InControl 2 Appliance Setup Guide

for Appliance Software 2.10.0

(Last updated: 2022-05-27)

Contents

1. Virtual Appliance
    - 1.1 Introduction
    - 1.2 Hardware Requirements
    - 1.3 Installation on VMware ESXi
        - Requirement
        - Networking
        - Creating InControl and DB VMs
    - 1.4 Installation on Microsoft Hyper-V
        - Networking
        - Creating InControl and DB VMs
        - Uploading and Adding data storage to the VMs
        - Powering up VMs
    - 1.5 Installation on AWS
        - 1.5.1 Preparing AMIs
            - 1.5.1.1 For general AWS regions
            - 1.5.1.2 For AWS GovCloud
                - Uploading the images to S3 Bucket
                - Creating the required import role and policy
                - Importing the AMI to AWS
        - 1.5.2 Setting up network
        - 1.5.3 Setting up security groups
        - 1.5.4 Setting up Route 53 Hosted private zone
        - 1.5.5 Creating DNS update role
        - 1.5.6 Launching instances
            - 1.5.6.1 For general AWS regions
            - 1.5.6.2 For AWS GovCloud
        - 1.5.7 Associate Elastic IP address
        - 1.5.8 Reset control panel admin password on AWS

1.6 Installation on Google Cloud Platform
1.6.1 Uploading the image
1.6.2 Importing the image
1.6.3 Setting up the firewall
1.6.4 Creating the instances
1.7 Accessing the Control Panel
1.8 IP Address Configuration and Password Reset Over the Console
1.9 Software License
1.10 Device Expiration Date Synchronization with Peplink InControl

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 Upgrading a system newer than 2.9.0
13.2 Upgrading a system earlier than 2.9.0

13.2.1 For VMware ESXi
13.2.2 For Microsoft Hyper-V and versions prior to 2.9.0

14. Upgrading InControl Hardware Appliance

15. Release Notes
Release notes for 2.10.0
Release notes for 2.9.4.1
Release notes for 2.9.4
Release notes for 2.9.3.2
Release notes for 2.9.3.1
Release notes for 2.9.3
Release notes for 2.9.2.2
Release notes for DB-2021215
Release notes for 2.9.2.1
Release notes for 2.9.2
Release notes for 2.9.1.5
Release notes for 2.9.1.4
Release notes for 2.9.1.3
Release notes for 2.9.1.2
Release notes for 2.9.1.1
Release notes for 2.9.1
Release notes for 2.9.0.6
Release notes for 2.9.0.5
Release notes for 2.9.0.4
Release notes for 2.9.0.3
Release notes for 2.9.0.2
Release notes for DB-20210323

Appendix 1: Procedure for creating a Facebook App ID

Appendix 2: Procedure for preparing the data for setting up “Sign in with Apple”.

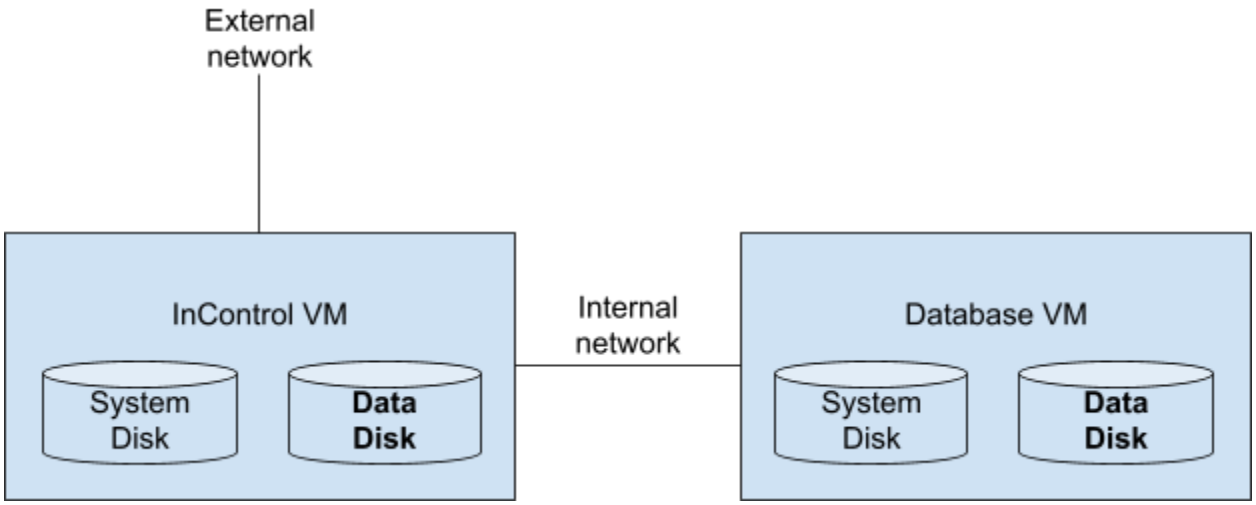
1. Virtual Appliance

1.1 Introduction

InControl 2 Virtual Appliance runs on top of a virtualization server. VMware ESXi and Microsoft Hyper-V are supported. For cloud services, Amazon Cloud Service and Google Cloud Platform are supported.

The system consists of two VMs (Virtual Machines), namely IC (InControl) VM and DB (database) VM.

For VM systems, 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 the outside.



1.2 Hardware Requirements

For up to 100 devices

	InControl VM	Database VM
CPU	Dual-core minimum. Quad-core preferred	
Memory Size	8 GB	8 GB
System Disk Size	24 GB	24 GB

Data Disk Size	20 GB	100 GB

For up to 1000 devices

	InControl VM	Database VM
CPU	Quad-core 3.4 GHz Xeon	
Memory Size	16 GB	12 GB
System Disk Size	24 GB	24 GB
Data Disk Size	30 GB	1 TB

For up to 5000 devices

	InControl VM	Database VM
CPU	16-core 3.4 GHz Xeon	
Memory Size	64 GB	32 GB
System Disk Size	24 GB	24 GB
Data Disk Size	40 GB	5 TB

The minimum memory requirement is 8 GB for the InControl VM. Systems with memory less than 8 GB are not recommended. The system stability and performance may be affected.

Important: The actual system requirement depends on not only the number of devices but also the devices' functionality and usage. E.g. GPS data availability, the number of cellular WANs, the number of client connections per hour, etc. The resource requirements for MAX models tend to be higher than those for Balance and AP One models. The above requirement figures are for average usage.

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

Requirement

The installation images have been verified to be working on VMware ESXi 6.7 and 7.0. ESXi 6.5 is not supported.

Networking

Please create two vSwitches namely “WAN” and “Internal”.

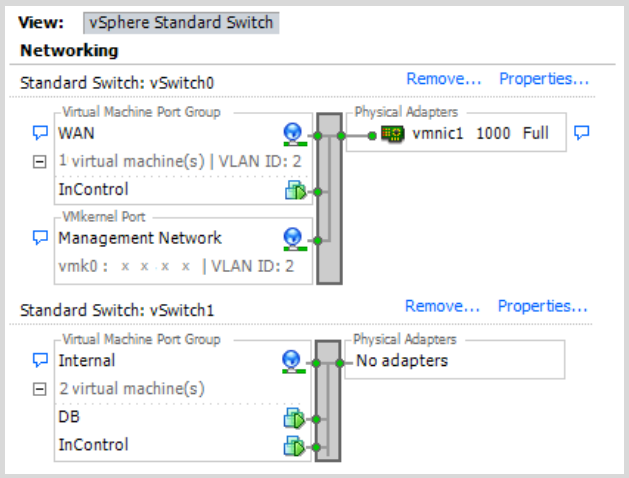
The "`WAN`" is for connecting to the outside world and will need a physical network adapter attached. The first network adapter of the InControl VM shall be assigned to this network.

The "`Internal`" 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**: As the “Internal” network segment is on the subnet 192.168.1.0/24 by default, the WAN interface cannot be on 192.168.1.0/24 too. You may change the subnet DB VM’s “Internal” interface’s IP on the console (see chapter 1.8) and change the IC VM’s Internal interface IP and the DB server setting on the control panel.

For the ESXi’s web console, navigate to “Networking” > “Port groups”.

For vSphere client, navigate to ESXi host > Configuration > Networking.



Creating InControl and DB VMs

Step 1. Download the latest Virtual Appliance and Database Server Installation Image file from https://www.peplink.com/support/incontrol-appliance-images-downloads/

Step 2. Extract the downloaded `.zip` files.

The extracted file names and sizes are as follows:

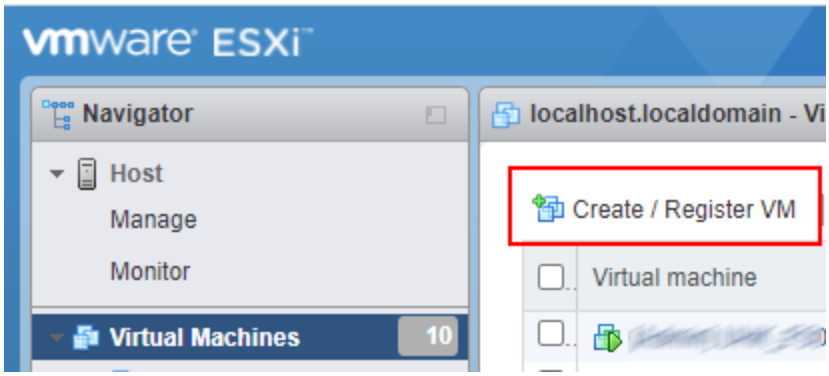
InControl-System-2.9.4.1-vmware.zip:

File name	Size (Bytes)
InControl IC VM.nvram	8,684
InControl ICA IC VM.ovf	16,136
InControl IC VM-0.vmdk	23,661,537,792
InControl IC VM-1.vmdk	70,144

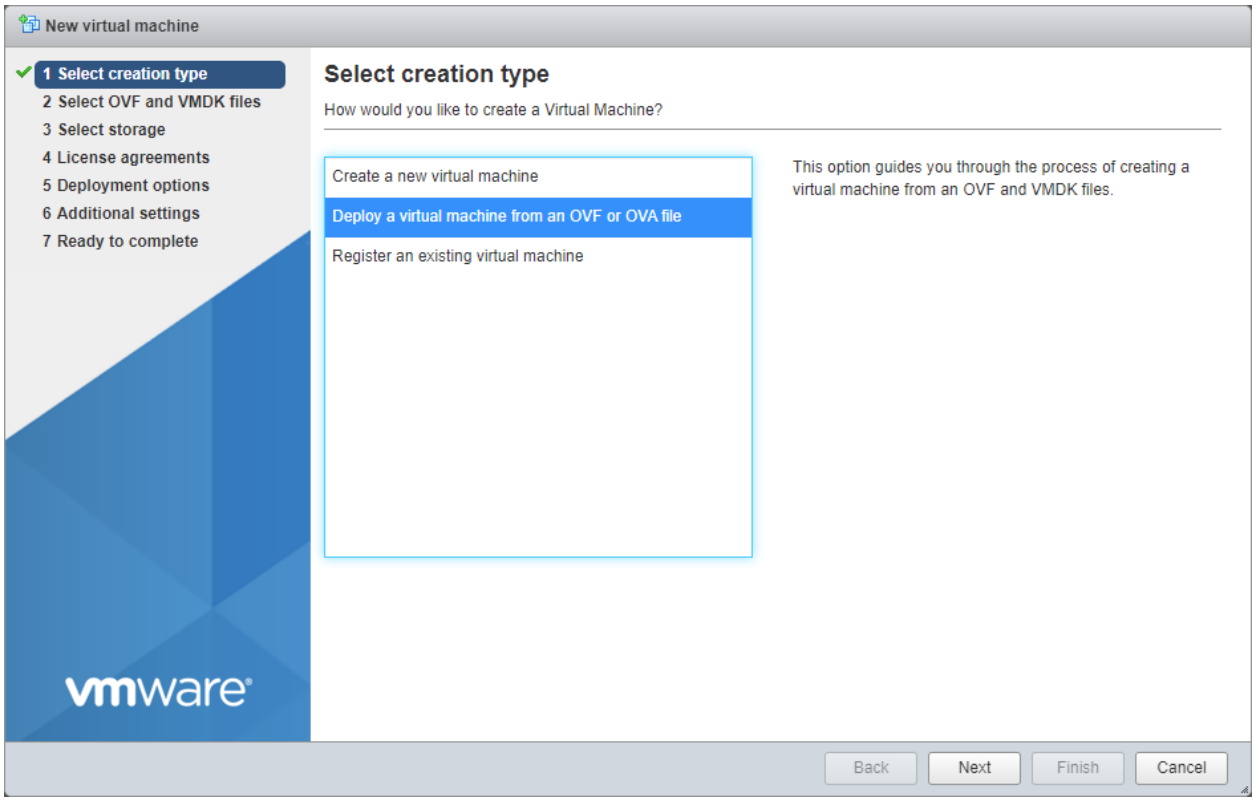
DB-System-20211215-vmware.zip:

File name	Size (Bytes)
InControl DB VM.nvram	8,684
InControl DB VM.ovf	15,217
InControl DB VM-0.vmdk	22,586,257,408
InControl DB VM-1.vmdk	80,384

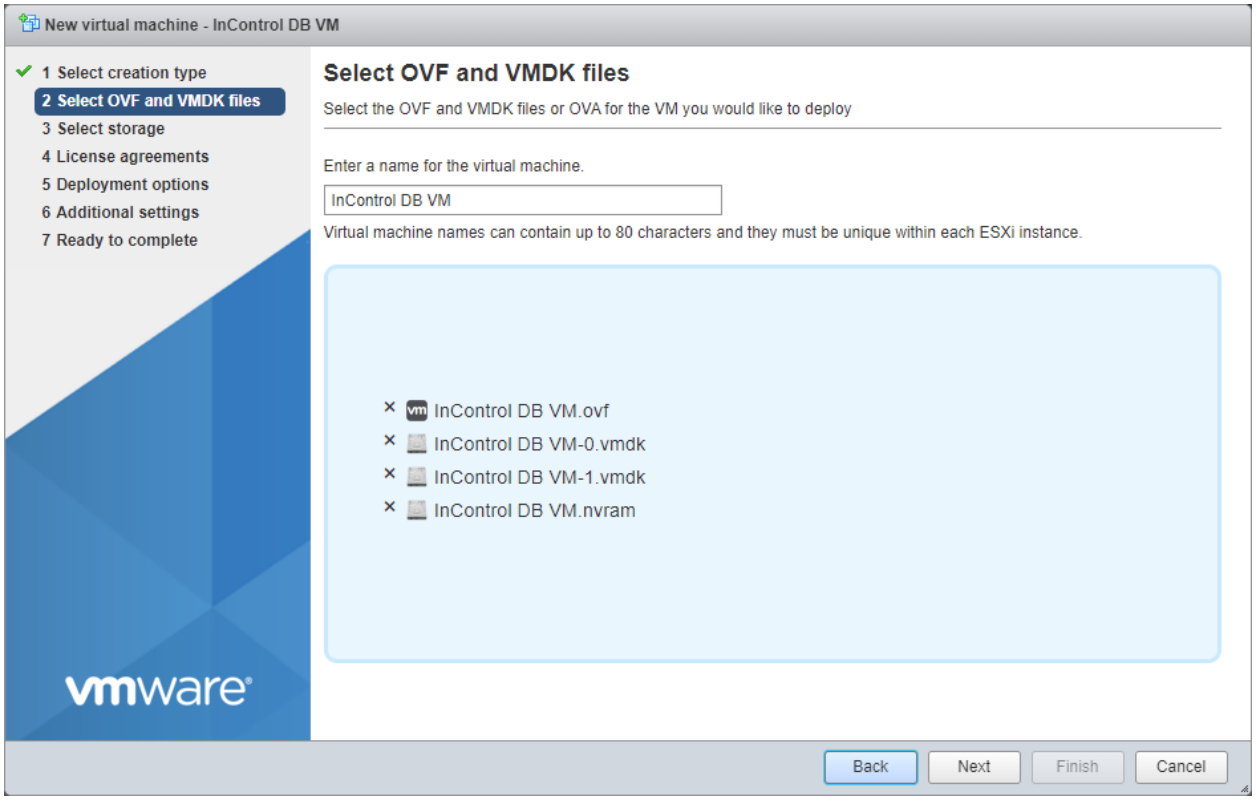
Step 3. On the ESXi web console, navigate to "Virtual Machines". Click the "Create / Register VM" button.



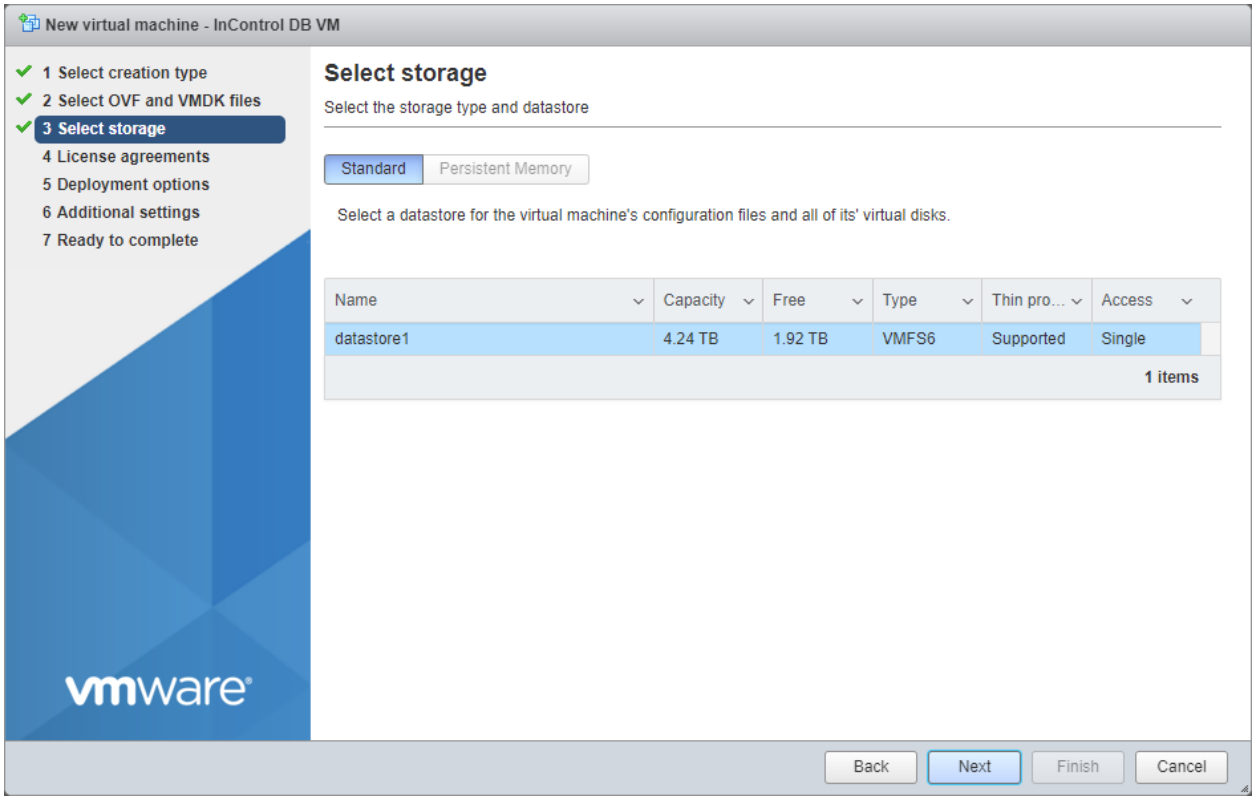
Step 4. Select the creation type "Deploy a virtual machine from an OVF or OVA file". Click "Next".



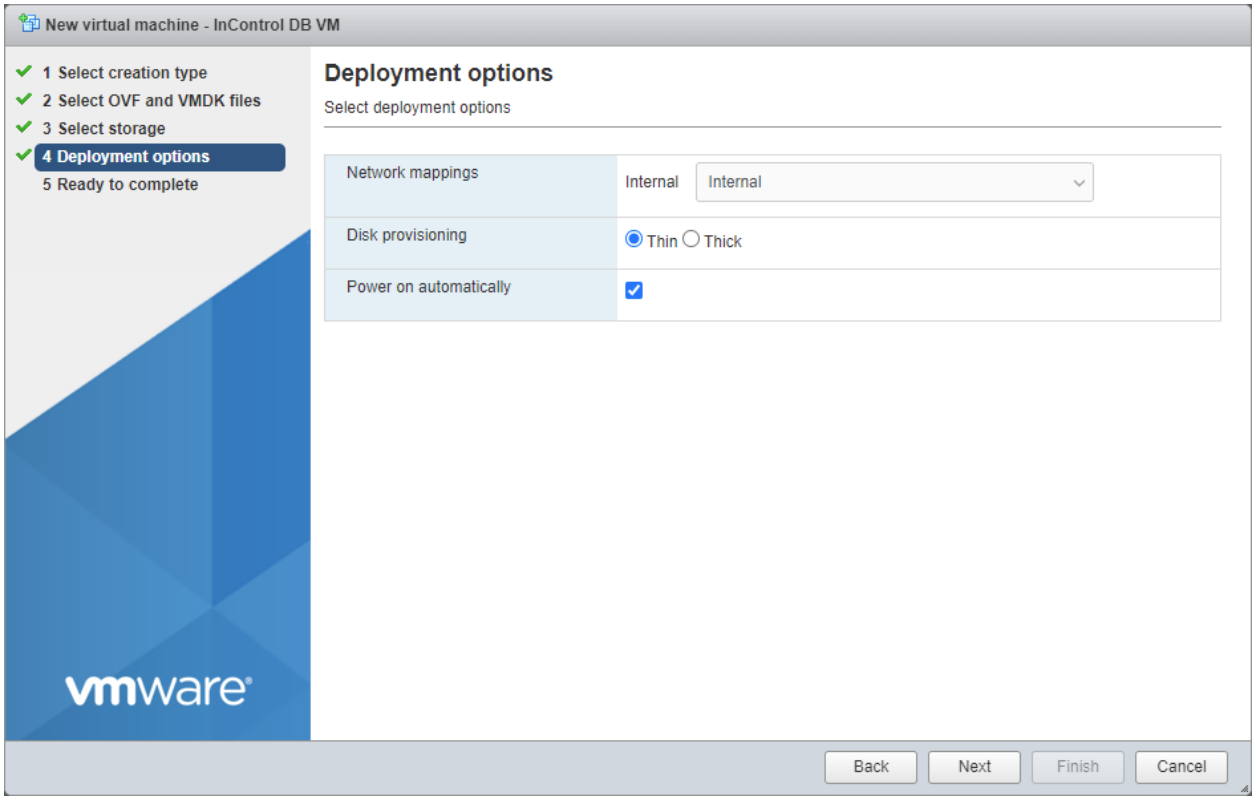
Step 5. Input a name for the virtual machine. E.g. "InControl DB VM". Drag and drop **all four files** into the drop zone. Click "Next".



Step 6. Select the storage. Click "Next".

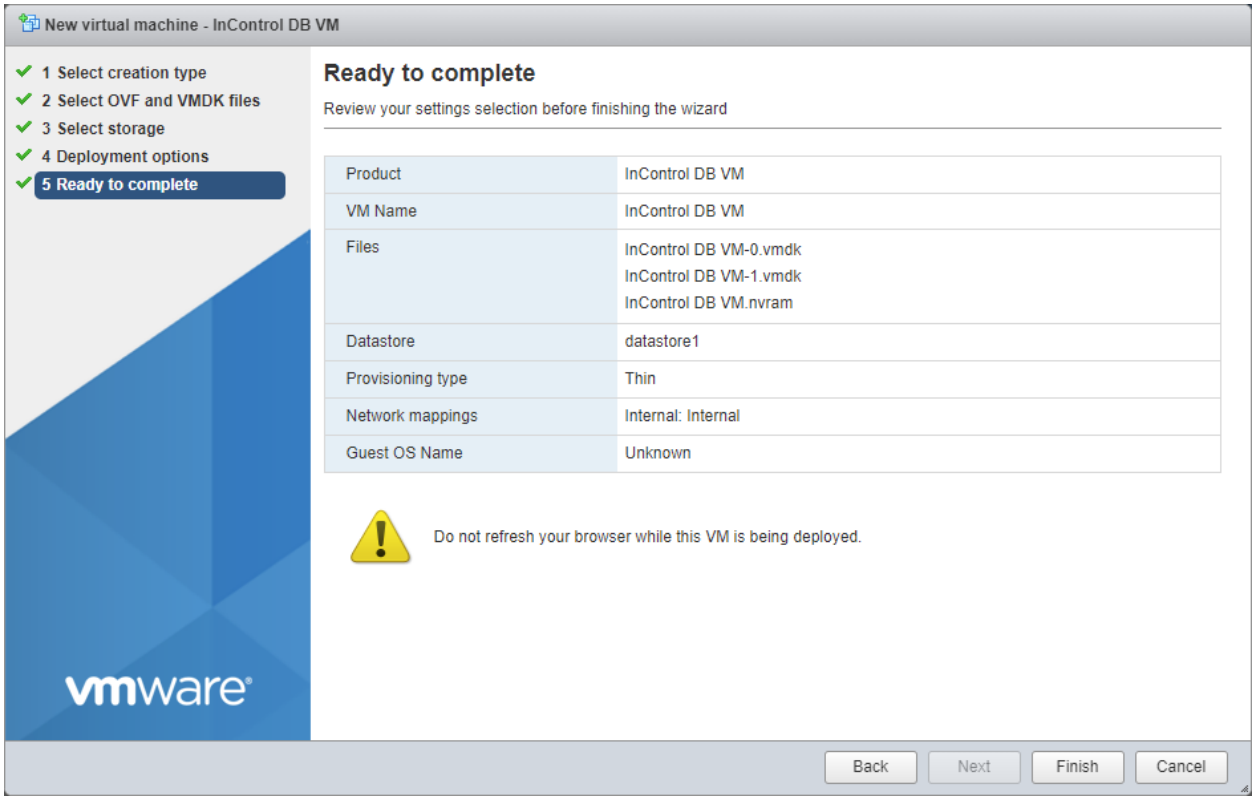


Step 7. In the Network mappings field, choose the network "`Internal`" that you created earlier. Leave the rest settings intact. Click "Next".



Step 8. Press “Finish”. The files will be uploaded. After the upload completes, the DB VM will start automatically.

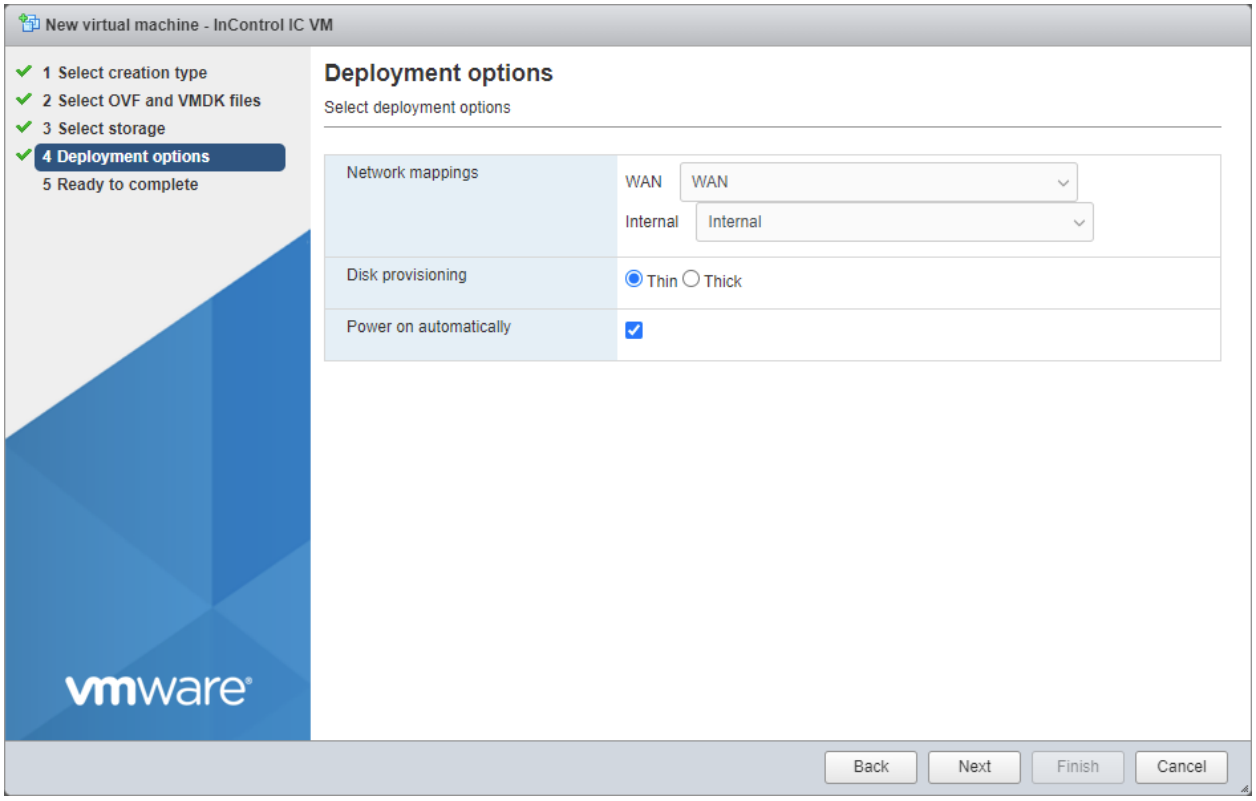
Note: You can safely ignore the error message “A required disk image was missing”. The disk will be created automatically when the VM is started.



Step 9: Repeat steps 3 to 8 for the InControl VM.

In step 5, input "InControl IC VM" as the name of the virtual machine. Drag and drop **all four files** into the drop zone.

In step 7, choose "WAN" for "WAN", "Internal" for "Internal".



The InControl VM will start automatically when the files are completely uploaded and imported.

1.4 Installation on Microsoft Hyper-V

Networking

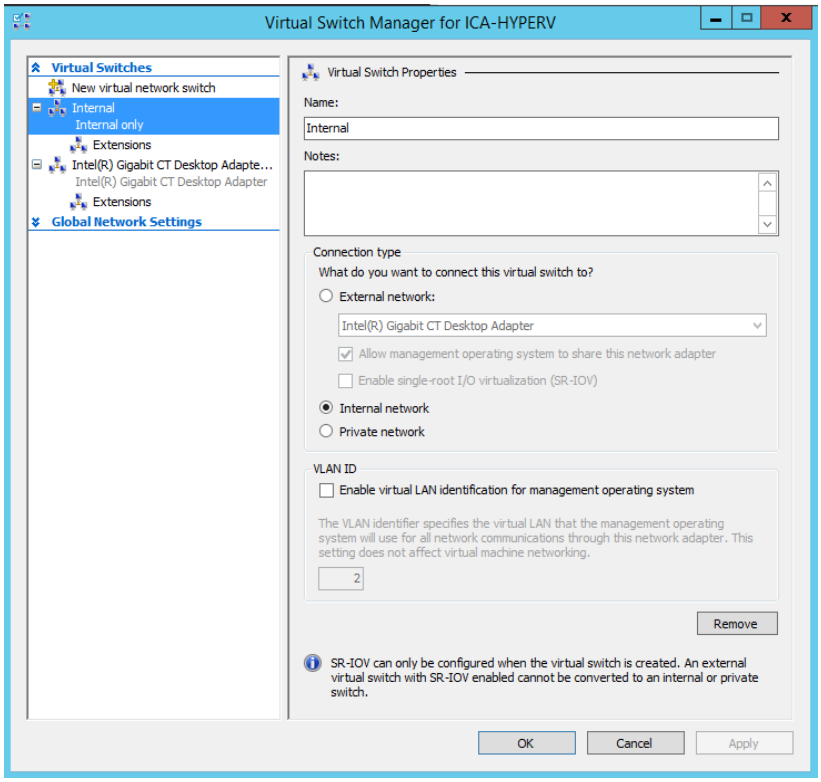
First of all, please create two networks on the Hyper-V host.

