

InControl 2 Appliance Setup Guide

for Virtual and Hardware Appliance 2.7.1

(Last updated: 2018-07)

Contents

[1. Virtual Appliance](#)

[1.1 Introduction](#)

[1.2 Minimum 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](#)

[2.3 Input E-mail Delivery Settings](#)

[2.4 Input FTP/SFTP Archive Server Settings](#)

[2.5 Facebook App Settings \(for Captive Portal\)](#)

[3. Setting up Devices to Report to InControl](#)

[Method 1: By configuring devices individually - for Internet isolated environment](#)

[Method 2: By Configuring or Redirecting Devices from the Peplink InControl - for Internet accessible environment](#)

[4. Logging Into InControl Appliance Web Site](#)

[5. Importing Devices](#)

[6. Creating an Organization, Group and Adding Devices](#)

[7. API Access](#)

[8. Settings on Your Firewall](#)

[8.1 For Hardware Appliance's Management Port](#)

[9. Upgrading InControl Virtual Appliance](#)

[9.1 For VMware ESXi](#)

[9.2 For Microsoft Hyper-V](#)

[10. Upgrading InControl Hardware Appliance](#)

[11. Facebook App ID Creation Procedure](#)

[12. Release Notes](#)

[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](#)

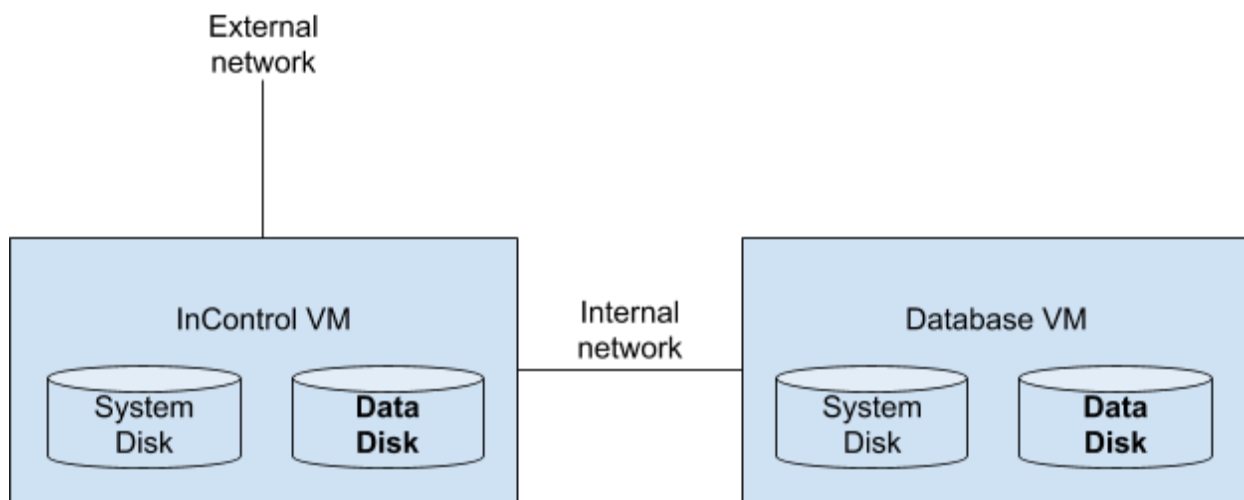
1. Virtual Appliance

1.1 Introduction

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

It consists 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 Minimum Hardware Requirements

- CPU: Dual core minimum. Quad core preferred for more than 100 devices.
- Memory : 8 GB (6 GB for the InControl and 2 GB for the DB)
- Storage:
 - 100 GB for up to 100 online devices
 - 500 GB for 1000 to 2000 online devices (The amount 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.)

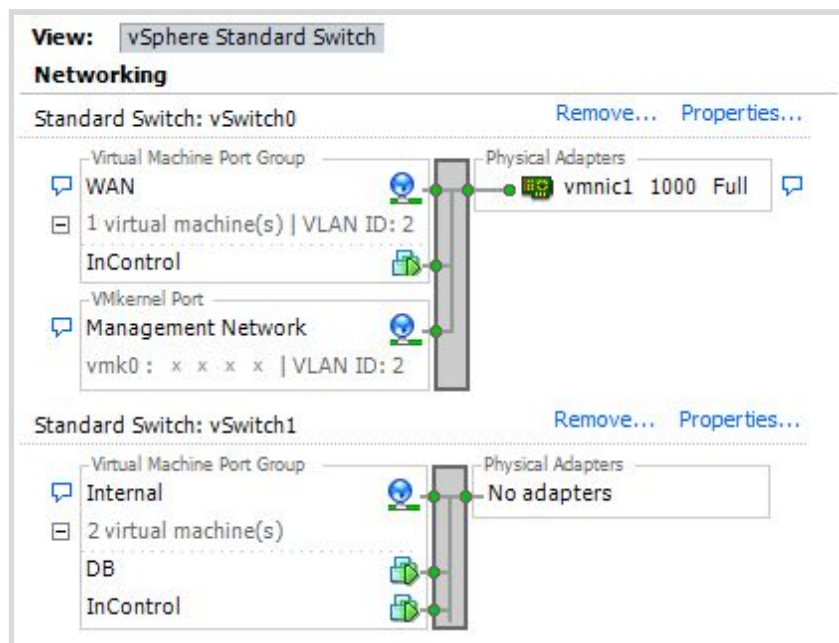
1.3 Installation on VMware ESXi 6.0 and ESXi 5.5

Peplink distributes two **tgz** files: `InControl-System.tgz` and `DB-System.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

First of all, please create two networks on the ESXi host > Configuration > Networking. One is called "Internal". It is for inter-InControl-DB communication, no physical adapter is needed. Another one is called "WAN" which is for connecting to the outside world, and will need a physical network adapter attached.

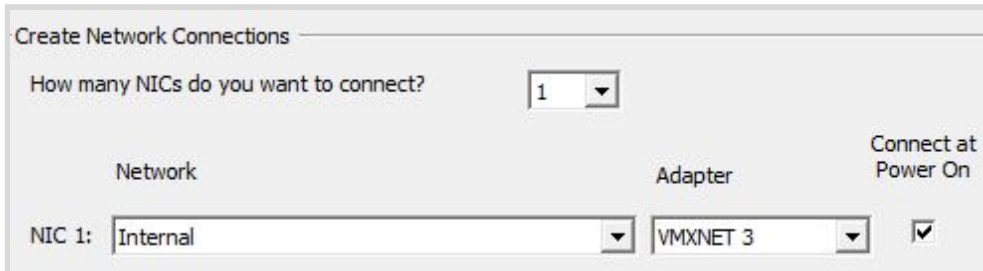
NOTE: The WAN interface cannot be on the subnets 192.168.1.0/24 or 192.168.30.0/24 because they are reserved for internal communication within the system.



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:

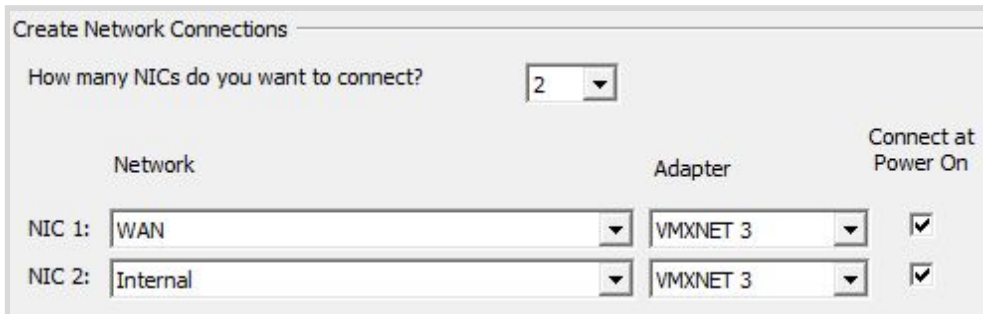


Create Network Connections

How many NICs do you want to connect? 1

Network	Adapter	Connect at Power On
NIC 1: Internal	VMXNET 3	<input checked="" type="checkbox"/>

InControl VM:



Create Network Connections

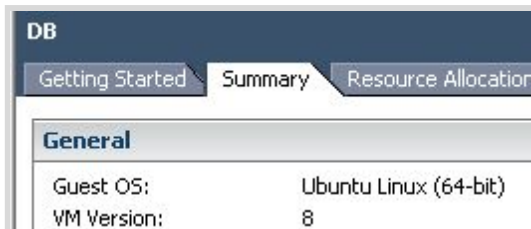
How many NICs do you want to connect? 2

Network	Adapter	Connect at Power On
NIC 1: WAN	VMXNET 3	<input checked="" type="checkbox"/>
NIC 2: Internal	VMXNET 3	<input checked="" type="checkbox"/>

Uploading and adding data storage to the VMs

Extract the tgz's on your desktop.

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.

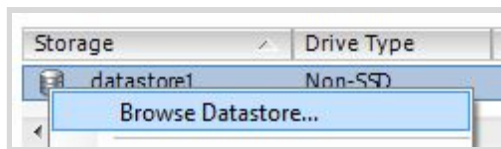


DB

Getting Started Summary Resource Allocation

General

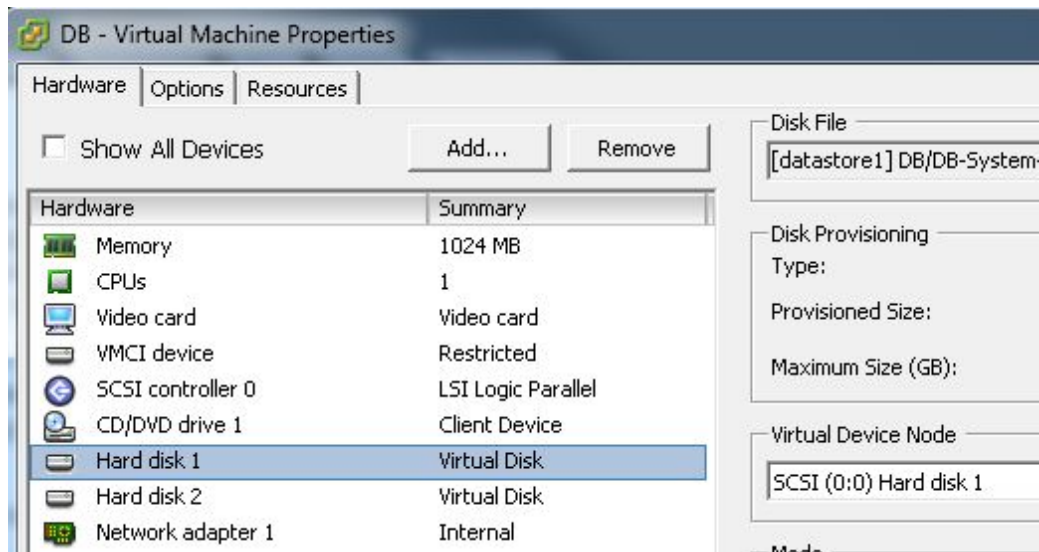
Guest OS:	Ubuntu Linux (64-bit)
VM Version:	8



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

Note: you can extract the `tgz` in the ESXi terminal, but with an error. Only the flat file will be available and you will need to create the `vmrk` parameter file manually with `vi`.

