InControl 2 Appliance Setup Guide

for Appliance Software 2.14.2.7

(Last updated: 2026-05-14)

Contents

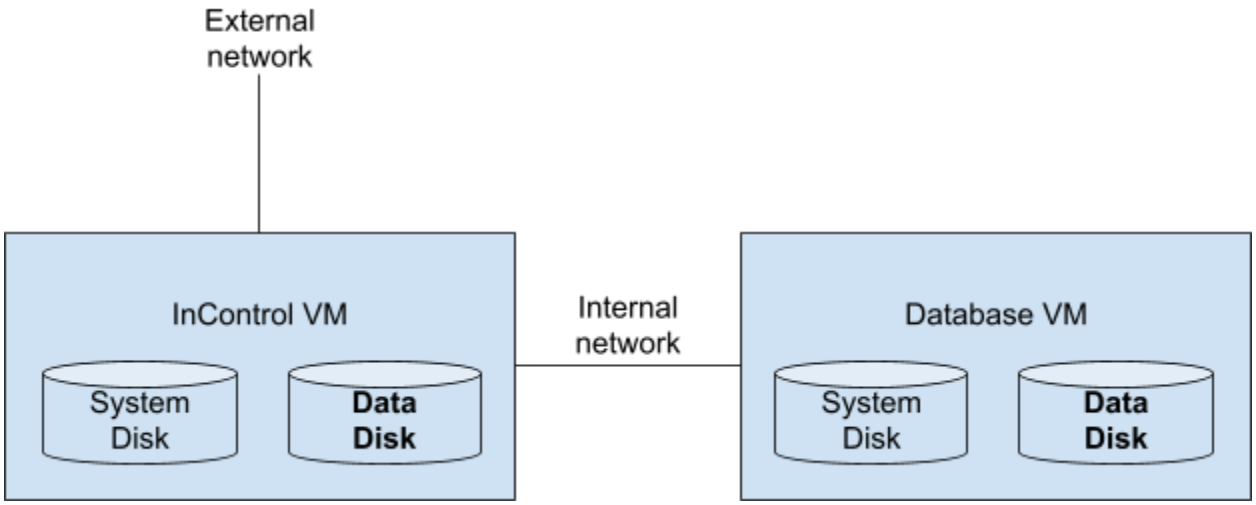
1. Virtual Appliance

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	12 GB	8 GB
AWS EC2 Instance Type	r6i.large	r6i.large
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	24 GB	12 GB
AWS EC2 Instance Type	r6i.xlarge	r6i.xlarge
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	96 GB	32 GB
AWS EC2 Instance Type	r6i.4xlarge	c6i.4xlarge
System Disk Size	24 GB	24 GB
Data Disk Size	40 GB	5 TB

The minimum memory requirement is 12 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 4. Input FTP/SFTP Archive Server Settings for details.

1.3 Installation on VMware ESXi

Compatibility

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”.

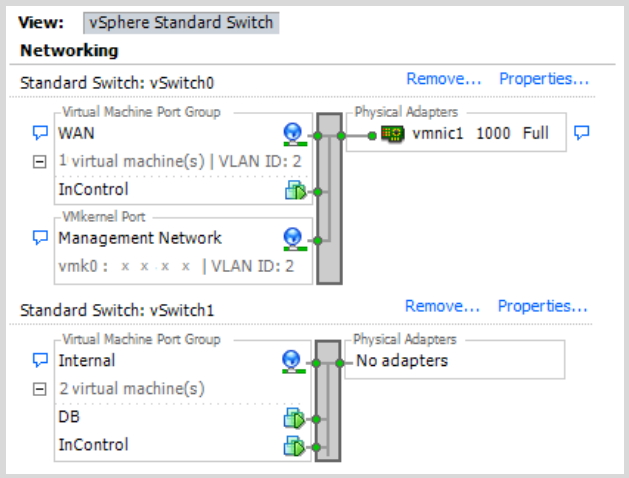
The "`WAN`" is for connecting to the outside world and will need a physical network adapter attached. The first network adapter of the InControl VM shall be assigned to this network.

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 1.9) 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:

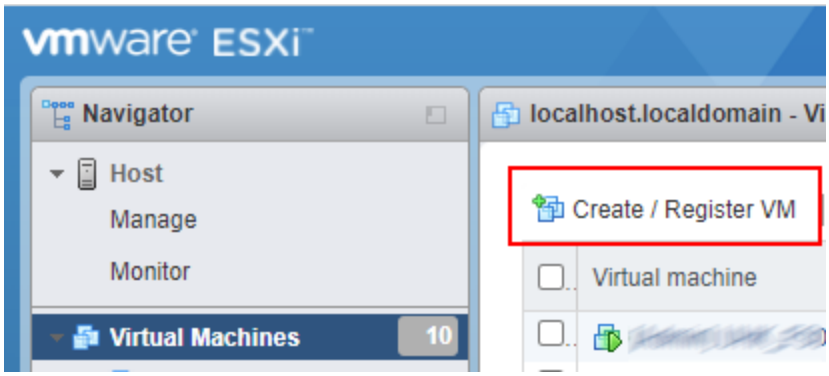
InControl-System-2.9.4.1-vmware.zip:

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

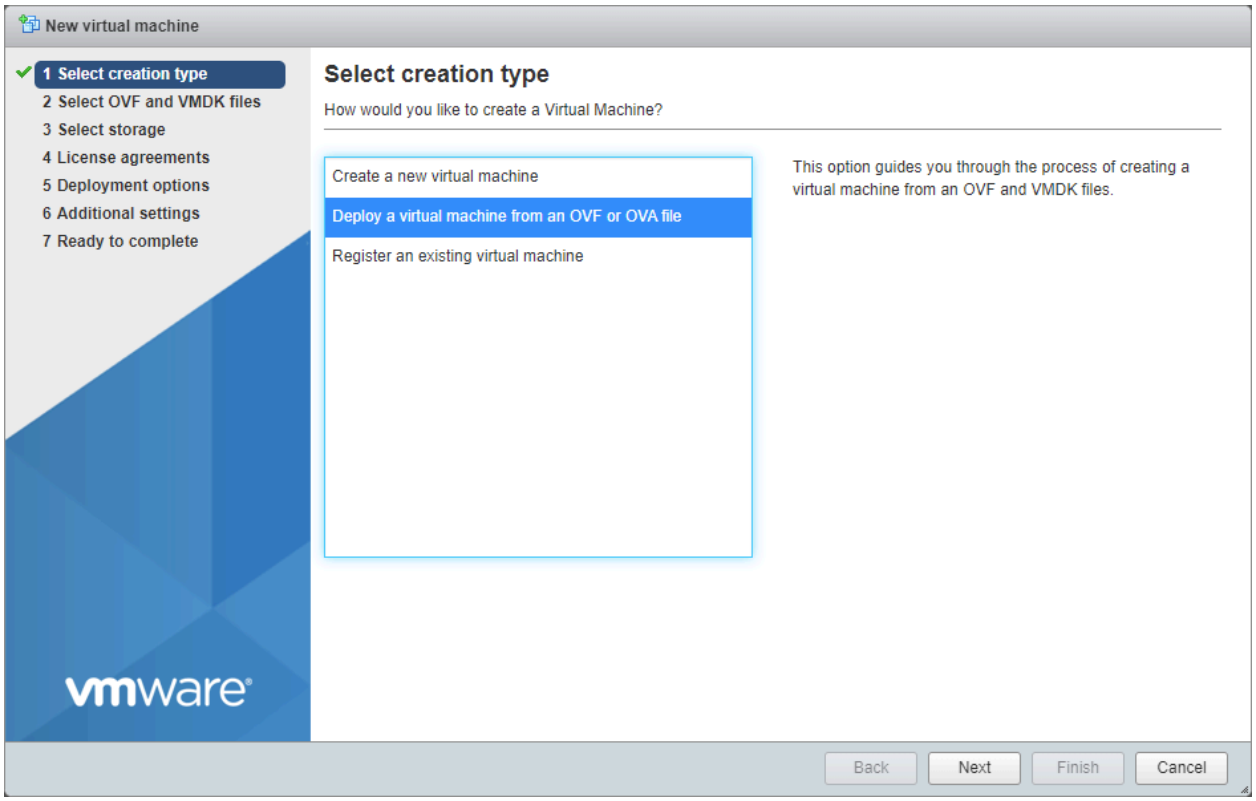
DB-System-20211215-vmware.zip:

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

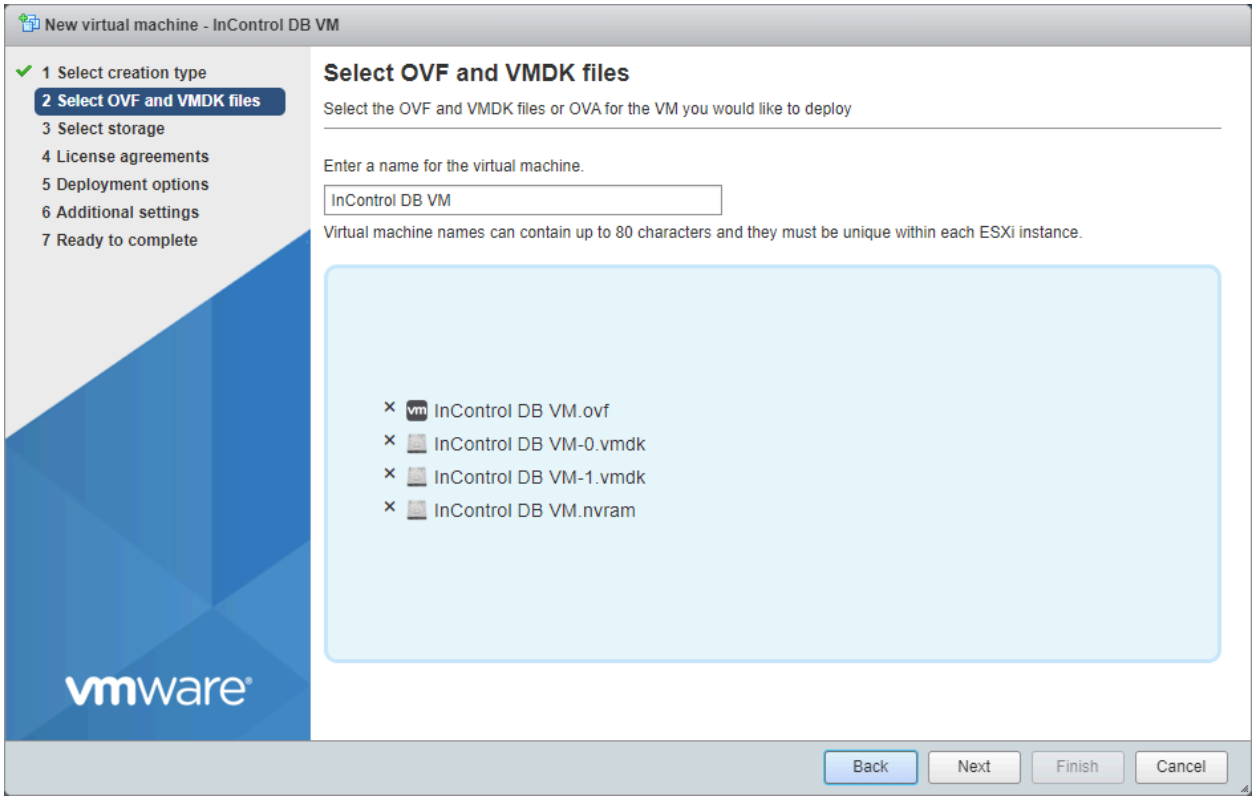
Step 3. On the ESXi web console, navigate to "Virtual Machines". Click the "Create / Register VM" button.



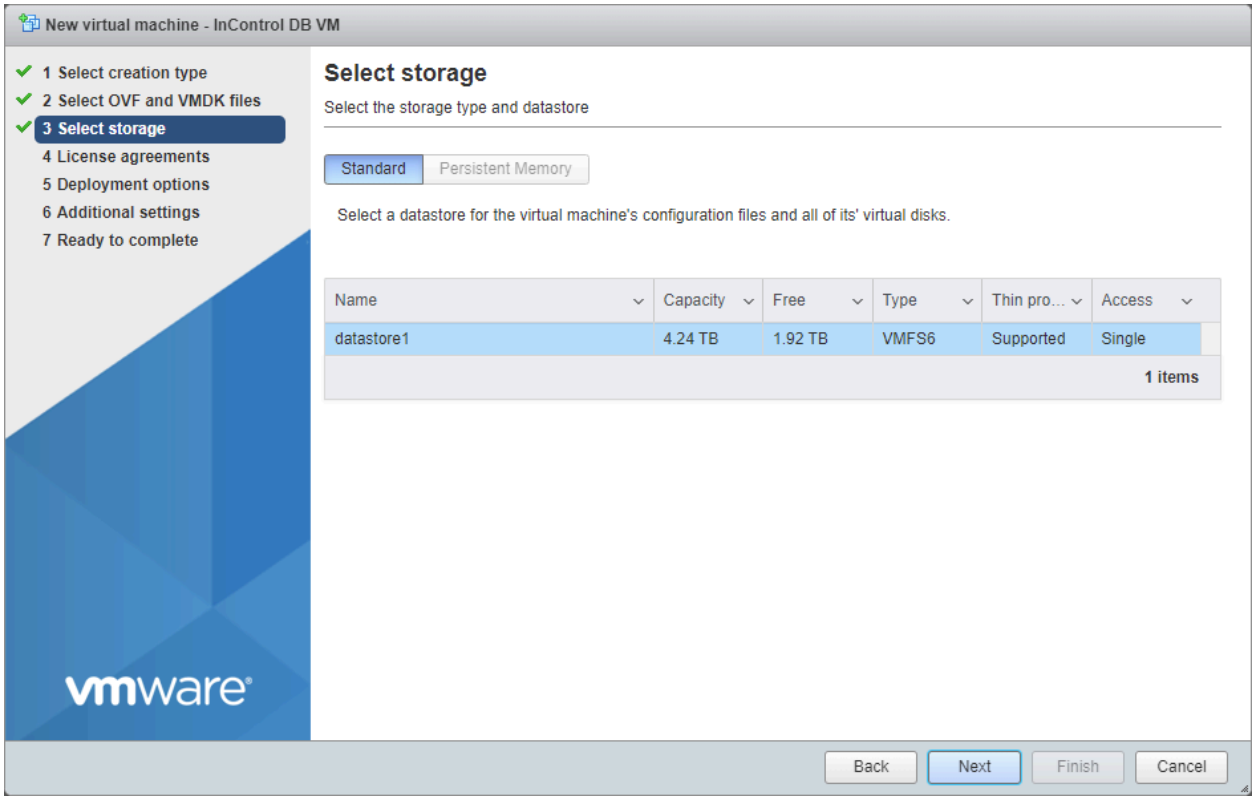
Step 4. Select the creation type "Deploy a virtual machine from an OVF or OVA file". Click "Next".



