InControl 2 Appliance Setup Guide

for Virtual and Hardware Appliance 2.7.3.6

(Last updated: 2019-01)

Contents

1. Virtual Appliance
   - 1.1 Introduction
   - 1.2 Hardware Requirements
   - 1.3 Installation on VMware ESXi 6.0 and ESXi 5.5
     - Networking
     - Creating InControl and DB VMs
     - Uploading and adding data storage to the VMs
   - 1.4 Installation on Hyper-V Windows 2012 R2
     - Networking
     - Creating InControl and DB VMs
     - Uploading and Adding data storage to the VMs
   - 1.5 Powering up VMs
   - 1.6 Accessing the Control Panel
   - 1.7 Software License
2. Hardware Appliance
   - 2.1 Accessing Control Panel
   - 2.2 License Key
3. Input E-mail Delivery Settings
4. Map Settings
   - Input Google Maps API Key
   - OpenStreetMap Settings
5. Input FTP/SFTP Archive Server Settings
6. Facebook App Settings (for Captive Portal)
7. Setting up Devices to Report to InControl
   - Method 1: By Configuring Devices Individually - for Internet Isolated Environments
   - Method 2: By Configuring or Redirecting Devices from the Peplink InControl - for Internet-Accessible Environments

8. Logging Into InControl Appliance Web Site

9. Importing Devices

10. Creating an Organization, Group, and Adding Devices

11. API Access

12. Settings on Your Firewall
    12.1 For Hardware Appliance's Management Port

13. Upgrading InControl Virtual Appliance
    13.1 For VMware ESXi
    13.2 For Microsoft Hyper-V

14. Upgrading InControl Hardware Appliance

15. Facebook App ID Creation Procedure

16. Release Notes
    Release notes for 2.7.3.6
    Release notes for 2.7.3.5
    Release notes for 2.7.3.2
    Release notes for 2.7.3.1
    Release notes for 2.7.3
    Release notes for 2.7.1
    Release notes for 2.6.2
    Release notes for 2.6.1 (no appliance image released)
    Release notes for 2.6.0 (no appliance image released)
    Release notes for 2.5.2

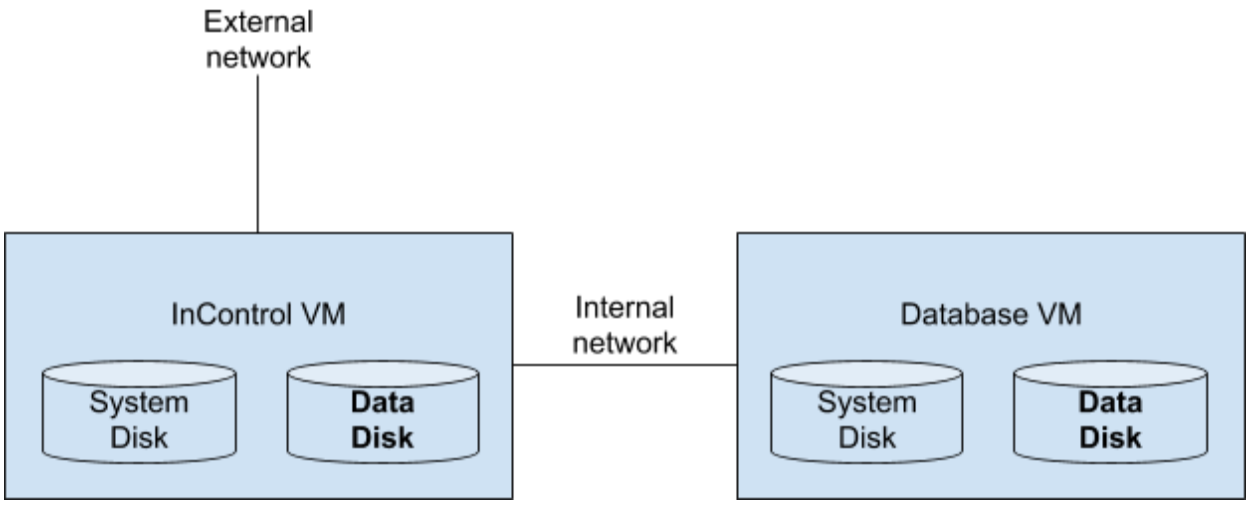
1. Virtual Appliance

1.1 Introduction

InControl 2 Virtual Appliance runs on top of virtualization server. VMware ESXi and Microsoft Hyper-V are supported currently.

It consists of two VMs (Virtual Machines). They are InControl VM and DB (database) VM.

The setup requires two Virtual Switches in the virtualization server. One is for internal communication between the InControl VM and the DB VM. Another one is for web access and device communication from external.



1.2 Hardware Requirements

InControl and database virtual machines (VM):

- CPU: Dual-core minimum. Quad-core preferred for more than 100 devices.
- Memory :
  - InControl VM: 8 GB for up to 100 online devices
  - Database VM: 4 GB for up to 100 online devices
- Storage:
  - InControl VM's system disk: 8 GB
  - Database VM's system disk: 2 GB
  - InControl VM's data disk: 20 GB
  - Database VM's data disk:

- 100 GB for up to 100 online devices
- 500 GB for 1000 to 2000 online devices

Note: the number of online devices can be managed depends on their usage and functionality. E.g. whether GPS is enabled, number of client connections per hour, etc.

External archive server:

- An FTP or SFTP server: as much storage as possible. Please see chapter 5. Input FTP/SFTP Archive Server Settings for details.

1.3 Installation on VMware ESXi 6.0 and ESXi 5.5

Peplink distributes two **tgz** files: `InControl-System-x.y.z.tgz` and `DB-System-x.y.z-yyyymmdd.tgz`. They contain bootable systems of the InControl virtual appliance and a MySQL database respectively. You will use them to start one InControl Appliance and one MySQL DB VM.

Networking

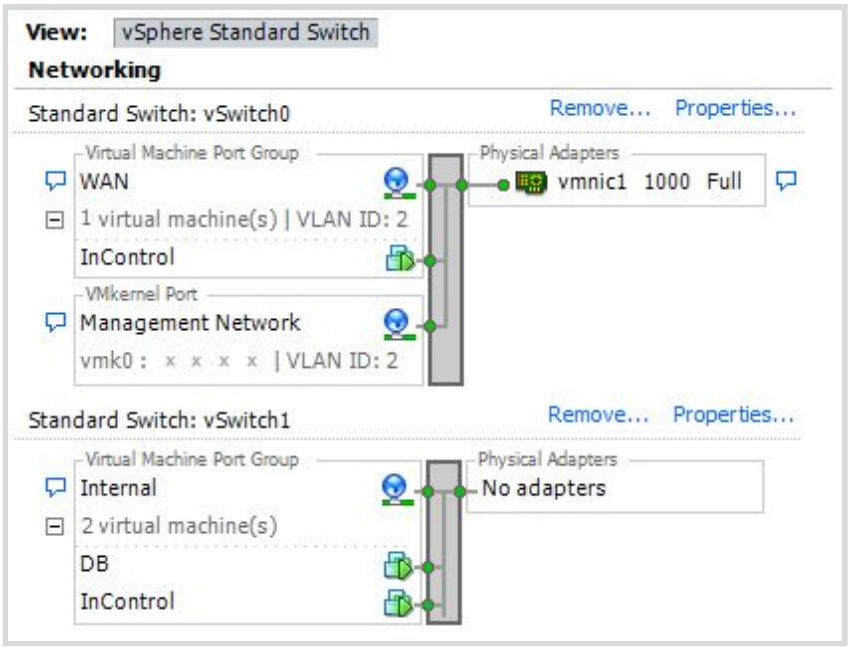
Please create two vSwitches in ESXi host > Configuration > Networking.

The first one is called "`WAN`" which is for connecting to the outside world and will need a physical network adapter attached. The first network adapter of the InControl VM shall be assigned to this network.

The second one is called "`Internal`". It is for inter-InControl-DB communication, no physical adapter is needed. The second network adapter of the InControl VM and the single network adapter on the Database VM shall be assigned to this network.

Note 1: A DHCP server is required on the WAN segment during the initial installation. The InControl VM will acquire an IP for its WAN from the DHCP server. You may configure the system with a static IP when you have access to the control panel.

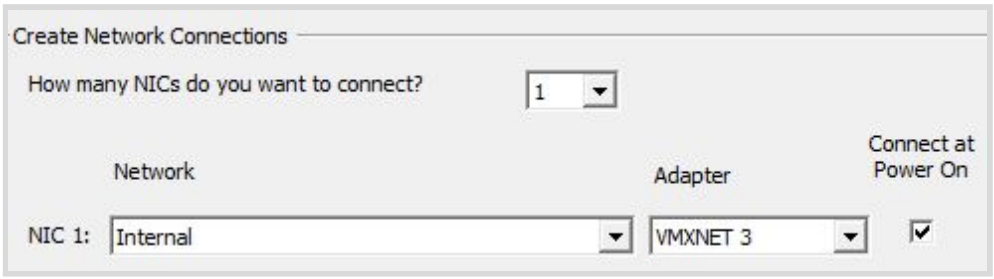
Note 2: The WAN interface cannot be on the subnets 192.168.1.0/24 because it is reserved to the “Internal” network.


View:
vSphere Standard Switch
Networking
Standard Switch: vSwitch0
Remove...
Properties...
Virtual Machine Port Group
WAN
1 virtual machine(s) | VLAN ID: 2
InControl
VMkernel Port
Management Network
vmk0 : x x x x | VLAN ID: 2
Physical Adapters
vmnic1 1000 Full
Standard Switch: vSwitch1
Remove...
Properties...
Virtual Machine Port Group
Internal
2 virtual machine(s)
DB
InControl
Physical Adapters
No adapters

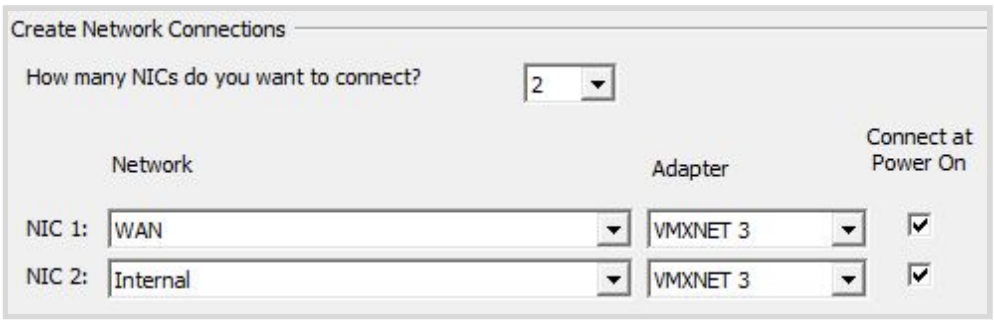
Creating InControl and DB VMs

In the vSphere Client, create 2 new Virtual Machines called "`DB`" and "`InControl`" for Ubuntu Linux (64 bit) guest operating systems. For the DB, you will need only one Network Connection on the `Internal` network. For InControl, you will need the `WAN` network on NIC1 and the `Internal` network on NIC2. (For the disk, just choose anything as we will remove it anyway.)

DB VM:



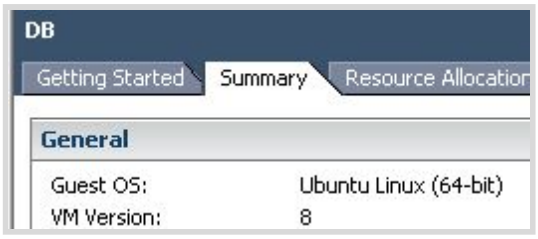
InControl VM:

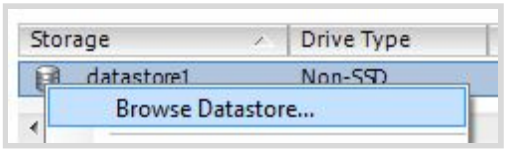


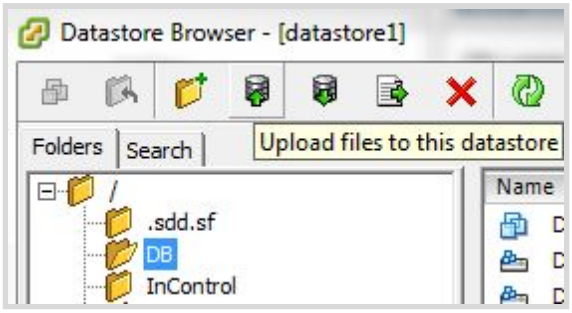
Uploading and adding data storage to the VMs

Extract the .tgz files on a PC (do not extract at the command line of the ESXi server. Its "tar" command could not extract the file correctly.)

Go to the VM's Summary tab and right-click on your datastore to browse it. There you can upload the `DB-System-flat.vmdk` + `DB-System.vmdk` to the DB directory, and the `InControl-System-flat.vmdk` + `InControl-System.vmdk` to the InControl directory. You should see this as one file in the Datastore Browser. If you see two files, you will need to open the small vmdk file with a text editor and fix the name of the flat file.

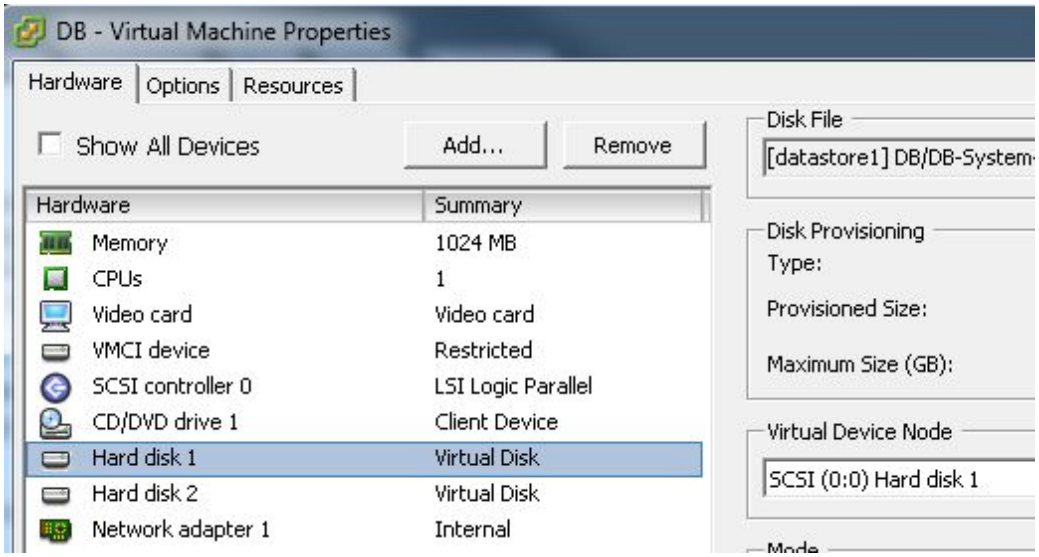






Alternatively, you can activate the ssh function, and scp the 2 files to the corresponding directories (`/vmfs/volumes/datastore1/DB` & `/vmfs/volumes/datastore1/InControl`).

Now you can 'Edit Settings' of each VM. Remove the existing hard disk. For the InControl VM, add the `InControl-System.vmdk` on `SCSI (0:0)` and create an empty 20 GB disk on `SCSI (0:1)`. For DB, follow the same but add 20GB of disk storage for general testing purpose or add 100 GB / 500 GB for up to 100 devices / 2000 devices that you plan to manage with the system. (See Introduction - Minimum Hardware Requirements)


DB - Virtual Machine Properties
Hardware
Options
Resources
Show All Devices
Add...
Remove
Hardware
Summary
Memory
1024 MB
CPUs
1
Video card
Video card
VMCI device
Restricted
SCSI controller 0
LSI Logic Parallel
CD/DVD drive 1
Client Device
Hard disk 1
Virtual Disk
Hard disk 2
Virtual Disk
Network adapter 1
Internal
Disk File
[datastore1] DB/DB-System
Disk Provisioning
Type:
Provisioned Size:
Maximum Size (GB):
Virtual Device Node
SCSI (0:0) Hard disk 1
Mode

1.4 Installation on Hyper-V Windows 2012 R2

Peplink distributes two VMDK files: `InControl-System.vhd` and `DB-System.vhd`. They are bootable systems of the InControl virtual appliance and a MySQL database respectively. You will use them to start one InControl and one MySQL DB VM.

