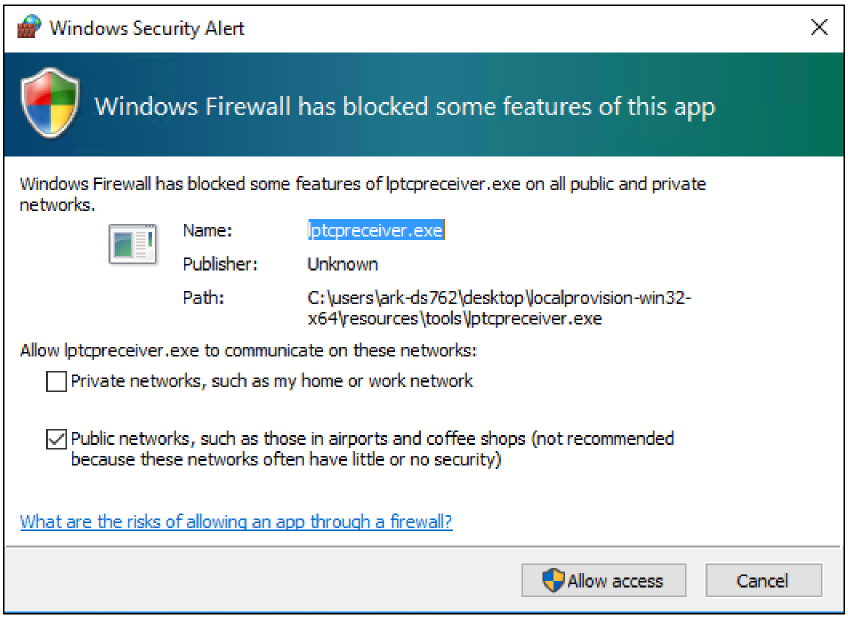
LocalProvision-win32-x64 ›

Name	Date modified
libGLESv2.dll	7/29/2019 2:46 PM
LICENSE	7/29/2019 2:18 PM
LICENSES.chromium.html	7/29/2019 2:43 PM
LocalProvision.exe	8/7/2019 8:55 AM
natives_blob.bin	7/29/2019 2:49 PM
resources.pak	7/29/2019 2:52 PM
snapshot_blob.bin	7/29/2019 2:59 PM

Step 4: Click **Discover** button



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



Windows Firewall has blocked some features of lptcpreceiver.exe on all public and private networks.

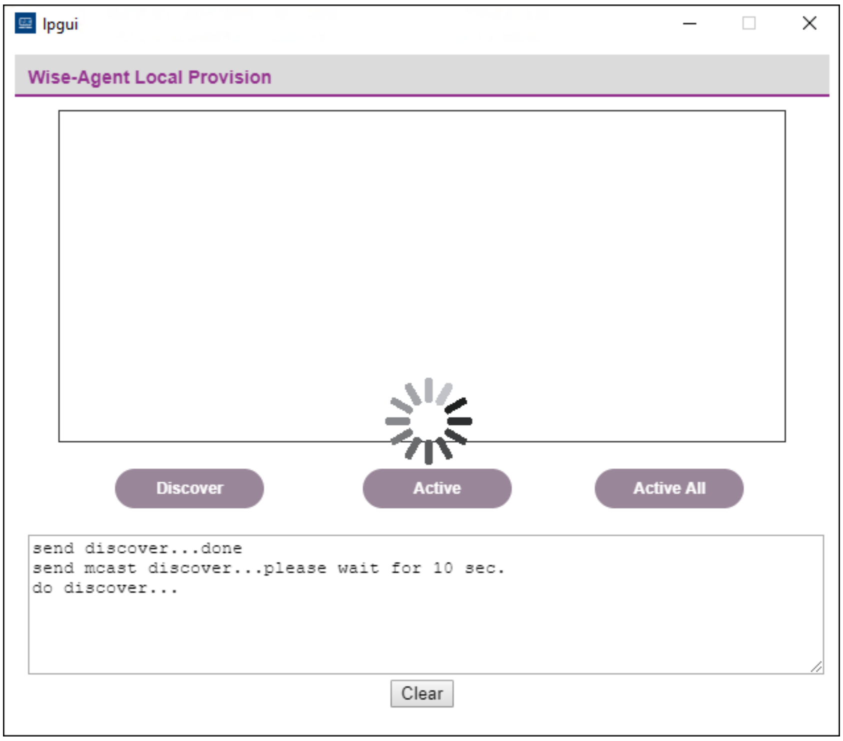
Name: lptcpreceiver.exe
Publisher: Unknown
Path: C:\users\ark-ds762\desktop\localprovision-win32-x64\resources\tools\lptcpreceiver.exe

Allow lptcpreceiver.exe to communicate on these networks:

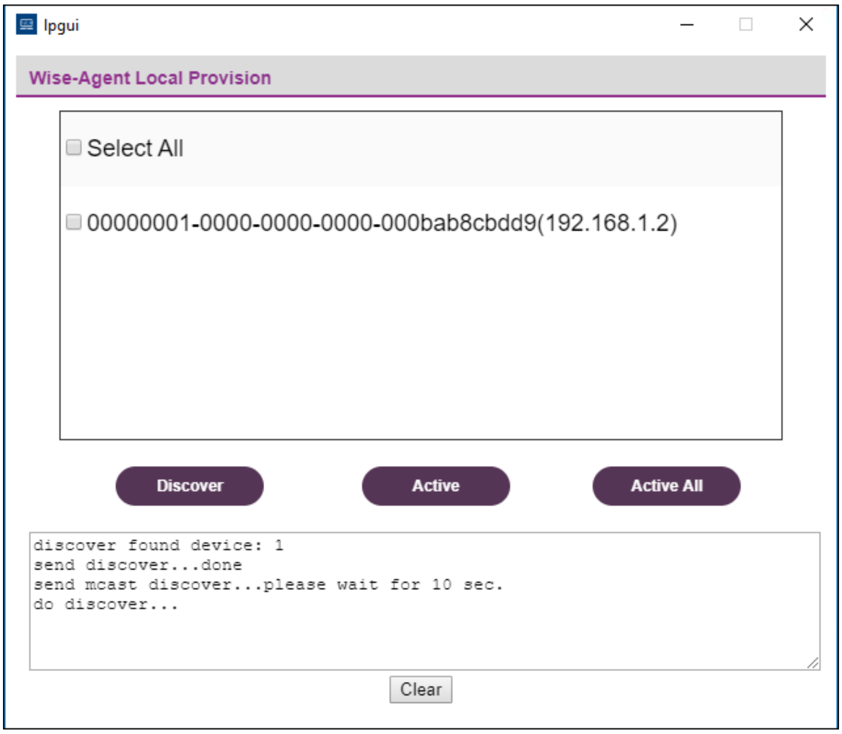
□ Private networks, such as my home or work network

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

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



```
send discover...done
send mcast discover...please wait for 10 sec.
do discover...
```

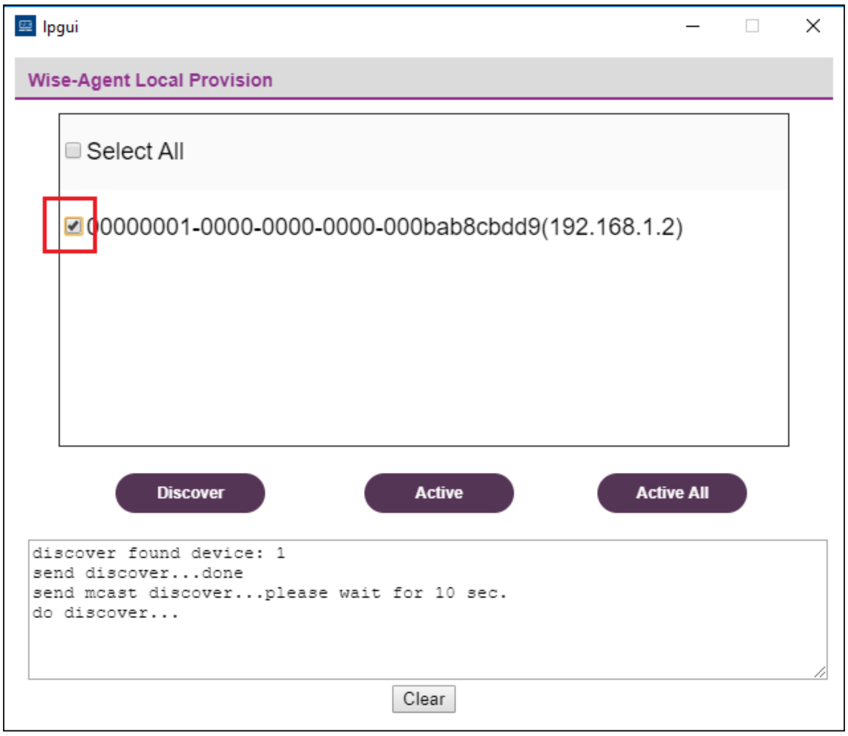


□ Select All

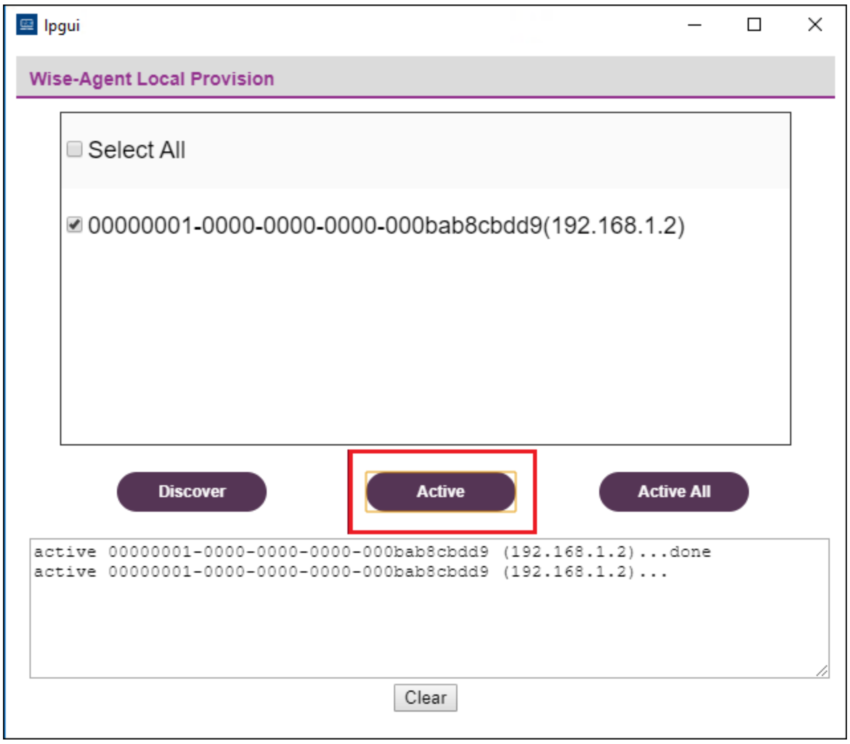
□ 00000001-0000-0000-0000-000bab8cbdd9(192.168.1.2)

```
discover found device: 1
send discover...done
send mcast discover...please wait for 10 sec.
do discover...
```

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


lpgui
Wise-Agent Local Provision
☐ Select All
☑ 00000001-0000-0000-0000-000bab8cbdd9(192.168.1.2)
Discover
Active
Active All
Clear

```
discover found device: 1
send discover...done
send mcast discover...please wait for 10 sec.
do discover...
```


lpgui
Wise-Agent Local Provision
☐ Select All
☑ 00000001-0000-0000-0000-000bab8cbdd9(192.168.1.2)
Discover
Active
Active All
Clear

```
active 00000001-0000-0000-0000-000bab8cbdd9 (192.168.1.2)...done
active 00000001-0000-0000-0000-000bab8cbdd9 (192.168.1.2)...
```

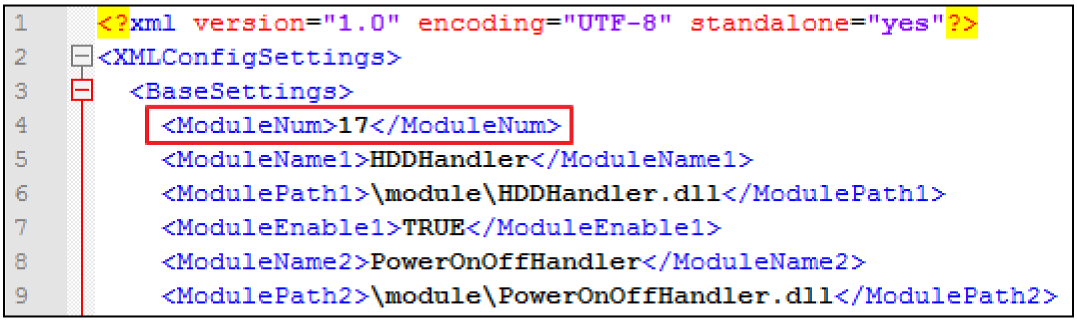
Until now, the checked devices should connect to server after few second later.

4.8.1 Troubleshooting

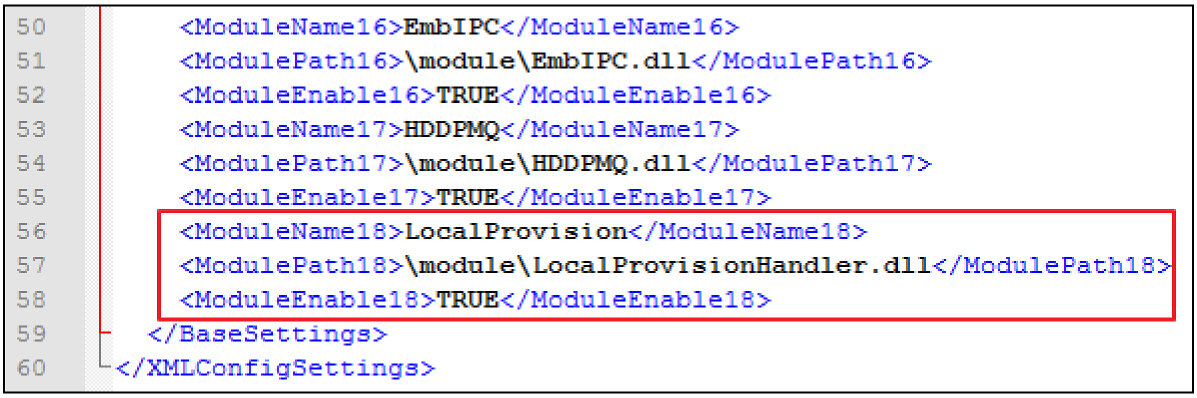
Why can’t I find some WISE-Agent devices? Please help check following:

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.



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<XMLConfigSettings>
  <BaseSettings>
    <ModuleNum>17</ModuleNum>
    <ModuleName1>HDDHandler</ModuleName1>
    <ModulePath1>\module\HDDHandler.dll</ModulePath1>
    <ModuleEnable1>TRUE</ModuleEnable1>
    <ModuleName2>PowerOnOffHandler</ModuleName2>
    <ModulePath2>\module\PowerOnOffHandler.dll</ModulePath2>
```



```
    <ModuleName16>EmbIPC</ModuleName16>
    <ModulePath16>\module\EmbIPC.dll</ModulePath16>
    <ModuleEnable16>TRUE</ModuleEnable16>
    <ModuleName17>HDDPMQ</ModuleName17>
    <ModulePath17>\module\HDDPMQ.dll</ModulePath17>
    <ModuleEnable17>TRUE</ModuleEnable17>
    <ModuleName18>LocalProvision</ModuleName18>
    <ModulePath18>\module\LocalProvisionHandler.dll</ModulePath18>
    <ModuleEnable18>TRUE</ModuleEnable18>
  </BaseSettings>
</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-Agent by UDP port **9178** and TCP port **9177**, please check if your IT block these ports in your local network.

4.9 How to Secure Connect to DeviceOn though X.509

This section tries to teach you how to connect DeviceOn server through x509. There are two topics we will cover through this document. The first part will show you how to get the credential files from DeviceOn server. Another part will show you how to configure WISE-Agent and make it connect DeviceOn sever through x509.

4.9.1 Prerequisite

- Your operation system should install the following software.
  - DeviceOn Server that is greater than version **4.4.2**
  - WISEAgent
  - OpenSSL

4.9.2 Steps to Generate the Credential Files

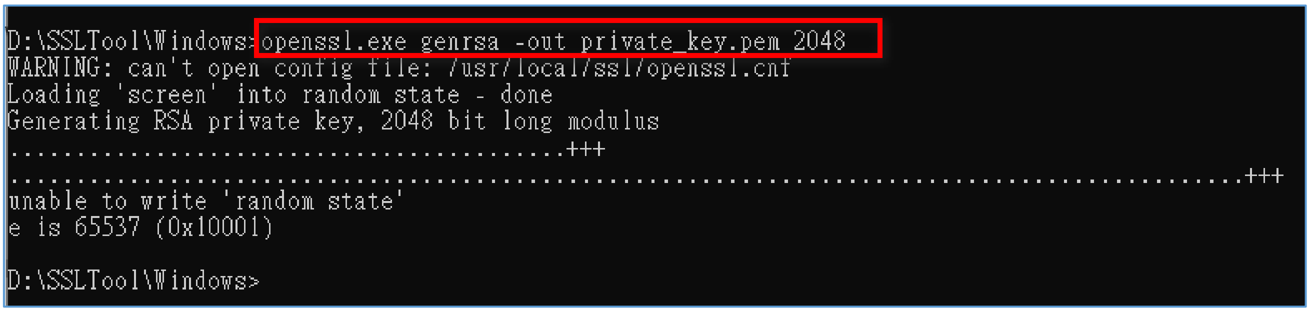
In this session, you will learn how to create a private key file with OpenSSL command line tools. You can upload the created private key file to DeviceOn server and then download the zip file from server.

To understand this SOP, you should have the knowledge of the following topics:

- Generate the private key file with OpenSSL command line tool.
- Get the credential files from DeviceOn server.

Step 1: Press **Win+X** to open the Command Prompt.
Step 2: Navigate to the OpenSSL bin directory.
Step 3: Enter the following command to generate a private key:

```
openssl.exe genrsa –out private_key.pem 2048
```

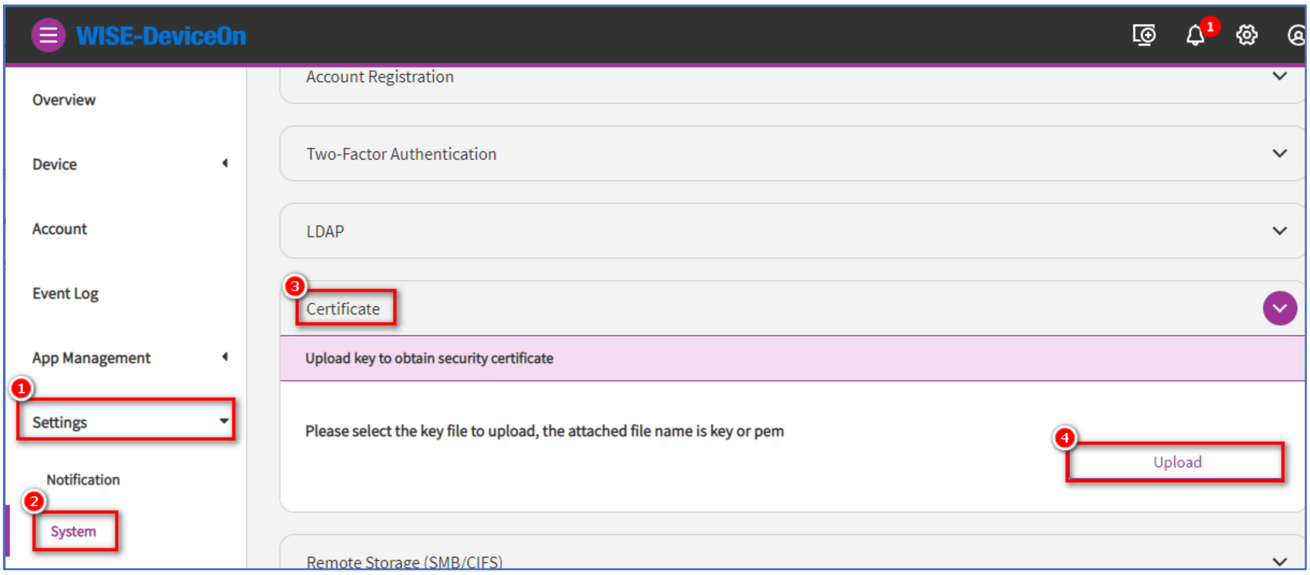


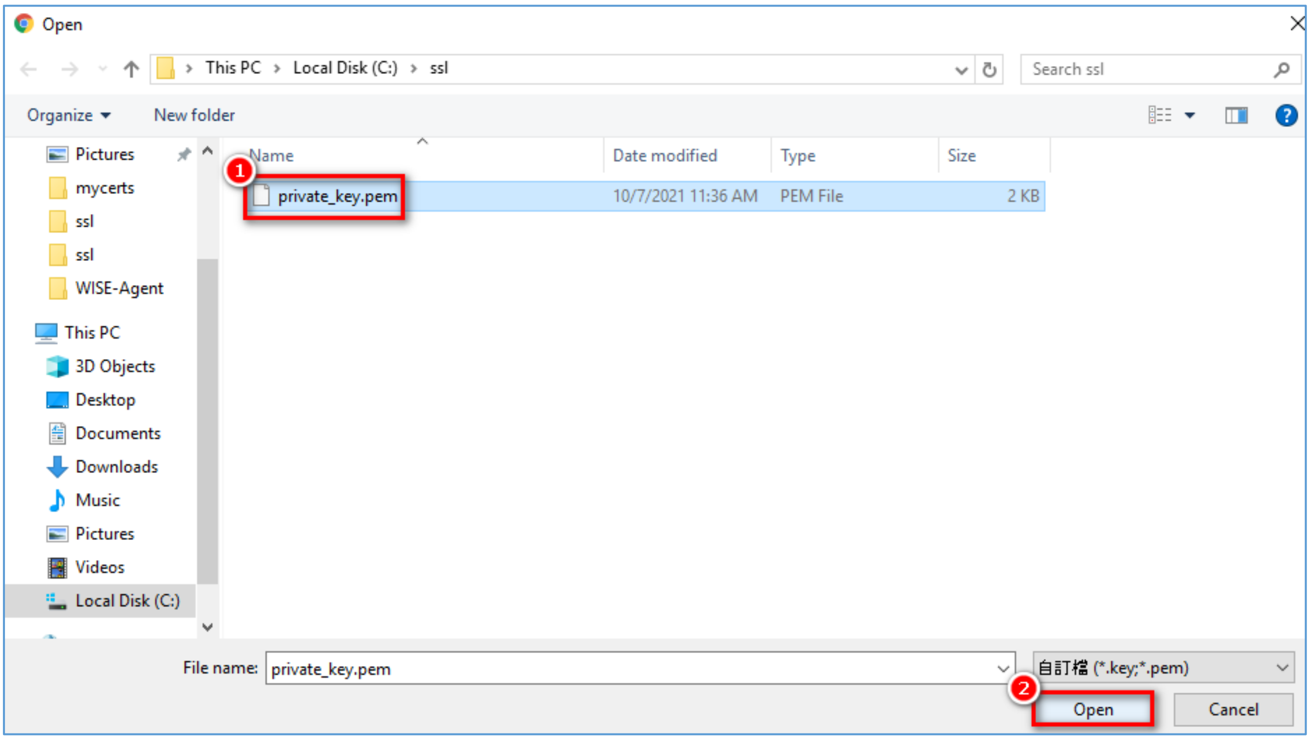
```
D:\SSLTool\Windows>openssl.exe genrsa -out private_key.pem 2048
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.......................................+++
.........................................................................................+++
unable to write 'random state'
e is 65537 (0x10001)

D:\SSLTool\Windows>
```

Step 4: Once complete, you will find the name **private_key.pem** that under the directory.

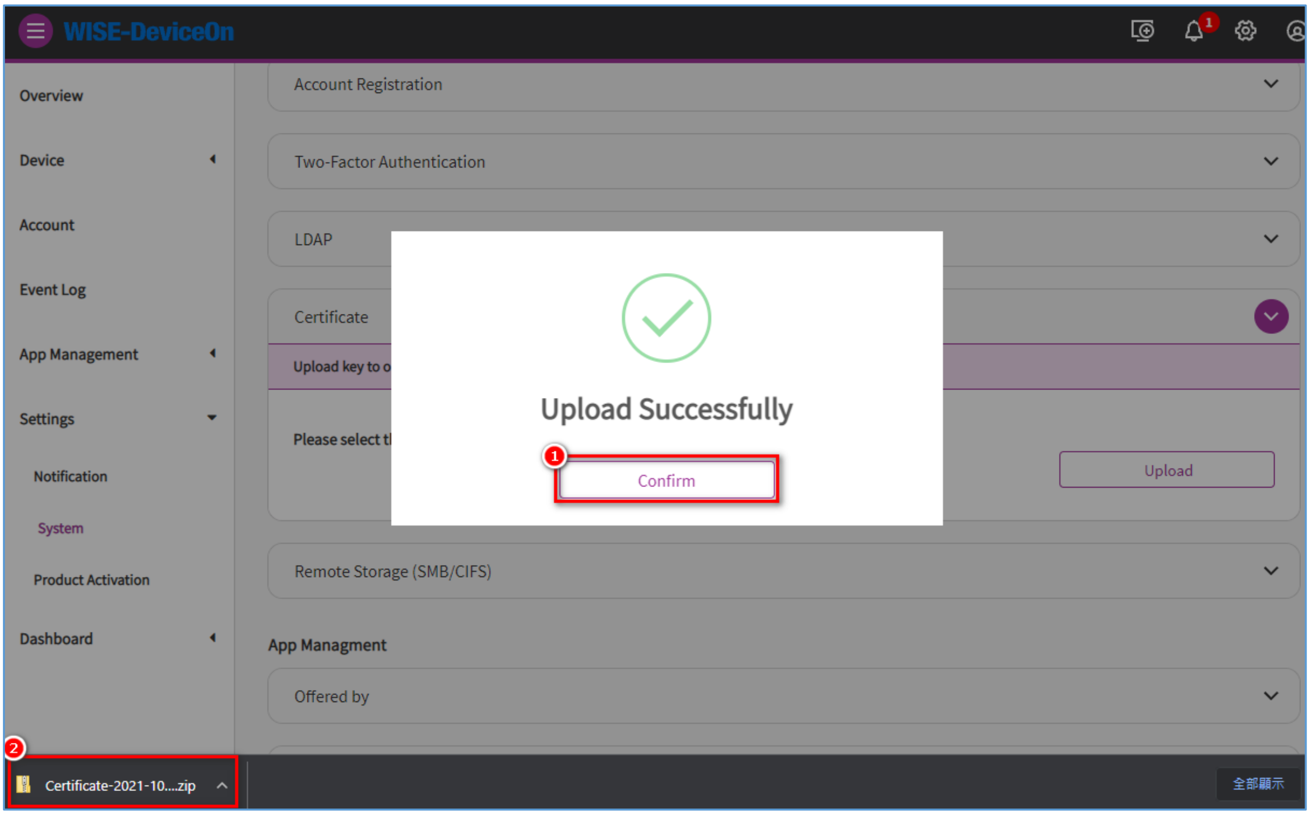
4.9.3 Steps to Download the Credential Files from DeviceOn Server

Step 1: Sign in to the DeviceOn server portal.
Step 2: From the menu on the left, under **Settings**, select **System**.
Step 3: On the right panel, extend **Certificate**, select **Upload** and browser the private key file that you created before.

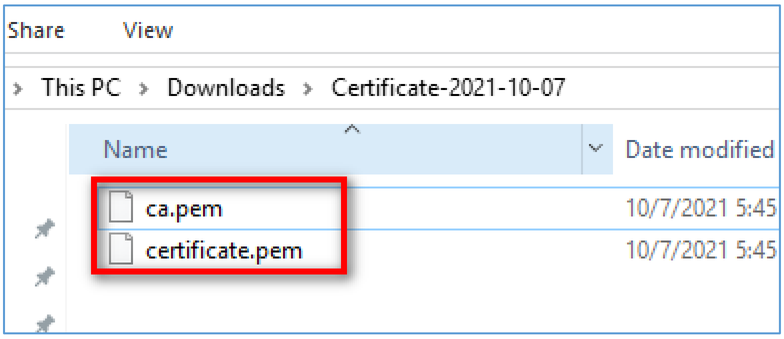

WISE-DeviceOn
1
Overview
Device
Account
Event Log
App Management
1
Settings
Notification
2
System
Account Registration
Two-Factor Authentication
LDAP
3
Certificate
Upload key to obtain security certificate
Please select the key file to upload, the attached file name is key or pem
4
Upload
Remote Storage (SMB/CIFS)



Step 4: If anything well, you should get a zip file named **Certificate-xxxx-xx-xx.zip**.



Step 5: Extract the zip file. There are two files in the zip. One is the client credential files named **certificate.pem** and another is the root certificate **ca.pem**.



4.9.4 Steps to Configure the Setting of WISE-Agent

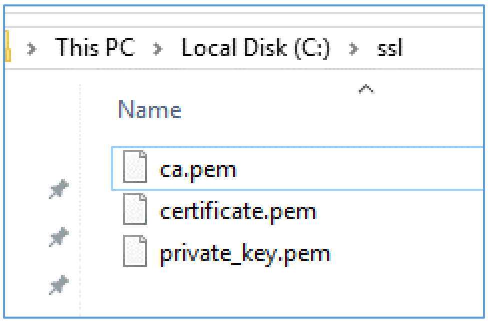
In this session, you will learn how to configure the WISE-Agent and make it connect DeviceOn server through the credential files that generated previously.

To understand this SOP, you should have the knowledge of the following topics:

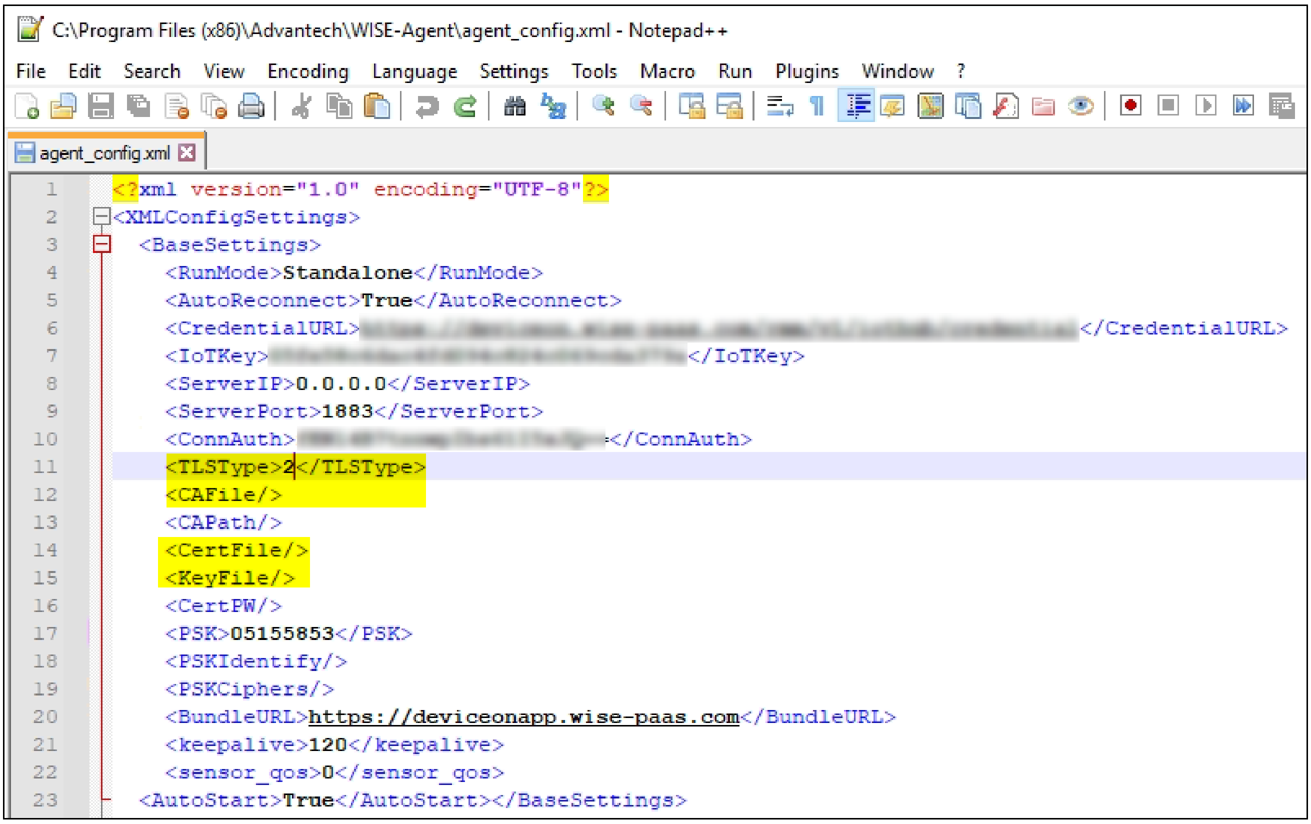
- Where the agent’s configuration file is.
- Adjust the agent’s settings for connecting DeviceOn server through x509.

Step 1: Open the **agent_config.xml** that existed in the installation folder of WISE-Agent.

Step 2: Copy the credential files to a folder **outside** the WISE-Agent installation path. They should contain three files. Just like the following picture



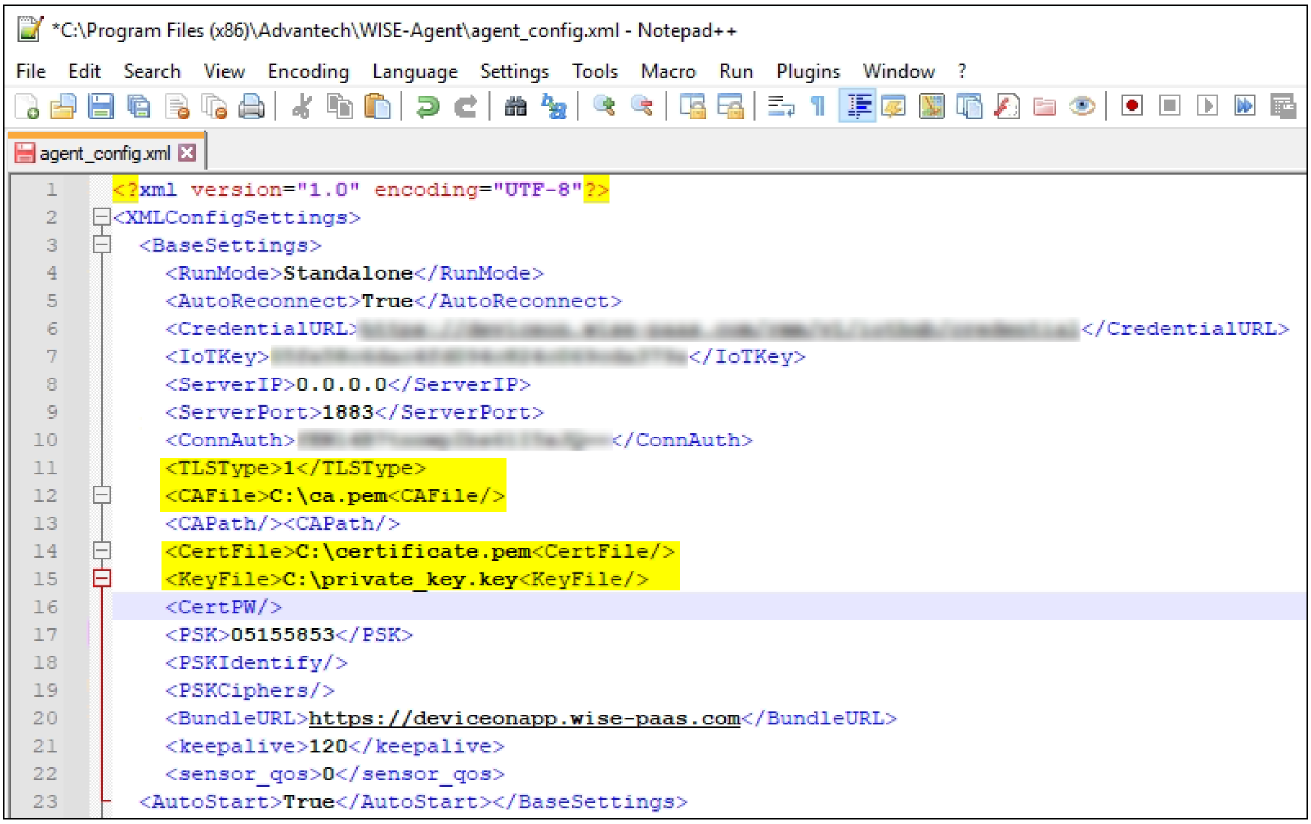
Step 3: Open **agent_config.xml** with your familiar editor. There are four tags which you should adjust. They are **TLSType**, **CAFile**, **CertFile** and **KeyFles**.