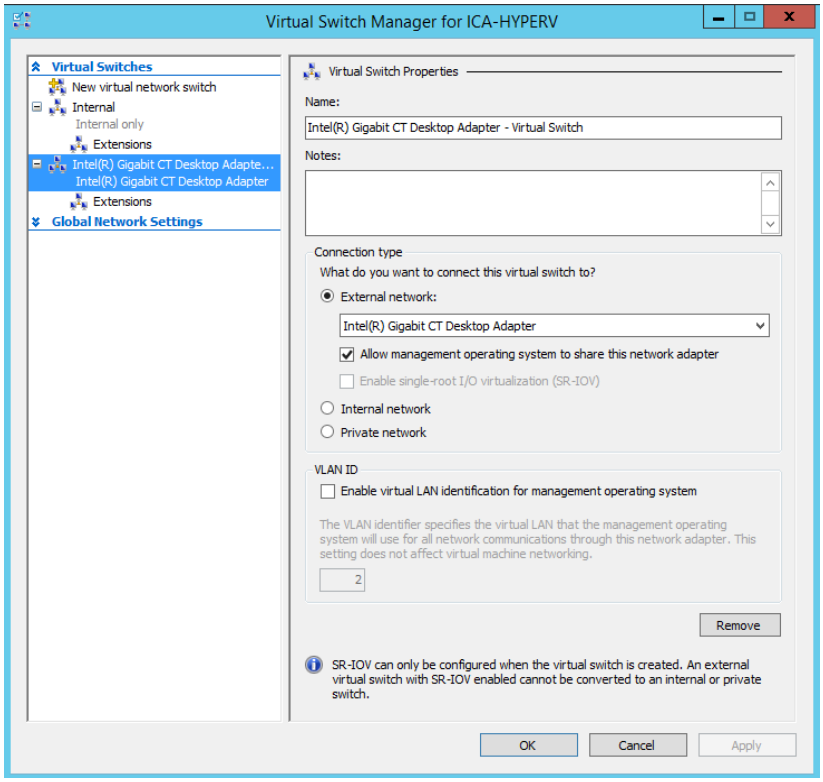
The first one is called "`WAN`" which is for connecting to the outside world and will need a physical network adapter attached. The first network adapter of the InControl VM shall be assigned to this network.

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: As the “Internal” network segment is on the subnet 192.168.1.0/24 by default, the WAN interface cannot be on 192.168.1.0/24 too. You may change the subnet DB VM’s “Internal” interface’s IP on the console (see chapter 1.8) and change the IC VM’s Internal interface IP and the DB server setting on the control panel.


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

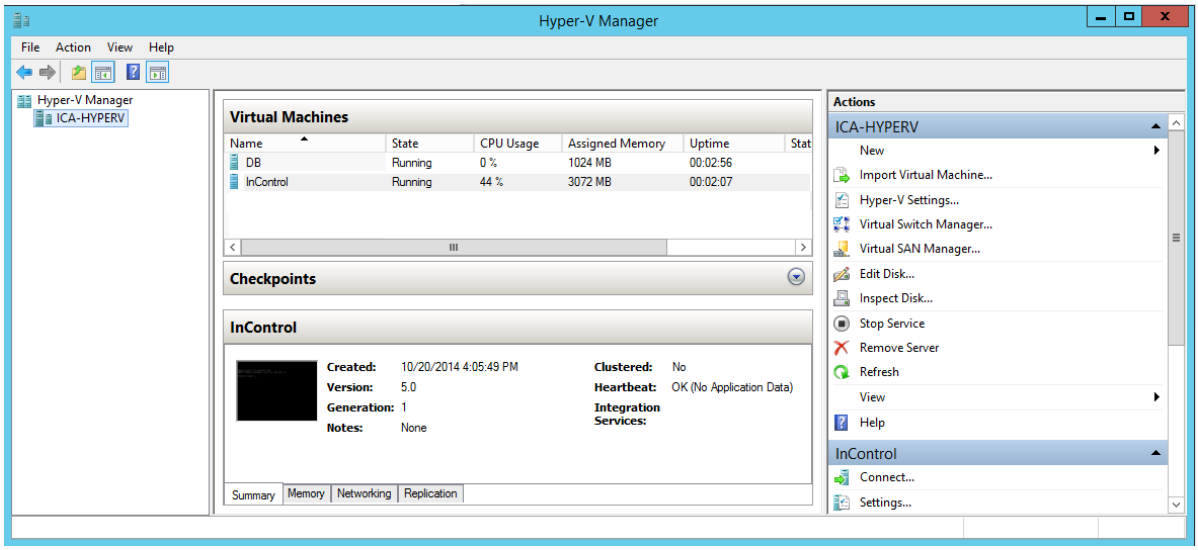
Peplink publishes two VHDX files: `InControl-System-2.9.0.2.vhdx` and `DB-System-20210323.vhdx`. They are bootable systems of the InControl virtual appliance and a MySQL database respectively. You will use them to start one InControl and one Database VM.

Download the latest Virtual Appliance and Database Server image files in `.vhdx` format from
https://www.peplink.com/support/incontrol-appliance-images-downloads/

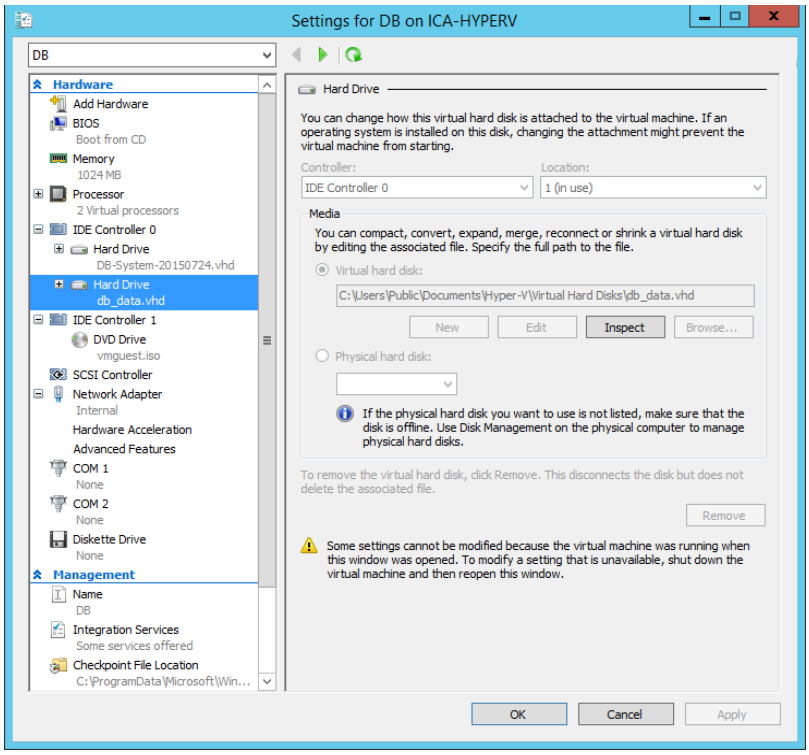
The .vhdx file names and sizes are as follow:

File name	Size (Bytes)
InControl-System-2.9.0.2.vhdx	25,035,800,576
DB-System-20210323.vhdx	25,035,800,576

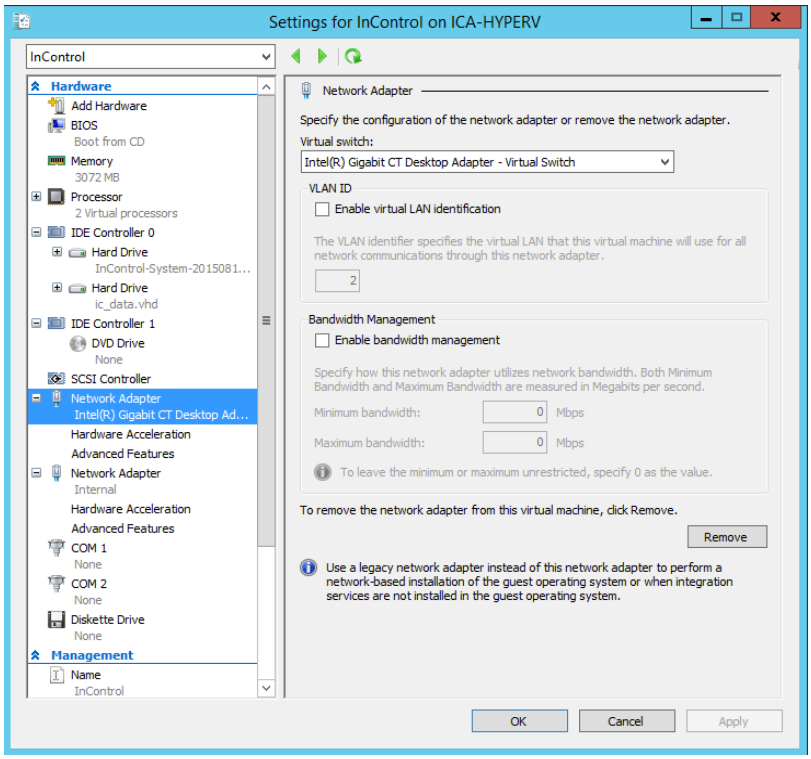
In the Hyper-V Manager, create two new Virtual Machines called `DB` and `InControl` for Ubuntu Linux (64 bit) guest operating systems. Our test was on first-generation VMs. For the DB VM, you need only one network connection on the Internal network. For the InControl VM, you'll need the WAN network and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



DB VM:



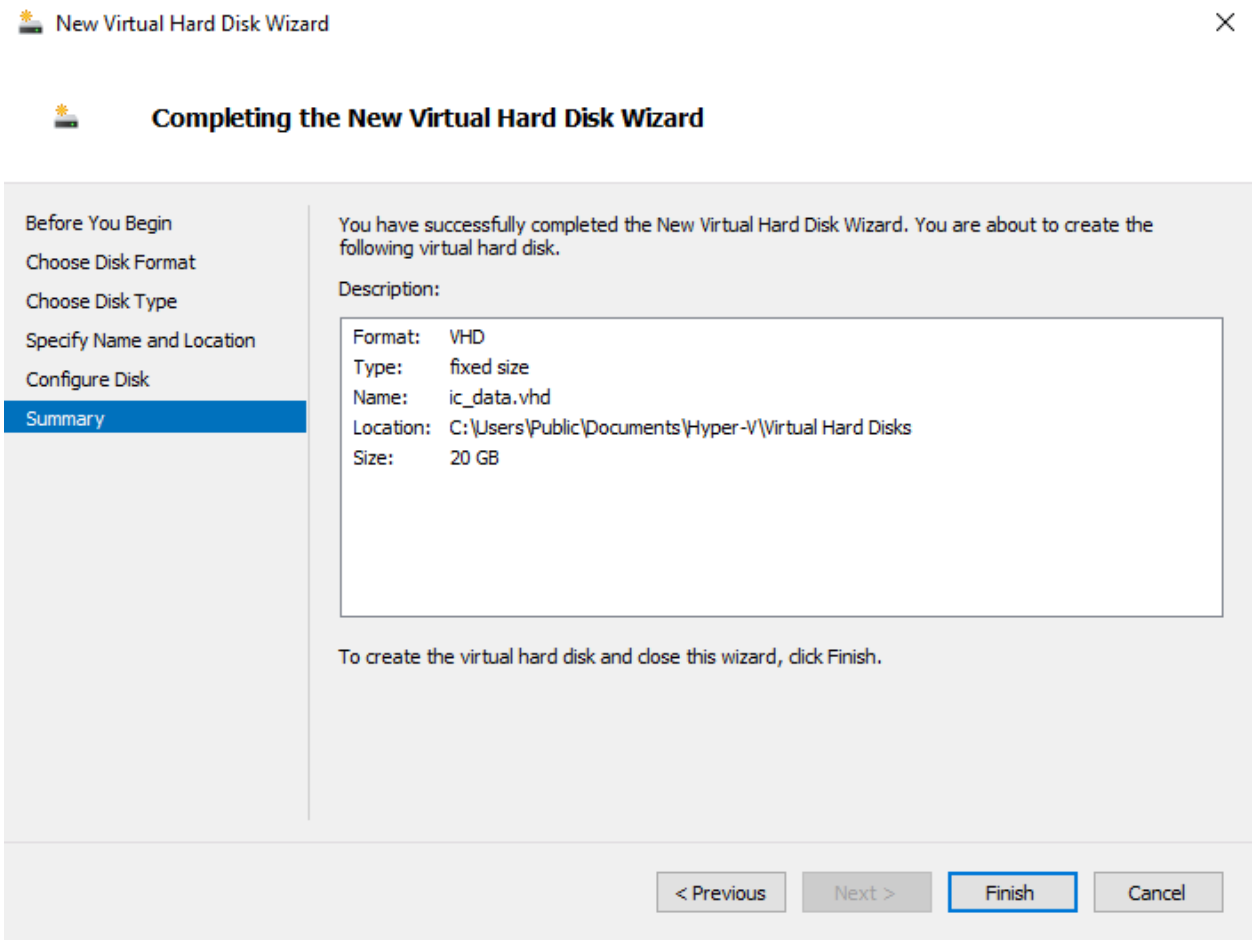
InControl VM:



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 20GB disk on IDE (0:1). For the DB VM, follow the same but add 100 GB of disk storage for supporting 100 devices. See Introduction - Minimum Hardware Requirements

Choose VHDX - fixed-size data disks.



After the installation, please perform a firmware update. Please refer to chapter 13.1.

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.

1.5 Installation on AWS

1.5.1 Preparing AMIs

1.5.1.1 For general AWS regions

For general AWS regions, you can send an email containing your 12-digit Amazon account number as well as the planned deployment region to ica@peplink.com. Peplink will share two AMIs directly into your AWS account. You will be able to find the AMIs when filtering for 'Private AMI' in the AMI page of the corresponding region.

1.5.1.2 For AWS GovCloud

For AWS GovCloud, you should receive two image files from Peplink.

In order to complete the installation steps, you have to prepare a PC that has `aws-cli` installed and is configured to run with your access key ID and secret access key, and with the default region set.

Your account also needs to be able to create and assign IAM roles and policies, create buckets in S3, create and launch EC2 instances, and create a VPC.

Note: The file paths for AWS CLI commands should be specified in full with respect to your OS. E.g.
- Windows: "`file://C:\Users\username\My Documents\trust-policy.json`"
- Mac and Linux: "`file:///Users/username/trust-policy.json`"

Uploading the images to S3 Bucket

Create or use an existing bucket within the same AWS region of your planned deployment. Upload the two disk files to the bucket, saving the bucket name and the file path.

While files are uploading, you may continue to prepare the environment.

Creating the required import role and policy

You will need to import the AMI from your S3 bucket using the `aws-cli`. Firstly, you will need to create the roles. You shall save the following piece of text to a file named ***trust-policy.json*** on your computer.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": { "Service": "vmie.amazonaws.com" },
         "Action": "sts:AssumeRole",
         "Condition": {
            "StringEquals":{
               "sts:Externalid": "vmimport"
            }
         }
      }
   ]
}
```

Then, run the following command to create the role:

```
aws iam create-role --role-name vmimportpeplink
--assume-role-policy-document "file:///trust-policy.json"
```

(Please change the file path as described above.)

Second, save the following piece of text to a file named ***role-policy.json*** on your computer. Change the BUCKETNAME to match yours:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect": "Allow",
         "Action": [
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket"
         ],
         "Resource": [
```

```
            "arn:aws:s3:::BUCKETNAME",
            "arn:aws:s3:::BUCKETNAME/*"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "ec2:ModifySnapshotAttribute",
            "ec2:CopySnapshot",
            "ec2:RegisterImage",
            "ec2:Describe*"
         ],
         "Resource": "*"
      }
   ]
}
```

Then run the following command to create the role.

```
aws iam put-role-policy --role-name vmimportpeplink
--policy-name vmimportpeplink --policy-document
"file:///role-policy.json"
```

(Please change the file path as described above.)

Importing the AMI to AWS

Create two files and insert the following content, after changing to correct bucket name:

db.json:

```
[
  {
    "Description": "InControl DB System",
    "Format": "VHDX",
    "UserBucket": {
        "S3Bucket": "YOURBUCKETNAME",
        "S3Key": "DB-System-20210323.vhdx"
    }
}]
```

icva.json:

```
[
  {
    "Description": "InControl IC System",
    "Format": "VHDX",
    "UserBucket": {
        "S3Bucket": "YOURBUCKETNAME",
```

```
            "S3Key": "InControl-System-2.9.0.2.vhdx"
        }
    }]
```

Once your disk images have been successfully uploaded to S3, run the following commands to import the files as AMIs.

```
aws ec2 import-image --disk-containers "file:///db.json"
--role-name vmimportpeplink

aws ec2 import-image --disk-containers "file:///icva.json"
--role-name vmimportpeplink
```

Please change the file paths as described above. Each command will take around 25 minutes to complete. They shall also return an import task ID. You can run the following command with the task ID specified to monitor their import progress:

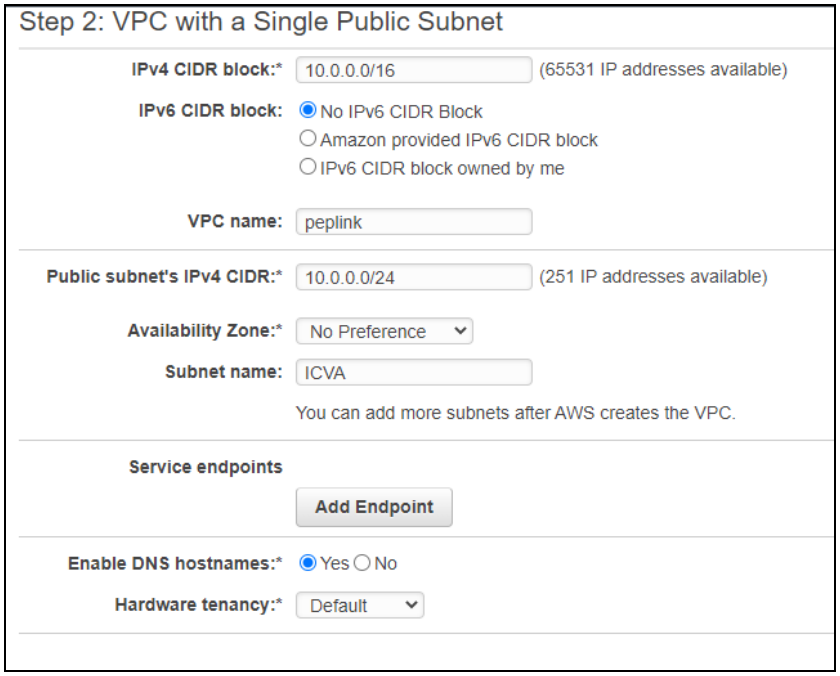
```
aws ec2 describe-import-image-tasks --import-task-ids
import-ami-IMPORT_TASK_ID
```

1.5.2 Setting up network

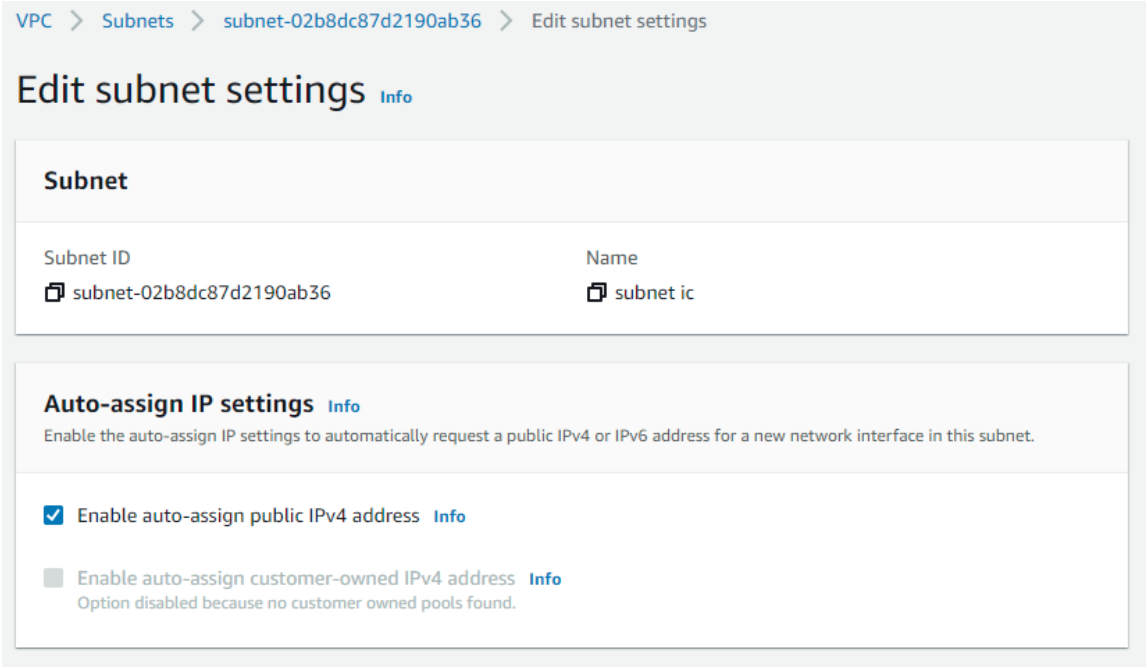
InControl virtual appliances require to be set up in a VPC for virtual machines to communicate in a secured environment.

Please connect to your Amazon console and open VPC under Network and Content Delivery.

Click on Launch VPC Wizard. Select **VPC with a Single Public Subnet**.



Once your VPC is created, go to Subnet, after selecting your newly created subnet, go to the "Actions" menu and click on **Edit subnet settings**, In the Auto-assign IP settings section, check the **Enable auto-assign public IPv4 address** option.



1.5.3 Setting up security groups

InControl Virtual Appliance requires two security groups, one for IC server and one for DB server. Go to the "Security Groups" tab under "EC2" and click on Create security group.

Create the first security group for the InControl instance. Add the following **Inbound rules**. (Note: the last two rules are for UDP protocols.)

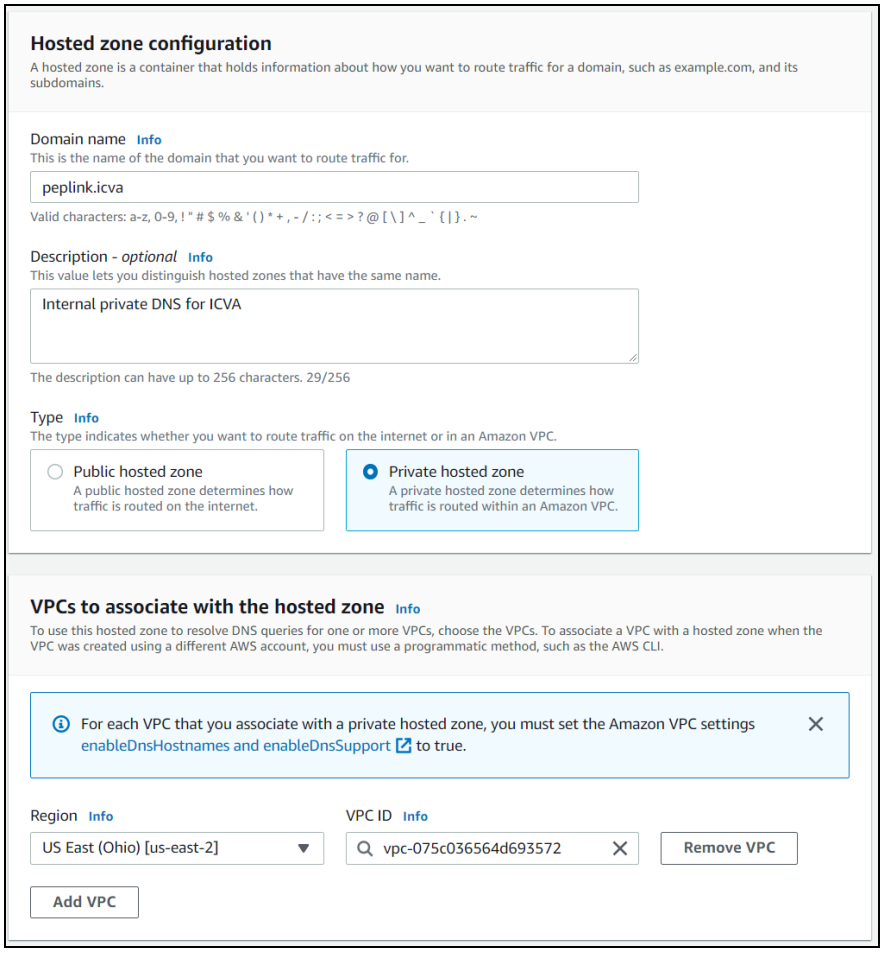
Protocol	Port	Source
TCP	4443	Any
TCP	443	Any
TCP	2222	Any
TCP	80	Any
TCP	1443	Any
TCP	5246	Any
UDP	5246	Any
UDP	53	Any

Create a second security group for the Database instance with the following inbound rules. **Do not forget to change the source with your VPC's subnet address**:

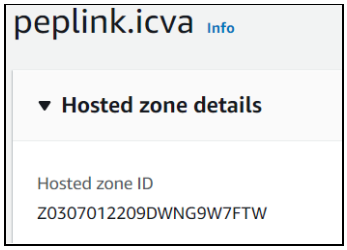
Protocol	Port	Source
TCP	3306	*The VPC's subnet address*
TCP	27017	*The VPC's subnet address*
TCP	6379	*The VPC's subnet address*
TCP	22	*The VPC's subnet address*

1.5.4 Setting up Route 53 Hosted private zone

Open the Route 53 > "Hosted zone". Click on **Create a new zone**.
Enter **`peplink.icva`** as the Domain name and select the Private zone option. In the next section, pick the region of your VPC and associate your InControl Virtual Appliance VPC with the private zone.
You can copy the domain name, as it will be used later.



After creation, click on details and copy the **Hosted zone ID**.



1.5.5 Creating DNS update role

Navigate to **Identity and Access Management (IAM)** and select **Policies**. Click the **Create Policy** button. Click the **JSON** tab. Paste the following content to the text editor. Replace *HOSTED_ZONE_ID* with the **Hosted zone ID** you copied above.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeTags",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/HOSTED_ZONE_ID"
        }
    ]
}
```

Click **Next: Tags**. Click **Next: Review**. On the **Review policy** screen, put ***AutoDNSUpdatePeplink*** to the **Name** field. Click **Create policy**.

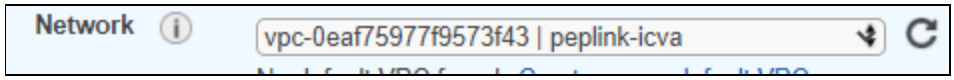
Navigate to **Identity and Access Management (IAM)** and select **Roles**. Click the **Create role** button. Choose **AWS service** > **EC2** and click **Next: Permission**. Select the policy ***AutoDNSUpdatePeplink*** that you just created. Click **Next: Tags**. Click **Next: Review**. On the **Review** screen, put ***AutoDNSUpdatePeplink*** to the **Role name** field. Click **Create role**.

1.5.6 Launching instances

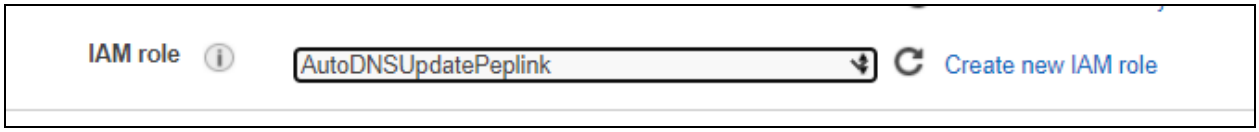
Please follow the instruction in chapter 1.5.1 to prepare the AMI images in your account. You shall launch a DB instance first and then an InControl instance. If your setup is on AWS GovCloud, please jump to chapter 1.5.6.2.

1.5.6.1 For general AWS regions

- Navigate to **EC2** and select **AMIs**.
- Select the AMI **DB-System-20211230** for a DB instance (**InControl-System-2.9.3** for an InControl instance) and click the **Launch** button
- Select the instance type **t3.large** or higher where the memory size is at least 8GB. Click **Next: Configure Instance Details**
- Set the **VPC**



Set the **IAM role** as *AutoDNSUpdatePeplink*.



Click on **Next: Attach Storage** and then **Next: Add Tags**.

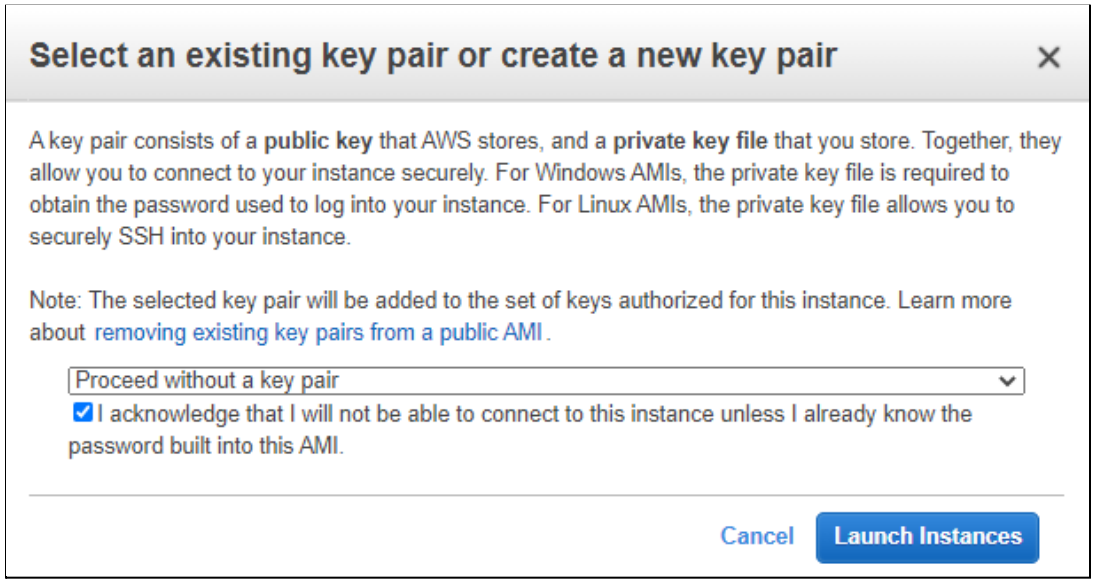
- Add the following tags and values respectively for InControl and DB. Replace *HOSTED_ZONE_ID* with the Route 53 private hosted zone ID.

DB Instance	
AUTO_DNS_ZONE	*HOSTED_ZONE_ID*
AUTO_DNS_NAME	`db.peplink.icva`
Name	`ICA DB`

InControl instance	
AUTO_DNS_ZONE	*HOSTED_ZONE_ID*
AUTO_DNS_NAME	`web.peplink.icva`
Name	`ICA IC`

Click the **Configure Security Group** button.

- Select the corresponding security group you created earlier. Click the **Launch** button.
- Select **Proceed without a key pair** for the key pair selection. Click "**Launch Instances**".



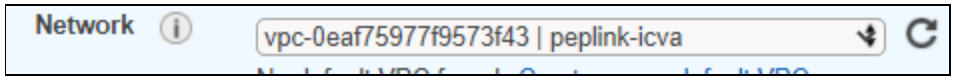
After a DB instance is launched, repeat the steps in this chapter to launch an InControl instance. After both instances are launched, wait around for about 5 minutes. Then you should be able to connect to the control panel:

`https://ICA_public_address:4443`

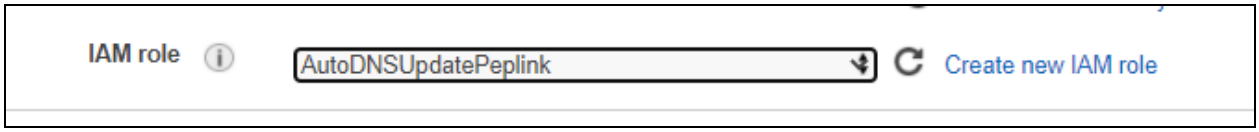
Please upgrade the firmware immediately. You may refer to chapter 13.1.

1.5.6.2 For AWS GovCloud

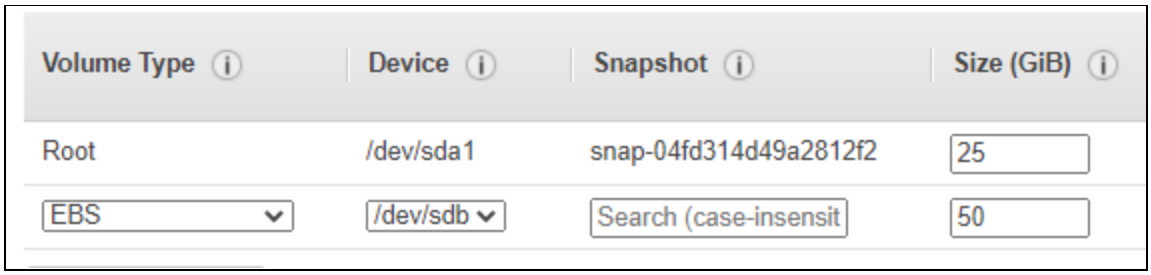
- Navigate to **EC2** and select **AMIs**.
- Select the AMI **DB-System-20210323** for a DB instance (**InControl-System-2.9.0.2** for an InControl instance) and click the **Launch** button
- Select the instance type **t2.large** (IMPORTANT) and click on **Next: Configure Instance Details** (After upgrading it to the latest firmware later, you can change the instances to other instance types.)
- Set the VPC as your peplink VPC



- Add the IAM role AutoDNSUpdatePeplink then click on **Next: Attach Storage**



- Add a new data volume with the chosen size for your infrastructure. The “Device” field of the secondary volume must be **/dev/sdb**.



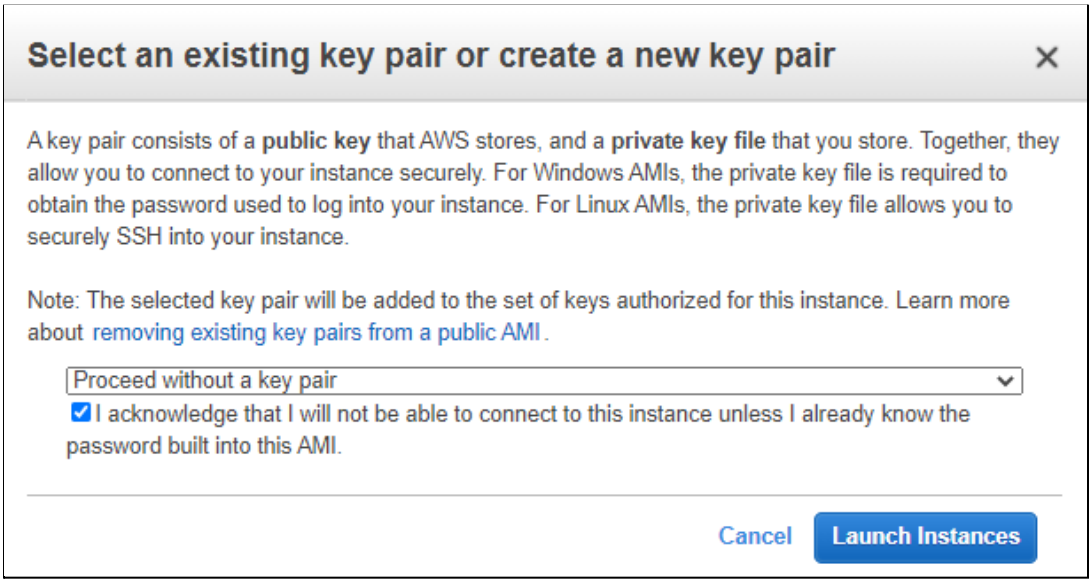
- Add the following tags and values respectively for InControl and DB. Replace *HOSTED_ZONE_ID* with the Route 53 private hosted zone ID.

DB Instance	
AUTO_DNS_ZONE	*HOSTED_ZONE_ID*
AUTO_DNS_NAME	`db.peplink.icva`
Name	`ICA DB`

InControl instance	
AUTO_DNS_ZONE	*HOSTED_ZONE_ID*
AUTO_DNS_NAME	`web.peplink.icva`
Name	`ICA IC`

Click the **Configure Security Group** button.

- Select the corresponding security group you created earlier. Click the **Launch** button.
- Select **Proceed without a key pair** for the key pair selection. Click **Launch Instances**.



After a DB instance is launched, repeat the steps in this chapter to launch an InControl instance. After both instances are launched, wait around for about 5 minutes. Then you should be able to connect to the control panel:

`https://ICA_public_address:4443`

Please upgrade the firmware immediately. You may refer to chapter 13.1.

1.5.7 Associate Elastic IP address

Navigate to **Network & Security** > **Elastic IPs**. Click the **Allocate Elastic IP address** button. Click the **Allocate** button. An IP address is allocated and selected. Click the **Actions** menu and choose the **Associate IP address** item. In the **Instance** field, type "*ICA IC*" and choose the ICA IC instance. Click the **Associate** button.

Your ICA's public IP address has been changed to the new elastic IP address. If you have decided on your "server name", you can update its DNS record and point it to the new elastic IP address.

1.5.8 Reset control panel admin password on AWS

In case you forgot your control panel admin password, you can reset it with EC2 instances' "user data" setting. First, stop the InControl instance. Second, once it is stopped, click **Actions** > **Instance settings** > **Manage User Data**

In the user data field, add a line as follows:

```
password=yournewpassword
```

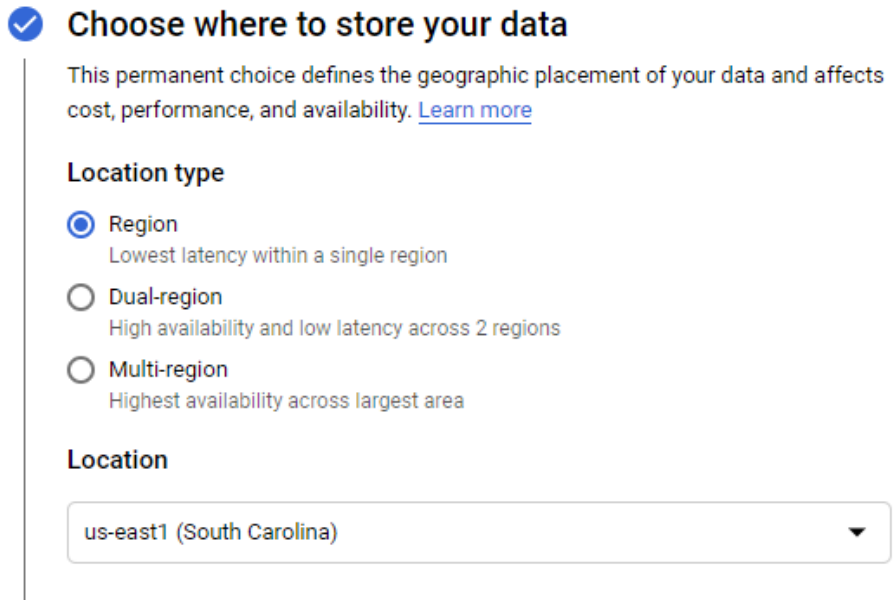
Input a password no longer than 16 characters. Press Save and start the InControl instance.

When it is started up, log in to the control panel with the new password once. Stop the instance. Go to “Manage User Data”, remove the message from the field, and press Save. Start the instance up again. Now, you have completed the password reset procedure. You can now log in to the control panel with the new password.

1.6 Installation on Google Cloud Platform

1.6.1 Uploading the image

Browse to Google Cloud Storage menu and create a new bucket.
Name your bucket and select the planned installation region. All other default settings can be kept.

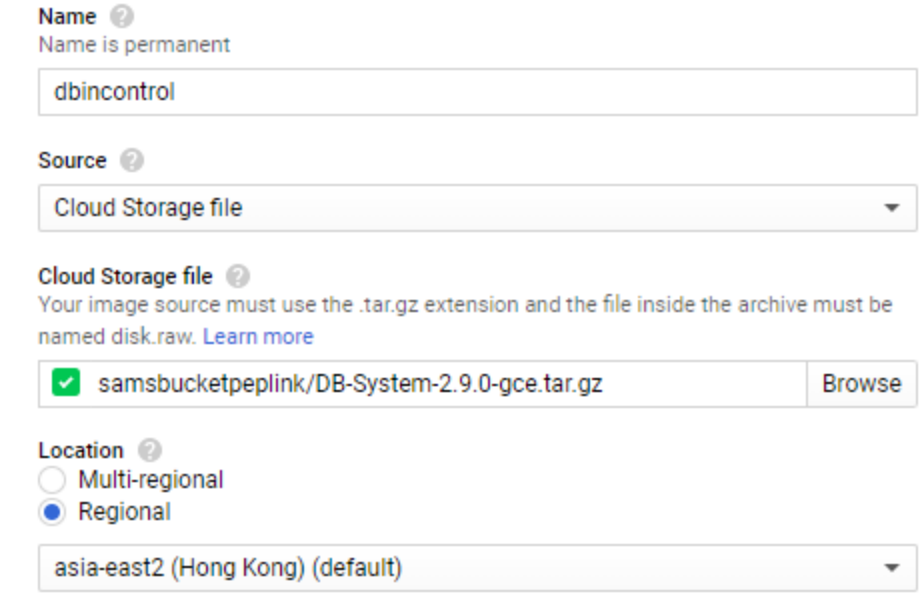


Once the bucket is created, open it and upload your DB and InControl images.

1.6.2 Importing the image

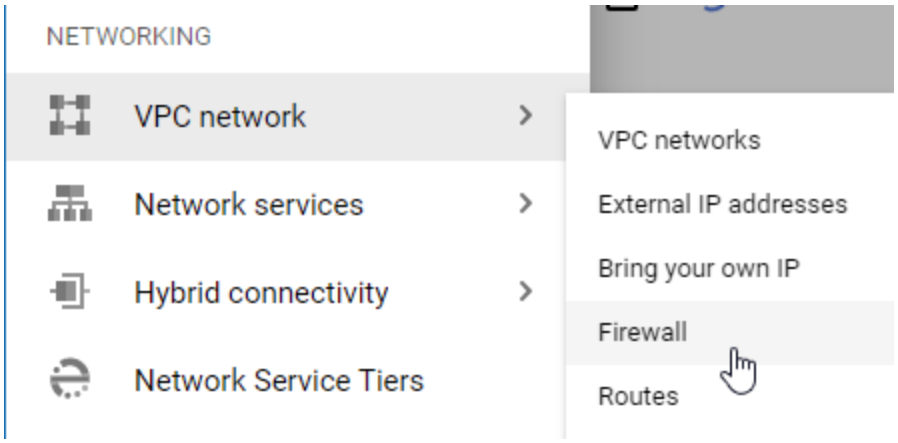
Once files are uploaded, browse to Google Cloud Compute Engine, then the Image menu under the Storage section.

Click on Create Image, name the image accordingly and select Source as Cloud Storage file, then select your bucket and the corresponding file. Then select the planned deployment region and click on Create.



1.6.3 Setting up the firewall

Browse to Networking / VPC Network / Firewall.



Click on Create Firewall rule:

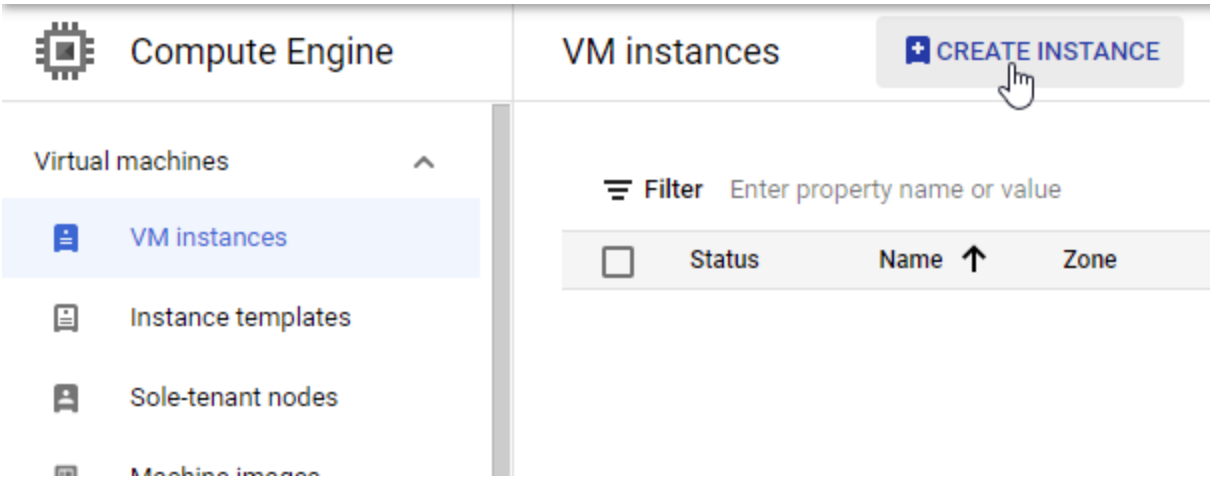
- Name your first rule “incontrol”
- Add a “Target tags” as “incontrol”
- Add a Source IP range from which your InControl instance will be reachable (eg: 0.0.0.0/0)
- Check TCP and paste the following: `80,443,2222,4443,5246`
- Check UDP and paste the following: `53,5246`
- Click on create

Now create a new firewall rule for DB:

- Name your rule “db”
- Add a “Target tags” as “db”
- Add a source IP range corresponding to the IP range of your VPC in the planned deployment region (eg: 10.170.0.0/20)
- Check TCP and paste the following: `22,3306,6379,27017`
- Click on Create

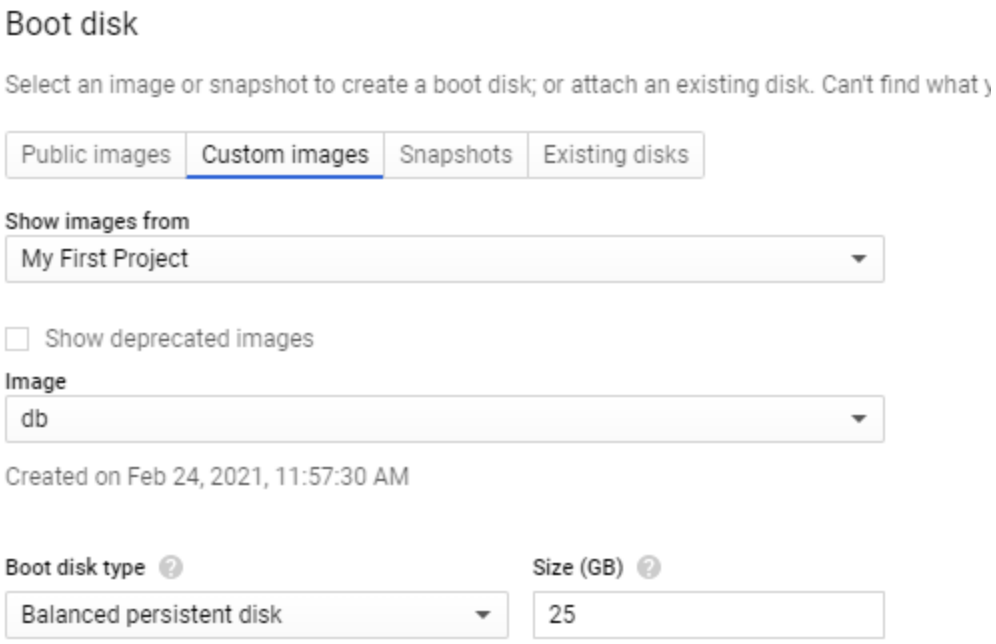
1.6.4 Creating the instances

Browse to Compute Engine / VM Instances and click on Create Instance.

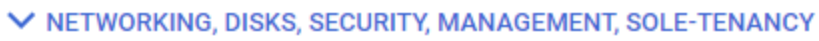


- Name your DB instance “ica-db”
- Select the desired machine configuration

- Under Boot disk section, click on Change and browse to Custom Images, select your project and the DB image then click on Select

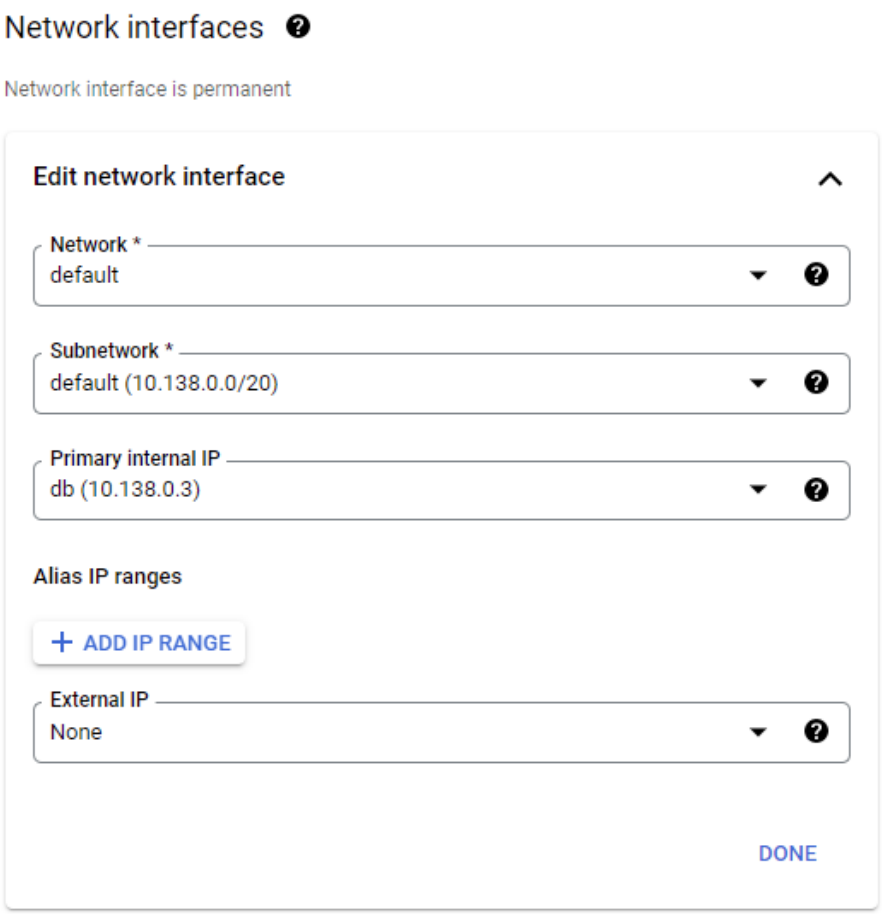


- Expand the “Networking, disks, security, management, sole-tenancy” menu



- Browse to Networking section
  - Add “db” as Network tag
  - In the Network interface section, edit the network interface:
    - Under Primary Internal IP, select Reserve Static IP Internal Address
    - Select Let Me Choose under “Static IP address” and input the desired IP for db instance

- Under External IP, select “None”

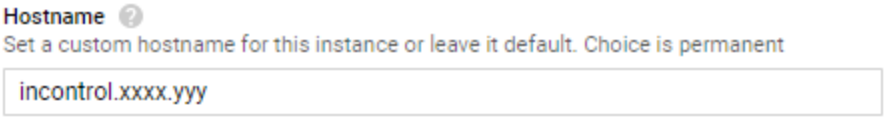


  - Click on Done
- Browse to the Disks section and add a new disk. Name it “ica-db-data”. Input size of 20 GB or above. Click Done.
- Click Create

Now create another new instance for the InControl:

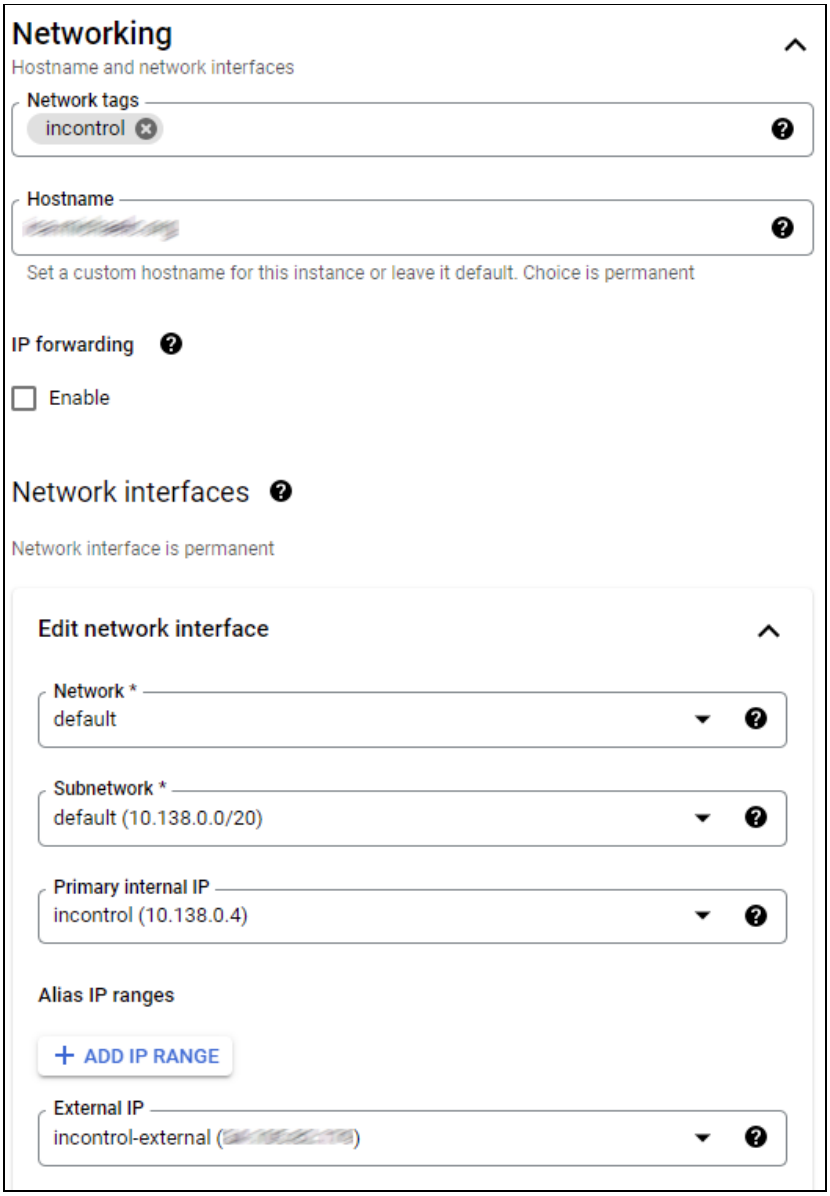
- Name your instance (eg: incontrol)
- Select the desired machine configuration
- Under Boot disk section, click on Change and browse to Custom Images, select your project and the InControl image then click on Select
- Expand the “Networking, disks, security, management, sole-tenancy” menu
- Browse to Networking tab

- Add “incontrol” as Network tag. Add your InControl target DNS name:



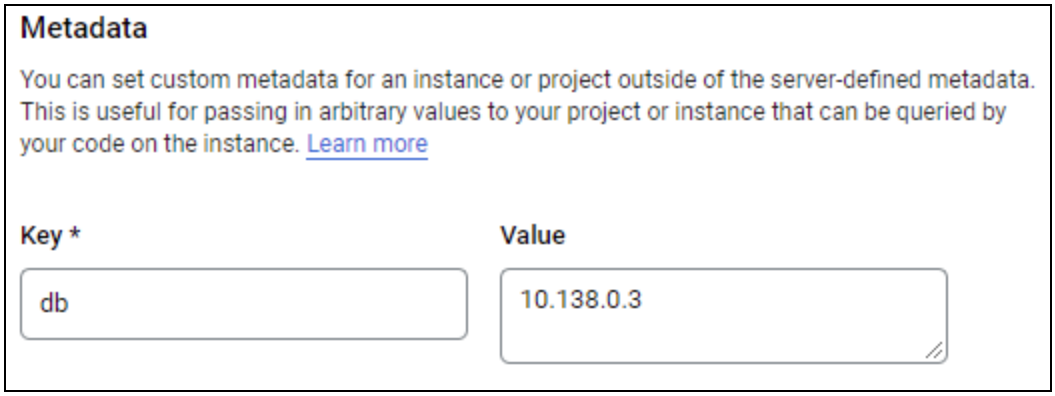
- Under Network interfaces, edit the network interface
  - Under Primary Internal IP, select Reserve Static IP Internal Address
  - Select “Let Me Choose” under “Static IP address” and input the desired IP for InControl instance
  - Under External IP, select either Create IP address or assign the desired existing IP address.

- Press Done.



- Browse to the Disks section and add a new disk. Name it “ica-ic-data”. Input size of 20 GB or above. Click Done.

- Under the Management tab, add a Metadata with the following key: “db” and the reserved private IP address of your DB instance as value.



- Click Create.

The system will take about 6 minutes to boot up for the first time if everything is set up correctly.

1.7 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 Status		
	InControl	Database
Status	Active	DB Online
License	Valid	-
Online Status on Peplink InControl	Online	-
Version	2.9.0.3	N/A
Disk Usage	Total: 19.46 GB Used: 6.55 GB (36%)	Total: 9.99 GB Used: 1.80 GB (19%)

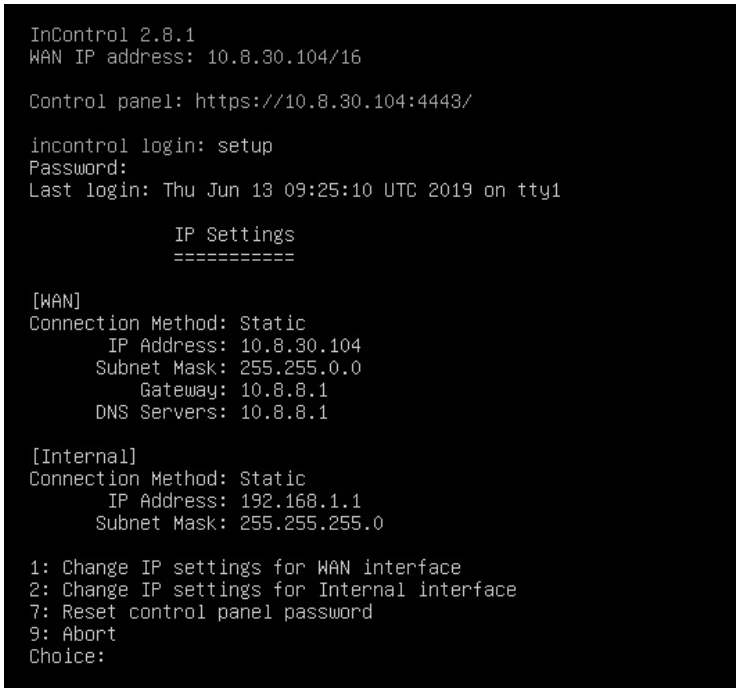
System Settings	
Product	InControl Appliance (Virtual)
Serial Number	[redacted]
Server Name	incontrol.[redacted]
Company Name	My Company
Service Name	My Company InControl
System Admin E-mail Address	sysadmin@my.domain
Tech Support E-mail Address	support@my.domain
Notification E-mail Sender Name	My Company InControl

After InControl VM is booted up for the first time, please update its firmware immediately. Please refer to chapter 13.1 for the upgrade details. Afterward, input a license key. Then update the server name and other settings.

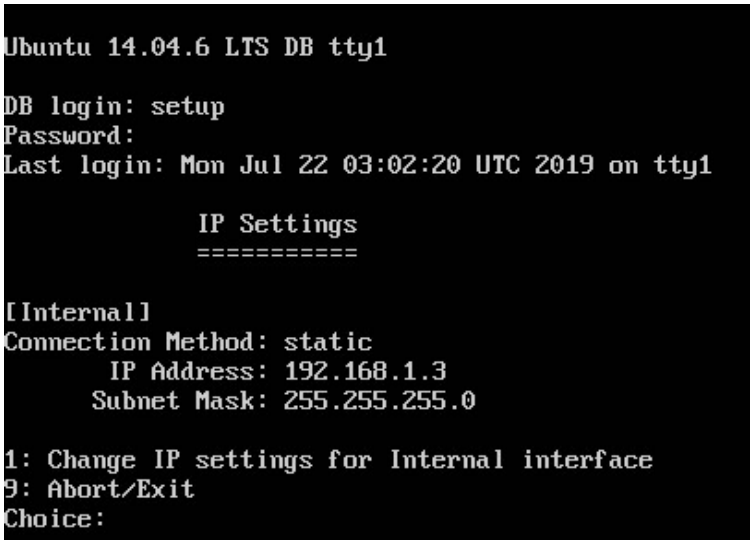
1.8 IP Address Configuration and Password Reset On the Console

For Hyper-V and VMware installations, you may configure the InControl and Database VM's IP address, and reset the InControl VM's control panel password by logging in to the console. The username and password are "`setup`" and "`setup`" respectively. (Note: the console username and password cannot be changed)

InControl VM:



Database VM



1.8.1 How to change the VMs' IP on the Internal network?

By default, the IP addresses of the InControl and database VMs are 192.168.1.1 and 192.168.1.3 respectively. If you have changed their IP addresses on the console, you must also navigate to the control panel and update the "Database IP Address" setting too.

Database Settings	
Database IP Address	192.168.1.3

1.9 Software License

A software license is required for the InControl virtual appliance to operate. The license ties to the Server Name you use to visit the InControl appliance website. To acquire an 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	

The "Max. Allowed Number of Active Devices" is normally not limited. For legacy licenses, the number is a positive integer.

Managed devices are required to be in-warranty or covered by an InControl subscription in order to appear online and be manageable. If the system is firstly installed or upgraded to 2.9.0 or above, the system will enter into a 7-day grace period. Within the period, device expiry date checks are not enforced. Devices could appear online as soon as they are reporting to the system. After the period, any number of within-warranty devices could be managed so long as the system's maximum resource capacity has not been reached.

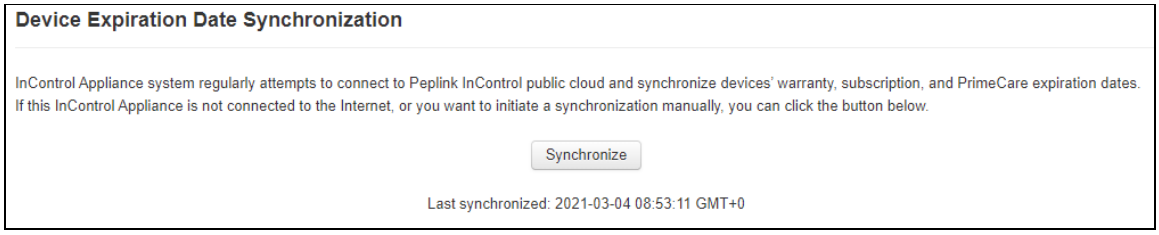
For systems with a legacy license, when the license usage reaches 100%, no more devices could appear online even if they are under warranty or subscription.

1.10 Device Expiration Date Synchronization with Peplink InControl

In order for the InControl Appliance to maintain the up-to-date warranty/subscription/PrimeCare date record, since version 2.9.0, the system automatically synchronizes devices' service expiration date records with Peplink InControl on the Internet every six hours. Peplink device firmware releases and product definitions are synchronized at the same time.

For systems that are isolated from the Internet, system administrators are required to prepare a PC that has web access to both the InControl Appliance and Peplink InControl. Whenever any

devices' service contract has been renewed in Peplink, on the PC's web browser, visit the appliance's MSP-level Device Management page (`https://{ICA_Address}/r/msp/device_management`) and click the Synchronize button in the "Device Expiration Date Synchronization" section.



The web browser will act as a proxy to securely transfer the records from the public Peplink InControl to the private InControl Appliance system.

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 that is accessible to the port's IP address. Connect it to the port with an Ethernet cable. For the 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)
Software Version	2.8.4
Serial Number	[redacted]
Server Name	incontrol.my.domain
Company Name	My Company
Service Name	My Company InControl
System Admin E-mail Address	ica@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

2.2 License Key

A license has been pre-installed for managing a certain number 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

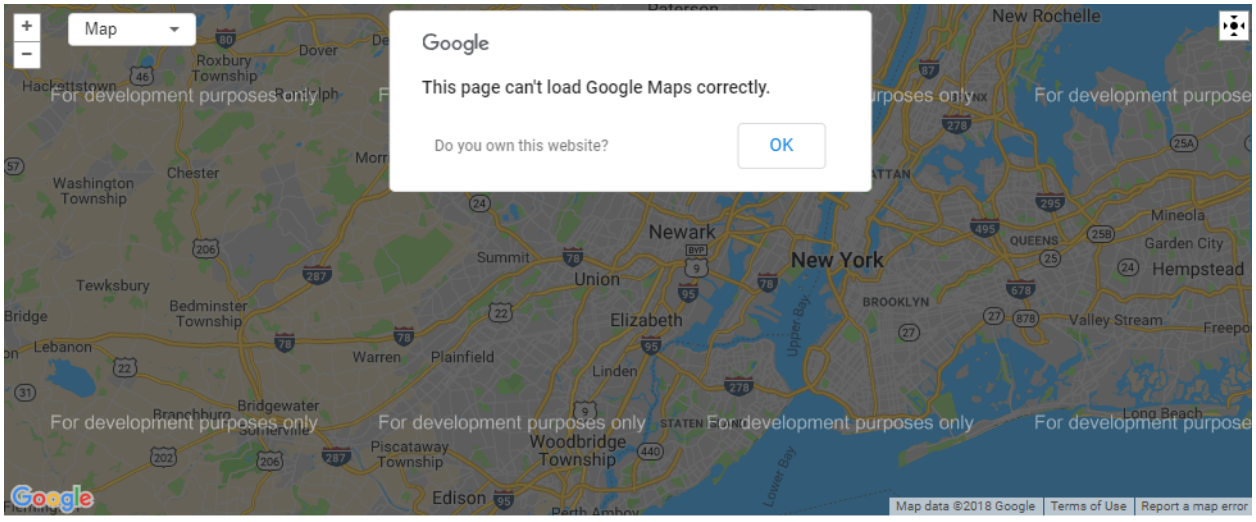