Networking

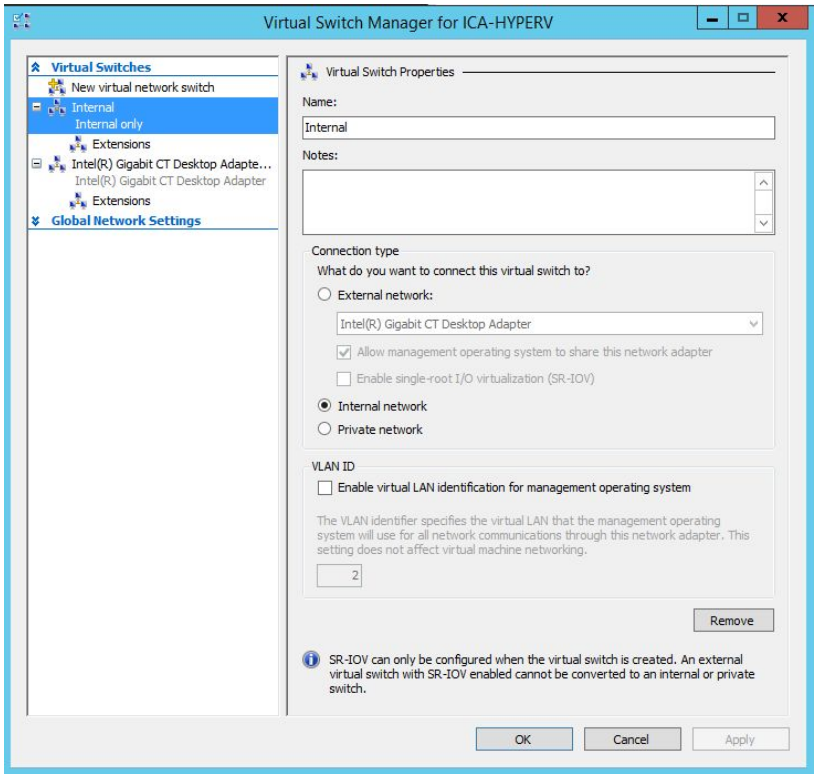
First of all, please create two networks on the Hyper-V host.

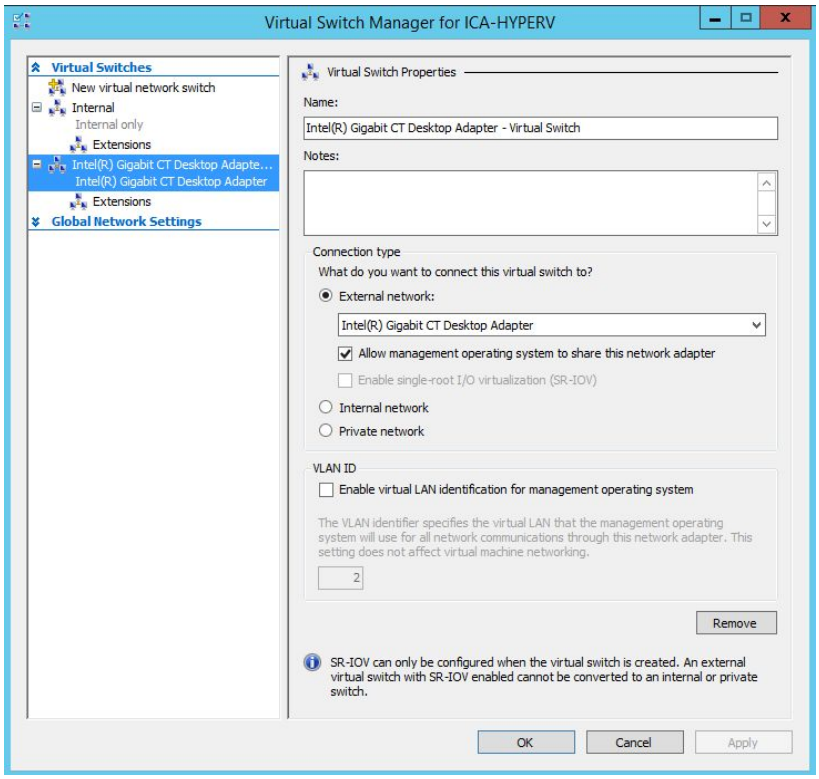
The first one is called "`WAN`" which is for connecting to the outside world and will need a physical network adapter attached. The first network adapter of the InControl VM shall be assigned to this network.

The second one is called "`Internal`". It is for inter-InControl-DB communication, no physical adapter is needed. The second network adapter of the InControl VM and the single network adapter on the Database VM shall be assigned to this network.

Note 1: A DHCP server is required on the WAN segment during the initial installation. The InControl VM will acquire an IP for its WAN from the DHCP server. You may configure the system with a static IP when you have access to the control panel.

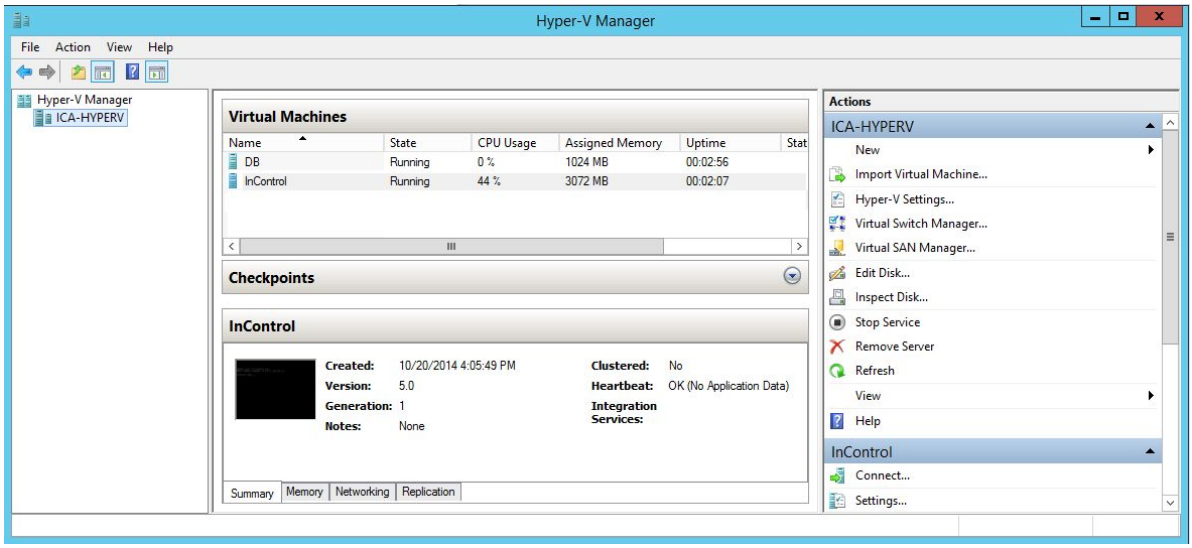
Note 2: The WAN interface cannot be on the subnets 192.168.1.0/24 because it is reserved to the “Internal” network.


Virtual Switch Manager for ICA-HYPERV
Virtual Switches
New virtual network switch
Internal
Internal only
Extensions
Intel(R) Gigabit CT Desktop Adapte...
Intel(R) Gigabit CT Desktop Adapter
Extensions
Global Network Settings
Virtual Switch Properties
Name:
Internal
Notes:
Connection type
What do you want to connect this virtual switch to?
External network:
Intel(R) Gigabit CT Desktop Adapter
Allow management operating system to share this network adapter
Enable single-root I/O virtualization (SR-IOV)
Internal network
Private network
VLAN ID
Enable virtual LAN identification for management operating system
The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.
2
Remove
SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.
OK
Cancel
Apply

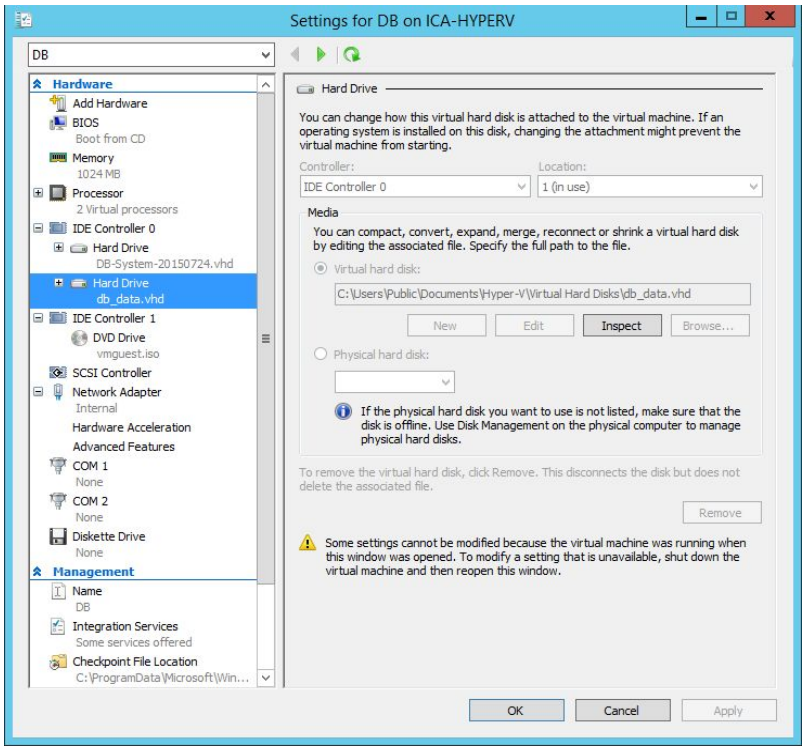

Virtual Switch Manager for ICA-HYPERV
Virtual Switches
New virtual network switch
Internal
Internal only
Extensions
Intel(R) Gigabit CT Desktop Adapte...
Intel(R) Gigabit CT Desktop Adapter
Extensions
Global Network Settings
Virtual Switch Properties
Name:
Intel(R) Gigabit CT Desktop Adapter - Virtual Switch
Notes:
Connection type
What do you want to connect this virtual switch to?
External network:
Intel(R) Gigabit CT Desktop Adapter
Allow management operating system to share this network adapter
Enable single-root I/O virtualization (SR-IOV)
Internal network
Private network
VLAN ID
Enable virtual LAN identification for management operating system
The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.
2
Remove
SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.
OK
Cancel
Apply

Creating InControl and DB VMs

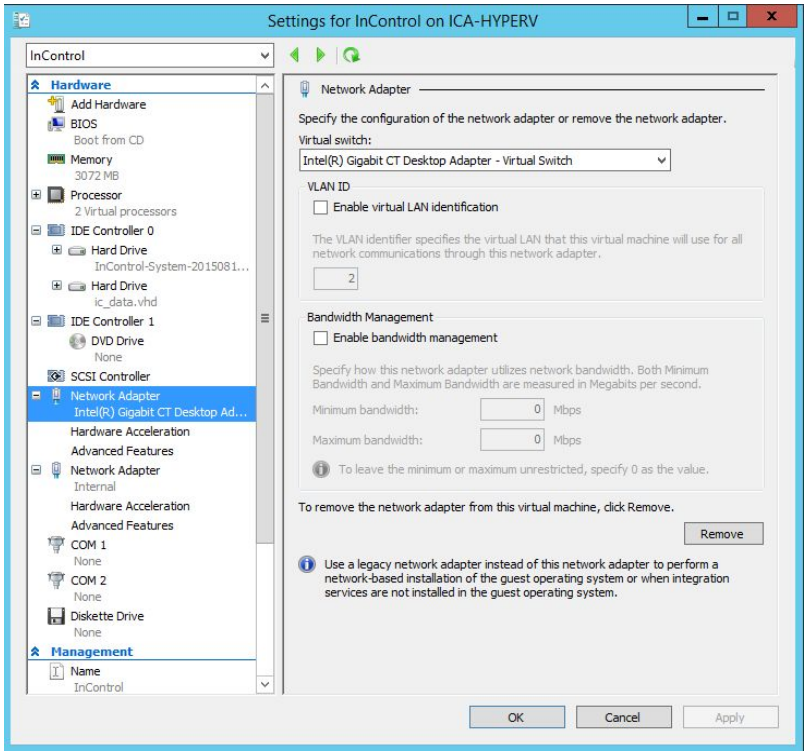
In the Hyper-V Manager, create 2 new Virtual Machines called `DB` and `InControl` for Ubuntu Linux (64 bit) guest operating systems. Our test was on first generation VMs. For the DB VM, you need only one network connection on the Internal network. For the InControl VM, you'll need the WAN network and the Internal network.



DB VM:



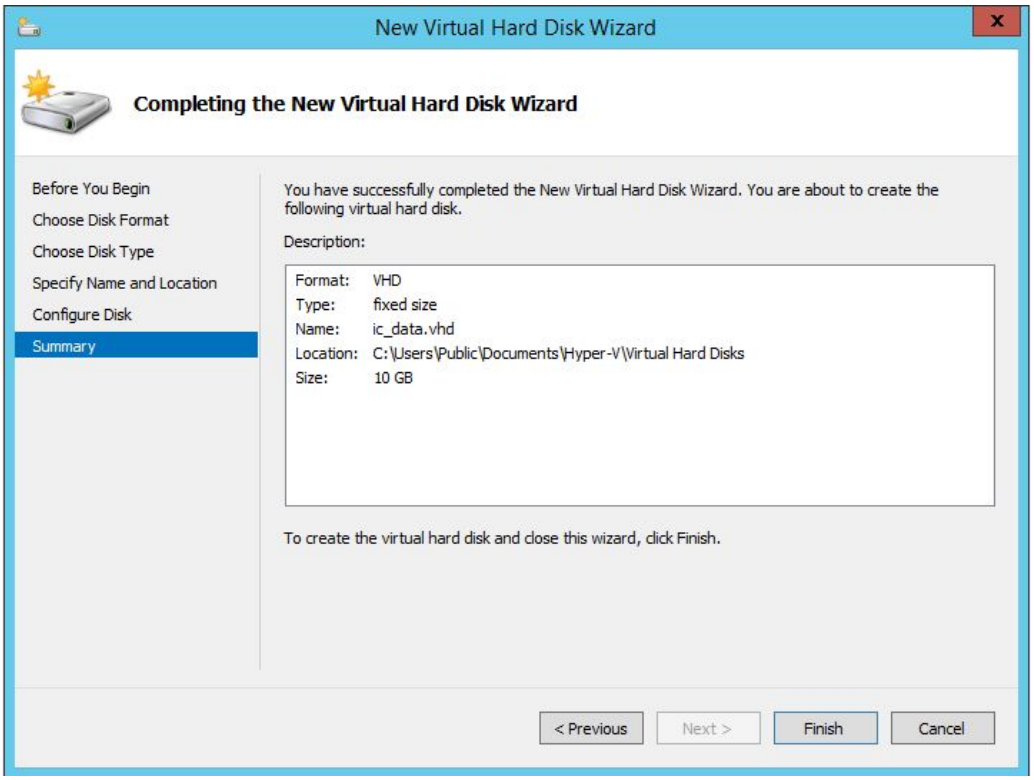
InControl VM:



Uploading and Adding data storage to the VMs

For the InControl VM, add the InControl-System.vhd on IDE (0:0) and create an empty 10GB disk on IDE (0:1). For DB, follow the same but add 20 GB of disk storage for general testing purpose or add 100 GB / 500 GB for up to 100 devices / 2000 devices that you plan to manage with the system. (See Introduction - Minimum Hardware Requirements)

Choose VHD - fixed size data disks.