C:\Program Files (x86)\Advantech\WISE-Agent\agent_config.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
agent_config.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<XMLConfigSettings>
  <BaseSettings>
    <RunMode>Standalone</RunMode>
    <AutoReconnect>True</AutoReconnect>
    <CredentialURL>[redacted]</CredentialURL>
    <IoTKey>[redacted]</IoTKey>
    <ServerIP>0.0.0.0</ServerIP>
    <ServerPort>1883</ServerPort>
    <ConnAuth>[redacted]</ConnAuth>
    <TLSType>2</TLSType>
    <CAFile/>
    <CAPath/>
    <CertFile/>
    <KeyFile/>
    <CertPW/>
    <PSK>05155853</PSK>
    <PSKIdentify/>
    <PSKCiphers/>
    <BundleURL>https://deviceonapp.wise-paas.com</BundleURL>
    <keepalive>120</keepalive>
    <sensor_qos>0</sensor_qos>
  <AutoStart>True</AutoStart></BaseSettings>
```

Step 4: Configure the TLSType, CAFile, CertFile and KeyFile as below.

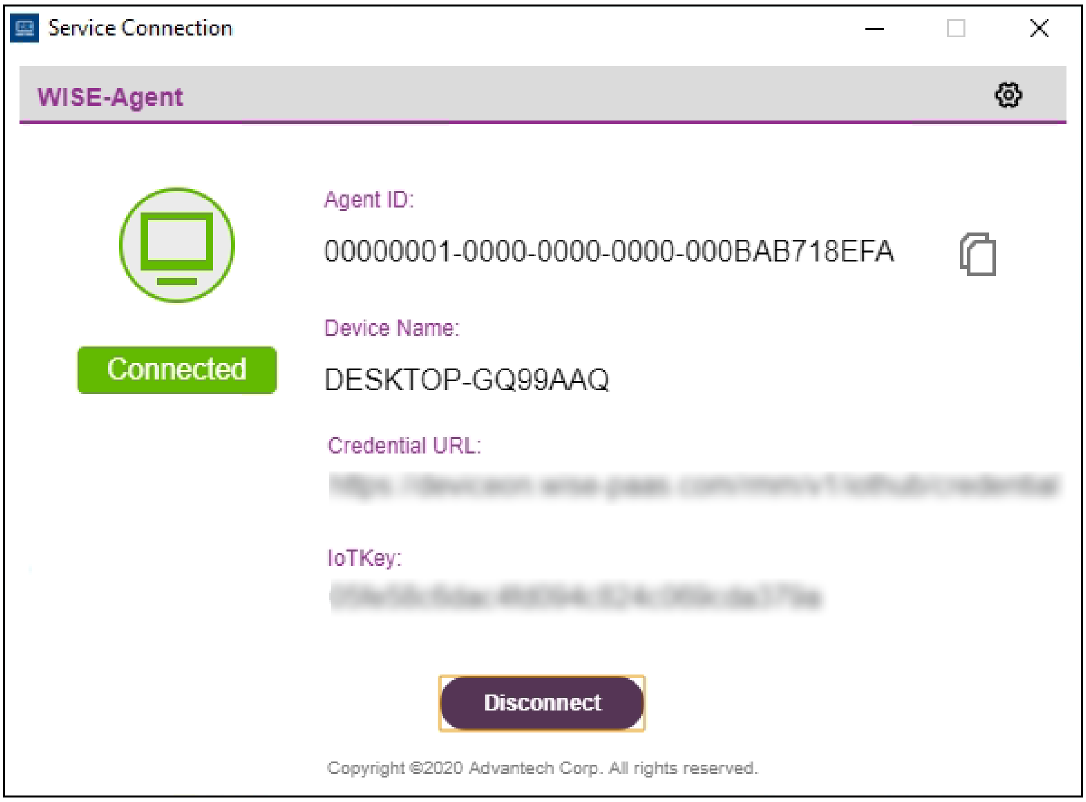
- TLSType to **1**.
- CAFile to **<Credential Path>\ca.pem**
- CertFile to **<Credential Path>\certificate.pem**
- KeyFile to **<Credential Path>\Private_Key.key**



*C:\Program Files (x86)\Advantech\WISE-Agent\agent_config.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
agent_config.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<XMLConfigSettings>
  <BaseSettings>
    <RunMode>Standalone</RunMode>
    <AutoReconnect>True</AutoReconnect>
    <CredentialURL>[redacted]</CredentialURL>
    <IoTKey>[redacted]</IoTKey>
    <ServerIP>0.0.0.0</ServerIP>
    <ServerPort>1883</ServerPort>
    <ConnAuth>[redacted]</ConnAuth>
    <TLSType>1</TLSType>
    <CAFile>C:\ca.pem<CAFile/>
    <CAPath/><CAPath/>
    <CertFile>C:\certificate.pem<CertFile/>
    <KeyFile>C:\private_key.key<KeyFile/>
    <CertPW/>
    <PSK>05155853</PSK>
    <PSKIdentify/>
    <PSKCiphers/>
    <BundleURL>https://deviceonapp.wise-paas.com</BundleURL>
    <keepalive>120</keepalive>
    <sensor_qos>0</sensor_qos>
  <AutoStart>True</AutoStart></BaseSettings>
```

Step 5: Save **agent_config.xml** and reconnect to server. If anything goes well, the WISE-Agent should show connected.



Agent ID:
00000001-0000-0000-0000-000BAB718EFA

Device Name:
DESKTOP-GQ99AAQ

Credential URL:
[redacted]

IoTKey:
[redacted]

Copyright ©2020 Advantech Corp. All rights reserved.

5. DeviceOn Development Guide

5.1 WISE-Agent Plugin Development

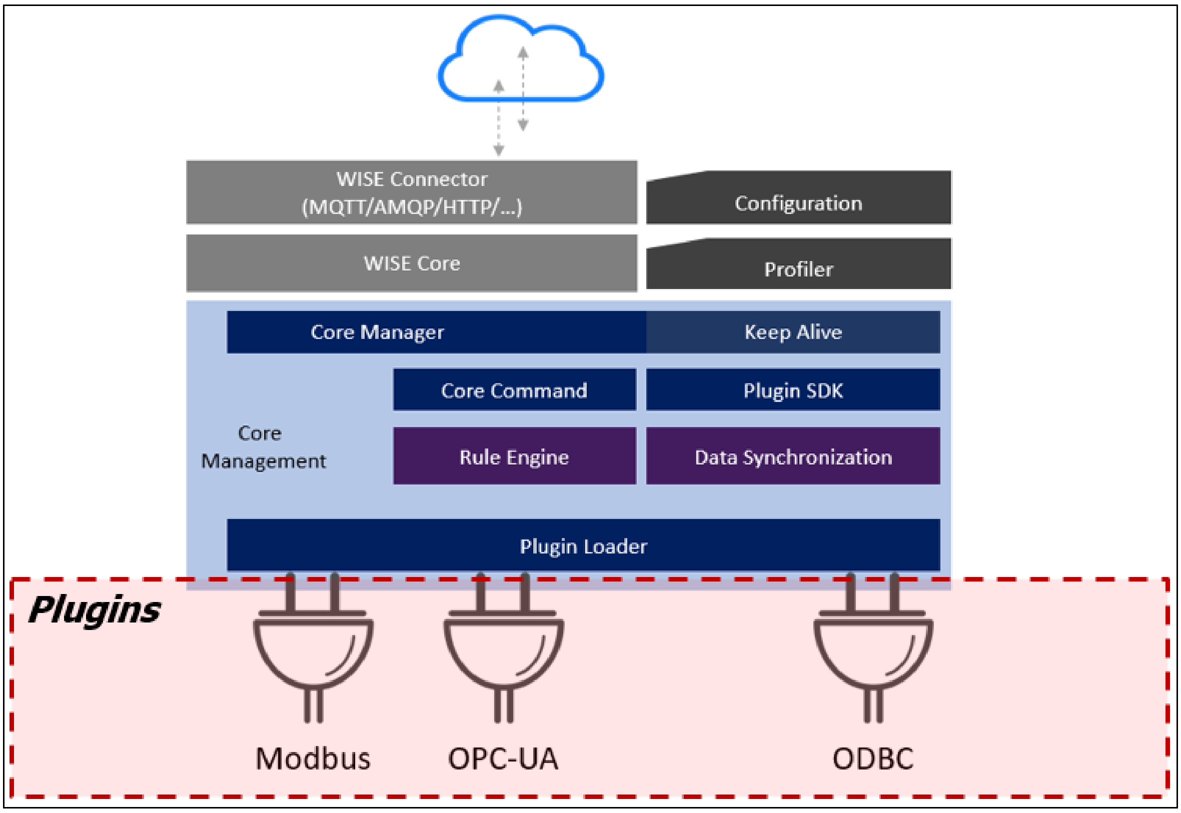
Advantech provides an edge software tool to communicate and exchange information between IoT (Internet of Thing) devices and DeviceOn cloud, called a WISE-Agent. The WISE-Agent not only provides a rich set of users friendly, intelligent, standardization and scalability.

- **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 IoTHub 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.

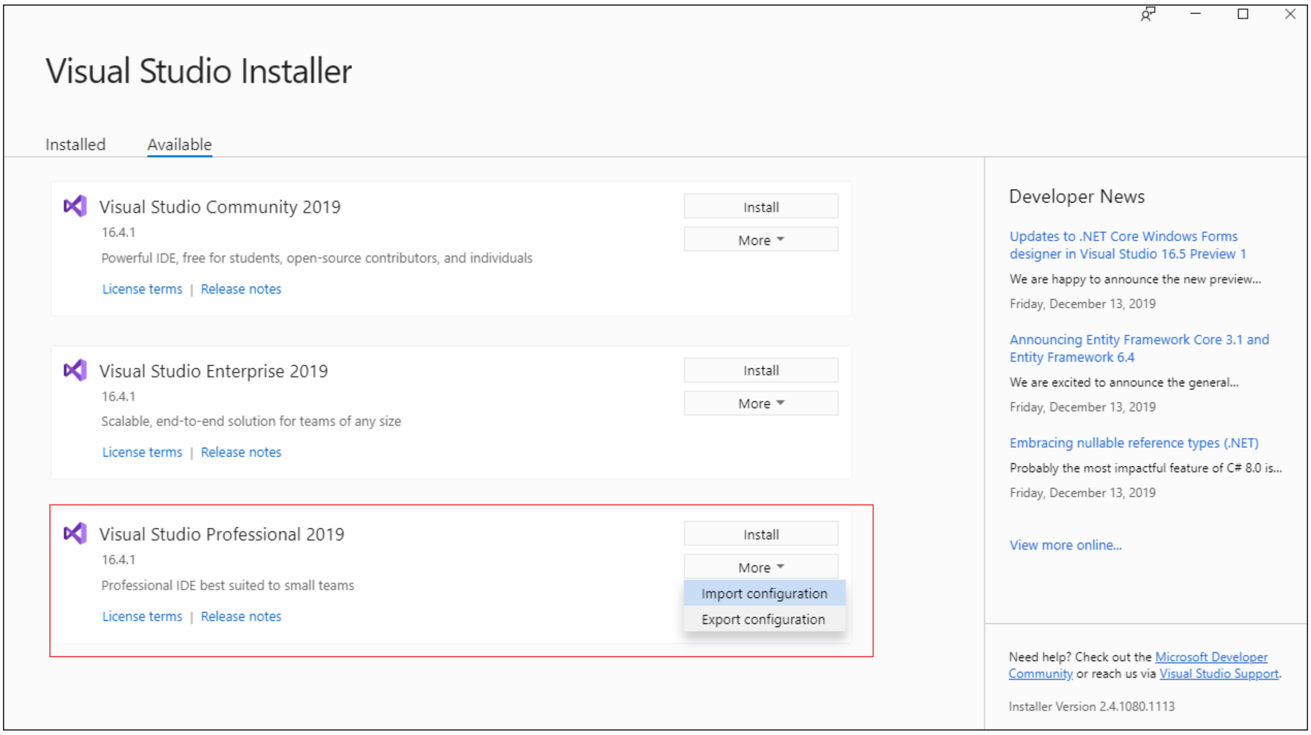
- ✧ **SUSI Control**: Monitoring and Control Advantech Hardware Platform
- ✧ **HDD Monitoring:** Monitoring Hard Drives (HDD, SSD) Usage, Healthy and S.M.A.R.T Information, especially for Advantech SQFlash.
- ✧ **Network Monitoring:** Monitoring Network Interface Usage, Throughput…
- ✧ **Process Monitoring:** 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 for Windows Plugin
- Android NDK for Android Plugin
- 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



Visual Studio Installer

Visual Studio Community 2019
16.4.1
Powerful IDE, free for students, open-source contributors, and individuals

Visual Studio Enterprise 2019
16.4.1
Scalable, end-to-end solution for teams of any size

Visual Studio Professional 2019
16.4.1
Professional IDE best suited to small teams

Developer News

Updates to .NET Core Windows Forms designer in Visual Studio 16.5 Preview 1
We are happy to announce the new preview...
Friday, December 13, 2019

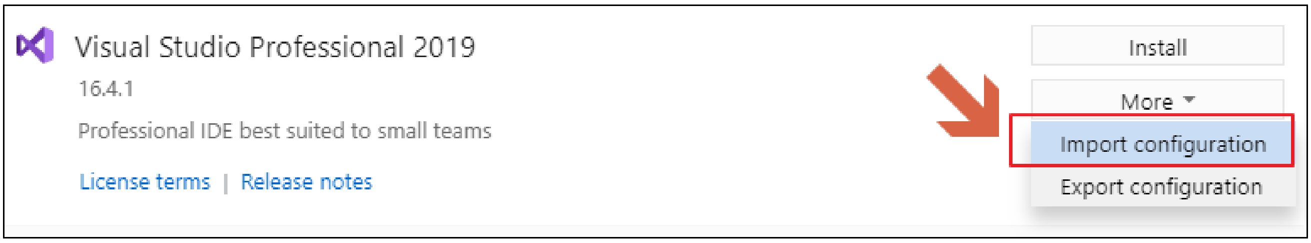
Announcing Entity Framework Core 3.1 and Entity Framework 6.4
We are excited to announce the general...
Friday, December 13, 2019

Embracing nullable reference types (.NET)
Probably the most impactful feature of C# 8.0 is...
Friday, December 13, 2019

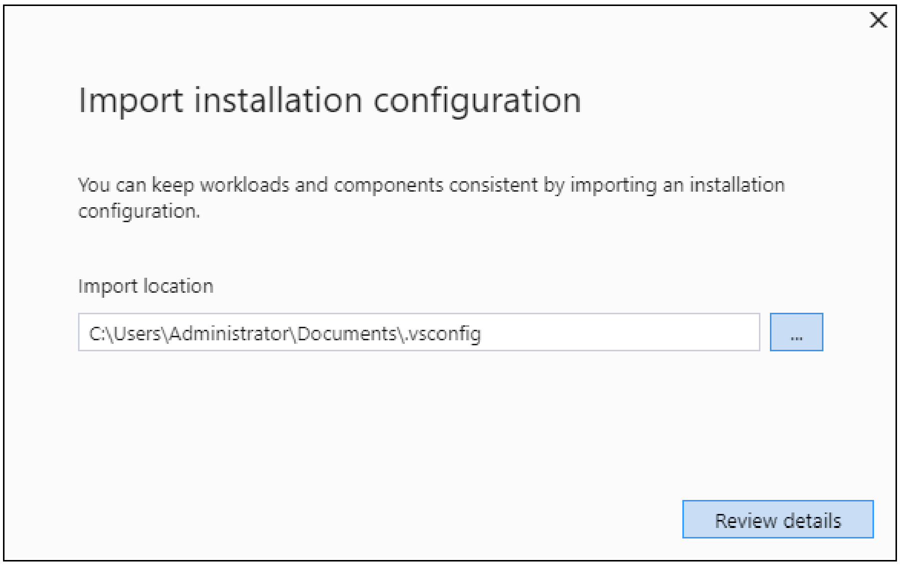
View more online...

Need help? Check out the Microsoft Developer Community or reach us via Visual Studio Support.

Installer Version 2.4.1080.1113



Visual Studio Professional 2019
16.4.1
Professional IDE best suited to small teams



Import installation configuration

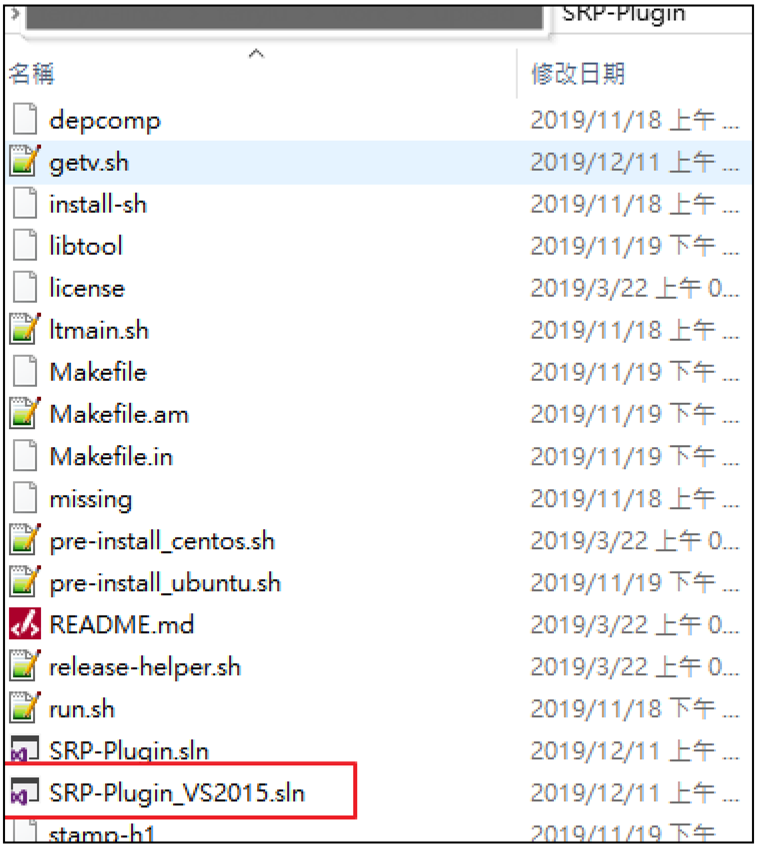
You can keep workloads and components consistent by importing an installation configuration.

Import location: C:\Users\Administrator\Documents\.vsconfig

Step 2: Download SRP-Plugin,

https://gitlab.edgecenter.io/ei-paas-edge-connect/SRP-Plugin

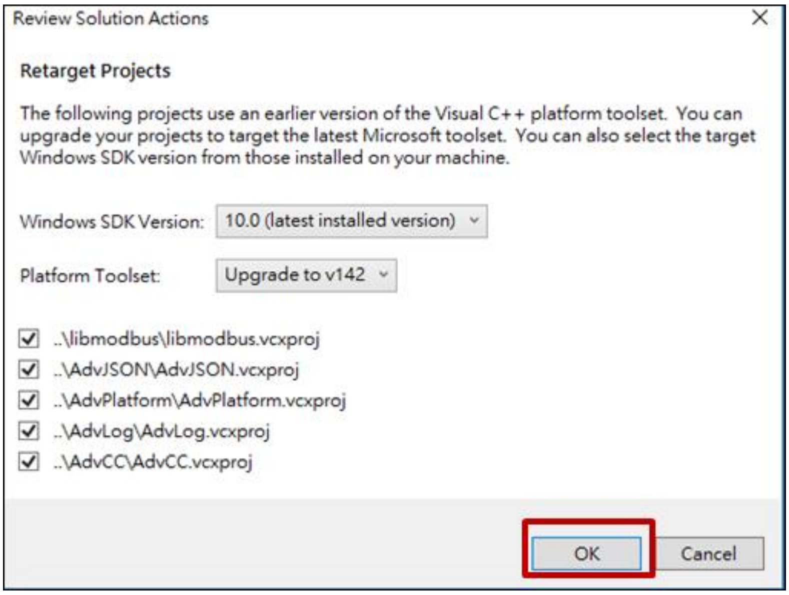
Step 3: Open SRP-Plugin solution file, **SRP-Plugin-V2015.sln**



[redacted] SRP-Plugin

名稱	修改日期
depcomp	2019/11/18 上午 ...
getv.sh	2019/12/11 上午 ...
install-sh	2019/11/18 上午 ...
libtool	2019/11/19 下午 ...
license	2019/3/22 上午 0...
ltmain.sh	2019/11/18 上午 ...
Makefile	2019/11/19 下午 ...
Makefile.am	2019/11/19 下午 ...
Makefile.in	2019/11/19 下午 ...
missing	2019/11/18 上午 ...
pre-install_centos.sh	2019/3/22 上午 0...
pre-install_ubuntu.sh	2019/11/19 下午 ...
README.md	2019/3/22 上午 0...
release-helper.sh	2019/3/22 上午 0...
run.sh	2019/11/18 下午 ...
SRP-Plugin.sln	2019/12/11 上午 ...
SRP-Plugin_VS2015.sln	2019/12/11 上午 ...
stamp-h1	2019/11/19 下午

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



Review Solution Actions

Retarget Projects

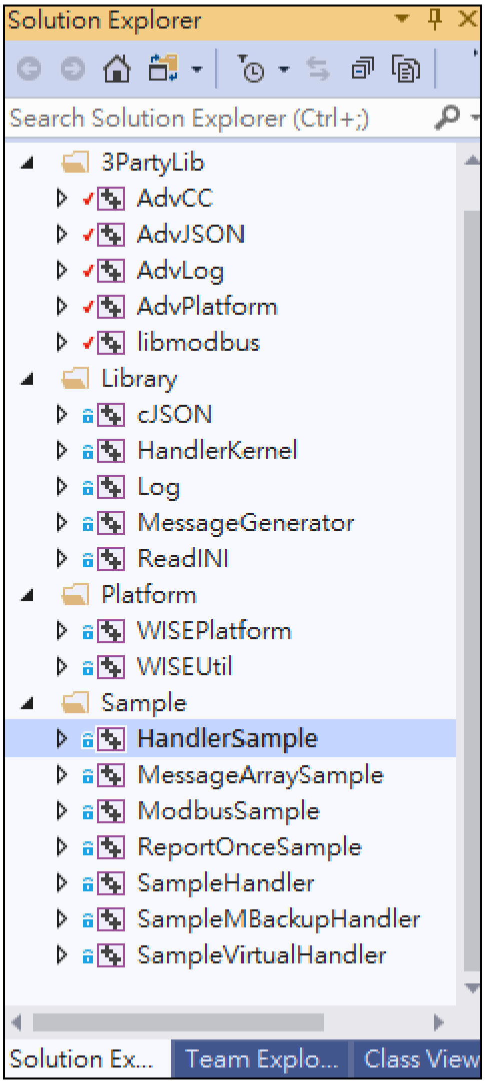
The following projects use an earlier version of the Visual C++ platform toolset. You can upgrade your projects to target the latest Microsoft toolset. You can also select the target Windows SDK version from those installed on your machine.

Windows SDK Version: 10.0 (latest installed version)

Platform Toolset: Upgrade to v142

☑ ..\libmodbus\libmodbus.vcxproj
☑ ..\AdvJSON\AdvJSON.vcxproj
☑ ..\AdvPlatform\AdvPlatform.vcxproj
☑ ..\AdvLog\AdvLog.vcxproj
☑ ..\AdvCC\AdvCC.vcxproj

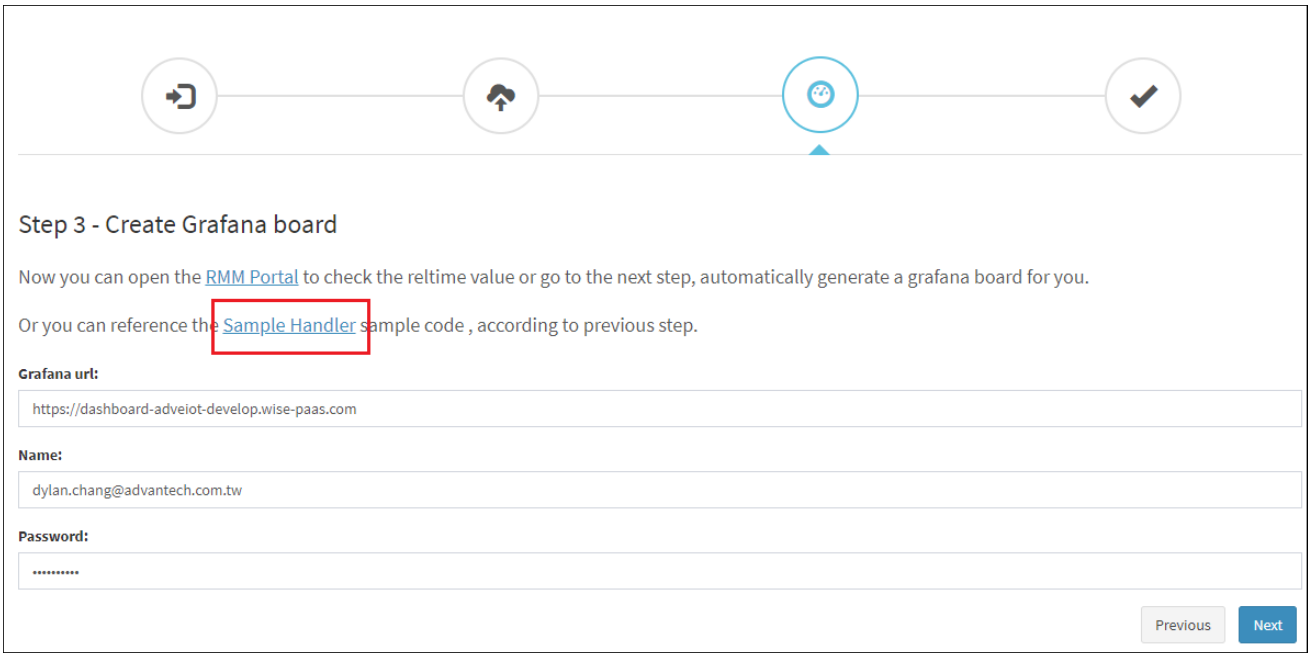
Step 5: You can implement new plugin base on plugin sample project.



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:

https://dashboard-adveiot-develop.wise-paas.com

Name:

dylan.chang@advantech.com.tw

Password:

••••••••••

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.

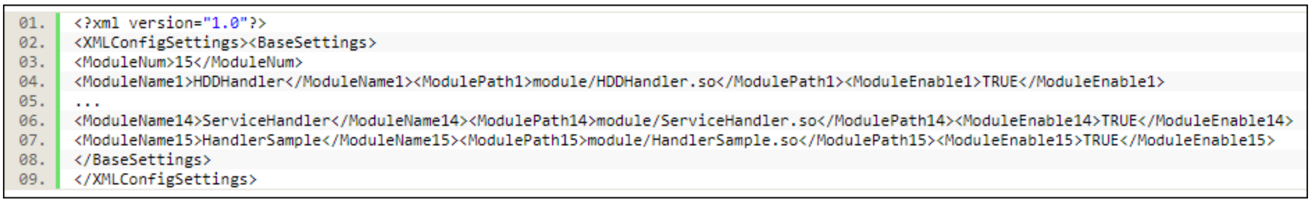
Step 11: After successfully completing the compilation, you can find all the **.dll** files in below path “**SRP-Plugin\Debug\module**”

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.

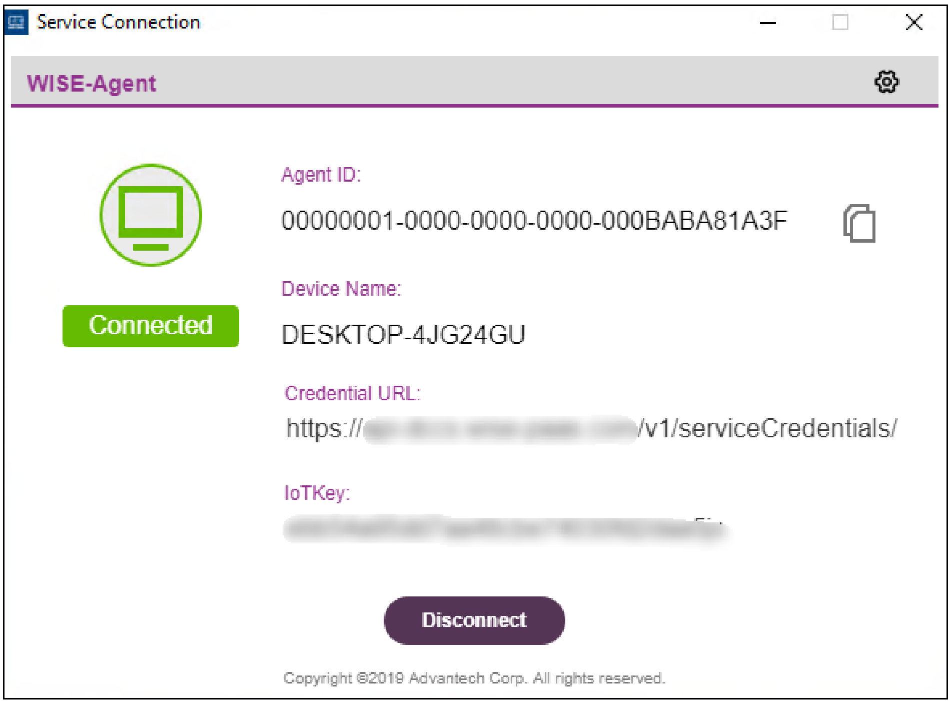
Step 14: Modify **module_config.xml** on “C:\Program Files (x86)\Advantech\WISE-Agent\module\module_config.xml”

- 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”.



Agent ID:
00000001-0000-0000-0000-000BABA81A3F

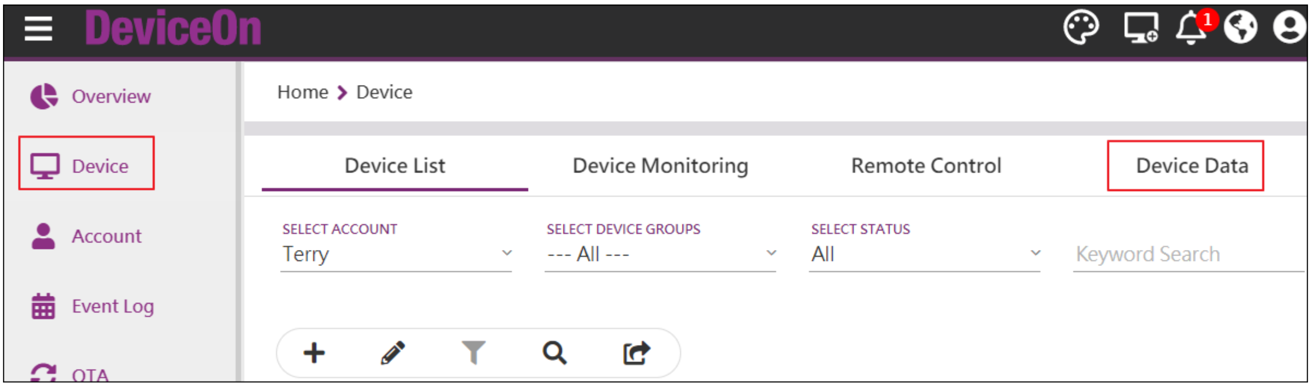
Device Name:
DESKTOP-4JG24GU

Credential URL:
https://[redacted]/v1/serviceCredentials/

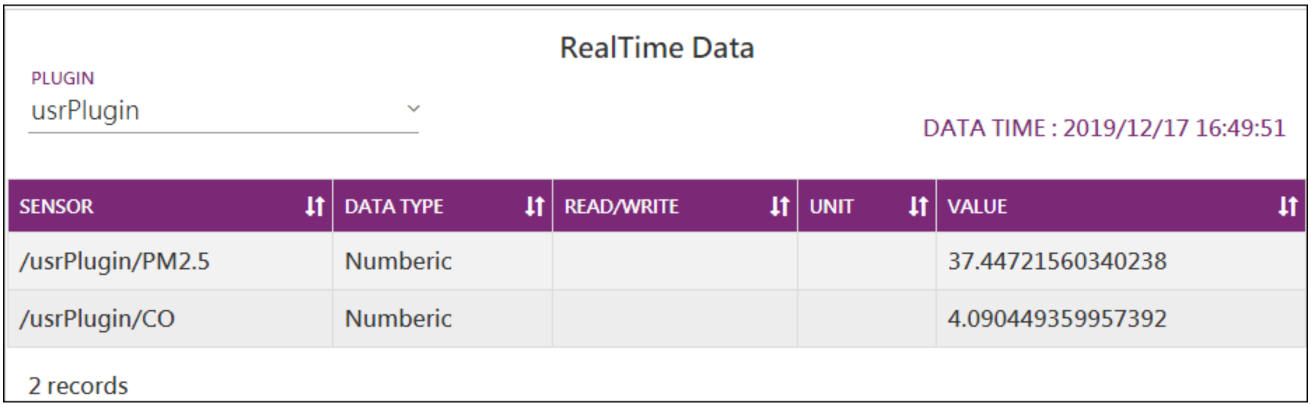
IoTKey:
[redacted]

Copyright ©2019 Advantech Corp. All rights reserved.

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



SELECT ACCOUNT: Terry
SELECT DEVICE GROUPS: --- All ---
SELECT STATUS: All



RealTime Data

PLUGIN: usrPlugin

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

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

2 records

5.1.4 Develop a Plugin on Linux Environment

5.1.5 Multiple Languages Support in Linux Plugin

The DeviceOn handshake protocol only supports UTF-8 encoded string. WISE-Agent for Windows platform will automatically convert the ANSI string to UTF-8 string. But in the Linux platform, plugin developers need to maintain the string conversion with the iconv library themselves.

Step 1: Prepare the compile environment with **iconv** library. In some cross-compile, developers may need to download **iconv** source code and cross-compile yourself.

Step 2: Add **iconv** include into source code

```
#include "iconv.h"
```

Step 3: Add Convert API into source code, the sample code is converted GB2312 to UTF-8

```
int GB2312ToUTF8(char* pOut, int iOutLen, const char* pIn, int iInLen)
{
        int len = -1;
        char* inbuff = (char*) pIn;
        char* outbuff = calloc(1, iOutLen);
        iconv_t cd;
        size_t inlen = iInLen;
        size_t outlen = iOutLen;

        cd = iconv_open("utf-8", "gb2312");
        if (cd==(iconv_t)-1)
                return len;
        len = iconv(cd, &inbuff, &inlen, &outbuff, &outlen);

        return len;
}
```

Step 4: Convert the multi-language string to UTF-8 before insert into JSON string

```
char utf8value[32] = {0};
char gbvalue[32] = "some GB2312 string";

GB2312ToUTF8(utf8value, sizeof(utf8value), gbvalue, 4);
srand(time(NULL));
ret = createTagValJson(data, sizeof(data),
                  "pm2.5", TYPE_FLOAT( (double)(rand()%20) +
(rand()%10)/10.0 ),     // 0.0 ~ 20.0
                  "enabled", TYPE_BOOL( (rand()%2==0)?false:true ),
                  "notify", TYPE_NULL(),
                  "level", TYPE_INT(rand()%5), // 0~5
                  "description", TYPE_STRING(utf8value),
                  NULL);
fprintf(stderr, "sensor json: [%s]\n", data);
```

Step 5: In Makefile, developers may need to add '**-liconv**' in LDFLAGS

5.1.6 Develop a Plugin on Android Environment

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

Step 2: In Plugin SDK (SRP-Plugin) folder, execute **android_build.sh**, where

- CMD : -b : build, -c : clean
- APP_ABI : x86, armeabi-v7a and so on

For example, to build an armeabi-v7a arch plugin you may enter:

source android_build.sh -b armeabi-v7a &

Step 3: You can find the release build file in
"**SRP-Plugin/~/obj/local/armeabi-v7a/libHandlerSample.so**" folder.

Step 4: Copy **libHandlerSample.so** to DUT in the **/system/lib/module/**.
Step 5: Modify **module_config.xml in** DUT as 5.1.3 step 14 described.
Step 6: Check handler as 5.1.3 step 16 described.

5.2 DeviceOn UI Plugin Development

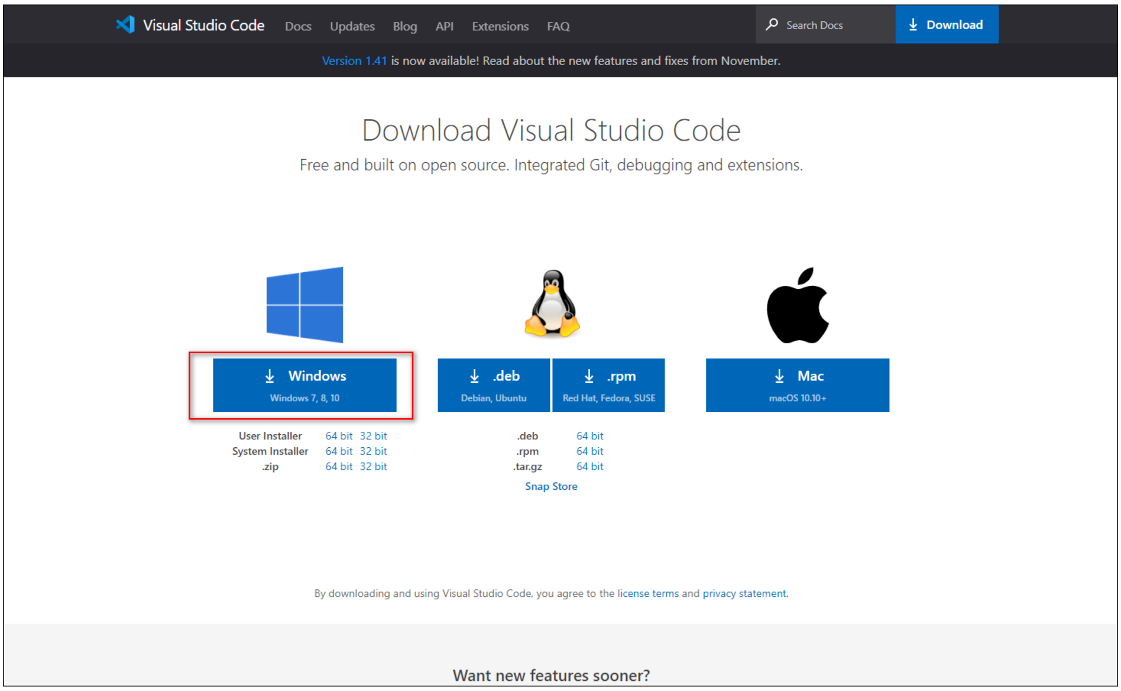
Actually, DeviceOn provide plenty of features to remote management, control to your edge devices, but it's hard to meet all domains application, such as, medical, traffic, energy system and etc. Fortunately, DeviceOn provide APIs and Addins (web user interface) for users to develop their own solution.