To create new accounts, the system has to be able to send confirmation emails to do account confirmation. So please configure the SMTP server settings, as well as the “Notification E-mail Sender Name” and “Notification Sender E-mail Address” in the System Settings above accordingly.

E-mail Delivery Settings		
SMTP Server	smtp.my.domain	
SMTP Port	587	
SMTP Username	smtp-user	
SMTP Password	••••••••••••••••	
SMTP Authentication	Login (default) ▼	
SMTP TLS Encryption	Enabled (default) ▼	
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

By default, the maps showing on the system are served by a Peplink managed OpenStreetMaps system. If you want to use Google Maps instead, you are required to apply an API key from Google, add billing information to it, and input the API key to InControl Appliance's control panel page. If a key is not provided, a screen like this may be displayed:



Please follow the instructions shown 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. The setting is available at Organization Settings.

OpenStreetMap Settings

When you choose to use OpenStreetMap, the mapping images and geocoding requests will be served by Peplink's OpenStreetMap servers by default. You could change to using your servers 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, historical event log events, GPS locations, and cellular signal data are only kept in the MySQL database for 5 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 it 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	

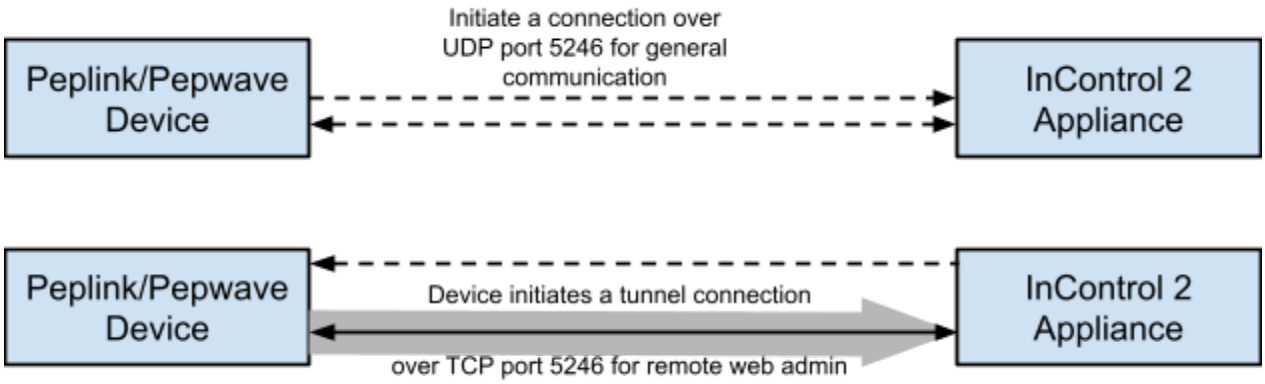
Hourly device usage	2 days	
Hourly client usage	1 month	
Daily client/device usage	60 days	
Monthly device usage	2 years	
Device online/offline history	6 months	
Social network user data	2 years	
Operation log	2 years	
Event log	30 days	1 year
GPS data	5 days	1 year
WAN Quality / Cellular reports	5 days	6 months

6. Facebook App Settings (for Captive Portal)

Please refer to Appendix 1 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 a 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).

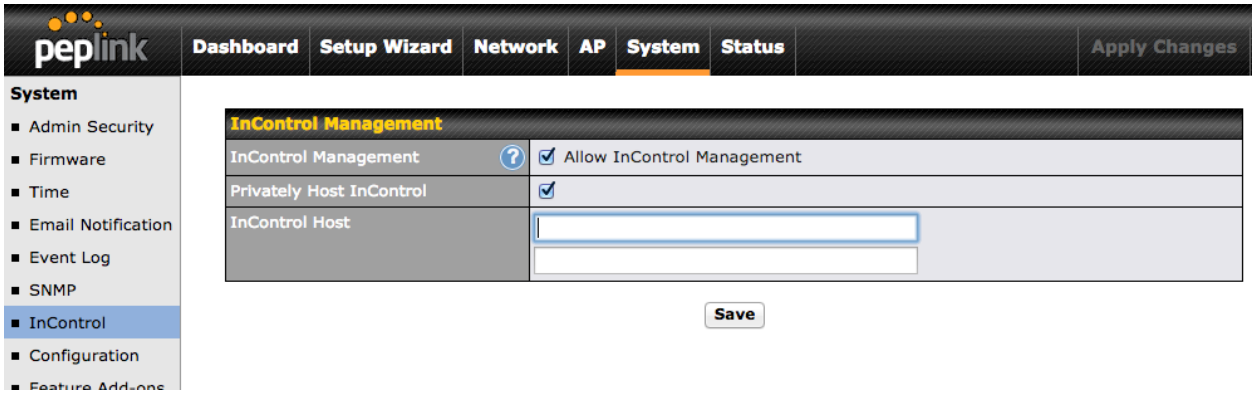


There are two ways to configure your Peplink/Pepwave devices to report to your InControl appliance instead of the Peplink InControl in the public cloud.

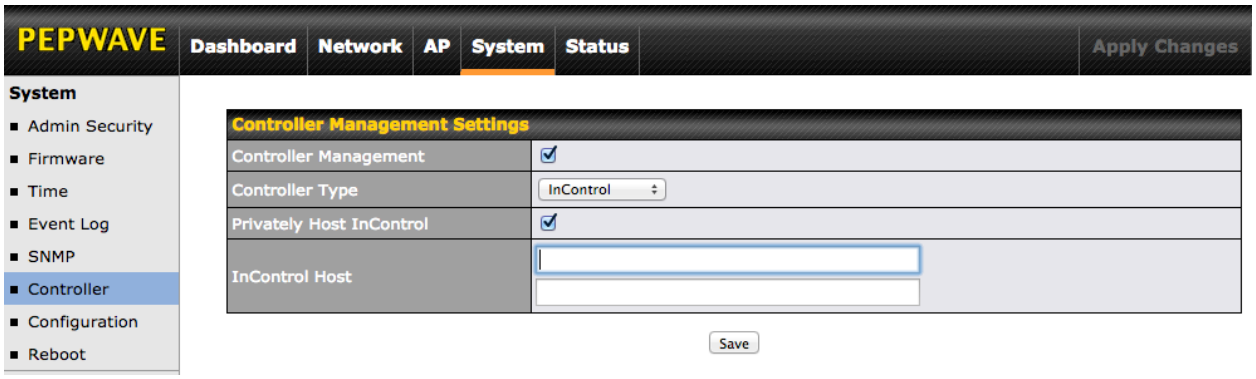
Method 1: By Configuring Devices Individually - for Internet Isolated Environments

Log in 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 firmware 6.1.2 or above. Login to the web admin and navigate to System > InControl.



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

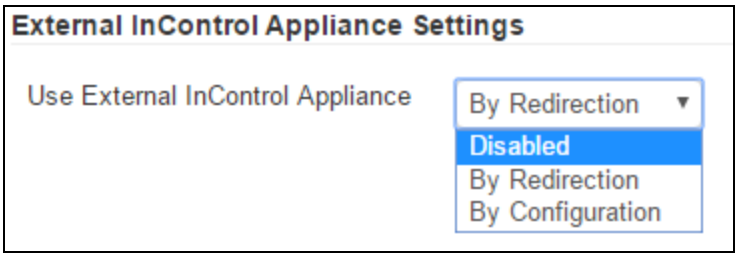


Input your InControl's IP address to the first InControl Host field.

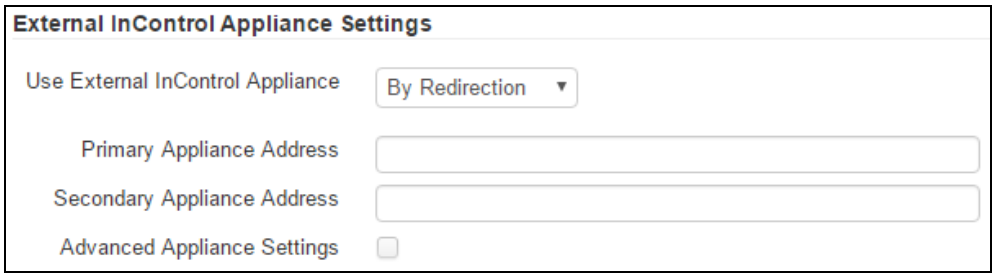
Method 2: By Configuring or Redirecting Devices from the Peplink InControl - for Internet-accessible Environments

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-level **Device System Management** 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.



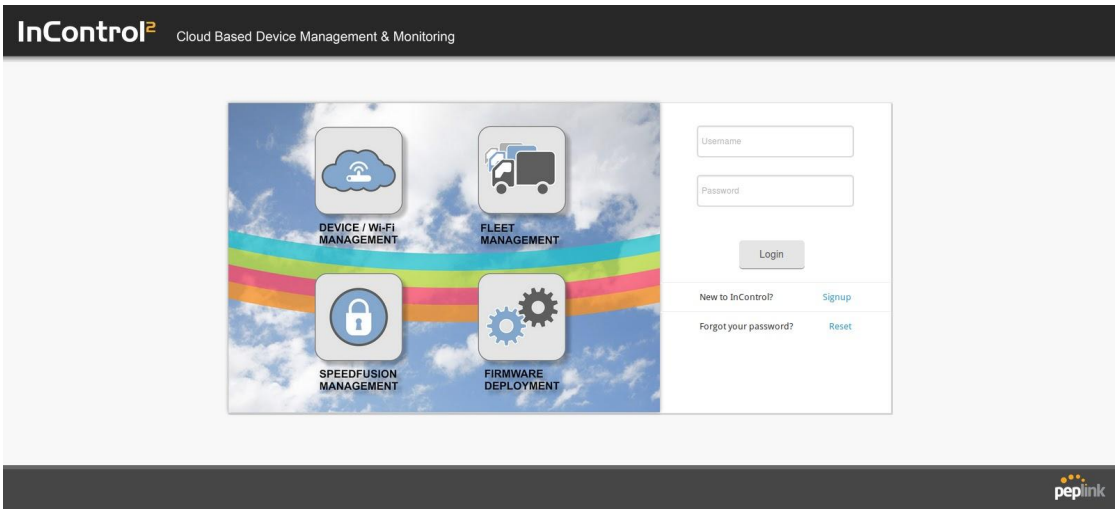
If you choose ***By Redirection***, devices will also connect to Peplink InControl first every time they startup. This option allows you to change your InControl Appliance's address easily in the future.



If you choose ***By Configuration***, your InControl Appliance address(es) will be saved persistently to your devices. After your devices receive 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 failover to connect to Peplink InControl if they failed to connect your InControl Appliance.

8. Logging Into InControl Appliance Web Site

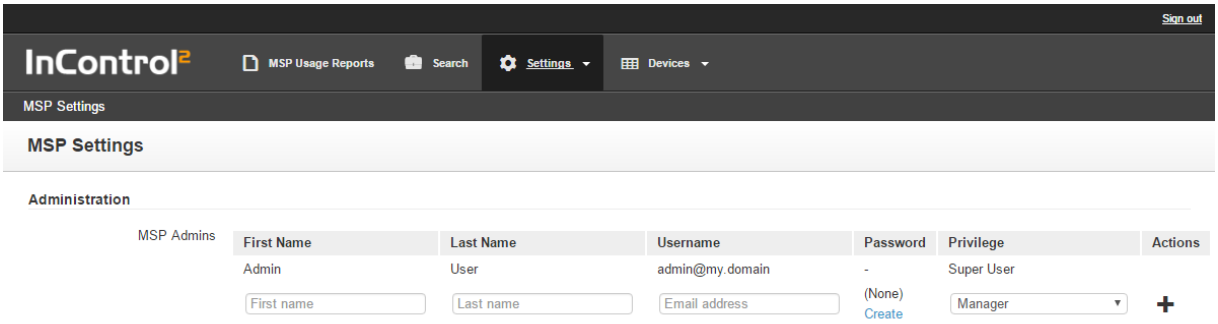


To access the InControl website, you must visit its hostname instead of its IP address. Your PC is required to resolve the hostname into the server IP address. You may add a local DNS record to your PC by editing its "`hosts`" file. It is "`%SystemRoot%\System32\drivers\etc\hosts`" for Windows or "`/etc/hosts`" 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, 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 InControl, you will see an MSP (Managed Service Provider) administration page which is for managing the InControl system. To manage MSP administrator accounts, navigate to Settings > MSP Settings.

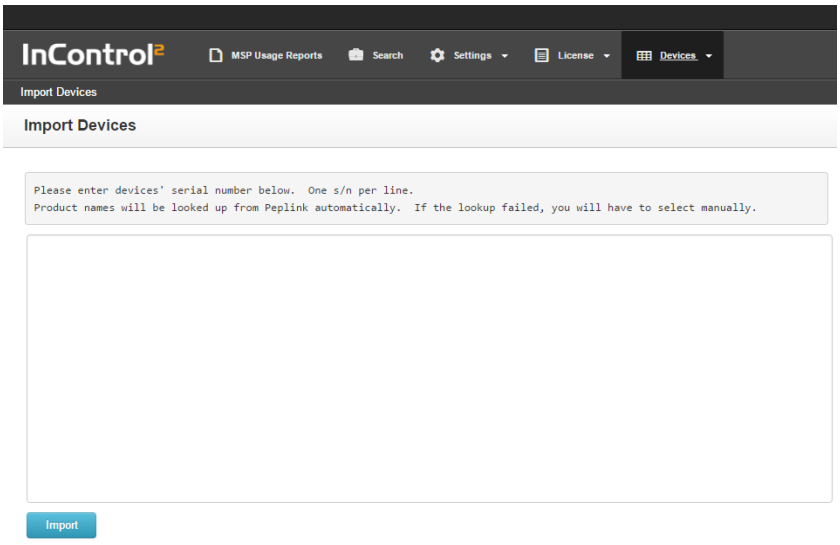


Note for InControl Hardware Appliance: the appliance's website is only accessible from the WAN port. (It is **not** accessible from the LAN or Management ports.)

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.



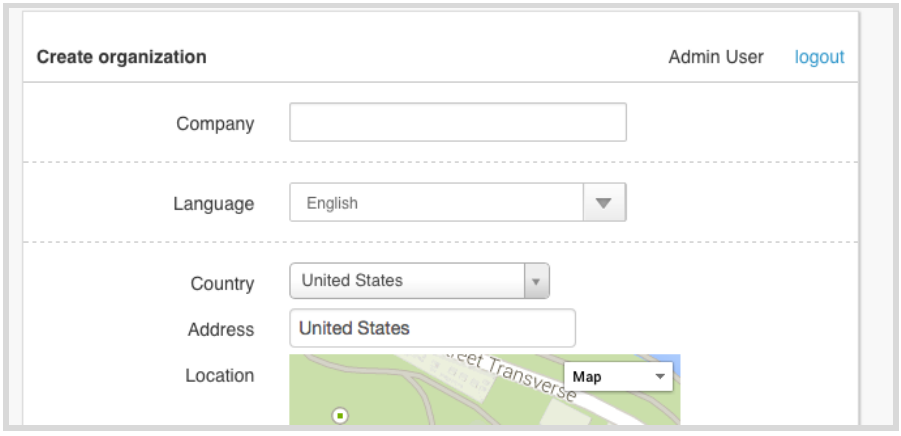
InControl Appliance will attempt to query the Peplink server what products the serial numbers are. If successful, the devices will be imported. If not, you will be prompted to select each device's product name.

Organization administrators (i.e. non-system administrators) can add the devices now.

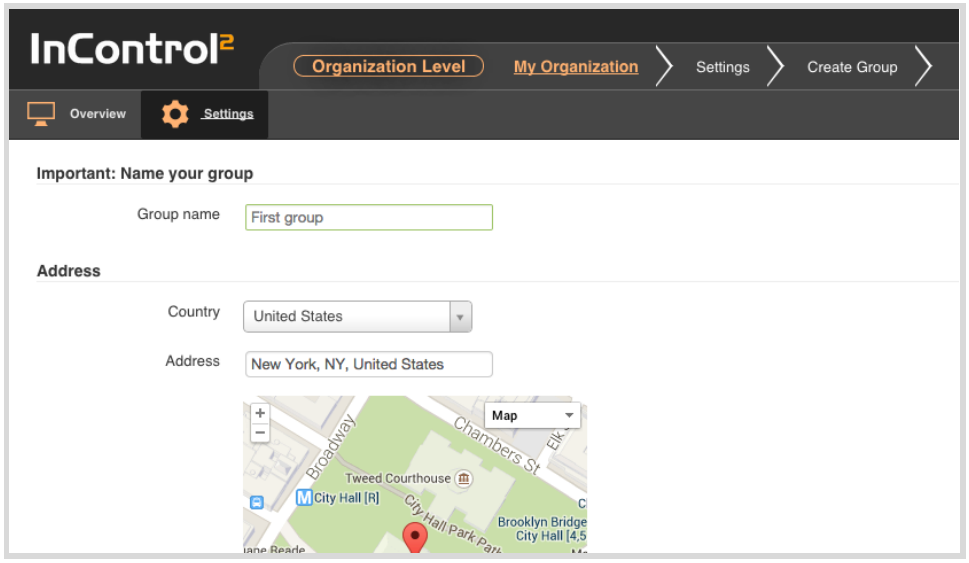
10. Creating an Organization, Group, and Adding Devices

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

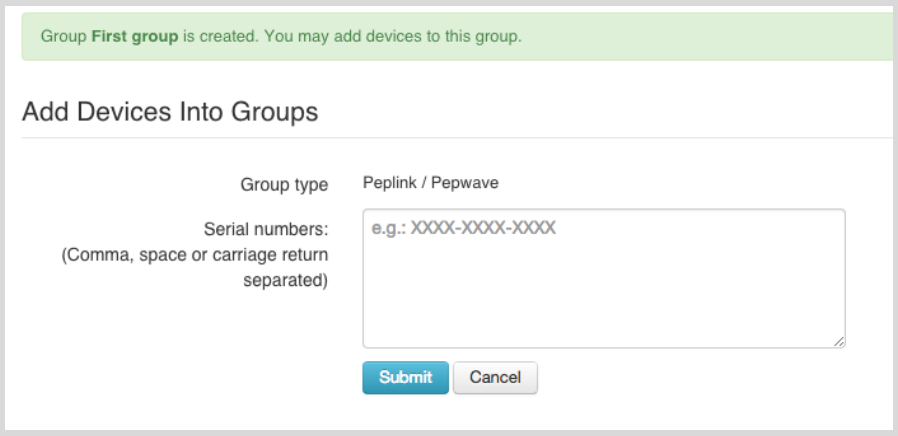
You may create more organizations by entering into an organization (e.g. “My Organization”). Then on the organization menu on the right of the screen, click “Create Organization”.



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 the “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 (if port 5246 is not reachable, port 1443 will be tried)	Device communication for remote web admin.
	TCP 443	Web accesses.
	TCP 80	Automatic acquisition and renewal of SSL certificate for InControl appliance from letsencrypt.org (optional)
	TCP 4443	Web accesses to control panel
	UDP 53	Dynamic DNS service and automatic acquisition and renewal of SSL certificate for devices from letsencrypt.org (optional)
	TCP 2222	Direct remote assistance (optional, needed by Peplink for troubleshooting only when outbound to ra.peplink.com on TCP 443 is not accessible)
Outbound	ra.peplink.com on TCP 443	Remote assistance (optional, recommended)
	api.ic.peplink.com on TCP 443	For lively look up device's model when importing serial numbers (optional, recommended)
	download.peplink.com on TCP 443	Device firmware validation (optional)
	push.ic.peplink.com on TCP 443	Push notifications for the InControl 2 mobile app (optional)
	acme-v02.api.letsencrypt.org on TCP 443	Automatic acquisition and renewal of SSL certificate for InControl appliance from letsencrypt.org (optional)
	*.peplink.com on UDP 5246 (details)	For lively device service expiration date synchronization* and transferring FusionHub licenses from InControl 2 (public cloud) to FusionHub units connected to the InControl Appliance.

		(recommended) * Lively service expiration date sync is required for SaaS and Region Networks identification in outbound policy/firewall rules to work regardless of whether the appliance's license is legacy or modern.
	Time server on UDP 123	Network time sync
	DNS resolver on UDP 53	DNS resolutions

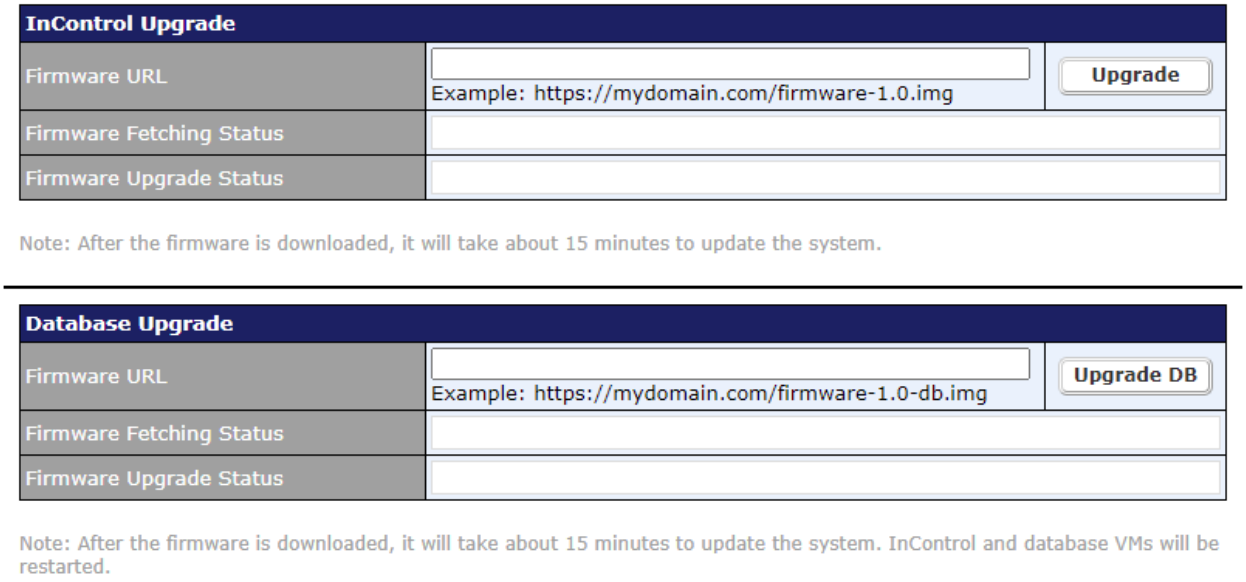
12.1 For Hardware Appliance's Management Port

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 (not required since 2.8.2)

13. Upgrading InControl Virtual Appliance

13.1 Upgrading a system newer than 2.9.0

Starting from InControl Virtual Appliance version 2.9.0, the system could be upgraded by simply submitting firmware URLs to two fields on the control panel page. One field is for the InControl VM, and one is for the Database VM.



You can find the firmware URLs from
https://www.peplink.com/support/incontrol-appliance-images-downloads/

If you are required to upgrade both Database and InControl VMs, you should always upgrade the Database VM first. Upgrade the InControl VM only after the Database VM boots up with the latest firmware completely.

If your system is disconnected from the Internet, you will need to download the firmware files manually and upload them to an internal web server which is accessible by the InControl VM. Then input the firmware files' internal URLs into the two fields on the control panel page. The system will download the files and upgrade the two VMs.

13.2 Upgrading a system earlier than 2.9.0

To upgrade from any release earlier than 2.9.0, you will need to upgrade to 2.9.0.2 first and then upgrade to the latest release by following the instructions in chapter 13.1 above.

To upgrade to 2.9.0.2, you should upgrade the system by replacing the two VMs' system disks. As long as the InControl VM's data disk and Database VM are kept intact, all old settings (including IP address, admin password, etc.) and devices' data will be seamlessly carried over.

Before performing an upgrade, we encourage you to download the latest backup from the control panel first.

13.2.1 For VMware ESXi

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

Step 2. Extract .tgz files on a PC. ".tgz" is shorthand of ".tar.gz". Extract the files with a file extractor on your PC or Mac. (Note: Do not extract on the ESXi server's command shell as its "tar" command is incompatible with the file.)