1.5 Powering up VMs

Power up the DB VM first. After one minute, power up the InControl VM. They will initialize their attached data disk automatically. The InControl VM takes about 5-10 minutes to start up for the first time, 2 minutes for subsequent boot ups.

1.6 Accessing the Control Panel

After the system is fully started up which typically takes about two minutes, you can access the Control Panel page on the InControl VM via your browser to configure the InControl virtual appliance.

Check the InControl IP address from the VM console. You can access the control panel page at `https://{incontrol.ip.address}:4443/`. The default username and password are both "**admin**".

System Settings	
Product	InControl Appliance (Virtual)
Appliance Version	2.7.3
Software Version	N/A
Serial Number	N/A
Domain	my.domain
Server Name	incontrol.my.domain *(Must be a subdomain of "Domain")*
Company Name	My Company
Service Name	My Company InControl
System Admin E-mail Address	noreply@my.domain
Tech Support E-mail Address	noreply@my.domain
Notification E-mail Sender Name	My Company InControl
Notification Sender E-mail Address	noreply@peplink.com

You may change the domain name on the control panel. By default, the domain name is "`my.domain`".

1.7 Software License

A software license is required for the InControl system to operate. To acquire for a paid or evaluation license, please email your Server Name shown on the Control Panel and your order number (if any) to ica@peplink.com. Peplink will send you back a license key. Input it into the License Key field to activate. The device's serial number will be assigned at the same time.

License		
Server Name	incontrol.my.domain	
License Key		Submit
Max. Allowed Number of Active Devices	50	
Expiry Date	n/a	

2. Hardware Appliance

2.1 Accessing Control Panel

After the system is fully started up which typically takes about two minutes, you can access the Control Panel page from a browser on a PC to configure the InControl appliance.

You can visit the control panel over its **Management port** or **WAN port** from a PC. The unit's management port's IP address is 192.168.5.10 by default. The WAN port IP address is acquired from a DHCP server by default. You could find its IP address from the LCD panel. (Note that the WAN subnet must not be 192.168.1.0/24, 192.168.5.0/24 and 192.168.30.0/24.)

On your PC, assign it with a static IP address which is accessible to the port's IP address. Connect it to the port with an Ethernet cable. For management port, you can access the control panel page at http://192.168.5.10:8000/. For WAN port, the page is at `https://{wan.ip.address}:4443/`. The default username is "**admin**" and the password is "**admin**"

System Settings	
Product	InControl Appliance (Hardware)
Appliance Version	2.7.3
Software Version	N/A
Serial Number	N/A
Domain	my.domain
Server Name	incontrol.my.domain *(Must be a subdomain of "Domain")*
Company Name	My Company
Service Name	My Company InControl
System Admin E-mail Address	noreply@peplink.com
Tech Support E-mail Address	support@peplink.com
Notification E-mail Sender Name	My Company InControl
Notification Sender E-mail Address	noreply@peplink.com

You may change the domain name on the control panel. By default, the domain name is "`my.domain`" for testing your setup.

2.2 License Key

A license has been pre-installed for managing a certain amount of devices. After you have purchased a new license, Peplink will send you back a license key. You can input it into the License Key field and activate the license.

License		
Server Name	incontrol.my.domain	
License Key		Submit
Max. Allowed Number of Active Devices	100	

3. Input E-mail Delivery Settings

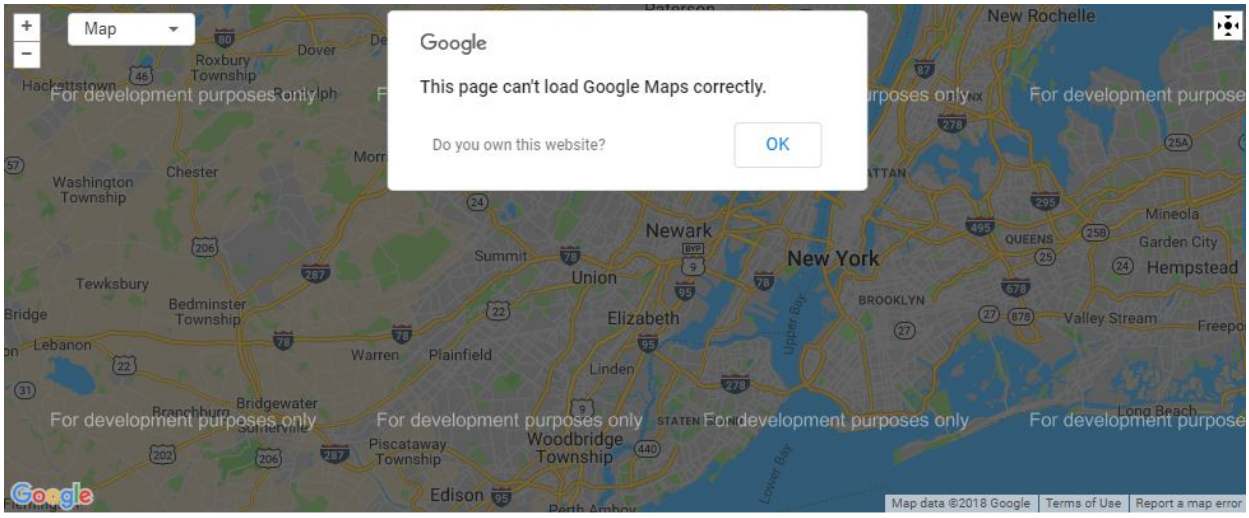
In order to create new accounts, the system has to be able to send confirmation emails to do account confirmation. So please configure the SMTP server settings, as well as the "Notification Email Sender Name" and "Notification Sender Email Address" in the System Settings above accordingly.

E-mail Delivery Settings		
SMTP Server	smtp.my.domain	
SMTP Port	587	
SMTP Username	smtp-user	
SMTP Password	••••••••••••	
SMTP Authentication	Login ▾	
SMTP HELO Domain	mydomain.com	
Testing E-mail Address		Test
Testing E-mail Delivery Status	*Note: Save E-mail Delivery Settings before testing.*	

4. Map Settings

Input Google Maps API Key

Since InControl Appliance 2.7.3, to conform to the latest Google Maps API policy, no API key comes with the InControl Appliance. Customers are required to apply one from Google, add billing information to it and input the API key to InControl Appliance' control panel page. If a key is not provided, a screen like this may be displayed:



Please follow the instructions showing on the Google Maps API Key Settings panel to apply for an API key.

Maps Settings	
Google Maps API Key	
	Note: To register for a Google Maps API Key: - Sign in Google Cloud Platform, create a new project named "InControl Appliance". - Navigate to *APIs & Services > Dashboard*. - Click the link *ENABLE APIS AND SERVICES* at the top of the page. - Choose and enable both *Maps JavaScript API* and *Geocoding API*. - Navigate to *APIs & Services > Credentials > Create credentials*. Choose *API key* for the *Application type*. - Finally, add billing information to the project by following the instructions on this site.
OpenStreetMap Tile Server URL Prefix	https://osm.peplink.com/tiles /{z}/{x}/{y}.png
OpenStreetMap Nominatim Server URL	https://osm.peplink.com/geocode

If you do not want to use Google Maps, you may choose to display maps with the OpenStreetMap in Organization Settings.

OpenStreetMap Settings

When you choose to use OpenStreetMap, the mapping images and geocoding requests are actually served by Peplink's OpenStreetMap servers by default. You could change to use your own servers instead by inputting the server URLs to the *OpenStreetMap Tile Server URL Prefix* and *Nominatim Server URL* fields.

5. Input FTP/SFTP Archive Server Settings

As a relational database is not good at storing bulky data, so historical event log events, GPS locations, and cellular signal data are only kept in the MySQL database for 7 days. Before they are removed from the database, the system will archive the data to the archive server daily if an FTP or SFTP server is configured.

When the data is requested over the web or API, the system will automatically choose to retrieve the data from the database or the archive server and return to the user or API client. So you are encouraged to set up an FTP/SFTP archive server for storing those historical data.

Below are data retention periods of various types of data:

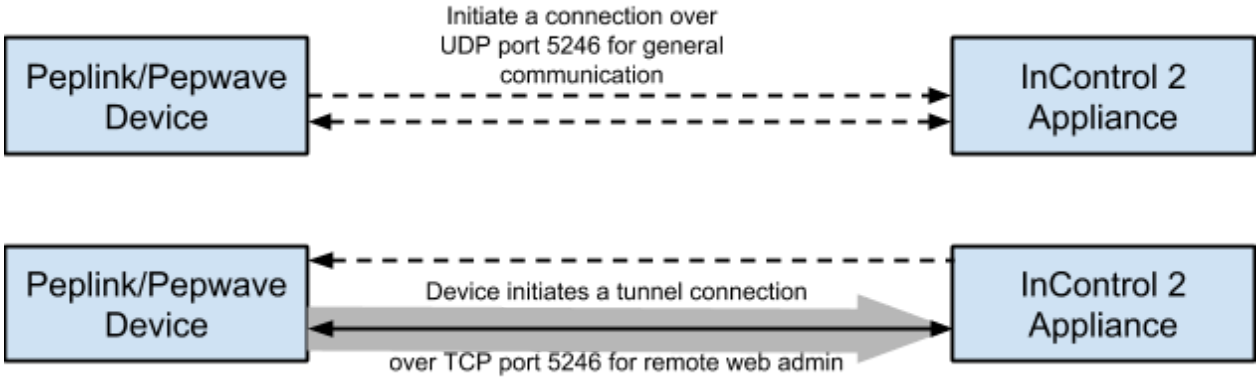
Data	**Retention period**	
	without archive server	**with archive server**
Per-minute device usage	14 days	
Hourly device usage	2 days	
Hourly client usage	1 month	
Daily client/device usage	60 days	
Monthly client/device usage	6 months	
Device online/offline history	6 months	
Social network user data	2 years	
Operation log	2 years	
Event log	30 days	1 year
GPS data	5 days	1 year
Cellular reports	5 days	6 months

6. Facebook App Settings (for Captive Portal)

Please refer to chapter 13 Facebook App ID Creation Procedure for how to acquire a Facebook app ID.

7. Setting up Devices to Report to InControl

Unlike SNMP, Peplink/Pepwave devices initiate InControl management communication with the server. The device speaks to InControl at least every 28 secs to maintain a session. With such design, devices could set up a two-way communication channel with InControl even if they are behind a NAT router. The communications are over UDP port 5246 (for general communication) and TCP port 5246 (for Remote Web Admin only).

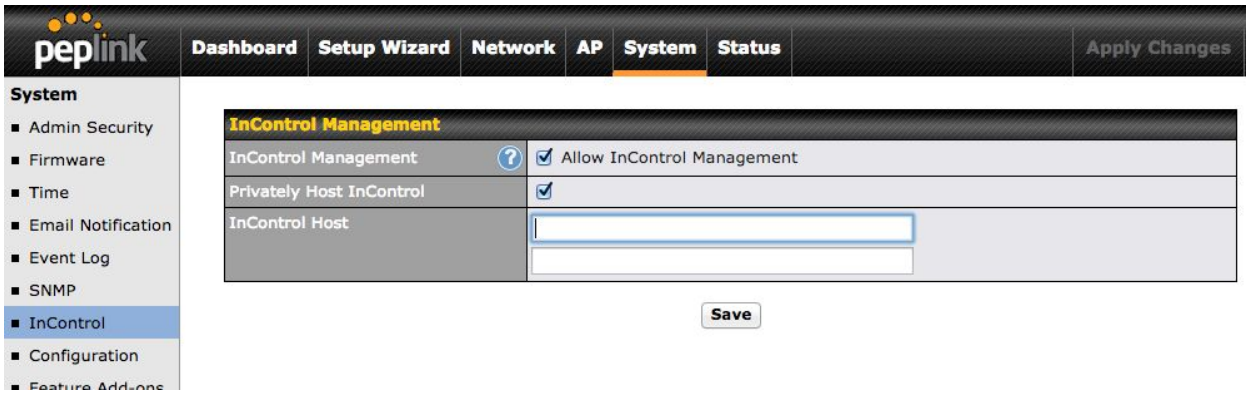


There are two ways to tell your Peplink/Pepwave devices to report to your InControl appliance instead of the Peplink InControl in the public cloud.

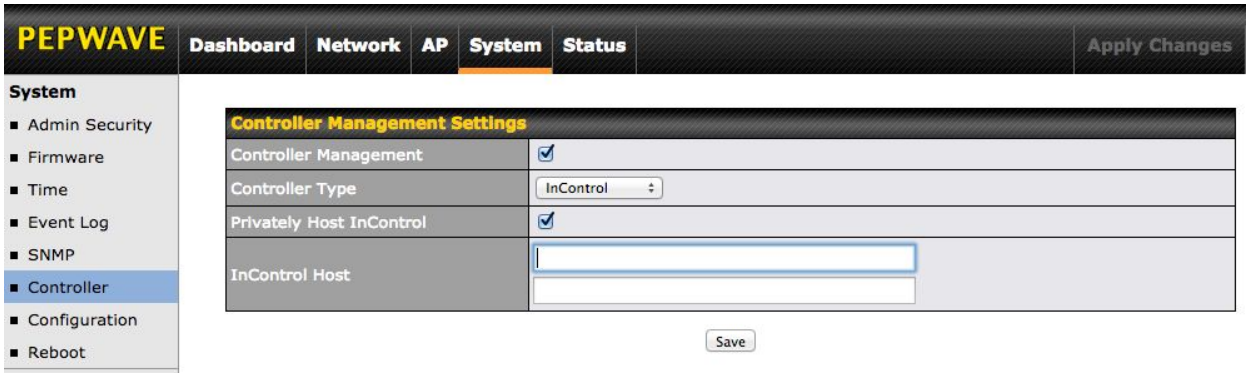
Method 1: By Configuring Devices Individually - for Internet Isolated Environments

Login to the devices' web admin and put your InControl's WAN IP address or hostname to it. If a hostname is used, please make sure a DNS record for it has been created so that devices could resolve the InControl Appliance's IP address from it.

For Peplink Balance and Pepwave MAX devices, they will have to be loaded with the firmware 6.1.2 or above. Login to the web admin and navigate to System > InControl.



For Pepwave AP's, you will need firmware 3.5.0 or above. Please navigate to System > Controller.

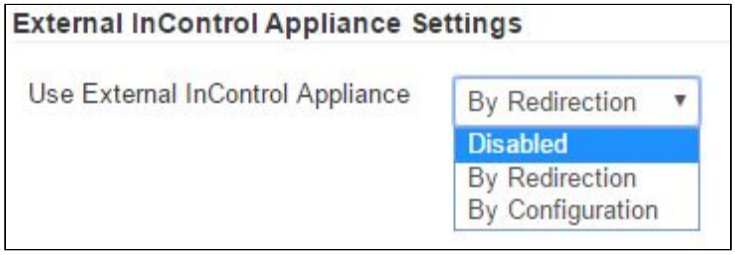


Input your InControl's IP address to the first InControl Host field.