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.



Version 1.41 is now available! Read about the new features and fixes from November.

Download Visual Studio Code

Free and built on open source. Integrated Git, debugging and extensions.

User Installer	64 bit	32 bit
System Installer	64 bit	32 bit
.zip	64 bit	32 bit

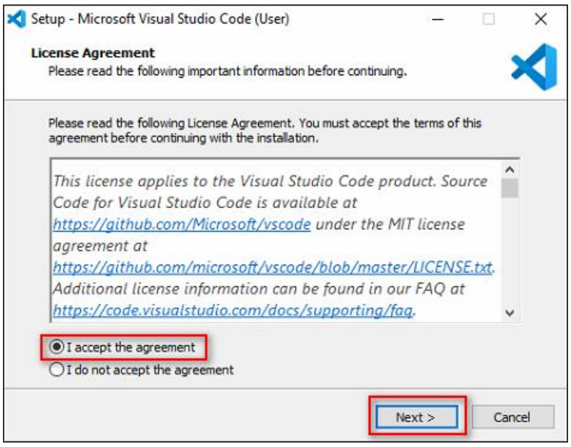
.deb	64 bit
.rpm	64 bit
.tar.gz	64 bit

Snap Store

By downloading and using Visual Studio Code, you agree to the license terms and privacy statement.

Want new features sooner?

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

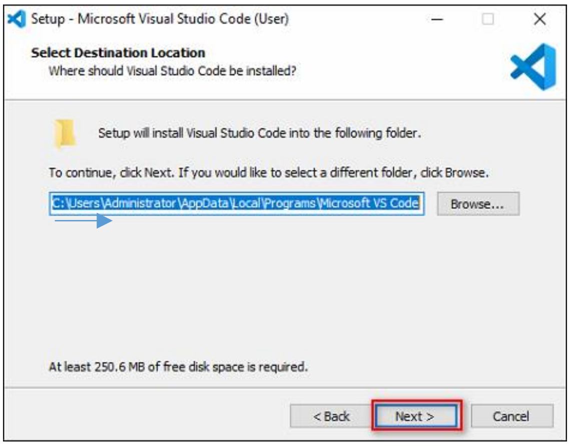

Setup - Microsoft Visual Studio Code (User)

License Agreement
Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

This license applies to the Visual Studio Code product. Source Code for Visual Studio Code is available at https://github.com/Microsoft/vscode under the MIT license agreement at https://github.com/microsoft/vscode/blob/master/LICENSE.txt. Additional license information can be found in our FAQ at https://code.visualstudio.com/docs/supporting/faq.

● I accept the agreement
○ I do not accept the agreement


Setup - Microsoft Visual Studio Code (User)

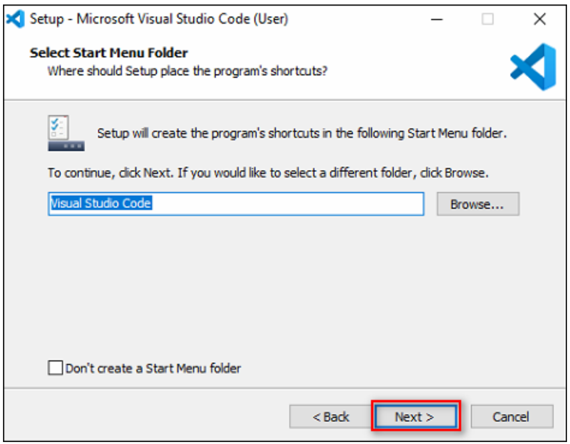
Select Destination Location
Where should Visual Studio Code be installed?

Setup will install Visual Studio Code into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Users\Administrator\AppData\Local\Programs\Microsoft VS Code

At least 250.6 MB of free disk space is required.



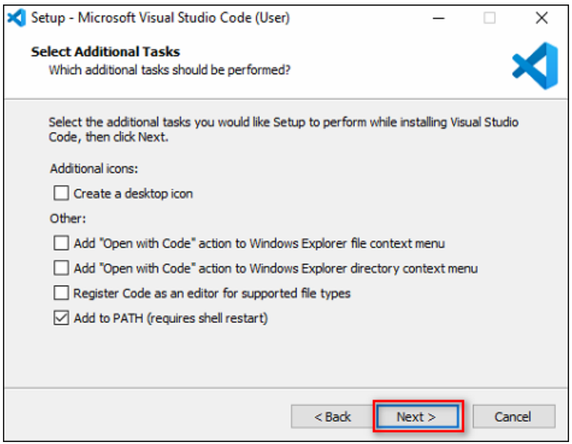
Setup - Microsoft Visual Studio Code (User)

Select Start Menu Folder
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

Visual Studio Code

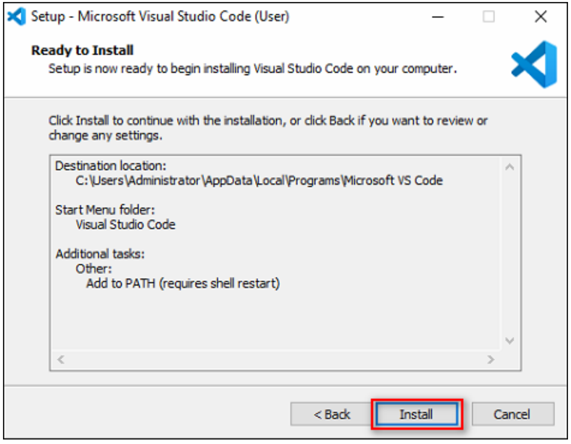


Setup - Microsoft Visual Studio Code (User)

Select Additional Tasks
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing Visual Studio Code, then click Next.

Additional icons:
□ Create a desktop icon
Other:
□ Add "Open with Code" action to Windows Explorer file context menu
□ Add "Open with Code" action to Windows Explorer directory context menu
□ Register Code as an editor for supported file types
☑ Add to PATH (requires shell restart)

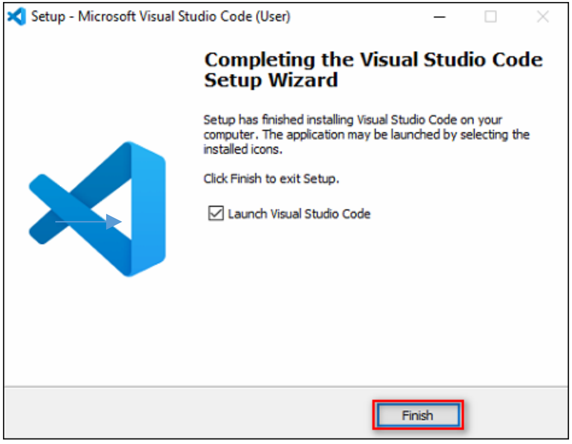


Setup - Microsoft Visual Studio Code (User)

Ready to Install
Setup is now ready to begin installing Visual Studio Code on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
    C:\Users\Administrator\AppData\Local\Programs\Microsoft VS Code

Start Menu folder:
    Visual Studio Code

Additional tasks:
    Other:
      Add to PATH (requires shell restart)
```



Setup - Microsoft Visual Studio Code (User)

Completing the Visual Studio Code Setup Wizard

Setup has finished installing Visual Studio Code on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ Launch Visual Studio Code

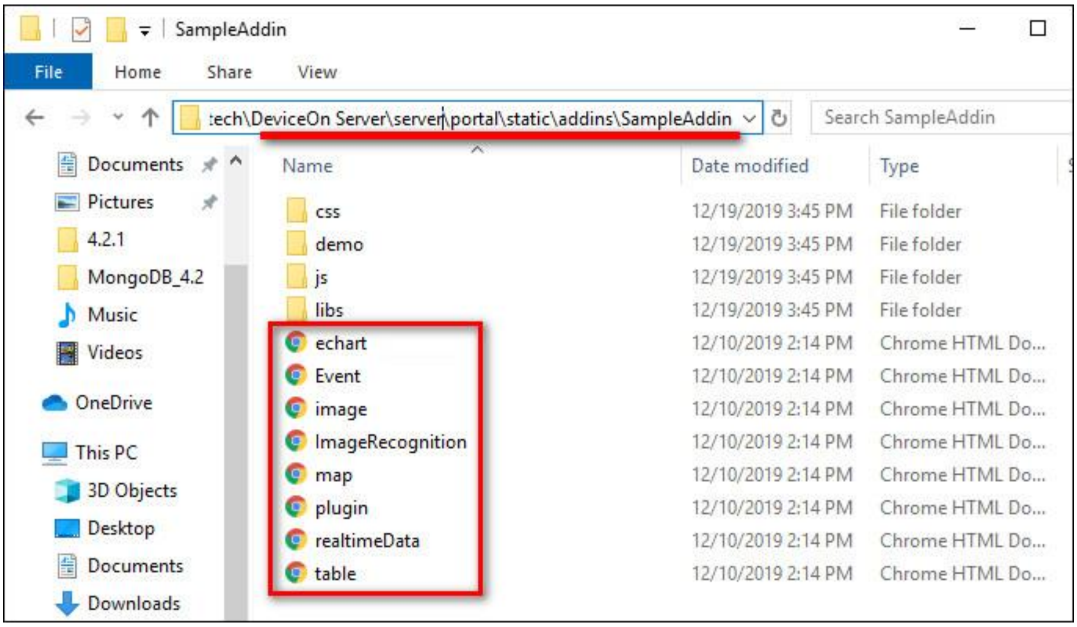
Step 3: Install DeviceOn Server, if you don't install DeviceOn Server before, please reference Section 2.2.

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**.

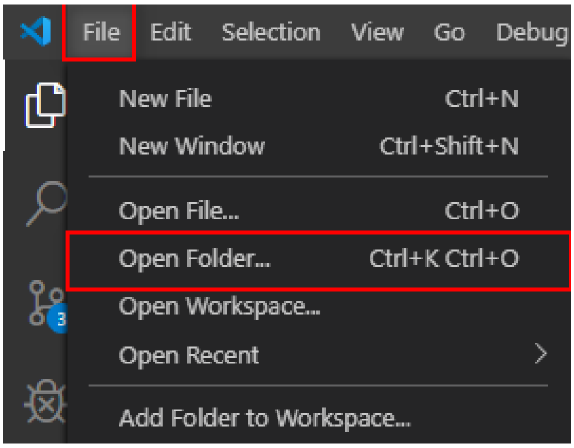
Here are serval Add-in examples (***.html**) that we provide, for your reference.



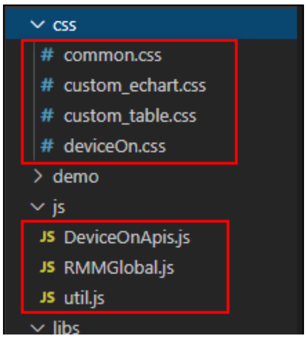
Name	Date modified	Type
css	12/19/2019 3:45 PM	File folder
demo	12/19/2019 3:45 PM	File folder
js	12/19/2019 3:45 PM	File folder
libs	12/19/2019 3:45 PM	File folder
echart	12/10/2019 2:14 PM	Chrome HTML Do...
Event	12/10/2019 2:14 PM	Chrome HTML Do...
image	12/10/2019 2:14 PM	Chrome HTML Do...
ImageRecognition	12/10/2019 2:14 PM	Chrome HTML Do...
map	12/10/2019 2:14 PM	Chrome HTML Do...
plugin	12/10/2019 2:14 PM	Chrome HTML Do...
realtimeData	12/10/2019 2:14 PM	Chrome HTML Do...
table	12/10/2019 2:14 PM	Chrome HTML Do...

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

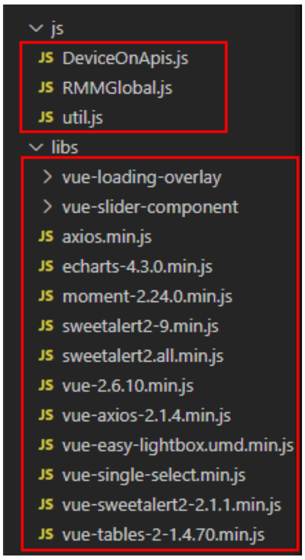
\DeviceOn Server\server\portal\static\addins\SampleAddin\



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



css
common.css
custom_echart.css
custom_table.css
deviceOn.css
demo
js
DeviceOnApis.js
RMMGlobal.js
util.js
libs

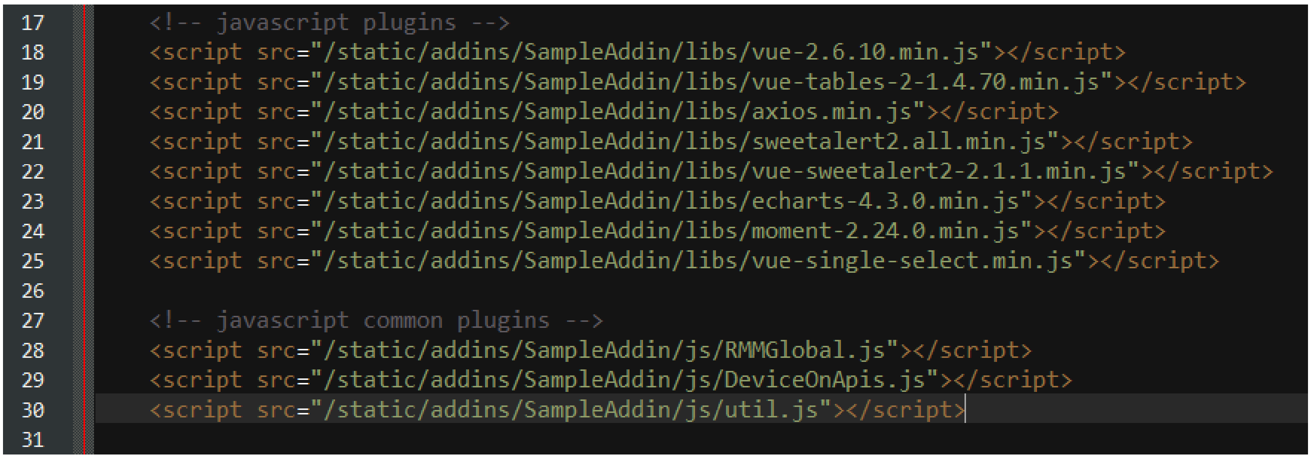


js
DeviceOnApis.js
RMMGlobal.js
util.js
libs
vue-loading-overlay
vue-slider-component
axios.min.js
echarts-4.3.0.min.js
moment-2.24.0.min.js
sweetalert2-9.min.js
sweetalert2.all.min.js
vue-2.6.10.min.js
vue-axios-2.1.4.min.js
vue-easy-lightbox.umd.min.js
vue-single-select.min.js
vue-sweetalert2-2.1.1.min.js
vue-tables-2-1.4.70.min.js

- **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.

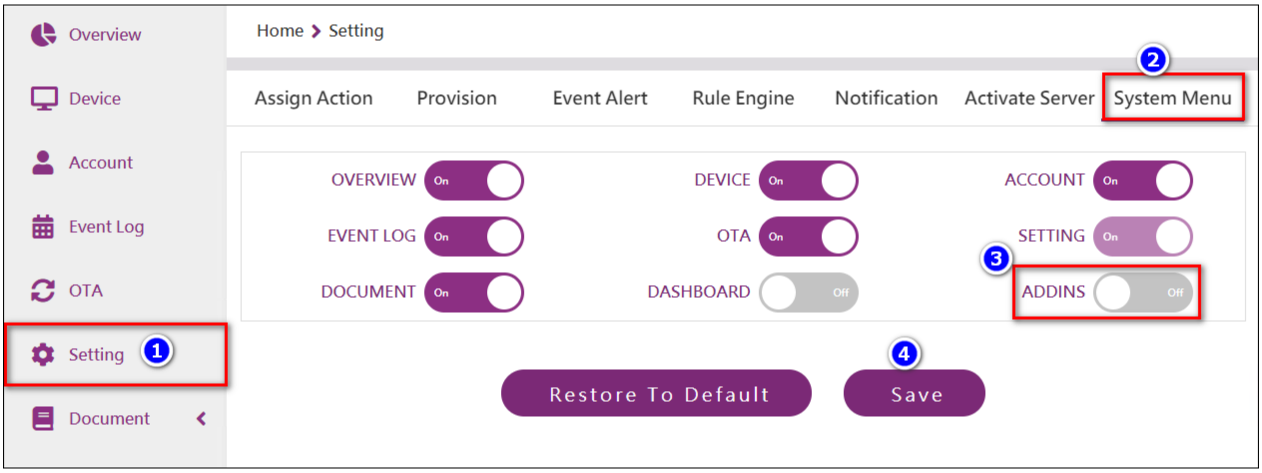
Line 18 to 30 (demo.html) to include java script library, you could place your library in the relative path, or alternatively, given library URL from CDNjs.



```
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
```

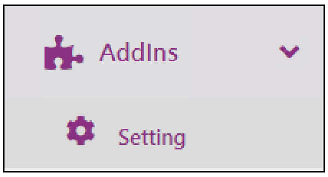
```
<!-- CDNjs-->
<script src="https://code.jquery.com/jquery.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/3.3.7/js/bootstrap.min.js"></script>
```

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

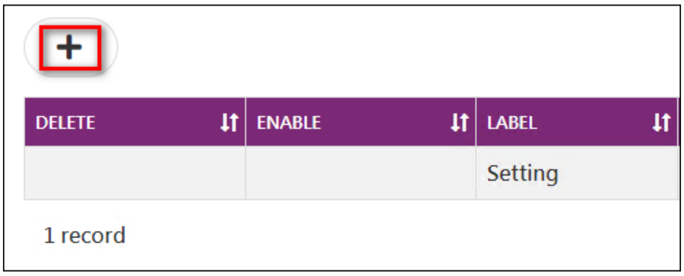


OVERVIEW	On	DEVICE	On	ACCOUNT	On
EVENT LOG	On	OTA	On	SETTING	On
DOCUMENT	On	DASHBOARD	Off	ADDINS	Off

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

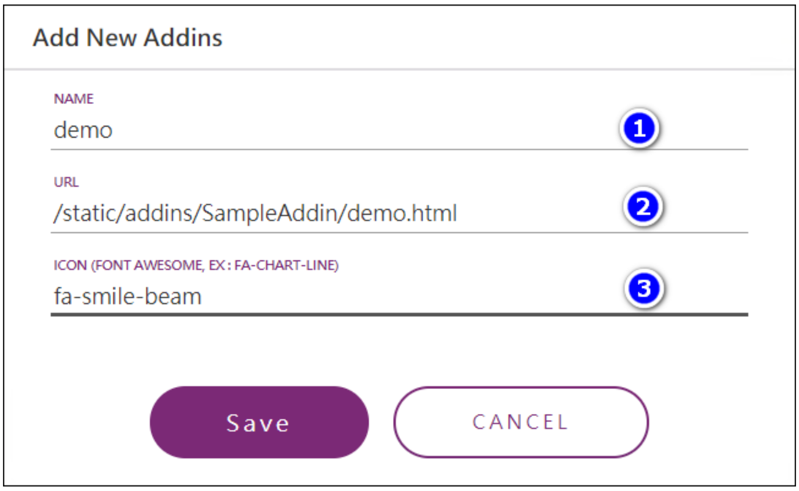


Step 6: Click on the “**Setting**” (**Addins** -> **Setting**) to add your Addins.



DELETE	ENABLE	LABEL
		Setting

1 record


Add New Addins

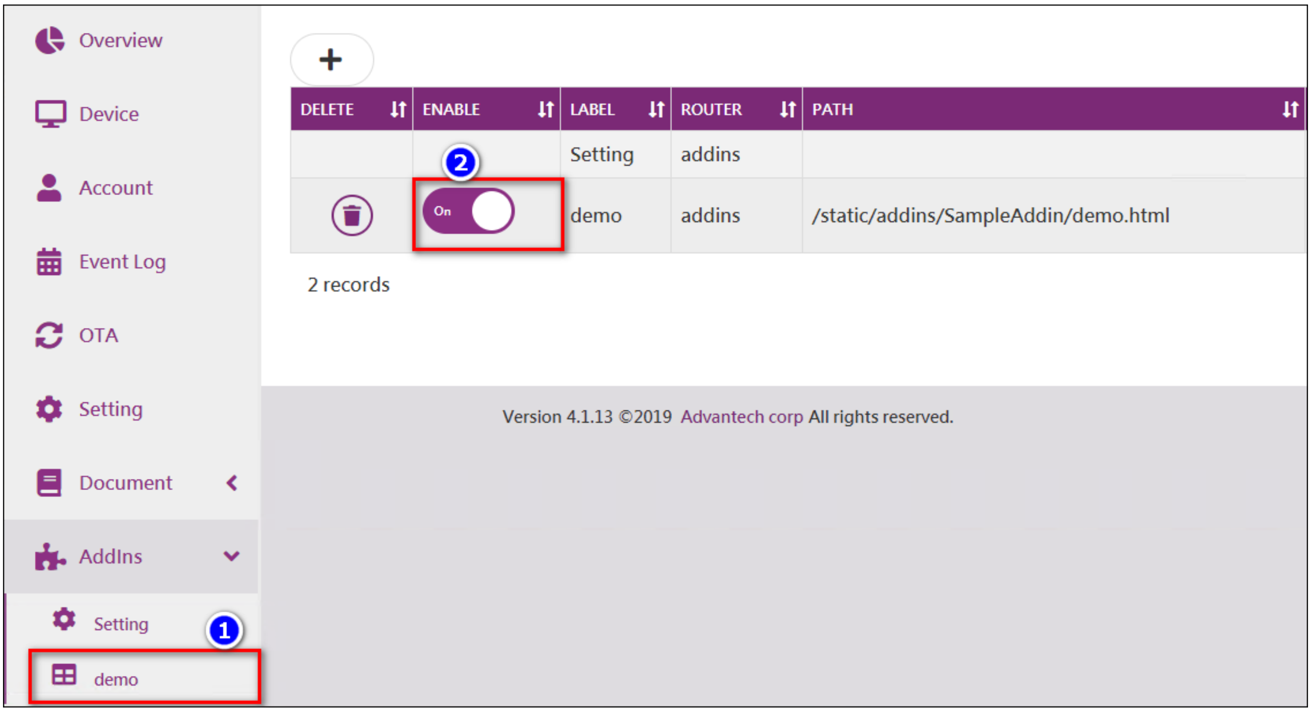
NAME
demo

URL
/static/addins/SampleAddin/demo.html

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

- **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.

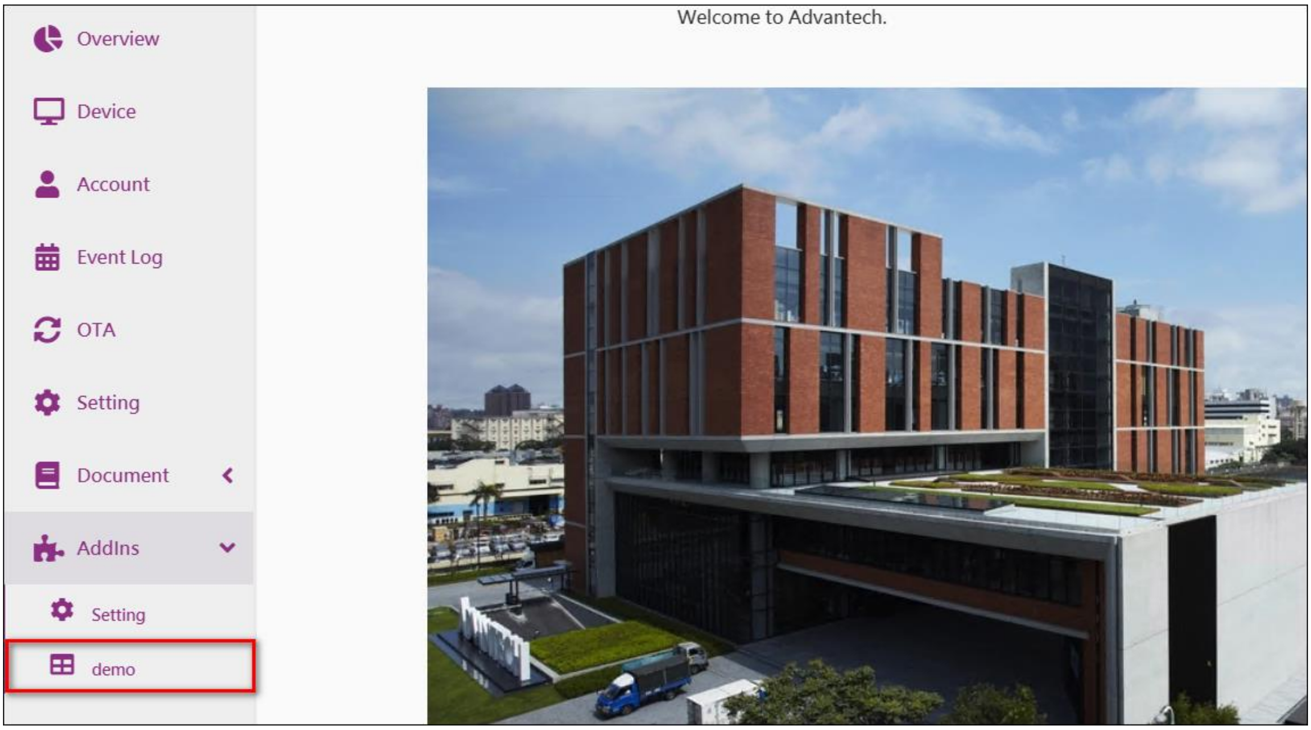


DELETE	ENABLE	LABEL	ROUTER	PATH
		Setting	addins	
	On	demo	addins	/static/addins/SampleAddin/demo.html

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.

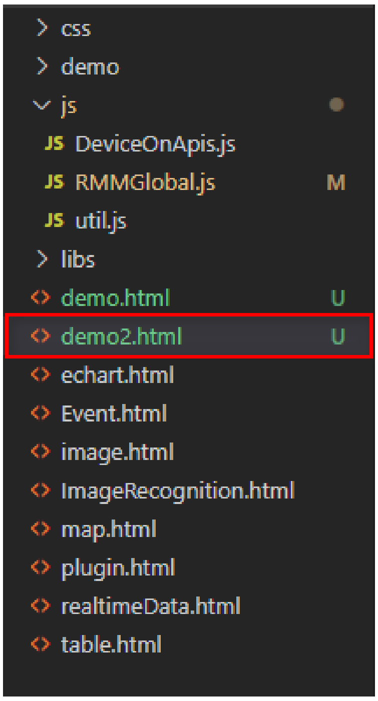
3. DeviceOnApis.devicegroups.get.devicesAll(data)

   To get all devices which under this aid's account from database.

4. DeviceOnApis.devicegroups.get.devices(gid, data)

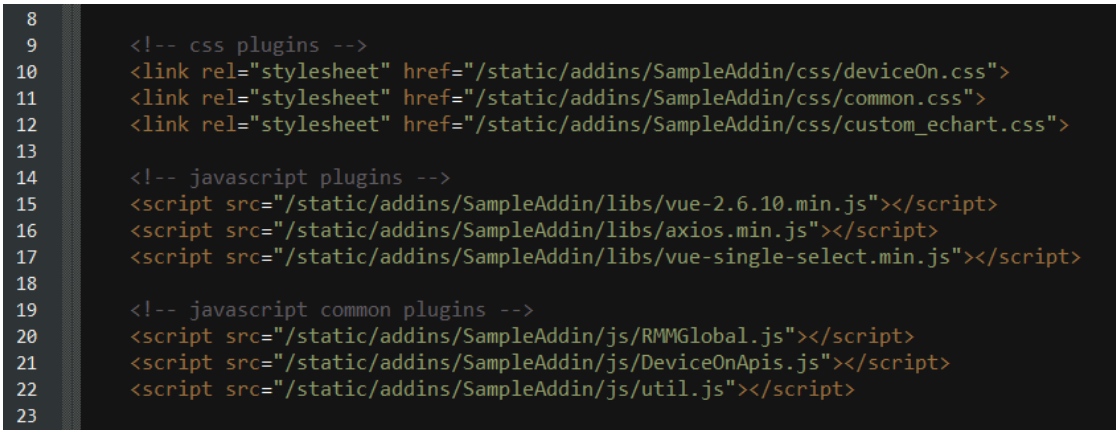
   To get all devices which under this gid's group from database.

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



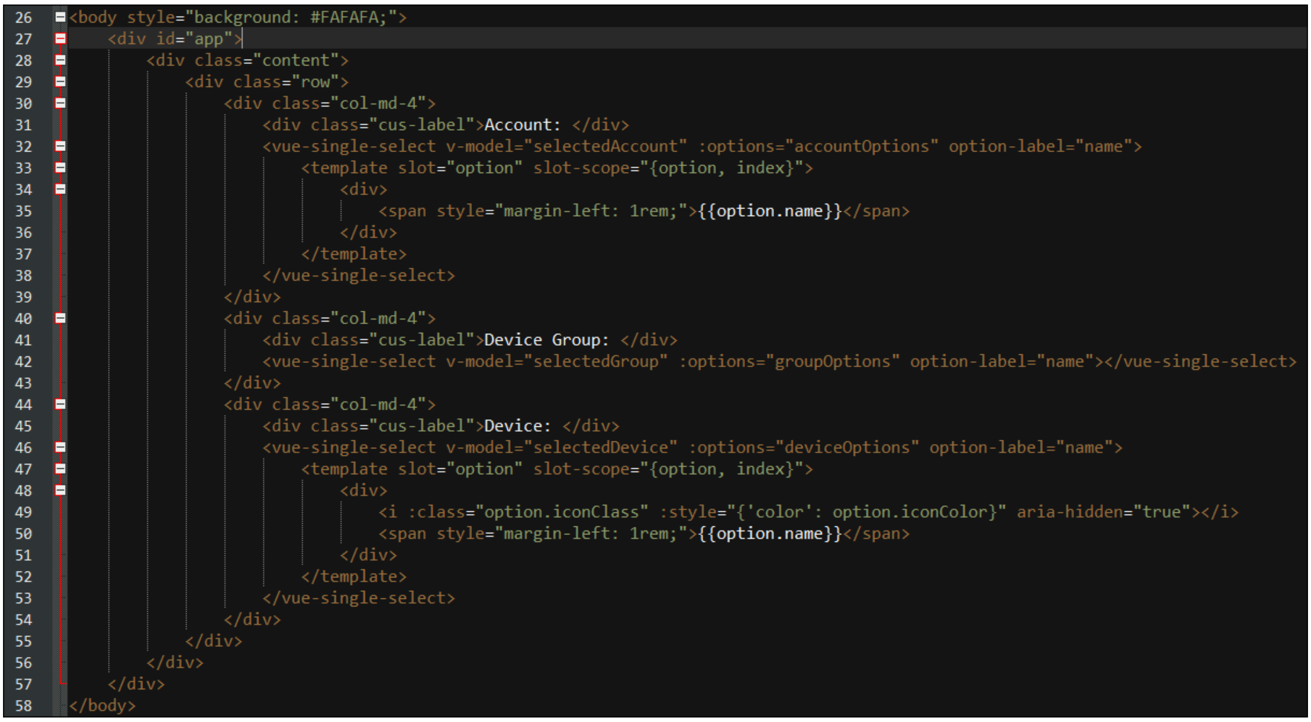
```
> css
> demo
v js
   JS DeviceOnApis.js
   JS RMMGlobal.js          M
   JS util.js
> libs
<> demo.html               U
<> demo2.html              U
<> echart.html
<> Event.html
<> image.html
<> ImageRecognition.html
<> map.html
<> plugin.html
<> realtimeData.html
<> table.html
```

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



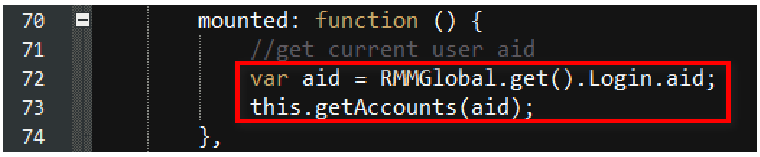
```
8
9       <!-- css plugins -->
10      <link rel="stylesheet" href="/static/addins/SampleAddin/css/deviceOn.css">
11      <link rel="stylesheet" href="/static/addins/SampleAddin/css/common.css">
12      <link rel="stylesheet" href="/static/addins/SampleAddin/css/custom_echart.css">
13
14      <!-- 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)



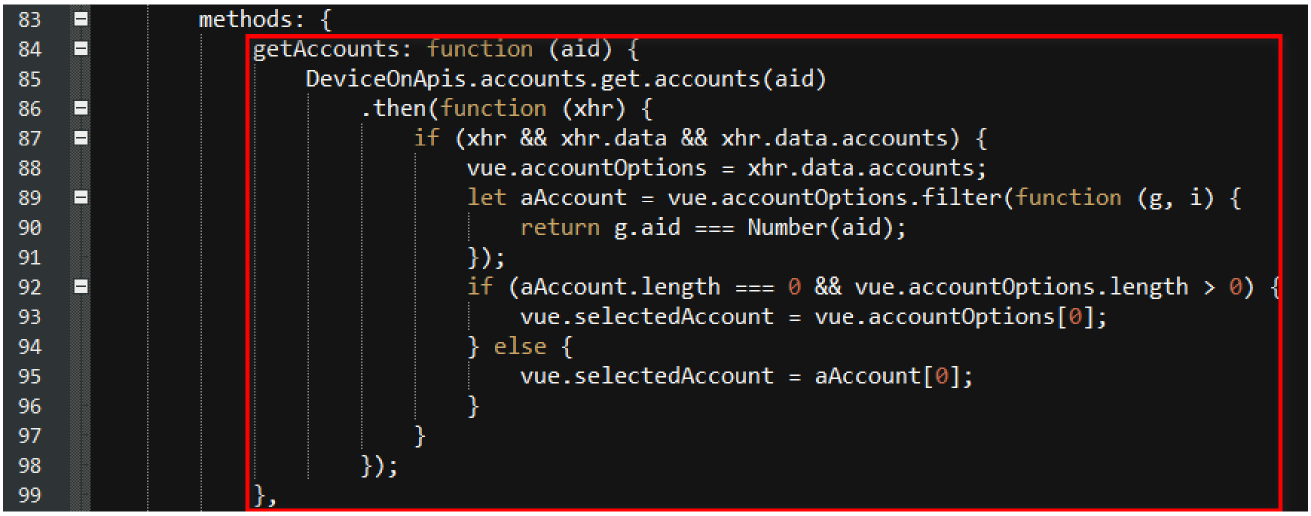
```
<body style="background: #FAFAFA;">
    <div id="app">
        <div class="content">
            <div class="row">
                <div class="col-md-4">
                    <div class="cus-label">Account: </div>
                    <vue-single-select v-model="selectedAccount" :options="accountOptions" option-label="name">
                        <template slot="option" slot-scope="{option, index}">
                            <div>
                                <span style="margin-left: 1rem;">{{option.name}}</span>
                            </div>
                        </template>
                    </vue-single-select>
                </div>
                <div class="col-md-4">
                    <div class="cus-label">Device Group: </div>
                    <vue-single-select v-model="selectedGroup" :options="groupOptions" option-label="name"></vue-single-select>
                </div>
                <div class="col-md-4">
                    <div class="cus-label">Device: </div>
                    <vue-single-select v-model="selectedDevice" :options="deviceOptions" option-label="name">
                        <template slot="option" slot-scope="{option, index}">
                            <div>
                                <i :class="option.iconClass" :style="{'color': option.iconColor}" aria-hidden="true"></i>
                                <span style="margin-left: 1rem;">{{option.name}}</span>
                            </div>
                        </template>
                    </vue-single-select>
                </div>
            </div>
        </div>
    </div>
</body>
```

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



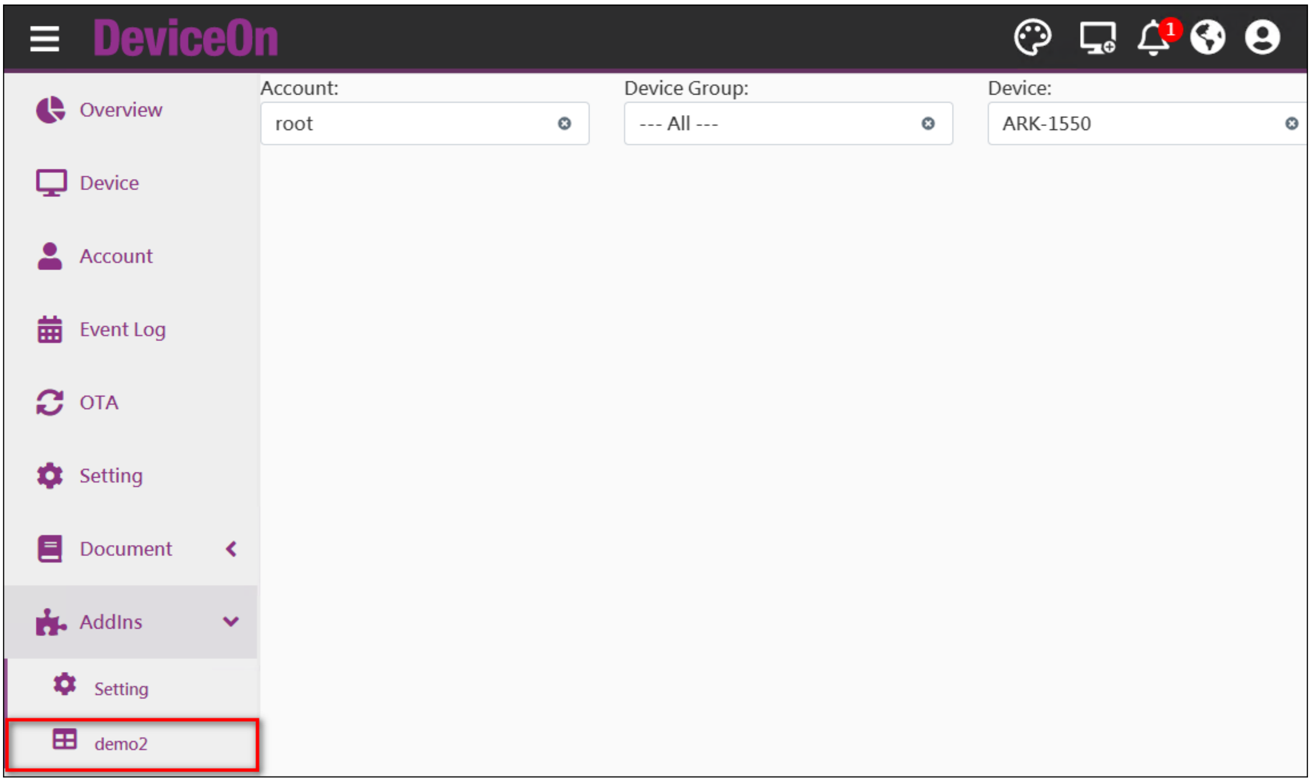
```
    mounted: function () {
        //get current user aid
        var aid = RMMGlobal.get().Login.aid;
        this.getAccounts(aid);
    },
```

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



```
    methods: {
        getAccounts: function (aid) {
            DeviceOnApis.accounts.get.accounts(aid)
                .then(function (xhr) {
                    if (xhr && xhr.data && xhr.data.accounts) {
                        vue.accountOptions = xhr.data.accounts;
                        let aAccount = vue.accountOptions.filter(function (g, i) {
                            return g.aid === Number(aid);
                        });
                        if (aAccount.length === 0 && vue.accountOptions.length > 0) {
                            vue.selectedAccount = vue.accountOptions[0];
                        } else {
                            vue.selectedAccount = aAccount[0];
                        }
                    }
                });
        },
```

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



Account: root

Device Group: --- All ---

Device: ARK-1550

6. FAQ

6.1 General

6.1.1 How to Get DeviceOn Product Information & News?

You are welcome to visit the following pages for more information and experience on DeviceOn.