The extracted file names and sizes are as follows:

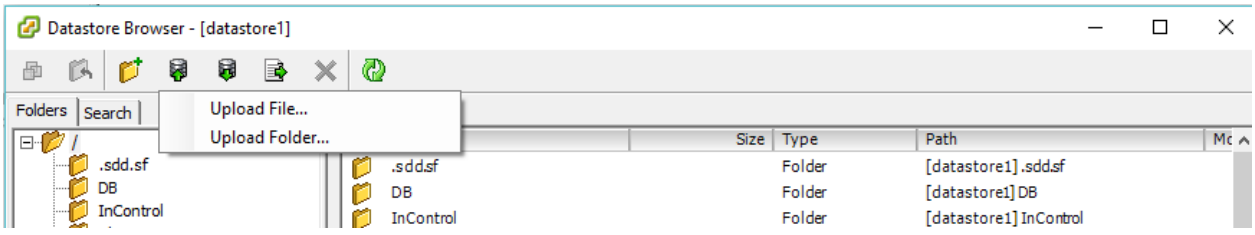
InControl-System-2.9.0.2-vmdk.tgz:

File name	Size (Bytes)
InControl-System-2.9.0.2-vmdk/InControl-System-2.9.0.2-flat.vmdk	25,769,803,776
InControl-System-2.9.0.2-vmdk/InControl-System-2.9.0.2.vmdk	688

DB-System-20210323-vmdk.tgz:

File name	Size (Bytes)
DB-System-20210323-vmdk/DB-System-20210323-flat.vmdk	26,843,545,600
DB-System-20210323-vmdk/DB-System-20210323.vmdk	660

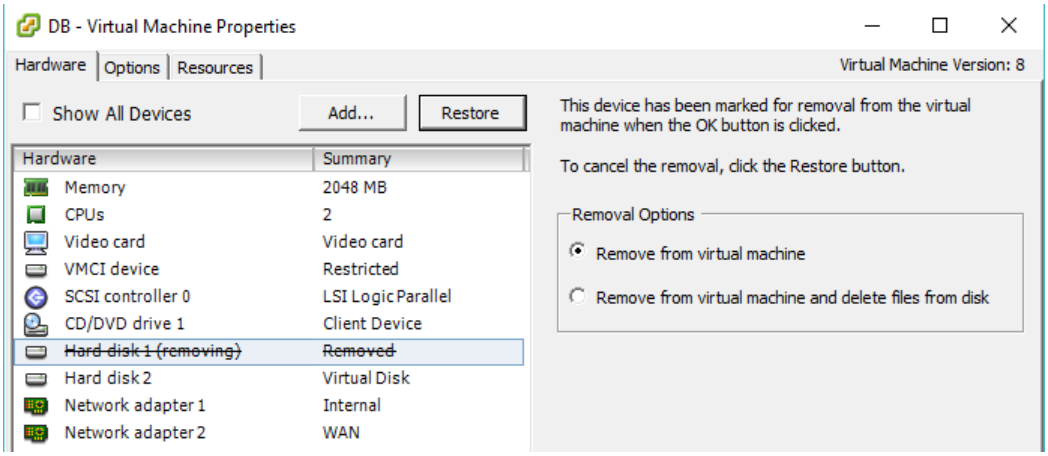
Step 3. Start the Datastore Browser in the vSphere Client. Use it to upload the `InControl-System*.vmdk` and `DB-System-*.vmdk` files to folders, say, "`InControl`" and "`Database`" in the datastore respectively. After finishing uploading the two files, the two files will be shown as one item in the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



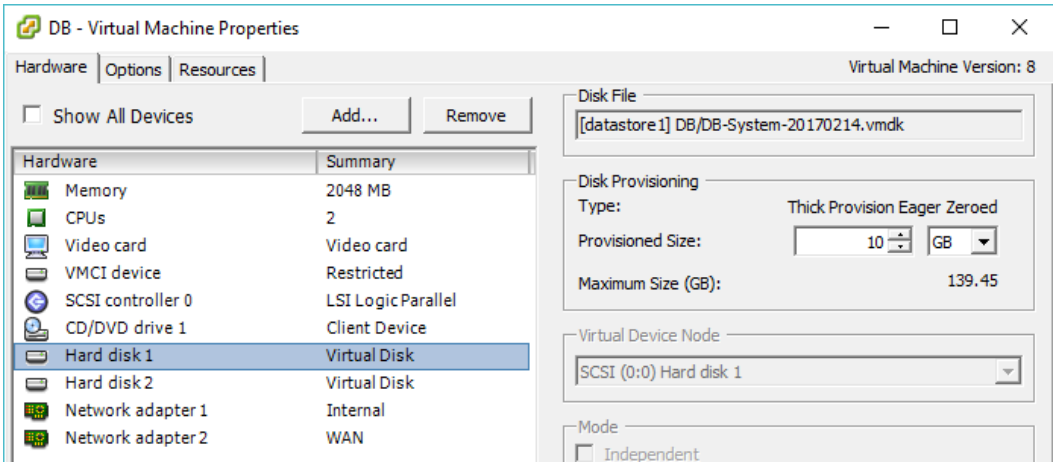
Step 4. Restart VMs in the following order:

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"

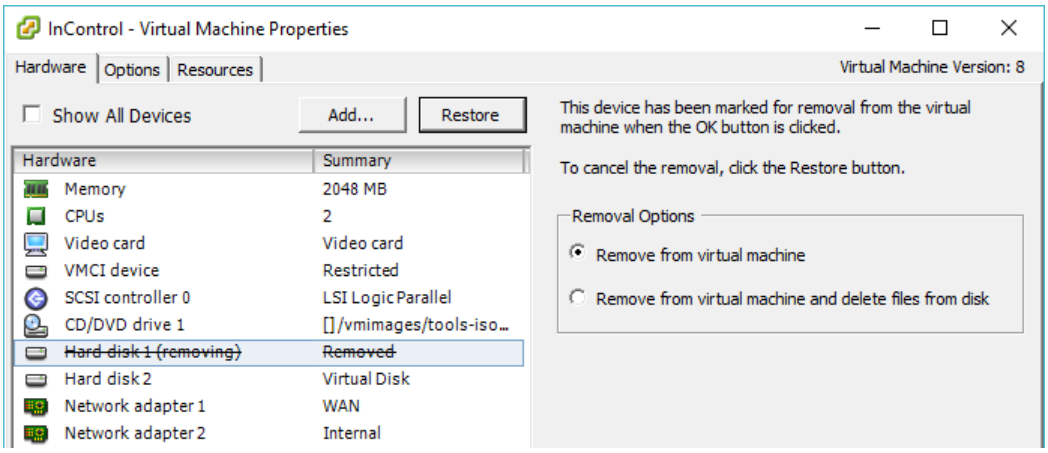


4. Open DB VM Properties again
    - Select 'Add…" > "Existing virtual disk…" > Browse and select the disk file "DB-System-20210323.vmdk"
    - Select SCSI 0:0 Hard disk as the Virtual Device Node

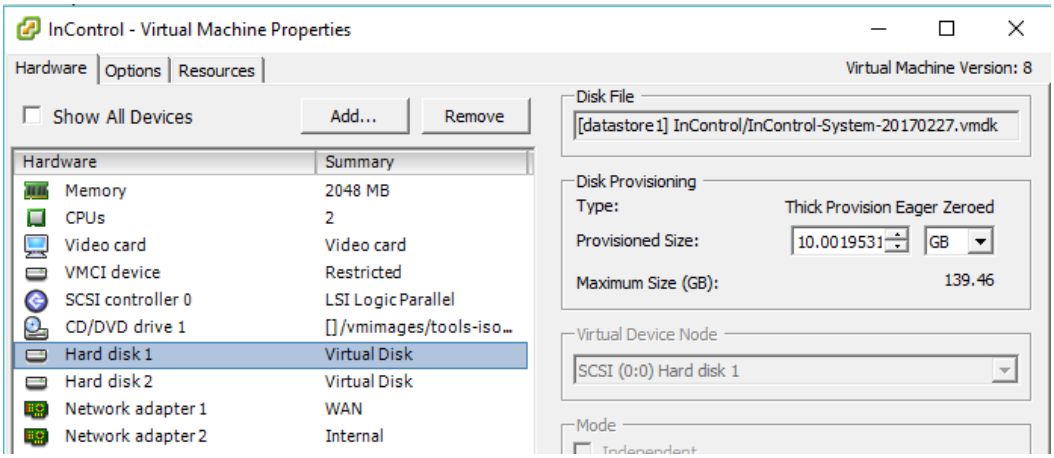


5. Start DB VM
6. Open InControl VM Properties
    - Identify and select the system hard disk (usually "Hard disk 1")
    - Select the "Remove from virtual machine" radio button (without deleting it)

- Press "OK"



7. Open InControl VM properties again
   - Select 'Add…" > "Existing virtual disk…" > Browse and select the disk file "InControl-System-2.9.0.2.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.

13.2.2 For Microsoft Hyper-V and versions prior to 2.9.0

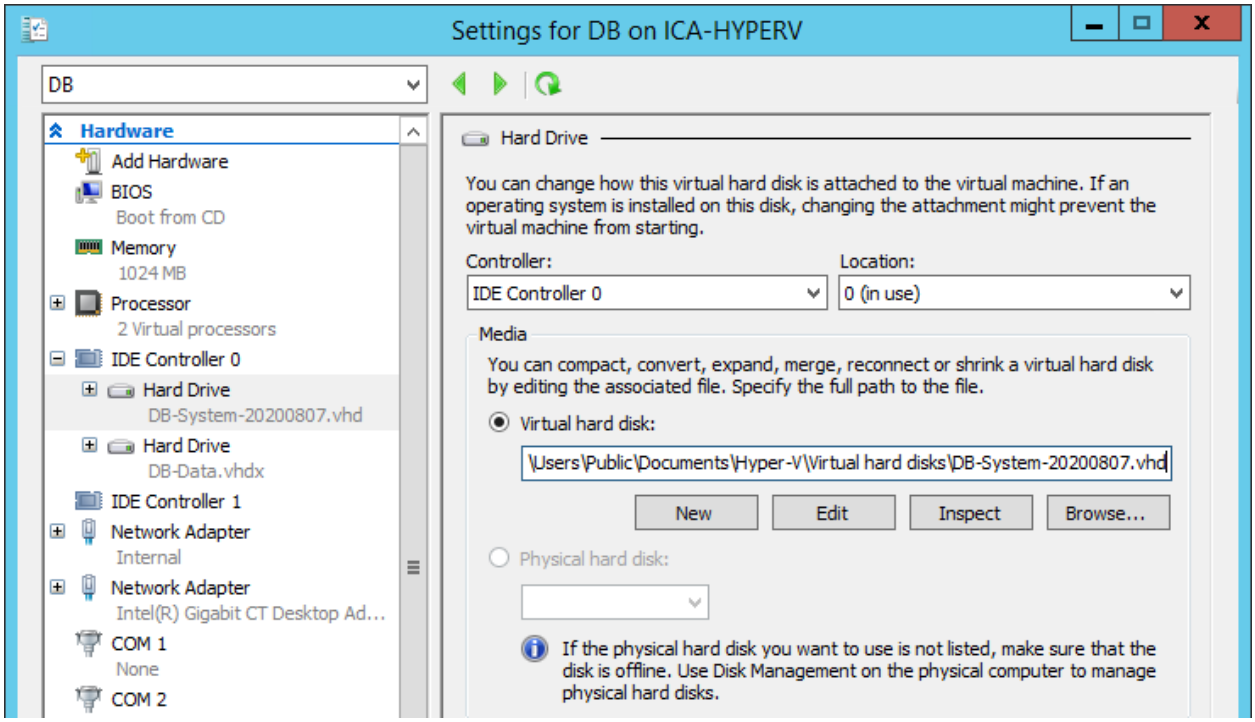
Step 1. Download the Virtual Appliance 2.9.0.2 and Database Server 202103223 image files in `.vhdx` format from https://www.peplink.com/support/incontrol-appliance-images-downloads/

Uncompress the .vhdx.gz files into .vhdx files. The .vhdx file names and sizes are as follow:

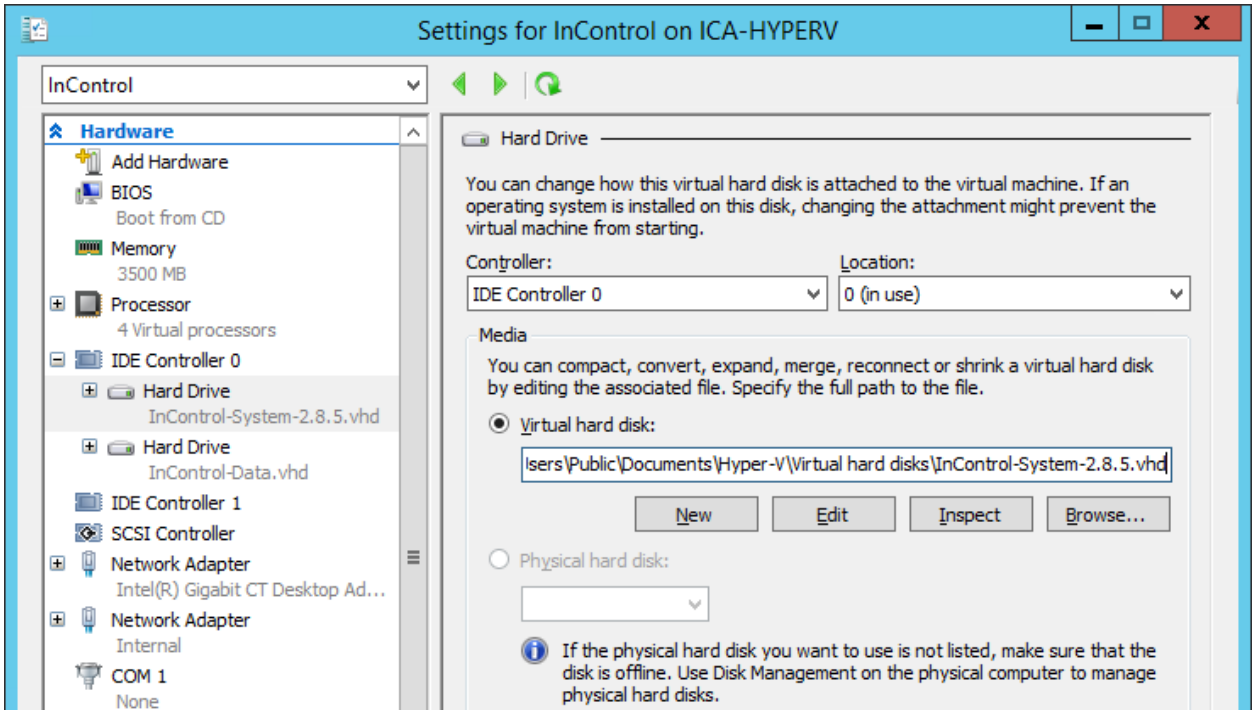
File name	Size (Bytes)
InControl-System-2.9.0.2.vhdx	25,035,800,576
DB-System-20210323.vhdx	25,035,800,576

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-20210323.vhdx` 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-2.9.0.2.vhdx` 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

NOTE: Firmware for InControl Hardware Appliance is only available up to 2.8.6.1.

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.

Note: Before performing an upgrade, we encourage you to download the latest backup from the control panel first.

15. Release Notes

Release notes for 2.10.0

What's new

- Added Remote Desktop, VNC, SSH, and Telnet protocol support to InTouch. See a new setting on the control panel.
- Added clients' device types in client listing.
- Added group-level LAN Network Settings.
- Added route advertisement configurations.
- WAN up/down notifications: added an option to notify for priority-1 WANs only.
- Added Firewall Settings to SSID Settings screen for AP products.
- Web Admin Management
    - Added LAN access settings.
    - Added settings for authenticating with a TACACS+ server.
- SIM Pool

    - Added device online/offline indicators to “SIM card reports” > “Devices and SIM cards”.
    - Device list > Actions menu, added an item: “Create per-device custom SIM pools...”.
    - Added SIM pool usage summary that is sent at the end of billing cycles.
    - Added Pushover notification support to SIM pools.
- PepVPN/SpeedFusion
    - PepVPN connection profiles on devices can now be preserved when moving them between groups where their PepVPN topology profiles are at the group level or creating an organization from groups.
    - Added Packet Fragmentation option.
    - Added advanced parameters for Dynamic Weighted Bonding.
    - Released FusionHub licenses can now be deleted.
    - Added SpeedFusion trial information to device details pages.
    - Supported unmanned license applications to FusionHubs launched in AWS EC2.
    - Fixed: PepVPN management page did not take PrimeCare licenses into account.
- Device list > Column Customization: added a “Cellular Firmware” column.
- Firewall and outbound policy rule set order can now be changed by drag-n-drop.
- Added an e-mail opt-in option to the user profile page.
- Allowed to change not only Wi-Fi radio 2 but all radios’ operating modes (AP or WAN selection).
- In updating device info with a CSV file, if the latitude and longitude values are omitted, they will be looked up from the address field.
- Clicking on an event’s latitude/longitude will open the location in Google Maps in a new browser tab.
- In daily and monthly usage reports, added an option to display projected day-end and month-end usages respectively.
- Bulk configuration: added options to preserve the firewall, outbound policy, and web admin & CLI settings in the uploaded configuration file.
- In creating firewall or outbound policy rules, WAN and PepVPN names can optionally be selected in the connection name field.
- Added options to control the visibility of some UI controls and pages to Group Administrators.
- Added VDSL-specific status information to VDSL WAN details.
- The "Grouped Networks" setting is available to FusionHub-only groups.
- Added a KVM start-up setting in Device System Management.
- Fixed: in Group-level Device & Wi-Fi Reports > Top Devices, device names were not clickable.
- In captive portal profiles, you can now optionally put one of three special variables to the “General Description” field. The variables’ values defined in the control panel will be

displayed in the General Description field on the captive portal login page. This feature is for displaying a time-limited notice in all captive portals in the system without needing to modify every single captive portal profile every time. (InControl virtual appliance only.)

Release notes for 2.9.4.1

What's new

- Fixed: Remote Web Admin was not working in 2.9.4.
- Fixed: extra VLAN networks were displayed for SD Switches when the switch is offline.
- Fixed: Usage of sub-protocols in DPI reports were incorrect.
- Fixed: Disabled Wi-Fi WANs were incorrectly shown on Device Details pages.

Release notes for 2.9.4

What's new

- Added IP-based and serial-port-based InTouch (aka out-of-band management, or OOBM) support. This features allows you to visit client devices' website behind Peplink/Pepwave routers through InControl. Added an "InTouch Settings" item to the device-level Settings menu for configuration. If InTouch profiles are defined, an InTouch button will be shown on the top of the device's details and the group overview screens for accessing the client devices.
  Note 1: IP-based InTouch traffic is counted as SpeedFusion Cloud traffic.
  Note 2: The feature requires firmware 8.2.0 or above.
  Note 3: IP-based InTouch support is disabled by default. It can be enabled on the control panel. A wildcard DNS record and a wildcard SSL certificate are required.
- Revised PepVPN configuration UI and status UI in the logical view. A new color scheme was used. Legends added. The logical view can display very large numbers of nodes.
- Device list > Actions > AP Routing Mode...: added a "Bridge Mode, without LAN IP address" option.
- Device list > Wi-Fi AP State…: offline devices' AP state can now be changed before they come online.
- WAN up/down history: WAN standby event was ignored. It is now treated as WAN up.

Release notes for 2.9.3.2

What's new

- Fixed: the Firmware Releases page at the MSP level might not load.

- Fixed a logical error in Device Expiration Date Synchronization. Devices' InControl hyperlinks showing on Peplink SpeedFusion Connect website incorrectly led to Peplink InControl instead of InControl Appliance.
- Fixed bugs with "Sign-in with Apple".
- Fixed: the Firewall Log menu item was not shown for FusionHub devices.
- Updated the invitation email to be sent to new organization/group users.

Release notes for 2.9.3.1

What's new

- Added an option "Email Daily API Access Report to MSP Administrator" to the control panel
- Fixed: users were signed out when they navigate from hyperlinks on external websites to any InControl pages.
- Fixed: failed to validate custom device firmware URL.
- Fixed: Events in IPsec/PepVPN up/down history might be missing in some situations.
- Fixed: remote web admin might fail in some situations.
- Fixed an ICA firmware upgrade error: "Error! ICVA cannot be downgraded."

Release notes for 2.9.3

What's new

- Added Apple ID sign-in support. Its settings can be found in the control panel.