Now you can 'Edit Settings' of each VM. Remove the existing hard disk. For the InControl VM, add the `InControl-System.vmrk` 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](#))



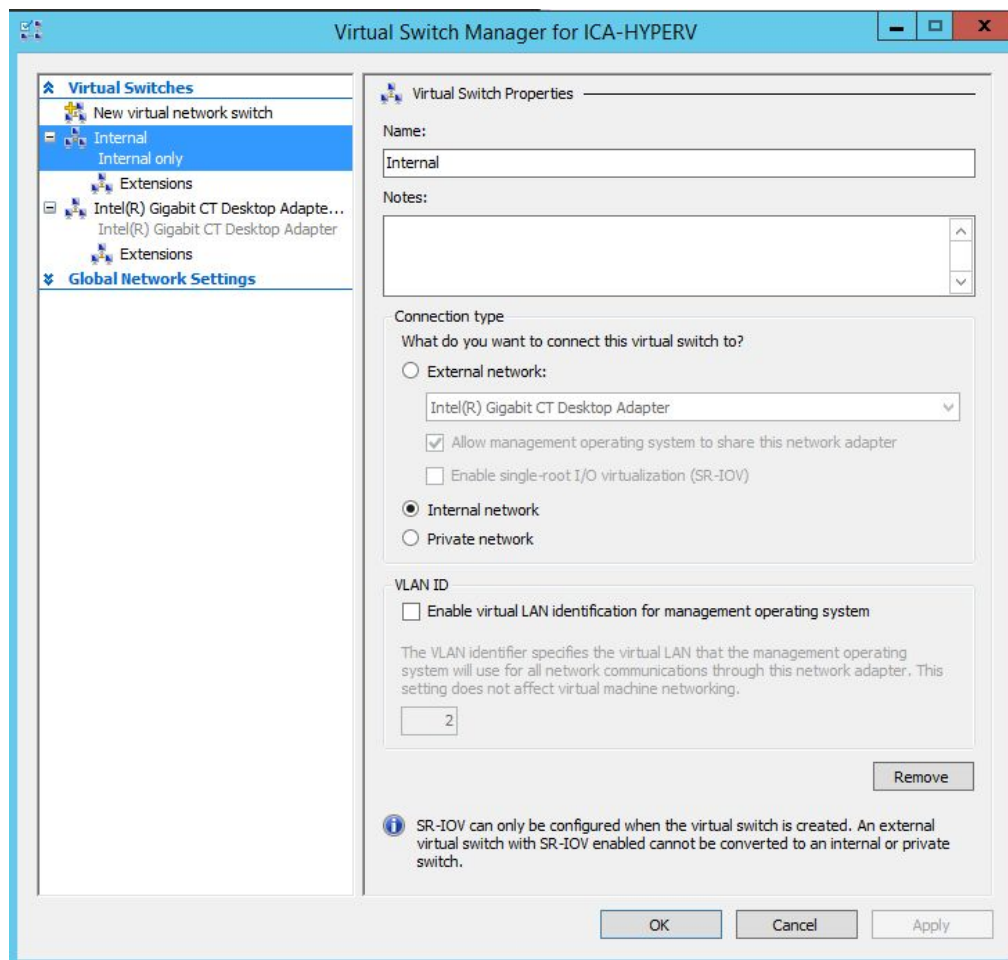
1.4 Installation on Hyper-V Windows 2012 R2

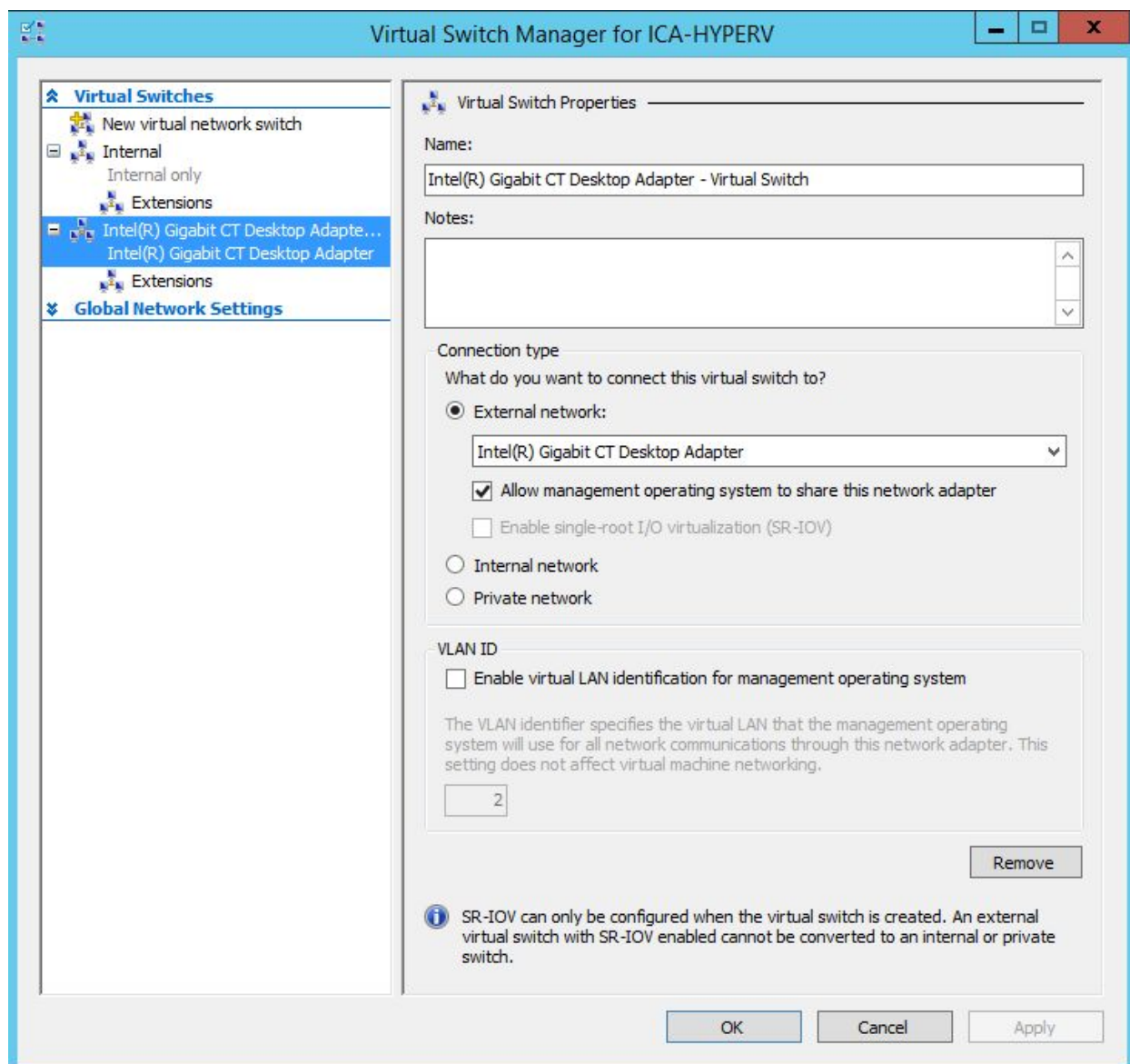
Peplink distributes two VMDK files: `InControl-System.vhd` and `DB-System.vhd`. They are bootable systems of the InControl virtual appliance and a MySQL database respectively. You will use them to start one InControl and one MySQL DB VM.

Networking

First of all, please create two networks on the Hyper-V host. One is called "Internal". It is for inter-InControl-DB communication, no physical adapter is needed. Another one is called "WAN" which is for connecting to the outside world, and will need a physical network adapter attached.

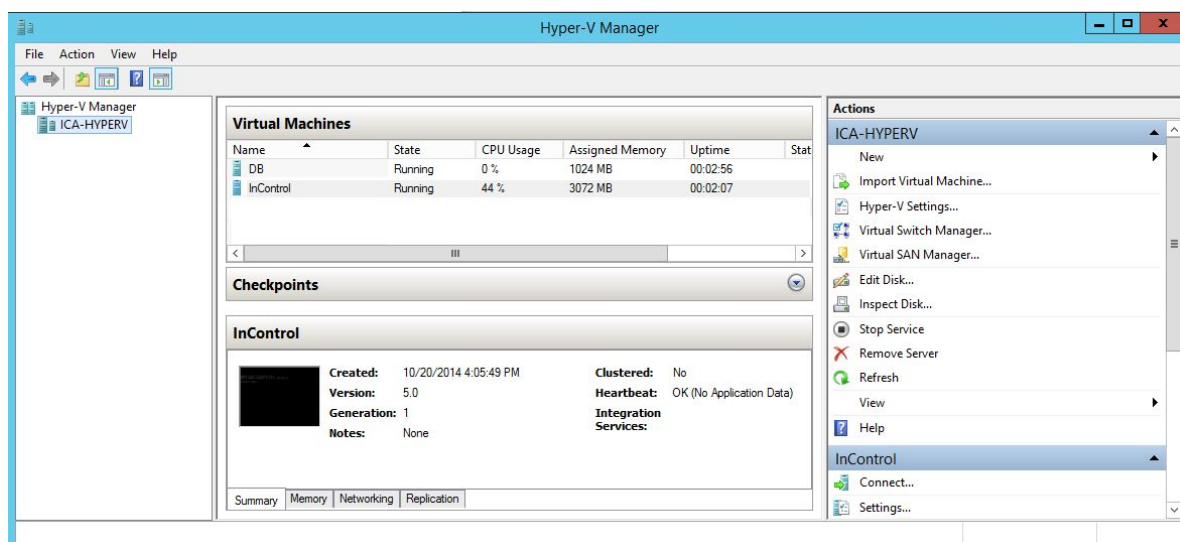
NOTE: The WAN interface cannot be on the subnets 192.168.1.0/24 or 192.168.30.0/24 because they are reserved for internal communication within the system.