- DeviceOn Product Page
- News & Solution Package

6.1.2 How to Get WISE-Agent Installer?

The WISE-Agent supports Windows 7 SP1, 8, and 10, you could download latest version from DeviceOn portal, otherwise click here to get installer package. Please contact us to get Ubuntu x64 18.04/16.04 or others support.

6.1.3 How to Monitor Device Hardware Information?

The device hardware information includes FAN Speed, Voltage, Watchdog and brightness. Before monitoring this information on DeviceOn, please make sure your device is Advantech hardware and with SUSI driver support. Recommend to download SUSI driver from Advantech Support site for your hardware platform first. Click here get the latest driver version.

6.1.4 How to Purchase a License File for Non-Advantech Device?

Please contact Advantech sales and we will provide further assistance in the order process. After that, you will get a license key from the email.

6.1.5 How Do I Find My DevieOn License File?

When your purchase is complete you will receive an email with your license file from WISE-Marketplace, this unlocks the on-premise version of WISE-DeviceOn.

6.1.6 How Many Devices Could be Managed on DeviceOn?

It depends on your server configuration. Taking the Azure DeviceOn VM specification, as an example, the instance D2sV3 can manage **1000**pcs devices. If you need to manage more than 1000 devices, please contact us for advanced solution and architecture.

6.1.7 Does DeviceOn Support on Cloud?

Yes, the DeviceOn is listed on Azure and AWS Marketplace, it’s single console that can manage several devices at the same time.

6.1.8 How to Deploy DeviceOn on Azure?

It is really simple that just login Azure Marketplace and search for **DeviceOn**, then follow the steps to create a virtual machine. Here is a Quick Start Guide to deploy through Azure Marketplace.

6.1.9 What Operating System Are Supported on WISE-Agent?

- Windows 7 SP1/8/10 32-bit/64-bit
- Ubuntu 16.04, 18.04, 20.04 x64
- Ubuntu Core
- Ubuntu 18.04 on Nvidia Jetson
- CentOS 7.7, 8.2 x64
- Other Linux flavours (e.g. Yocto) on x86 or RISC (on a per project basis)
- Android on RISC (on a per project basis)

6.1.10Can DeviceOn Perform Bulk Operations on Devices Remotely?

Yes, group the devices for different attributes and set the task for each group, bulk operation can be finished.

6.1.11 Does DeviceOn Provide Integration Document for Customization?

DeviceOn offers easy customization with a complete REST API for core management on the server side, and an SDK on the device side that enables the development of custom plugins.

6.1.12 How to Upgrade Software, Firmware via DeviceOn?

DeviceOn has OTA (Over the Air) function to remote provisioning and updates on firmware, driver, and software at the scale.

6.1.13 Does Azure Provide the Similar Service Compare with DeviceOn?

Azure offers "Azure IOT Central" which is the most similar with DeviceOn. But, DeviceOn is a solution which already integrates many functions that is specialized in Device Management. Either "Azure Monitor" or "Azure IOT Central" is actually part of the function of DeviceOn. If you are looking for the total solution for your device monitoring/ troubleshooting, DeviceOn must be the best option.

6.1.14 Which Tier (Size) of Azure VM Should I Select and Cost Estimate?

It is recommended that users select **D2sV3** (2Cores 8G RAM) to meet most cases, you may refer below scenarios that we verified. The list price of VM, storage is based on Azure calculator and the data center in **Southeast Asia** (Singapore)

- Case I, Standard IPC Device Management (Hardware, Network, Hard Disk, System), **25Tags/min**

Azure VM Tier	Device Number	Storage Required/mo	Storage Tier (HDD) Recommended (Monthly Retention)	Price Estimation VM + Storage (USD)/mo
D2sV5 (2 Cores 8G) ($158.46/mo)	10	1.09G	S6 (64G), $3.06/mo	**$161.52**
	100	8.22G	S6 (64G), $3.06/mo	**$161.52**
	500	39.9G	S10 (128G), $5.94/mo	**$164.4**
	1,000	79.5G	S10 (128G), $5.94/mo	**$164.4**
	3,800	302.1G	S20 (512G), $21.81/mo	**$180.27**
D4sV5 (4 Cores 16G) ($316.87/mo)	7,500	596.25G	S30 (512G), $41.01/mo	**$357.88**

- Case II, Standard IPC Device Management (Hardware, Network, Hard Disk, System), **187Tags/min**

Azure VM Tier	Device Number	Storage Required/mo	Storage Tier (HDD) Recommended (Monthly Retention)	Price Estimation VM + Storage (USD)/mo
D2sV5 (2 Cores 8G) ($158.46/mo)	10	4.692G	S6 (64G), $3.06/mo	**$161.52**
	100	44.22G	S10 (128G), $5.94/mo	**$164.4**
	500	219.9G	S20 (512G), $21.81/mo	**$180.27**
	2,400	1,061.28G	S40 (2,048G), $81.97/mo	**$240.43**
D4sV5 (4 Cores 16G) ($316.87/mo)	4,000	1,759.2G	S40 (2,048G), $81.97/mo	**$398.84**

- Case III, Data Collection, **15Tags/sec**

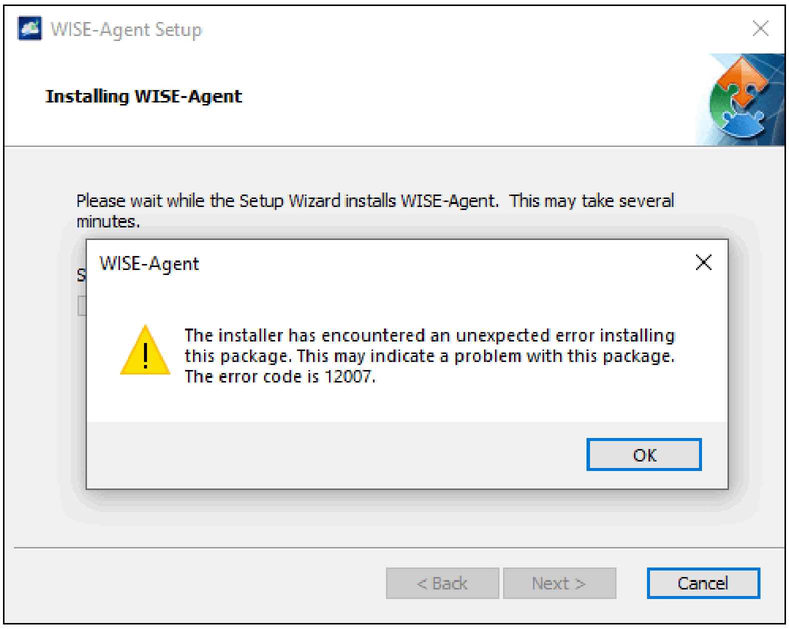
Azure VM Tier	Device Number	Storage Required/mo	Storage Tier (HDD) Recommended (Monthly Retention)	Price Estimation VM + Storage (USD)/mo
D2sV5 (2 Cores 8G) ($158.46/mo)	10	21.18G	S10 (128G), $5.94/mo	**$164.4**
	100	209.1G	S20 (512G), $21.81/mo	**$180.27**
	300	626.7G	S30 (1,024G), $41.01/mo	**$199.47**
	800	1,671.3G	S40 (2,048G), $81.97/mo	**$240.43**
D4sV5 (4 Cores 16G) ($316.87/mo)	1300	2,714.7G	S50 (4,096G), $163.84/mo	**$480.71**

6.1.15 How Can I Get Support?

In addition to browsing the user manual from technical portal to find answer to your questions, product support is available via email. Please contact below windows to get further information.
Product PM/RD: Rison.Yeh/Sephiroth.Wang

6.2 Technical

6.2.1 Why Cannot the WISE-Agent Install? With error code 12007?



WISE-Agent Setup

Installing WISE-Agent

Please wait while the Setup Wizard installs WISE-Agent. This may take several minutes.

WISE-Agent

The installer has encountered an unexpected error installing this package. This may indicate a problem with this package. The error code is 12007.

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.

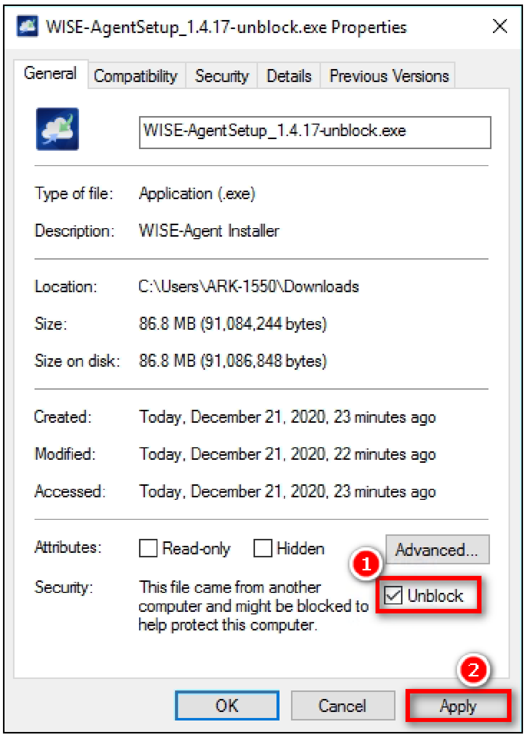
6.2.2 Why does the installation UI not appear after I execute the WISE-Agent?

You see the “this file came from another computer and might be blocked” error when you try to open a downloaded or transferred file from another computer. For instance, if you receive an email attachment, the file might be blocked because it came from another computer.

When the file is not verified or not originated on your computer, Windows might block the file execution for security concerns.

Now, this doesn’t happen to every file you download or transfer. However, depending on the file type and file origin, Windows automatically triggers the security response. However, false positives can happen. Fortunately, it is easy to unblock the file downloaded from another computer. In fact, Windows even provides proper options to do so. Let me show you how.

- In the General tab, you will see a new option at the bottom of the window. Select the Unblock checkbox and click on the Apply button.



WISE-AgentSetup_1.4.17-unblock.exe Properties

WISE-AgentSetup_1.4.17-unblock.exe

Type of file: Application (.exe)

Description: WISE-Agent Installer

Location: C:\Users\ARK-1550\Downloads

Size: 86.8 MB (91,084,244 bytes)

Size on disk: 86.8 MB (91,086,848 bytes)

Created: Today, December 21, 2020, 23 minutes ago

Modified: Today, December 21, 2020, 22 minutes ago

Accessed: Today, December 21, 2020, 23 minutes ago

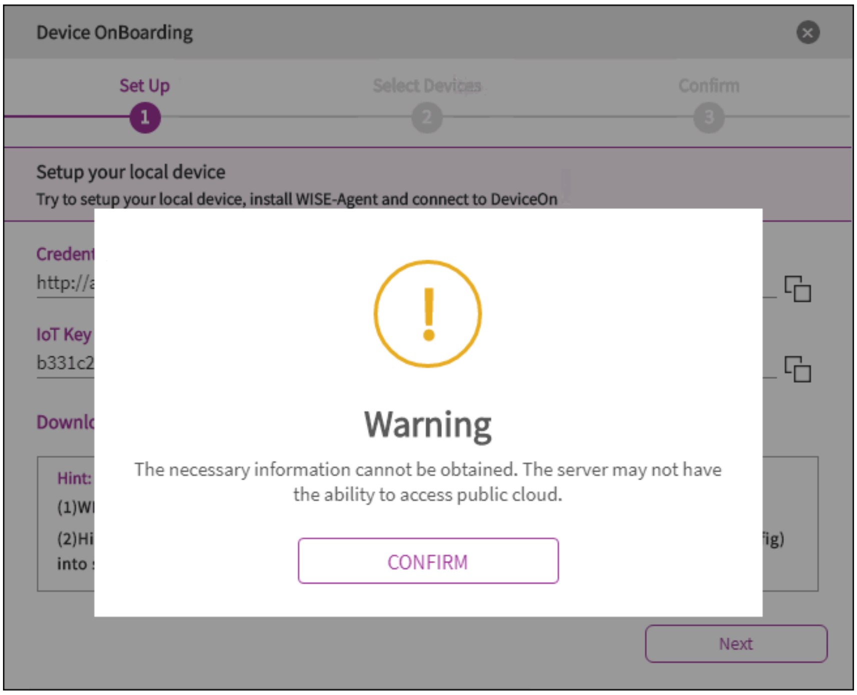
Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer. ☑ Unblock

- As soon as you click on the Apply button, Windows will unblock the file. The option will disappear too. Click on the Ok button to close the window.

6.2.3 Why the WISE-Agent Cannot Download from Device Onboarding?

In order to allow users to obtain the latest and stable WISE-Agent, the DeviceOn team will place the latest version on the cloud. When this message appears, it means that your server network cannot access the cloud or does not have network connectivity.



Device OnBoarding

Setup your local device

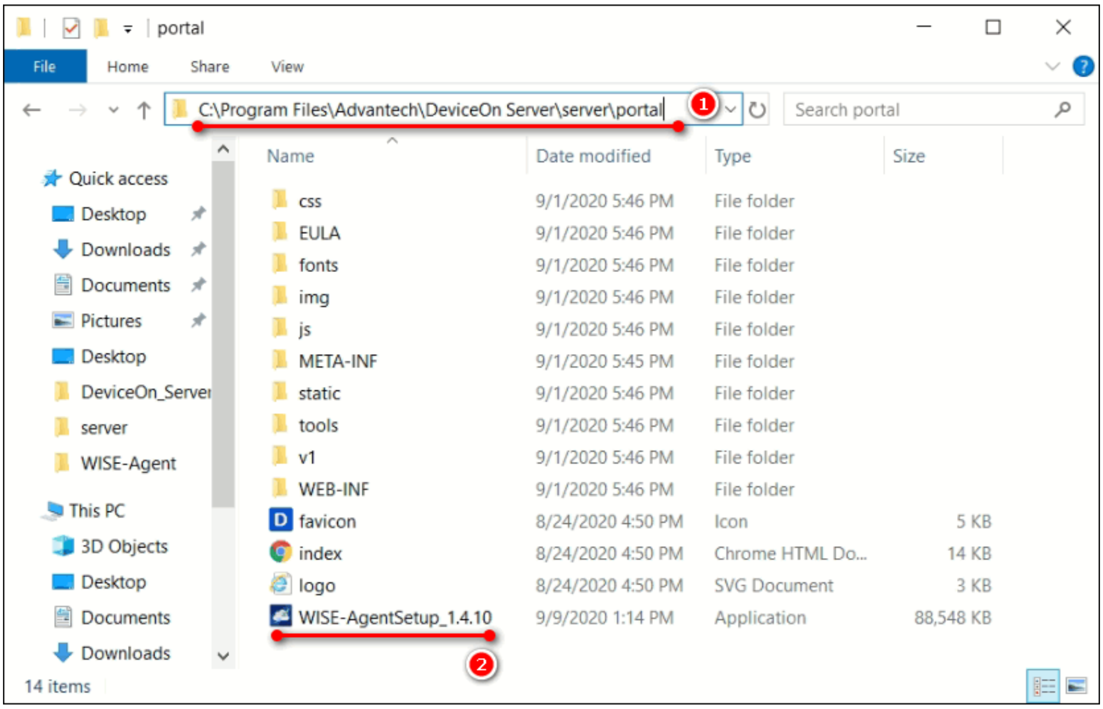
Try to setup your local device, install WISE-Agent and connect to DeviceOn

Warning

The necessary information cannot be obtained. The server may not have the ability to access public cloud.

You could download WISE-Agent through your mobile device or laptop and put it in the following path. The file name must be "**WISE-AgentSetup_x.y.z**".

Installation Path: \DeviceOn Server\server\portal\



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

Name	Date modified	Type	Size
css	9/1/2020 5:46 PM	File folder	
EULA	9/1/2020 5:46 PM	File folder	
fonts	9/1/2020 5:46 PM	File folder	
img	9/1/2020 5:46 PM	File folder	
js	9/1/2020 5:46 PM	File folder	
META-INF	9/1/2020 5:45 PM	File folder	
static	9/1/2020 5:46 PM	File folder	
tools	9/1/2020 5:46 PM	File folder	
v1	9/1/2020 5:46 PM	File folder	
WEB-INF	9/1/2020 5:46 PM	File folder	
favicon	8/24/2020 4:50 PM	Icon	5 KB
index	8/24/2020 4:50 PM	Chrome HTML Do...	14 KB
logo	8/24/2020 4:50 PM	SVG Document	3 KB
WISE-AgentSetup_1.4.10	9/9/2020 1:14 PM	Application	88,548 KB

6.2.4 Why the Acronis and McAfee failed to Install?

Since the installer package require .Net Framework 3.5 dependency, please help to confirm is .Net Framework 3.5 installed on your devices.

6.2.5 Why Your SMTP Server Cannot Send a Mail?

Case I: Your DeviceOn service is deployed on Azure cloud and your SMTP server adopt port 25.

Starting on November 15, 2017, outbound email messages that are sent directly to external domains (such as outlook.com and gmail.com) from a virtual machine (VM) are made available only to certain subscription types in Microsoft Azure. Outbound SMTP connections that use TCP port 25 were blocked. (Port 25 is primarily used for unauthenticated email delivery.)

This change in behavior applies only to new subscriptions and new deployments since November 15, 2017. Referenced site>

Case II: Always authentication failed through your Gmail account.

Step 1: Less secure apps & your Google Account.

Please enter to the page with your Google account and set it to **Enable**.

Step 2: Unlocking Google's Gmail CAPTCHA

Please enter to the page with your Google account and click **Continue**.

6.2.6 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

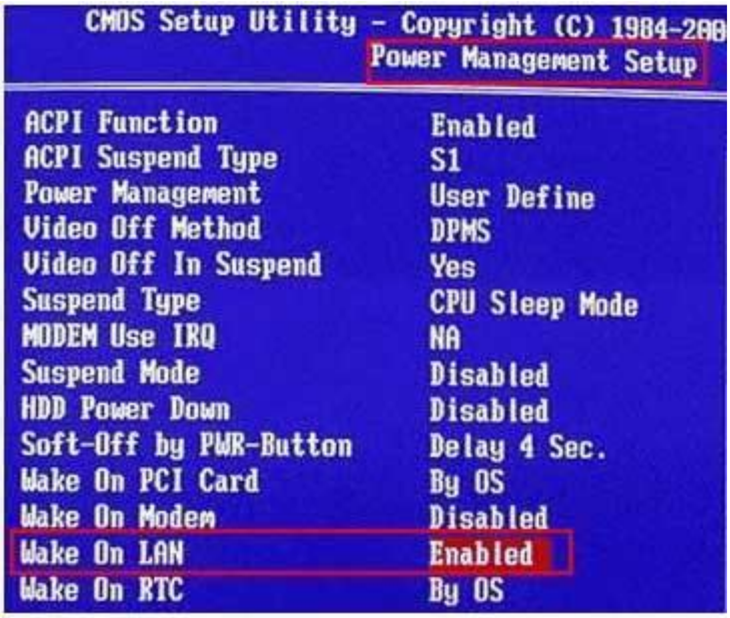
Enabling Wake-on-LAN is done in two steps, both of which are described below. The first sets up the motherboard by configuring Wake-on-LAN through BIOS before the operating system boots, and the next logs into the operating system and makes some small changes there. The first step with the BIOS is valid 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.

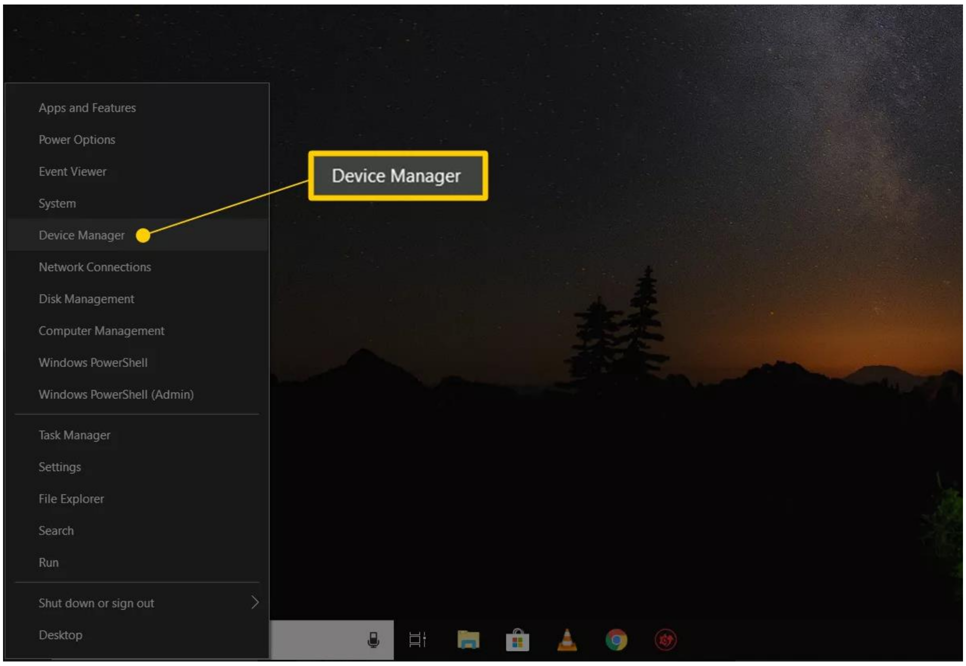


```
CMOS Setup Utility - Copyright (C) 1984-200
                           Power Management Setup

ACPI Function                 Enabled
ACPI Suspend Type             S1
Power Management              User Define
Video Off Method              DPMS
Video Off In Suspend          Yes
Suspend Type                  CPU Sleep Mode
MODEM Use IRQ                 NA
Suspend Mode                  Disabled
HDD Power Down                Disabled
Soft-Off by PWR-Button        Delay 4 Sec.
Wake On PCI Card              By OS
Wake On Modem                 Disabled
Wake On LAN                   Enabled
Wake On RTC                   By OS
```

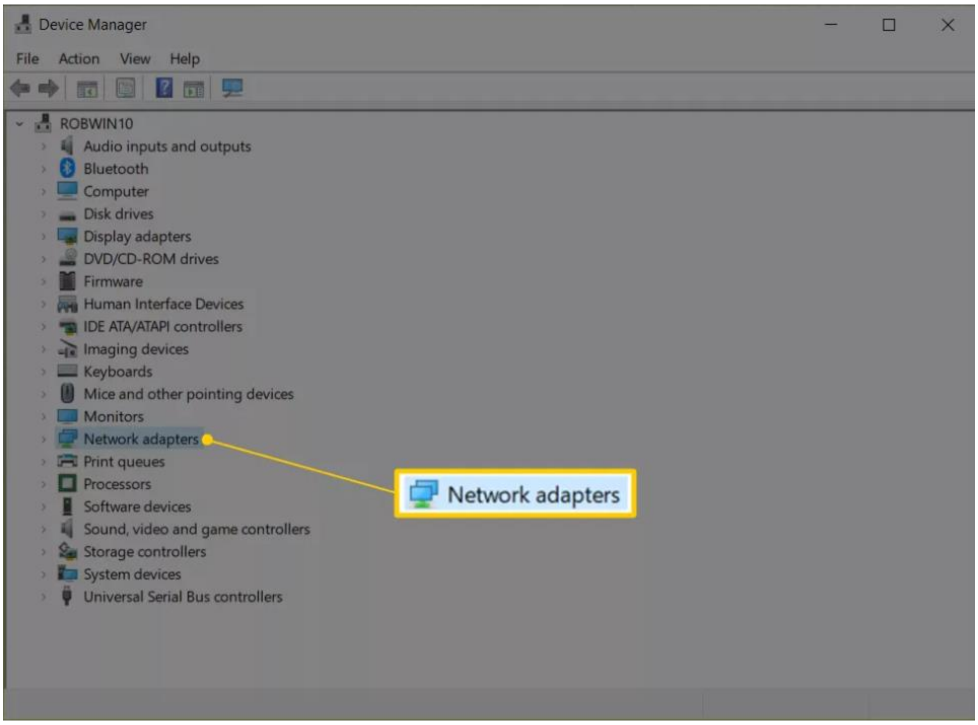
Step 2: Windows operating system WoL setup

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

1. Open Device Manager



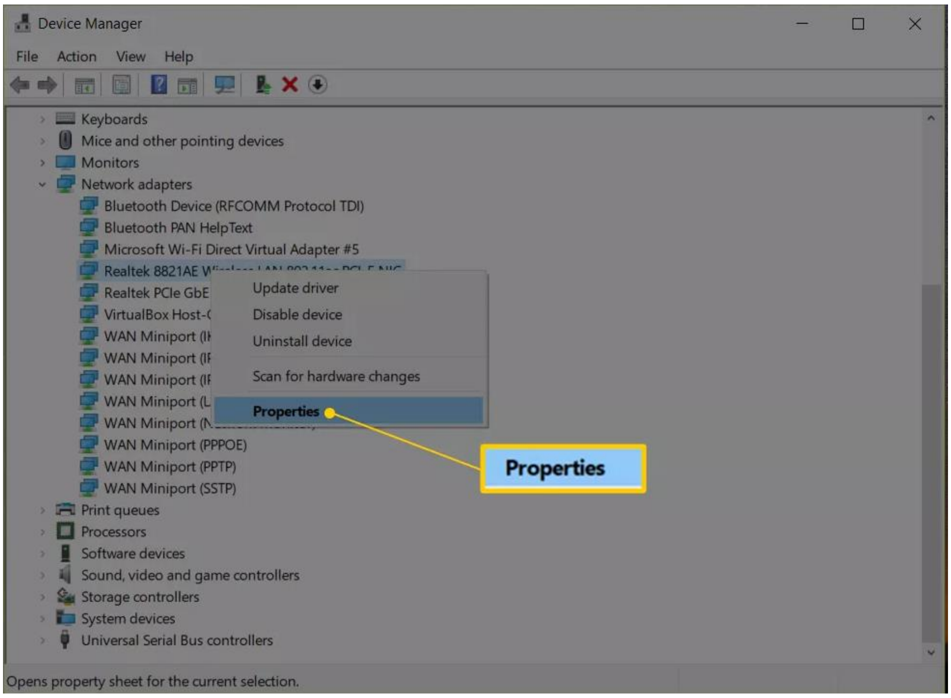
2. Find and open the Network adapters section.



Network adapters

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**.

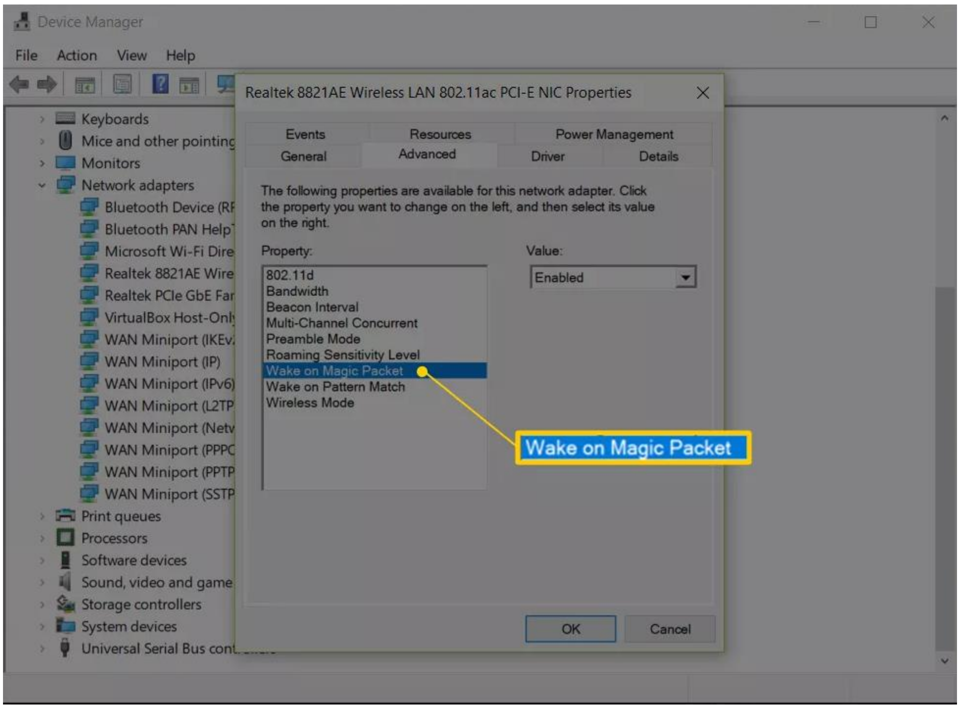


Opens property sheet for the current selection.

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.



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

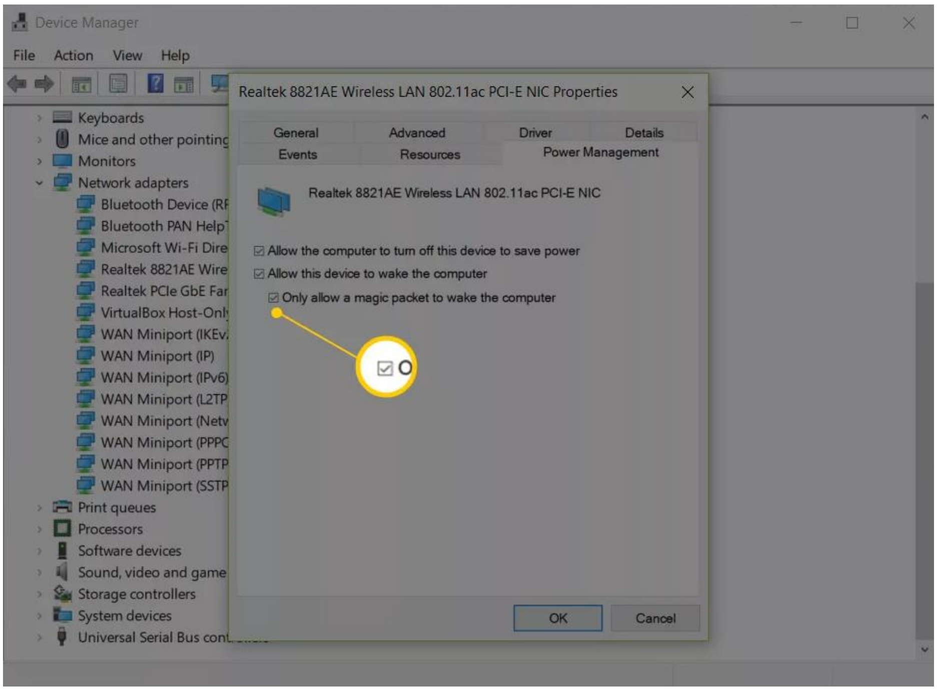
Property:

802.11d
Bandwidth
Beacon Interval
Multi-Channel Concurrent
Preamble Mode
Roaming Sensitivity Level
Wake on Magic Packet
Wake on Pattern Match
Wireless Mode

Value: Enabled

Wake on Magic Packet

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**.



Realtek 8821AE Wireless LAN 802.11ac PCI-E NIC

☑ Allow the computer to turn off this device to save power
☑ Allow this device to wake the computer
☑ Only allow a magic packet to wake the computer

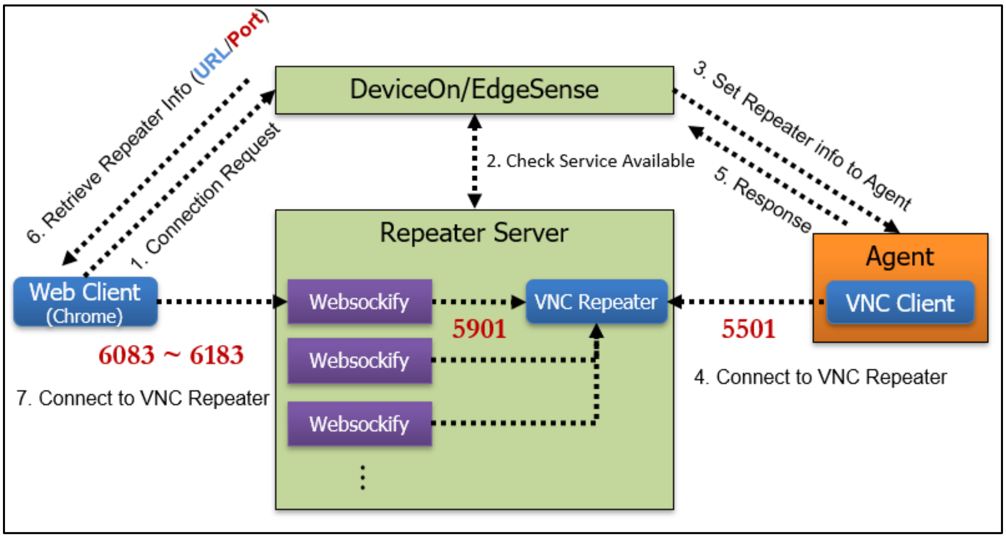
☑ O

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

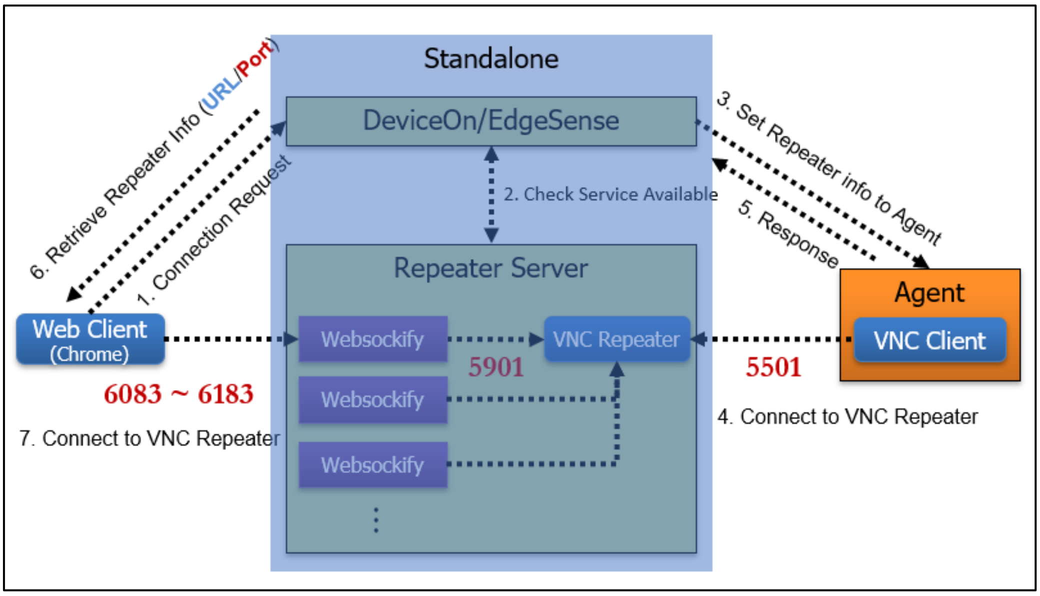
10. **Click or tap OK to save the changes and exit that window. You can also close** Device Manager.

6.2.7 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.