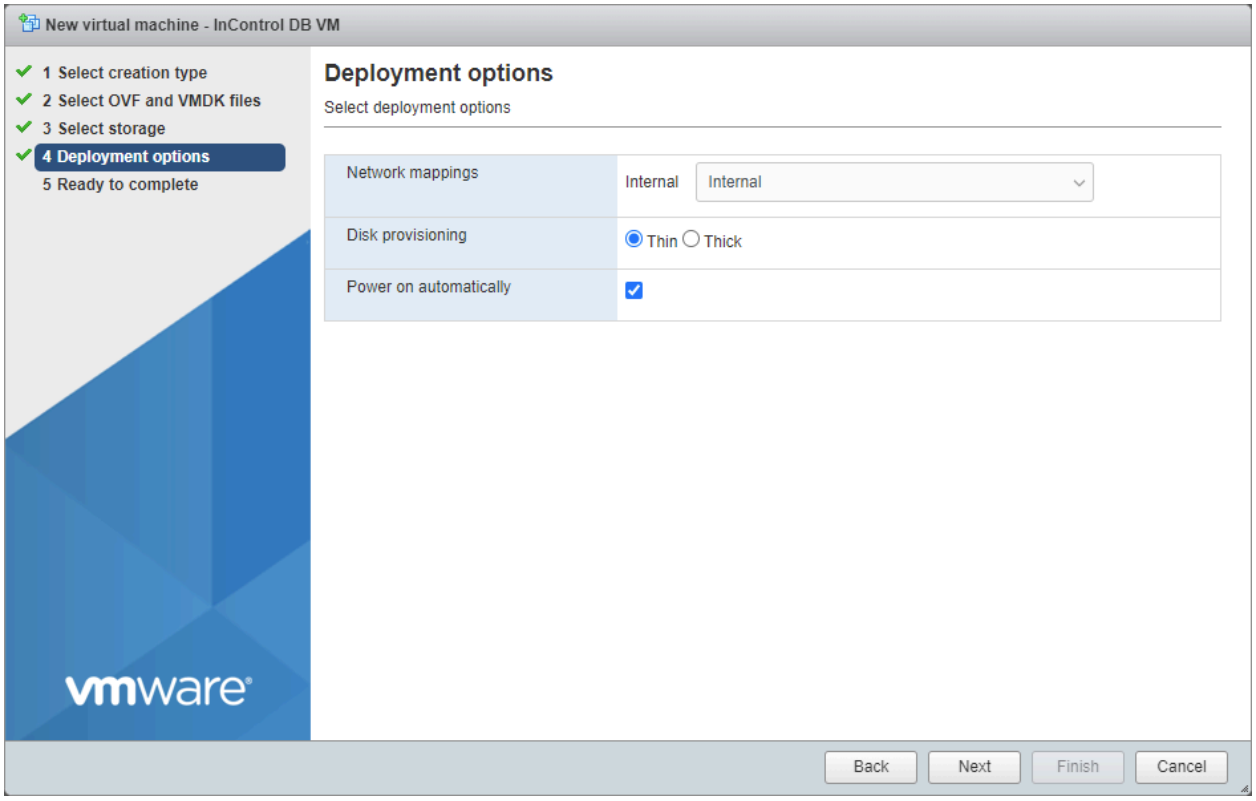
Step 5. Input a name for the virtual machine. E.g. "InControl DB VM". Drag and drop **all four files** into the drop zone. Click "Next".



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

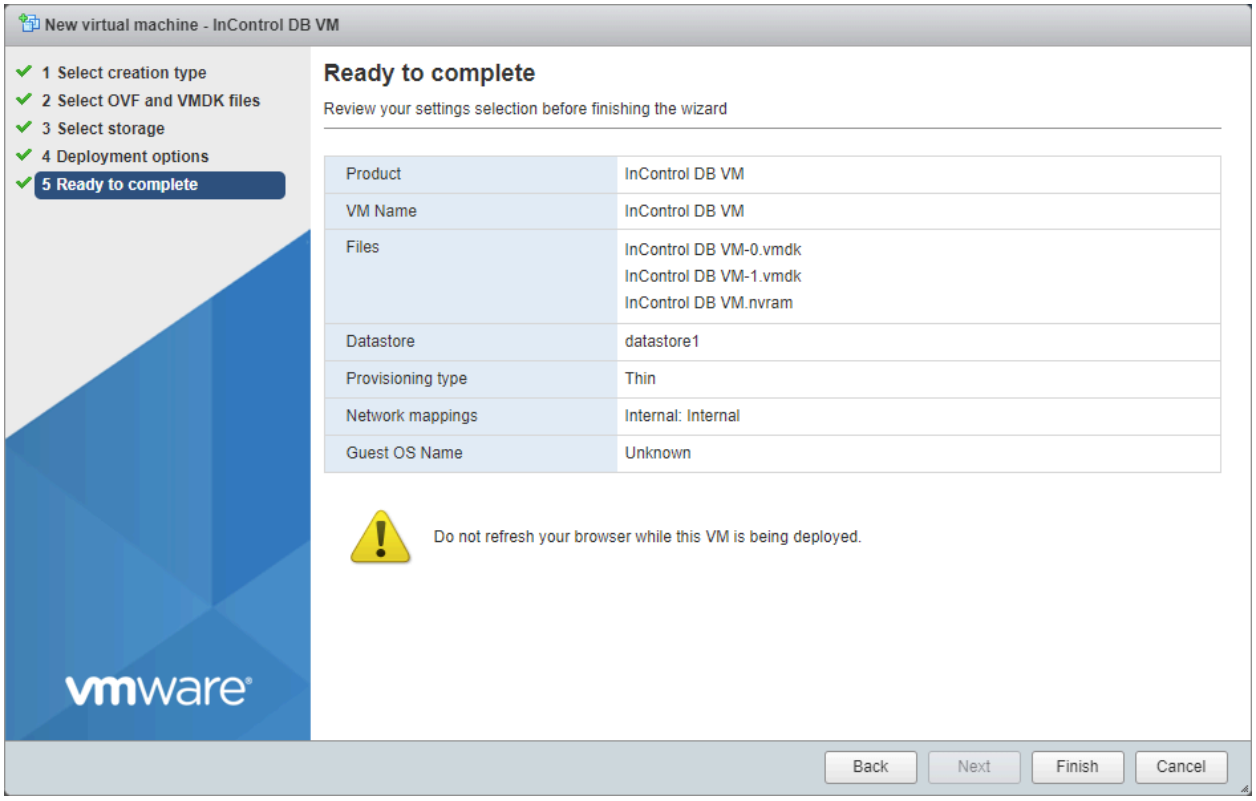


Step 7. In the Network mappings field, choose the network "`Internal`" that you created earlier. Leave the rest settings intact. Click "Next".



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

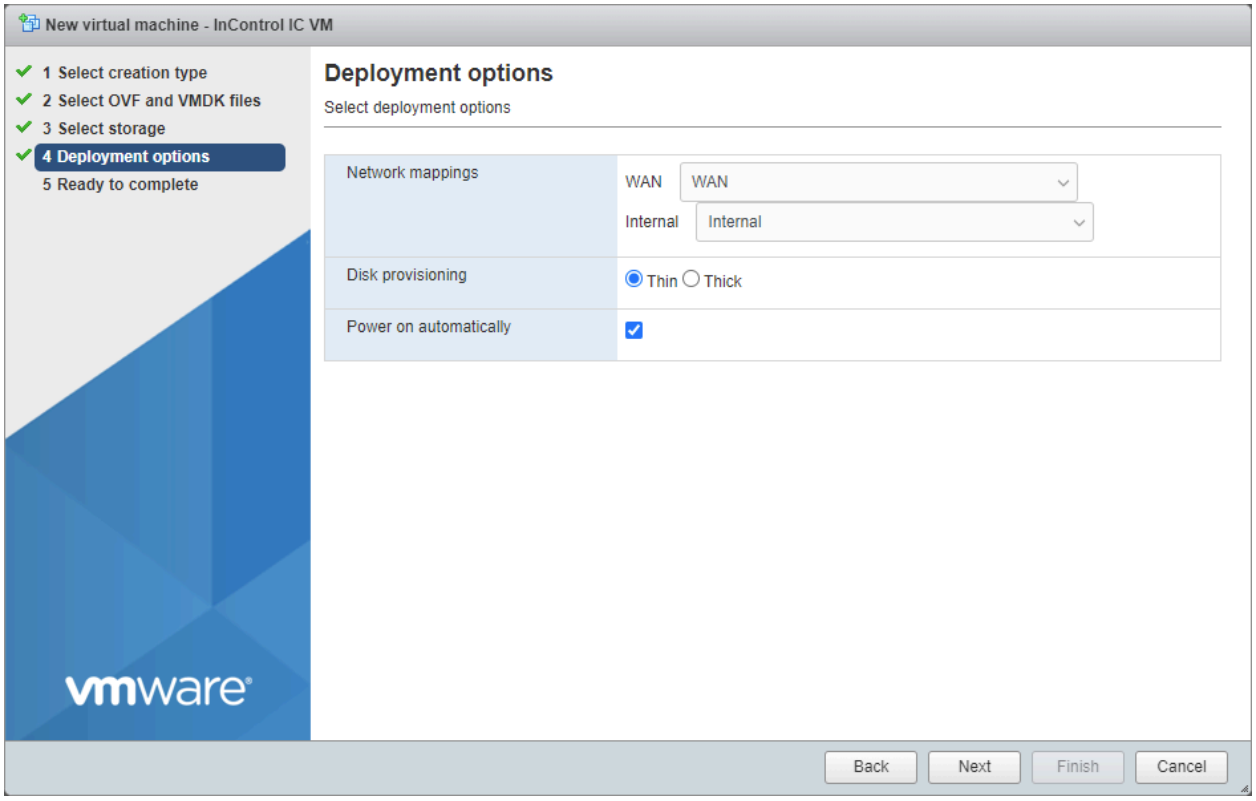
Note: You can safely ignore the error message “A required disk image was missing”. The disk will be created automatically when the VM is started.



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

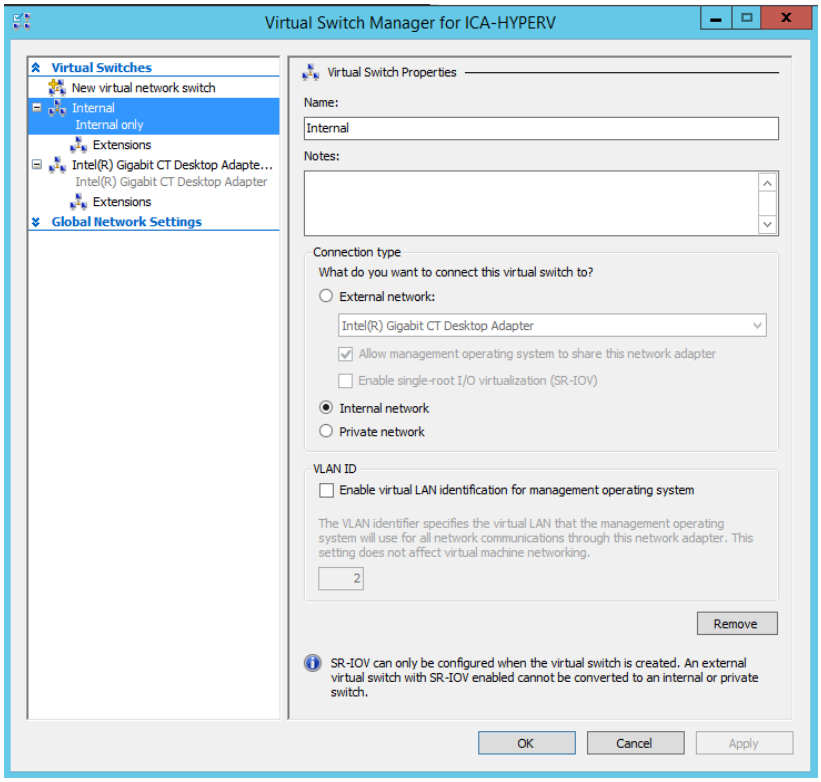
First of all, please create two networks on the Hyper-V host.