- Added Amazon Web Services Transit Gateway integration. Please find the setup guide HERE.
- Added data usage reports for all cellular WANs of all devices in a group. For the Device Selection field on the group-level Usage Reports, when more than one product is selected and the devices contain WAN names prefixed "Cellular", the Connection menu will now include an item "Cellular*".
- When deleting a user from an organization, you will be prompted for removing the user from group(s) if the user is a group user too.
- Device-level map: when using the Google Geolocation API to locate devices, the devices' marker will surround by a semi-opaque circle for indicating their possible locations.
- Group and device-level map: added a ruler button. Clicking it will allow you to measure the distance between two or multiple points on the map.

Release notes for 2.9.2.2

What's new

- Fixed: the Device Expiration Date Synchronization for InControl appliances that can communicate with the public InControl was not working.
- Fixed: the retention period for per-minute bandwidth report data was 5 days only. It is now corrected to 14 days.
- Fixed: Timestamps in real-time bandwidth reports may be shown in an incorrect time zone.
- Fixed: error in importing a FusionHub license pack key.
- AWS: added support of EC2 instance types with NVME-based SSD storage. E.g. t3, c5, m5, etc.

Release notes for DB-2021215

Here are the changes since DB-20210323:

- Added support of all x86 based AWS EC2 instance types.

Release notes for 2.9.2.1

What's new

- Fixed: captive portals did not function. A "9001 timeout" error is shown when logging to any captive portals.
- Fixed: only six days of usage data was included in emailed weekly data usage reports.
- Geofencing: if a device is selected by multiple fences, email notifications for all of the fences' events, instead of just the first fence's events only, will now be sent out.

Release notes for 2.9.2

What's new

- Added an option to the control panel for allowing the system to send devices' information to InControl in the public cloud.
- Added an option "Redirect to public InControl" to External InControl Appliance Settings.
- Revamped and simplified WAN Quality Reports:
    - Improved the display of 5G and LTE-A signal data.
    - Added a "signal bar" line to the chart.

    - Detailed signal data is displayed in the tooltip when hovering over a point in the chart.
    - The last selected WAN and chart zoom level are saved and restored in the next visit.
- SSID Settings:
    - Added SSID security mode Enhanced Open (OWE).
    - Added 802.1X version option to WPA2 and WPA/WPA2 - Enterprise.
- Added a per-radio option "Disable when no Internet" to Radio Settings.
- Notifications:
    - Added third-party app Pushover support.
    - Added notifications “PLMN Switch Over” and “Too Many Firmware Update Attempts”.
- Undefined device tags are allowed in all tag fields in configuration screens. The tags will be created upon saving the fields.
- PepVPN configuration:
    - In creating a star topology network, the DR secondary hub device can now be later hardware revisions than the primary hub device.
    - In creating an organization-level profile, devices in PepVPN-disabled groups can now be chosen optionally.
- Devices are allowed to move between groups when the only PepVPN profiles in use are at the organization level.
- Device details:
    - Added event flags to the timeline of the map on device details pages.
    - VLANs and Management Interfaces can now be sortable by VLAN IDs or names.
- Added some quick web admin links to the Remote Web Admin menu.
- "WAN Performance Analysis Server" can be enabled in Device Tools.
- Group Overview:
    - The page navigation control is now available both above and below the device list table.
    - Added firmware version filter on devices.
    - Added devices’ latitude and longitude to device CSV files.
- In group-level Firmware Policy, instead of just the products in the group, all products in the organization can optionally be displayed.
- Added ruleset cloning support to Firewall and Outbound Policy.
- Added a data size unit selector to the quota and initial usage fields in SIM pools of SIM Card Reports.
- Details are logged to the operation log for “Device IP Settings” changes.
- Added an API endpoint for downloading organization-level per-device bandwidth usage: `/rest/o/{organization_id}/bandwidth_per_device`.
- Any excessive IPsec events are now discarded.

- In Device System Management, the length of randomly generated and manually entered web admin passwords have been increased to 12 and 10 characters respectively. A mix of upper and lower case alphabets and numbers is also required.
- When users change their passwords, all sessions except the existing one will be invalidated (signed out). The user will also be notified by e-mail for the change.

Release notes for 2.9.1.5

What's new

- Fixed: a scheduling service failed to start up on InControl appliance 2.9.1.4. The following features were affected. Last GPS location may be lost. Firmware cannot be applied to devices. LetsEncrypt certificates cannot be renewed. Organization-level SIM usage reports are not updated.
- Fixed: a web server's log file was not rotated. The InControl data disk usage kept growing.
- Fixed: InControl incorrectly enabled the DHCP server on LAN/VLANs where the LAN/VLANs are device-managed and their DHCP setting is disabled on the device end.
- Fixed: InControl pages cannot be loaded occasionally.
- Removed Google ID authentication support from captive portals.

Release notes for 2.9.1.4

What's new

- Fixed: the API and captive portal service may stop responding when captive portals are applied to Balance/MAX and their usage is very high.
- Improved the performance in loading the PepVPN configuration page for groups/organizations that contain many devices and profiles.
- Fixed: report e-mailing was not working.
- Fixed: e-mail alerts were not sent and firmware was not applied under a rare network condition (where the hostname reversely resolved from the ICA's WAN interface's IP address is not forwardly resolvable).
- Fixed: the organization listing in the MSP System Usage Reports did not include the pre-created default organization when the system is newly set up.
- Fixed: an access token cannot be acquired on the API documentation.
- Fixed: an extended DHCP option defined in VLAN networks cannot be applied to devices.
- Fixed: incorrect WAN as LAN ports' status.
- Fixed: duplicated geofencing notifications might be sent

Release notes for 2.9.1.3

What's new

- Fixed: firmware profiles cannot be added to MSP-level Firmware Releases.
- Fixed: GA device firmware profiles were not imported from InControl regularly (for systems with outgoing access to api.ic.peplink.com on TCP port 443).

Release notes for 2.9.1.2

What's new

- Fixed: an error "Failed to submit license" incorrectly displayed in saving an InControl Appliance license key while the key is actually applied successfully.
- Fixed: Wi-Fi WAN's RSSI-to-signal-level mapping in WAN Quality Reports
- Fixed an XSS vulnerability with the captive portal system.
- Fixed: the server name in HTTP/S notification URLs did not allow private IP addresses.
- Fixed: failed in logging in as admin@my.domain for fresh installations.

Release notes for 2.9.1.1

What's new

- Fixed: InControl Appliance's SNMP service was not working
- Fixed: Find My Peplink service did not respond to DNS queries.
- Fixed: over counted clients' usages in hourly, daily, and monthly usage reports.
- Fixed: weekly usage reports were not emailed out.
- Fixed: sharable Captive Portal Preview URL was broken
- Enhanced: ensured user-password-related emails are delivered.

Release notes for 2.9.1

What's new

- Added a few security enhancements on MSP user sessions:
    - Added an option on the MSP Settings page: "Force MSP users to enable two-factor authentication".
    - Added an option on the MSP Settings page: "Require two-factor authentication for all MSP users every time they sign in"

    - When MSP admin signs in with a Google ID, the "*I do not have the authenticator with me*" link is now unavailable on the two-factor authentication sign-in screen.
    - MSP administrators can disable a user's two-factor authentication. After disabled, the user will receive a notification.
    - Replaced the MSP setting "Idle Sessions" with "Session Timeout". MSP user sessions will not last for more than this amount of time.
- Fixed: unable to import 8.1.2 firmware profiles from InControl 2 for systems with Internet connectivity.
- Fixed a compatibility issue in sending email notifications via Gmail introduced in 2.9.0.6.
- Fixed: unable to renew ICA's SSL certificate from Let's Encrypt.