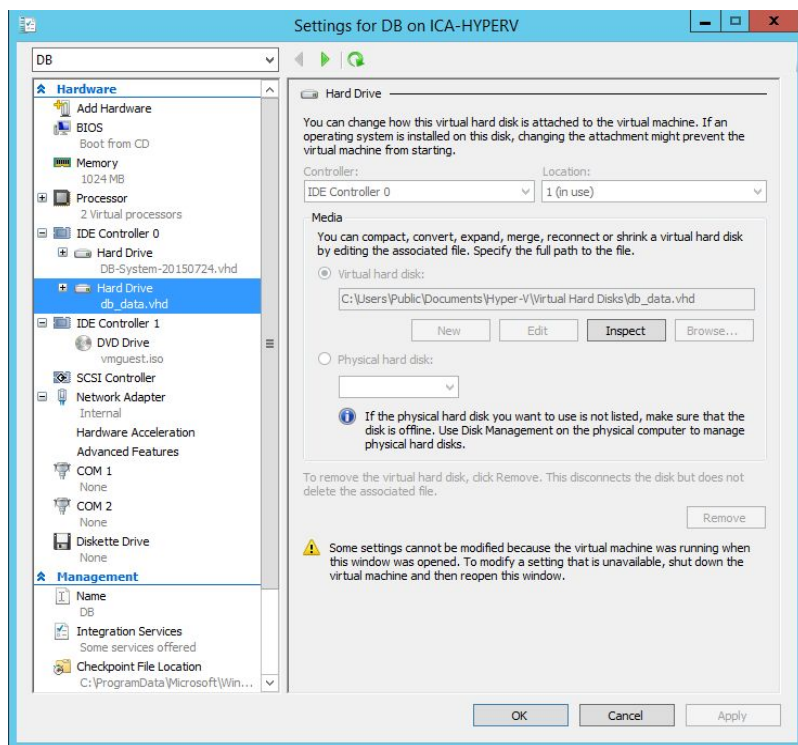


Creating InControl and DB VMs

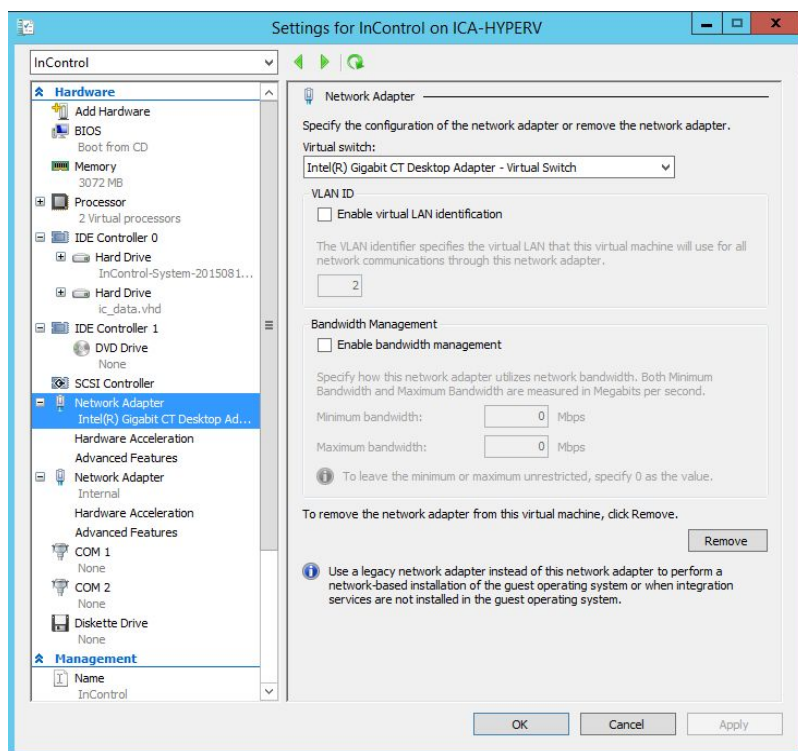
In the Hyper-V Manager, create 2 new Virtual Machines called **DB** and **InControl** for Ubuntu Linux (64 bit) guest operating systems. Our test was on first generation VMs. For the DB VM, you need only one network connection on the Internal network. For the InControl VM, you'll need the WAN network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



DB VM:



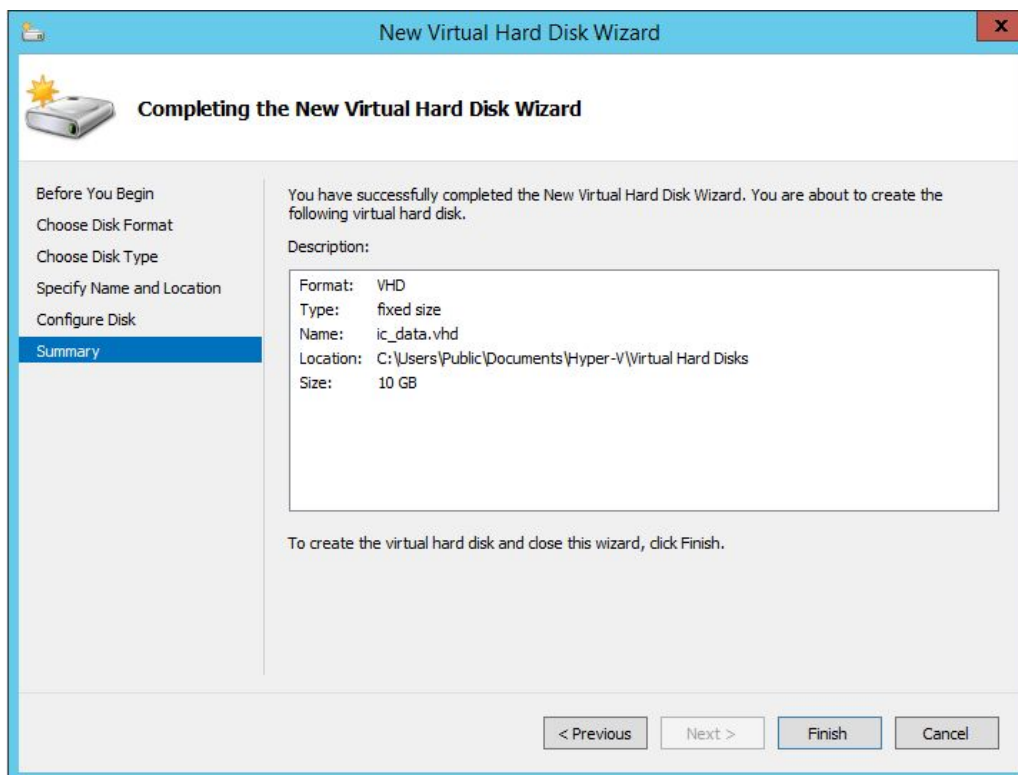
InControl VM:



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 at 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 Control Panel

System Settings	
Product	InControl Appliance (Software)
Appliance Version	2.5.2
Software Version	2.5.2
Serial Number	N/A
Domain	<input type="text" value="my.domain"/>
URL Host Name	<input type="text" value="incontrol.my.domain"/> <small>(Must be a subdomain of "Domain")</small>
Company Name	<input type="text" value="My Company"/>
Service Name	<input type="text" value="My Company InControl"/>
System Admin E-mail Address	<input type="text" value="noreply@my.domain"/>
Tech Support E-mail Address	<input type="text" value="support@my.domain"/>
Notification E-mail Sender Name	<input type="text" value="My Company InControl"/>
Notification Sender E-mail Address	<input type="text" value="noreply@my.domain"/>

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 Device ID 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	
Device ID	60110569E07ACFAE11E757F7783144F7
License Key	<input type="text"/> <input type="button" value="Submit"/>
Max. Number of Managed Devices	N/A
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.

On your PC, assign it with a static IP address which is accessible to the port's. 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 Control Panel

System Settings	
Software Version	
Serial Number	N/A
Domain	<input type="text" value="mydomain.com"/>
URL Host Name	<input type="text" value="incontrol.mydomain.com"/>
Company Name	<input type="text" value="My Company"/>
Service Name	<input type="text" value="My Company InControl"/>
System Admin Email Address	<input type="text" value="sysadmin@mydomain.com"/>
Tech Support Email Address	<input type="text" value="support@mydomain.com"/>
Notification Email Sender Name	<input type="text" value="My Company InControl"/>
Notification Sender Email Address	<input type="text" value="noreply@mydomain.com"/>
Web Server SSL Certification	<div> <div>1UE</div> <div>AxMMbXlkb21haW4uY29tMB4XDTE0MDk</div> <div>yNTFvMDRvMFE0XDTF1MDkxNTFvMDRvM</div> </div>

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	
Device ID	60110569E07ACFAE11E757F7783144F7
License Key	<input type="text"/> <input type="button" value="Submit"/>
Max. Number of Managed Devices	N/A
Expiry Date	N/A

2.3 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	<input type="text" value="smtp.my.domain"/>
SMTP Port	<input type="text" value="587"/>
SMTP Username	<input type="text" value="smtp-user"/>
SMTP Password	<input type="password" value="....."/>
SMTP Authentication	<input type="button" value="Login"/> ▾
SMTP HELO Domain	<input type="text" value="mydomain.com"/>
Testing E-mail Address	<input type="text"/> <input type="button" value="Test"/>
Testing E-mail Delivery Status	<i>Note: Save E-mail Delivery Settings before testing.</i>

2.4 Input FTP/SFTP Archive Server Settings

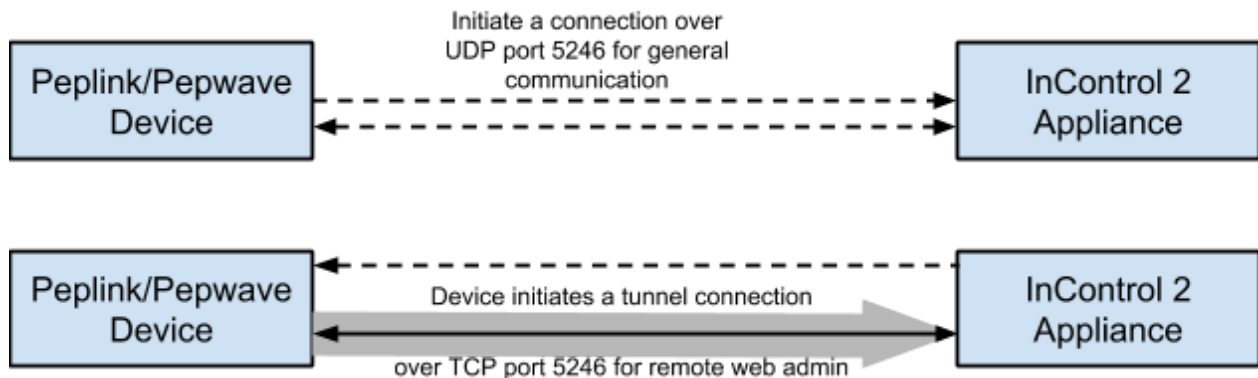
As a relational database is not good at storing bulky data, so historical event log events, GPS locations, and cellular signal data are only kept in the MySQL database for 7 days. When an FTP or SFTP server is defined, the system will archive the data to the server daily before removing. When the data 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 setup an FTP/SFTP archive server for storing those historical data.