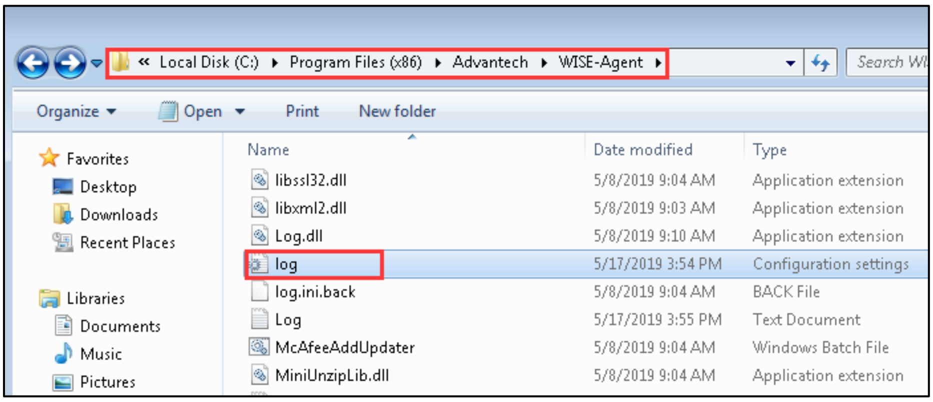


6.2.8 How to Enable and Adjust WISE-Agent Log Levels

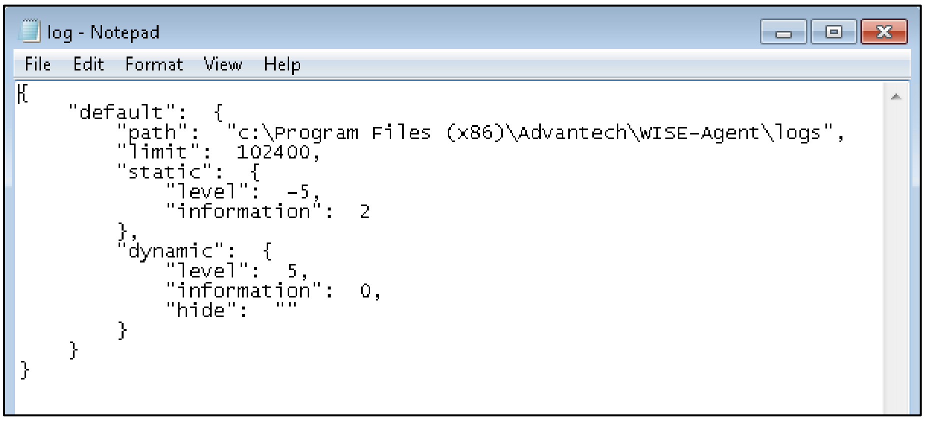
[WISE-Agent v-1.3.x & v-1.2.x]

Step 1: Adjust configuration file on WISE-Agent

Open **log.ini** on Installation path



Name	Date modified	Type
libssl32.dll	5/8/2019 9:04 AM	Application extension
libxml2.dll	5/8/2019 9:03 AM	Application extension
Log.dll	5/8/2019 9:10 AM	Application extension
log	5/17/2019 3:54 PM	Configuration settings
log.ini.back	5/8/2019 9:04 AM	BACK File
Log	5/17/2019 3:55 PM	Text Document
McAfeeAddUpdater	5/8/2019 9:04 AM	Windows Batch File
MiniUnzipLib.dll	5/8/2019 9:04 AM	Application extension

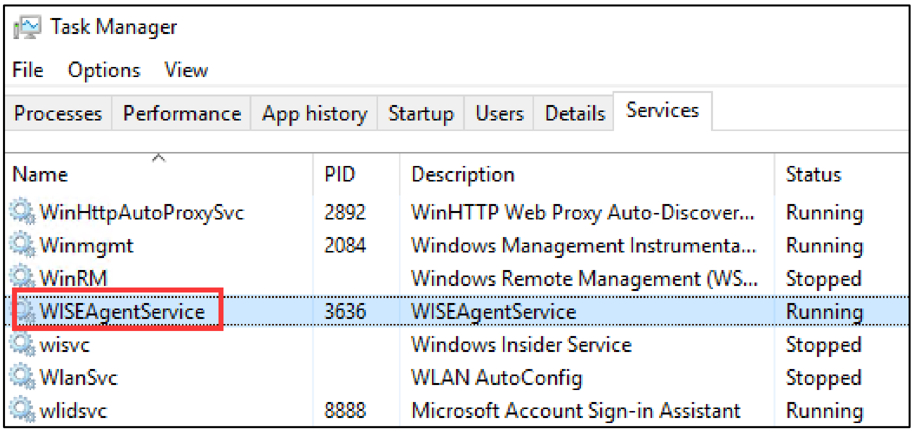


```
{
    "default":  {
        "path":  "c:\Program Files (x86)\Advantech\WISE-Agent\logs",
        "limit":  102400,
        "static":  {
            "level":  -5,
            "information":  2
        },
        "dynamic":  {
            "level":  5,
            "information":  0,
            "hide":  ""
        }
    }
}
```

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

Step 2: Restart WISE-Agent

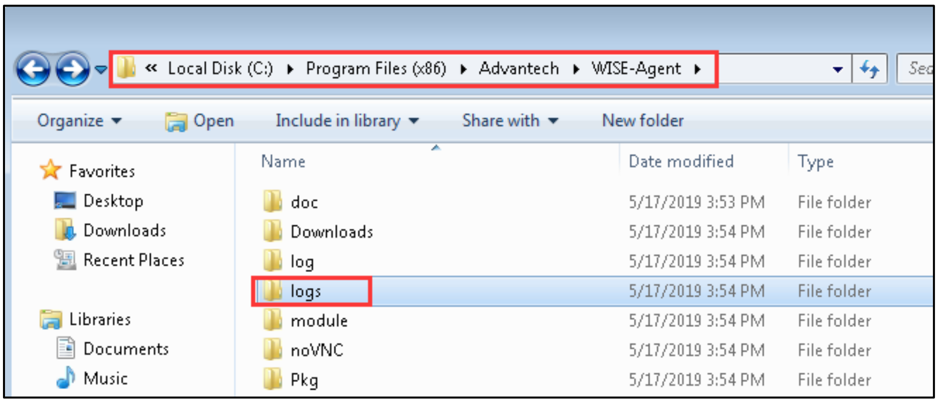
Open “Task Manager” and switch to “Services”, and restart “WISEAgentService”



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

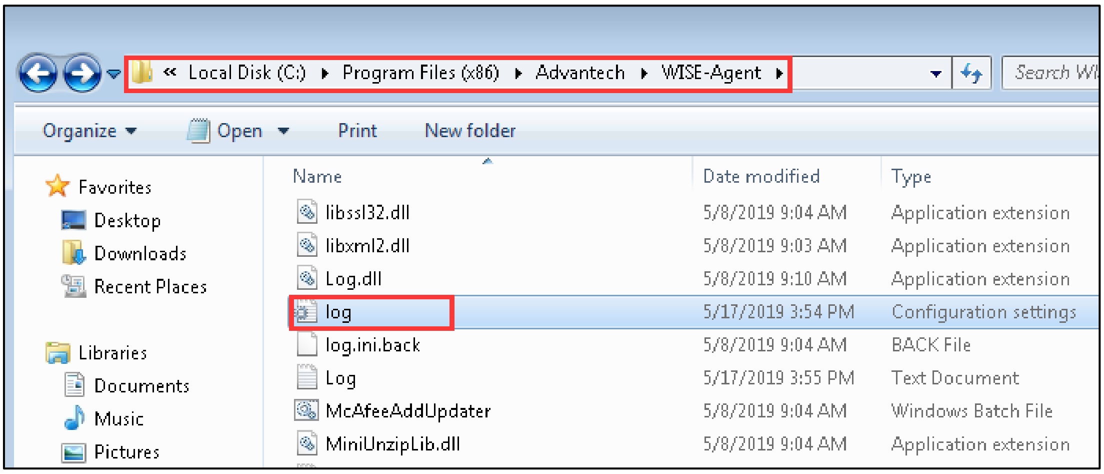


Name	Date modified	Type
doc	5/17/2019 3:53 PM	File folder
Downloads	5/17/2019 3:54 PM	File folder
log	5/17/2019 3:54 PM	File folder
logs	5/17/2019 3:54 PM	File folder
module	5/17/2019 3:54 PM	File folder
noVNC	5/17/2019 3:54 PM	File folder
Pkg	5/17/2019 3:54 PM	File folder

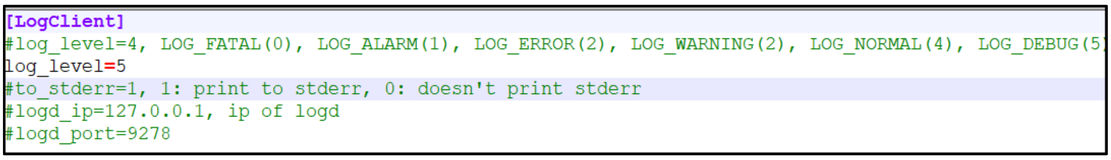
[WISE-Agent v-1.4.x and above]

Step 1: Adjust configuration file on WISE-Agent

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



Name	Date modified	Type
libssl32.dll	5/8/2019 9:04 AM	Application extension
libxml2.dll	5/8/2019 9:03 AM	Application extension
Log.dll	5/8/2019 9:10 AM	Application extension
log	5/17/2019 3:54 PM	Configuration settings
log.ini.back	5/8/2019 9:04 AM	BACK File
Log	5/17/2019 3:55 PM	Text Document
McAfeeAddUpdater	5/8/2019 9:04 AM	Windows Batch File
MiniUnzipLib.dll	5/8/2019 9:04 AM	Application extension

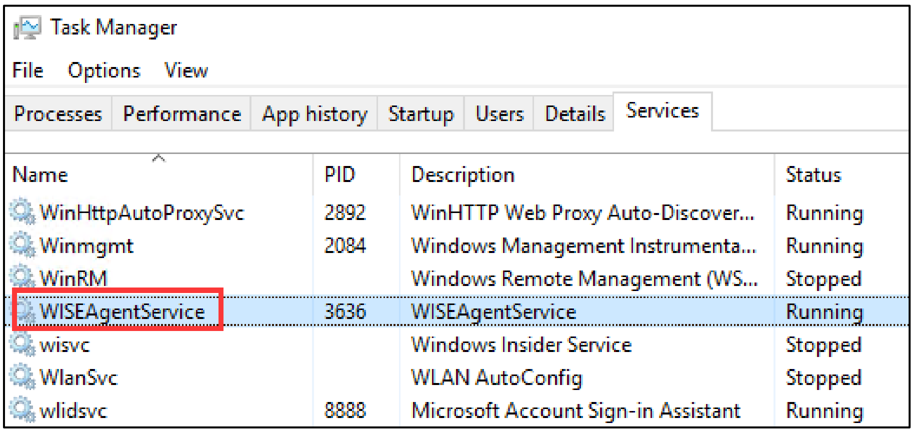


```
[LogClient]
#log_level=4, LOG_FATAL(0), LOG_ALARM(1), LOG_ERROR(2), LOG_WARNING(2), LOG_NORMAL(4), LOG_DEBUG(5
log_level=5
#to_stderr=1, 1: print to stderr, 0: doesn't print stderr
#logd_ip=127.0.0.1, ip of logd
#logd_port=9278
```

Adjust **log_level** from 4 to 5.

Step 2: Restart WISE-Agent

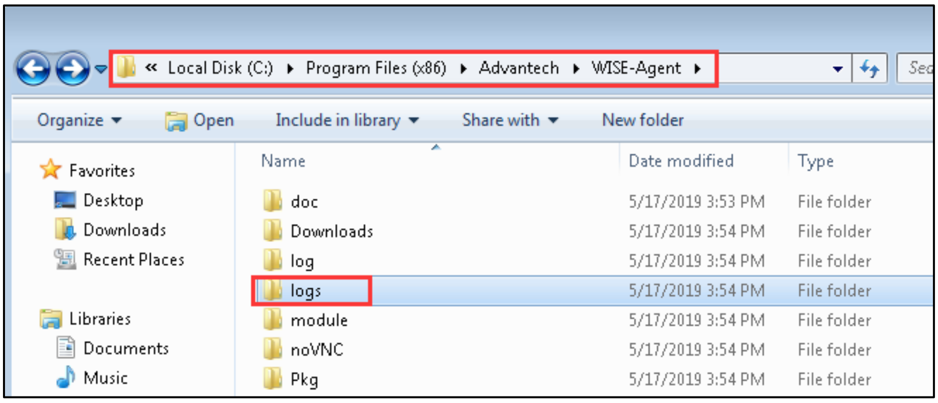
Open “Task Manager” and switch to “Services”, and restart “WISEAgentService”


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

Step 3: Retrieve log files from WISE-Agent

The log files under the Installation path\logs



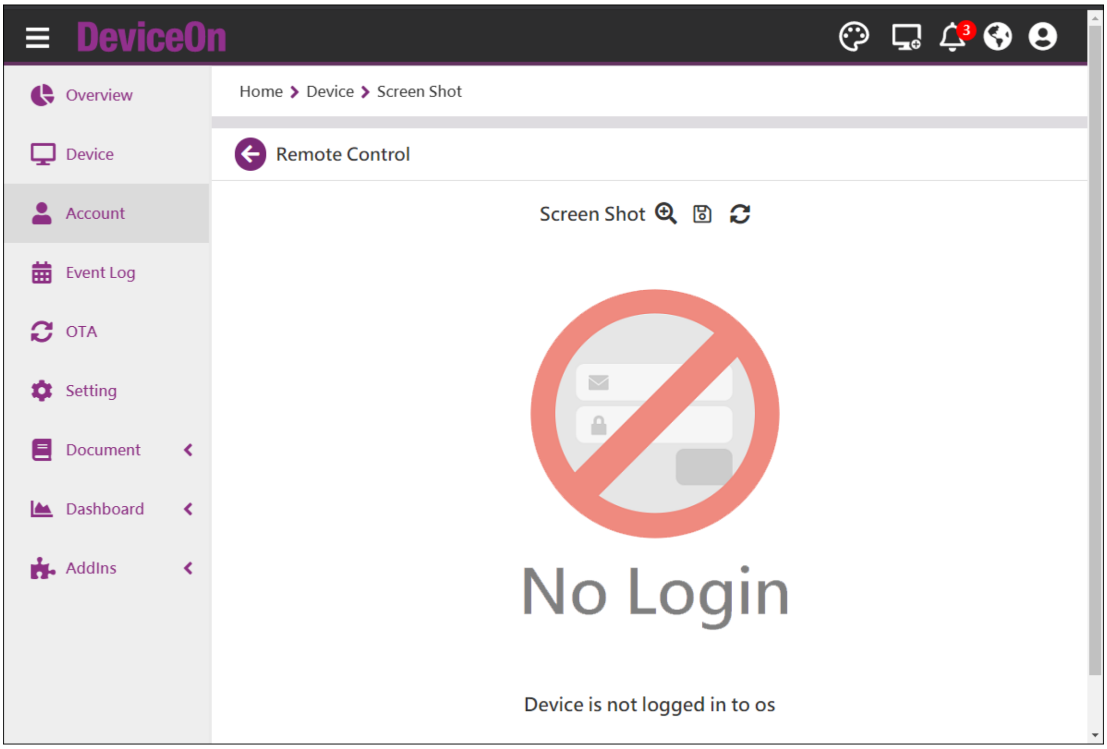
Name	Date modified	Type
doc	5/17/2019 3:53 PM	File folder
Downloads	5/17/2019 3:54 PM	File folder
log	5/17/2019 3:54 PM	File folder
logs	5/17/2019 3:54 PM	File folder
module	5/17/2019 3:54 PM	File folder
noVNC	5/17/2019 3:54 PM	File folder
Pkg	5/17/2019 3:54 PM	File folder

6.2.9 Why the Dashboard Cannot Display All the Data within the Interval?

DeviceOn provide the Simple JSON interface to access sensor data from the edge device, there are two mechanisms to retrieve data, one is **Sampling** to scatter the value of the interval, require lot's of computing resource of databases. The other is **Raw** to return latest raw data with **5000** records. Both of two methods support data within **7** days only.

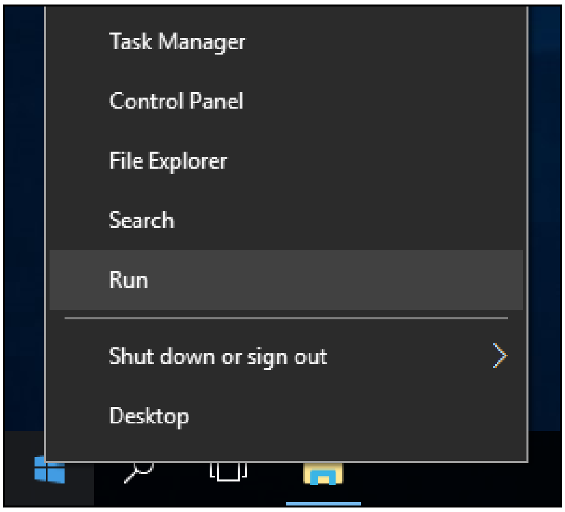
6.2.10Why Cannot Screenshot and Always Show Device "No Login"

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

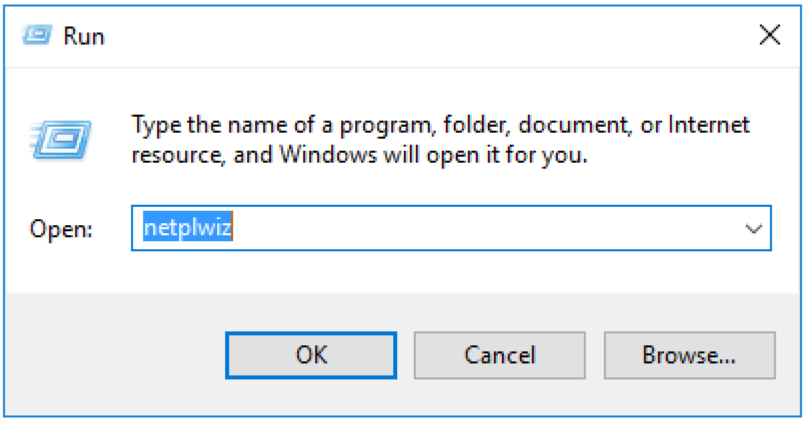


Device is not logged in to os

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.

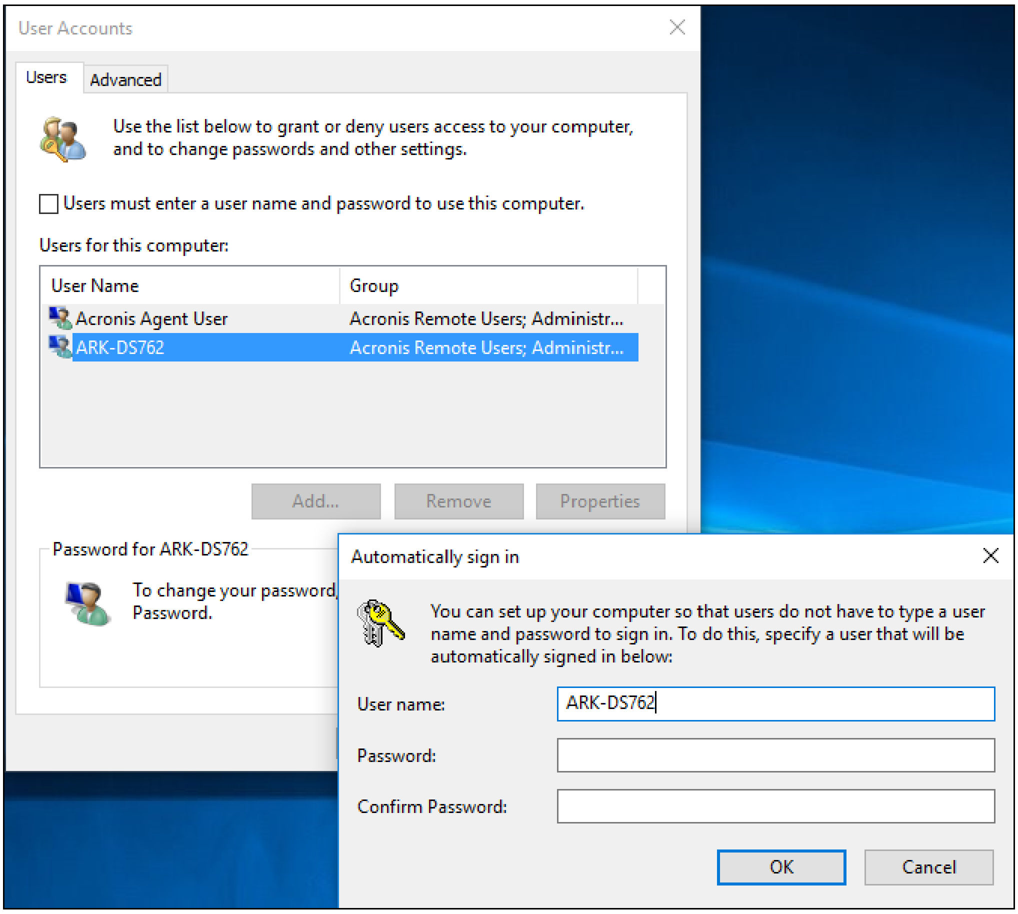


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

Open: netplwiz

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.



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

□ Users must enter a user name and password to use this computer.

Users for this computer:

User Name	Group
Acronis Agent User	Acronis Remote Users; Administr...
ARK-DS762	Acronis Remote Users; Administr...

Password for ARK-DS762

To change your password, Password.

You can set up your computer so that users do not have to type a user name and password to sign in. To do this, specify a user that will be automatically signed in below:

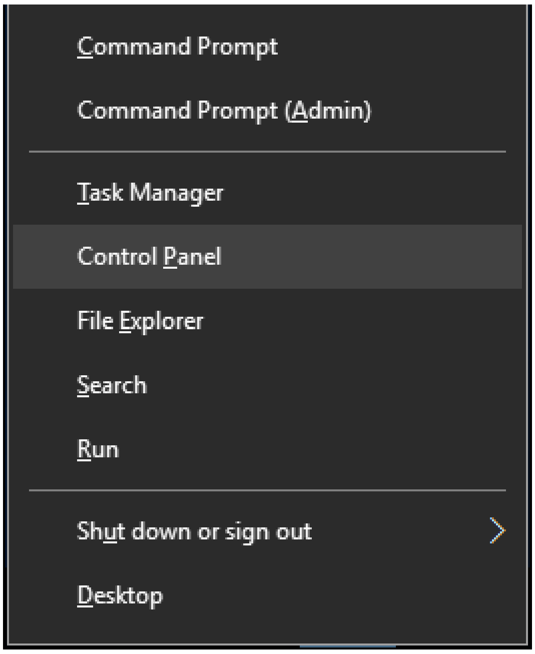
User name: ARK-DS762

Password:

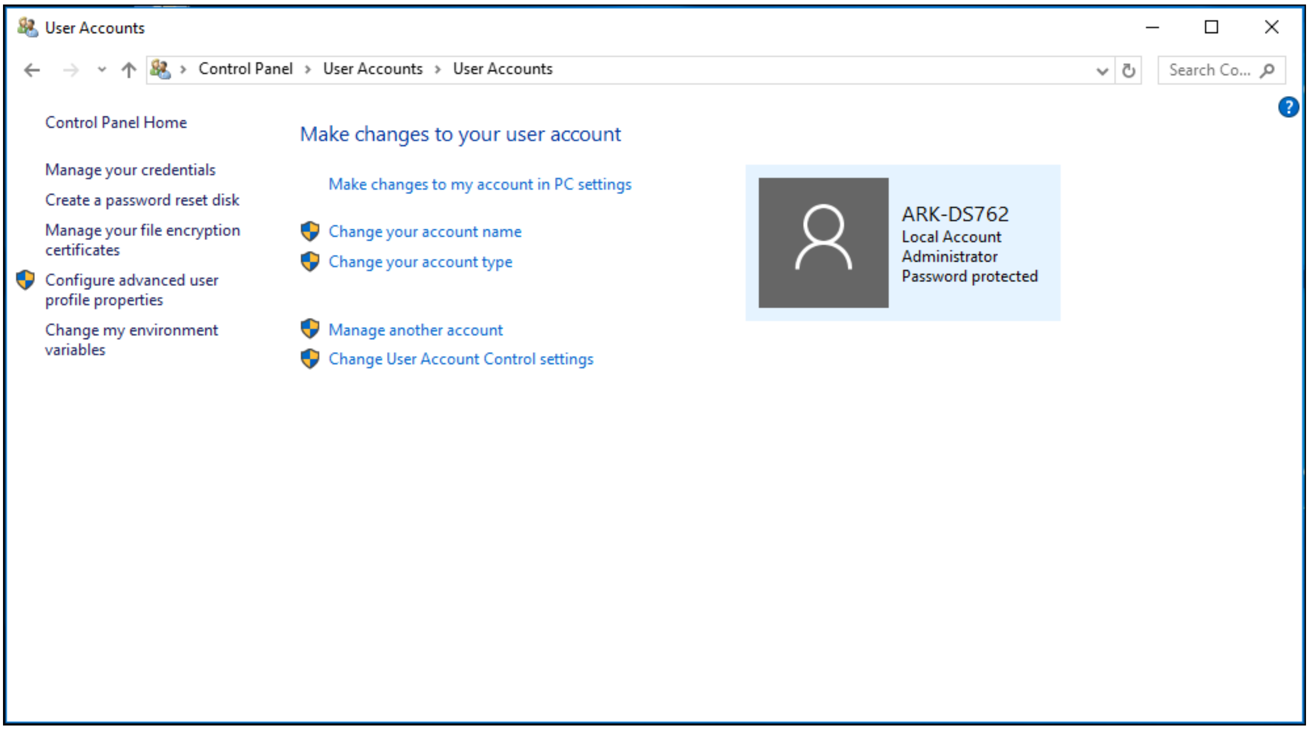
Confirm Password:

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).

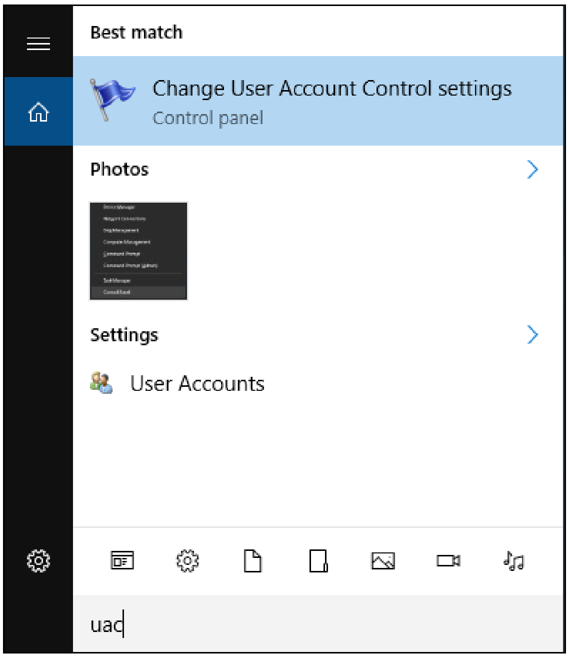
Step 1: Press Windows Key ⊞ + X hotkeys together on the keyboard and choose the "Control Panel" item.



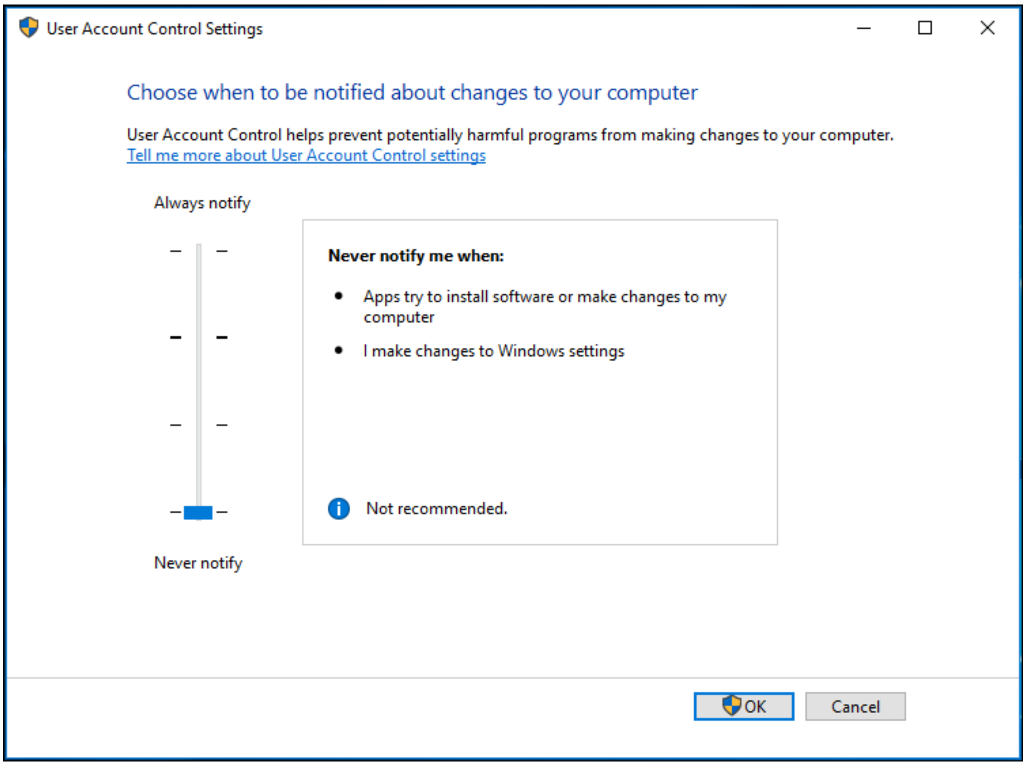
Step 2: Go to the following path: “**Control Panel\User Accounts\User Accounts**” There you will find the Change User Account Control settings link. Click it.


User Accounts
Control Panel › User Accounts › User Accounts
Search Co...
Control Panel Home
Manage your credentials
Create a password reset disk
Manage your file encryption certificates
Configure advanced user profile properties
Change my environment variables
Make changes to your user account
Make changes to my account in PC settings
Change your account name
Change your account type
Manage another account
Change User Account Control settings
ARK-DS762
Local Account
Administrator
Password protected

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).



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

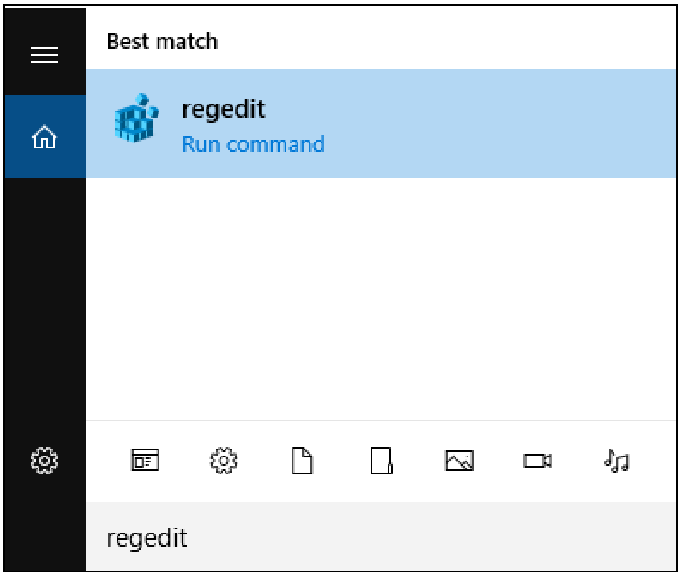
Never notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

Not recommended.

Never notify

Step 4: Enter the "***regedit***" in the Search box to open the Registry Editor.



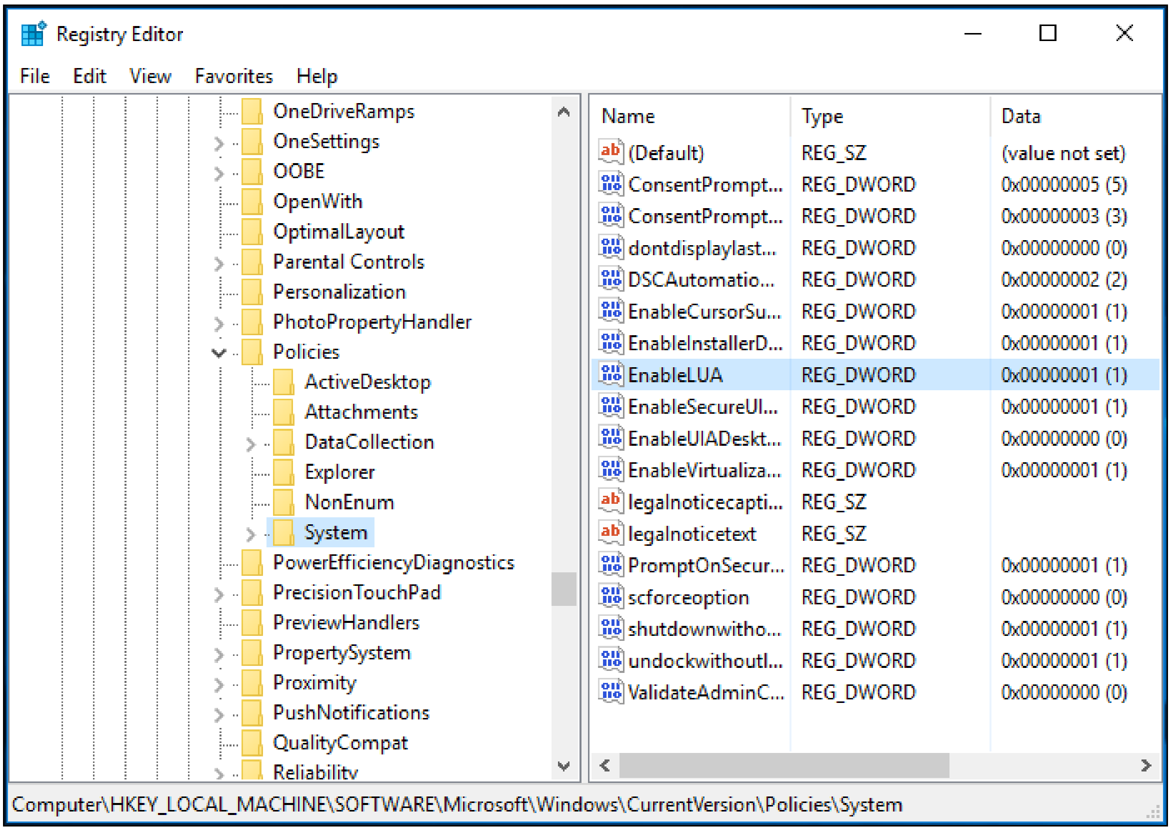
Best match

regedit
Run command

regedit

Step 5: Navigate to the following key:

“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System”

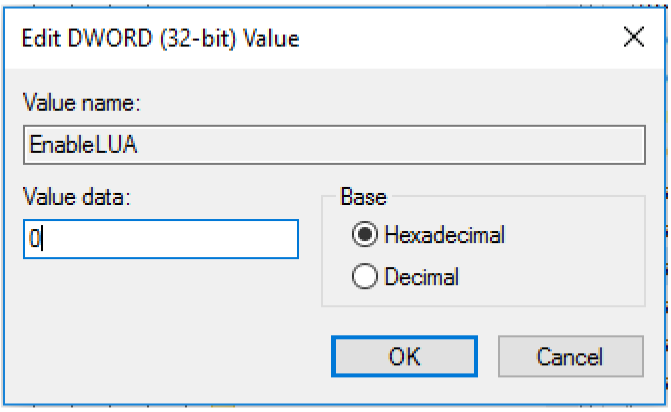


OneDriveRamps
OneSettings
OOBE
OpenWith
OptimalLayout
Parental Controls
Personalization
PhotoPropertyHandler
Policies
ActiveDesktop
Attachments
DataCollection
Explorer
NonEnum
System
PowerEfficiencyDiagnostics
PrecisionTouchPad
PreviewHandlers
PropertySystem
Proximity
PushNotifications
QualityCompat
Reliability

Name	Type	Data
(Default)	REG_SZ	(value not set)
ConsentPrompt...	REG_DWORD	0x00000005 (5)
ConsentPrompt...	REG_DWORD	0x00000003 (3)
dontdisplaylast...	REG_DWORD	0x00000000 (0)
DSCAutomatio...	REG_DWORD	0x00000002 (2)
EnableCursorSu...	REG_DWORD	0x00000001 (1)
EnableInstallerD...	REG_DWORD	0x00000001 (1)
EnableLUA	REG_DWORD	0x00000001 (1)
EnableSecureUI...	REG_DWORD	0x00000001 (1)
EnableUIADeskt...	REG_DWORD	0x00000000 (0)
EnableVirtualiza...	REG_DWORD	0x00000001 (1)
legalnoticecapti...	REG_SZ	
legalnoticetext	REG_SZ	
PromptOnSecur...	REG_DWORD	0x00000001 (1)
scforceoption	REG_DWORD	0x00000000 (0)
shutdownwitho...	REG_DWORD	0x00000001 (1)
undockwithoutl...	REG_DWORD	0x00000001 (1)
ValidateAdminC...	REG_DWORD	0x00000000 (0)

Computer\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**.