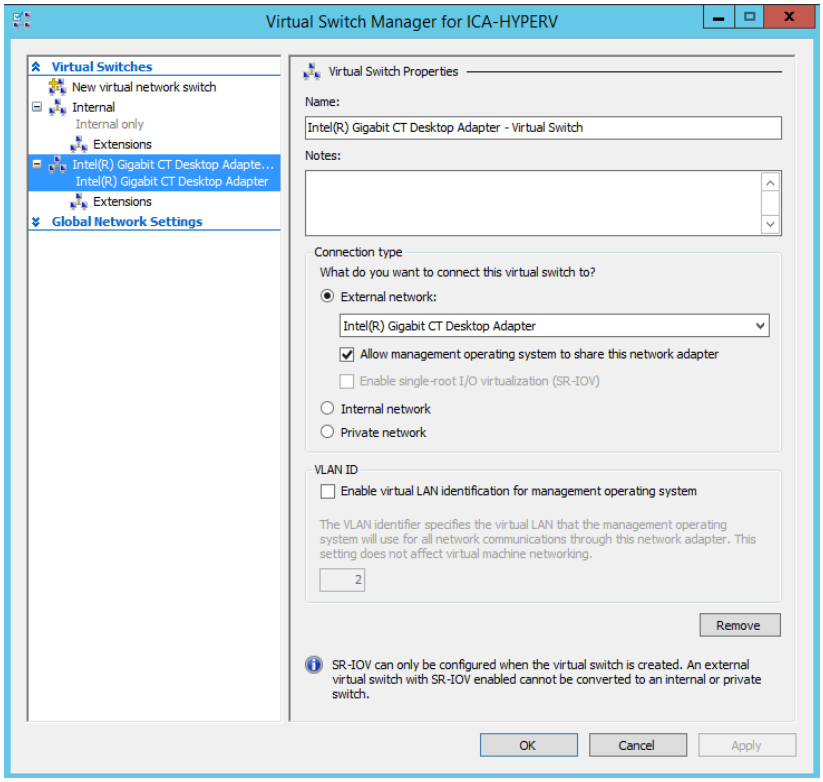
The first one is called "`WAN`" which is for connecting to the outside world and will need a physical network adapter attached. The first network adapter of the InControl VM shall be assigned to this network.

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 1.9) 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

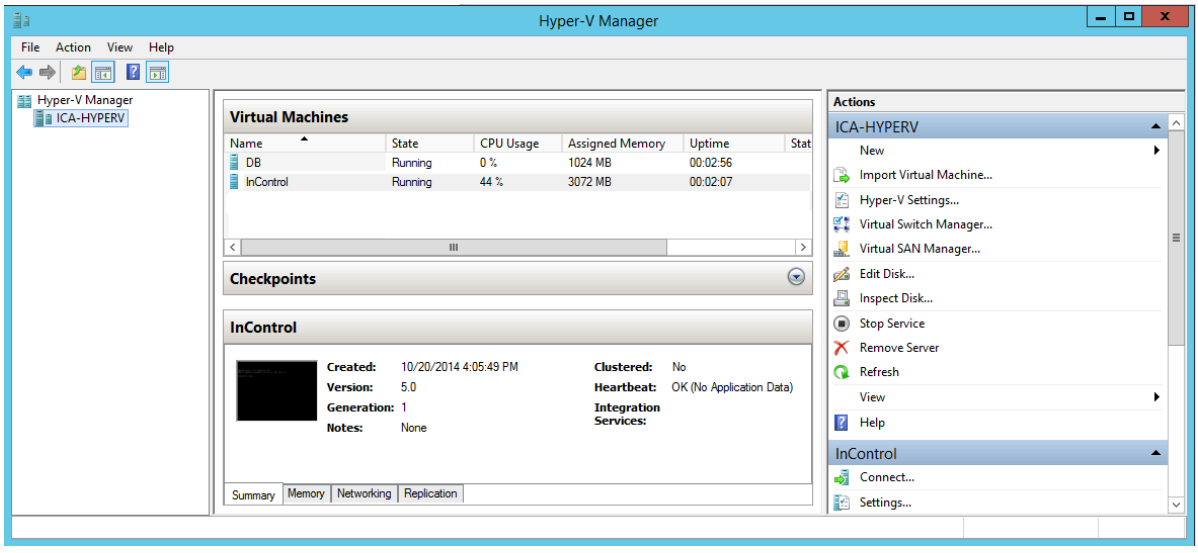
Peplink publishes two VHDX files: `InControl-System-2.9.0.2.vhdx` and `DB-System-20210323.vhdx`. They are bootable systems of the InControl and database services respectively. You will use them to start one InControl and one Database VM.

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

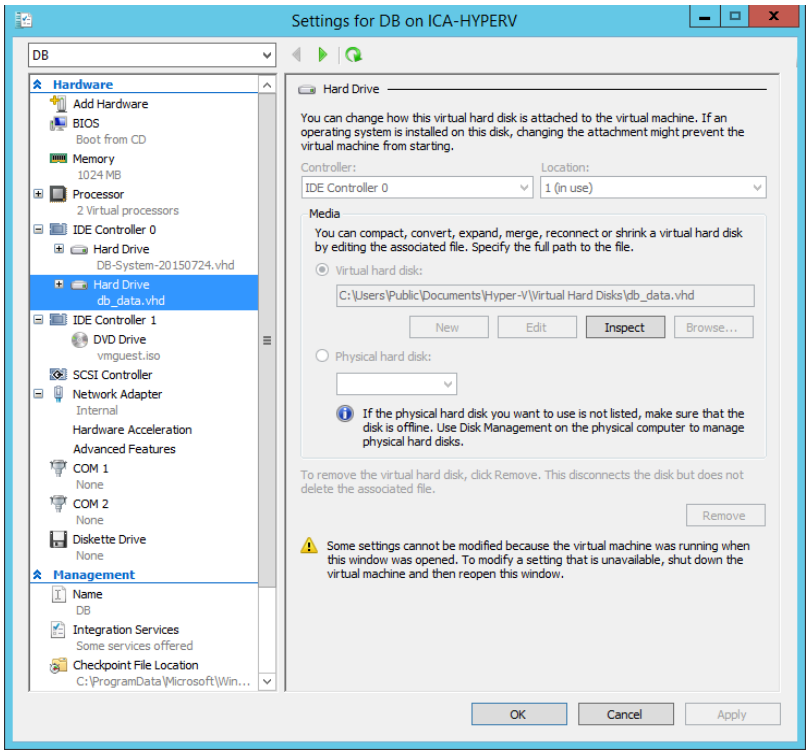
The .vhdx file names and sizes are as follow:

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

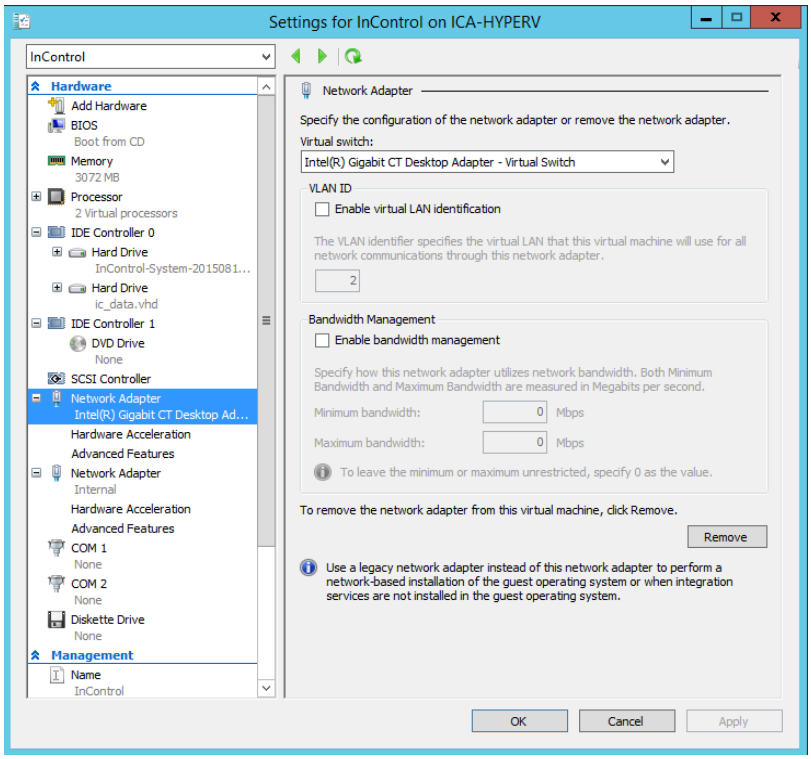
In the Hyper-V Manager, create two new Virtual Machines called `DB` and `InControl` for Ubuntu Linux (64 bit) guest operating systems. Our test was on first-generation VMs. For the DB VM, you need only one network connection on the Internal network. For the InControl VM, you'll need the WAN network and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



DB VM:



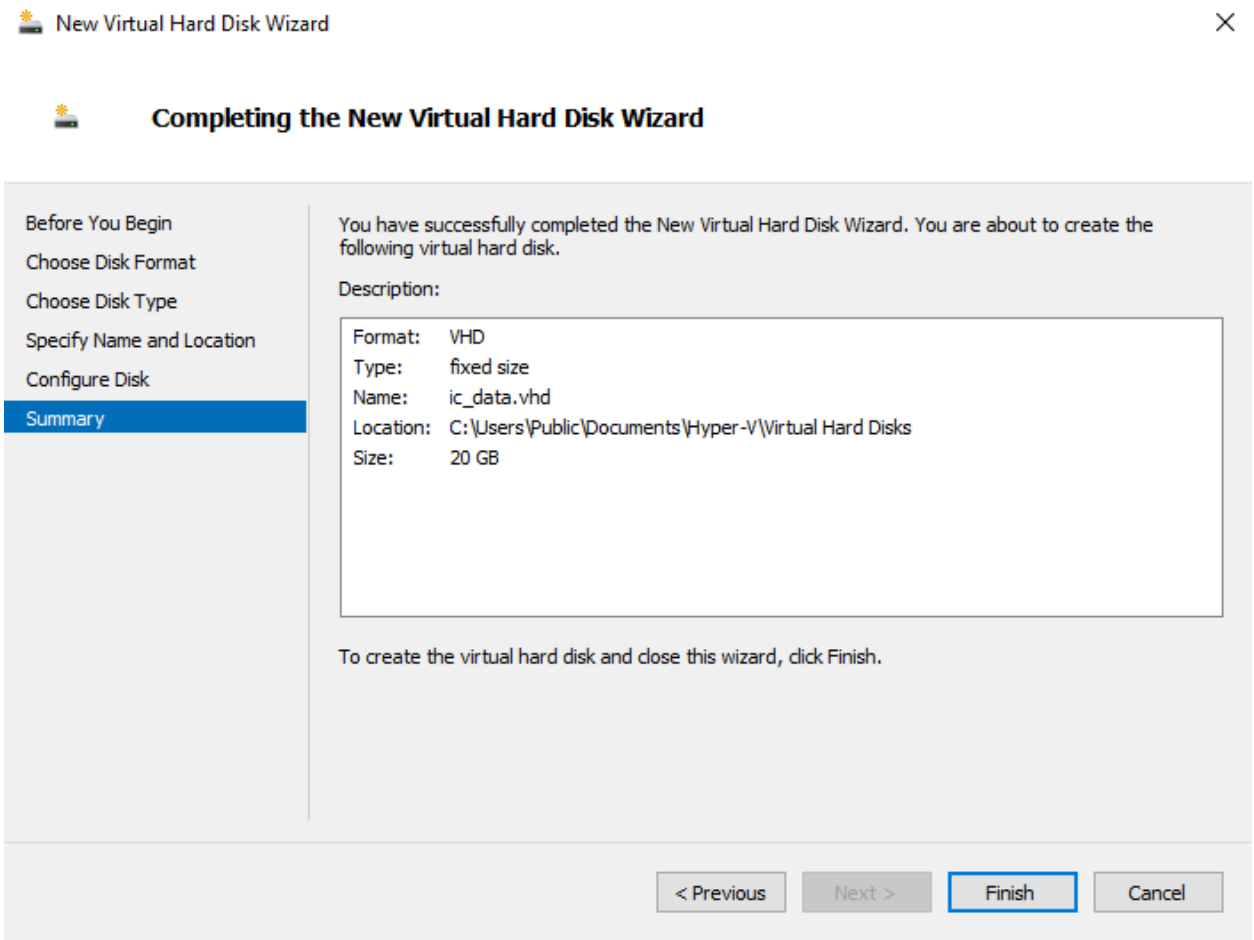
InControl VM:



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 11.1.

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.

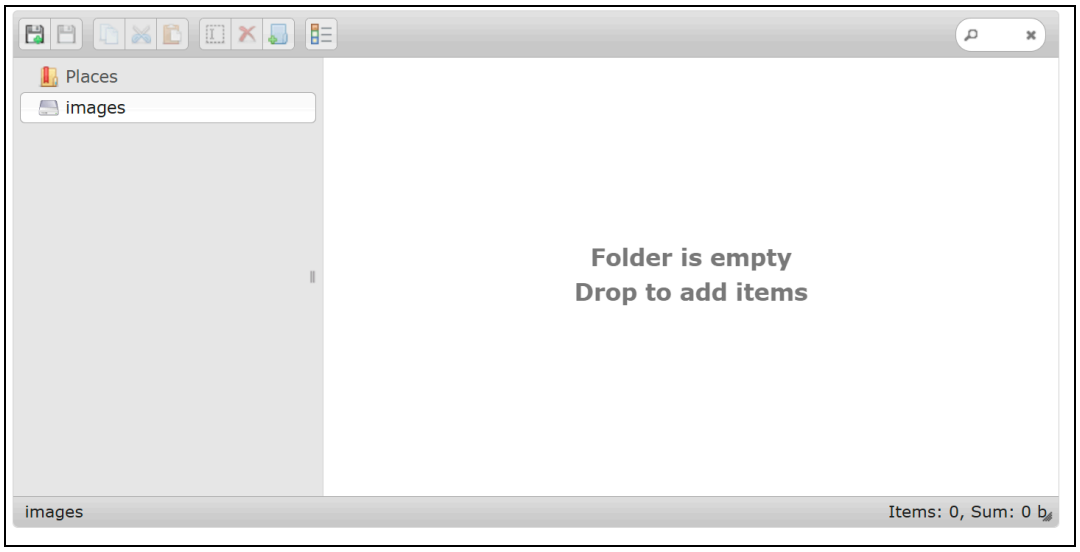
1.5 Installation on KVM on Peplink Edge Computing Platform

The InControl Virtual Appliance supports running on KVM on the Peplink Edge Computing platform. Please visit this page for the supported models that come with 16GB or more memory.