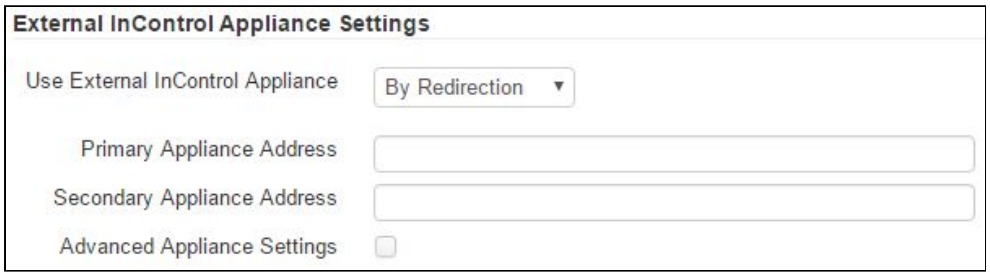
Method 2: By Configuring or Redirecting Devices from the Peplink InControl - for Internet-Accessible Environments

If your devices are accessible to both the Internet and your InControl appliance, you can follow this method. First, sign in to https://incontrol2.peplink.com/ . Create an organization and a group by following the on-screen instructions. Add your devices to the group. Then go to the Group Settings page and scroll down to the **External InControl Appliance Settings** section.

You could choose to redirect or configure your devices to connect to your InControl appliance.



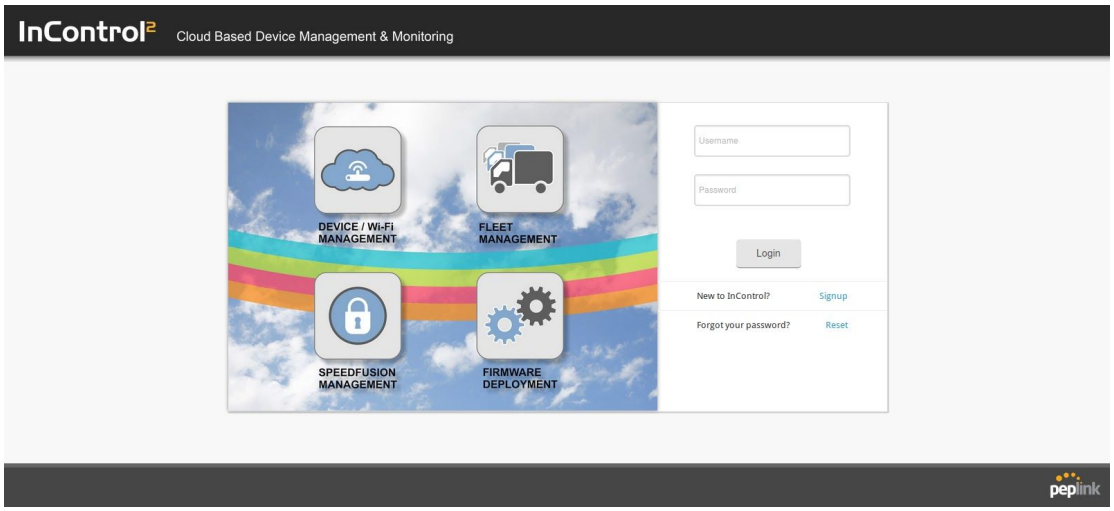
If you choose ***By Redirection***, devices will also connect to Peplink InControl first every time they start up. This option allows you to change your InControl Appliance's address easily in the future.



If you choose ***By Configuration***, your InControl Appliance address(es) will be saved persistently to your devices. After your device received the setting, they will connect to your InControl Appliance directly on startup without connecting to Peplink InControl. The appliance address will be lost if a device is reset to factory defaults.

You could configure devices to fail over to connect to Peplink InControl if they failed to connect your InControl Appliance.

8. Logging Into InControl Appliance Web Site

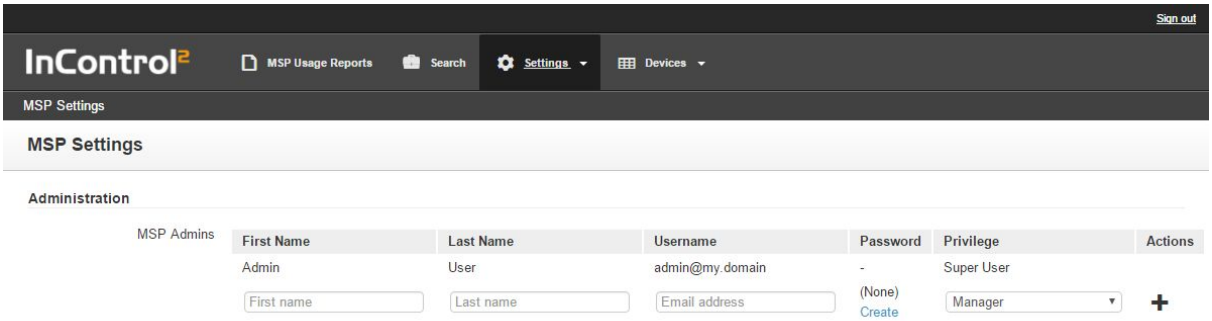


In order to access the InControl website, you must visit its hostname instead of its IP address. Your PC is required to resolve the hostname into the server IP address. You may add a local DNS record to your PC by editing its "`hosts`" file. It is "`%SystemRoot%\System32\drivers\etc\hosts`" for Windows or "`/etc/hosts`" for Mac and Linux. Let's say the InControl IP is 10.8.7.6. The hosts file shall contain:

```
10.8.7.6 incontrol.my.domain
```

Now you can access the InControl website from the PC's web browser. By default, the InControl's URL is https://incontrol.my.domain/ . The default username is **`admin@my.domain`** (note: do not replace "`my.domain`" with anything else) and the password is **`12345678`**.

After logging into the InControl, you will see an MSP (Managed Service Provider) administration page which is for managing the InControl system. To managing MSP administrator accounts, navigate to Settings > MSP Settings.

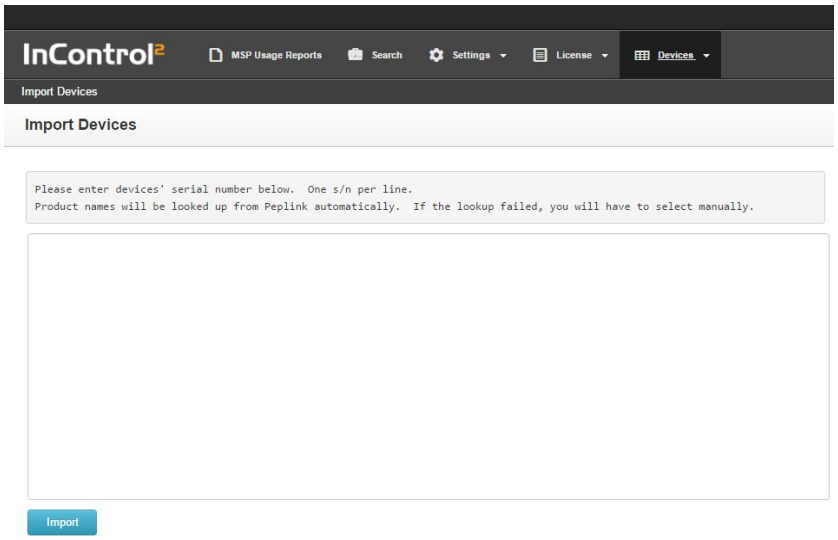


Note for InControl Hardware Appliance: the appliance's website is only accessible from the WAN port. (It is **not** accessible from the LAN or Management ports.)

9. Importing Devices

Before organization administrators can add devices into their organizations, the InControl system administrator (in InControl 2, we call the administrator as MSP Administrator) must import the devices' serial number in advance. After an MSP administrator logged into the InControl website, navigate to "Devices" > "Import Devices".

Input serial numbers in the text area, one serial number per line.



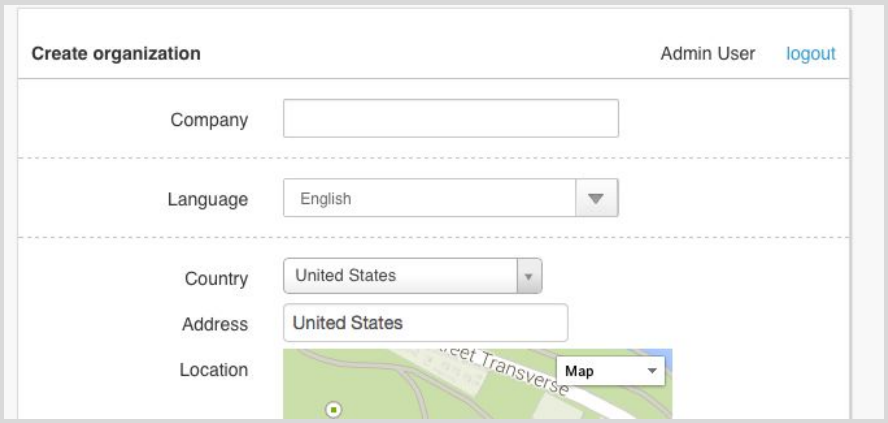
InControl Appliance will attempt to query Peplink server what products the serial numbers are. If success, the devices will be imported. If not, you will be prompted to select each device's product name.

Organization administrators (i.e. non-system administrators) are able to add the devices now.

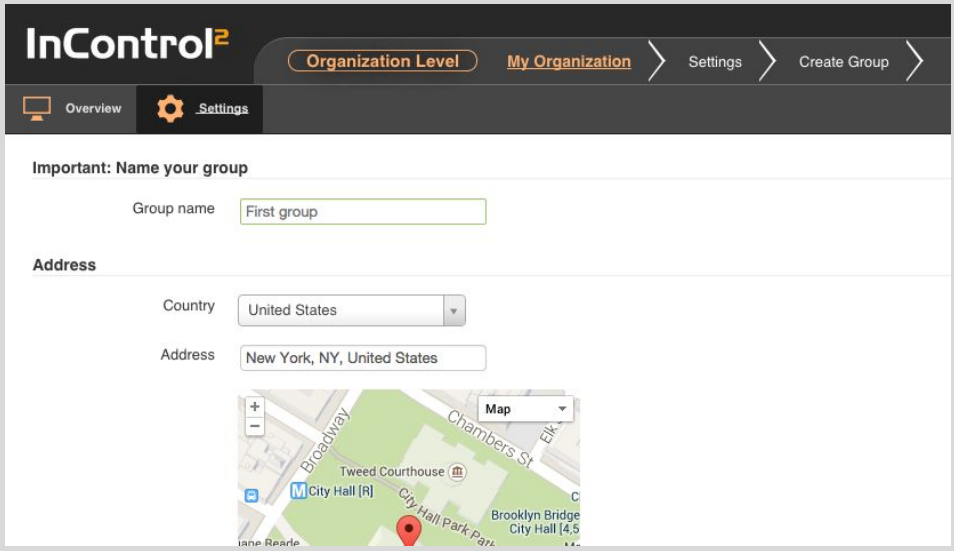
10. Creating an Organization, Group, and Adding Devices

An organization is pre-created which is called “My Organization”. You can find it on the MSP Reports page.

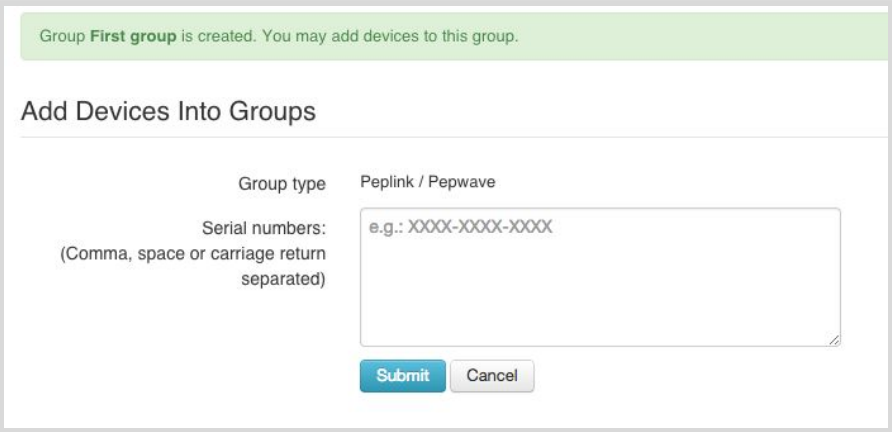
You may create more organizations by entering into an organization (e.g. “My Organization”). Then on the organization menu on the right of the screen, click “Create Organization”.



After you created an organization, you will be redirected to a group creation page. Devices are put into a group.



After creating a group, you will be redirected to “Add Devices Into Groups” page.



After the devices are added and the devices are powered up, you should see the devices become online in the InControl.

11. API Access

An API is available for software developers to programmatically retrieve the data as you see on the InControl appliance's website. You can visit `https://{incontrol.server.name}/api/restful_api` for the API documentation and testing tool.

12. Settings on Your Firewall

Please allow the following traffic to pass through if a firewall is set up in front of the appliance.

Direction	Protocol	Purpose
Inbound	UDP 5246	Device communication
	TCP 5246	Remote Web Admin
	TCP 443	Web accesses
	TCP 4443	Web accesses to control panel
	UDP 53	Dynamic DNS service and automatic SSL certificate acquisition from letsencrypt.org (optional)
Outbound	ra.peplink.com on TCP 443	Remote assistance (optional)
	download.peplink.com on TCP 443	Device firmware validation (optional)
	api.ic.peplink.com on TCP 443	Product name lookup when importing

		devices Latest device firmware updates (optional)
	push.ic.peplink.com on TCP 443	Push notifications for the InControl 2 mobile app (optional)
	*.letsencrypt.org on TCP 443	Automatic SSL certificate acquisition from letsencrypt.org (optional)
	*.peplink.com on UDP 5246 (details)	For transferring FusionHub licenses from InControl 2 (public cloud) to FusionHub units connected to the InControl Appliance (optional)
	UDP 123	Network time sync
	UDP 53	DNS resolutions

12.1 For Hardware Appliance's Management Port

Direction	Protocol	Purpose
Inbound	TCP 8000	Non-secure web accesses to control panel (optional)
Outbound	download.peplink.com on TCP 443	ICA firmware download
	UDP 53	DNS resolution for ICA firmware download

13. Upgrading InControl Virtual Appliance

13.1 For VMware ESXi

Step 1. Download the latest Virtual Appliance and Database Server image files in `.tgz` format from https://www.peplink.com/support/downloads/incontrol-appliance-image-and-installation-guide/

Step 2. Extract the `.tgz` files **on a PC** (do not extract at the command line of the ESXi server. Its "tar" command could not extract the file correctly.) Take InControl 2.7.3.6 as an example. The extracted file names and sizes are as follow:

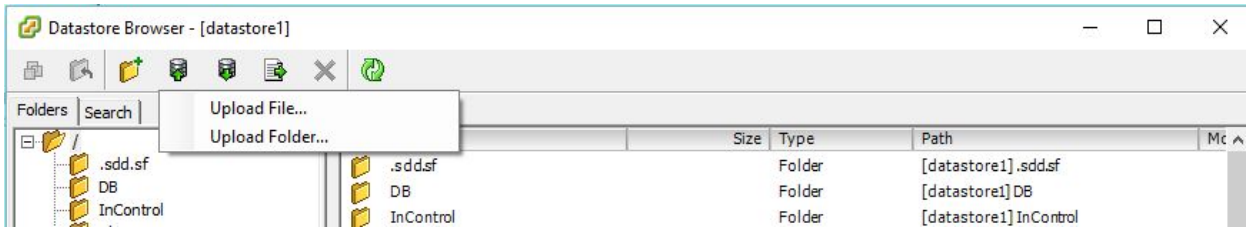
InControl-System-2.7.3.6.tgz:

File name	Size (Bytes)
InControl-System-2.7.3.6/InControl-System-2.7.3.6-flat.vmdk	10,739,515,392
InControl-System-2.7.3.6/InControl-System-2.7.3.6.vmdk	574

DB-System-20170622.tgz:

File name	Size (Bytes)
DB-System-20170622/DB-System-20170622-flat.vmdk	10,737,418,240
DB-System-20170426/DB-System-2017622.vmdk	568

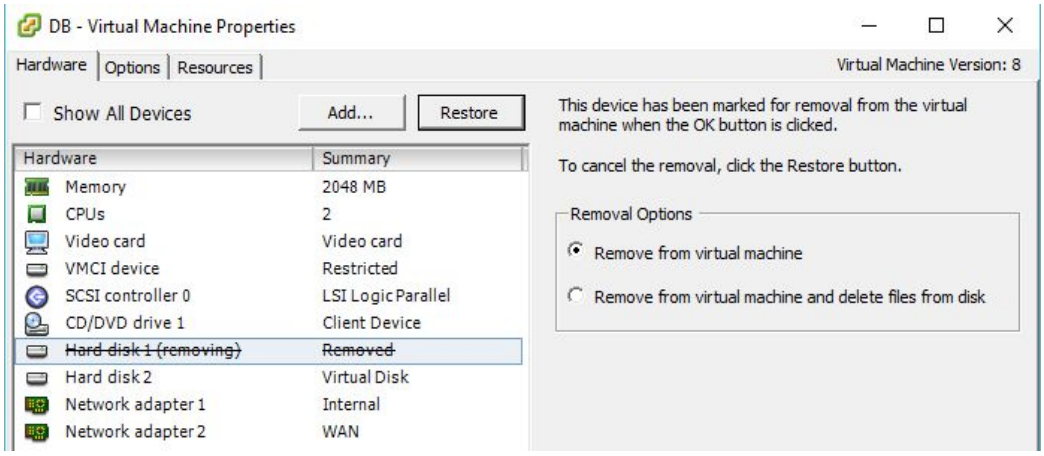
Step 3. Start the Datastore Browser in the vSphere Client. Use it to upload the `InControl-System*.vmdk` and `DB-System-*.vmdk` files to folders, say, "`InControl-System-2.7.3.6`" and "`DB-System-20170622`" in the datastore respectively. After finished uploading the two files, the two files will be shown as one item in the Datastore Browser.