2.5 Facebook App Settings (for Captive Portal)

Please refer to chapter [13 Facebook App ID Creation Procedure](#) for how to acquire a Facebook app ID.

3. 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).

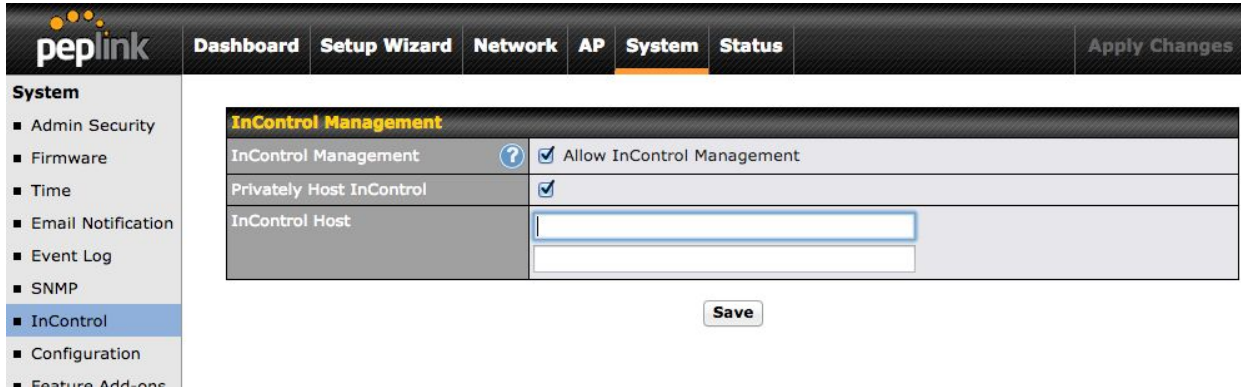


There are two ways to tell your Peplink/Pepwave devices to report to your InControl appliance instead of the Peplink InControl in the public cloud.

Method 1: By configuring devices individually - for Internet isolated environment

Login to the devices' web admin and put your InControl's WAN IP address or host name to it. If a host name 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.

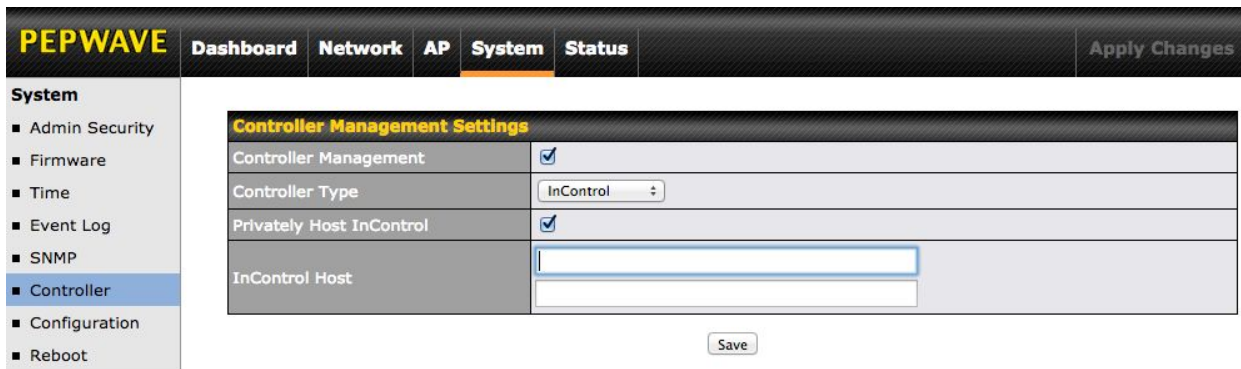


The screenshot shows the Peplink web admin interface. The top navigation bar includes 'Dashboard', 'Setup Wizard', 'Network', 'AP', 'System' (highlighted), and 'Status'. An 'Apply Changes' button is on the right. The left sidebar lists 'System' settings: Admin Security, Firmware, Time, Email Notification, Event Log, SNMP, InControl (highlighted), Configuration, and Feature Add-ons. The main content area is titled 'InControl Management' and contains a table with the following rows:

InControl Management	
InControl Management	<input checked="" type="checkbox"/> Allow InControl Management
Privately Host InControl	<input checked="" type="checkbox"/>
InControl Host	<input type="text"/>

A 'Save' button is located at the bottom right of the settings area.

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



The screenshot shows the PEPWAVE web admin interface. The top navigation bar includes 'Dashboard', 'Network', 'AP', 'System' (highlighted), and 'Status'. An 'Apply Changes' button is on the right. The left sidebar lists 'System' settings: Admin Security, Firmware, Time, Event Log, SNMP, Controller (highlighted), Configuration, and Reboot. The main content area is titled 'Controller Management Settings' and contains a table with the following rows:

Controller Management Settings	
Controller Management	<input checked="" type="checkbox"/>
Controller Type	InControl
Privately Host InControl	<input checked="" type="checkbox"/>
InControl Host	<input type="text"/>

A 'Save' button is located at the bottom right of the settings area.

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 environment

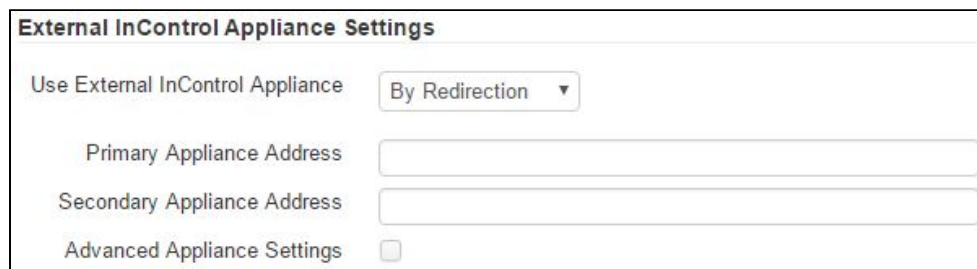
If your devices are accessible to both the Internet and your InControl appliance, you can follow this method. First, sign in to <https://incontrol2.peplink.com/>. Create an organization and a group by following the on-screen instructions. Add your devices to the group. Then go to the Group Settings page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



The screenshot shows the 'External InControl Appliance Settings' section. The 'Use External InControl Appliance' dropdown menu is open, displaying four options: 'By Redirection', 'Disabled', 'By Redirection', and 'By Configuration'. The 'Disabled' option is currently selected and highlighted in blue.

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.



The screenshot shows the 'External InControl Appliance Settings' form. The 'Use External InControl Appliance' dropdown is set to 'By Redirection'. Below this, there are two text input fields for 'Primary Appliance Address' and 'Secondary Appliance Address'. At the bottom, there is a checkbox for 'Advanced Appliance Settings' which is currently unchecked.

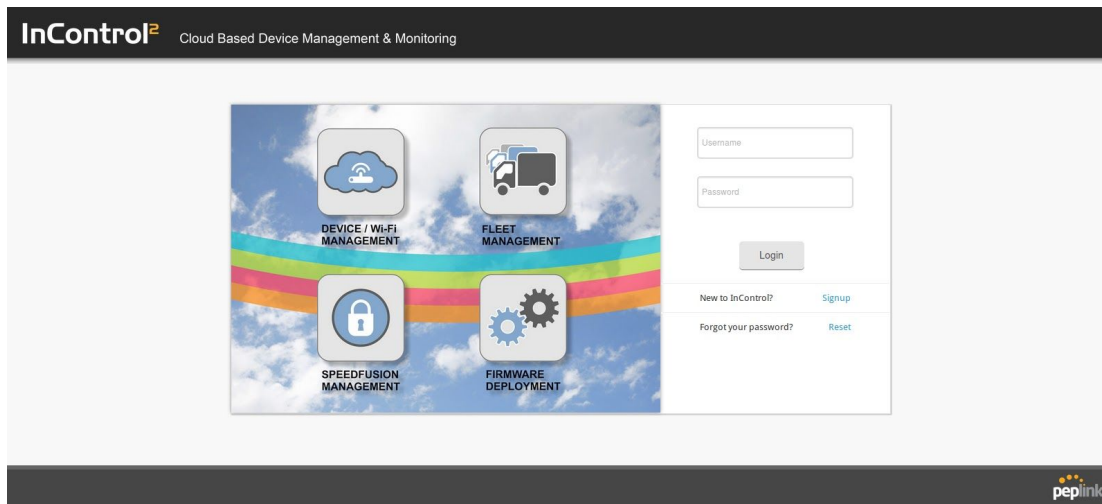
If you choose **By Configuration**, your InControl Appliance address(es) will be saved persistently to your devices. After your device received the setting, they will connect to your InControl Appliance directly on start up without connecting to Peplink InControl. The appliance address will be lost if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



The screenshot shows the 'External InControl Appliance Settings' form. The 'Use External InControl Appliance' dropdown is set to 'By Configuration'. Below this, there are two text input fields for 'Primary Appliance Address' and 'Secondary Appliance Address'. A note is displayed: 'Note: If this field left blank, devices will be configured to connect to Peplink InControl in the public cloud'. Below the input fields, there is a checkbox for 'Fail over to Peplink InControl in Public Cloud' which is currently unchecked. At the bottom, there is a checkbox for 'Advanced Appliance Settings' which is currently unchecked.