Here is the setup procedure.

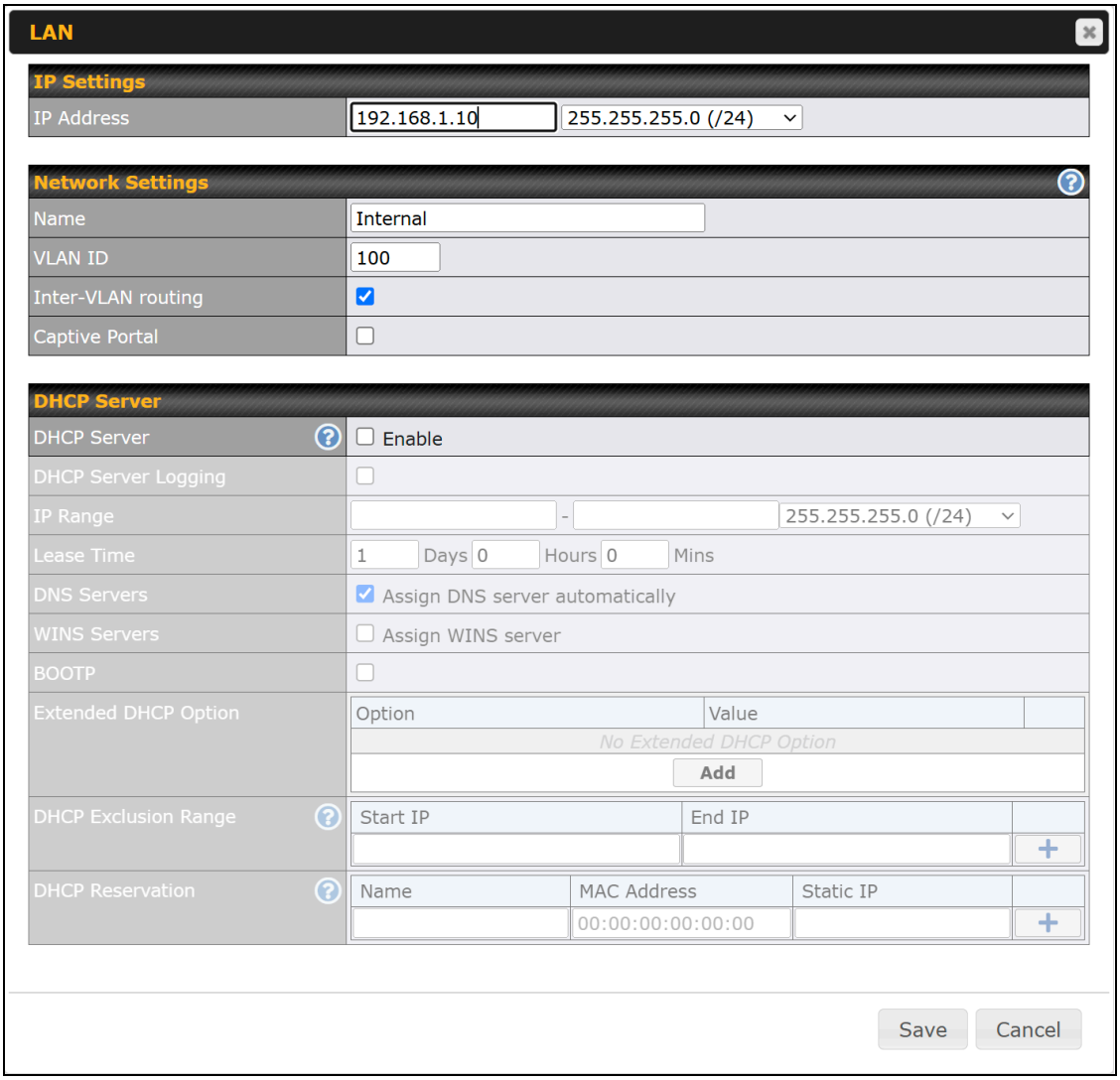
1. You have to prepare an Ubuntu terminal for managing the KVM on the command line.
2. Log in as root. Run '`apt install qemu-utils and libvirt-clients`' to install the required packages.
3. Create empty data disks by running:
   `qemu-img create -f qcow2 DB-Data.qcow2 100G`
   `qemu-img create -f qcow2 InControl-Data.qcow2 20G`
   where the "20G" and "100GB" are the disks' sizes. They are good for small setups.
4. Download the two files to your local PC.
5. Download the installation files for KVM in ZIP format from the download site to your local PC. Extract the files. You will find the files: `icva.xml`, `dbvm.xml`, `InControl-System.qcow2`, and `DB-System.qcow2`.
6. On your local PC, log in to the Peplink device's web admin with a web browser. Navigate to "System" > "Storage Manager". Click the first "Configure" button and review the partition settings. Allocate as much space to KVM as possible.
7. Navigate to "Advanced" > "Edge Computing" > KVM", enable KVM, and press "Save".

8. Click the first “here” link on the page to open the file manager.



Drag the four `qcow2` files and drop into the empty area of the file manager. Wait until the upload is complete.

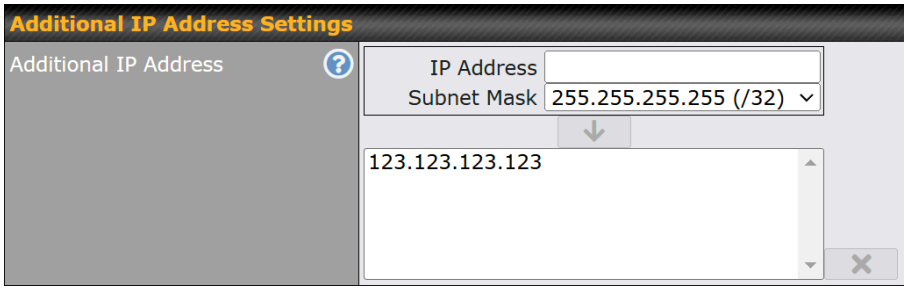
9. Navigate to “Network” > “LAN” > “Network Settings”. Create an “Internal” VLAN for inter IC VM and DB VM communications. Click “New LAN” and change the settings as shown below:



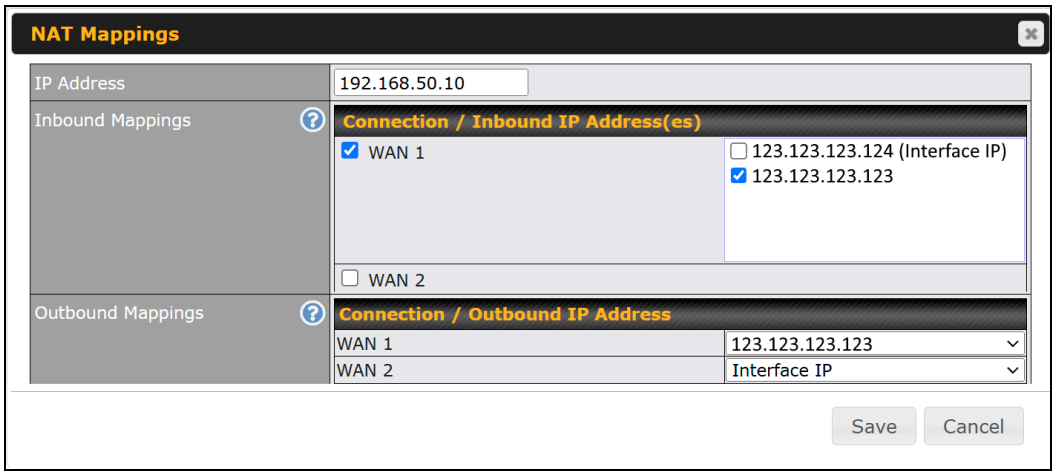
If you change the "VLAN ID" to a number other than 100, you will have to edit the two XML files and replace the string "`br_vlan100`" with "`br_vlan`*`NNN`*" where *`NNN`* is the new VLAN ID.

10. Navigate to "Network" > "WAN". Assuming that you are connected to the network on "WAN 1" and a static IP address is assigned to it. Click on it to edit its settings. Scroll down to the "Additional IP Address Settings" section, and add a second IP address to it.

This IP address will be for accessing the InControl from the external.



11. Navigate to “Advanced” > “NAT Mappings”. Assuming the IC VM’s internal IP address is 192.168.50.1 on the Untagged LAN. Change the Inbound and Outbound Mapping to its external IP address.



12. Press “Apply Changes”.
13. Transfer the “`icvm.xml`” and “`dbvm.xml`” to a directory of your Ubuntu system.
14. At the directory storing the above two files, run the following command to connect to the KVM on the Peplink device and enter into a “`virsh`” shell:
    `virsh -c qemu+tcp://`***`PEPLINK_IP`***`/system`
    where the ***`PEPLINK_IP`*** is the Peplink device’s LAN or WAN IP address. Enter your “`admin`” and the web admin password as the “authentication name” and “password” respectively:

```
$ virsh -c qemu+tcp://192.168.1.10/system
Please enter your authentication name: admin
Please enter your password: <web admin password>
Welcome to virsh, the virtualization interactive terminal.

Type:  'help' for help with commands
       'quit' to quit
```

```
virsh #
```

15. At the `virsh` prompt, run "`define dbvm.xml`" and "`define icvm.xml`".
16. Run "`start dbvm`" and "`start icvm`" to start the two VMs.
17. Start a VNC client on your local PC to connect to the Peplink device's IP (on the display number) to access the IC VM's console. Log in to the console with the username and password "`setup`" and "`setup`". Change the system's IP address to your desired IP address on the Balance's LAN subnet.
    (The DB VM's console is also accessible on port 5901 or display number 1.)
18. Log in to the control panel and upgrade the system.

The installation is completed.

1.6 Installation on AWS

1.6.1 Preparing AMIs

1.6.1.1 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.

1.6.1.2 For AWS GovCloud

For AWS GovCloud, you should receive two image files, namely `InControl-System-2.14.2.2-ami-root.raw`, `InControl-System-2.14.2.2-ami-data.raw`, and `DB-System-20260224-ami.raw` 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": "raw",
      "UserBucket": {
          "S3Bucket": "YOURBUCKETNAME",
          "S3Key": "YOURSUBFOLDER/DB-System-20260224-ami.raw"
      }
  }]
```

icva.json:

```
  [
    {
      "Description": "InControl VM System Disk",
      "Format": "raw",
      "UserBucket": {
          "S3Bucket": "YOURBUCKETNAME",
          "S3Key": "YOURSUBFOLDER/InControl-System-2.14.2.2-root-ami.raw"
      }
    },
    {
      "Description": "InControl VM Data Disk",
      "Format": "raw",
      "UserBucket": {
          "S3Bucket": "YOURBUCKETNAME",
          "S3Key": "YOURSUBFOLDER/InControl-System-2.14.2.2-data-ami.raw"
      }
    }
  ]
```

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
```

1.6.2 Setting up network

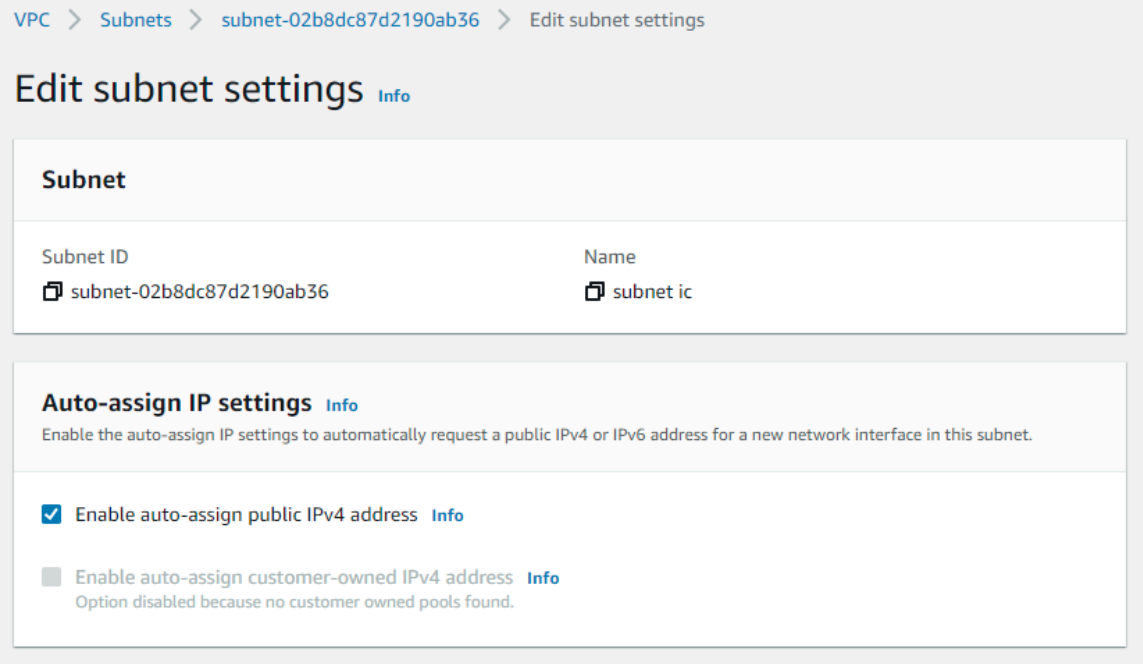
InControl Virtual Appliances require to be set up in a Virtual Private Cloud (VPC) for virtual machines to communicate in a secured environment.