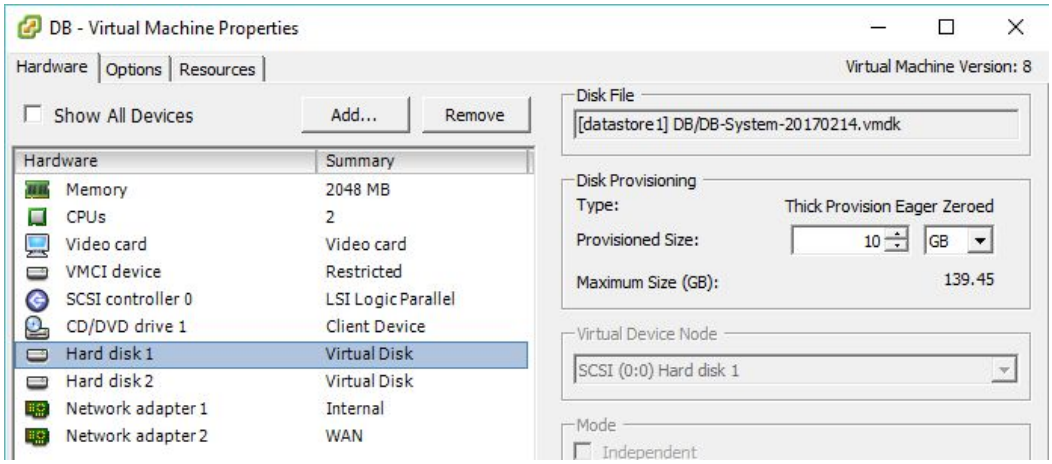
Step 4. Restart VMs in the following order:

1. Stop InControl VM. Wait until fully stopped
2. Stop DB VM. Wait until fully stopped
3. Open DB VM Properties,
    - Identify and select the system hard disk (usually "Hard disk 1")
    - Select the "Remove from virtual machine" radio button (without deleting it)

- Press "OK"

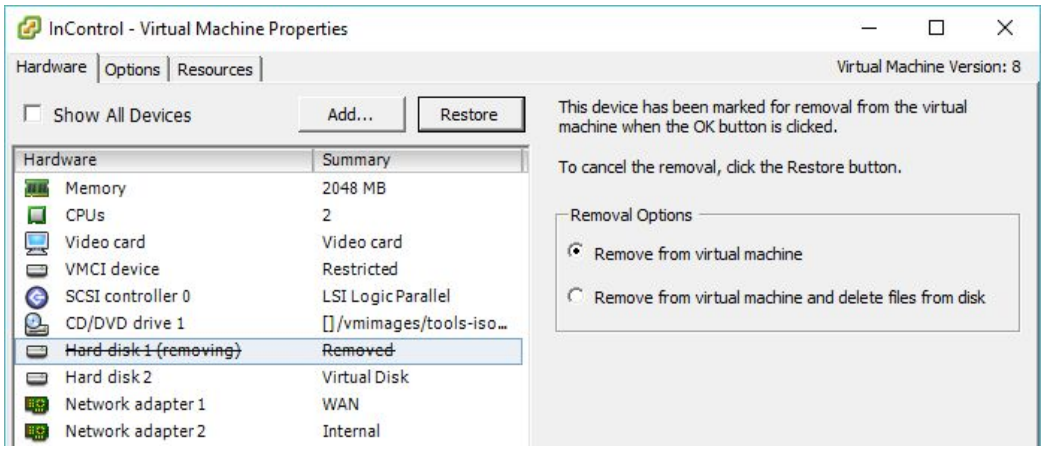


4. Open DB VM Properties again
   - Select 'Add…" > "Existing virtual disk…" > Browse and select the disk file "DB-System-*xxx-yyyymmdd*.vmdk"
   - Select SCSI 0:0 Hard disk as the Virtual Device Node

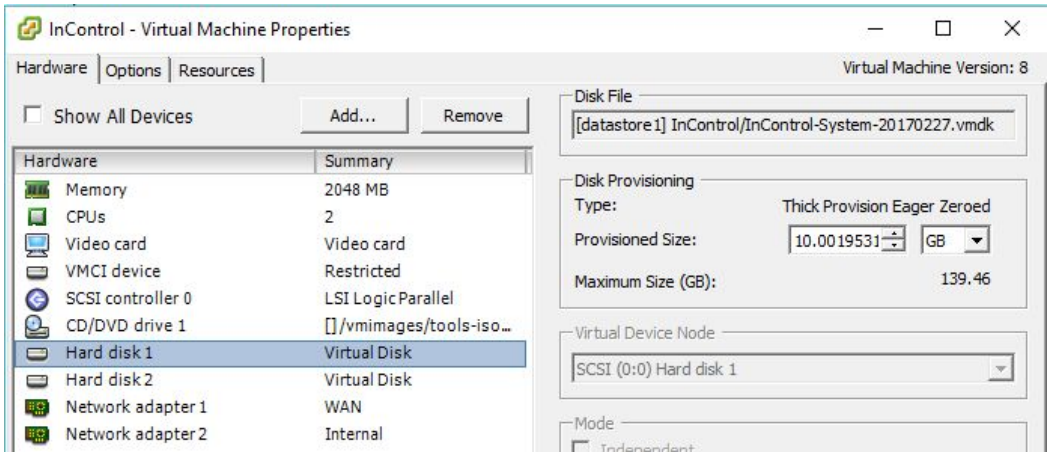


5. Start DB VM
6. Open InControl VM Properties
   - Identify and select the system hard disk (usually "Hard disk 1")
   - Select the "Remove from virtual machine" radio button (without deleting it)

- Press "OK"



7. Open InControl VM properties again
   - Select 'Add…" > "Existing virtual disk…" > Browse and select the disk file "InControl-*a.b.c*/InControl-System-*x.y.z*.vmdk"
   - Select SCSI 0:0 Hard disk as the Virtual Device Node



8. Inspect the DB VM's console. When it has booted up completely, start the InControl VM. Finished.

13.2 For Microsoft Hyper-V

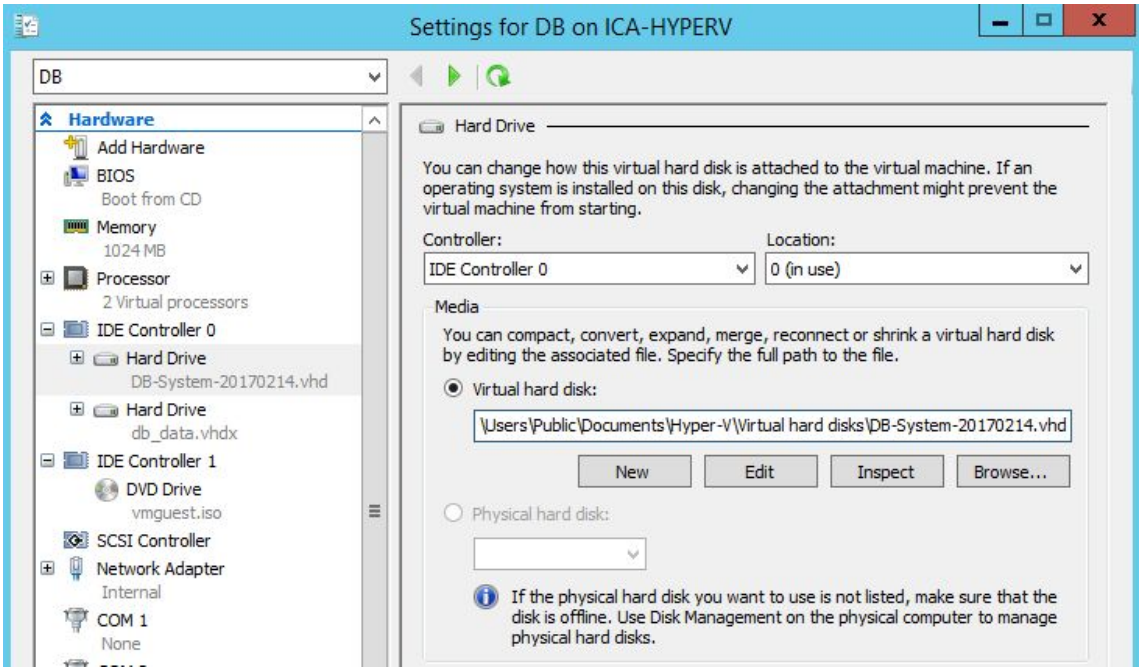
Step 1. Download the latest Virtual Appliance and Database Server image files in `.vhd` format from https://www.peplink.com/support/downloads/incontrol-appliance-image-and-installation-guide/

Take InControl 2.7.3.6 as an example. The .vhd file names and sizes are as follow:

File name	Size (Bytes)
InControl-System-2.7.3.6.vhd	8,608,834,048
DB-System-2.4.0-20170644.vhd	4,297,073,152

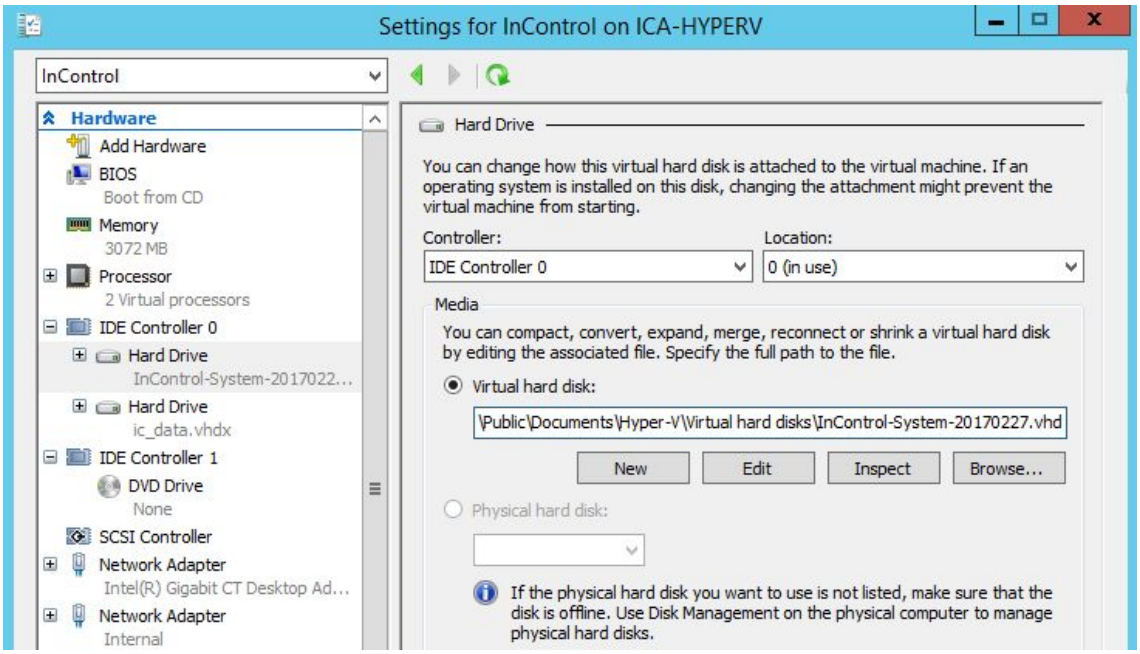
Step 2. Deployment

1. Stop InControl VM. Wait until fully stopped
2. Stop DB VM. Wait until fully stopped
3. Open DB VM Settings. Identify and select the system hard disk. Replace the virtual hard disk with the newly downloaded `DB-System-a.b.c-yyyymmdd.vhd` file. The "Location" for IDE Controller should be 0.



4. Start DB VM.

5. Open InControl VM settings. Identify and select the system hard disk. Replace the virtual hard disk with the newly downloaded `InControl-System-a.b.c.vhd` file. The "Location" for IDE Controller should be 0.



6. Inspect the DB VM's console. When it has booted up completely, start the InControl VM. Finished!

14. Upgrading InControl Hardware Appliance

Peplink regularly releases InControl appliance firmware. When you receive a firmware URL from Peplink, you could upgrade your InControl Appliance by opening the Control Panel page and pasting the URL to the Firmware URL field in the **InControl Upgrade** section.

After clicking the Upgrade button, it will download the firmware from the URL and perform an upgrade. Excluding the download time, the process should typically take about 25 mins.

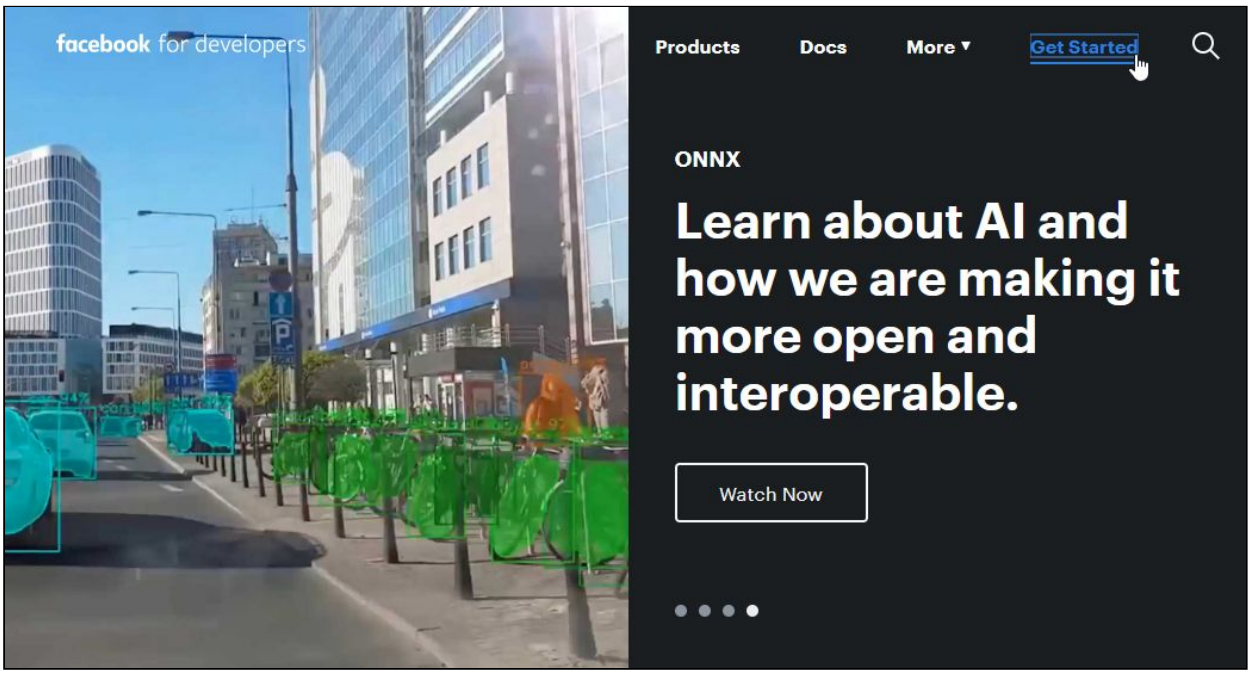
IMPORTANT: Please note that the system downloads the firmware via the management port instead of its WAN port. So please make sure the management port's gateway could route to the Internet. If the management had no Internet access, you may download the firmware file locally and put it to a local web server on the management network. Then you input the firmware's local URL to the Firmware URL field.