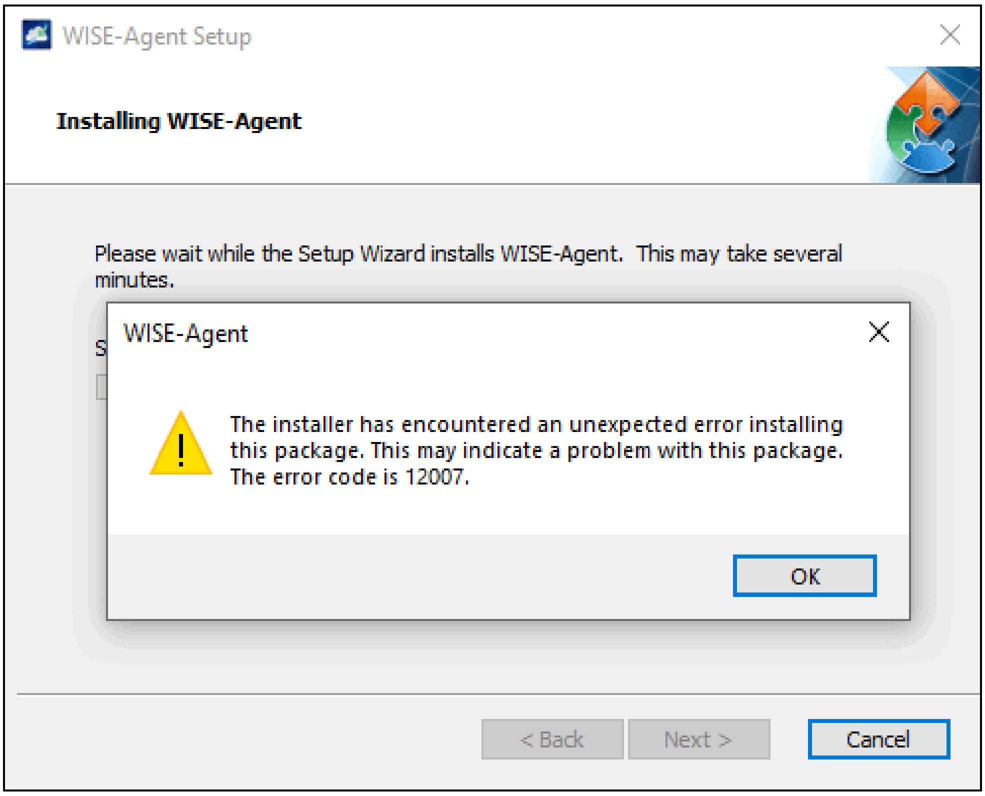
Edit DWORD (32-bit) Value

Value name: EnableLUA

Value data: 0

Base: ● Hexadecimal ○ Decimal

Step 7: Restart your computer.



WISE-Agent Setup

Installing WISE-Agent

Please wait while the Setup Wizard installs WISE-Agent. This may take several minutes.

WISE-Agent

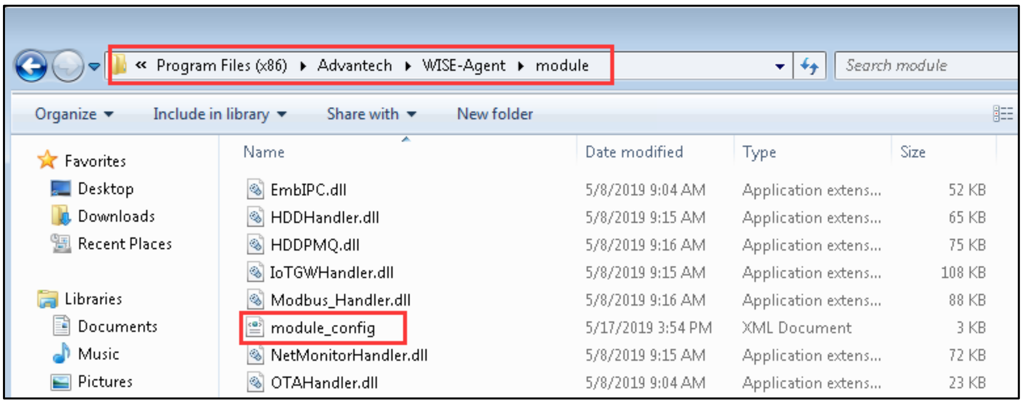
The installer has encountered an unexpected error installing this package. This may indicate a problem with this package. The error code is 12007.

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.

6.2.11 How to Enable/Disable Plugins on WISE-Agent

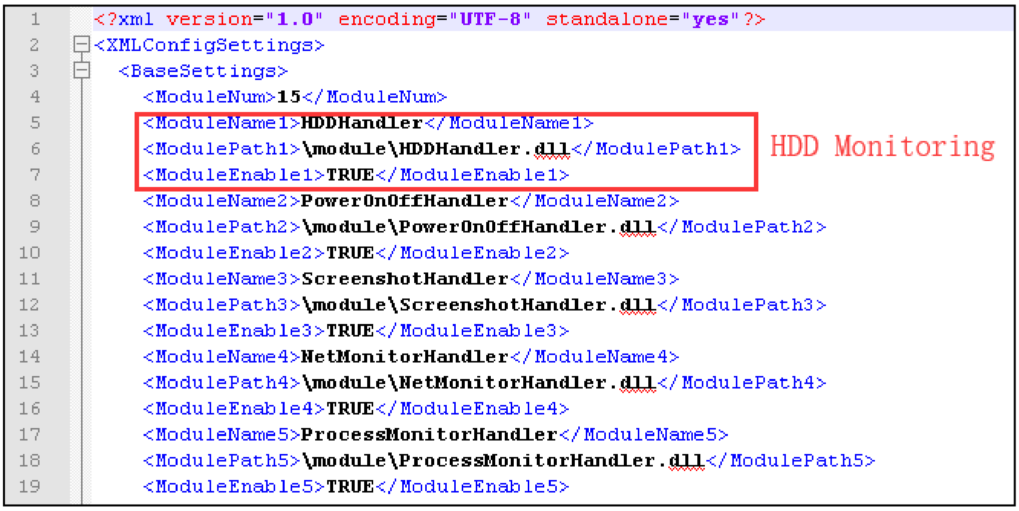
Step 1: Adjust configuration file on WISE-Agent

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



Name	Date modified	Type	Size
EmbIPC.dll	5/8/2019 9:04 AM	Application extens...	52 KB
HDDHandler.dll	5/8/2019 9:15 AM	Application extens...	65 KB
HDDPMQ.dll	5/8/2019 9:16 AM	Application extens...	75 KB
IoTGWHandler.dll	5/8/2019 9:15 AM	Application extens...	108 KB
Modbus_Handler.dll	5/8/2019 9:16 AM	Application extens...	88 KB
module_config	5/17/2019 3:54 PM	XML Document	3 KB
NetMonitorHandler.dll	5/8/2019 9:15 AM	Application extens...	72 KB
OTAHandler.dll	5/8/2019 9:04 AM	Application extens...	23 KB

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

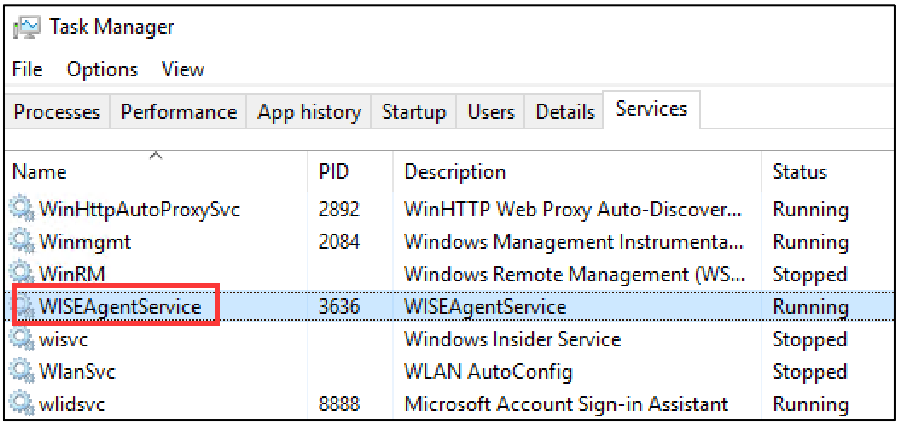


```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<XMLConfigSettings>
  <BaseSettings>
    <ModuleNum>15</ModuleNum>
    <ModuleName1>HDDHandler</ModuleName1>
    <ModulePath1>\module\HDDHandler.dll</ModulePath1>
    <ModuleEnable1>TRUE</ModuleEnable1>
    <ModuleName2>PowerOnOffHandler</ModuleName2>
    <ModulePath2>\module\PowerOnOffHandler.dll</ModulePath2>
    <ModuleEnable2>TRUE</ModuleEnable2>
    <ModuleName3>ScreenshotHandler</ModuleName3>
    <ModulePath3>\module\ScreenshotHandler.dll</ModulePath3>
    <ModuleEnable3>TRUE</ModuleEnable3>
    <ModuleName4>NetMonitorHandler</ModuleName4>
    <ModulePath4>\module\NetMonitorHandler.dll</ModulePath4>
    <ModuleEnable4>TRUE</ModuleEnable4>
    <ModuleName5>ProcessMonitorHandler</ModuleName5>
    <ModulePath5>\module\ProcessMonitorHandler.dll</ModulePath5>
    <ModuleEnable5>TRUE</ModuleEnable5>
```

HDD Monitoring

Step 2: Restart WISE-Agent

Open “Task Manager” and switch to “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

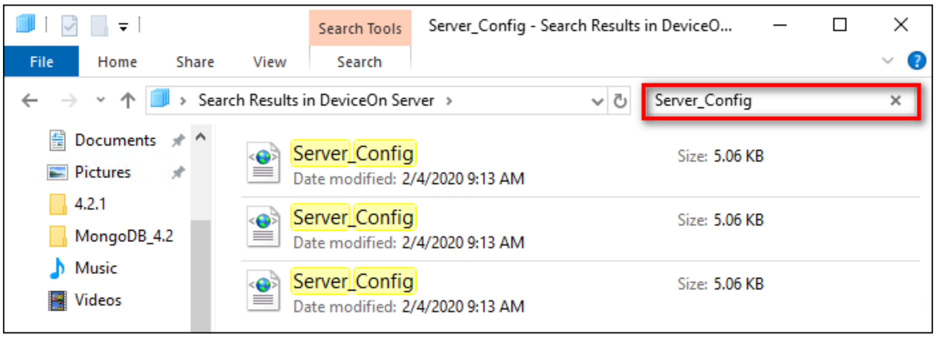
Restart “WISEAgentService” to connect to DeviceOn

6.2.12 How to Adjust 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\)

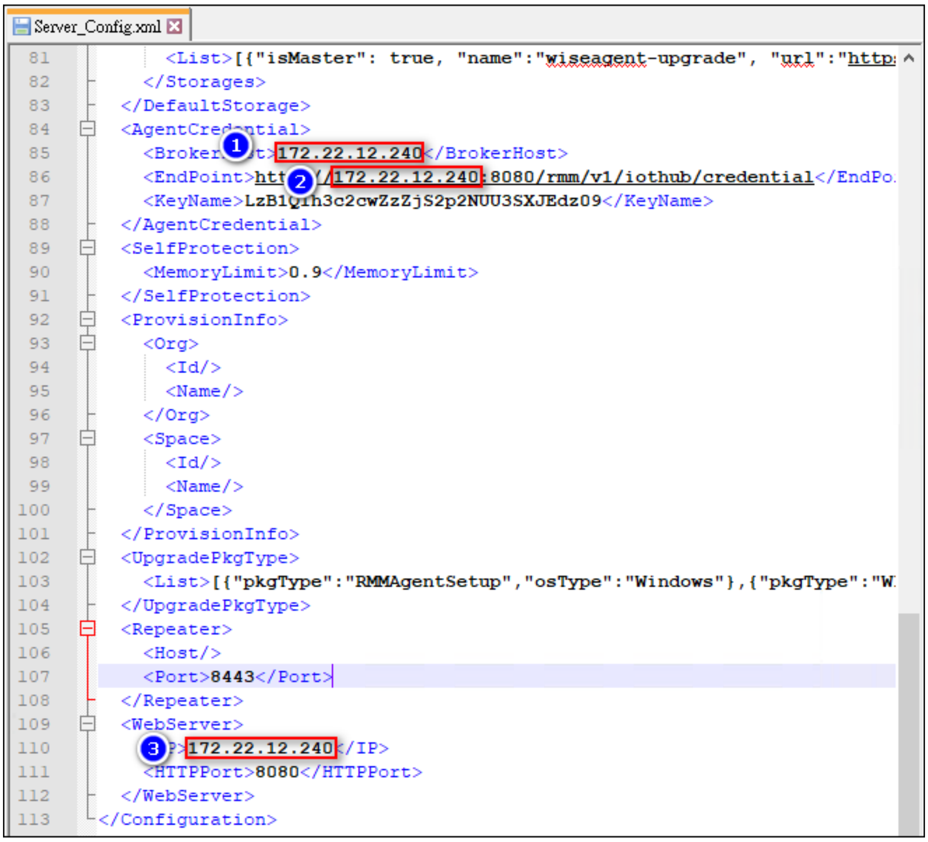


Server_Config
Date modified: 2/4/2020 9:13 AM
Size: 5.06 KB

Server_Config
Date modified: 2/4/2020 9:13 AM
Size: 5.06 KB

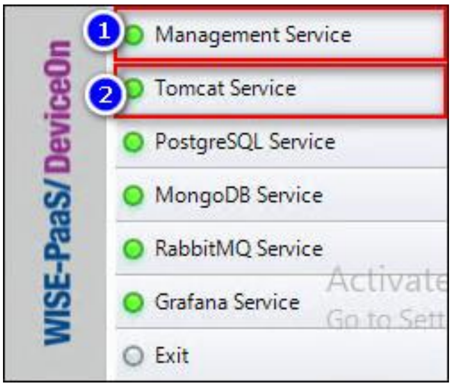
Server_Config
Date modified: 2/4/2020 9:13 AM
Size: 5.06 KB

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



```
      <List>[{"isMaster": true, "name":"wiseagent-upgrade", "url":"http:
    </Storages>
  </DefaultStorage>
  <AgentCredential>
    <BrokerHost>172.22.12.240</BrokerHost>
    <EndPoint>http://172.22.12.240:8080/rmm/v1/iothub/credential</EndPo
    <KeyName>LzB1Qih3c2cwZzZjS2p2NUU3SXJEdz09</KeyName>
  </AgentCredential>
  <SelfProtection>
    <MemoryLimit>0.9</MemoryLimit>
  </SelfProtection>
  <ProvisionInfo>
    <Org>
      <Id/>
      <Name/>
    </Org>
    <Space>
      <Id/>
      <Name/>
    </Space>
  </ProvisionInfo>
  <UpgradePkgType>
    <List>[{"pkgType":"RMMAgentSetup","osType":"Windows"},{"pkgType":"W
  </UpgradePkgType>
  <Repeater>
    <Host/>
    <Port>8443</Port>
  </Repeater>
  <WebServer>
    <IP>172.22.12.240</IP>
    <HTTPPort>8080</HTTPPort>
  </WebServer>
</Configuration>
```

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

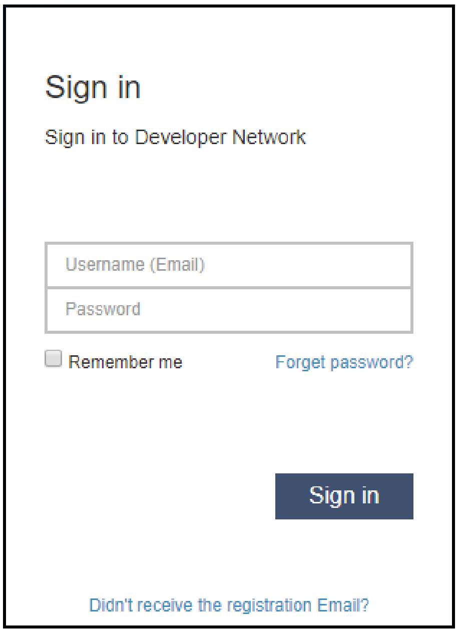


6.2.13 How to Migrate EdgeSense Database to DeviceOn (WISE-PaaS/EnSaaS)

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 into your WISE-PaaS/EnSaaS Management portal


Sign in

Sign in to Developer Network

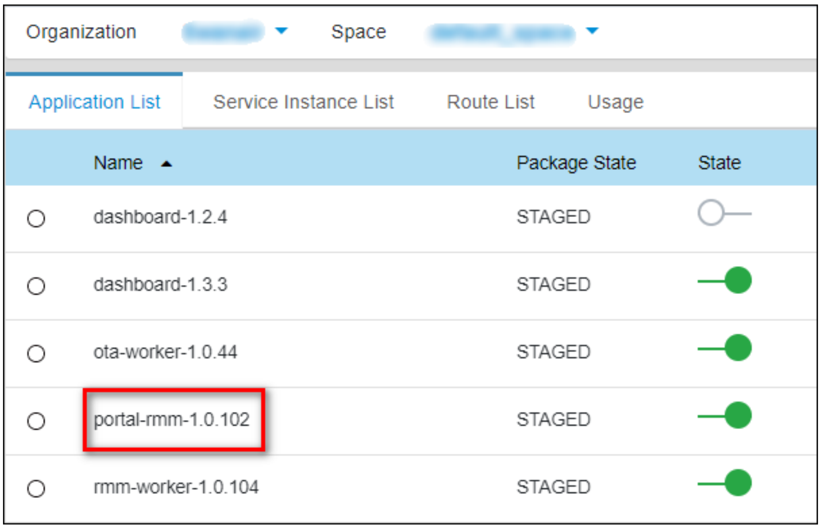
Username (Email)

Password

□ Remember me Forget password?

Didn't receive the registration Email?

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



Organization [redacted] ▾ Space [redacted] ▾

	Name ▲	Package State	State
○	dashboard-1.2.4	STAGED	
○	dashboard-1.3.3	STAGED	
○	ota-worker-1.0.44	STAGED	
○	portal-rmm-1.0.102	STAGED	
○	rmm-worker-1.0.104	STAGED	

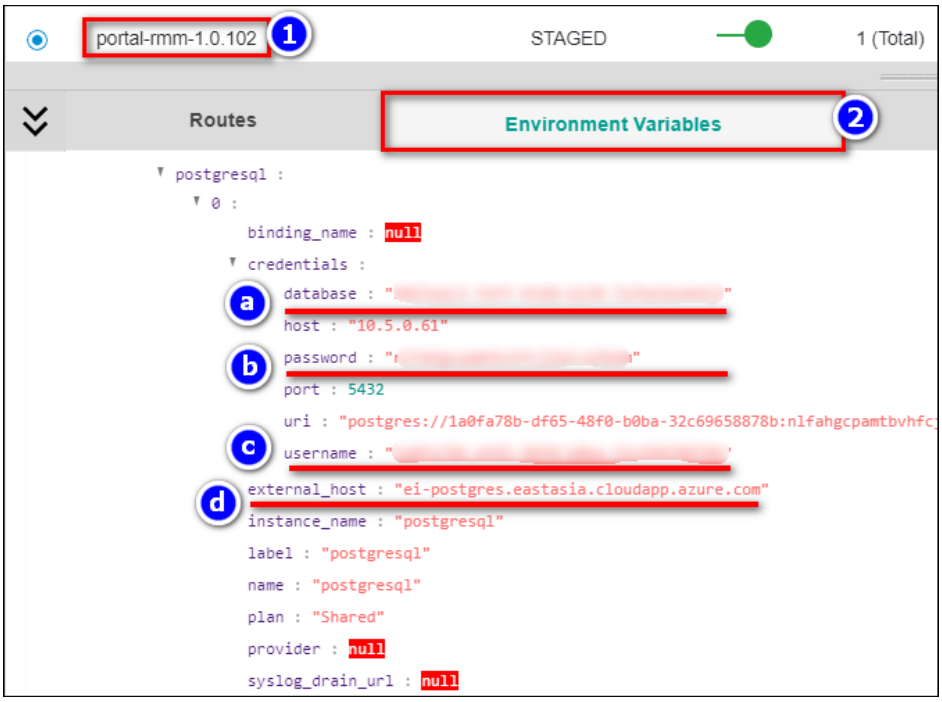
Step 3: Retrieve PostgreSQL information via Application (“portal-rmm-1.0.x”) environment, click on the application.

a. DATABASE_NAME

b. DATABASE_PASSWORD

c. DATABASE_USERNAME

d. DATABASE_HOST



● portal-rmm-1.0.102 STAGED 1 (Total)

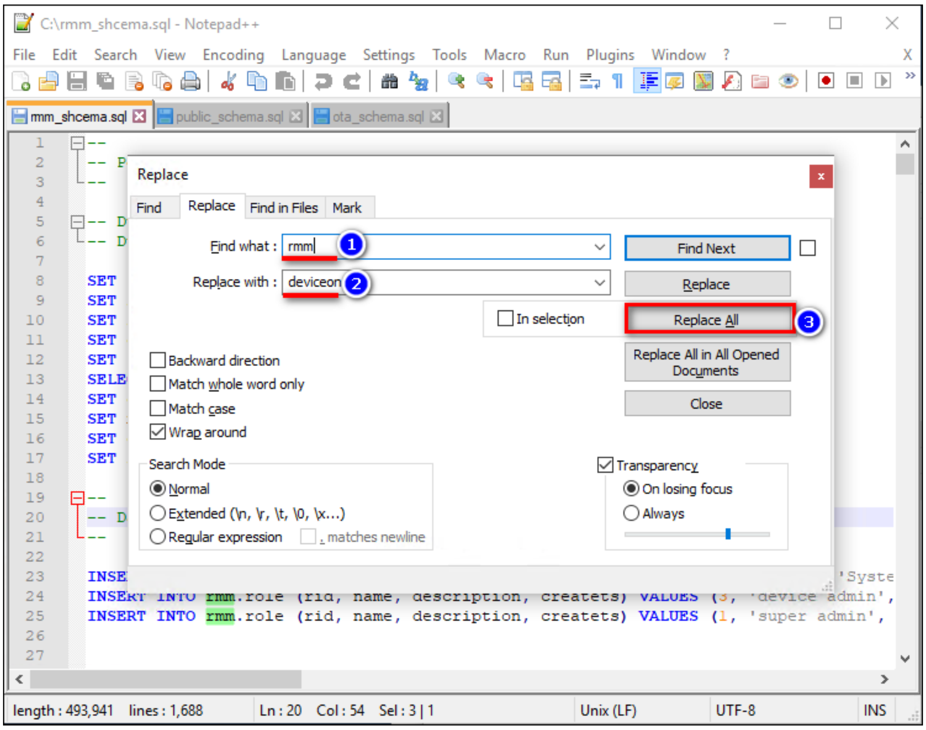
```
▾ postgresql :
   ▾ 0 :
      binding_name : null
    ▾ credentials :
        database : "[redacted]"
        host : "10.5.0.61"
        password : "[redacted]"
        port : 5432
        uri : "postgres://1a0fa78b-df65-48f0-b0ba-32c69658878b:nlfahgcpamtbvhfc
        username : "[redacted]"
      external_host : "ei-postgres.eastasia.cloudapp.azure.com"
      instance_name : "postgresql"
      label : "postgresql"
      name : "postgresql"
      plan : "Shared"
      provider : null
      syslog_drain_url : null
```

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.

```
pg_dump.exe -h DATABASE_HOST -U DATABASE_USERNAME --column-inserts --data-only --schema=rmm --dbname=DATABASE_NAME --file=d:\rmm_schema.sql
pg_dump.exe -h DATABASE_HOST -U DATABASE_USERNAME --column-inserts --data-only --schema=public --dbname=DATABASE_NAME --file=d:\public_schema.sql
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**”.


C:\rmm_shcema.sql - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
rmm_shcema.sql
public_schema.sql
ota_schema.sql
Replace
Find
Replace
Find in Files
Mark
Find Next
Replace
Replace All
Replace All in All Opened Documents
Close
1
2
3

Find what : rmm

Replace with : deviceon

□ In selection

□ Backward direction
□ Match whole word only
□ Match case
☑ Wrap around

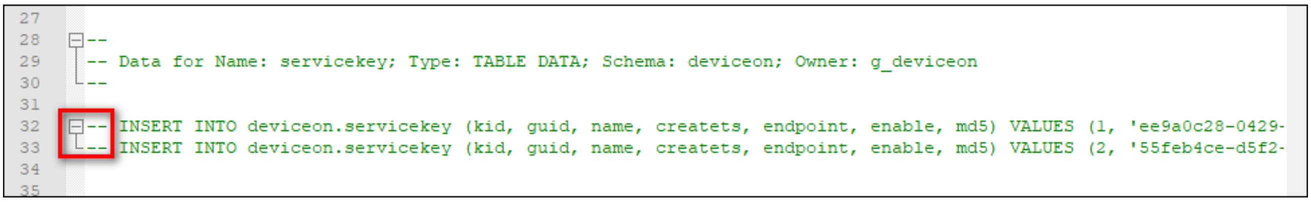
Search Mode
● Normal
○ Extended (\n, \r, \t, \0, \x...)
○ Regular expression □ . matches newline

☑ Transparency
● On losing focus
○ Always

```
INSERT INTO rmm.role (rid, name, description, createts) VALUES (3, 'device admin',
INSERT INTO rmm.role (rid, name, description, createts) VALUES (1, 'super admin',
```

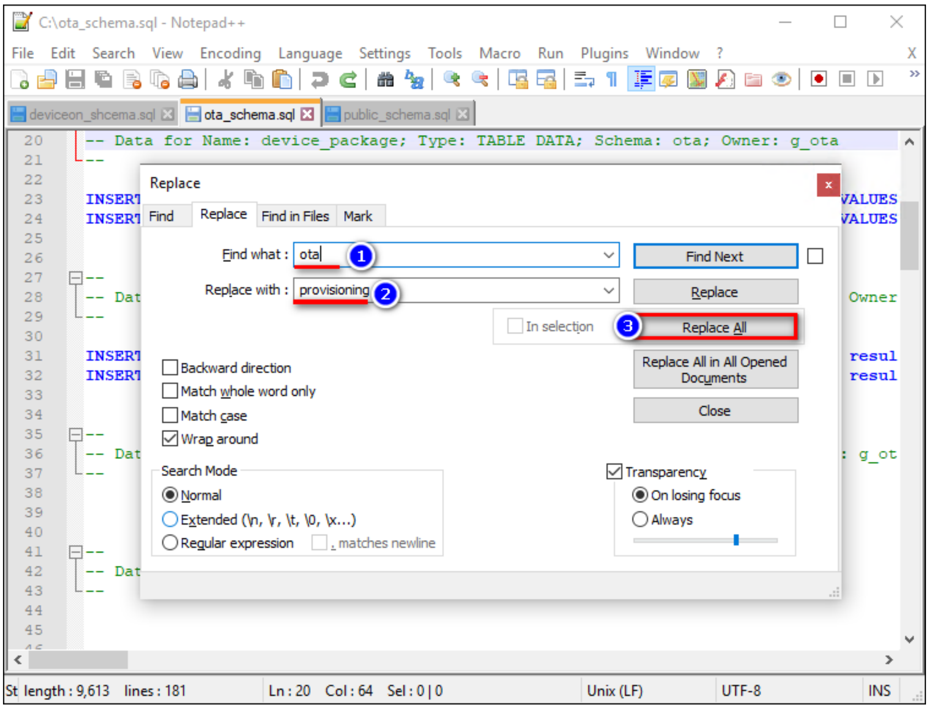
length : 493,941 lines : 1,688 Ln : 20 Col : 54 Sel : 3 | 1 Unix (LF) UTF-8 INS

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



```
--
-- Data for Name: servicekey; Type: TABLE DATA; Schema: deviceon; Owner: g_deviceon
--

--INSERT INTO deviceon.servicekey (kid, guid, name, createts, endpoint, enable, md5) VALUES (1, 'ee9a0c28-0429-
--INSERT INTO deviceon.servicekey (kid, guid, name, createts, endpoint, enable, md5) VALUES (2, '55feb4ce-d5f2-
```

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



C:\ota_schema.sql - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
deviceon_shcema.sql
ota_schema.sql
public_schema.sql
Replace
Find
Replace
Find in Files
Mark
Find Next
Replace
Replace All
Replace All in All Opened Documents
Close
Search Mode
Transparency
1
2
3

```
-- Data for Name: device_package; Type: TABLE DATA; Schema: ota; Owner: g_ota
--
INSERT ... VALUES
INSERT ... VALUES
-- Dat ... Owner
INSERT ... resul
INSERT ... resul
-- Dat ... : g_ot
-- Dat
```

Find what : ota

Replace with : provisioning

□ In selection

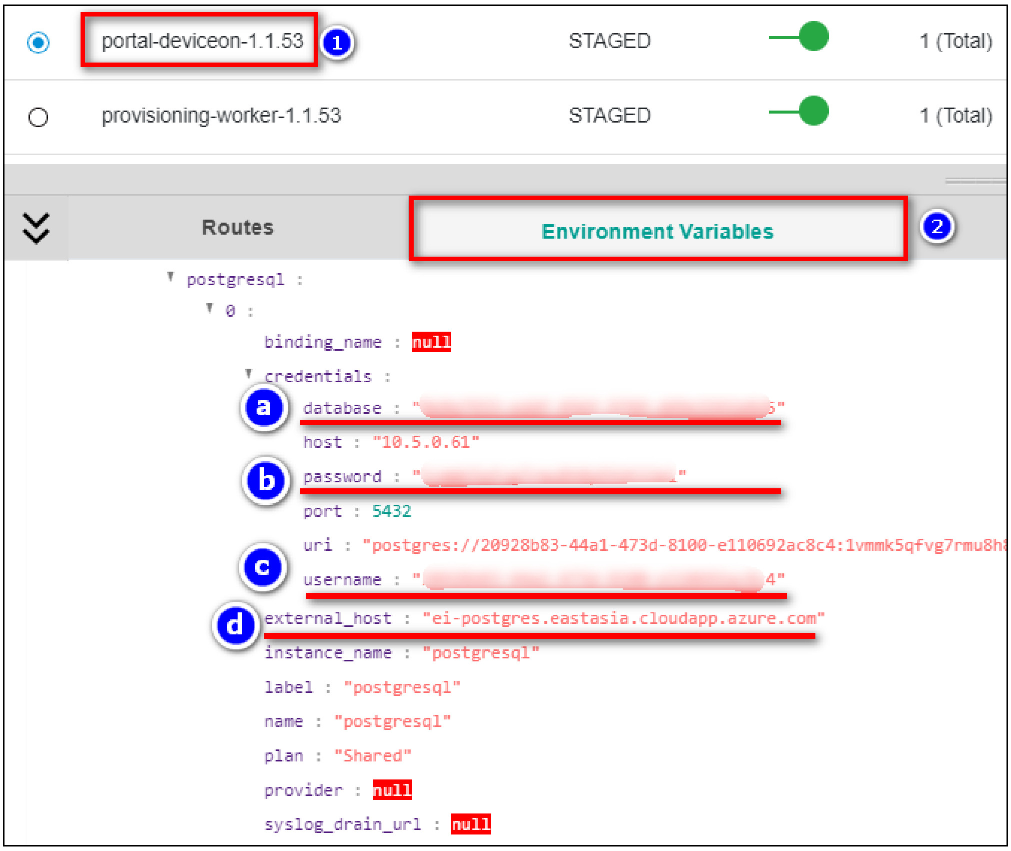
□ Backward direction
□ Match whole word only
□ Match case
☑ Wrap around

Search Mode: ● Normal ○ Extended (\n, \r, \t, \0, \x...) ○ Regular expression □ . matches newline

☑ Transparency: ● On losing focus ○ Always

St length : 9,613 lines : 181 Ln : 20 Col : 64 Sel : 0 | 0 Unix (LF) UTF-8 INS

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.



●	portal-deviceon-1.1.53	STAGED	1 (Total)
○	provisioning-worker-1.1.53	STAGED	1 (Total)

```
▼ postgresql :
   ▼ 0 :
      binding_name : null
      ▼ credentials :
         database : "[redacted]"
         host : "10.5.0.61"
         password : "[redacted]"
         port : 5432
         uri : "postgres://20928b83-44a1-473d-8100-e110692ac8c4:1vmmk5qfvg7rmu8h
         username : "[redacted]"
      external_host : "ei-postgres.eastasia.cloudapp.azure.com"
      instance_name : "postgresql"
      label : "postgresql"
      name : "postgresql"
      plan : "Shared"
      provider : null
      syslog_drain_url : null
```

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.

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

```
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.

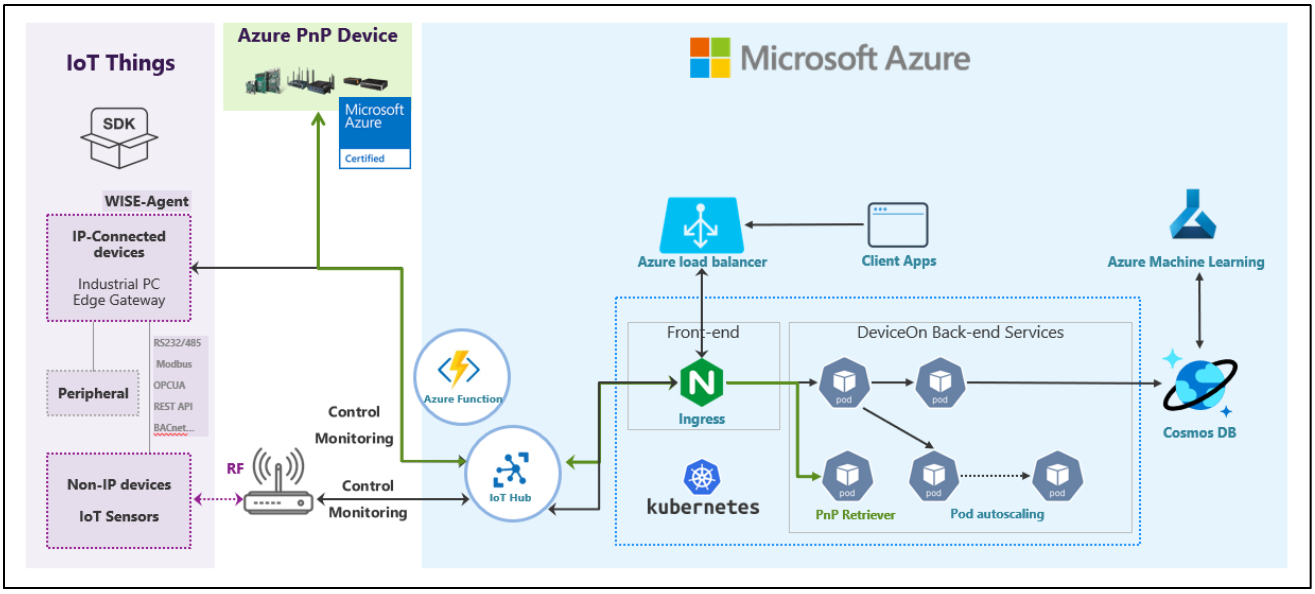
```
mongorestore.exe --host DATABASE_HOST --db DATABASE_NAME --collection COLLECTION_NAME D:\mongodb\COLLECTION_NAME.bson --username DATABASE_USERNAME --password DATABASE_PASSWORD
```

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, IoTHub, 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.



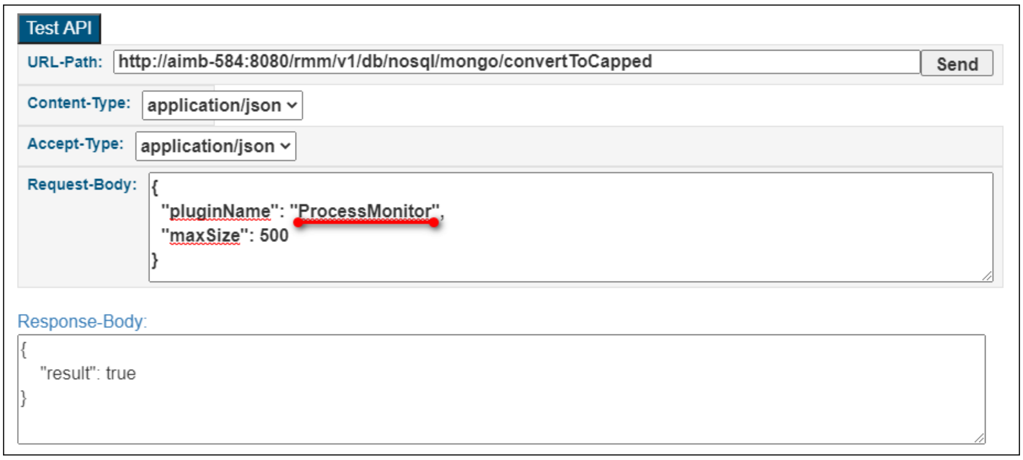
6.2.14 How to Enable Data Retention on DeviceOn

The device’s raw data, such as hardware information, voltage, FAN, network or the wireless sensor data are stored into MongoDB. If ran out of disk storage, the MongoDB service would be stopped. To avoid this situation, you could set up the retention size of each collection on MongoDB via the API or MongoDB command, if the collection existed. Second method, you can adjust the configuration (Server_Config.xml) to enable retention for all collections after the DeviceOn server installed. However, the second method will affect newly created collections only.