If you are going to launch the InControl EC2 instances in an existing VPC, please make sure both the “DNS hostnames” and “DNS resolution” options of the VPC are enabled.

Otherwise, please log in into the Amazon console, open the VPC service, and follow the following instructions:

1. Click the “*Create VPC*” button.
2. Choose “*VPC and more*” for the “*Resources to create*” field.
3. Fill in the VPC settings:
    a. Fill in a IPv4 CIDR block that you prefer.
    b. No IPv6 CIDR block is necessary.
    c. The “*Tenancy*” can be “*Default*”.
    d. The “*Availability Zones*” can be “*1”* or above.
    e. The number of public subnets can be “*0*”
    f. The number of private subnets can be “*2*” or above.
    g. “*NAT gateways*” can be “*None*”.
    h. “*VPC endpoints*” shall be “*None*”.
    i. **IMPORTANT**: both “*DNS hostnames*” and “*DNS resolutions*” options shall be enabled.
4. Press the “*Create VPC*” button.
5. Once the VPC has been created, record the VPC ID. Click into “*Subnets*” and search for the newly created subnet(s) by the recorded VPC ID. Click into the subnet that you want to launch InControl instances, click the “*Actions*” menu, and then click “*Edit subnet settings*”. Check the “*Enable auto-assign public IPv4 address*” option and press the *Save*

button.



6. Navigate to “Internet gateways”. Click the “Create internet gateway” button. Give the gateway a name and click the “Create internet gateway” button. Record the internet gateway’s ID.
7. Select the newly created internet gateway, select the action “Attach to VPC”. Choose the created VPC.
8. Navigate to “Route tables”. For each route table in the VPC, select it, click “Actions” and “Edit routes”. Add a route for the Destination “`0.0.0.0/0`” to the Internet gateway’s ID.

1.6.3 Setting up security groups

InControl Virtual Appliance requires two security groups, one for the InControl server and one for the Database 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	Description
TCP	4443	Any	Control panel website
TCP	443	Any	InControl website
TCP	2222	Any	Remote assistance (direct)

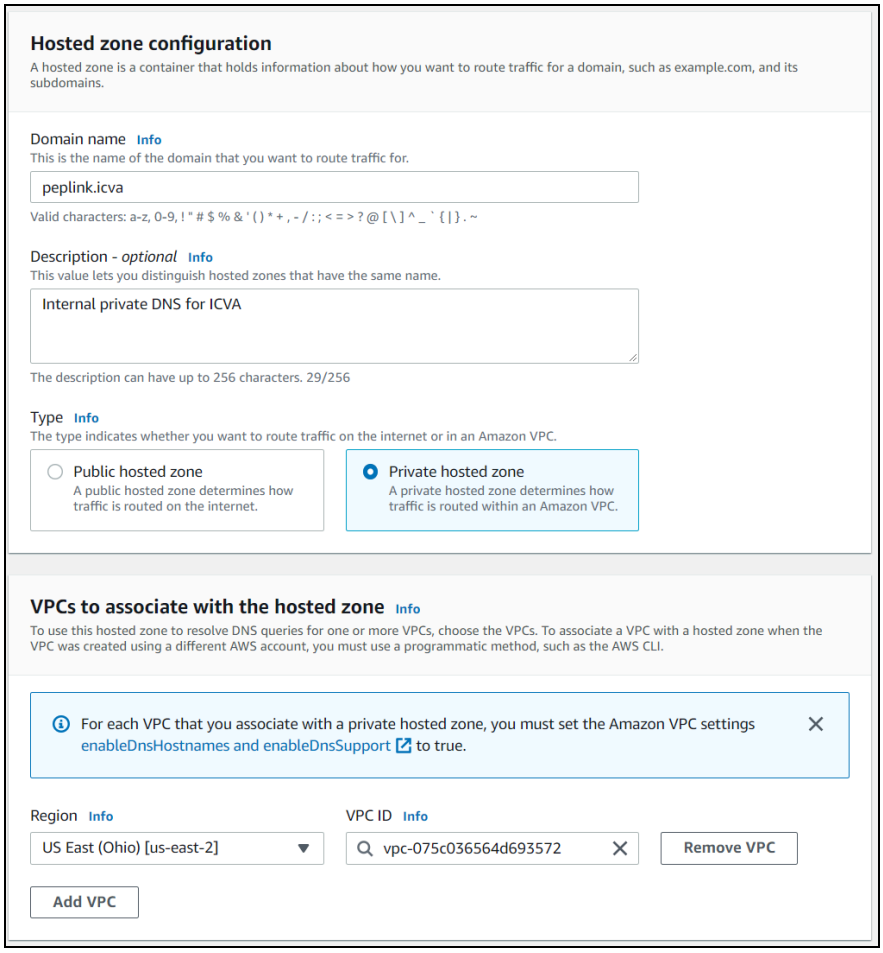
TCP	80	Any	InControl web redirector
TCP	1443	Any	Remote web admin
TCP	5246	Any	Remote web admin
UDP	5246	Any	Device communication
UDP	53	Any	Find My Peplink DDNS

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**:

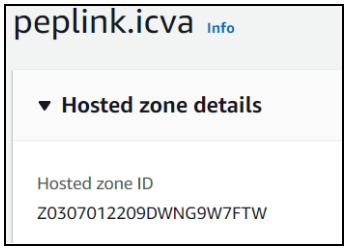
Protocol	Port	Source	Description
TCP	3306	*The VPC's subnet address*	MySQL database
TCP	27017	*The VPC's subnet address*	MongoDB
TCP	6379	*The VPC's subnet address*	Redis
TCP	22	*The VPC's subnet address*	SSH, management
All ICMP (IPv4)	-	*The VPC's subnet address*	Troubleshooting

1.6.4 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**.



1.6.5 Creating a role for Route 53 DNS update and snapshot creation

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**.

Click the **Create Policy** button again. Click the **JSON** tab. Paste the following content to the text editor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Click **Next: Tags**. Click **Next: Review**. On the **Review policy** screen, put ***AllowSnapshotCreation*** 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 policies ***AutoDNSUpdatePeplink*** and ***AllowSnapshotCreation*** that you just created. Click **Next: Tags**. Click **Next: Review**. On the **Review** screen, put a name, say, ***AutoDNSUpdatePeplink***, in the **Role name** field. Click **Create role**.

1.6.6 Launching instances

Please follow the instruction in chapter 1.6.1 to prepare the AMI images in your account. You shall launch a DB instance first and then an InControl instance.

- Navigate to **EC2** and select **AMIs**.
- Select the AMI **DB-System-20260224** for a DB instance (**InControl-System-2.14.2.2** for an InControl instance) and click the **Launch** button
- In the Name field, input "*ICVA InControl*" and "*ICVA Database*" for InControl and DB instance, respectively.
- Click **Add additional tags**. Add the following tags and values respectively for InControl and DB. Replace *HOSTED_ZONE_ID* with the Route 53 private hosted zone ID. You may change the domain "peplink.icva" in the AUTO_DNS_NAMEs to something else.

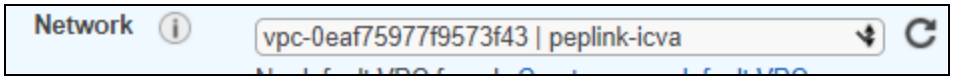
  Important: make sure no trailing space in the keys and values.

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

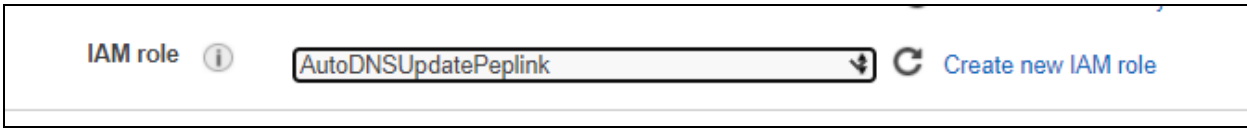
InControl instance	
Key	**Value**
AUTO_DNS_ZONE	*HOSTED_ZONE_ID*
AUTO_DNS_NAME	`web.peplink.icva`
Name	`ICA IC`

- In **Instance type**, select "t3.large" or higher where the memory size is at least 8GB.
- In the **Key pair** section, choose "Proceed without a key pair".

- In Network Settings,
  - choose your **VPC** and **Subnet**.



  - **Auto-assign public IP** must be enabled. The IP address is for the instances to make AWS Route 53 API calls to update their DNS records.
  - Select the corresponding security group you created earlier.
- In the **Configure storage** section, click **Add new volume**, set size to at least 50 GB. (Note: this step can be skipped for the InControl System AMI in the GovCloud because the volume has already been included in the AMI.)
- Expand the **Advanced details** section.
  - Set the **IAM role** as *AutoDNSUpdatePeplink*.



  - Set "Enable" and "V2 only (token required)" in the **Metadata accessible** and **Metadata version** fields, respectively.
- Click the **Launch instance** button.

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 11.1.

1.6.7 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.

1.6.8 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.

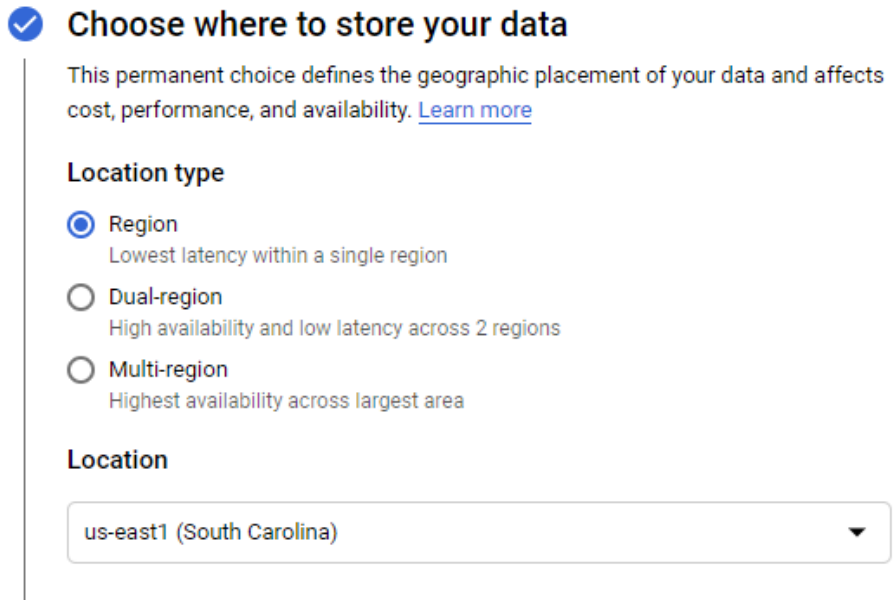
1.7 Installation on Google Cloud Platform

1.7.1 Request the disk images

You may email ica@peplink.com to request the disk images for Google Cloud. The disk images are `InControl-System-2.9.0.img` and `DB-System-20210323-gce.tar.gz`.

1.7.2 Uploading the images

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.

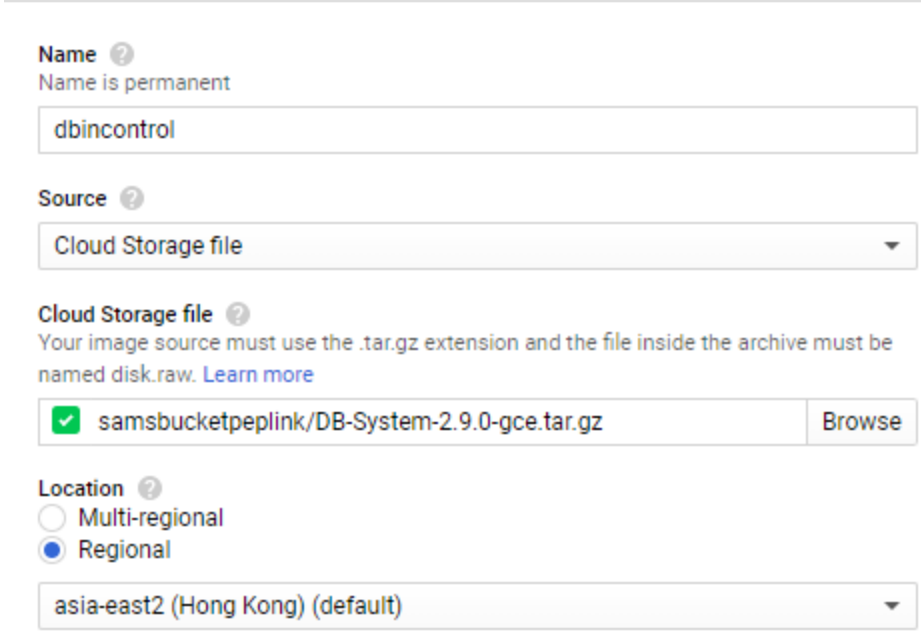


Once the bucket is created, open it and upload the downloaded DB and InControl images to it.