15. Facebook App ID Creation Procedure

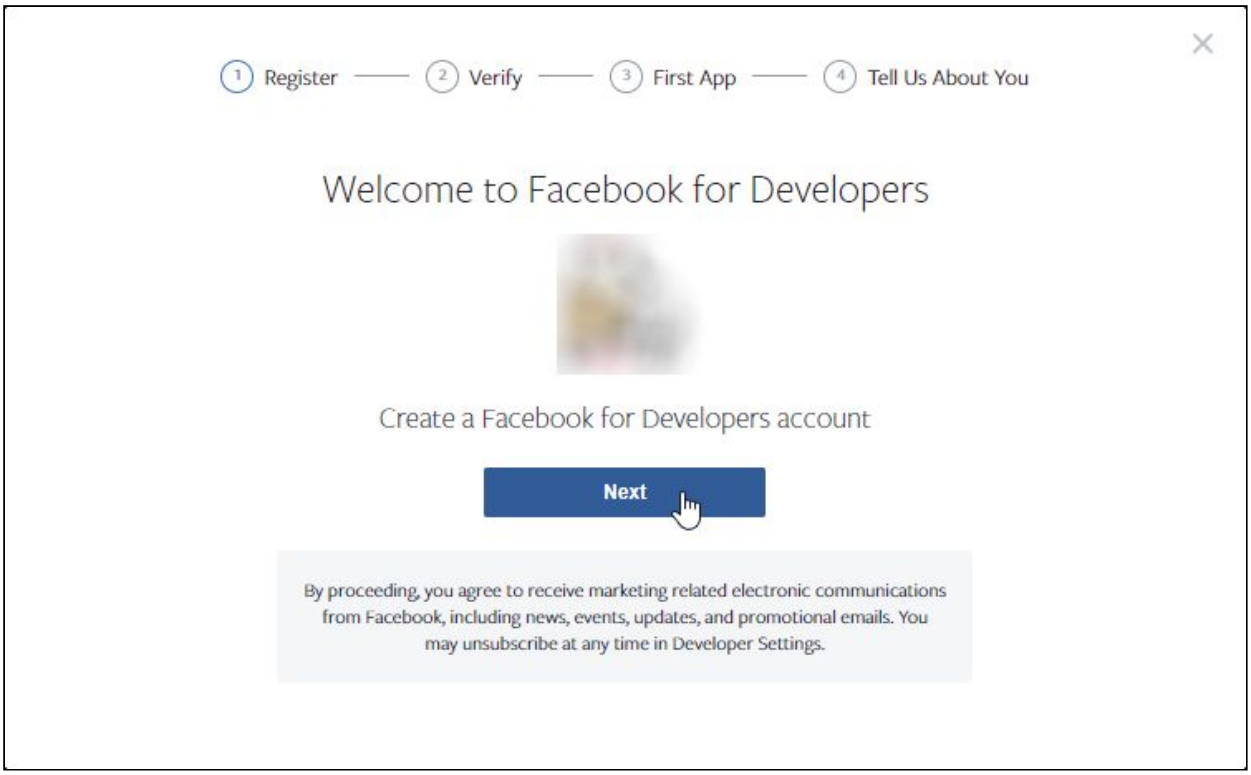
In order for the "Sign-in with Facebook" feature in the captive portal to work, a Facebook app has to be created in Facebook's developer console. prior to InControl 2.6.2, Peplink shared their own Facebook App for all InControl appliance installations. Since InControl 2.6.2, the Peplink's App ID no longer shares with InControl Appliance installations. Customers have to create their own Facebook app and input their app's ID and secret into the Control Panel.

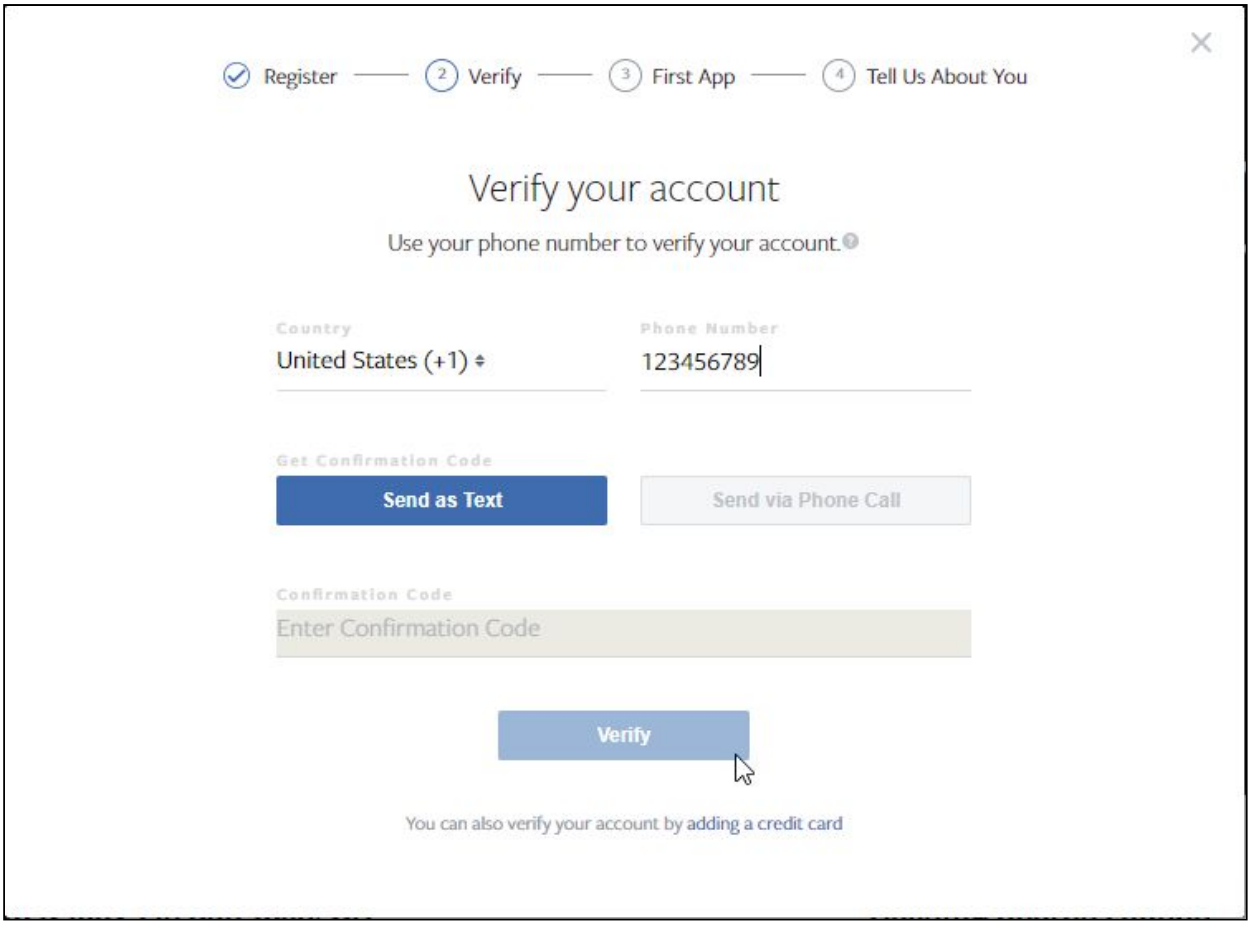
Below is a procedure for Facebook app ID creation:

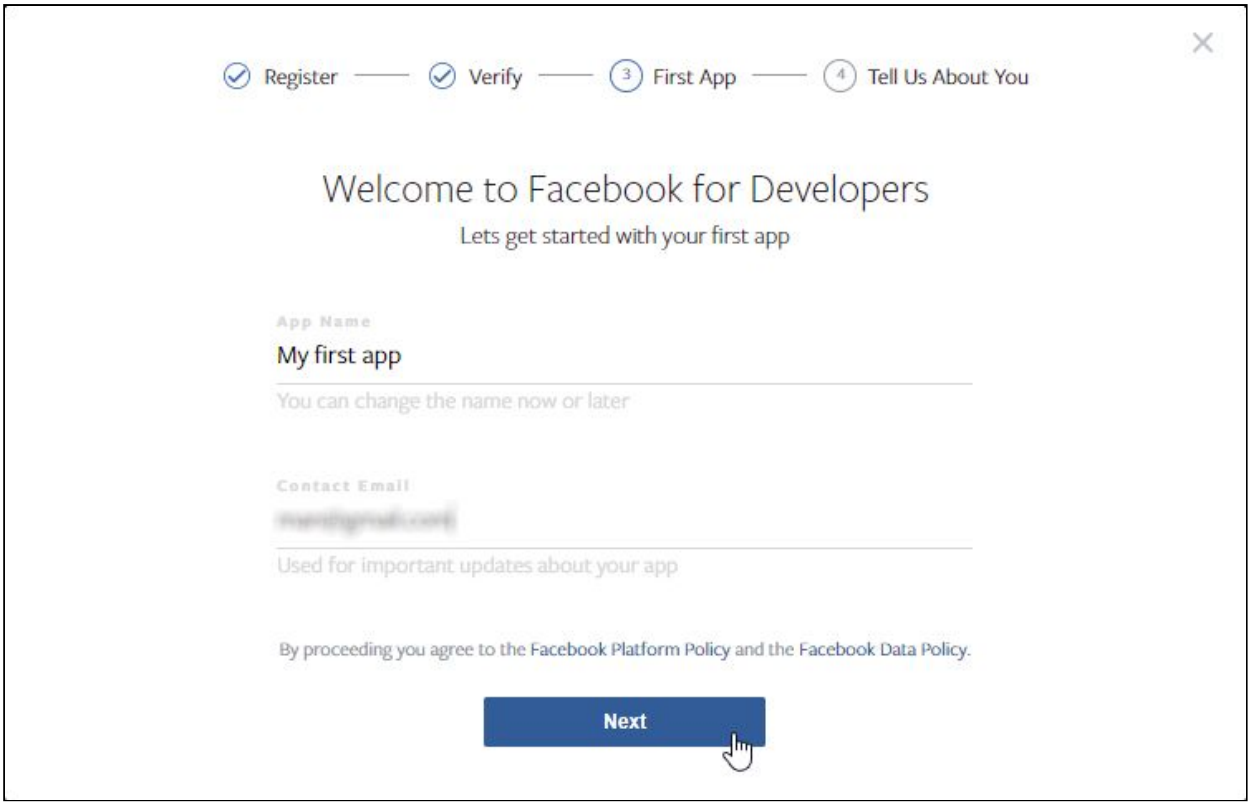
1. Login into https://developers.facebook.com/ and click Get Started:

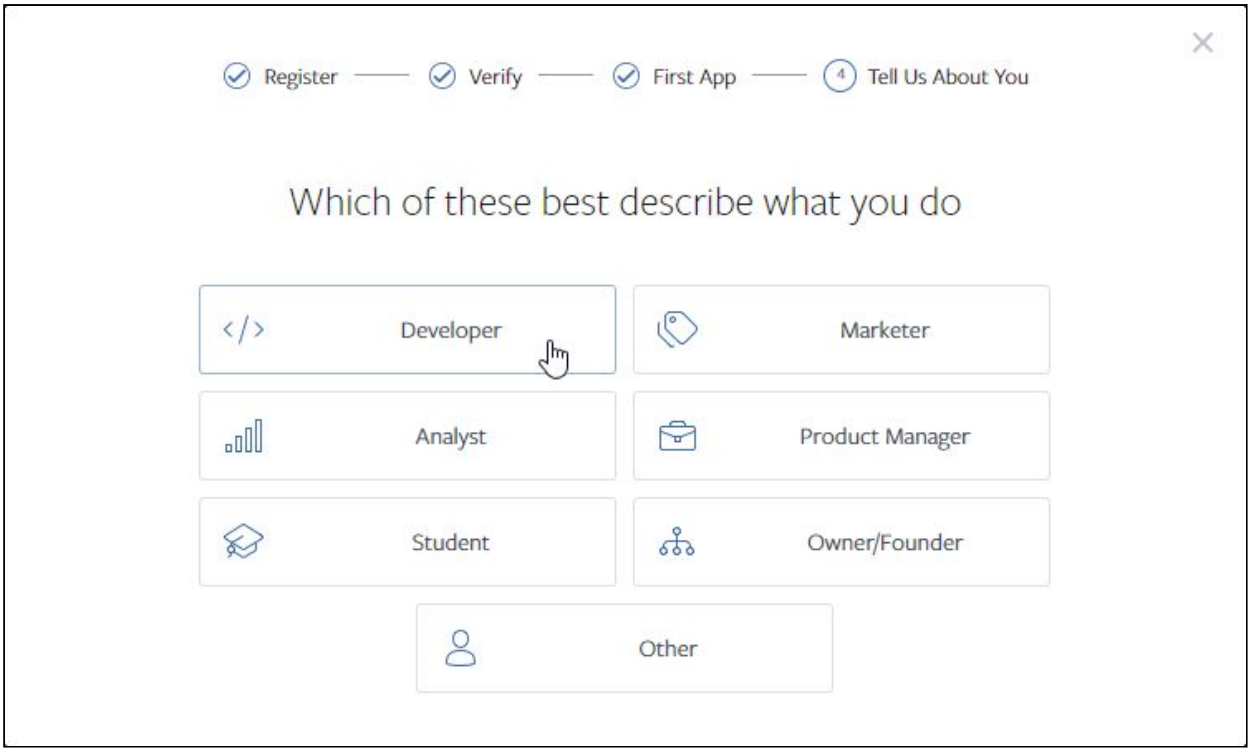


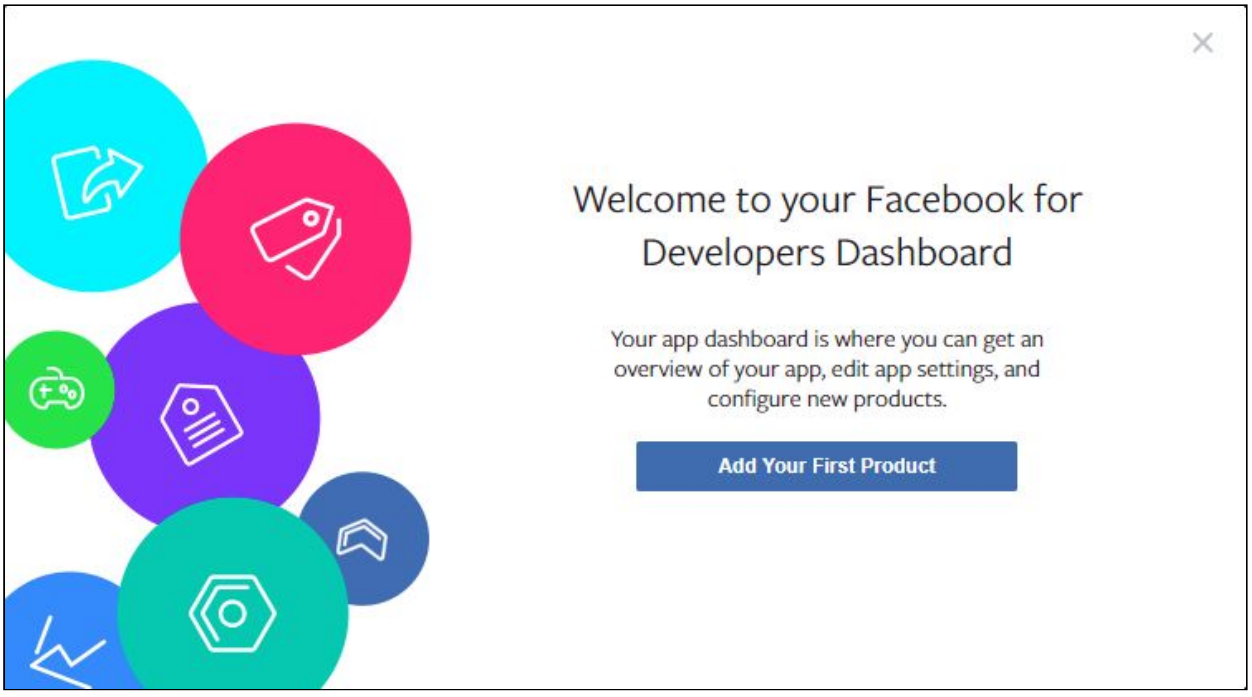
2. Go through the wizard by following the on-screen instructions. Click the "Add Your First Product" button on the final step.