- Device Details: enhanced the display of band information for 5G, LTE-A, and LTE.
- WAN Quality Reports: added secondary band information for 5G and LTE-A to the graph.
- Added: Device-level hourly, daily, and monthly PepVPN and per-SIM-slot cellular data usage.
- Added: Wi-Fi mesh and Band Steering settings in SSID Settings.
- Added: SNMP service configuration for devices.
- Added Protocol > DSCP to outbound policy & firewall rules.
- Bulk configurator: DDNS settings are now preserved.
- Added org_id, group_id, and SSID to HTTP/S notification response contents.
- Added: SD-Switch VLAN Usage and Station Usage.
- Added: emailing of group-level daily, weekly, and monthly device reports, Wi-Fi reports, usage reports, SIM pool reports, and the existing captive portal reports. At the organizational level, added usage reports and SIM pool reports. See the "Report Emailing" menu item under the group and organization Settings menu.
- Added a geo-fencing action which changes firmware schedule to "immediately". This allows a device to initiate a firmware update when it enters a geo-fence.
- Added "Passcode Management" to Device System Management > LCD Front Panel.
- Added: an Access Control List can now be imported from a configuration or text file.
- Added a "Sender E-mail Address" field to Captive Portal Settings for the E-mail access mode.
- Fixed: when a device's outbound policy (or firewall rules) is managed by InControl while its firewall rules (or outbound policy) are locally managed, all locally defined grouped networks will be removed even if they are being referenced by some locally managed firewall rules (or outbound policy). InControl now allows both device- and InControl-managed grouped networks to co-exist.
- Fixed: if a device is removed from an organization with the "retain settings" option enabled when it is added to another organization, its setting could not be retained.
- Added group-level API endpoint for enabling/disabling an SSID.
- Added SIM Slot status information to SIM Injector's Details screen.

Release notes for 2.9.0.6

What's new

- Added support of syncing PrimeCare license key to devices in an Internet-isolated environment. Please refer to "Device Expiration Date Synchronization" in chapter 1.10.
- Fixed: the API service might fail health checks and be restarted every 12 hours.
- Fixed: the API service cannot start up in a rare network environment (where the hostname reversely resolved from the WAN interface's IP address is not forwardly resolvable).

Release notes for 2.9.0.5

What's new

- Fixed: GPS location data, Event Log, WAN Quality data, firewall log, per-minute reporting data, and Air Monitor data were not archived into the configured external archive server (e.g. FTP, SFTP server). When the archived data is accessed, an error will be seen.
- Fixed: an "INTERNAL_ERROR" message displayed on Device Details screens for GPS devices that did have GPS location data but are not available in the last 3 days.
- Fixed: An "*All managed devices are offline right now!*" error message was incorrectly shown on the control panel of systems loaded with a legacy license and has not synced devices' service dates with the public InControl for more than 8 days.

Release notes for 2.9.0.4

What's new

- Added support of acquiring the InControl website's SSL certificate from Let's Encrypt automatically. See the Control Panel.
- Added: "Website Restrictions (Allowed Referrers)" settings under "User Profile > Client Applications".
- Fixed: SIM data and WAN signal usages were not recorded to the database in previous 2.9.0 releases.
- Fixed: when the MSP-level setting "show warranty expiration dates and notices" is disabled, the dates and notices in the organization-level device list were still shown.
- Fixed: No default values were filled for "MSP Settings > System Page Message" fields.
- Fixed: Bandwidth allowance and SIM card switching notifications were not sent in previous 2.9.0 releases.

- Fixed some UX issues on firmware upgrade.
- Added InControl website URL and serial number to the VM console.

Release notes for 2.9.0.3

What's new

- New: For systems loaded with a legacy license, InControl subscription expiry dates and expiration notices are no longer displayed.
- Added an MSP-level setting and an organization-level setting for choosing to show warranty expiration dates and notices or not.
- Fixed: If a group's devices are not browsed often on the web interface, the devices would disappear.
- Fixed: the datepicker UI controls on the MSP-level reports were broken.
- Updated: group-level hourly, daily, and monthly data usage reports now include the usage of devices that belonged to the group but have been moved away or removed.

Release notes for 2.9.0.2

IMPORTANT
This release requires Database VM version 20201214 or above.

What's new

- The underlying system has been completely reimplemented. It is now based on Ubuntu 20.04.
- Since this release, a device service expiration date validation is enforced. Only devices that are in warranty or covered by InControl subscription will appear online and be manageable. The first 7 days after upgrading to 2.9.0 (or above) is a grace period. No device expiration date check is enforced during the period. Whilst systems with a legacy license are not affected. The maximum number of managed online devices is still governed by the license number. For more details, please refer to chapter 1.9 Software License.
- The system will also automatically synchronize warranty, subscription, and PrimeCare expiry dates, as well as product definition and firmware releases, from the public InControl over the Internet. For installations that are isolated from the Internet, whenever any device service contract with Peplink has been renewed, the administrators will have to prepare a PC which has web access to both the InControl appliance system and the public InControl. On a web browser on the PC, navigate to the MSP-level Device Management page

(`https://{ICA_Address}/r/msp/device_management`) and click the Synchronize button in the “Device Expiration Date Synchronization” section. The web browser will act as a proxy to synchronize the dates for the InControl appliance from the public InControl. For more details, please refer to chapter 1.10.

- Both InControl and Database VMs support upgrading to future releases by issuing a firmware URL to the control panel. No system disk image replacement on the hypervisor will be required.
- Added support of running on Amazon Web Services and Google Compute Engine.
- Added: Local Service Firewall Rules.
- Added: Imported grouped networks and Outbound Policy with grouped networks from a config file.
- Supported enabling/disabling Air Monitor mode for products with a built-in AP. Require AP One firmware 3.6.2, 3.7.3, and 3.8.1 or above, and Balance/MAX firmware 8.1.1 or above.
- Added “Locate Device Position by Cell ID and Signal” settings in Organization Settings. Devices’ location could be looked up from cell ID and signal strength every five minutes when GPS location data is unavailable but cellular signal data is available.
- VLAN Networks
    - If the Default VLAN setting in a group’s VLAN Network Management page has not been configured, the default VLAN on the SD Switches will now be left unmanaged instead of setting to VLAN ID 1.
    - Added: VLAN network management can be disabled for SD Switches.
    - When IP clash is detected when adding a VLAN to a device, instead of auto picking another subnet, the VLAN will now be skipped.
    - The VLAN ID field on the SSID Settings screen can now be selected from one of the defined VLAN Networks.
- Added auto channel selection schedule for Wi-Fi APs under group-level Radio Settings.
- Added a Tags item under group levels reports. It shows what tags are applied to and allows you to add descriptions to them.
- Moved “OOBM Web Console” item out from the Settings menu to an “OOBM” button on the Device Details page top. Multiple serial ports are supported.
- Added a custom "Service provider" field to Ethernet and Wi-Fi WANs. Devices can be searched by this field in the device list.
- Added an option to force only Super Organization Administrators or all administrators to sign in with Two-Factor Authentication.
- For SIM cards with no MTN provided by the carrier, a custom MTN can now be defined for them in WAN details. Remarks for SIM cards can now also be defined under SIM Card Reports.
- Group listing in the Group Management page can be downloaded as a CSV file.
- Added API endpoints for creating, updating and deleting SIM Pool profiles.

- Device IP Settings: add DHCP reservation support.
- Display SpeedFusion Cloud service status on Device Details.
- On Organization and Group Level Settings screens, the user list can be downloaded as and uploaded from a CSV file.