- Collection existed:

Please refer to API document to convert collection to capped, the command takes a time (depend on your collection size) to process in the background.

```
/rmm/v1/db/nosql/mongo/convertToCapped
```



URL-Path: http://aimb-584:8080/rmm/v1/db/nosql/mongo/convertToCapped

Content-Type: application/json

Accept-Type: application/json

Request-Body:

```
{
  "pluginName": "ProcessMonitor",
  "maxSize": 500
}
```

Response-Body:

```
{
   "result": true
}
```

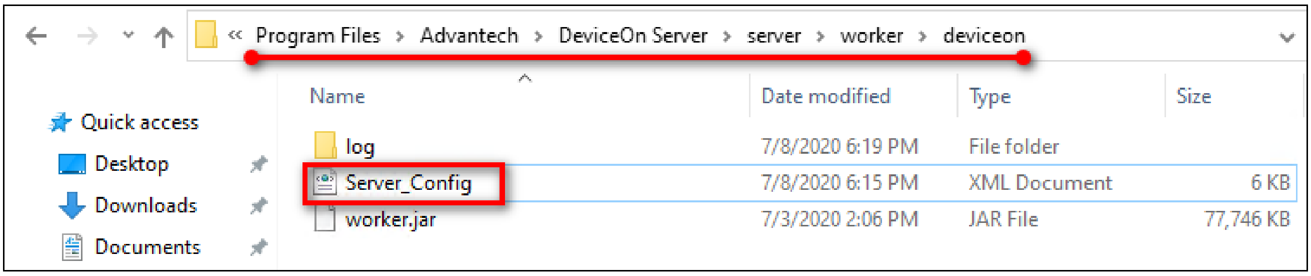
MongoDB Command line:

```
db.runCommand({"convertToCapped": "common_ProcessMonitor", size: 524288000});
```

- Collection non-existed (Apply to newly created):

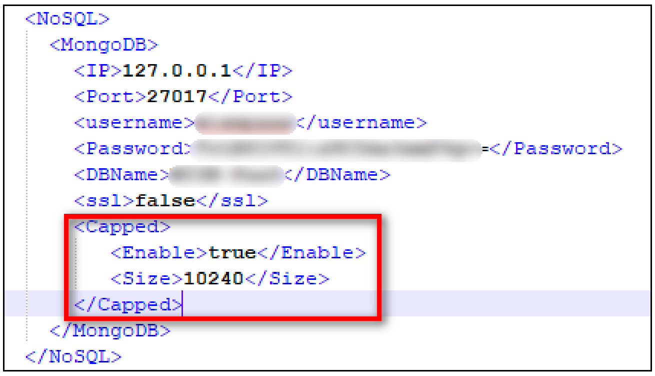
Please add the “Capped” item into Server_config.xml that locate on:

\DeviceOn Server\server\worker\deviceon\


« Program Files › Advantech › DeviceOn Server › server › worker › deviceon
Quick access
Desktop
Downloads
Documents

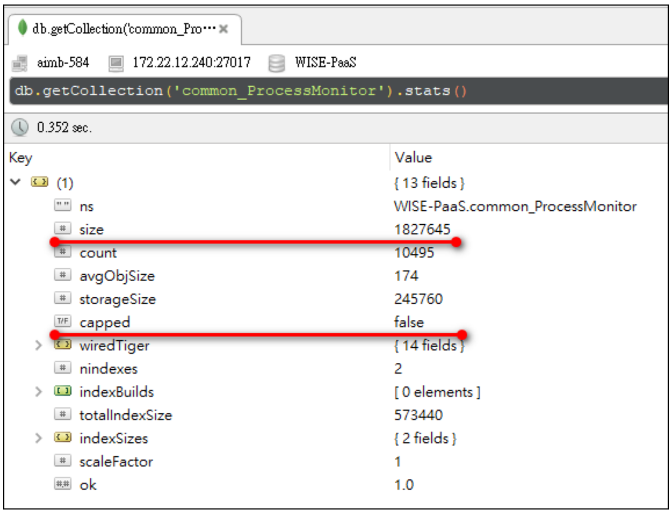
Name	Date modified	Type	Size
log	7/8/2020 6:19 PM	File folder	
Server_Config	7/8/2020 6:15 PM	XML Document	6 KB
worker.jar	7/3/2020 2:06 PM	JAR File	77,746 KB

The unit of size is MB, that’s mean the maximum size (uncompressed) is limited, and then restart the Management service.

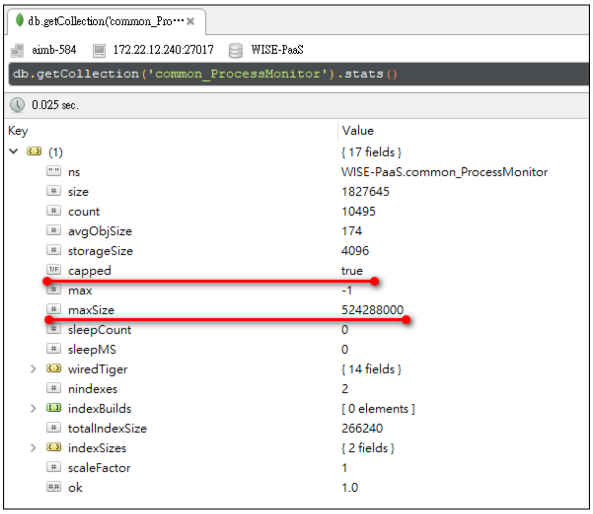


```
<NoSQL>
  <MongoDB>
    <IP>127.0.0.1</IP>
    <Port>27017</Port>
    <username>[redacted]</username>
    <Password>[redacted]</Password>
    <DBName>[redacted]</DBName>
    <ssl>false</ssl>
    <Capped>
       <Enable>true</Enable>
       <Size>10240</Size>
    </Capped>
  </MongoDB>
</NoSQL>
```

After that, you could check and confirm the collection applied through third party tool (Rob 3T).



```
db.getCollection('common_Pro···
aimb-584   172.22.12.240:27017   WISE-PaaS
db.getCollection('common_ProcessMonitor').stats()
0.352 sec.
Key                    Value
(1)                    { 13 fields }
  ns                   WISE-PaaS.common_ProcessMonitor
  size                 1827645
  count                10495
  avgObjSize           174
  storageSize          245760
  capped               false
  wiredTiger           { 14 fields }
  nindexes             2
  indexBuilds          [ 0 elements ]
  totalIndexSize       573440
  indexSizes           { 2 fields }
  scaleFactor          1
  ok                   1.0
```



```
db.getCollection('common_Pro···
aimb-584   172.22.12.240:27017   WISE-PaaS
db.getCollection('common_ProcessMonitor').stats()
0.025 sec.
Key                    Value
(1)                    { 17 fields }
  ns                   WISE-PaaS.common_ProcessMonitor
  size                 1827645
  count                10495
  avgObjSize           174
  storageSize          4096
  capped               true
  max                  -1
  maxSize              524288000
  sleepCount           0
  sleepMS              0
  wiredTiger           { 14 fields }
  nindexes             2
  indexBuilds          [ 0 elements ]
  totalIndexSize       266240
  indexSizes           { 2 fields }
  scaleFactor          1
  ok                   1.0
```

6.2.15 How to Enable HTTPS on DeviceOn Web Service

Generate Let's Encrypt certificate using Certbot for DeviceOn.

- Let’s Encrypt is a new free, automated, and open source, Certificate Authority.
- Certbot is a console based certificate generation tool for Let's Encrypt.

In this recipe, we will generate a Let's Encypt certificate using Certbot. This certificate will then be deployed for use in the DeviceOn server.

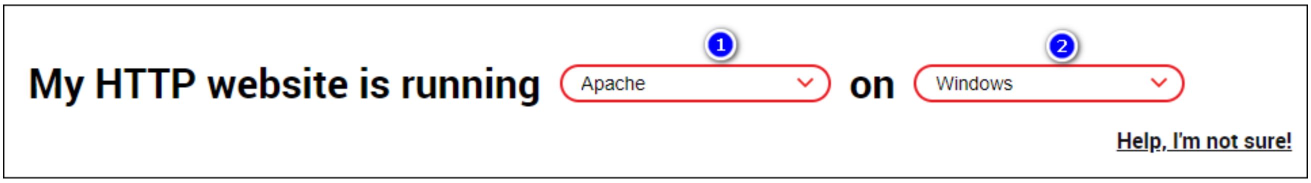
Dependancies:

- Port 443 for https needs to be open and available at time of executing certbot.
- Certbot needs root access while executing because only root is allowed to bind to any port below 1024.
- We will be using our own domain myminio.com as an example in this recipe. Replace with your own domain under your setup.

Step 1: Install Certbot

Install Certbot by following the documentation at https://certbot.eff.org/

Since the DeviceOn Web service is running on Apache Tomcat, please select to “Apache” and “Windows” to donwnload Certbot installer.

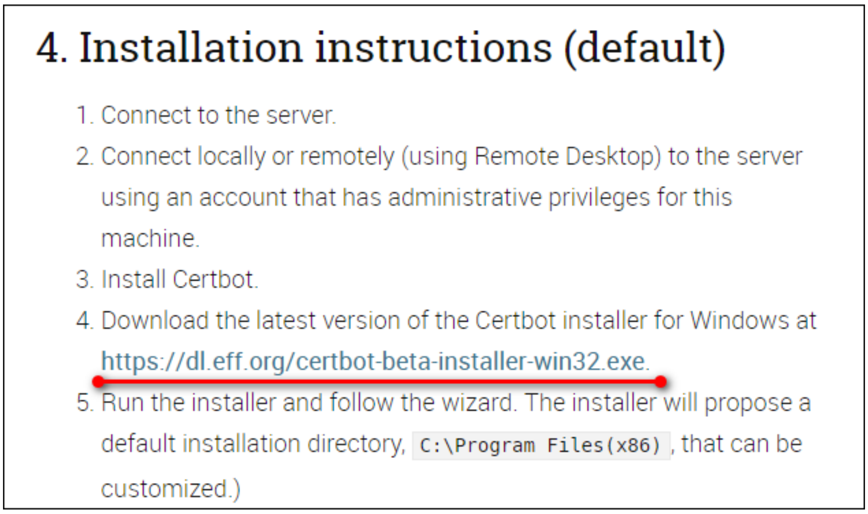


My HTTP website is running Apache on Windows

Help, I'm not sure!

Scrolling down the instruction, you may get the installer package on Step 4.

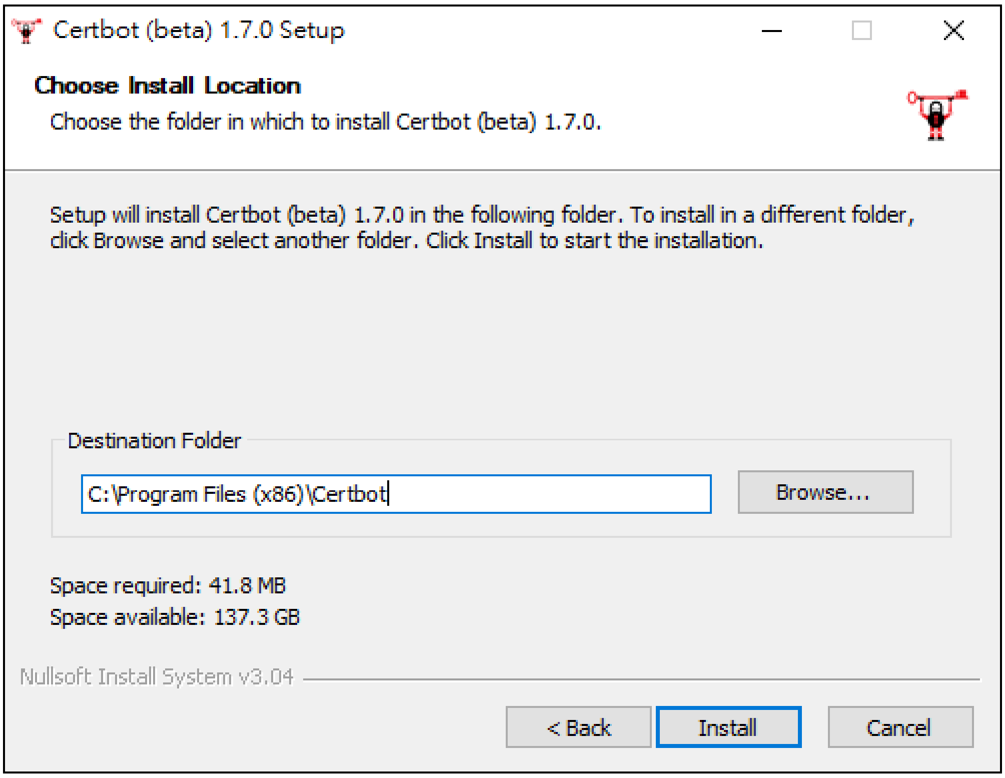
https://dl.eff.org/certbot-beta-installer-win32.exe



4. Installation instructions (default)

1. Connect to the server.
2. Connect locally or remotely (using Remote Desktop) to the server using an account that has administrative privileges for this machine.
3. Install Certbot.
4. Download the latest version of the Certbot installer for Windows at https://dl.eff.org/certbot-beta-installer-win32.exe.
5. Run the installer and follow the wizard. The installer will propose a default installation directory, `C:\Program Files(x86)`, that can be customized.)

Run the installer and follow the wizard. The installer will propose a default installation directory, C:\Program Files(x86), that can be customized.)



Certbot (beta) 1.7.0 Setup

Choose Install Location

Choose the folder in which to install Certbot (beta) 1.7.0.

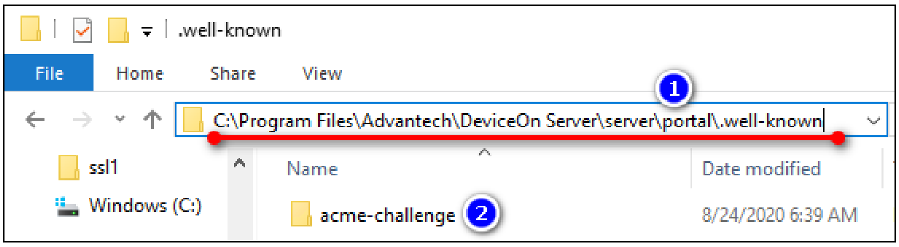
Setup will install Certbot (beta) 1.7.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files (x86)\Certbot

Space required: 41.8 MB
Space available: 137.3 GB

Step 2: Create the folder to authenticate

Create the folder named **acme-challenge** under **<DeviceOn Folder>\server\portal\.well-known**. If the folder "**.well-known**" is not exist, please create it manually (via CLI, for example: mkdir).



.well-known

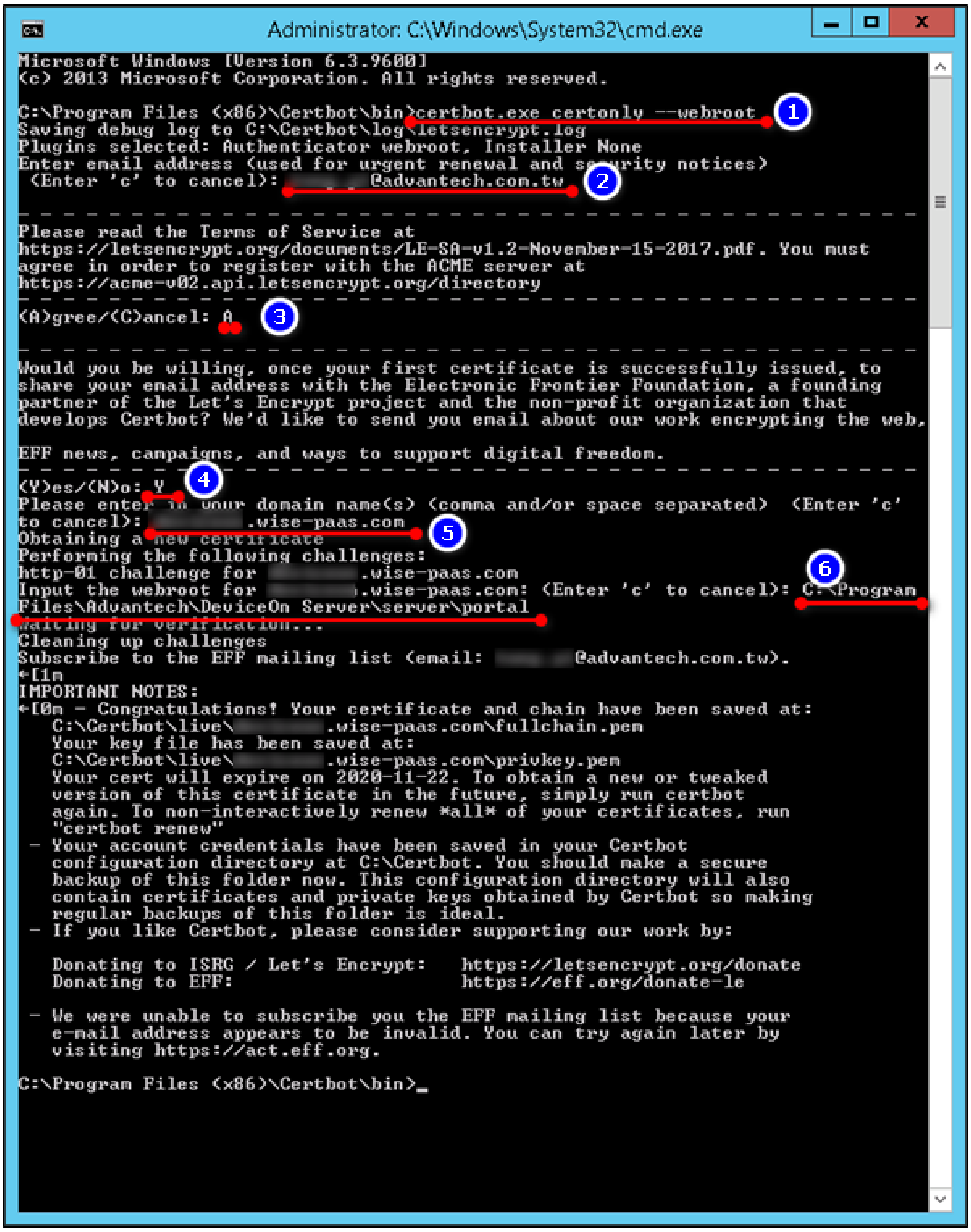
C:\Program Files\Advantech\DeviceOn Server\server\portal\.well-known

Name	Date modified
acme-challenge	8/24/2020 6:39 AM

Step 3: Choose how you'd like to run Certbot

Run the following command to create credential files and enter your website information. The domain name(s) should input yours and the webroot to (**\DeviceOn Path\server\portal\**)

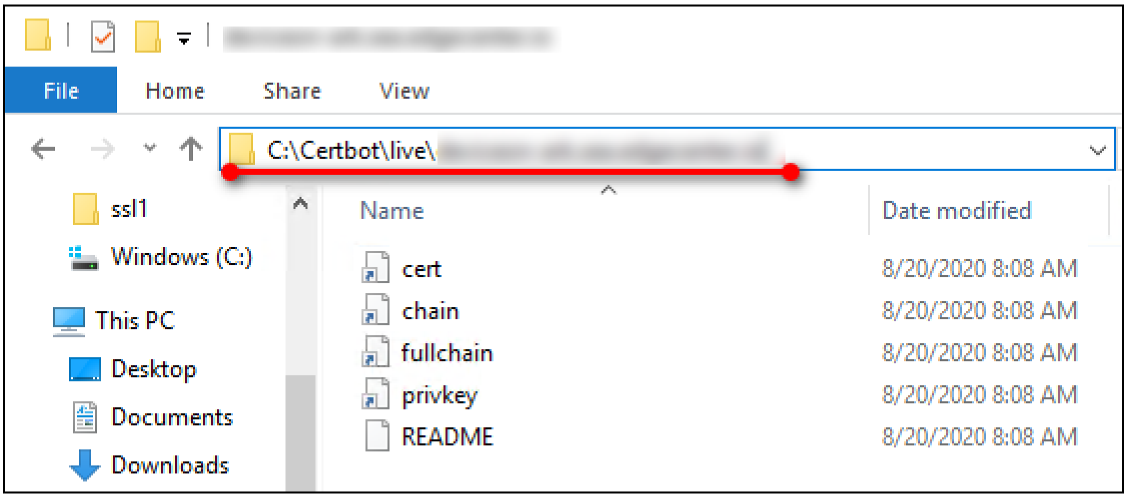
```
certbot.exe certonly --webroot
```



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Certbot\bin>certbot.exe certonly --webroot
Saving debug log to C:\Certbot\log\letsencrypt.log
Plugins selected: Authenticator webroot, Installer None
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): [redacted]@advantech.com.tw

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)gree/(C)ancel: A

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,

EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y
Please enter in your domain name(s) (comma and/or space separated)  (Enter 'c'
to cancel): [redacted].wise-paas.com
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for [redacted].wise-paas.com
Input the webroot for [redacted].wise-paas.com: (Enter 'c' to cancel): C:\Program
Files\Advantech\DeviceOn Server\server\portal
Waiting for verification...
Cleaning up challenges
Subscribe to the EFF mailing list (email: [redacted]@advantech.com.tw).
←[1m
IMPORTANT NOTES:
←[0m - Congratulations! Your certificate and chain have been saved at:
   C:\Certbot\live\[redacted].wise-paas.com\fullchain.pem
   Your key file has been saved at:
   C:\Certbot\live\[redacted].wise-paas.com\privkey.pem
   Your cert will expire on 2020-11-22. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at C:\Certbot. You should make a secure
   backup of this folder now. This configuration directory will also
   contain certificates and private keys obtained by Certbot so making
   regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le

 - We were unable to subscribe you the EFF mailing list because your
   e-mail address appears to be invalid. You can try again later by
   visiting https://act.eff.org.

C:\Program Files (x86)\Certbot\bin>_
```

Step 4: Install your certificate

You'll need to install your new certificate in the configuration file or interface for your webserver. Certificates are located in C:\Certbot\live\[certificate_name], where [certificate_name] is the name of your certificate (usually the first domain if the --cert-name flag has not been used on the certonly command)



cert 8/20/2020 8:08 AM
chain 8/20/2020 8:08 AM
fullchain 8/20/2020 8:08 AM
privkey 8/20/2020 8:08 AM
README 8/20/2020 8:08 AM

Step 5: Install your certificate on DeviceOn Web Services

- Open the **server.xml** on text editor tool that located in the **\DeviceOn Path\tomcat\conf\**
- Add the following XML attribute (Connector) into **Service** tag and give your certification path that generated on Step 4.

```
<Connector port="443"
    protocol="org.apache.coyote.http11.Http11AprProtocol"
    connectionTimeout="20000"
    useSendfile="false"
    compression="on"
    compressionMinSize="2048"
    noCompressionUserAgents="gozilla, traviata"

compressableMimeType="text/html,text/xml,text/plain,text/css,text/javascript,applicat
ion/javascript,application/xml,application/json"
    redirectPort="8443"
    maxThreads="150"
    scheme="https"
    secure="true"
    SSLEnabled="true">
    <UpgradeProtocol className="org.apache.coyote.http2.Http2Protocol"
        overheadWindowUpdateThreshold="-1"
        overheadDataThreshold="-1"
        writeTimeout="-1"
        streamWriteTimeout="-1"
        streamReadTimeout="-1"
        maxHeaderSize="8192"
        maxConcurrentStreams="300"
        readTimeout="-1"

compressibleMimeType="text/html,text/xml,text/plain,text/css,text/javascript,applicat
ion/javascript,application/json"
        compression="on" compressionMinSize="1024"/>
    <SSLHostConfig>
        <Certificate certificateKeyFile="C:\Certbot\live\<DNS>\privkey.pem"
                     certificateFile="C:\Certbot\live\<DNS>\cert.pem"
                     certificateChainFile="C:\Certbot\live\<DNS>\fullchain.pem"
                     type="RSA" />
    </SSLHostConfig>
</Connector>
```

Step 6: Restart DeviceOn web services (Tomcat_IoT) to reload the configuration

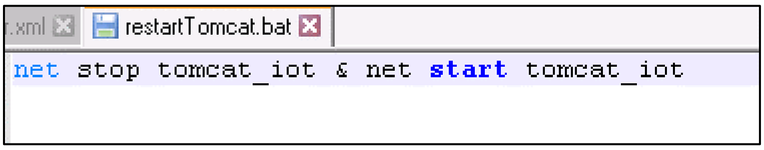
Step 7: Replace the certificate files that in the websockify folder.

```
xcopy "C:\Certbot\live\<DNS>\privkey.pem" "<INSTALLER_PATH>\server\portal\WEB-INF\classes\novnc\websockify\wise-paas.com.private.key" /Y
```

```
xcopy "C:\Certbot\live\<DNS>\cert.pem" "<INSTALLER_PATH>\server\portal\WEB-INF\classes\novnc\websockify\wise-paas.crt" /Y
```

Step 8: Enable to automatic renewal

- Create a batch file named restartTomcat.bat which content as below.



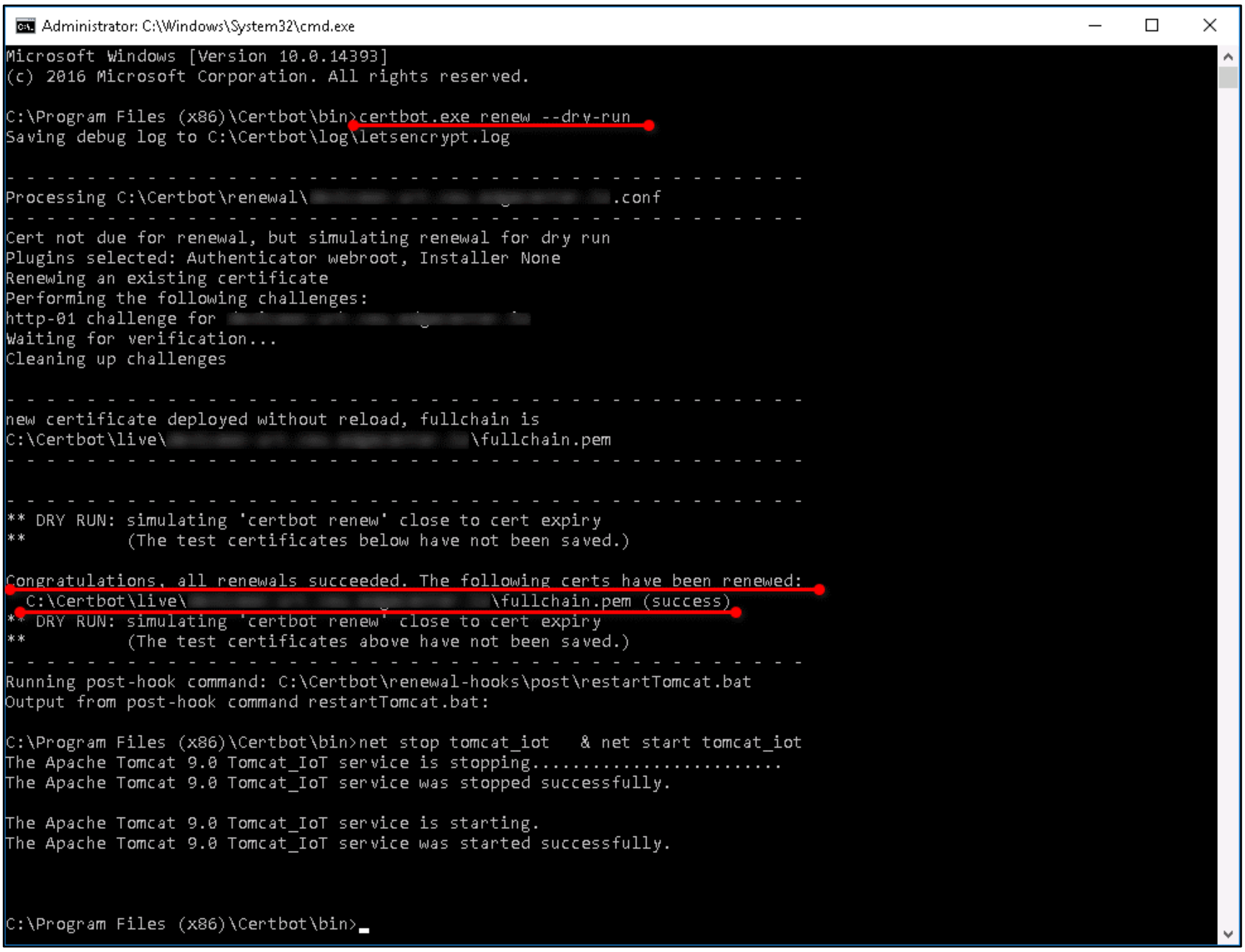
```
net stop tomcat_iot & net start tomcat_iot
```

- Copy the batch file into C:\Certbot\renewal-hooks\post\

Step 9 (Optional): Test automatic renewal, please run the following command

```
certbot.exe renew -dry-run
```

Step 10 (Optional): If you get all renewals succeeded, it means your configuration is correct.



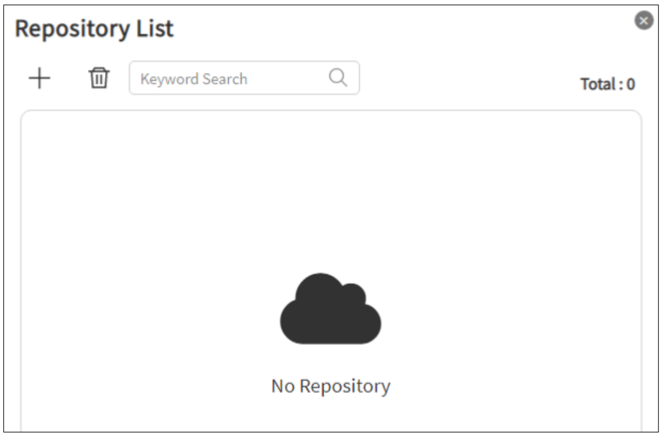
Administrator: C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Certbot\bin>certbot.exe renew --dry-run
Saving debug log to C:\Certbot\log\letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Processing C:\Certbot\renewal\[redacted].conf
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Cert not due for renewal, but simulating renewal for dry run
Plugins selected: Authenticator webroot, Installer None
Renewing an existing certificate
Performing the following challenges:
http-01 challenge for [redacted]
Waiting for verification...
Cleaning up challenges

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
new certificate deployed without reload, fullchain is
C:\Certbot\live\[redacted]\fullchain.pem
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
** DRY RUN: simulating 'certbot renew' close to cert expiry
**          (The test certificates below have not been saved.)

Congratulations, all renewals succeeded. The following certs have been renewed:
  C:\Certbot\live\[redacted]\fullchain.pem (success)
** DRY RUN: simulating 'certbot renew' close to cert expiry
**          (The test certificates above have not been saved.)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Running post-hook command: C:\Certbot\renewal-hooks\post\restartTomcat.bat
Output from post-hook command restartTomcat.bat:

C:\Program Files (x86)\Certbot\bin>net stop tomcat_iot   & net start tomcat_iot
The Apache Tomcat 9.0 Tomcat_IoT service is stopping.........................
The Apache Tomcat 9.0 Tomcat_IoT service was stopped successfully.

The Apache Tomcat 9.0 Tomcat_IoT service is starting.
The Apache Tomcat 9.0 Tomcat_IoT service was started successfully.



C:\Program Files (x86)\Certbot\bin>_
```

Step 11: Turn Windows firewall on inbound port **443** for your HTTPS, and make sure your network security rules allow.

6.2.16 How to Enable Passive Mode on DeviceOn FTP Server

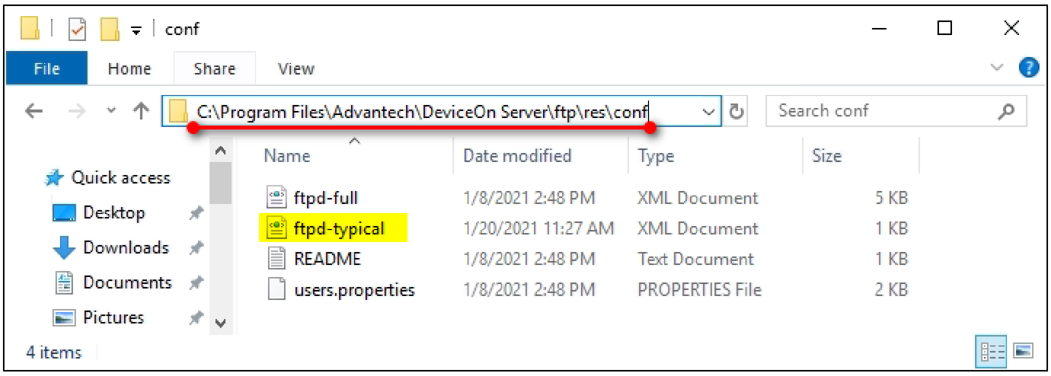
DeviceOn FTP default setting is active mode. However, FTP runs active mode may fail in cases where the server is behind a router or the server deplyed on Azure/AWS or other cloud's virtual machine. And that will cause DeviceOn initialize failure.



To solve this issue, you should change FTP server to **passive mode**.

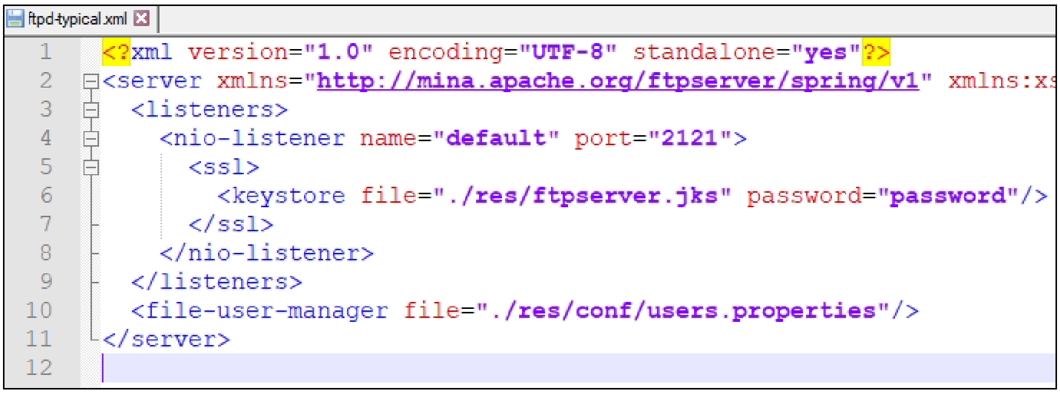
Below are step-by-step to change the setting. First is FTP server configuration, second is Network Security Group (Azure, AWS or your network security setting), and last to restart DeviceOn Server.

Step 1: Open the ftpd-typical.xml on text editor tool that located in the \DeviceOn Path\ftp\res\conf\



C:\Program Files\Advantech\DeviceOn Server\ftp\res\conf

Name	Date modified	Type	Size
ftpd-full	1/8/2021 2:48 PM	XML Document	5 KB
ftpd-typical	1/20/2021 11:27 AM	XML Document	1 KB
README	1/8/2021 2:48 PM	Text Document	1 KB
users.properties	1/8/2021 2:48 PM	PROPERTIES File	2 KB



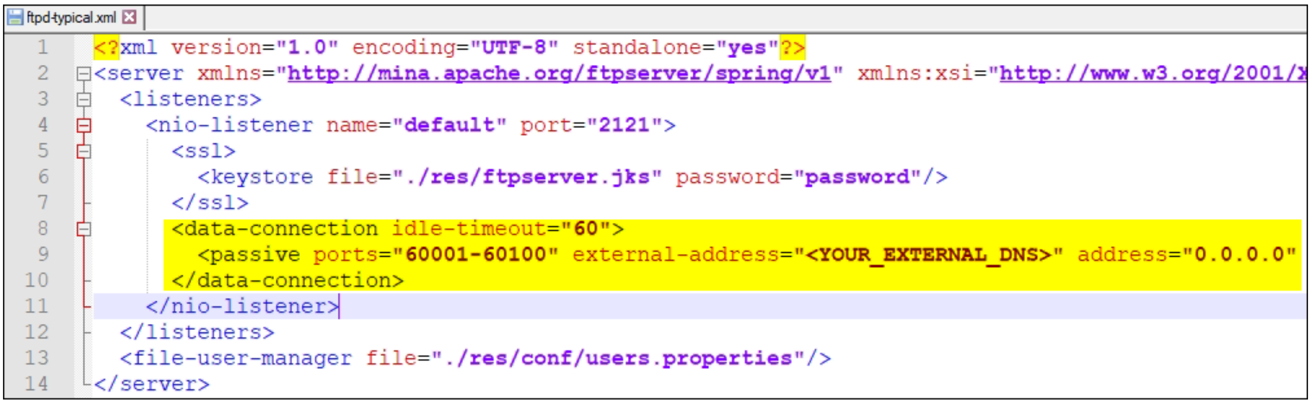
```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<server xmlns="http://mina.apache.org/ftpserver/spring/v1" xmlns:xs
  <listeners>
    <nio-listener name="default" port="2121">
      <ssl>
        <keystore file="./res/ftpserver.jks" password="password"/>
      </ssl>
    </nio-listener>
  </listeners>
  <file-user-manager file="./res/conf/users.properties"/>
</server>

```

Add the following XML attribute (data-connection) into listeners tag and give your **passive ports** range and **external DNS**.

```xml
<data-connection idle-timeout="60">

  <passive ports="60001-60100" external-address="<YOUR_EXTERNAL_DNS>" address="0.0.0.0" />
```

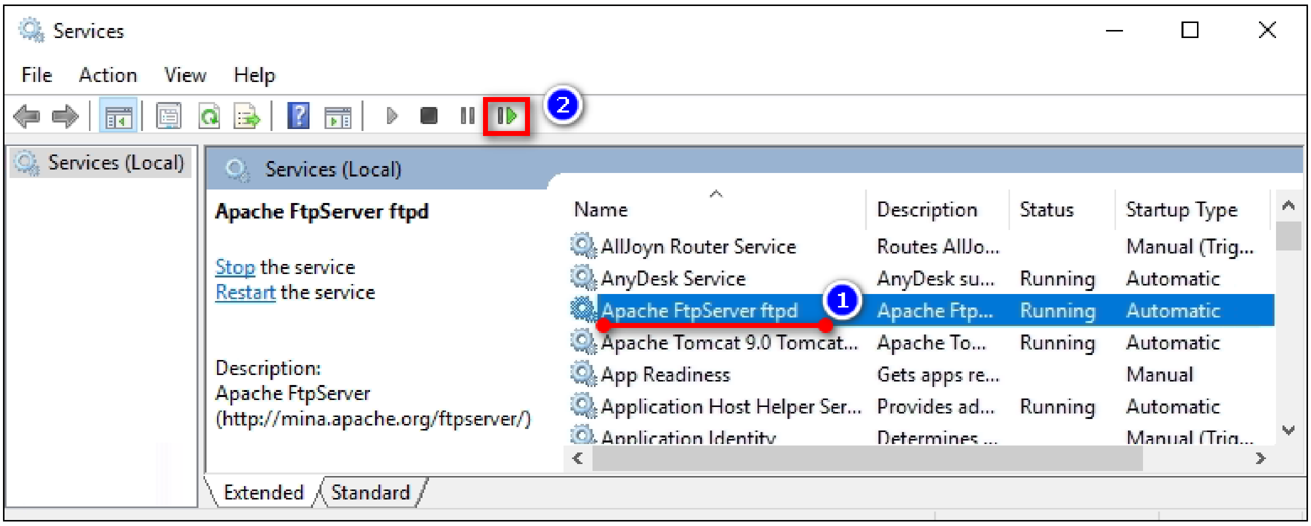
```
</data-connection>
```

"60001-60100" means in passive mode, ftp client uses port 60001 to 60100 to transfer data. You could change it to any available ports range. "**YOUR_EXTERNAL_DNS**" means in passive mode, client's destination domain name. You should replace it with real domain name which can be access from external side.