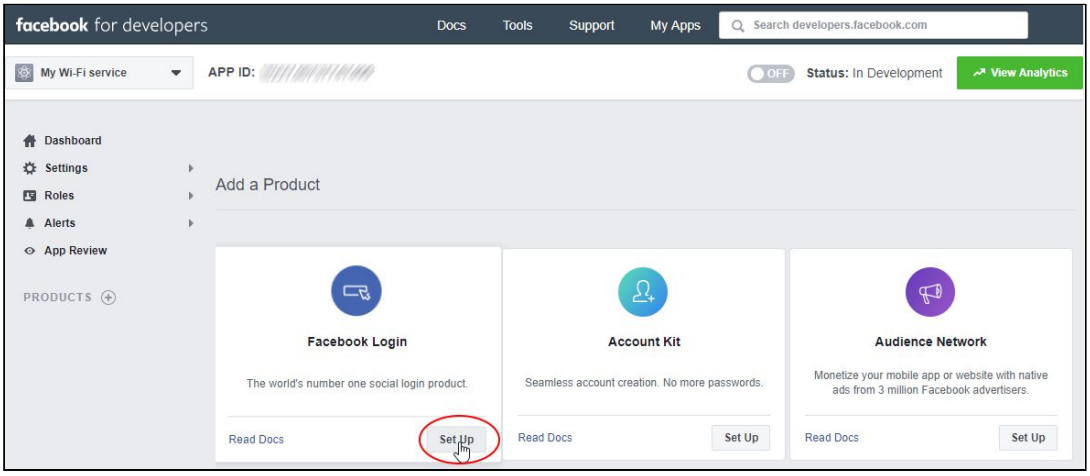

Register
2 Verify
3 First App
4 Tell Us About You
Verify your account
Use your phone number to verify your account.
Country
United States (+1)
Phone Number
123456789
Get Confirmation Code
Send as Text
Send via Phone Call
Confirmation Code
Enter Confirmation Code
Verify
You can also verify your account by adding a credit card


Register
Verify
3 First App
4 Tell Us About You
Welcome to Facebook for Developers
Lets get started with your first app
App Name
My first app
You can change the name now or later
Contact Email
Used for important updates about your app
By proceeding you agree to the Facebook Platform Policy and the Facebook Data Policy.
Next

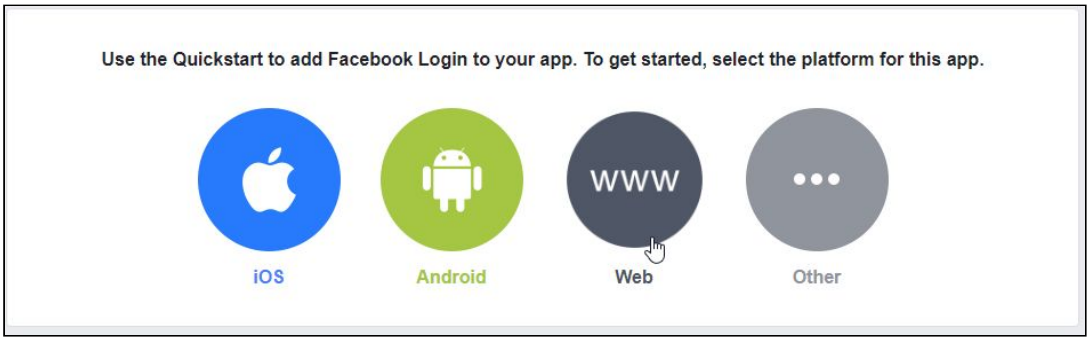

Register
Verify
First App
4
Tell Us About You
Which of these best describe what you do
Developer
Marketer
Analyst
Product Manager
Student
Owner/Founder
Other


Welcome to your Facebook for Developers Dashboard
Your app dashboard is where you can get an overview of your app, edit app settings, and configure new products.
Add Your First Product

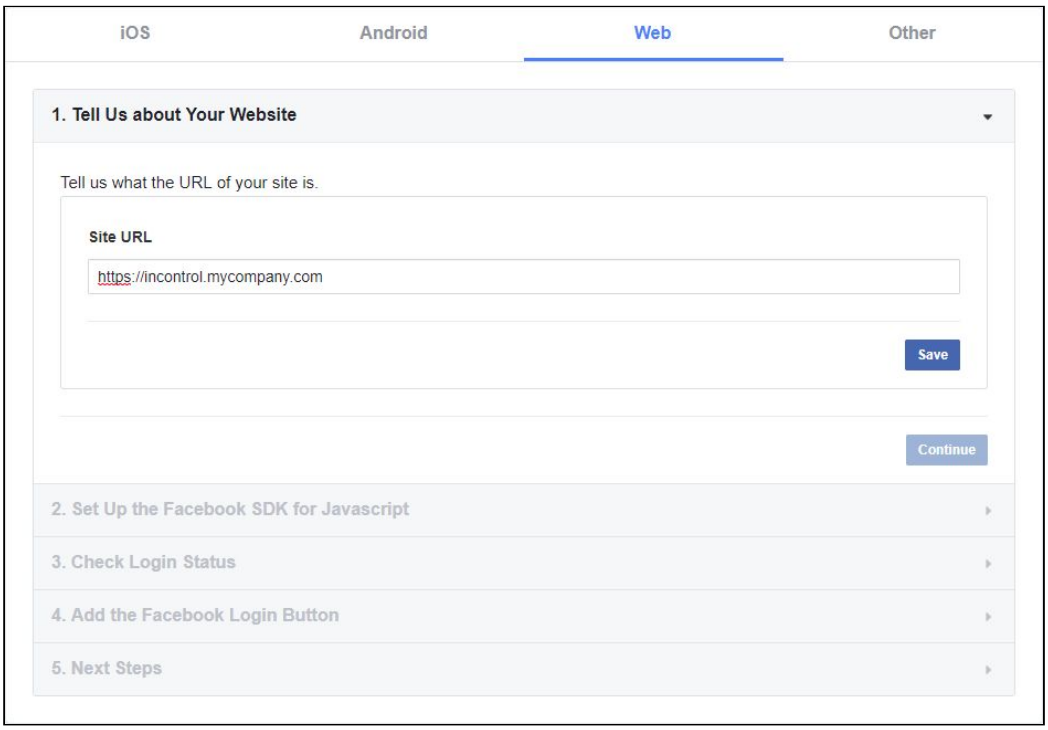
3. Click the “Set Up” button on the “Facebook Login” control



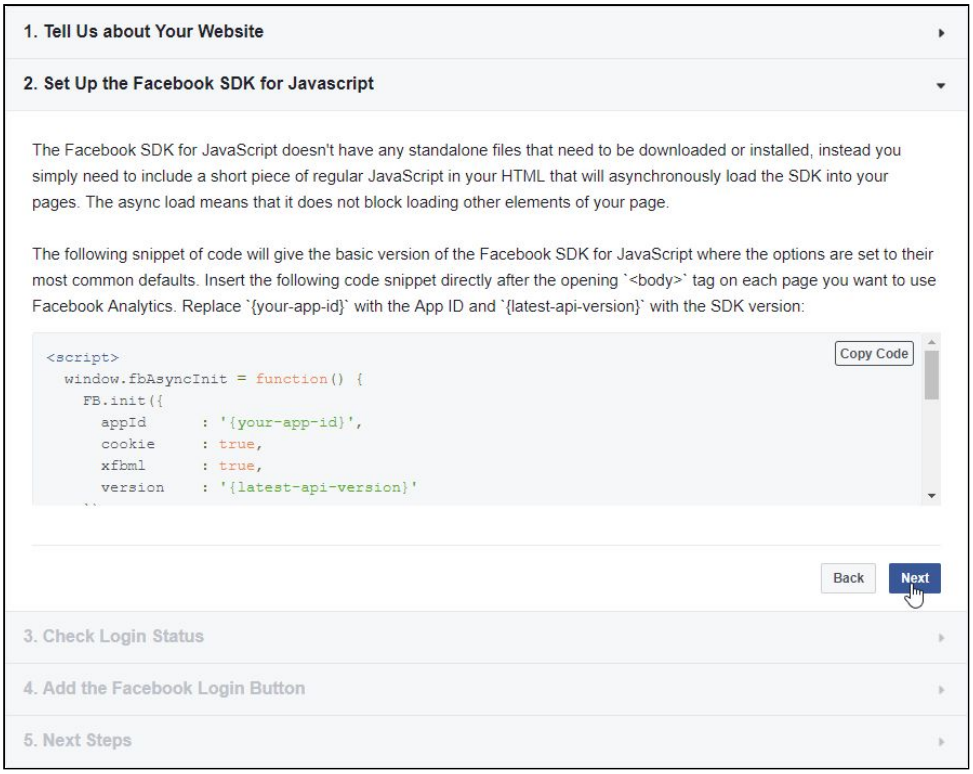
4. Click “Web”



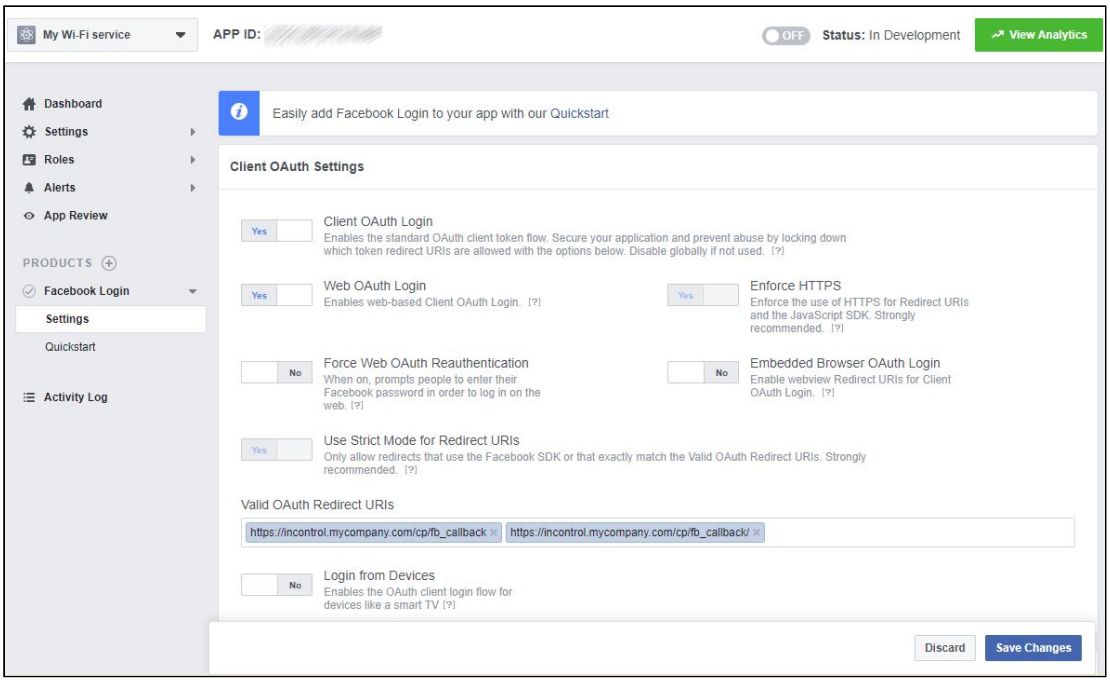
5. Input your InControl appliance's URL into the Site URL field:



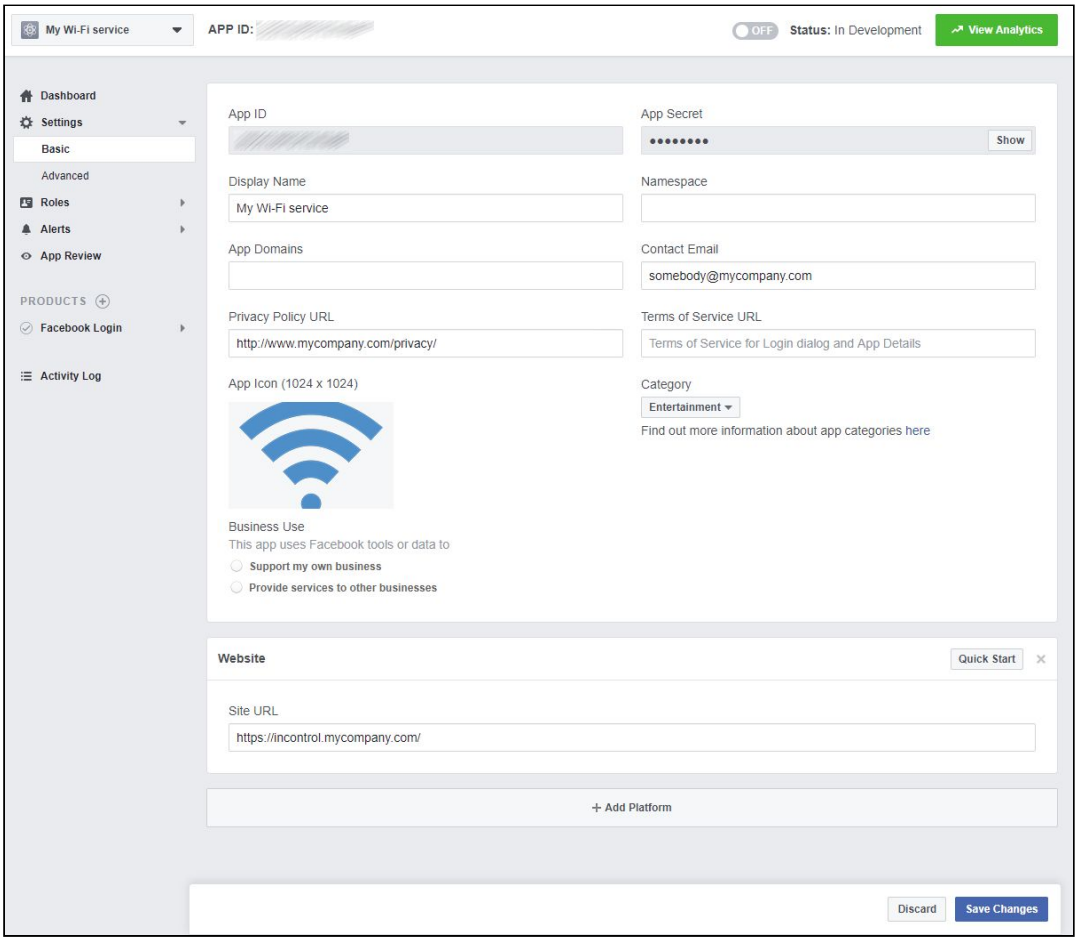
6. Click "Next".