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

4. Logging Into InControl Appliance Web Site

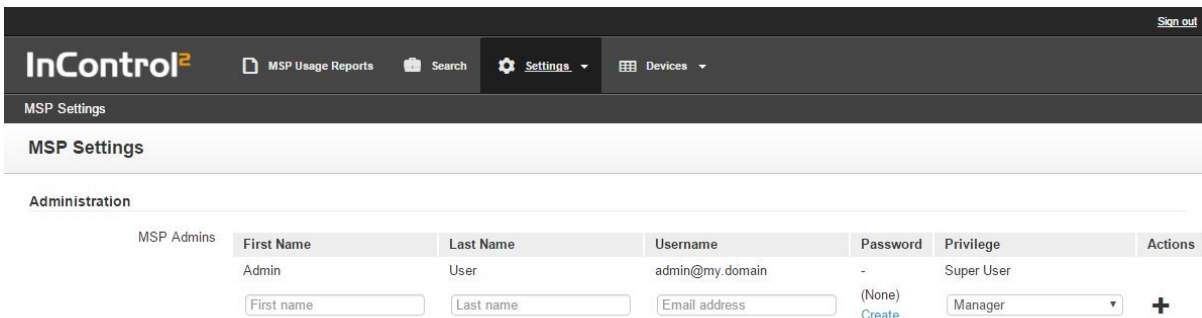


In order to access the InControl web site, you must visit its host name instead of its IP address. Your PC is required to resolve the host name into the server IP address. You may add a local DNS record to your PC by editing its “hosts” file. It is “%SystemRoot%\System32\drivers\etc\hosts” for Windows or “/etc/hosts” for Mac and Linux. Assuming 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 web site from the PC's web browser. By default, the InControl's URL is <https://incontrol.my.domain/>. The default username is **admin@my.domain** 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.



First Name	Last Name	Username	Password	Privilege	Actions
Admin	User	admin@my.domain	-	Super User	

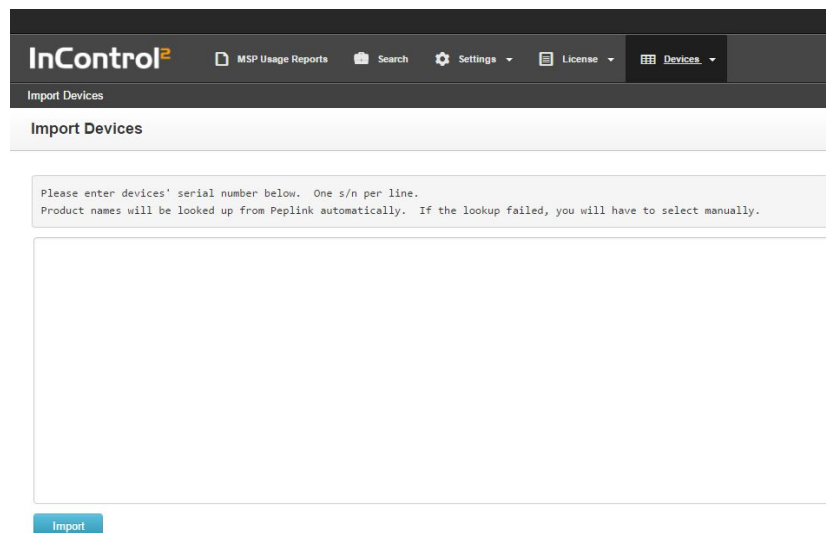
First name Last name Email address (None) Manager + Create

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

5. 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 web site, navigate to "Devices" > "Import Devices".

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



Please enter devices' serial number below. One s/n per line.
Product names will be looked up from Peplink automatically. If the lookup failed, you will have to select manually.

Import

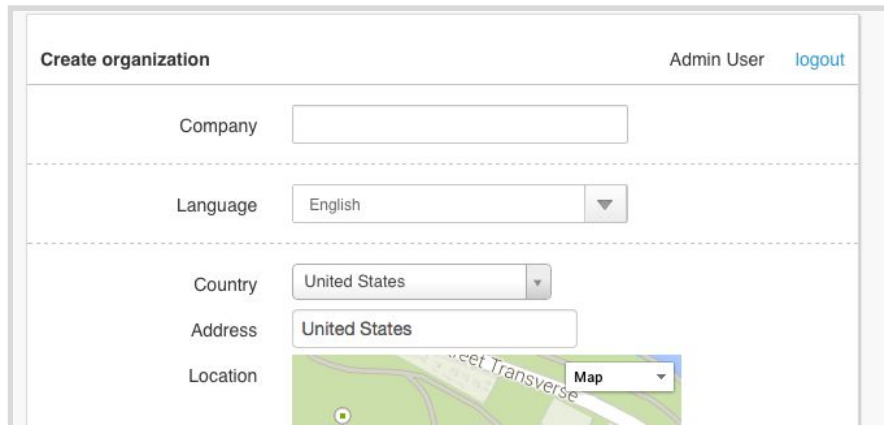
InControl Appliance will attempt to query Peplink server what products the serial numbers are. If success, the devices will be imported. If not, you will be prompted to select each device's product name.

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

6. Creating an Organization, Group and Adding Devices

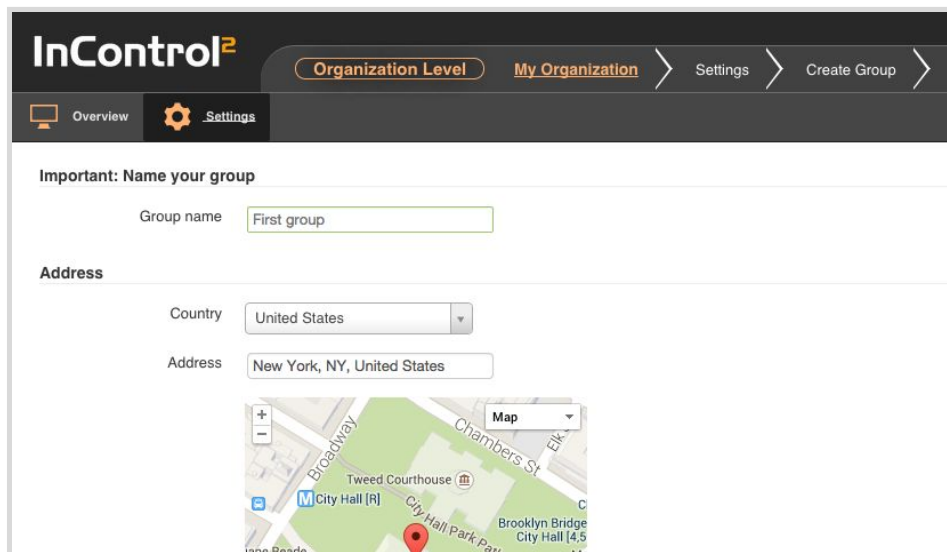
An organization is pre-created which is called “My Organization”. You can find it on the MSP Reports page.

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”.



The screenshot shows the 'Create organization' form. At the top right, it says 'Admin User' and 'logout'. The form has several fields: 'Company' (text input), 'Language' (dropdown menu set to 'English'), 'Country' (dropdown menu set to 'United States'), 'Address' (text input set to 'United States'), and 'Location' (a map with a red pin and a 'Map' dropdown menu). The map shows a street labeled 'Sweet Transverse'.

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



The screenshot shows the 'Create Group' page in the InControl 2 interface. The top navigation bar includes 'Organization Level', 'My Organization', 'Settings', and 'Create Group'. Below the navigation bar, there are tabs for 'Overview' and 'Settings'. The main content area is titled 'Important: Name your group'. It has a 'Group name' field with the text 'First group'. Below that, there is an 'Address' section with a 'Country' dropdown menu set to 'United States' and an 'Address' text input set to 'New York, NY, United States'. At the bottom, there is a map showing a location in New York City, with a red pin and a 'Map' dropdown menu. The map shows streets like Broadway, Chambers St, and City Hall Park.

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

Group **First group** is created. You may add devices to this group.

Add Devices Into Groups

Group type	Peplink / Pepwave
Serial numbers: (Comma, space or carriage return separated)	<div>e.g.: XXXX-XXXX-XXXX</div>
<div>SubmitCancel</div>	

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

7. API Access

An API is available for software developers to programmatically retrieve the data as you see on the InControl appliance's web site. You can visit

`https://{incontrol.address}/api/restful_api` for the API documentation and testing tool.

8. Settings on Your Firewall

Please allow the following traffic to pass through if a firewall is setup 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
	download.peplink.com on TCP 443	Device firmware validation
	api.ic.peplink.com on TCP 443	Product name lookup when importing devices Latest device firmware updates
	push.ic.peplink.com on TCP 443 (NEW)	Push notifications for the InControl 2 app (optional)
	*.letsencrypt.org on TCP 443	Automatic SSL certificate acquisition from letsencrypt.org (optional)
	*.peplink.com on UDP 5246 (NEW) (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

8.1 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

9. Upgrading InControl Virtual Appliance

9.1 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 2.5.2 as an example. The extracted file names and sizes are as follow:

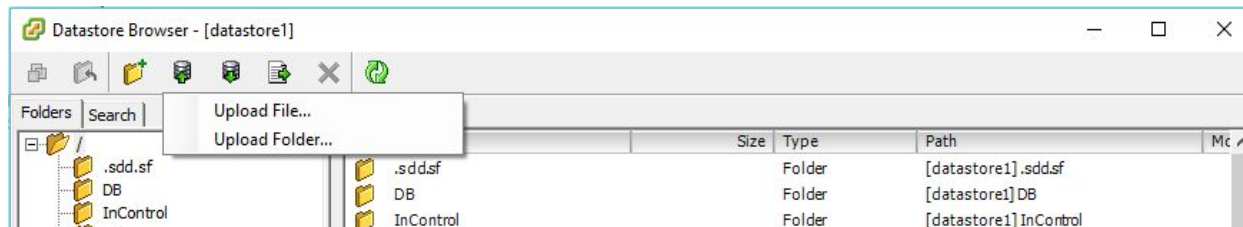
InControl-System-2.5.2.tgz:

File name	Size (Bytes)
InControl-System-2.5.2/InControl-System-20171101-flat.vmdk	10,487,808
InControl-System-2.5.2/InControl-System-20171101.vmdk	575

DB-System-20170622.tgz:

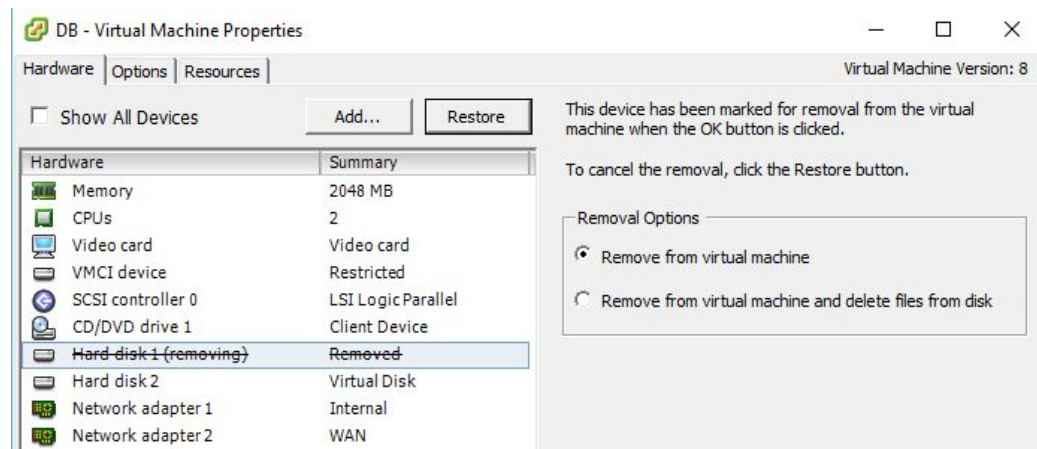
File name	Size (Bytes)
DB-System-20170622/DB-System-20170622-flat.vmdk	10,737,418,240
DB-System-20170426/DB-System-2017622.vmdk	568

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-2.5.2" 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.



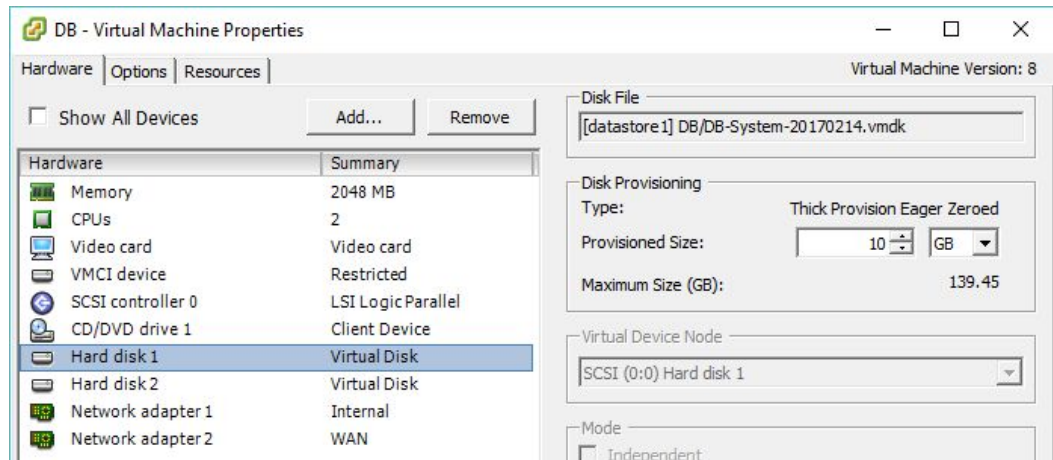
Step 4. Restart VMs in the following order:

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"

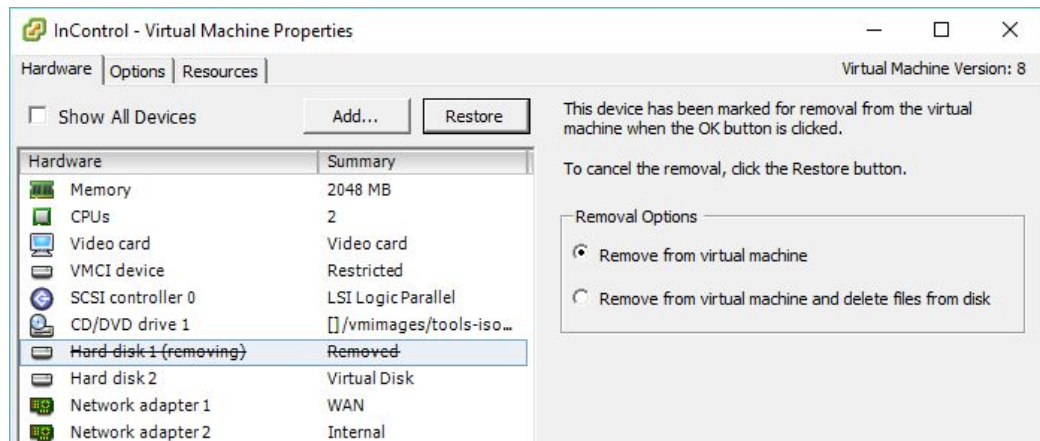
- Select SCSI 0:0 Hard disk as the Virtual Device Node



5. Start DB VM

6. Open InControl VM Properties

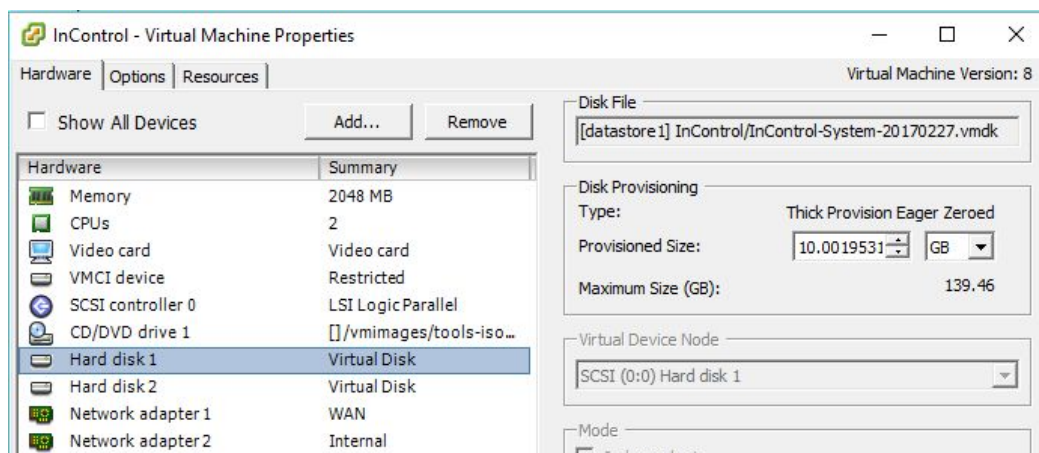
- Identify and select the system hard disk (usually "Hard disk 1")
- Select the "Remove from virtual machine" radio button (without deleting it)
- Press "OK"



7. Open InControl VM properties again

- Select 'Add...' > "Existing virtual disk..." > Browse and select the disk file "InControl-a.b.c/InControl-System-xxx-yyyymmdd.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.

9.2 For Microsoft Hyper-V

Step 1. Download the latest Virtual Appliance and Database Server image files in .vhd format from

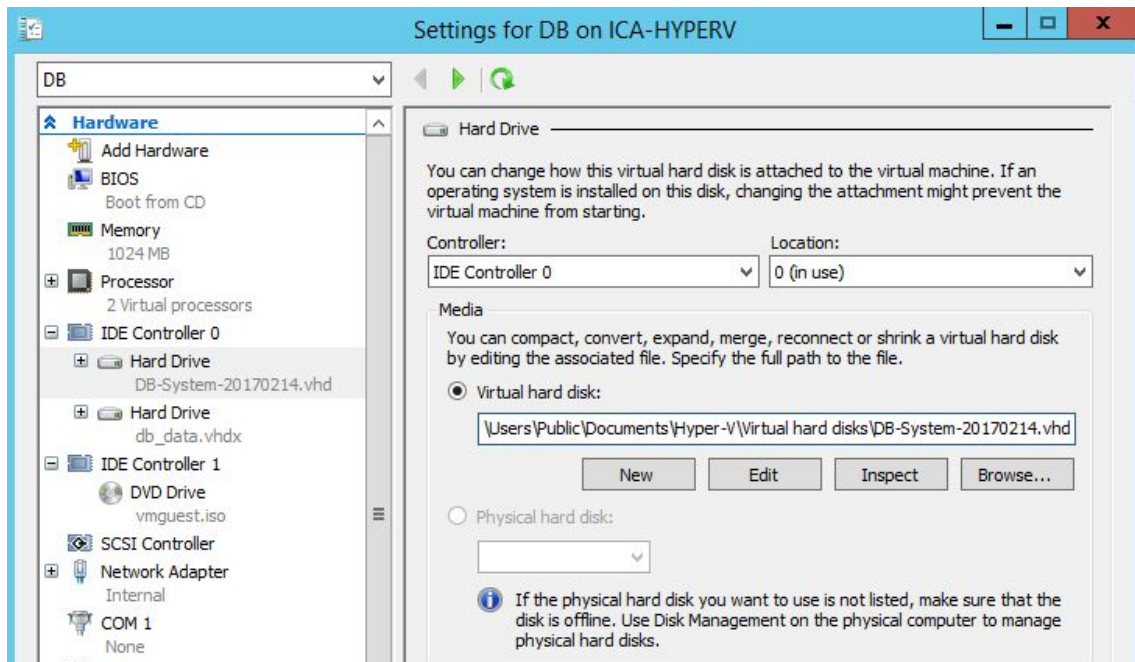
<https://www.peplink.com/support/downloads/incontrol-appliance-image-and-installation-guide/>

Take InControl 2.5.2 as an example. The .vhd file names and sizes are as follow:

File name	Size (Bytes)
InControl-System-2.5.2-20171101.vhd	8,606,732,800
DB-System-2.4.0-20170644.vhd	4,297,073,152