1.7.3 Importing the image

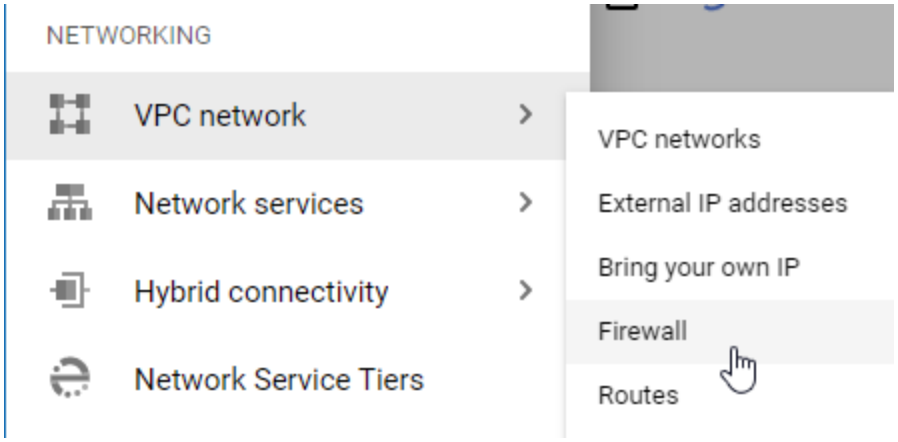
Once files are uploaded, browse to Google Cloud Compute Engine, then the Image menu under the Storage section.

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.



1.7.4 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 (e.g.: 0.0.0.0/0)
- Check TCP and paste the following: `80,443,2222,4443,5246`
- Check UDP and paste the following: `53,5246`

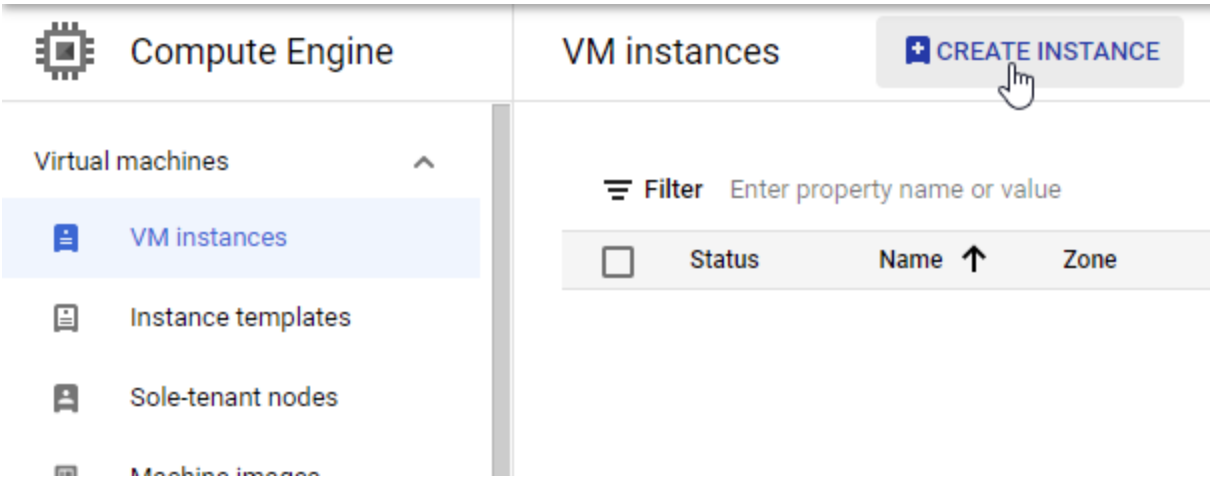
- Click on create

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 (e.g.: 10.170.0.0/20)
- Check TCP and paste the following: `22,3306,6379,27017`
- Click on Create

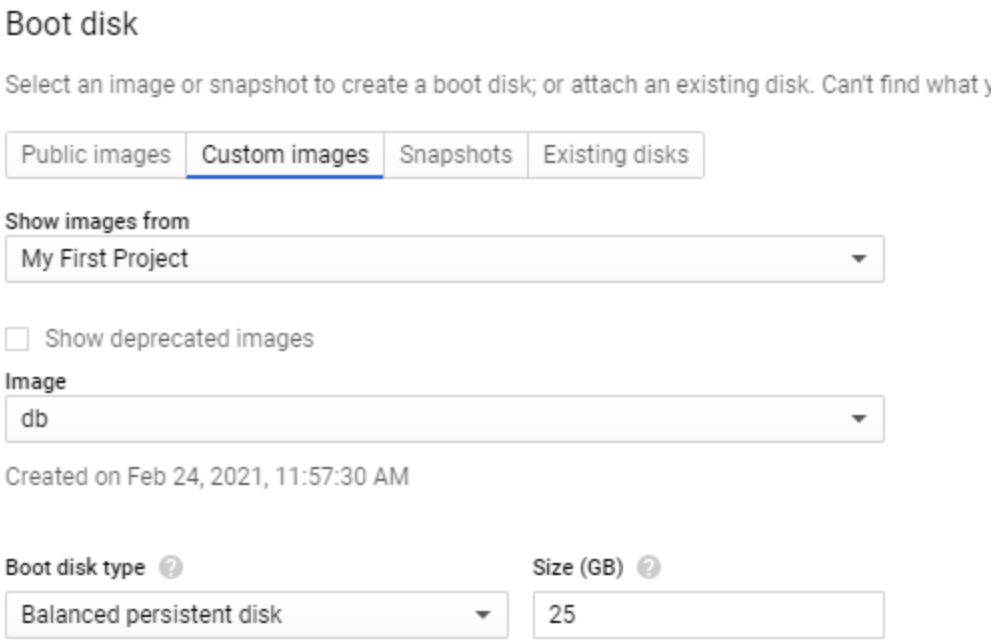
1.7.5 Creating the instances

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

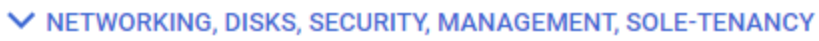


- Name your DB instance “ica-db”
- Select the desired machine configuration

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

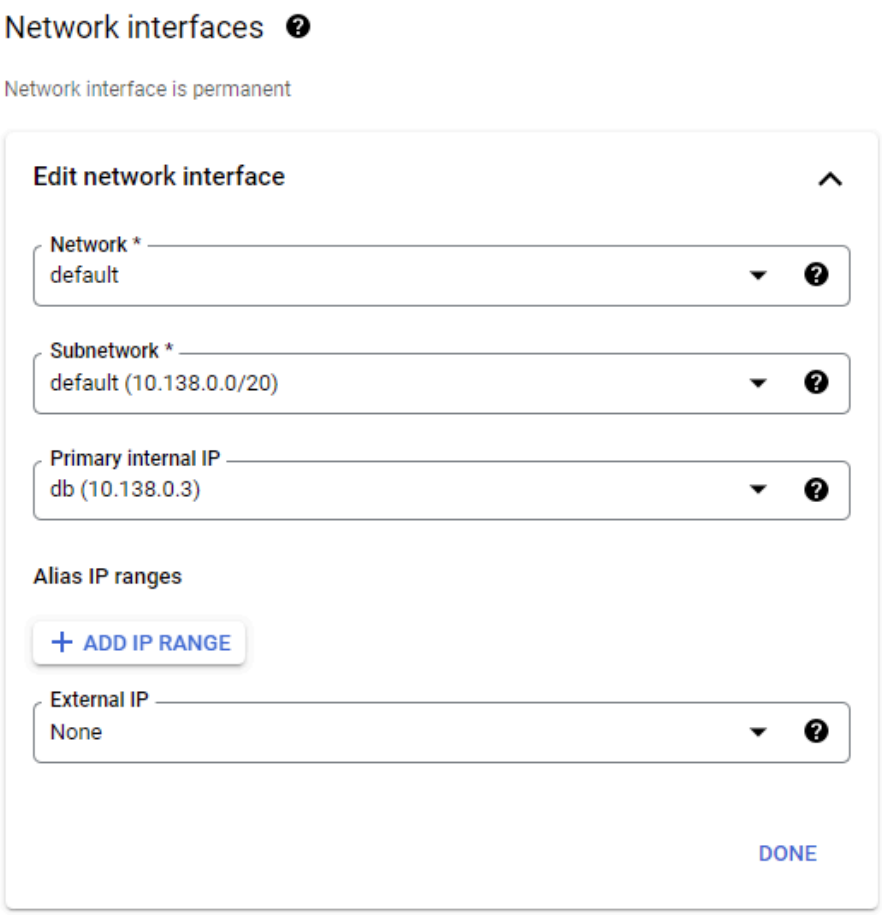


- Expand the “Networking, disks, security, management, sole-tenancy” menu



- 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”

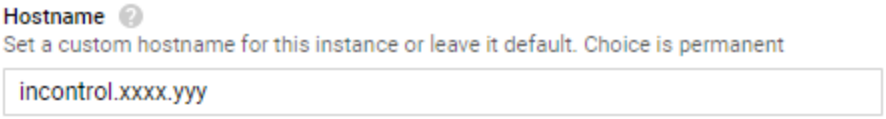


  - Click on Done
- Browse to the Disks section and add a new disk. Name it “ica-db-data”. Input size of 20 GB or above. Click Done.
- Click Create

Now create another new instance for the InControl:

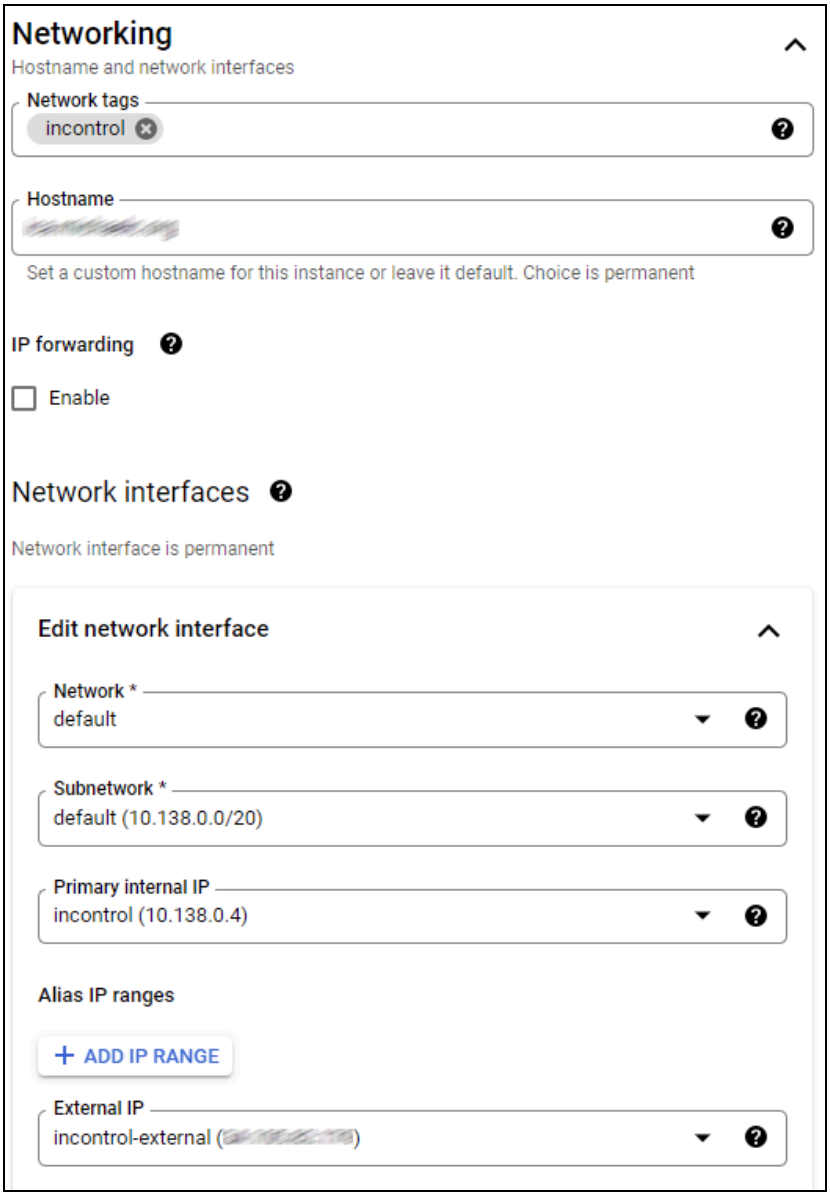
- Name your instance (e.g.: incontrol)
- Select the desired machine configuration
- Under Boot disk section, click on Change and browse to Custom Images, select your project and the InControl image then click on Select
- Expand the “Networking, disks, security, management, sole-tenancy” menu
- Browse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

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



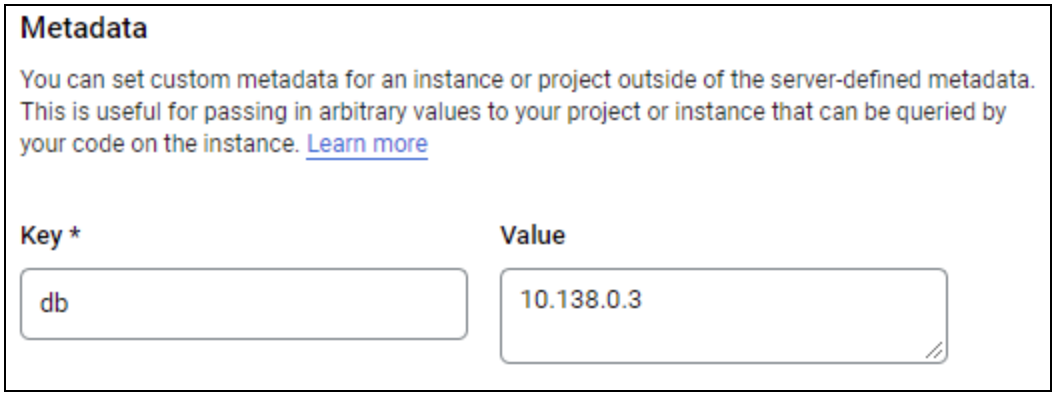
- Under Network interfaces, edit the network interface
  - Under Primary Internal IP, select Reserve Static IP Internal Address
  - Select “Let Me Choose” under “Static IP address” and input the desired IP for InControl instance
  - Under External IP, select either Create IP address or assign the desired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

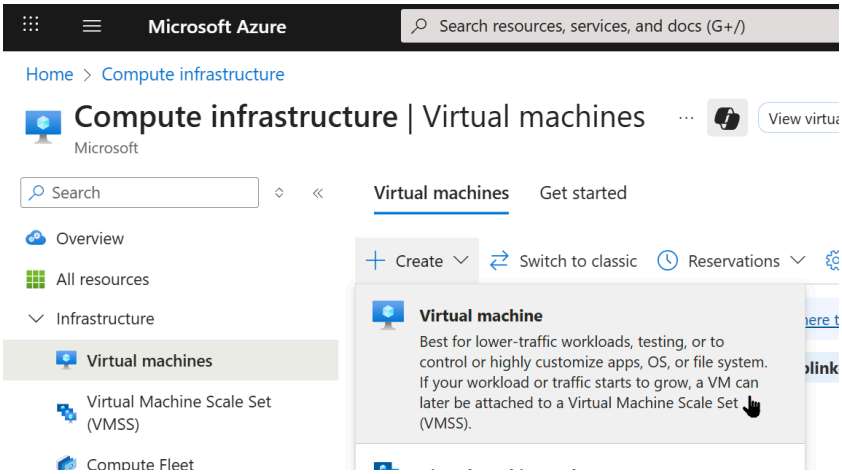
The system will take about 6 minutes to boot up for the first time if everything is set up correctly.