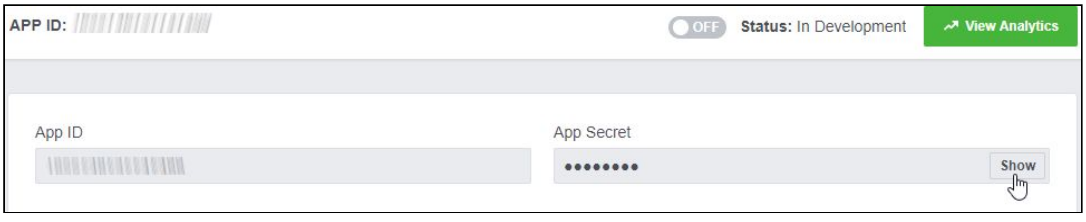
7. Input the following URLs into the “Valid OAuth Redirect URIs” field:
   `https://[InControl_URL]/cp/fb_callback` and
   `https://[InControl_URL]/cp/fb_callback/`



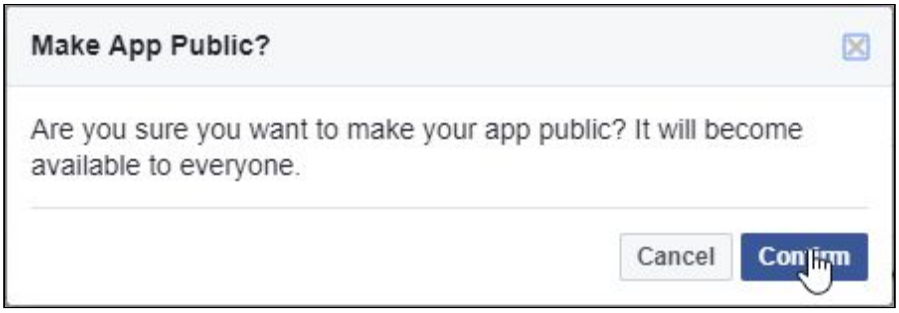
8. Fill in “Display Name”, “Contact Email”, “Privacy Policy URL” fields accordingly. Upload an App Icon in the dimension of 1024x1024. Press “Save Changes”.



9. Click the “Show” button to reveal the App Secret. Record the App ID and App Secret and input into the InControl Control panel’s “Facebook App Settings” field.



10. Finally, click the OFF switch and click Confirm to make the app public.



16. Release Notes

Release notes for 2.7.3.6

Here are the changes since 2.7.3.5:

- Google is shutting down the Google+ Sign-in API. It will cause earlier InControl releases' Sign-in with Google to fail intermittently from January 29, 2019 and completely from March 7, 2019. This release will no longer depend on the "Google+ Sign-in" API.
- Security fix: disabled SSLv2 and SSLv3 support on the secure web server for the control panel.
- Cellular reports: fixed the date range selector.

Release notes for 2.7.3.5

Here are the changes since 2.7.3.2:

- Added OpenStreetMap Server URL settings
- Improved system's availability
- Read-only users can only retrieve some less sensitive data via the API.
- Control panel
    - When a pair of wrong or mismatched SSL private key and certificate is uploaded, a pair of default private key and certificate will be used instead so that the InControl web site and the control panel could remain accessible.
    - (Software appliance) Added a link for downloading a diagnostic report and a button for restarting system services.
- Fixed: EDNS compliance issue
- The DHCP Server setting for all VLAN profiles can now be set to "Unmanaged".

Release notes for 2.7.3.2

Here are the changes since 2.7.3.1:

- Fixed: (Hardware appliance) License information is not displayed correctly on the LCD panel.
- Fixed: (Software appliance) Configured Google Maps API key was not displayed.
- Fixed: A "loop error" was displayed after signing-in in some installations.
- Fixed: Firmware policy might not be applied to first-appeared devices.
- Fixed: In outbound policy management, with preserve rules upon policy removal enabled, InControl applied rules were not preserved.

- PepVPN configuration wizard now supports very large star topologies.

Release notes for 2.7.3.1

Here are the changes since 2.7.3:

- Fixed: for ICAs 2.7.3 upgrading from versions prior to 2.7.1, users are not able to add devices.
- Fixed: Google Maps API keys may not be activated effectively in some situations.
- Updated the instructions of how to generate a Google Maps API key. In the Google Cloud Platform UI, you should enable not only "Maps JavaScript API", but also "Geocoding API".
- Included various UI bug fixes

Release notes for 2.7.3

IMPORTANT: since the release 2.7.3, InControl appliances' license key no longer ties to a hardware dependent device ID but the server name. So after upgrading to 2.7.3, the existing license will turn into a 7-day evaluation license. So before upgrading your InControl Hardware or Virtual Appliance to 2.7.3, please get a new license key by emailing your InControl Appliance's **serial number** and **server name** (aka "URL Host Name" which is showing on the control panel) to **ica@peplink.com**. Peplink personnel will send you back a new license key. You will have to enter this key onto the Control Panel page after an upgrade.

Here are the changes since 2.7.1:

- Captive portal: text alignment of General Description is adjustable.
- Geo-fencing: added an option to perform enabled actions upon fence modification or device addition
- Bulk Configurator: PepVPN profiles in configuration files can optionally be preserved.
- Fixed various issues in managing Pepwave Surf On-The-Go
- The licenses no longer tie to the hardware-dependent "device ID". It now ties to the server name. This will avoid the need of updating the license upon any virtual or physical hardware changes.
- Captive portal: guests no longer need to agree Peplink collect their personal data as Peplink has no access to the data on InControl appliances.
- Added a Google Maps API Key setting to the control panel. Please refer to chapter 4 Input Google Maps API Key for further details.
- Added SNMP service for monitoring the ICA. An SNMP read-only community setting is added to the control panel.

- Latest GA device firmware profiles were not synced from Peplink InControl 2 to ICA 2.7.1. Now they are synced again (if the ICA can communicate with Peplink InControl 2)
- The Linux kernel has been upgraded to 3.16.57.

Release notes for 2.7.1

Here are highlighted changes since 2.6.2:

- Daily backup archive of the InControl appliance is now downloadable from the Control Panel. It contains all essential data and configurations for restoring the system. It does not include reports, GPS location data, and event log. You are recommended to download a copy of the archive regularly. Note: Restoration of an InControl appliance from a backup archive has to performed by Peplink personnel in this stage.
- SpeedFusion configuration: added a “Suppress Endpoint IPs” option to Star Topology. Enabling it could maintain PepVPN connections uninterrupted for any potential endpoints’ IP address changes. This option is disabled for existing profiles and is enabled for newly created profiles.
- Captive Portal enhancements:
    - The Terms and Conditions and its checkbox label can be partially customizable.
    - Added skip sign-in (i.e. “No thanks”) option to e-mail and SMS access modes.
    - In token access mode, when concurrent login is allowed, data usage based quota can no longer be chosen now. Any existing profile with both concurrent login and data usage based quota enabled, the data usage quota will be disabled.
    - In open access mode, the Terms and Conditions checkbox could now optionally be hidden. If the “Connect” button text is changed to “I Agree”, guests could accept the Terms and Conditions and submit the form with one click.
    - An additional message could be put on the signed-in (landing) page. Hyperlinks could be included in the message in markdown syntax.
    - By default, the first page of the captive portal is pre-cached on the router/AP for faster accesses. This feature could now optionally disabled.
- Added NAS Identifier setting under WPA/WPA2 Enterprise mode of an SSID.
- Firmware setting for the same product but different hardware revisions can now be customized individually. The system now could ensure firmware is applied to supported hardware revisions only.
- PepVPN: allow to activate/inactivate a PepVPN connection by device tags.
- Introduced a new geo-fencing action: device tagging, which is for controlling any tag supported configuration (e.g. PepVPN, SSID, captive portal, etc.)
- When outbound policy and firewall rule management are enabled and a device is newly added to a group, if the device receives no rules, the outbound policy and firewall rules

on it were also cleared prior to this release. But now, you can choose to preserve the rules. For any groups created from now on, the rules on newly added devices will be preserved by default.

- *Device Web Admin Authentication* settings are moved to the group-level *Device System Management* page. The settings are split into sections for Balance/MAX, AP and SD Switch.
- Added notification for *Web Admin Login* and "*SIM Card Switch Over*" events
- Added silence period setting for geofencing notifications
- Added SIM lock setting to *Device Details* and *Device Management* pages (require firmware 7.1.1 or above)
- Added ability to choose devices by tags to receive external InControl appliance settings.
- Added a badge to indicate an AP One unit is operating in router mode.
- Added a new authentication mode *CoovaChilli* to external captive portals.
- Added a *Regenerate Key* option to "randomly generated key" field of an SSID.
- Introduced organization-level SpeedFusion Alliance FusionHub license (this type of license will be available to purchase later)
- Included various UI enhancements and bug fixes.

Note: In rare situations, the control panel may display "License not available" in the first boot after the upgrade. In case you see the message even the system has been up for 10 minutes, please press the Reboot button on the control panel once to restart the system. The license shall display correctly after that. This problem will be fixed in the next release.

Release notes for 2.6.2

Here are highlighted changes since 2.6.1:

1. In anticipation for the new data protection laws that will take effect on 25th May in Europe, in this release, we have updated the types of information to be collected through the captive portal and our Privacy Policy. Please also read the revised Privacy Policy carefully as the Privacy Policy will be presented to your Wi-Fi users.

   In order for the Sign-in with Facebook in the captive portal to continue to work in your InControl appliance, you have to apply for an app ID and secret from Facebook and enter them into the control panel. For the details, please refer to chapter 11. Facebook App ID Creation Procedure.

   When your user decides to log in to the captive portal with social network access mode, the system will only collect the following personal data through social networks:
   - E-mail address (if any);
   - User ID of the Social Media

Any other personal information or statistics will be deleted and no longer be available.

If you let a user log in through e-mail or SMS access modes, the system will collect the following information according to your chosen configuration:

- email address
- phone number
- name
- gender
- country

In addition, Wi-Fi usage duration, MAC Address, and IP address will be collected

The retention period for user information will be two years.

2. Added license status to the top of the System Usage Report page.
3. [Software Appliance] Added support of an optional second WAN interface. It is pre-configured to acquire an IP address from a DHCP server.

Release notes for 2.6.1 (no appliance image released)

Here are highlighted changes since 2.6.0:

- All existing *Organization Administrators* are now promoted as *Super Organization Administrators*. A new role *Organization Administrator* is introduced.
    - Social user data in captive portal reports and client details are now only visible to *Super Organization Administrators*, *Captive Portal Administrator*, and *Captive Portal Viewer*. Any other roles, such as the new *Organization Administrators* or *Group Administrators* also could not see any social user data.
    - *Super Organization Administrator* is now able to remove social user data.
    - You may consider to demote some *Super Organization Administrators* to *Organization Administrator* for those who should not have social user data access.
- Added a public API for creating Service Provider Default on devices.
- In moving a device from one group to another, you could choose to retain InControl generated settings in the target group.
- In Cellular Reports > Signal Strength & Quality chart, carrier and cellular signal information are now shown in the tooltip of the chart when hovering over a data point.
- In a captive portal profile's Preview and Customization screen, for e-mail access mode, added Phone Number, Gender and gender option text fields.

- For Balance/MAX's switch port list, Port Type and VLAN fields are now populated.
- Warranty expiration notification e-mails now include which InControl organization and group that devices reside in.

Release notes for 2.6.0 (no appliance image released)

Here are highlighted changes since 2.5.2:

- Introduced "Low Data Usage Mode". See the group-level "InControl Options" page. The mode is for reducing data usage on device-InControl communication and device locally generated traffic. A data usage calculator is also provided.
- Group creation page: allow to optionally clone SSID, VLAN, captive portal and schedule settings from an existing group.
- Notifications:
  - Added High Availability (HA) transition and Smart Reader attachment/detachment notifications
  - Added tags and notes to device up/down e-mail content
- PepVPN configuration:
  - You may now create a profile for connecting to an externally managed device. E.g. Suppose device A and B are managed in organization A and B respectively. Now you can create a PepVPN profile in organization A and B individually to connect them. (In End Point Device selection screen, select the "Show advanced settings" option and then click a new "Add Device" button.)
  - Added a path cost field to topologies
  - Add VLAN network selection for NAT mode in star topology profiles
- Group-level PepVPN status in tabular view revamped. Subnets of both ends are now displayed
- Added organization level SIM Pool Data Usage reports
- Added Extended DHCP Options to VLAN networks' default DHCP Server settings for Balance and MAX.
- Data roaming for cellular WANs could be enabled from the Actions menu in Device Management pages.
- API: added an endpoint for retrieving admin user list and their role in an organization
- Included various UI enhancements and bug fixes

Release notes for 2.5.2

Here are highlighted changes since 2.4.2-1:

- A SpeedFusion Alliance (SFA) FusionHub license could be applied to a FusionHub instance via an InControl Appliance release 2.5.2 (or above) instantly without requiring to

reboot the FusionHub. (See chapter 10 of the InControl 2 Appliance Setup Guide for the additional network access requirement)

- Added support to send notifications from InControl Appliance to the InControl mobile app. (See chapter 10 of the InControl 2 Appliance Setup Guide for the additional network access requirement)
- When captive portal guests sign in with Facebook, their relationship information is no longer collected as Facebook has stopped to provide the information.
- Introduced group-level SIM Pool Bandwidth Usage reports:
    - Bandwidth usage reports can automatically be grouped by the carrier.
    - Custom SIM pools could be defined by inputting IMSI's
    - Up to three usage alert levels could be defined.

  (Requires Firmware 7.0.2 or above)
- Channel width can now be configured in "Radio Settings" page.
- Added Bandwidth Management and QoS settings to the "SSID Settings" page for Pepwave AP devices.
- The routing mode (i.e. bridged or routed) of each AP Device can be changed on "Device Management" page.
- For devices supporting High Availability (HA), HA status is now shown on "Device Details" page.
- SpeedFusion configuration:
    - A device which is not managed under the same organization or not even managed by InControl can now be added to a star and point-to-point topology profile by its site ID. Enable the "Show advanced settings" option to unveil an "Add Device" button.
    - PepVPN connection (link) names can be customized.
    - Data port and path cost for each link can be customized on the "Advanced Link Settings" screen
    - Pre-shared Key (PSK) for existing profiles can be regenerated on "Advanced Link Settings" screen
    - Newly generated PSK's length increased from 45 to 64 characters.
- Group level SpeedFusion status in tabular view has been revamped.
- Ethernet port status is displayed on devices' details page for supported hardware models.
- GPS enabled devices' map UI on "Devices Details" and "Cellular Reports" have been redesigned.
- Added an option to use OpenStreetMap for all map displays. The map data are hosted by Peplink. It is useful for networks that have restricted access to google.com. See "Organization Settings" page for the option.