- Added "Nautical metric" to the Unit field in Organization Settings. Changed "Nautical" to "Nautical imperial".
- Event Log: added types “AP Controller” and “RADIUS”.
- InControl Options: added a "WAN quality data sampling interval" setting.
- Operation Log
    - Filtered events could be downloaded as a CSV file.
    - Added time zone setting.
    - Added source IP address to all sign-in’s events.
- When live status queries are disabled on the InControl Options screen, the Real-Time Bandwidth chart in device-level Bandwidth and Usage Reports is no longer displayed.
- Added notifications for “Device starts up” and GPIO events.
- Device Web Admin Management settings can now be applied to selected devices in a group only.
- SIM Reports: Add support of using ICCID to identify a SIM card.
- PepVPN / SpeedFusion Cloud.
    - PepVPN status is now shown on device lists.
    - The number of connected and configured PepVPN and SpeedFusion Cloud connections is now shown on device details and device list.
    - Fixed: For non-FusionHub devices, the “PepVPN Layer 3 Isolation option” under “Device Details > Edit” was not working on non-FusionHub devices. It has now been replaced by a new option “PepVPN Route Isolation”.
- Device Details screen shows whether the device is inside or outside a geofence.
- Device System Management: added “CLI SSH & Console” settings for SD Switches. The “Web Admin Access” settings also cover AP One devices.
- For users who are an administrator of multiple organizations, on the organization and group listing screen showing after logging in, they can now search for devices by name, s/n, model name or product code among all organizations and groups that they manage.

Release notes for DB-20210323

Here are the changes since DB-20201013:

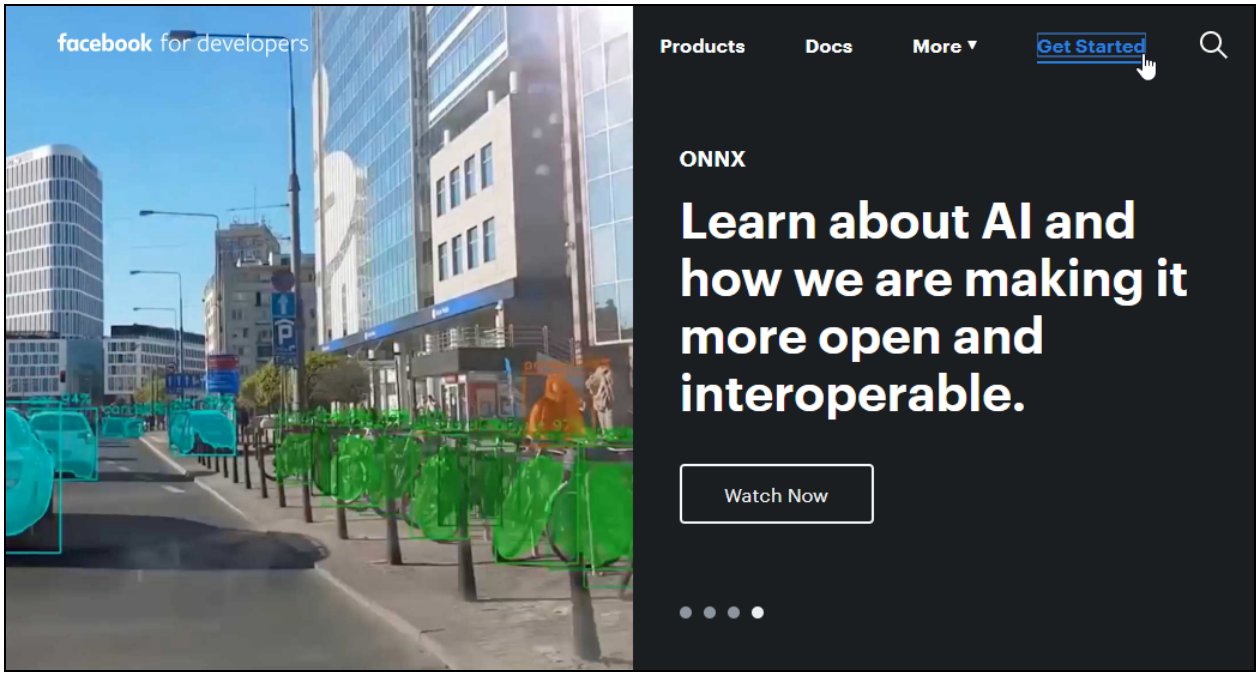
- Both InControl and Database VMs support could be upgraded by issuing a firmware URL to the InControl VM’s control panel since the next release. No system disk image replacement on the hypervisor will be required.
- Added support of running on Amazon Web Services and Google Compute Platform.

Appendix 1: Procedure for creating a Facebook App ID

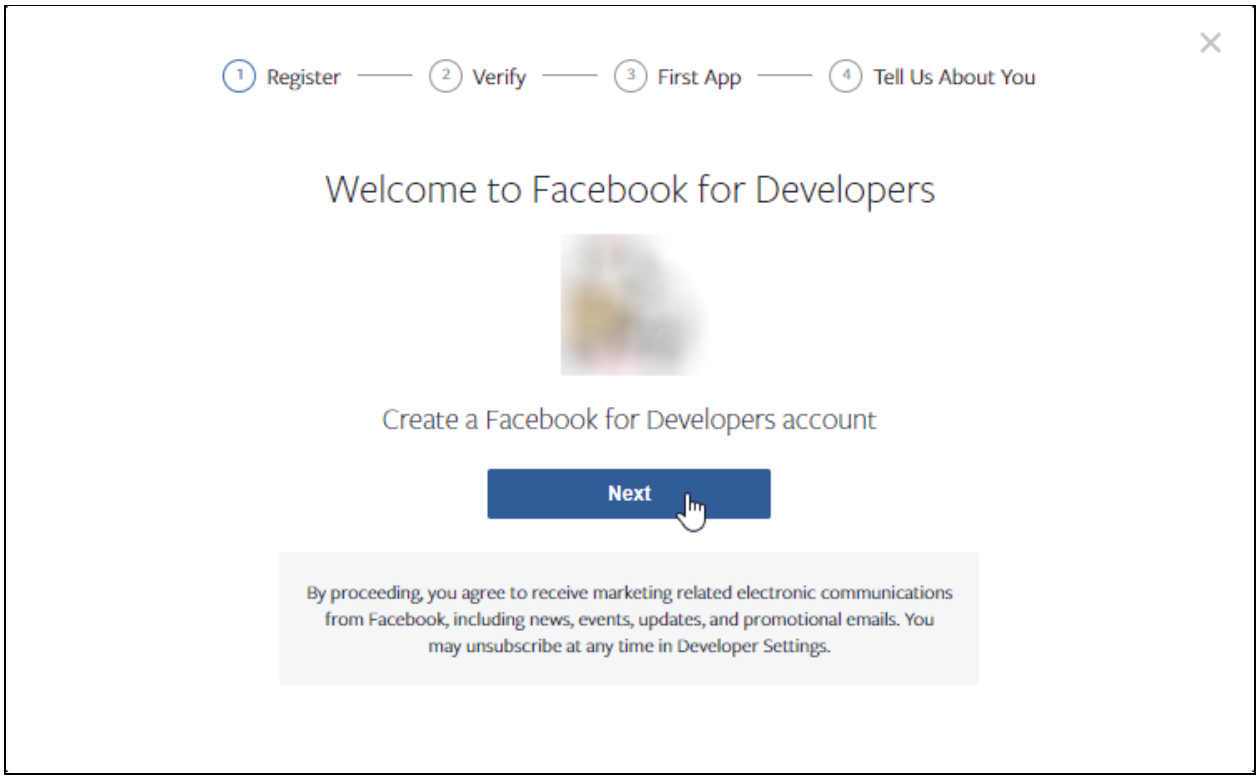
For the "Sign-in with Facebook" feature in the captive portal to work, a Facebook app has to be created in Facebook's developer console. Before InControl 2.6.2, Peplink shared its own Facebook App for all InControl appliance installations. Since InControl 2.6.2, Peplink's App ID no longer shares with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

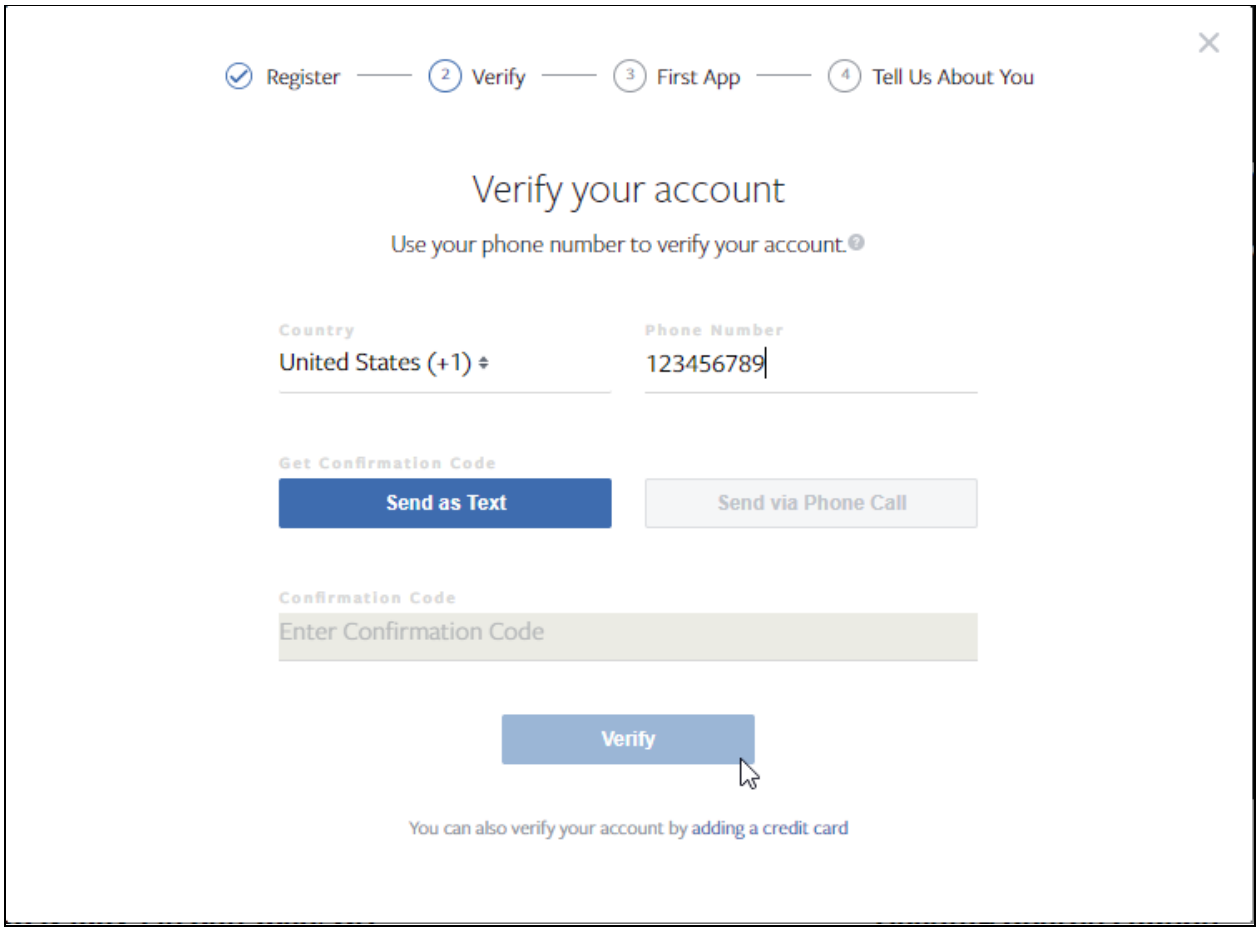
Below is a procedure for Facebook app ID creation:

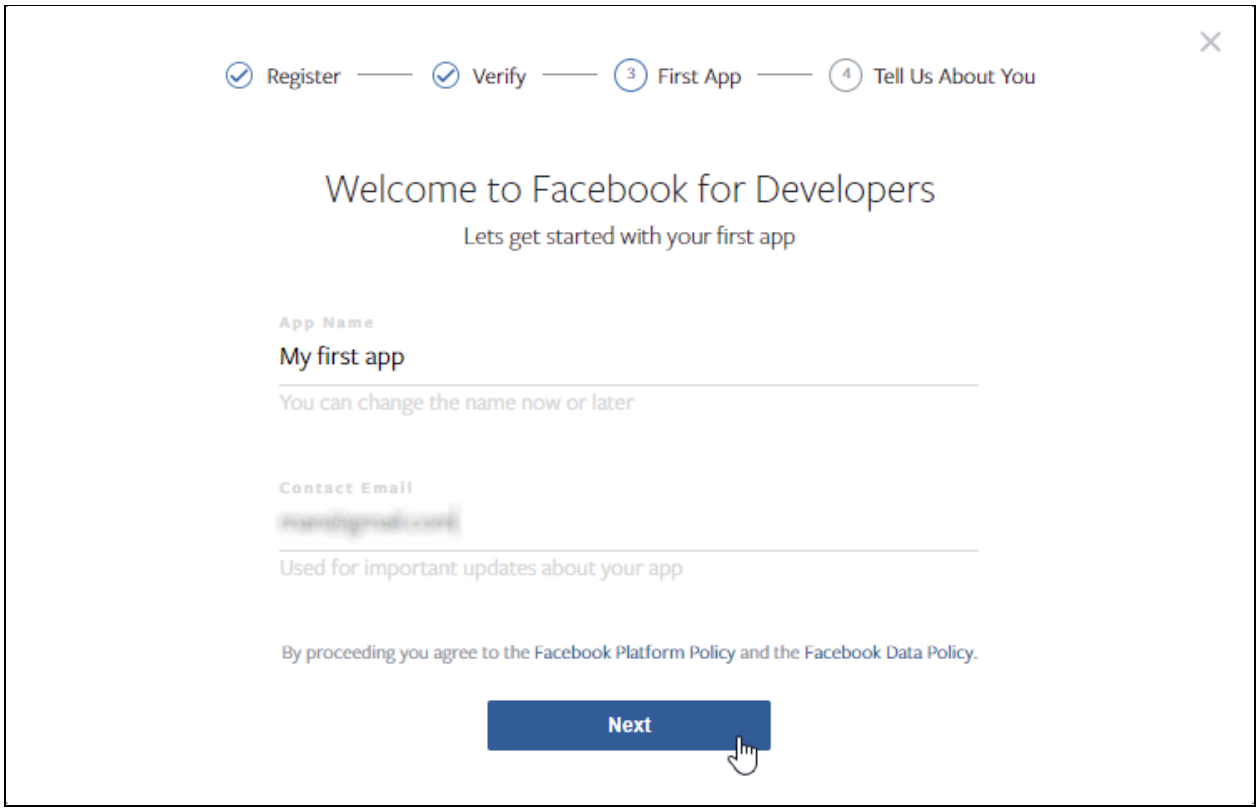
1. Login to https://developers.facebook.com/ and click Get Started:

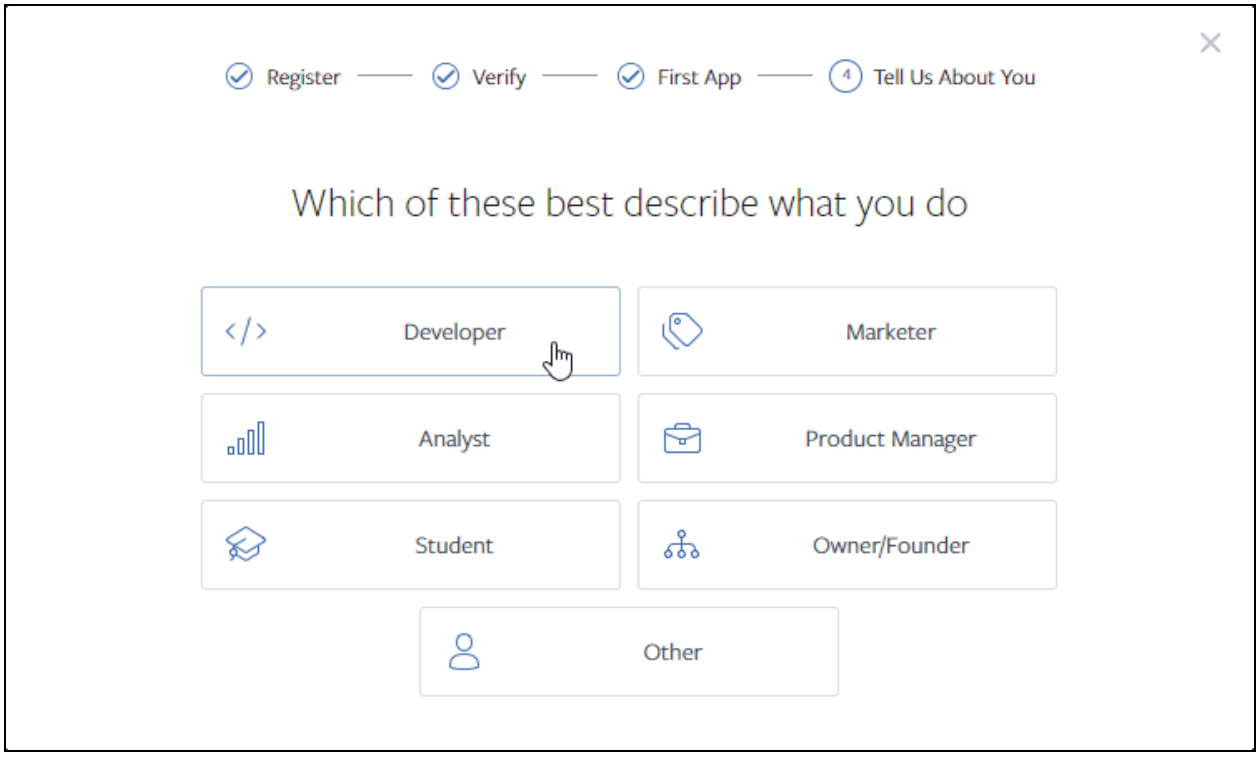


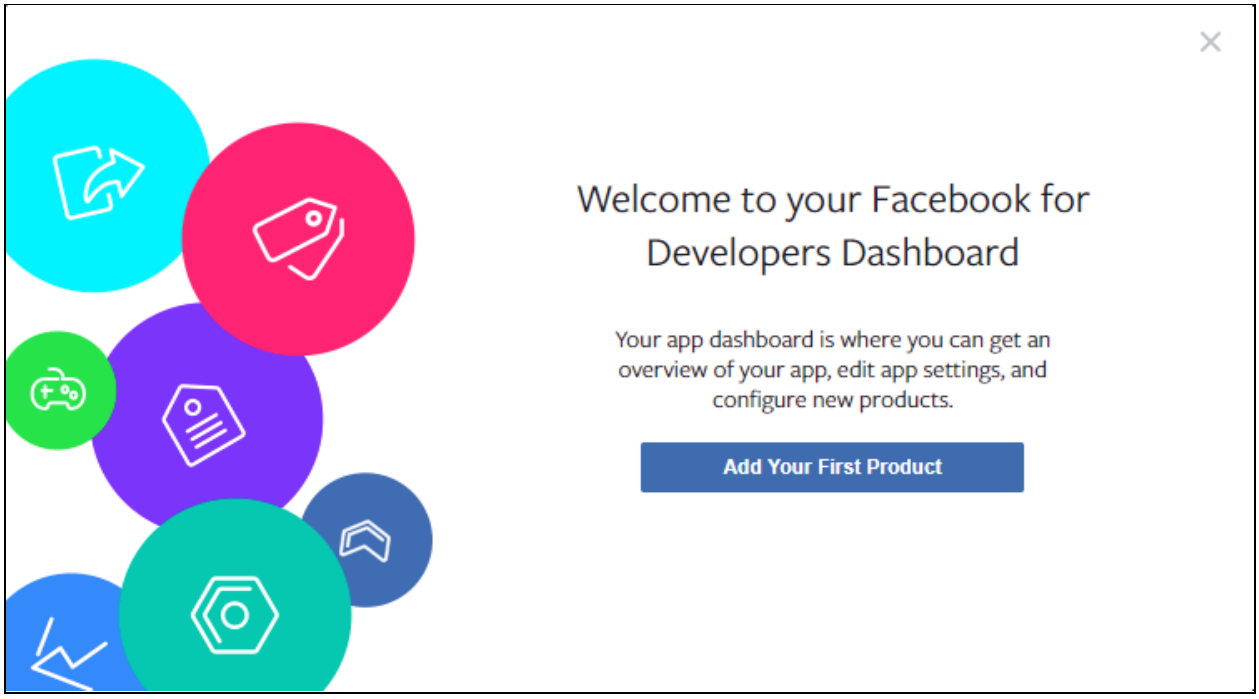
2. Go through the wizard by following the on-screen instructions. Click the "Add Your First Product" button on the final step.


1 Register
2 Verify
3 First App
4 Tell Us About You
Welcome to Facebook for Developers
Create a Facebook for Developers account
Next
By proceeding, you agree to receive marketing related electronic communications from Facebook, including news, events, updates, and promotional emails. You may unsubscribe at any time in Developer Settings.

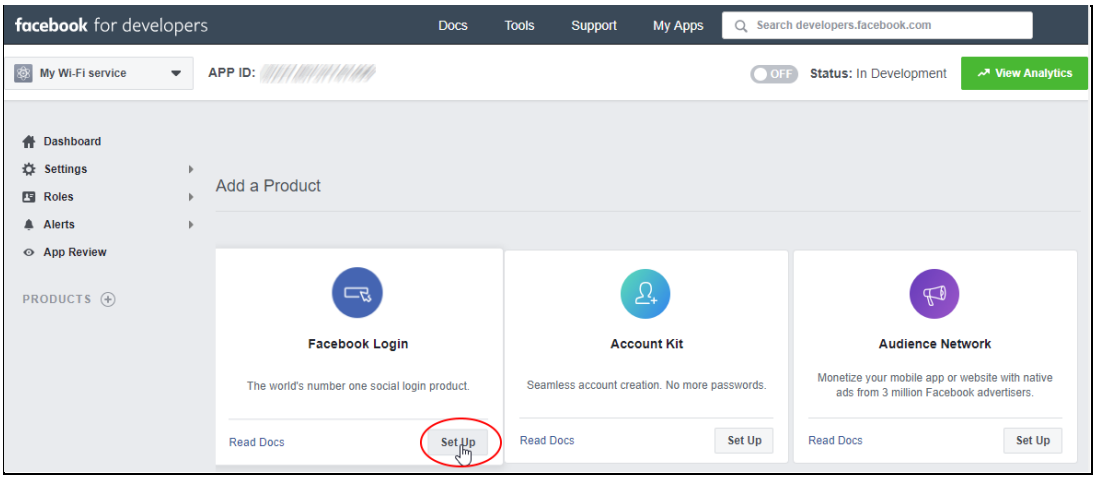

Register
2 Verify
3 First App
4 Tell Us About You
Verify your account
Use your phone number to verify your account.
Country
United States (+1)
Phone Number
123456789
Get Confirmation Code
Send as Text
Send via Phone Call
Confirmation Code
Enter Confirmation Code
Verify
You can also verify your account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

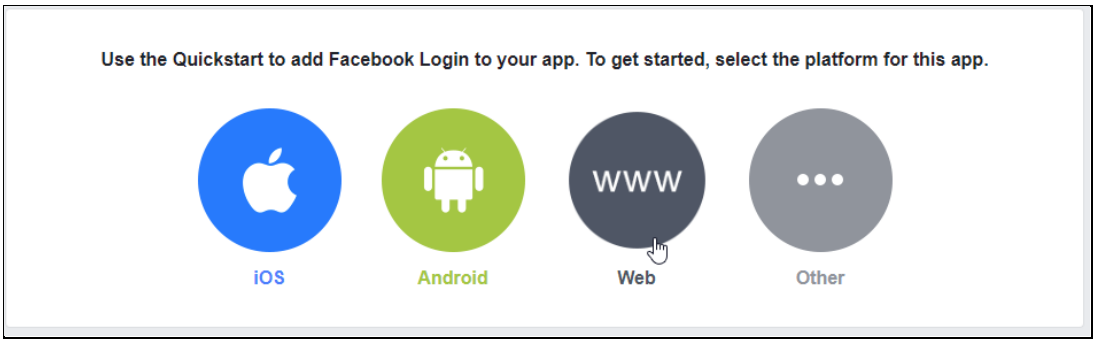

Register
Verify
First App
4
Tell Us About You
Which of these best describe what you do
Developer
Marketer
Analyst
Product Manager
Student
Owner/Founder
Other


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

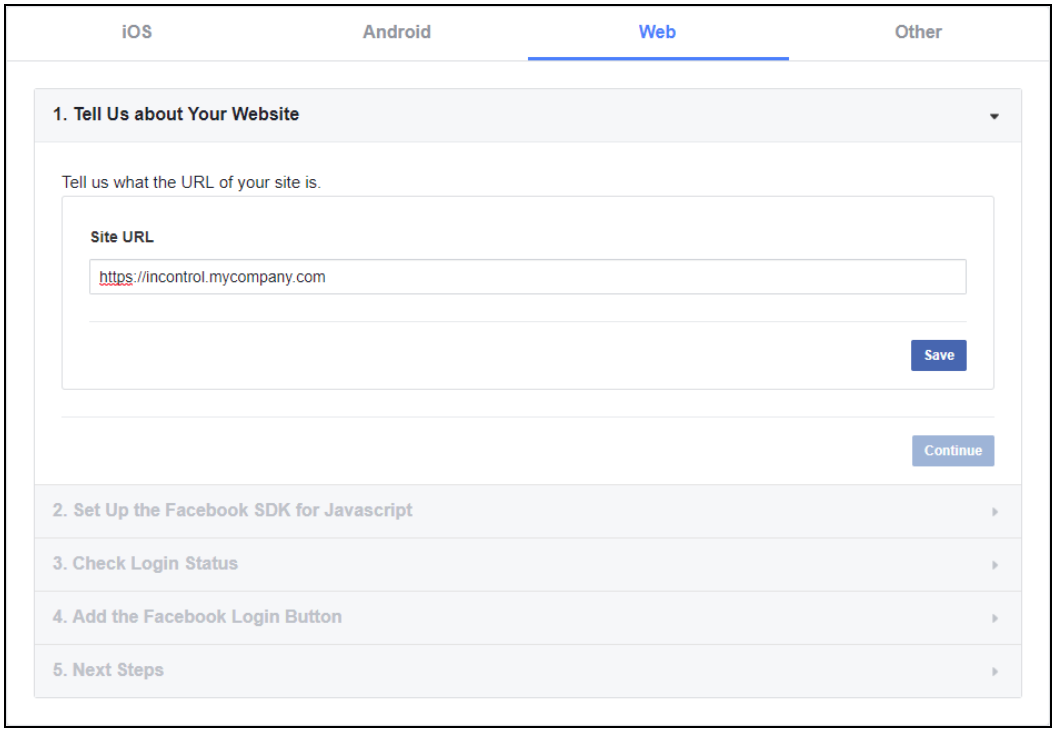
3. Click the “Set Up” button on the “Facebook Login” control



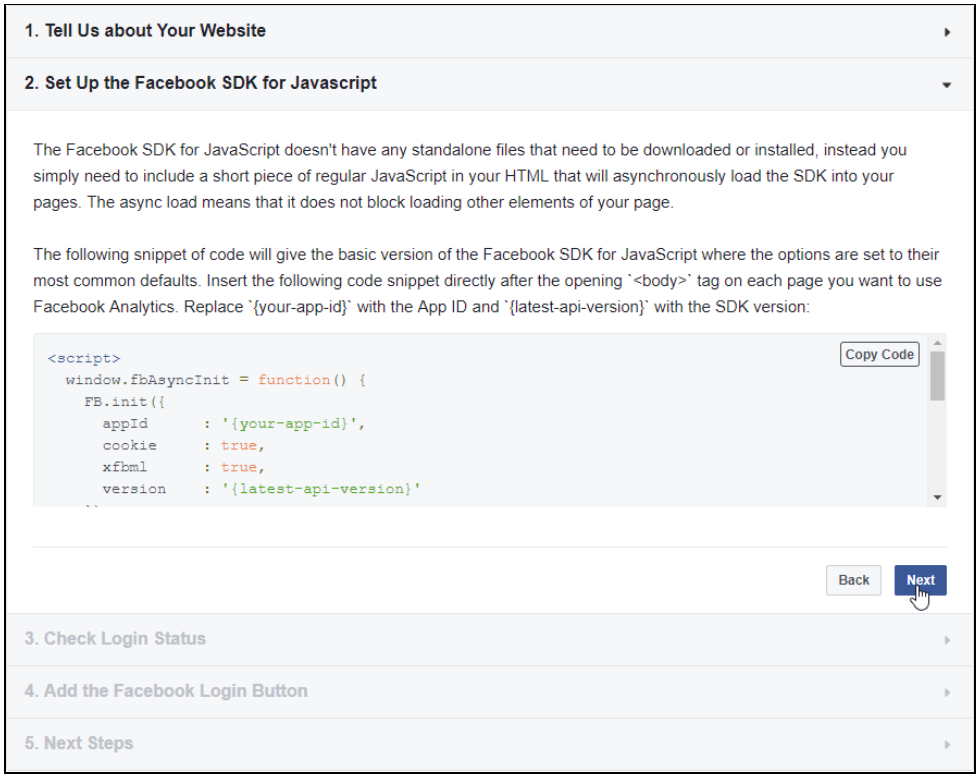
4. Click “Web”



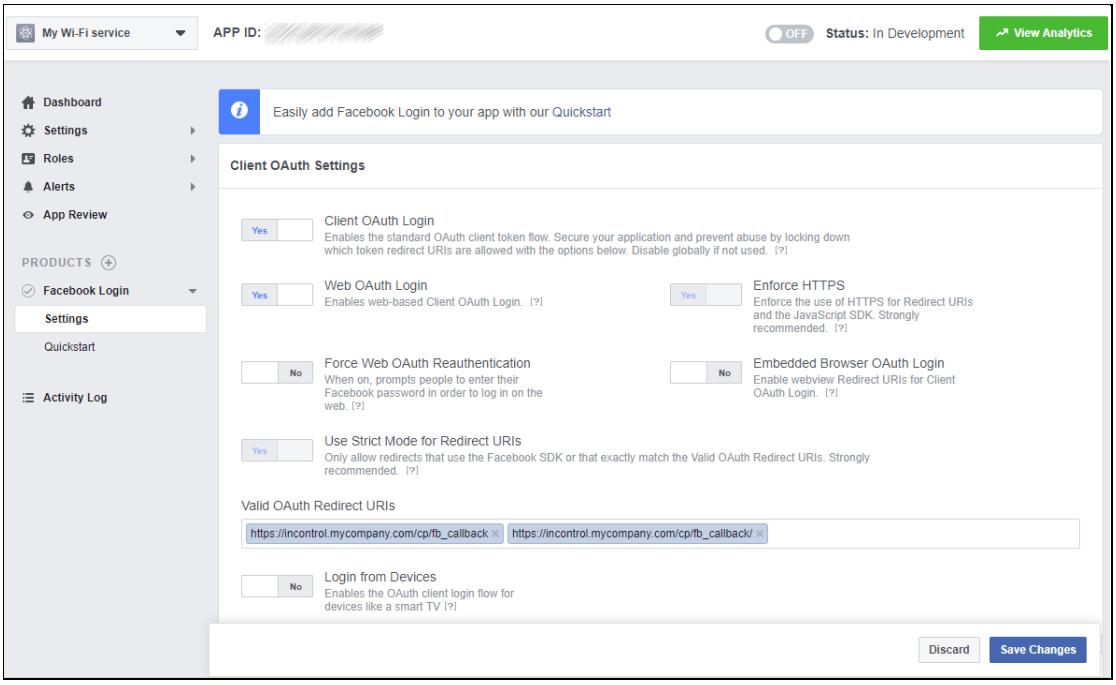
5. Input your InControl appliance's URL into the Site URL field:



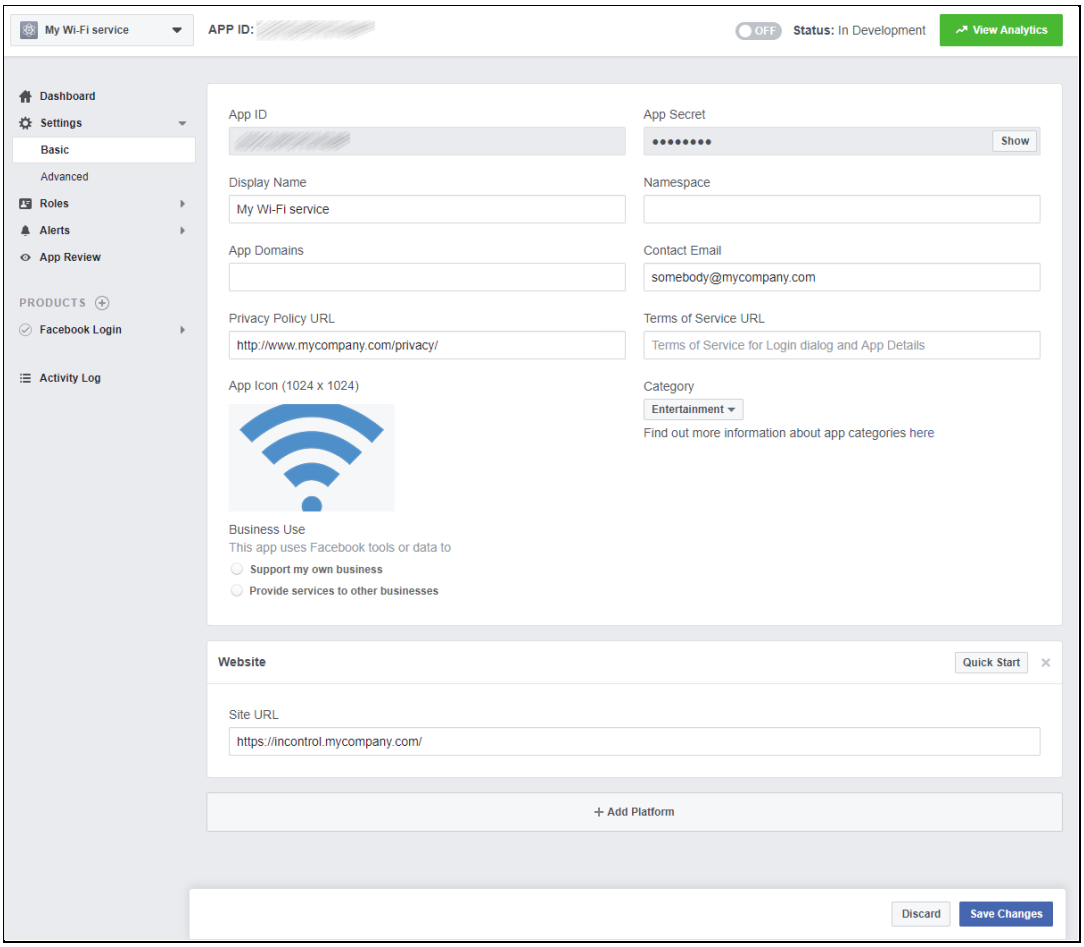
6. Click "Next".



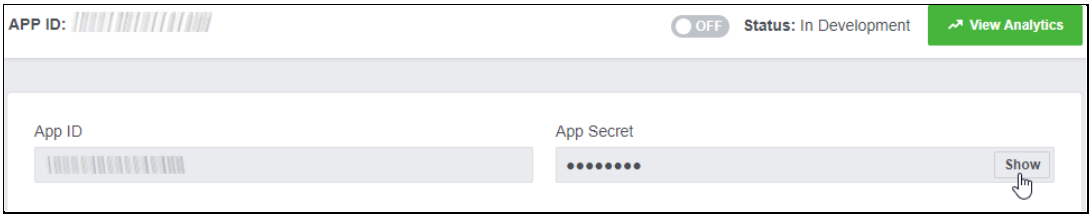
7. Input the following URLs into the “Valid OAuth Redirect URIs” field: `https://[InControl_URL]/cp/fb_callback` and `https://[InControl_URL]/cp/fb_callback/`



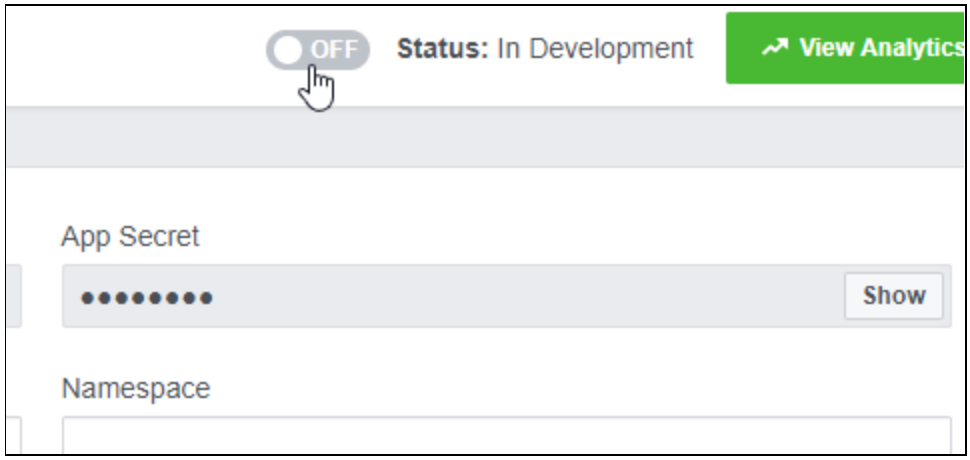
8. Fill in “Display Name”, “Contact Email”, “Privacy Policy URL” fields accordingly. Upload an App Icon in the dimension of 1024x1024. Press “Save Changes”.

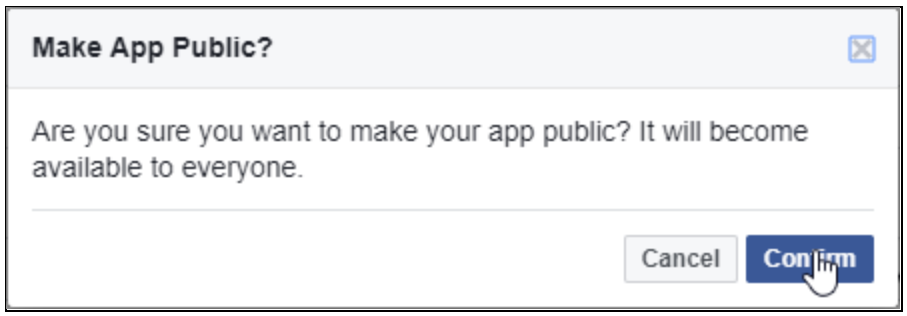


9. Click the “Show” button to reveal the App Secret. Record the App ID and App Secret and input into the InControl Control panel’s “Facebook App Settings” field.



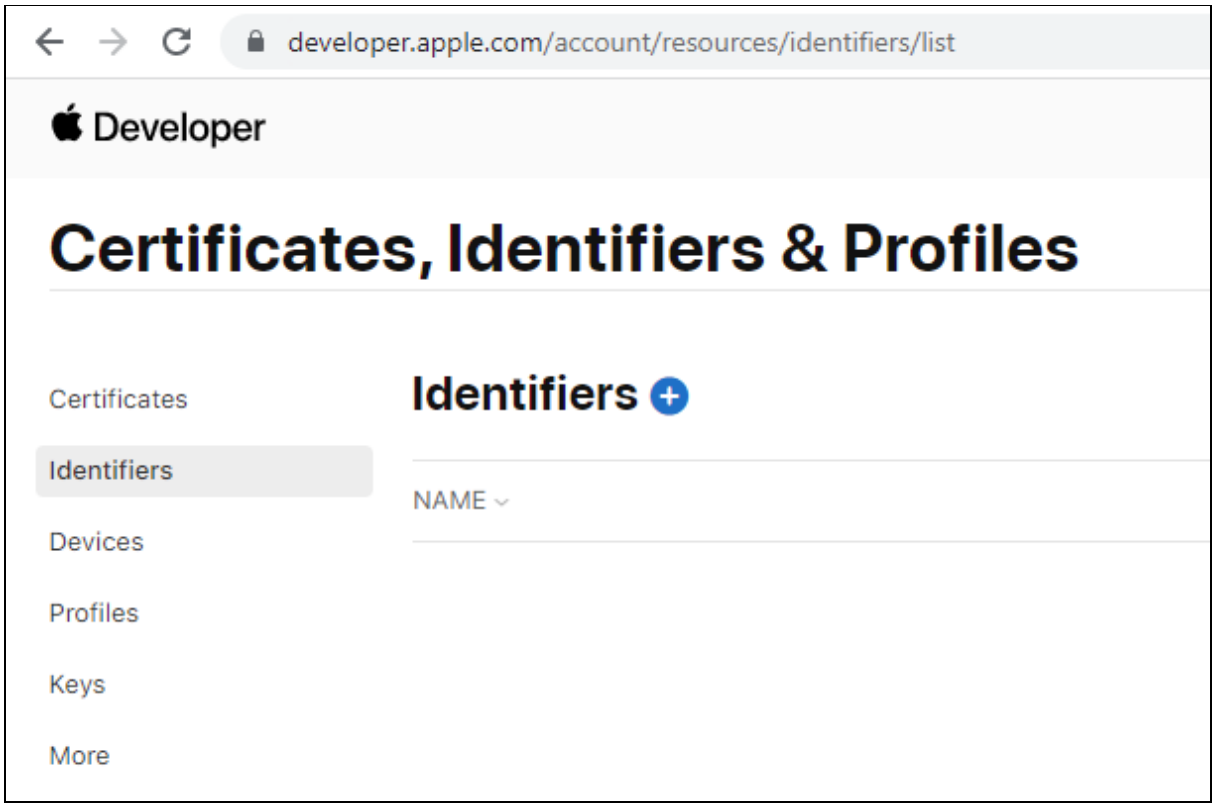
10. Finally, click the OFF switch and click Confirm to make the app public.



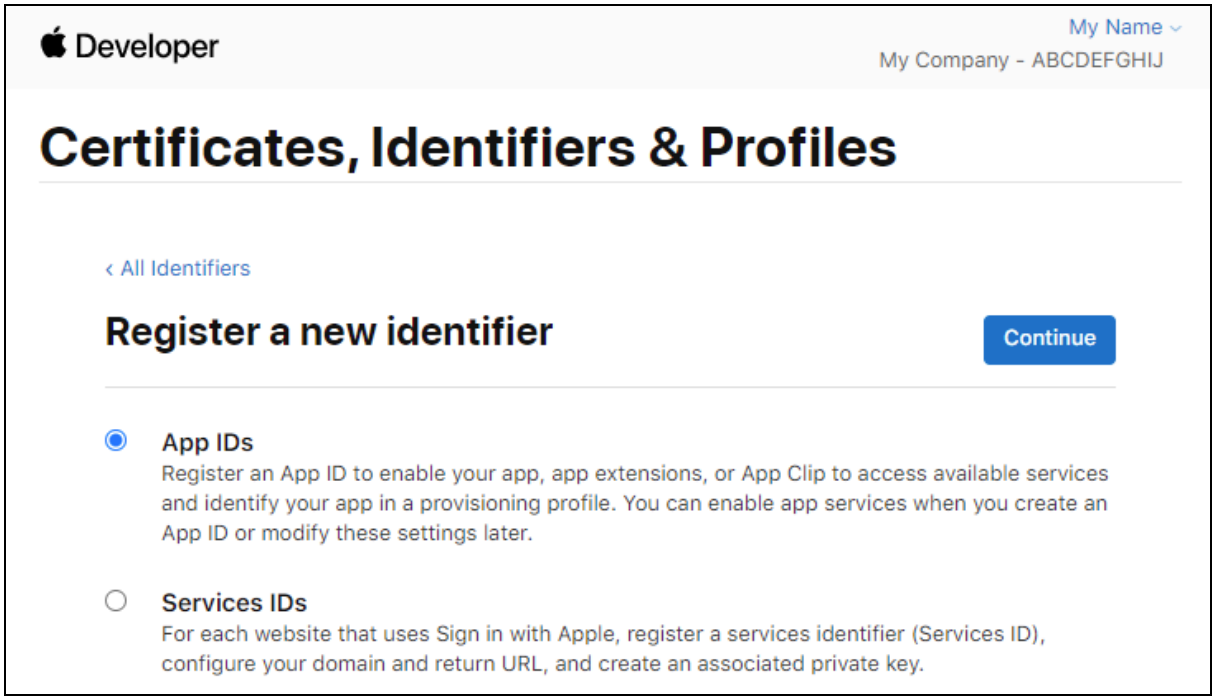


Appendix 2: Procedure for preparing the data for setting up "Sign in with Apple".

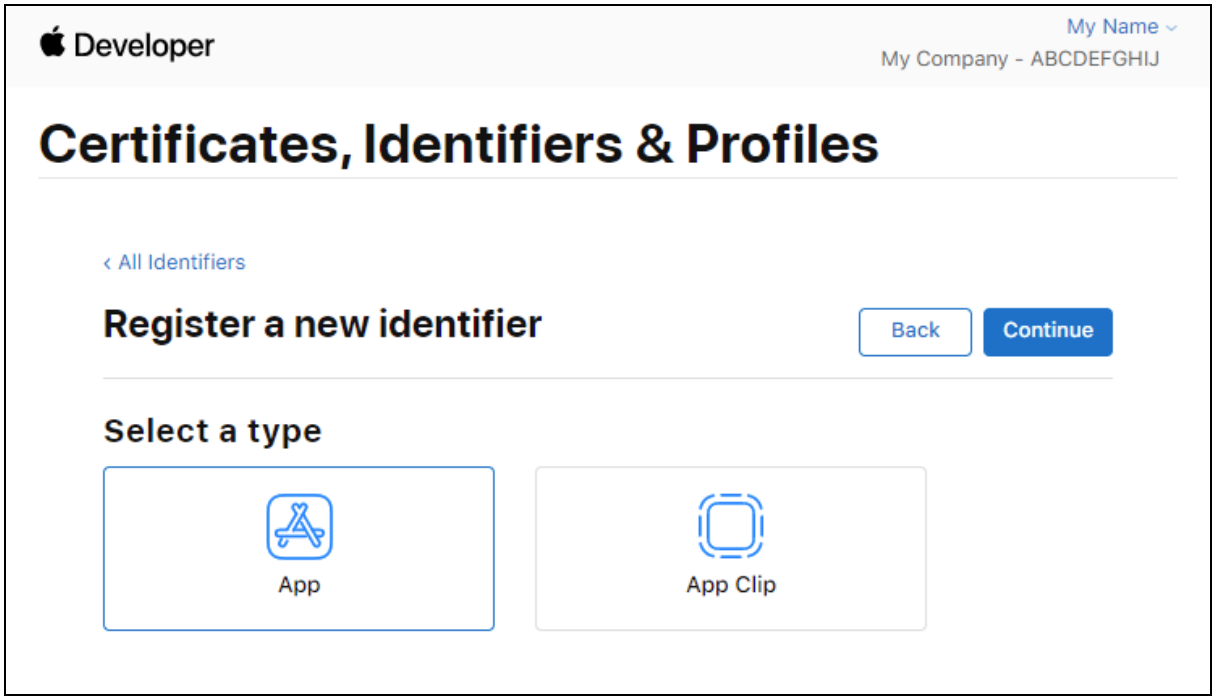
Login to https://developer.apple.com/account/resources/identifiers/list with your Apple Developer account.



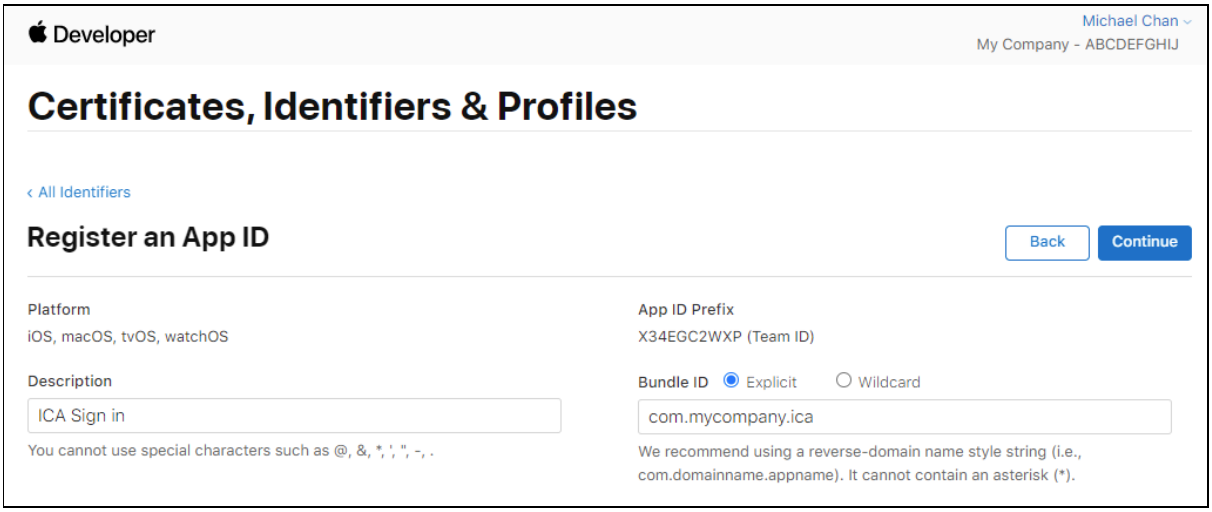
Press the "+" icon.



Select “App IDs”. Press Continue

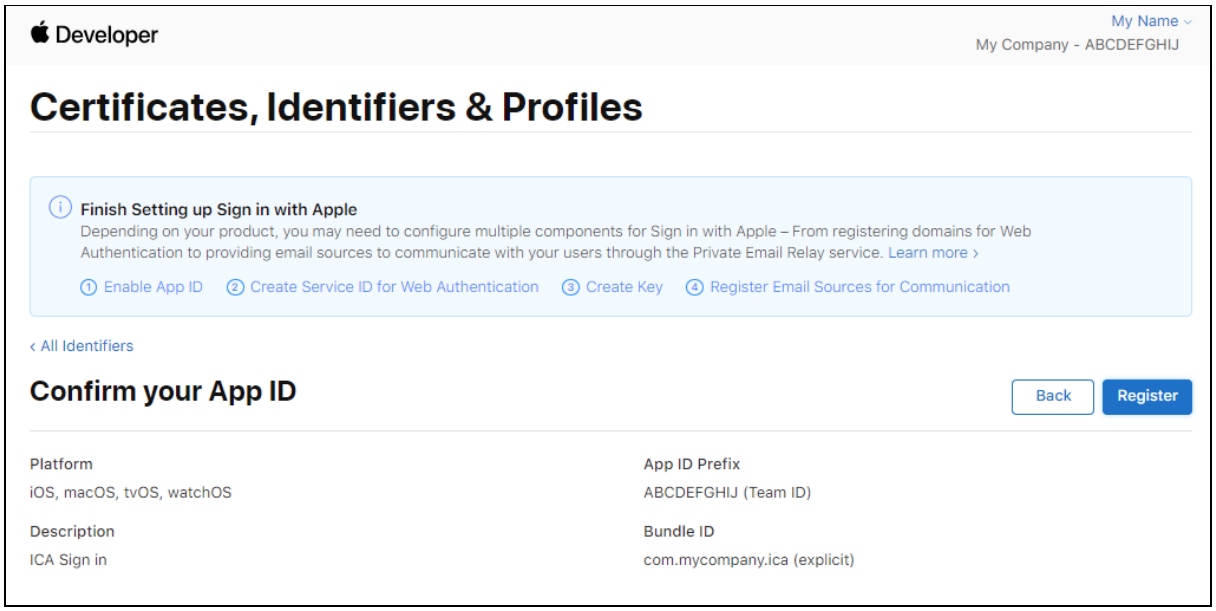


Select “App” and press Continue.

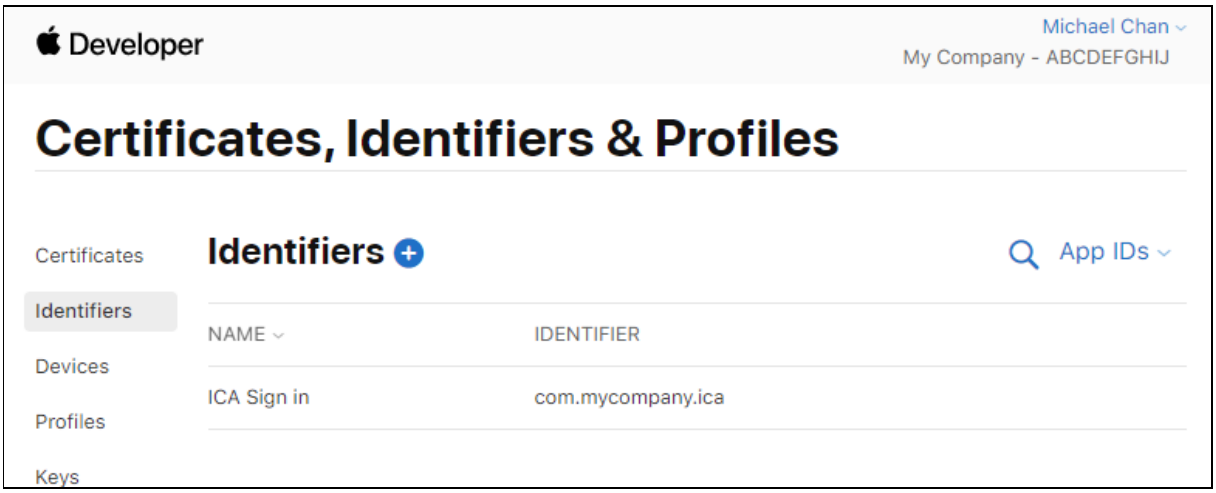


Enter “ICA Sign in” in the Description box. Choose “Explicit” and input a Bundle ID. Replace “com.mycompany.ica” with an identifier you decide.

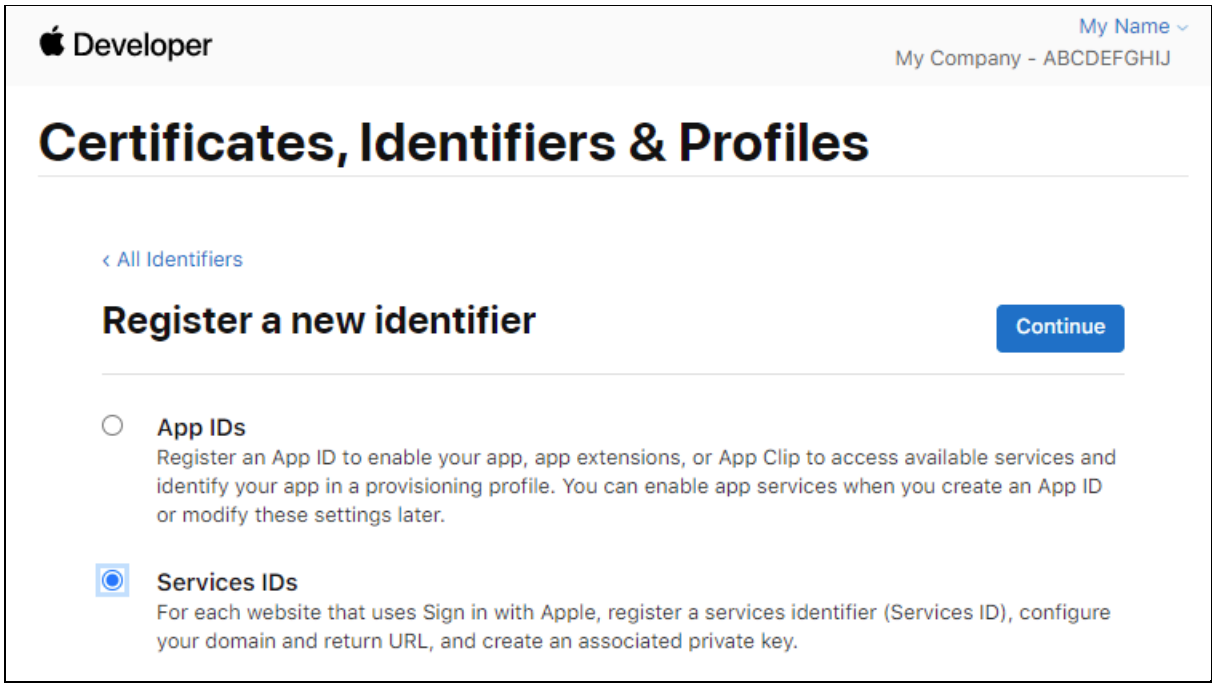
Scroll down and select “Sign in with Apple”. Press Continue



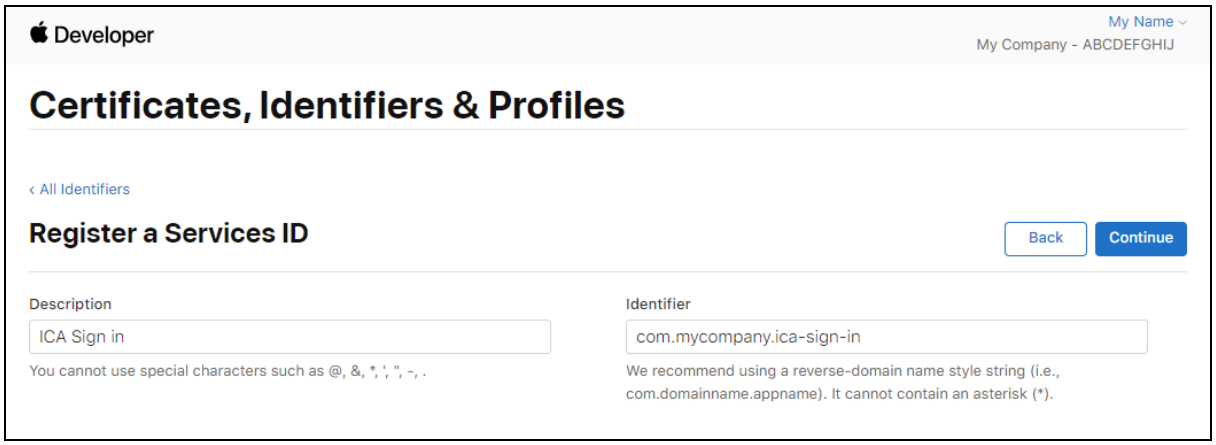
Press Register.



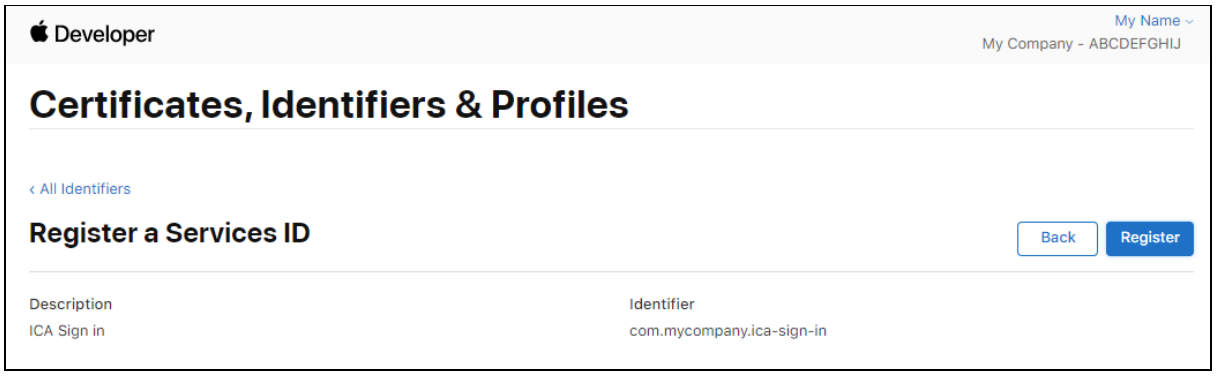
Press the “+” icon again.



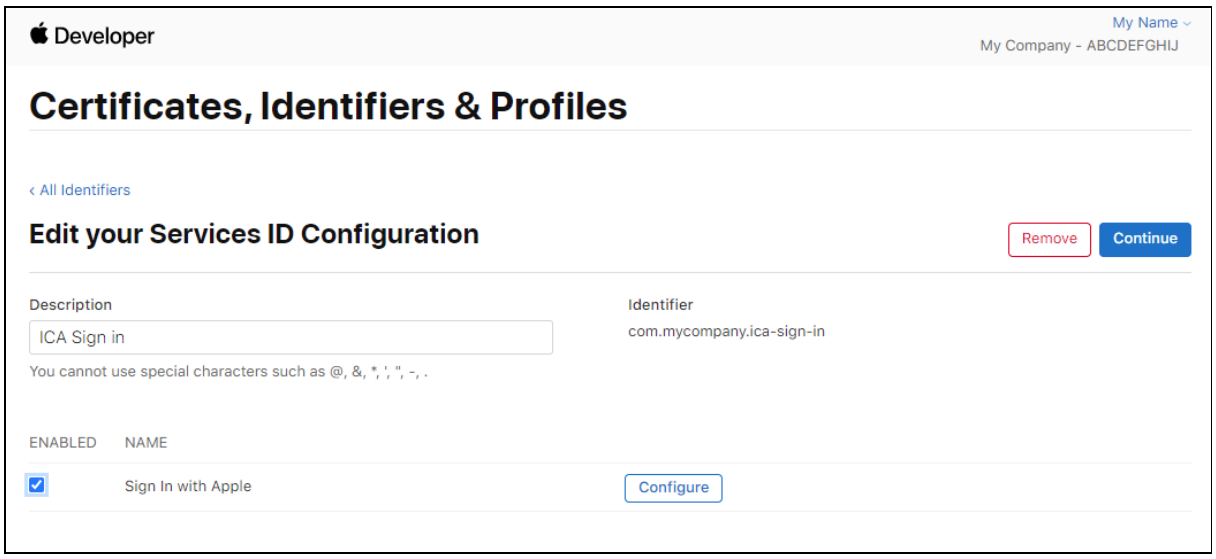
Select “Services IDs” and press Continue.



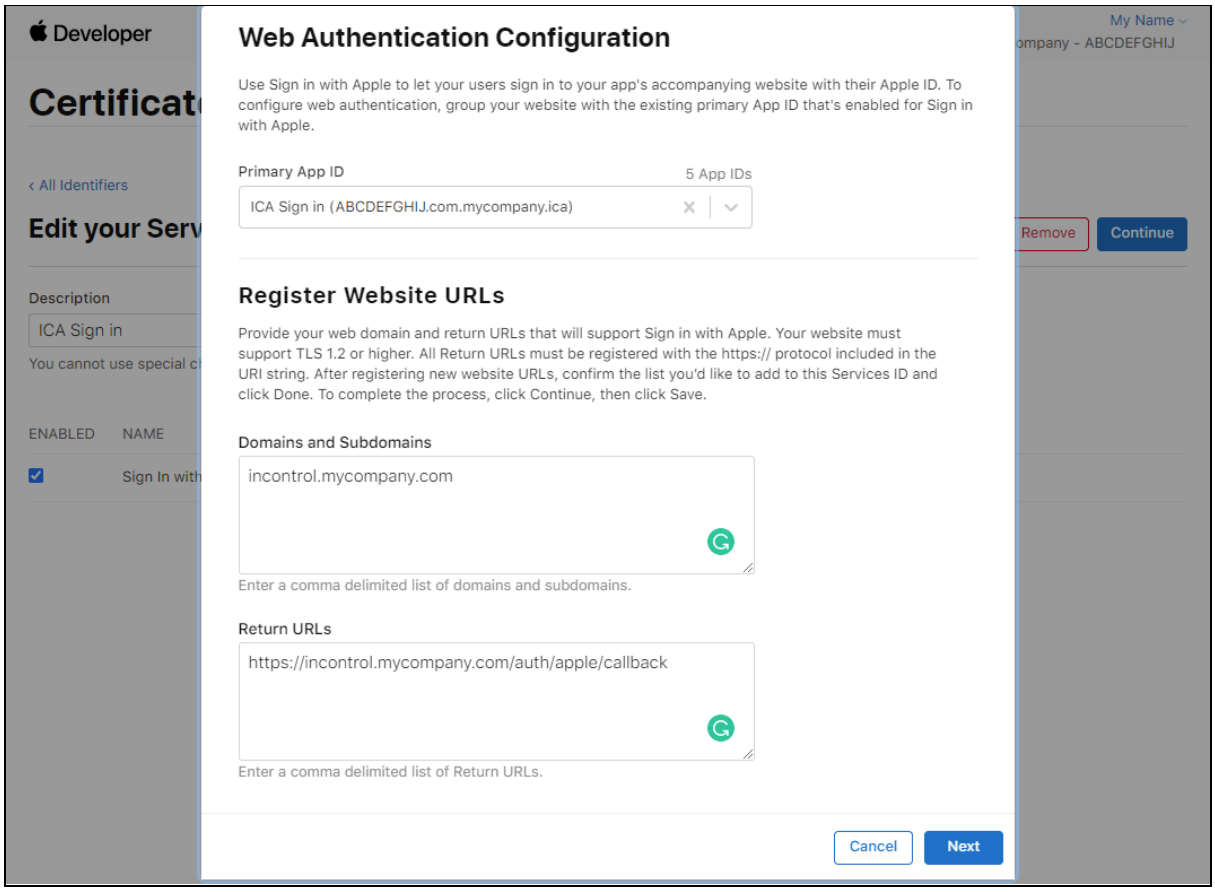
Replace “`com.mycompany.ica-sign-in`” with an identifier you decide. This is your “**Service ID**”. Record this down.



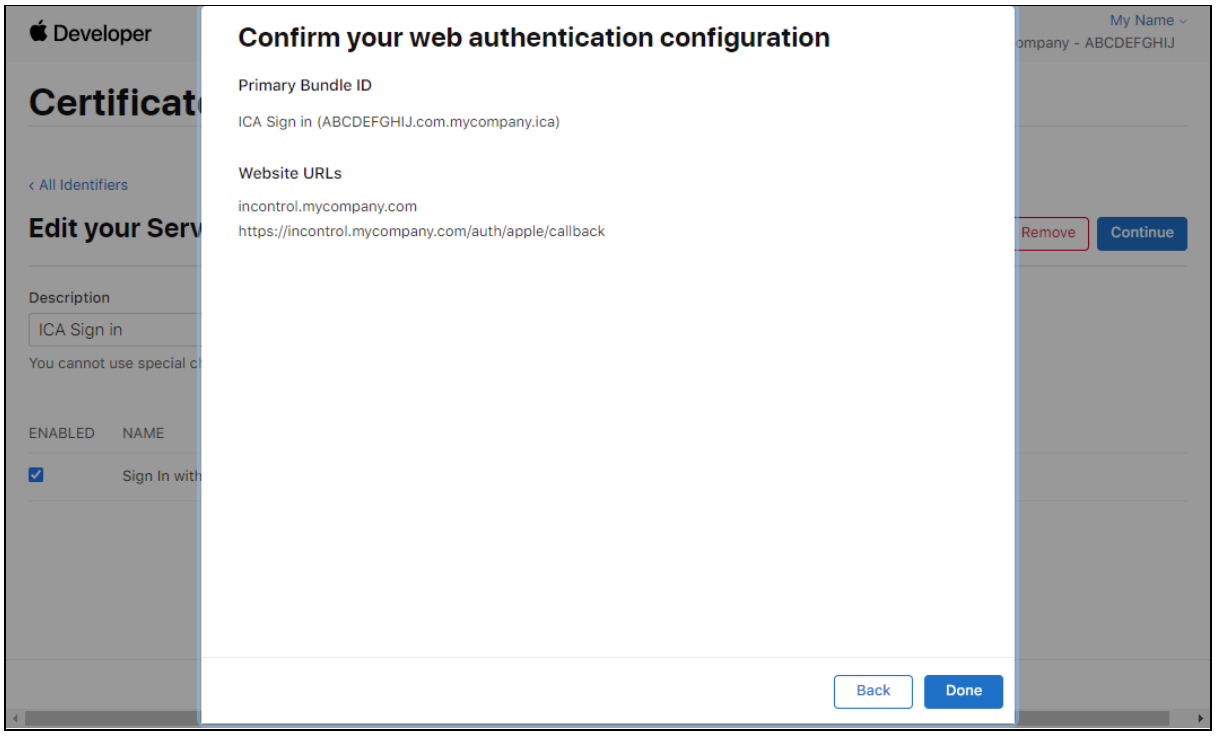
Press Register.



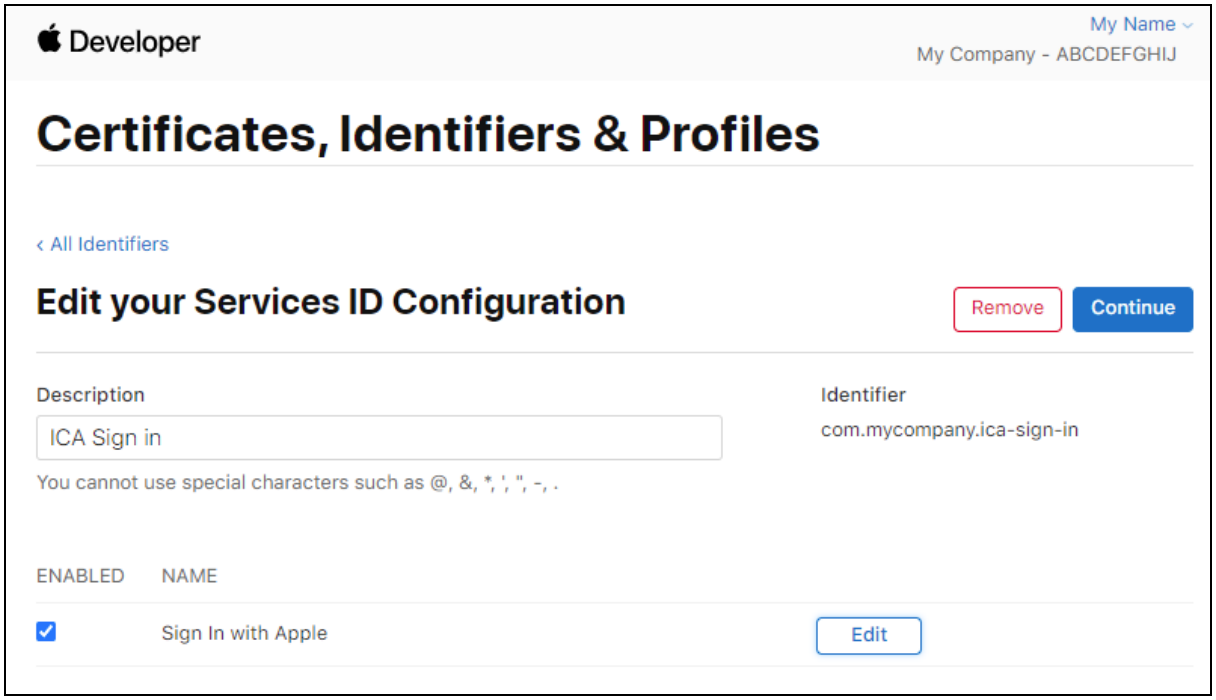
Press Configure.



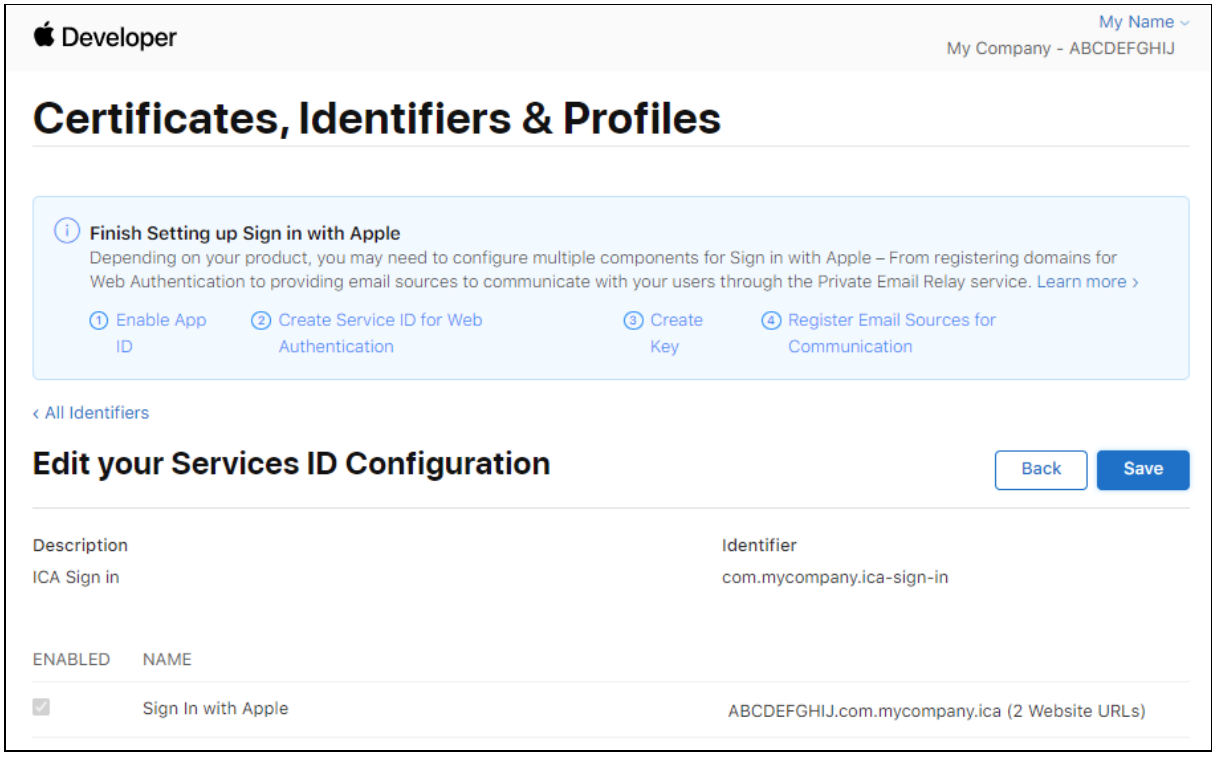
Replace "`incontrol.mycompany.com`" with your InControl's Server Name. The return URLs shall be "`https://{your_server_name}/auth/apple/callback`".



Press Done.

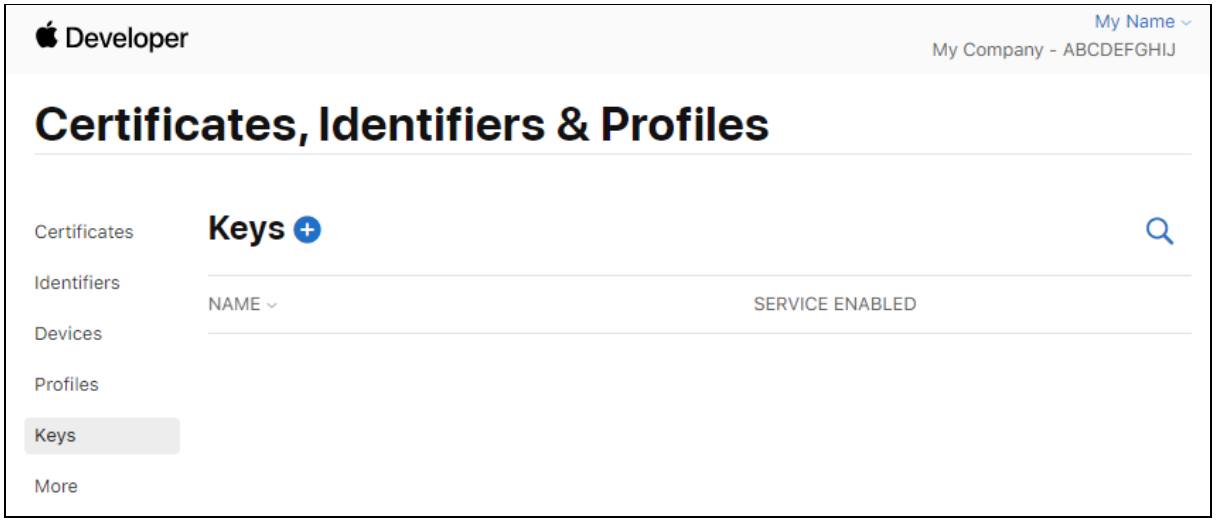


Press Continue.

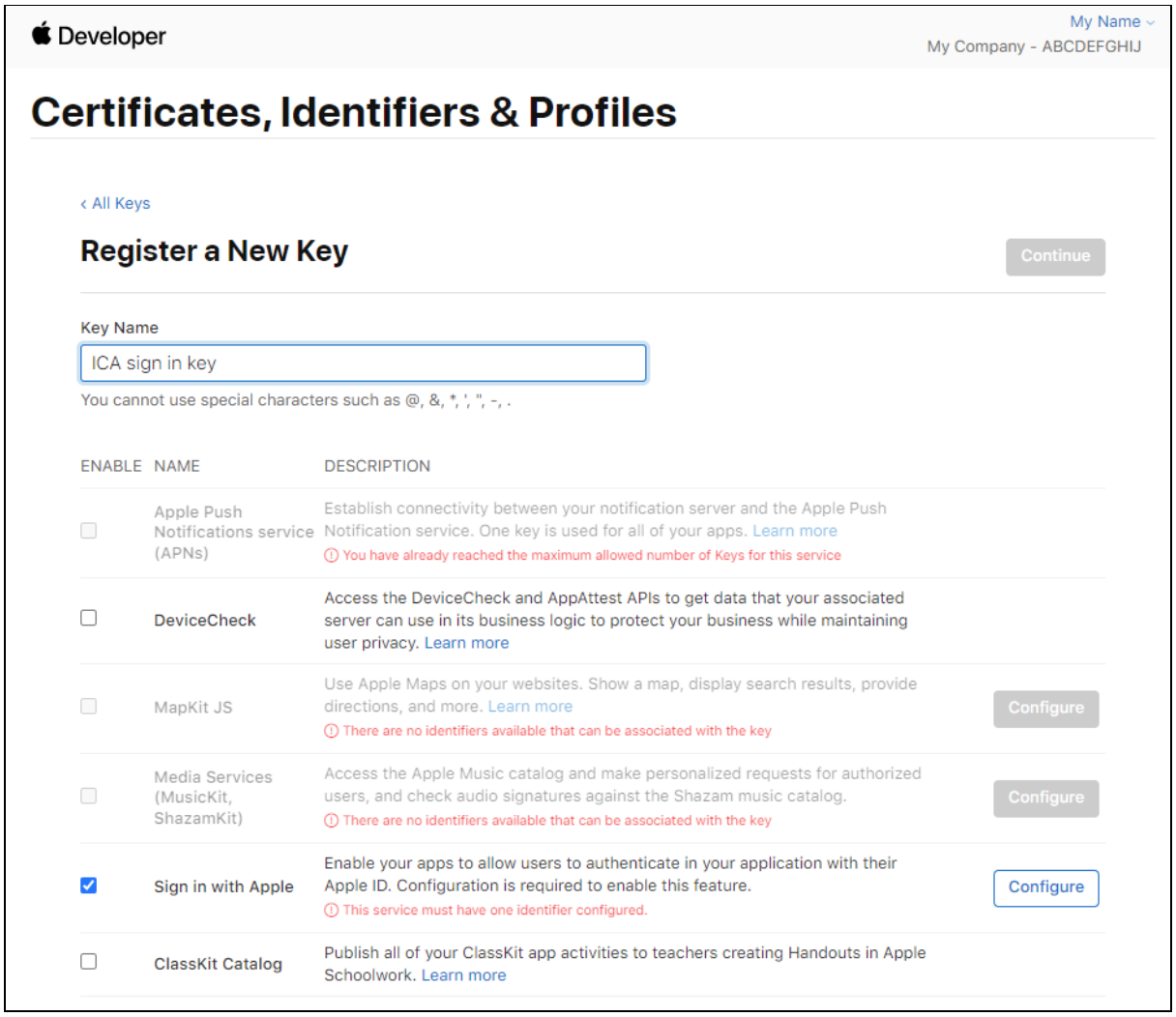


Press Save to save the Services ID.

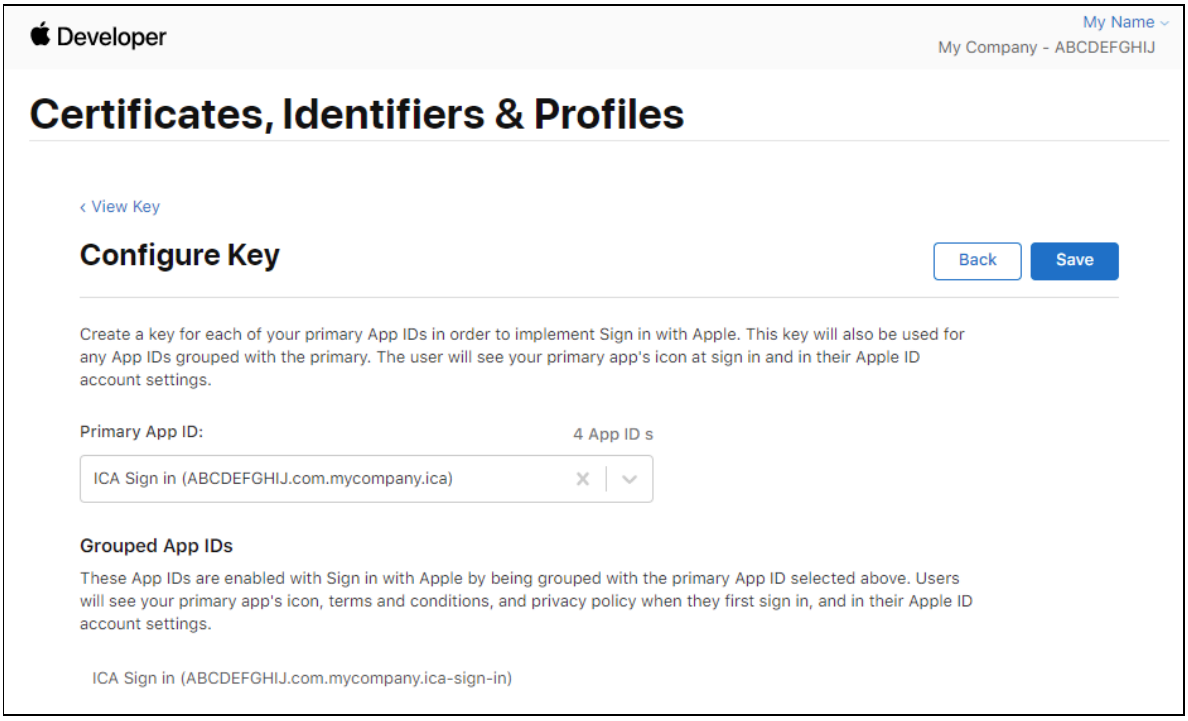
Then press the “Keys” item on the right navigation bar.



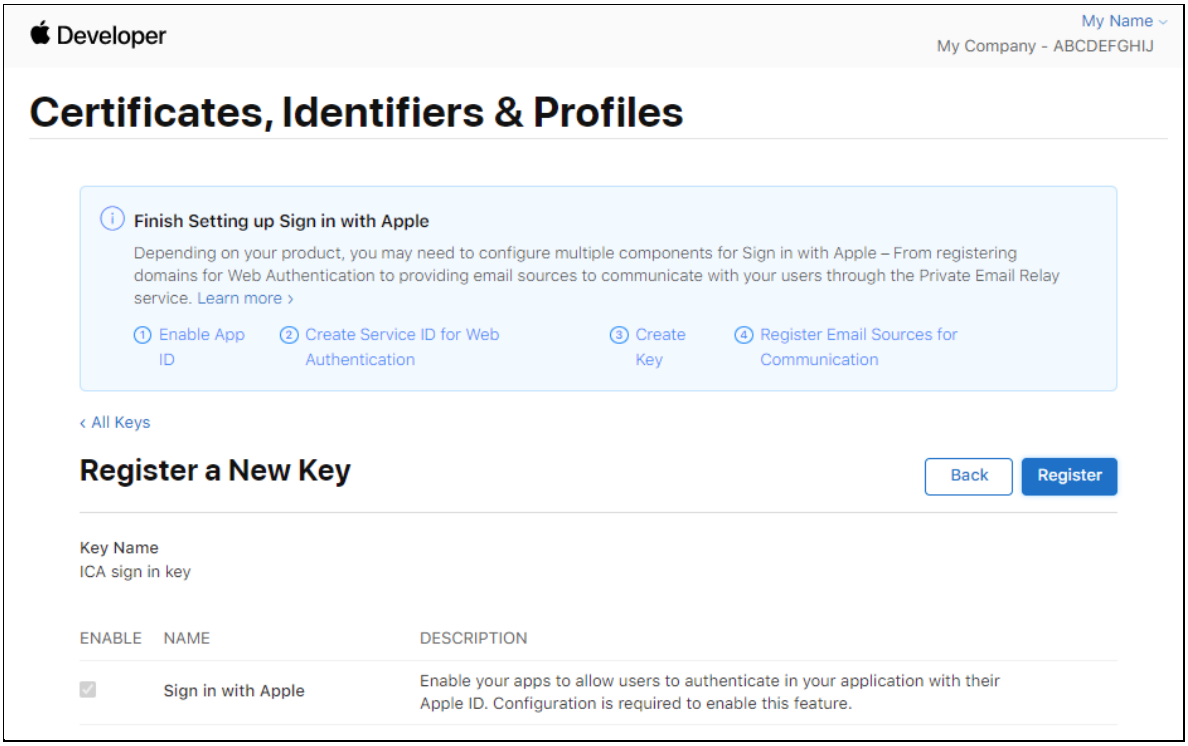
Press the “+” icon.



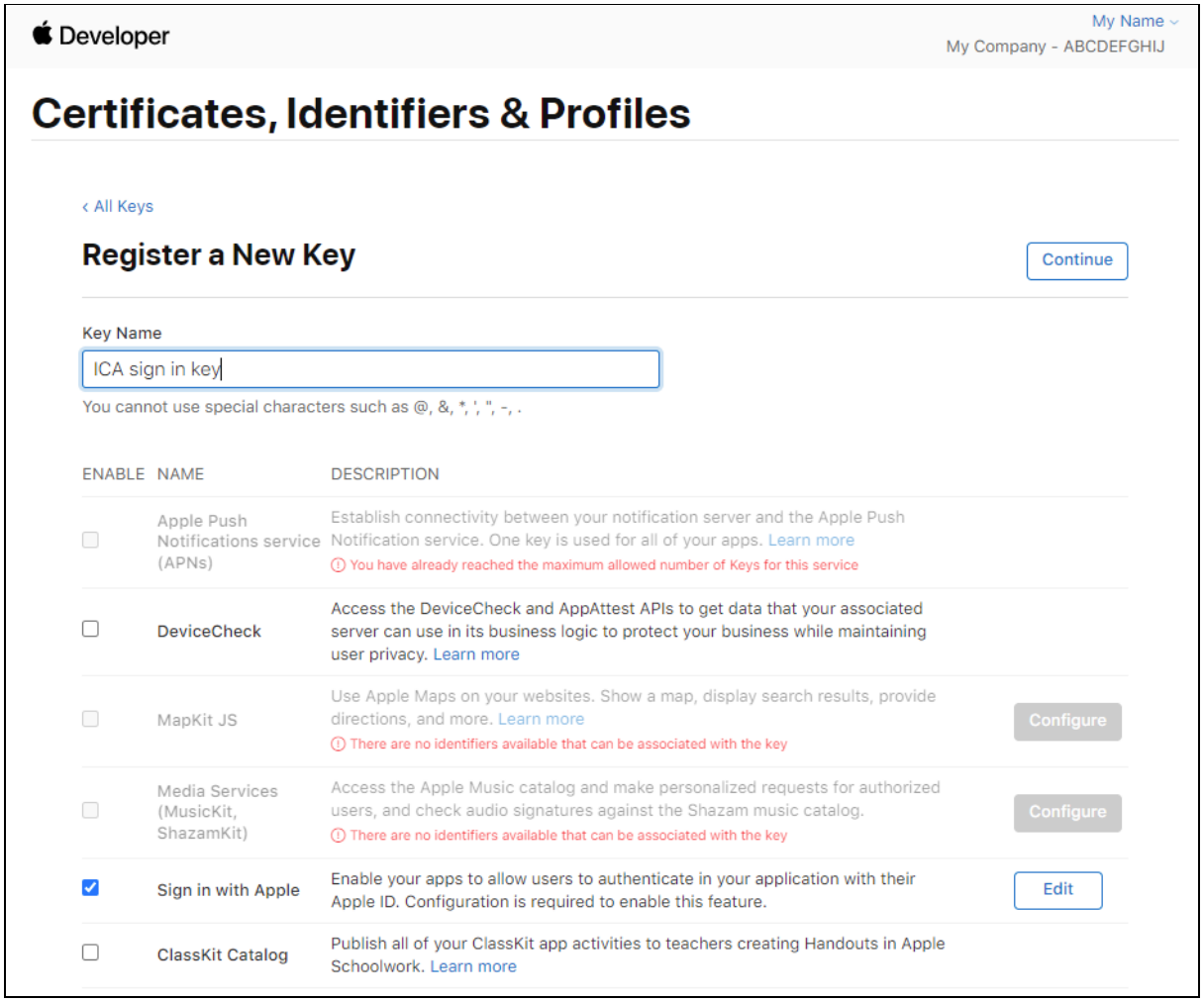
Input “ICA sign in key” in the Key Name field. Select “Sign in with Apple”. Press Configure.



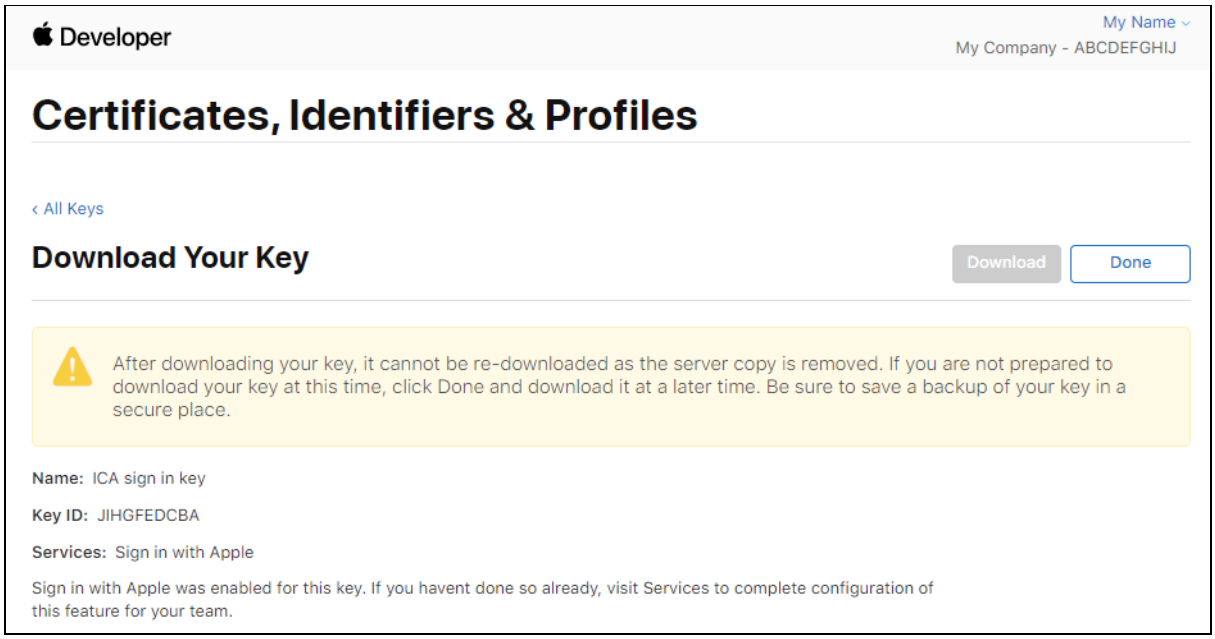
Select “ICA Sign in”. Press Save.



Press Register.



Press Continue.



Download the **key file** (IMPORTANT). Record the **Key ID**.

Press Done only after you have downloaded the key.

Record the **Team ID** showing on the upper-right corner (i.e. "*ABCDEFGHIJ*" in the above screen.)

Now you can fill in the **Services ID**, **Team ID**, and **Key ID**, and upload the **key file** to the control panel to finish the Sign-in with Apple setup.

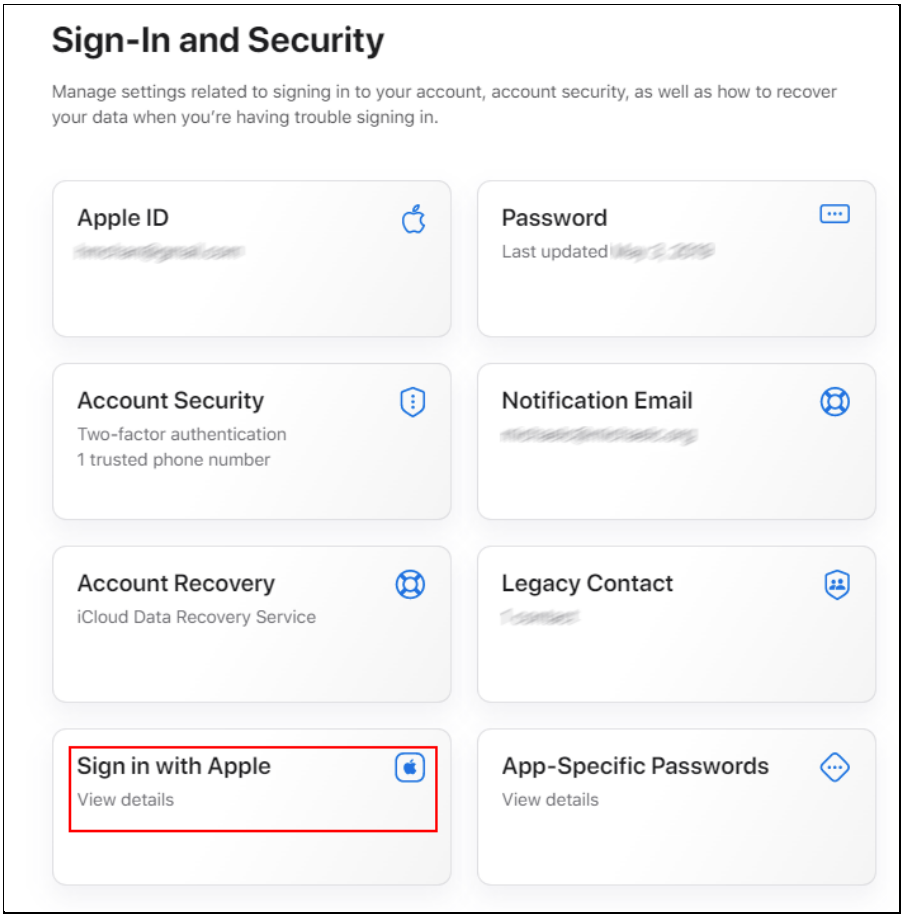
Note: when your users sign in to your InControl with Apple for the first time, they will be asked to choose whether to hide their email address from your InControl on Apple's website. It is a privacy feature of the Apple sign-in.

If they are self-signing up for an InControl account (like how Peplink InControl does), it will be up to them to choose to hide their email address or not.

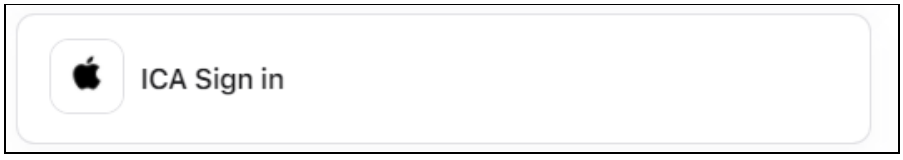
But if you are inviting them to sign in to an organization/group with their email address, then they must choose "Show My Email". Otherwise, InControl will only see them log in as an Apple-generated email address. It will not be their original email address that you have invited. So they will not be able to access the organization/group.

In case they have mistakenly chosen “Hide My Email”, you may either add their Apple-generated email address to the organization/group or advise them to follow the following procedure to change their preference:

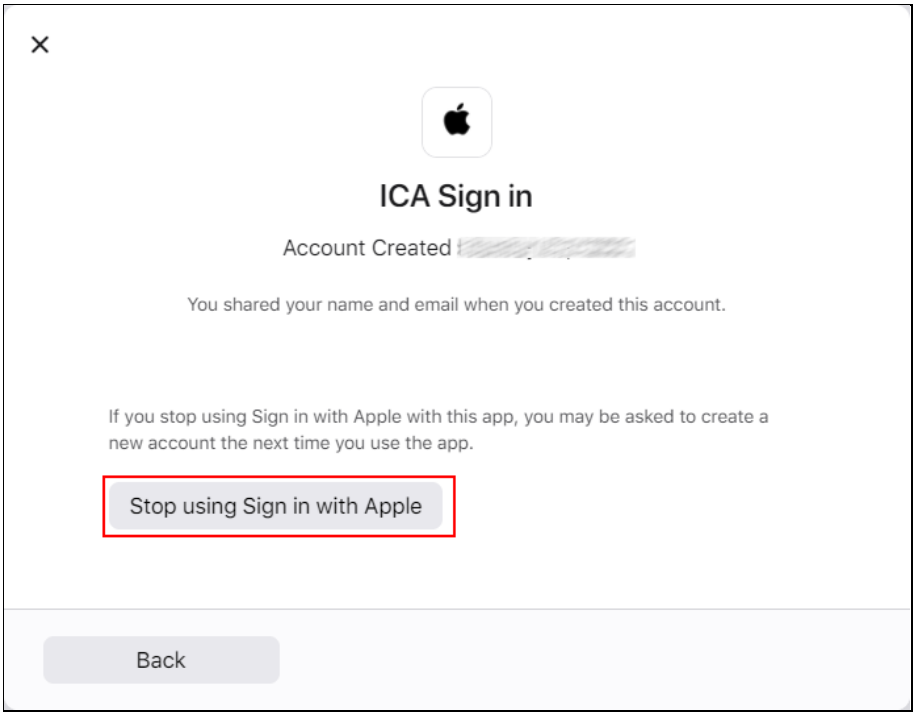
1. Login to https://appleid.apple.com
2. Choose "Sign in with Apple"



3. Select "ICA Sign in"



4. Click "Stop using Sign in with Apple" and then click "Stop using".



5. Sign out from your InControl. Sign in your InControl with Apple again. Choose "Share My Email" while logging in.

   Now their account is well set.