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<server xmlns="http://mina.apache.org/ftpserver/spring/v1" xmlns:xsi="http://www.w3.org/2001/X
  <listeners>
    <nio-listener name="default" port="2121">
      <ssl>
        <keystore file="./res/ftpserver.jks" password="password"/>
      </ssl>
      <data-connection idle-timeout="60">
        <passive ports="60001-60100" external-address="<YOUR_EXTERNAL_DNS>" address="0.0.0.0"
      </data-connection>
    </nio-listener>
  </listeners>
  <file-user-manager file="./res/conf/users.properties"/>
</server>
```

Step 2: Apply setting by restart service "Apache FtpServer ftpd"



Apache FtpServer ftpd

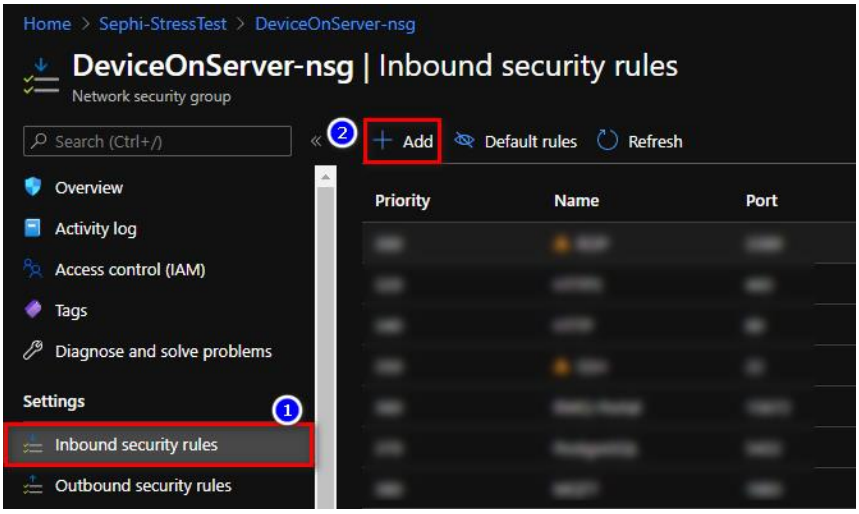
Stop the service
Restart the service

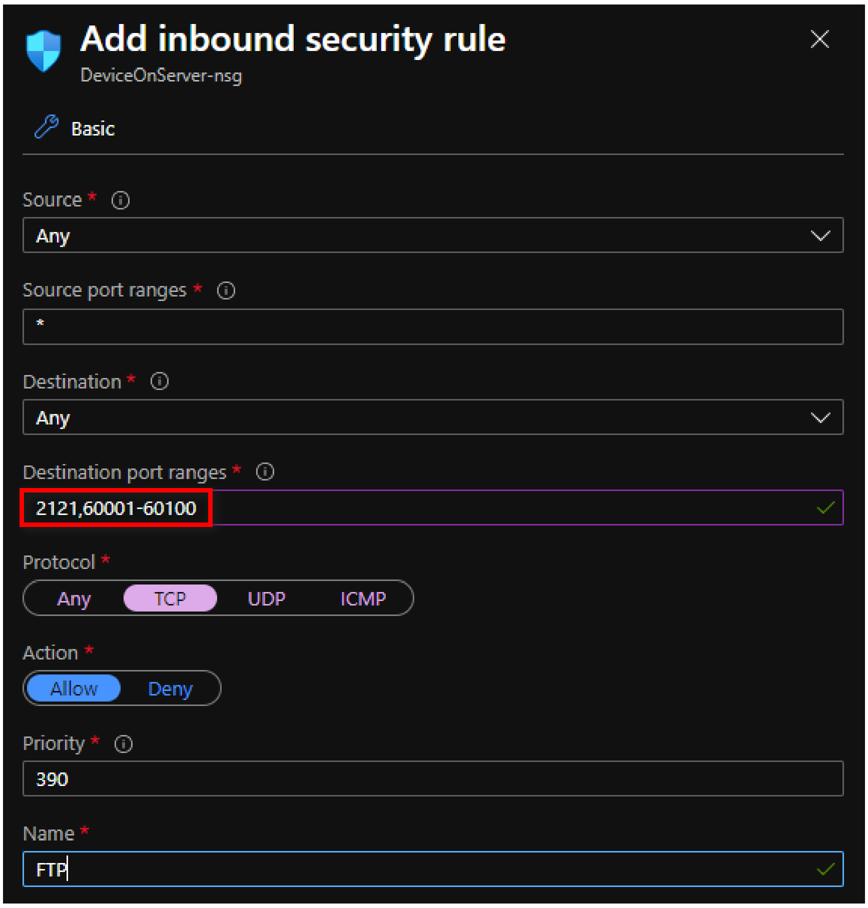
Description:
Apache FtpServer
(http://mina.apache.org/ftpserver/)

Name	Description	Status	Startup Type
AllJoyn Router Service	Routes AllJo...		Manual (Trig...
AnyDesk Service	AnyDesk su...	Running	Automatic
Apache FtpServer ftpd	Apache Ftp...	Running	Automatic
Apache Tomcat 9.0 Tomcat...	Apache To...	Running	Automatic
App Readiness	Gets apps re...		Manual
Application Host Helper Ser...	Provides ad...	Running	Automatic
Application Identity	Determines ...		Manual (Trig...

Step 3: Add inbound security rules on your network security group, make sure blow ports are available, and takes Azure as an example.

- 2121 (command port)
- 60001-60100 (Passive port)




Add inbound security rule

DeviceOnServer-nsg

Basic

Source * : Any

Source port ranges * : *

Destination * : Any

Destination port ranges * : 2121,60001-60100

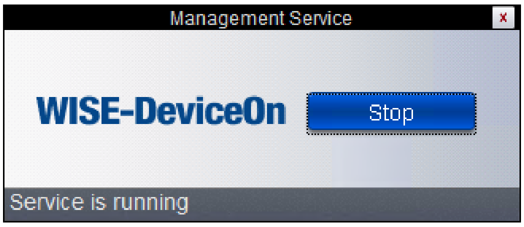
Protocol * : ○ Any ● TCP ○ UDP ○ ICMP

Action * : ● Allow ○ Deny

Priority * : 390

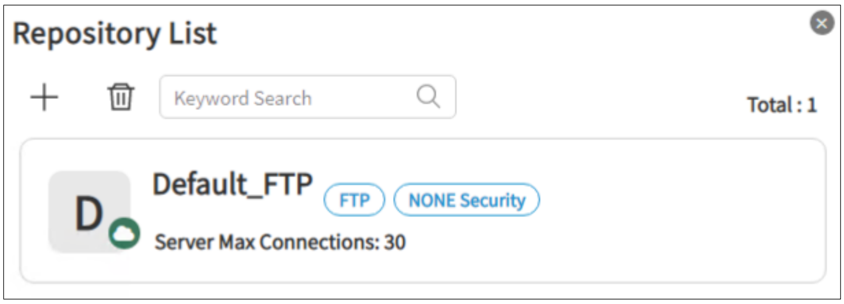
Name * : FTP

Step 4: Restart DeviceOn Server, stop/start the “Management Service”



Service is running

Back to DeviceOn portal, the default FTP appear in repository list.



Repository List

Default_FTP

Server Max Connections: 30

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)
	Edit	2FA Authentication	✓ (Only Self)	✓ (Only Self)	✓ (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)
	Edit	Share Device	✓	✓ (Only Self & Device Admin)	✓ (Only Self-Managed Devices)
	View	Search Unmanaged Devices	✓	✓	✓
	Control	Power, Remote Desktop, Terminal, Screenshot, Backup/Recovery, Protection, Windows Lockdown Actions…	✓	✓ (Only Self & Device Admin)	✓ (Only Self-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)
OTA Management	Create	Create Storage Repository	✓	✓	
	Edit	Edit Storage Repository	✓	✓	
	View	View Storage Repository	✓	✓	✓

	Delete	Delete Storage Repository	✓	✓	
	Upload	Upload OTA Package	✓	✓	✓
	View	View OTA Package	✓ (Only Self & Public App)	✓ (Only Self & Public App)	✓ (Only Self & Public App)
	Delete	Delete OTA Package	✓ (Only Self)	✓ (Only Self)	✓ (Only Self)
	Deploy	Deploy OTA Package	✓	✓ (Only Self-Managed & Device Admin Devices)	✓ (Only Self-Managed Devices)
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	✓ (Only Self-Managed Devices)

				Devices)	
	Edit	Edit Event Alert Setting	✓ (Only Self)	✓ (Only Self)	✓ (Only Self)
	Edit	Configure Alert Services (Email, SMS, WeChat, Telegram, LINE, Teams, Slack, Webhook.)	✓	✓	
	Edit	Production Activation	✓	✓	
	Create	Addins	✓	✓	
	Create/Edit	Dashboard	✓ (Only Self)	✓ (Only Self)	✓ (Only Self)
	Edit	System Report	✓	✓	
	Edit	System Menu	✓	✓	
	Edit	System Theme	✓ (Only Self)	✓ (Only Self)	✓ (Only Self)
	Edit	System Logo	✓	✓	
	Edit	System Login Page	✓	✓	
	Edit	System Overview Setting	✓ (Only Self)	✓ (Only Self)	✓ (Only Self)
	Edit	System Language Setting	✓ (Only Self)	✓ (Only Self)	✓ (Only Self)
	Edit	Server Time Zone	✓	✓	
	Edit	Account Registration			
	Edit	2FA Authentication	✓	✓	
	Edit	LDAP	✓	✓	
	Edit	Device X.509 Certification	✓	✓	
	Edit	Remote Storage (SMB/CIFS)	✓	✓	
	Edit	Data Export	✓	✓	
	Edit	Webhook	✓	✓	
	Edit	Syslog	✓	✓	
	Edit	App Store Setting Offered by &	✓	✓	

		Contact Support			
Device Map	CURD	Map Location	✓	✓	✓
	CURD	Map Device	✓	✓ (Only Self-Managed & Device Admin Devices)	✓ (Only Self)
Overview	CURD	Schedule	✓ (Only Self)	✓ (Only Self)	✓ (Only Self)
	View	View Event	✓ (All)	✓ (Only Self & Device Admin)	✓ (Only Self)
Rule	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

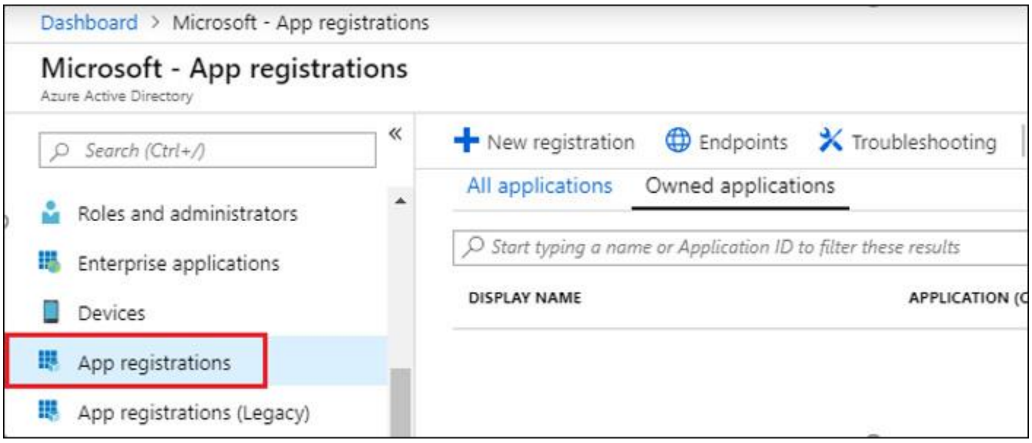
7.2.1 Method 1 – Create & Get Information on Azure Portal

Step 1: Create Your Application

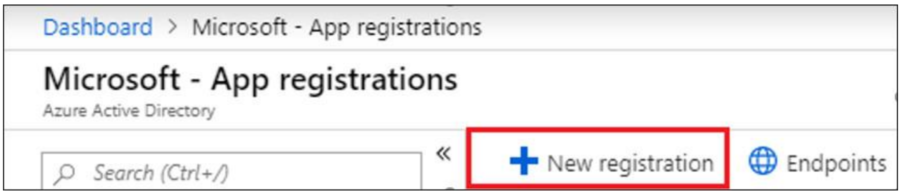
1.1. Log into your Azure Portal

1.2. Select [**Azure Active Directory**]

1.3. Select **[App registrations**]



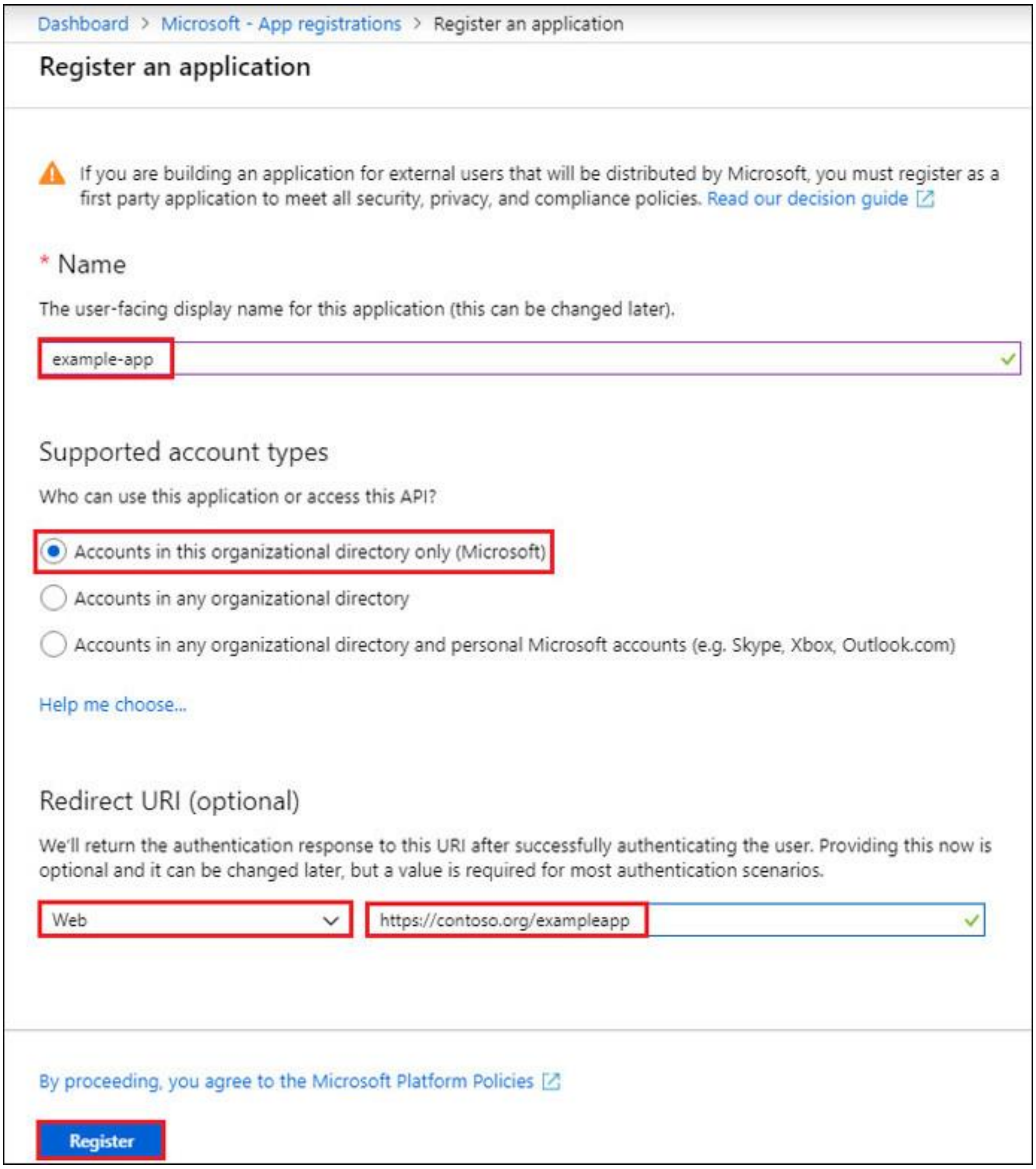
1.4. Add [**New Registration**]


Dashboard > Microsoft - App registrations
Microsoft - App registrations
Azure Active Directory
Search (Ctrl+/)
New registration
Endpoints

1.5. Setup your **Application Name** then click [**Register**].

- Enter your Application display name in **Name** filed.
- 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

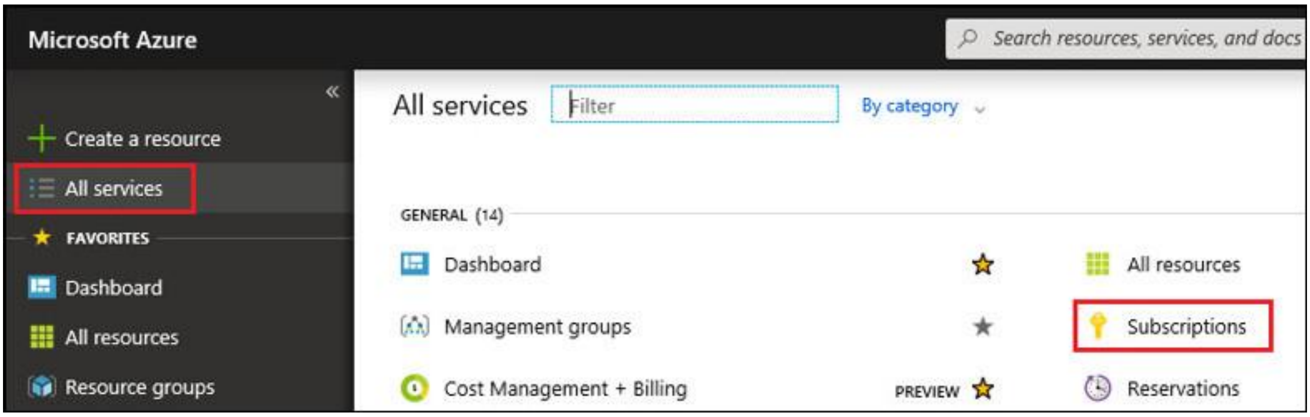
https://contoso.org/exampleapp

By proceeding, you agree to the Microsoft Platform Policies

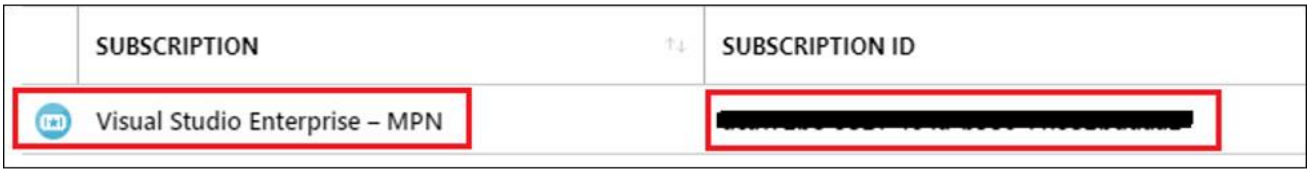
Step 2: Get Subscription ID

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.



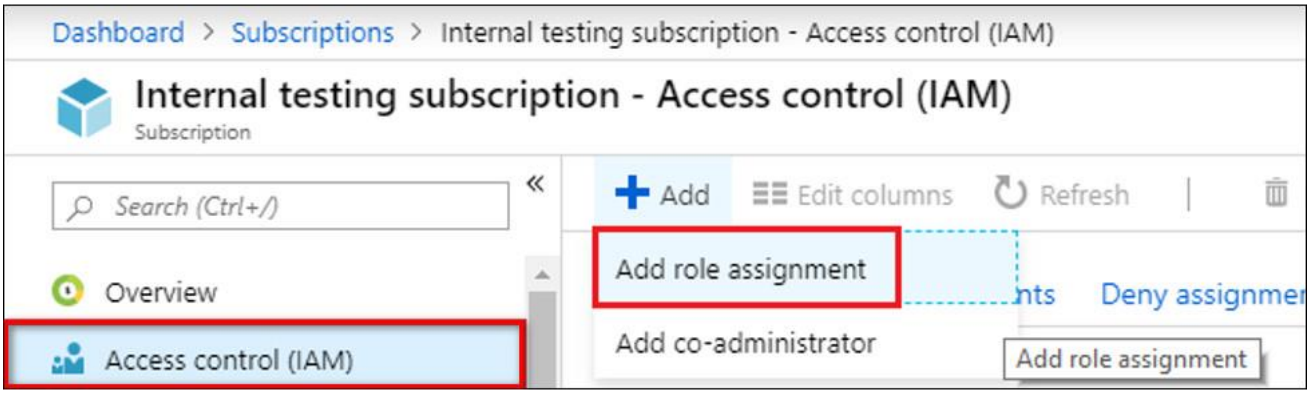
2.2. Find the Subscription you would like to assign to the Application created in the Step 1. Copy the **Subscription ID**, as this is one of the Azure data fields required on the WISE-PaaS Marketplace later. (**Ref: Marketplace field #A)**



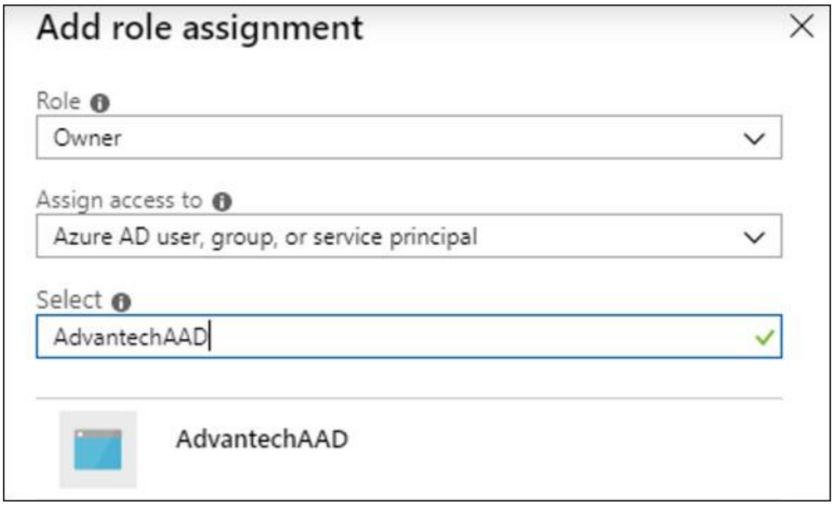
SUBSCRIPTION	SUBSCRIPTION ID
Visual Studio Enterprise – MPN	[redacted]

! 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

Role: Owner

Assign access to: Azure AD user, group, or service principal

Select: AdvantechAAD

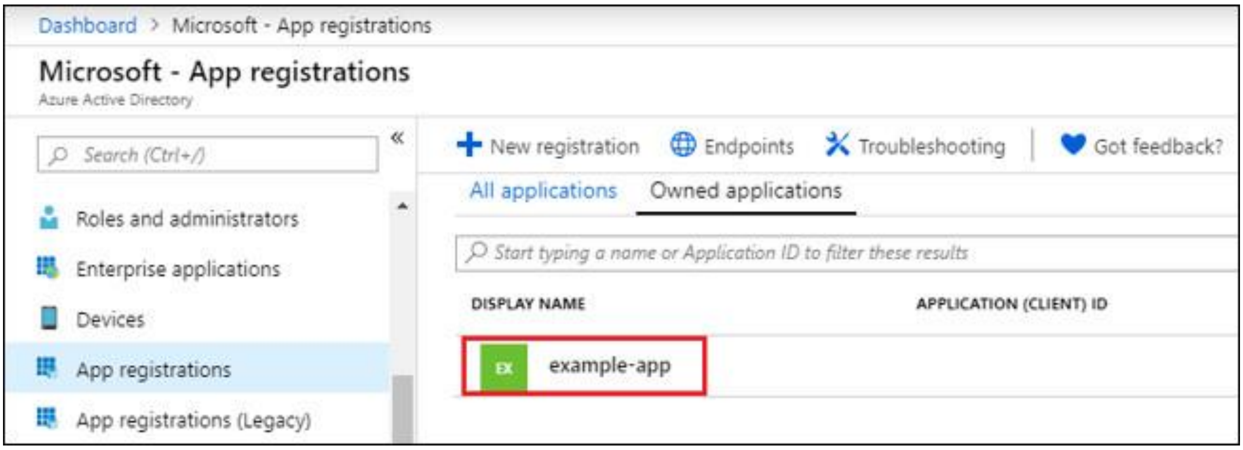
AdvantechAAD

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

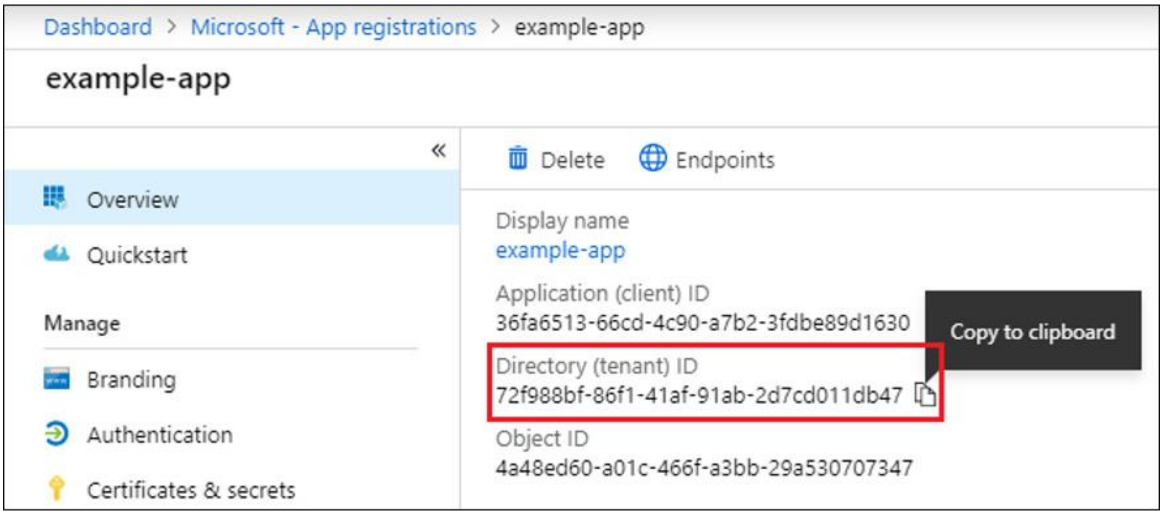


Microsoft - App registrations

Azure Active Directory

DISPLAY NAME	APPLICATION (CLIENT) ID
EX 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)**



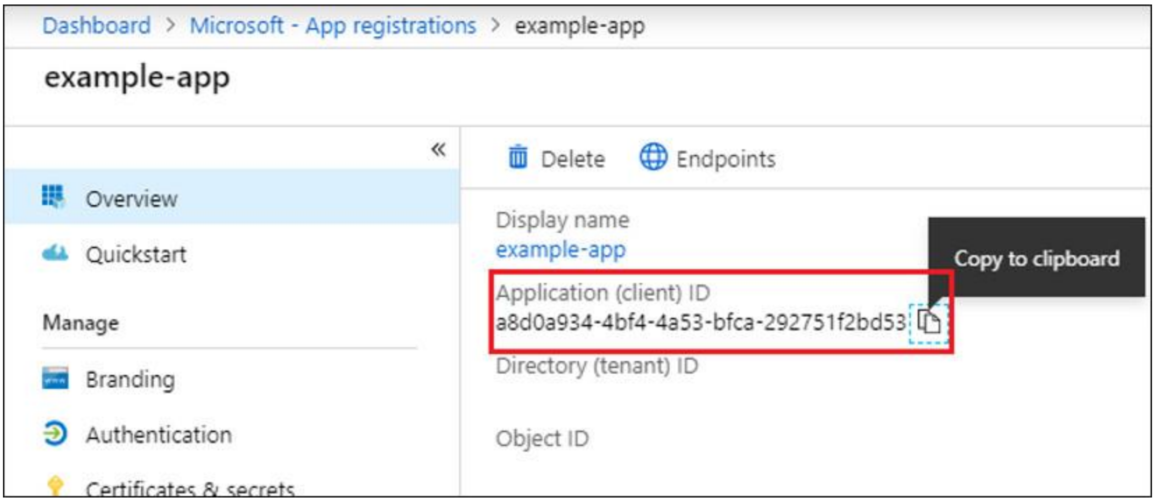
Display name
example-app

Application (client) ID
36fa6513-66cd-4c90-a7b2-3fdbe89d1630

Directory (tenant) ID
72f988bf-86f1-41af-91ab-2d7cd011db47

Object ID
4a48ed60-a01c-466f-a3bb-29a530707347

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)**



Display name
example-app

Application (client) ID
a8d0a934-4bf4-4a53-bfca-292751f2bd53

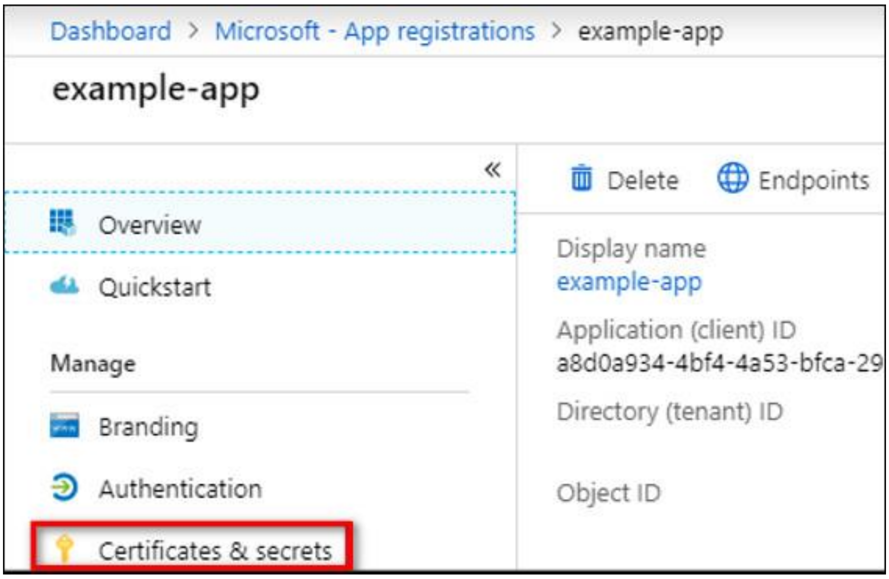
Directory (tenant) ID

Object ID

Step 4: Add & Get Client Secret

4.1. Select [**Certificates & secrets**]

4.2. Select **Client secrets** then **New client secret**



Dashboard > Microsoft - App registrations > example-app

example-app

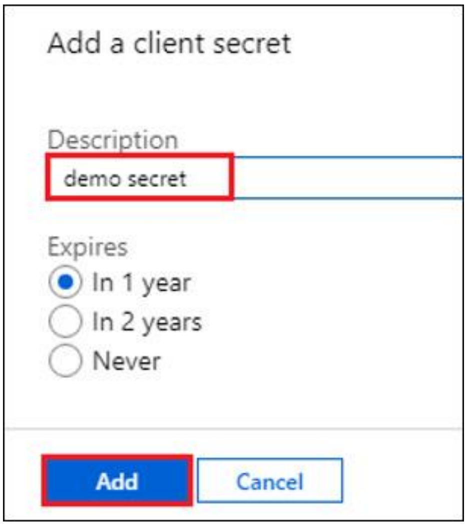
Display name
example-app

Application (client) ID
a8d0a934-4bf4-4a53-bfca-29

Directory (tenant) ID

Object ID

4.3. Provide a description for the new client secret, set up the expiration period. Then Click [**Add**]

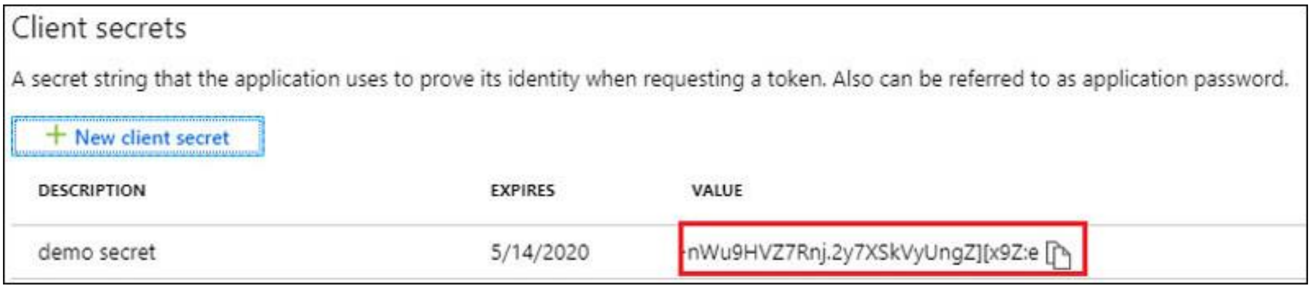


Add a client secret

Description: demo secret

Expires
● In 1 year
○ In 2 years
○ Never

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.

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

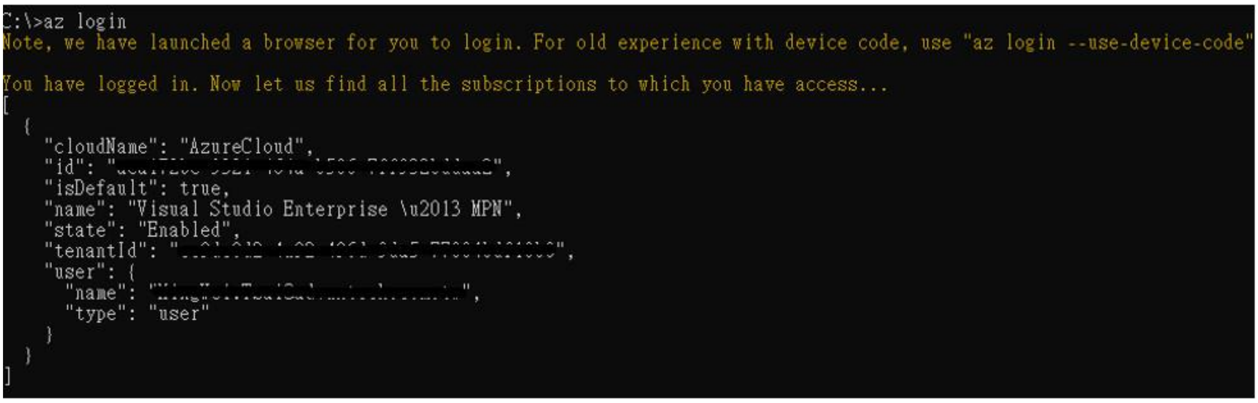
Step 2: Sign into the Azure Account

```
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

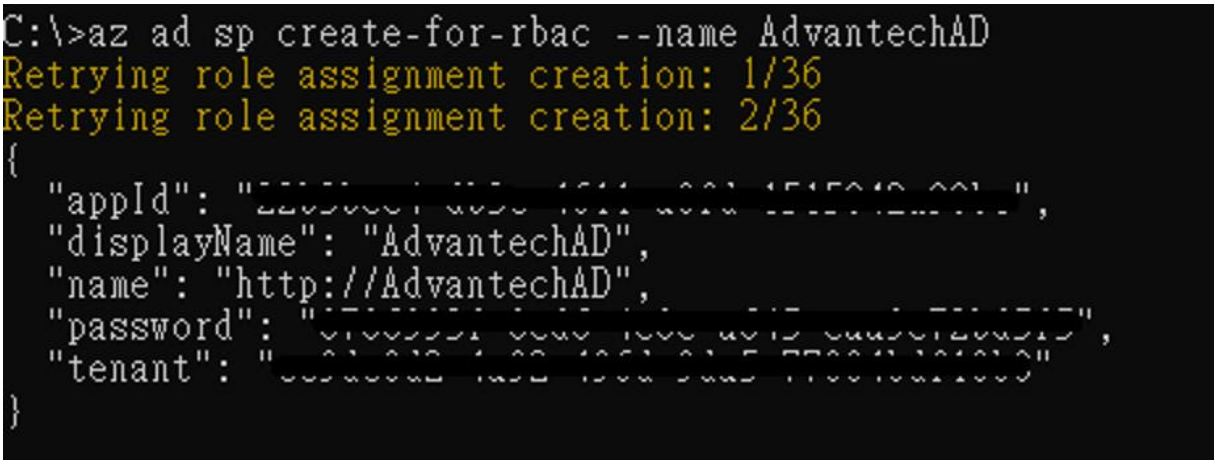
```
C:\>az account show --query id
```



```
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": "[redacted]",
    "isDefault": true,
    "name": "Visual Studio Enterprise \u2013 MPN",
    "state": "Enabled",
    "tenantId": "[redacted]",
    "user": {
      "name": "[redacted]",
      "type": "user"
    }
  }
]
```

Step 4: Create service principal and get Application ID, Tenant ID and Client Secret

```
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": "[redacted]",
  "displayName": "AdvantechAD",
  "name": "http://AdvantechAD",
  "password": "[redacted]",
  "tenant": "[redacted]"
}
```

Reference: Create an Azure service principal with Azure CLI >