1.8 Installation on Azure

Throughout this setup guide for Azure, we refer to the new version of Azure portal.

1.8.1 Create the InControl instance

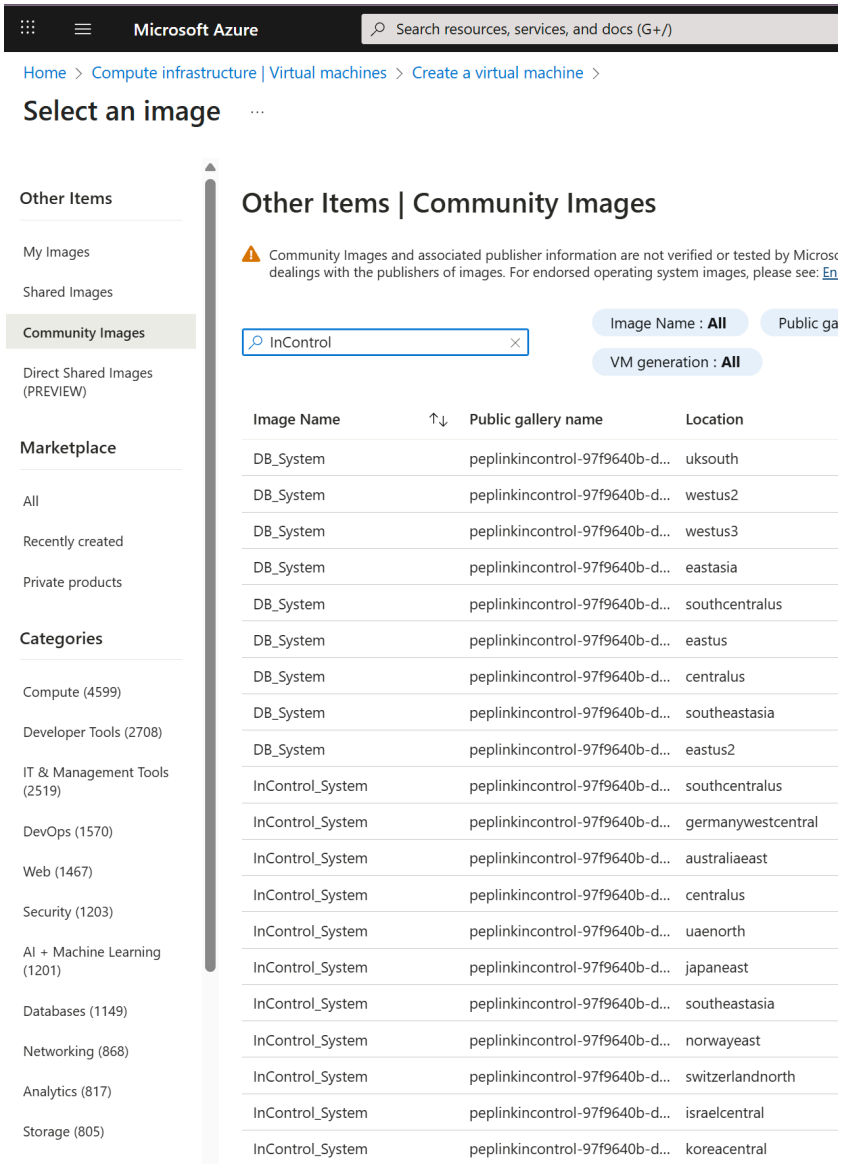
1. Sign in to the Azure Portal, navigate to the Azure service “Virtual machines”. Click “+ Create” > “Virtual machine”.



2. **Project details**: In the “Resource group” field under “Subscription”, click “Create new” and give it a name. E.g. “InControl”.

Tip: You are recommended to create a new resource group rather than choosing an existing one. Some existing resource group's settings might cause conflicts to the setup.

3. **Instance details > Basics**:
   - Enter a "Virtual machine name", e.g. "ICVA-InControl".
   - Leave the "Region", "Availability options", "Zone options", "Availability zone", and "Security type" fields unchanged. (A region will be selected after you choose an image.)
   - For the "Image" field, click "See all images", click "Community Images" on the left bar, and type "InControl" in the search box.



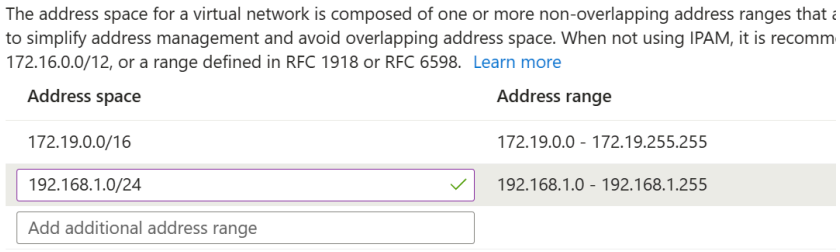
Click “Load more” if needed. Pick an “InControl_System” image that is at your favorite location. If your favorite location is available in Azure but not shown here, please send the location to ica@peplink.com.
- In the “Size” field, click “See all sizes” and choose “D4as_v4” (4 vcpus, 16 GiB memory, 32 GB storage) or above.
- Inbound port rules: Leave the “Allow selected ports” option selected. In the “Select inbound ports” field, enable “HTTP (80)” and “HTTPS (443)”, and disable “SSH (22)”. (We will review the rules later.)
- Licensing: choose “Other” in the “License type” field.
- Click “Next : Disks”

4. **Instance Details > Disks:**
   - OS disk: Leave the “OS disk size” field as “Image default”. Customize the rest field as you wish.
   - Data disks: click “Create and attach a new disk”. You can optionally customize the fields. For the Size field, you may choose “32 GiB” or larger. Click “OK”.
   - Click “Next : Networking”
5. **Instance Details > Networking:**
   - Virtual Network: you can optionally change the name by clicking “Edit virtual network”.
   - Subnet: click “Edit subnet”. In the “Name” field, enter “WAN”. You can optionally change the subnet IP settings. Press “Save”.
   - Customize the rest fields optionally.
   - Click “Next : Management”.
6. **Instance Details > Management, Monitoring, Advanced, and Tags**: You can optionally customize the settings. Click “Review + create”.
7. **Instance Details > Review + create:**
   After reviewing the settings, press “Create” and wait until the InControl VM deployment completes. Click “Go to resource”.
8. On the ICVA-InControl VM Overview screen, click the “Stop” button on the top bar.

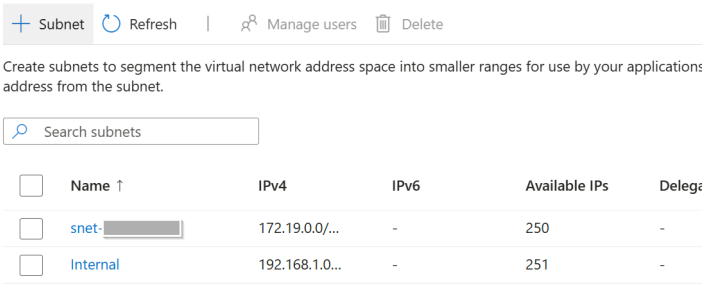
1.8.2 Create an internal network and attach a second network interface

9. On the left navigation bar, click “Network settings” under “Networking”. Click into the VM’s Virtual network’s detail screen.
10. You should be on a “vnet-xxxxxxxx” screen. On the left navigation bar, click “Address space” under “Settings”. In the “Add additional address range” text box, fill in

"192.168.1.0/24". Press "Save" on the page's bottom.



11. On the left navigation bar, select "Subnets" under "Settings". Press "+ Subnet". Input "Internal" in the "Name" field. In the "IPv4" > "IPv4 address range" field, select "192.168.1.0/24". Press "Add" on the page's bottom.



12. Navigate to the Home screen and select the "ICVA-InControl" VM. In the left navigation bar, select "Network settings" under "Networking". With the default network interface selected, in the "Rules" section in the lower half of the screen, you should see "HTTP" and "HTTPS" rules have already been defined. Click the "Create port rule" button to set up the rest inbound and outbound firewall rules as specified in chapter 10. Settings on Your Firewall. (By default, outbound accesses are unrestricted. You may keep the outbound rules unchanged in the testing phase.)
13. Click "Attach network interface" on the top bar. Click "Create and attach network interface" in the pop-up.
    On the Create network interface screen, in the "Network interface" section, input "Internal" in the "Name" field. In the Subnet field, choose "Internal (192.168.1.0/24)". In the "Private IP address" field, input "**192.168.1.5**" (IMPORTANT). Press "Create" on the page's bottom.
14. When the second network interface is created, the ICVA-InControl VM has been set up. Leave it stopped. Navigate back to the "Home" page and then "Virtual machines".

1.8.3 Create the Database instance

15. Click the "+ Create" button at the top bar, and click "Virtual machine". In the "Resource group" field, choose the resource group (e.g. "InControl") created in step 2.

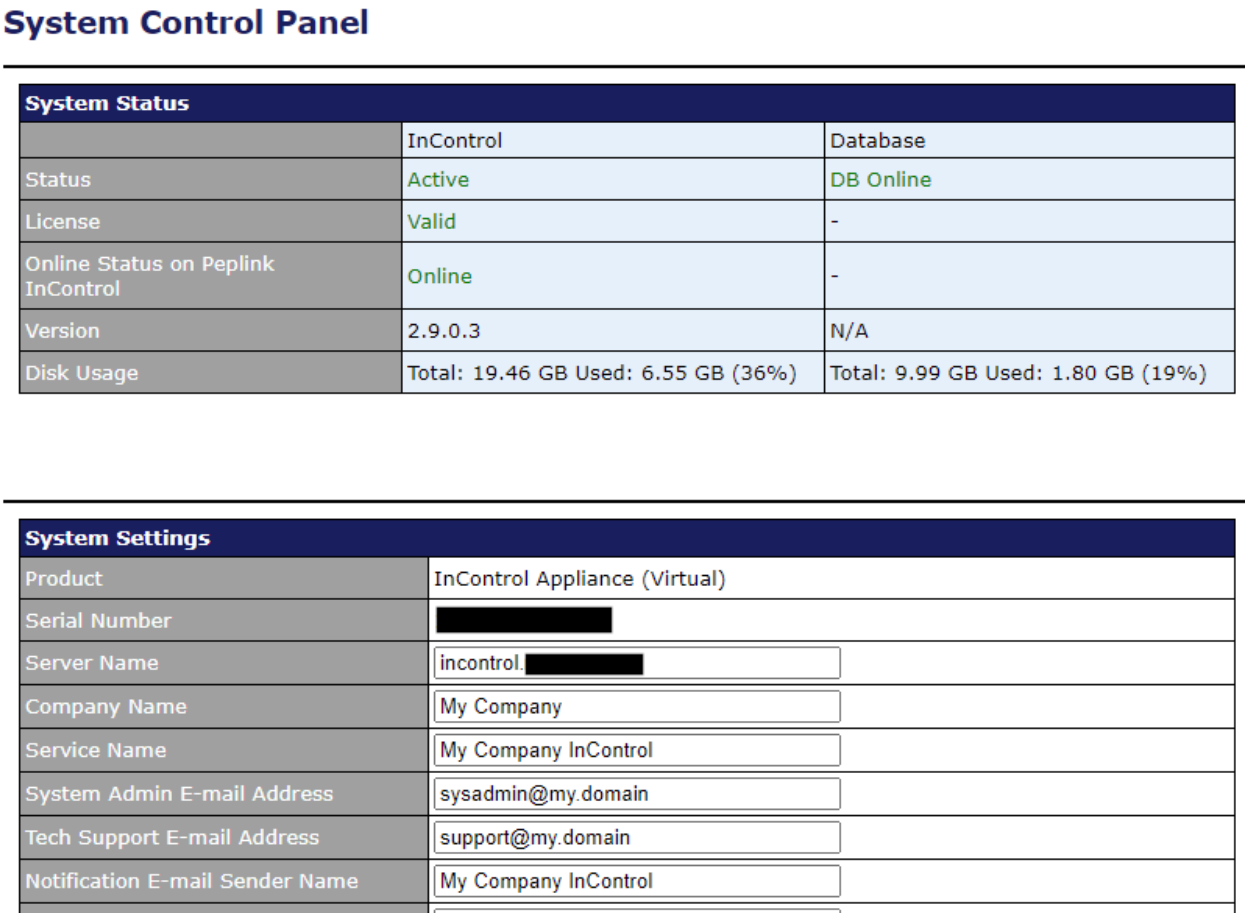
16. **Instance details > Basics**:
    - Enter a “Virtual machine name”, e.g. “ICVA-Database”.
    - Leave the “Region”, “Availability options”, “Zone options”, “Availability zone”, and “Security type” fields unchanged.
    - For the “Image” field, click “See all images”, click “Community Images” on the left bar, and type “InControl” in the search box.
    - Pick the “DB_System” image that is at the same location as the first VM.
    - In the “Size” field, click “See all sizes” and choose “D2s_v4” (2 vcpus, 8 GiB memory, 8 GB storage) or above.
    - Choose “None” for the “Public inbound ports”
    - Licensing: choose “Other” for the “License type”.
    - Click “Next : Disks”
17. **Instance Details > Disks:**
    - OS disk: Leave the “OS disk size” field as “Image default”. Customize the rest field as you wish.
    - Data disks: click “Create and attach a new disk”. You can optionally customize the fields. For the Size field, you may choose “32 GiB” or larger. Click “OK”.
    - Click “Next : Networking”
18. **Instance Details > Networking:**
    - Virtual Network: choose the “Virtual network” (VNet) created in step 5. I.e the same VNet as the InControl VM.
    - Subnet: select the “Internal” subnet. (Tip: if you don’t see it, you are likely not using a newly created resource group. If so, go back to step 2 and start over again.)
    - Public IP: select “None”
    - Customize the rest fields optionally.
    - Click “Next : Management”.
19. **Instance Details > Management, Monitoring, Advanced, and Tags**: You can optionally customize the settings. Click “Review + create”.
20. **Instance Details > Review + create:**
    After reviewing the settings, press “Create” and wait until the Database VM deployment completes. Click “Go to resource”.
21. Ensure the “Private IP address” of the ICVA-Database VM is 192.168.1.4. If not, stop the VM, click the link in the large “Network interface” drop-down menu to enter into the network interface settings screen. In “Settings” > “IP configuration” > “ipconfig1” > “Private IP address settings” > “Allocation”, choose “Static”. Then input “192.168.1.4” as the “Private IP address”. Press “Save”.
22. Navigate back to “Home” and select the ICVA-InControl VM. On the VM Overview screen, click the Start button on the top bar to start the ICVA-InControl.