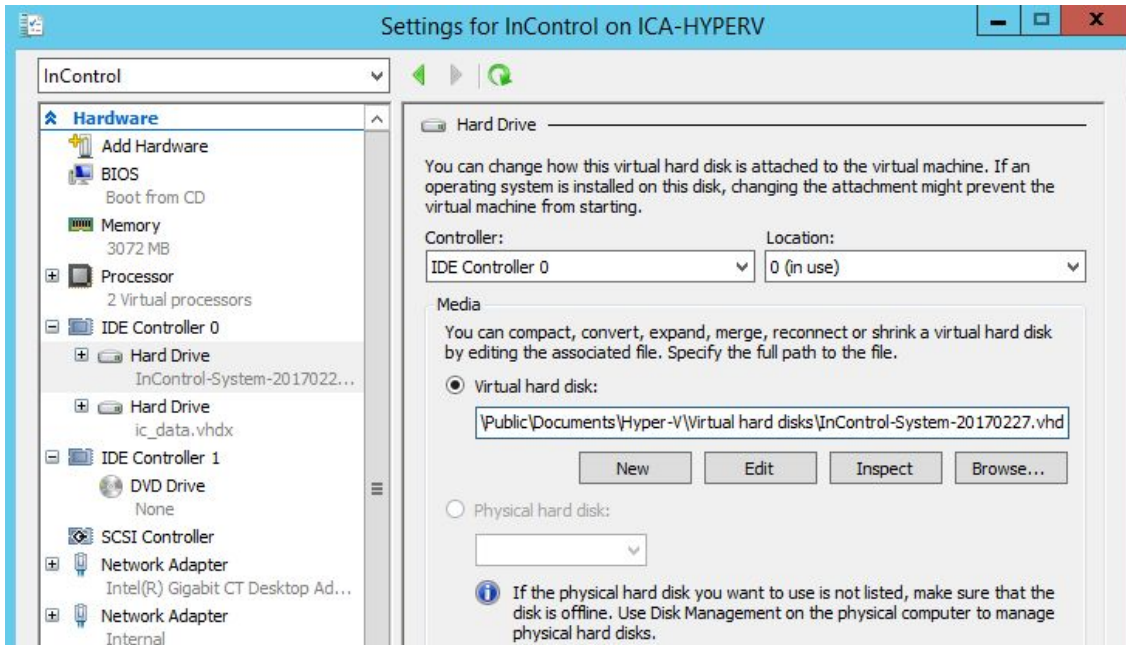
Step 2. Deployment

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-yyyyymmdd.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-yyyymmdd.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!

10. 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.

InControl Upgrade		
Firmware URL	<input type="text"/>	<input type="button" value="Upgrade"/>
	Example: https://mydomain.com/firmware-1.0.img	
Firmware Fetching Status	<input type="text"/>	
Firmware Upgrade Status	<input type="text"/>	

Note: Upgrading firmware will take about 25 mins.

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.

Please note that the system will download the firmware via the management port. So please make sure management port settings are correctly set. If the management network does not have Internet connectivity, you will have to download the firmware file locally and then put it to a local web server on the management network. Then input the firmware's local URL to the Firmware URL field.

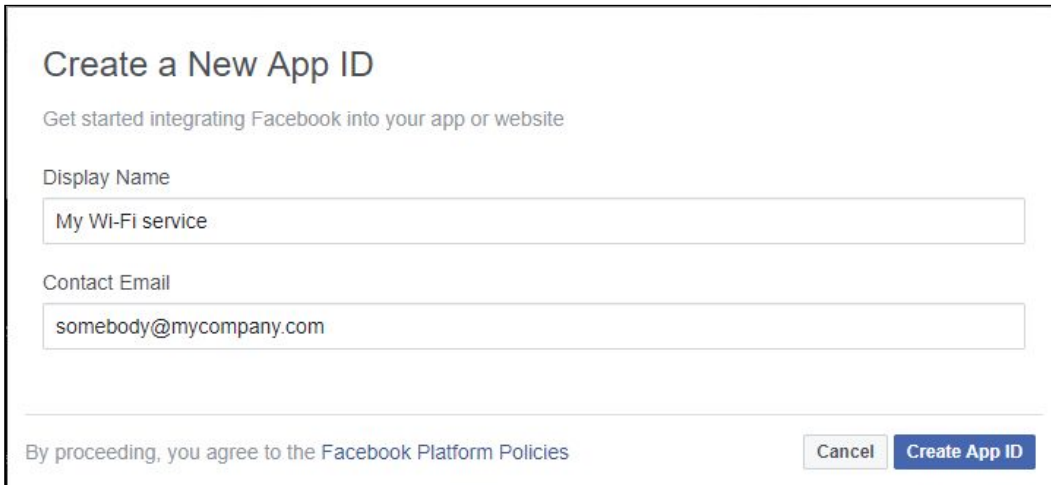
11. Facebook App ID Creation Procedure

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 has 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 to <https://developers.facebook.com/> and choose to "add a new app".

2. Enter a Display Name and Contact Email. Click the “Create App ID” button.



Create a New App ID

Get started integrating Facebook into your app or website

Display Name

My Wi-Fi service

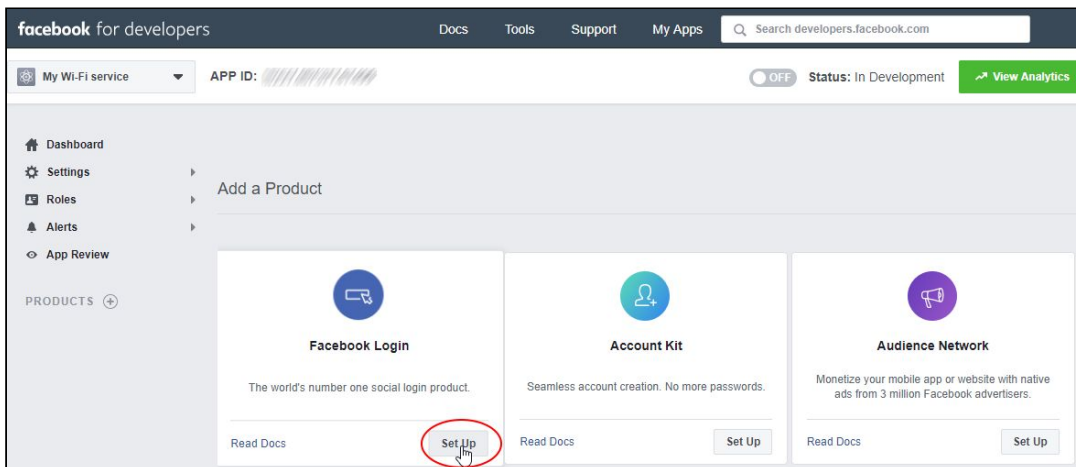
Contact Email

somebody@mycompany.com

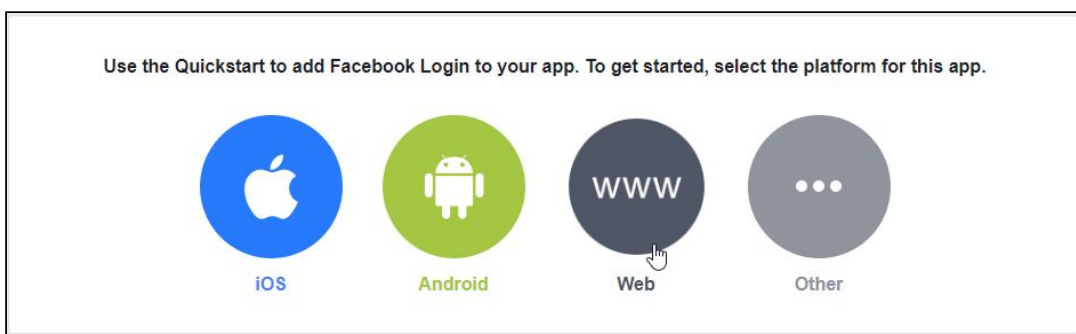
By proceeding, you agree to the Facebook Platform Policies

Cancel Create App ID

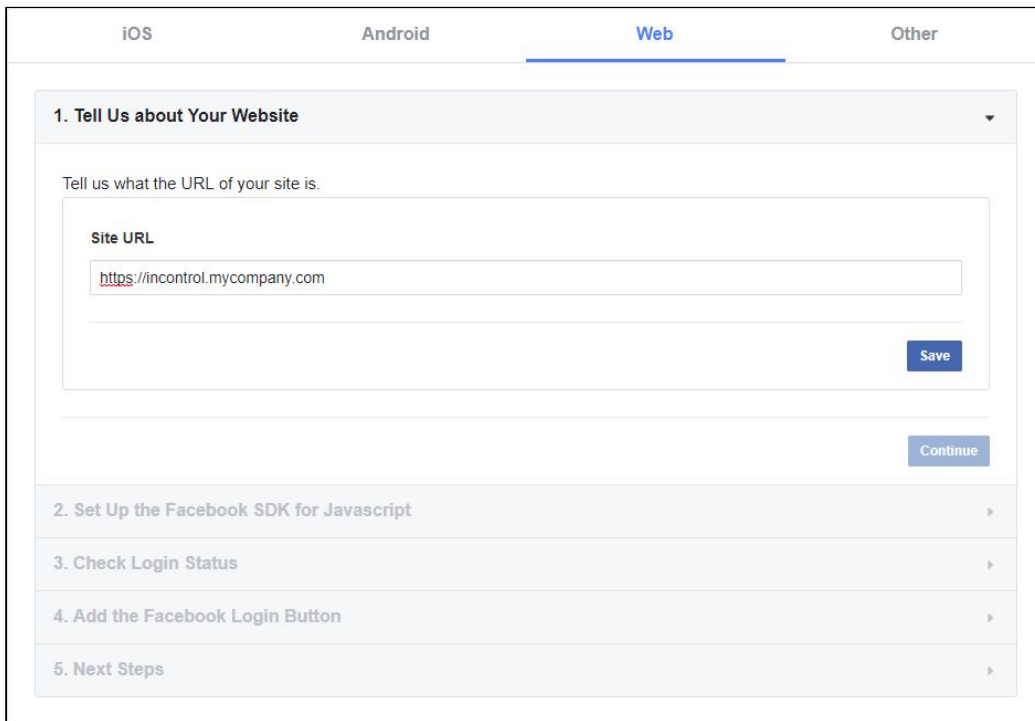
3. Click the “Set Up” button on the Facebook Login control



4. Click “Web”



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



iOS Android **Web** Other

1. Tell Us about Your Website

Tell us what the URL of your site is.

Site URL

Save

Continue

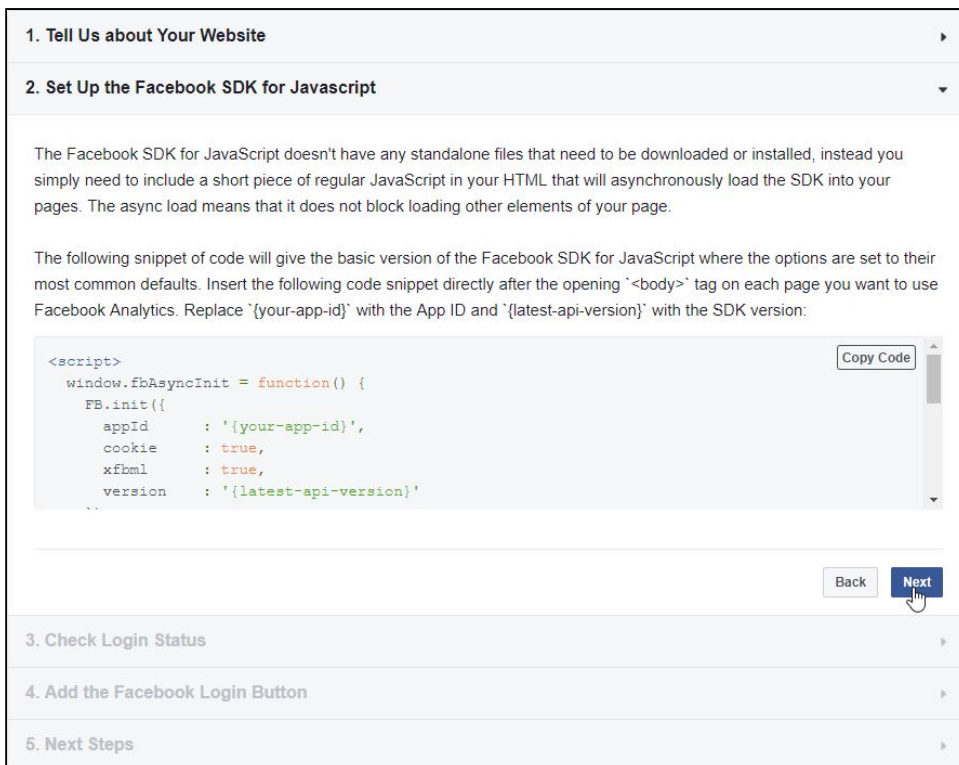
2. Set Up the Facebook SDK for Javascript

3. Check Login Status

4. Add the Facebook Login Button

5. Next Steps

6. Click "Next".



1. Tell Us about Your Website

2. Set Up the Facebook SDK for Javascript

The Facebook SDK for JavaScript doesn't have any standalone files that need to be downloaded or installed, instead you simply need to include a short piece of regular JavaScript in your HTML that will asynchronously load the SDK into your pages. The async load means that it does not block loading other elements of your page.

The following snippet of code will give the basic version of the Facebook SDK for JavaScript where the options are set to their most common defaults. Insert the following code snippet directly after the opening `` tag on each page you want to use Facebook Analytics. Replace `{your-app-id}` with the App ID and `{latest-api-version}` with the SDK version:

```
<script>
window.fbAsyncInit = function() {
  FB.init({
    appId      : '{your-app-id}',
    cookie     : true,
    xfbml     : true,
    version    : '{latest-api-version}'
  })
}
```

Copy Code

Back **Next**

3. Check Login Status

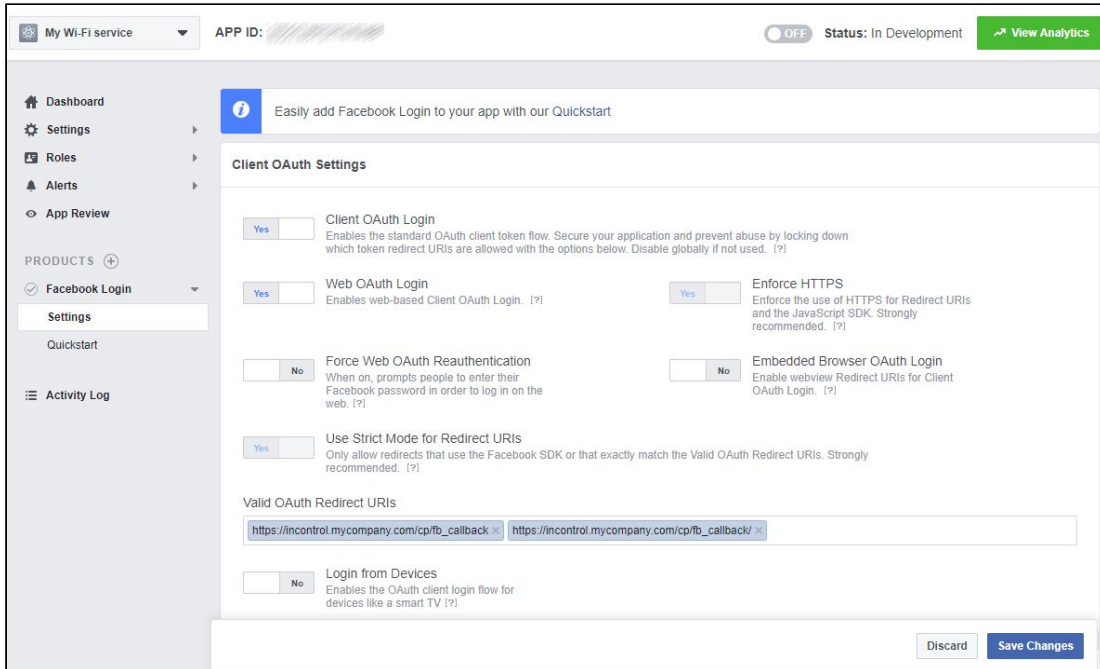
4. Add the Facebook Login Button

5. Next Steps

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/`



My Wi-Fi service APP ID: [REDACTED] OFF Status: In Development View Analytics

Dashboard Settings Roles Alerts App Review

PRODUCTS +

Facebook Login Settings Quickstart Activity Log

Client OAuth Settings

☒ Client OAuth Login
Enables the standard OAuth client token flow. Secure your application and prevent abuse by locking down which token redirect URIs are allowed with the options below. Disable globally if not used. [?]

☒ Web OAuth Login
Enables web-based Client OAuth Login. [?]

☒ Enforce HTTPS
Enforce the use of HTTPS for Redirect URIs and the JavaScript SDK. Strongly recommended. [?]

☐ Force Web OAuth Reauthentication
When on, prompts people to enter their Facebook password in order to log in on the web. [?]

☐ Embedded Browser OAuth Login
Enable webview Redirect URIs for Client OAuth Login. [?]

☒ Use Strict Mode for Redirect URIs
Only allow redirects that use the Facebook SDK or that exactly match the Valid OAuth Redirect URIs. Strongly recommended. [?]

Valid OAuth Redirect URIs

https://incontrol.mycompany.com/cp/fb_callback https://incontrol.mycompany.com/cp/fb_callback/

☐ Login from Devices
Enables the OAuth client login flow for devices like a smart TV [?]

Discard Save Changes

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

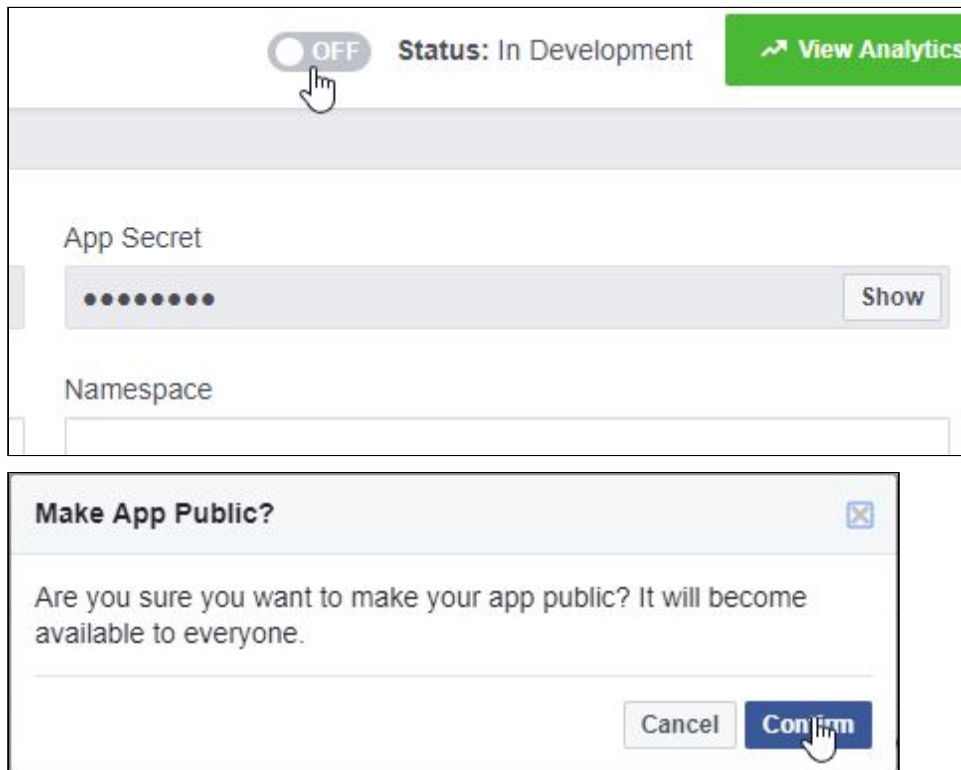
The screenshot shows the 'My Wi-Fi service' app configuration page. The left sidebar contains navigation links: Dashboard, Settings (Basic, Advanced), Roles, Alerts, App Review, PRODUCTS (Facebook Login), and Activity Log. The main content area has the following fields:

- App ID: [Redacted]
- App Secret: [Redacted] (Show button)
- Display Name: My Wi-Fi service
- Namespace: [Empty]
- App Domains: [Empty]
- Contact Email: somebody@mycompany.com
- Privacy Policy URL: http://www.mycompany.com/privacy/
- Terms of Service URL: Terms of Service for Login dialog and App Details
- App Icon (1024 x 1024): [Wi-Fi icon placeholder]
- Category: Entertainment (dropdown menu)
- Business Use: This app uses Facebook tools or data to
 - ☐ Support my own business
 - ☐ Provide services to other businesses
- Website: [Empty] (Quick Start button)
- Site URL: https://incontrol.mycompany.com/
- + Add Platform button
- Discard and Save Changes buttons

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.

This screenshot is a zoomed-in view of the App ID and App Secret fields. The App ID is [Redacted]. The App Secret is [Redacted] with a 'Show' button next to it. A mouse cursor is pointing at the 'Show' button.

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



12. Release Notes

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 be 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 is 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 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 portal.
- 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 situation, 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 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 is 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 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.