After a few minutes, the InControl Virtual Appliance's control panel will be accessible from the Internet. The installation is completed.

1.9 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 System 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://{server_name}: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%)

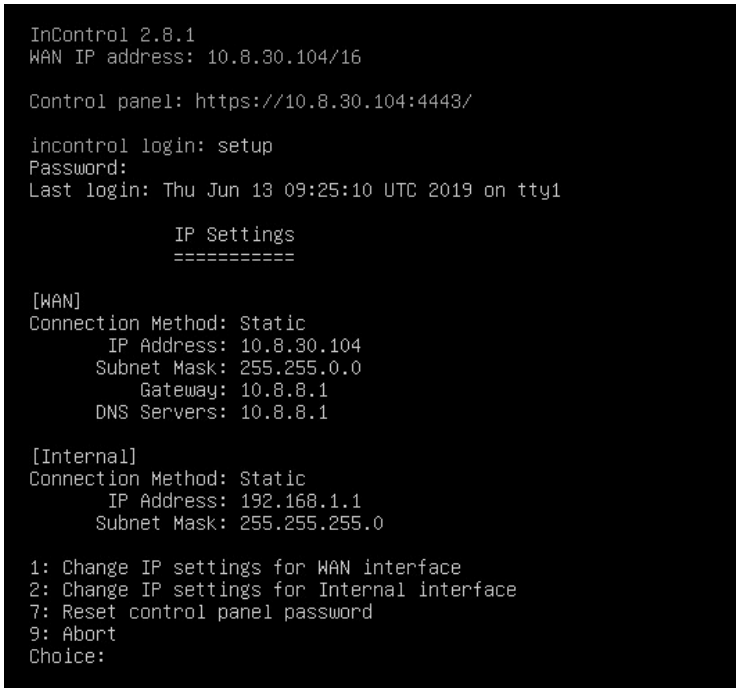
System Settings	
Product	InControl Appliance (Virtual)
Serial Number	[redacted]
Server Name	incontrol.[redacted]
Company Name	My Company
Service Name	My Company InControl
System Admin E-mail Address	sysadmin@my.domain
Tech Support E-mail Address	support@my.domain
Notification E-mail Sender Name	My Company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

After InControl VM is booted up for the first time, please update its firmware immediately. Please refer to chapter 11.1 for the upgrade details. Afterward, input a license key. Then update the server name and other settings.

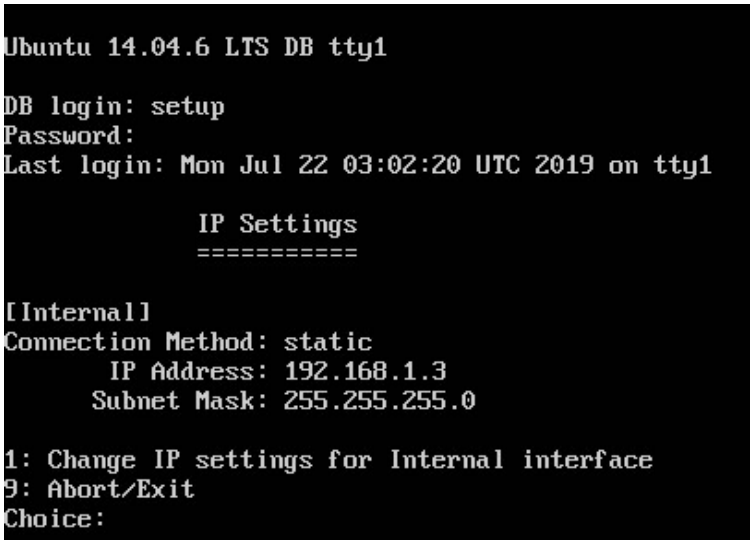
1.10 IP Address Configuration and Password Reset On the Console

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



1.10.1 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. You can change their Internet network IP addresses on the console as described above. But before making the changes, you will have to navigate to the control panel

and update the “Database IP Address” setting first. This settings to tell the InControl VM where the DB VM is.

Database Settings	
Database IP Address	192.168.1.3

1.11 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.

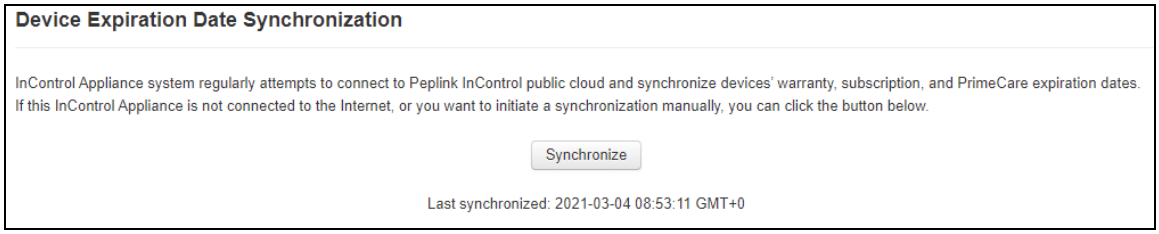
Managed devices are required to be in-warranty or covered by an InControl subscription in order to appear online and be manageable. If the system is firstly installed or upgraded to 2.9.0 or above, the system will enter into a 7-day grace period. Within the period, device expiry date checks are not enforced. 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.

1.12 Automatic Synchronization of Service Expiration Records

Since version 2.9.0, the InControl Appliance automatically synchronizes devices' service expiration records with Peplink InControl on the Internet every six hours. This ensures the appliance maintains up-to-date warranty, subscription, and PrimeCare date records. Additionally, the following data is synchronized at the same time:

- Device Feature Add-on activations
- New product and model definitions
- Firmware releases
- Captive portal default certificates



1.12.1 Synchronization via External Computer with Internet Connectivity

If the system is unable to access the Internet directly, system administrators can synchronize the data via a browser from a computer that has Internet connectivity and is able to reach the InControl Appliance. To do this:

1. Visit the appliance's MSP-level Device Management page at `https://{SERVER_NAME}/r/msp/device_management`
2. Click the **Synchronize** button in the "Device Expiration Date Synchronization" section.

When the web browser has Internet access and can reach Peplink InControl, clicking the **Synchronize** button will automatically complete the synchronization process.

1.12.2 Fully Offline Synchronization

If the system is entirely offline and the web browser cannot access the Internet, follow these steps:

1. Visit the appliance's MSP-level Device Management page at `https://{ICA_Address}/r/msp/device_management`.
2. The page will display on-screen instructions, prompting you to copy encrypted messages from the ICVA.
3. Paste the copied message into an InControl page (using remote desktop, email, etc.).

4. The InControl page will generate another encrypted message for you to copy.
5. Paste this message back into the ICVA page to complete the synchronization process.

If the system does not have an Internet connectivity to reach the Peplink InControl, whenever any devices' service contract has been renewed in Peplink, system administrators will be required to perform data synchronization manually by visiting the appliance's MSP-level Device Management page (`https://{SERVER_NAME}/r/msp/device_management`) and clicking the Synchronize button in the "Device Expiration Date Synchronization" section.

2. Input E-mail Delivery Settings

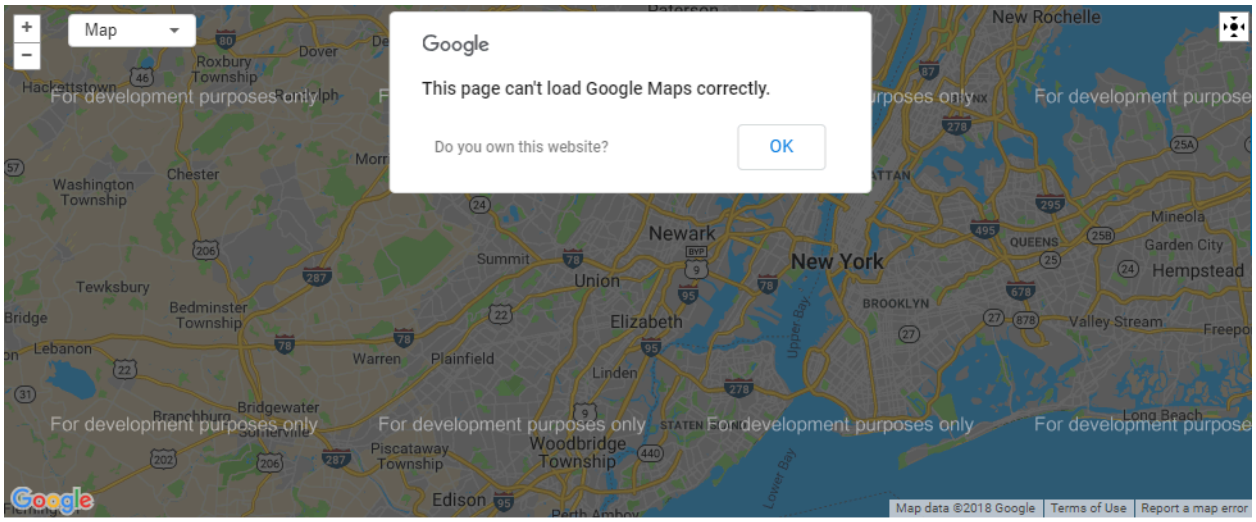
To create new accounts, the system has to be able to send confirmation emails to do account confirmation. So please configure the SMTP server settings, as well as the "Notification E-mail Sender Name" and "Notification Sender E-mail Address" in the System Settings above accordingly.

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.*	

3. 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.

4. 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.

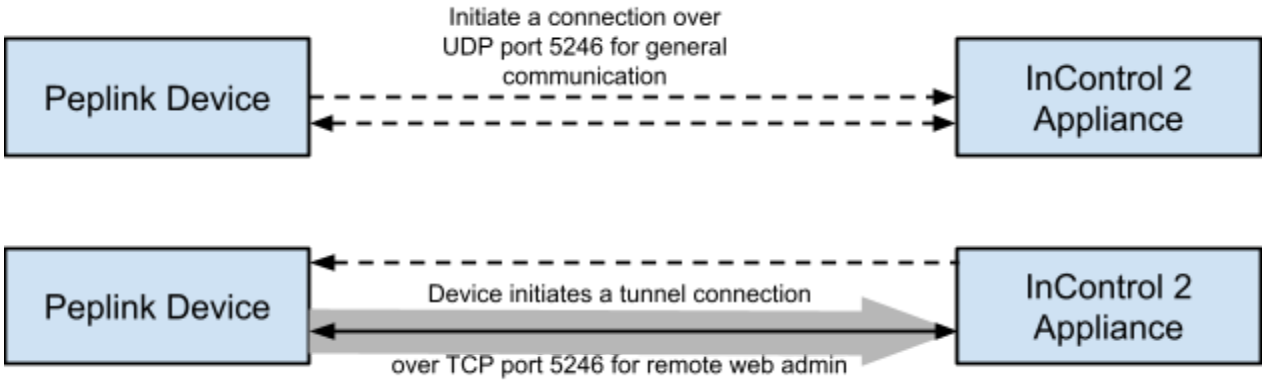
When the data is requested over the web or API, the system will automatically choose to retrieve the data from the database or the archive server and return it to the user or API client. So you are encouraged to set up an FTP/SFTP archive server for storing those historical data.

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

5. Setting up Devices to Report to InControl

Unlike SNMP, Peplink 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).

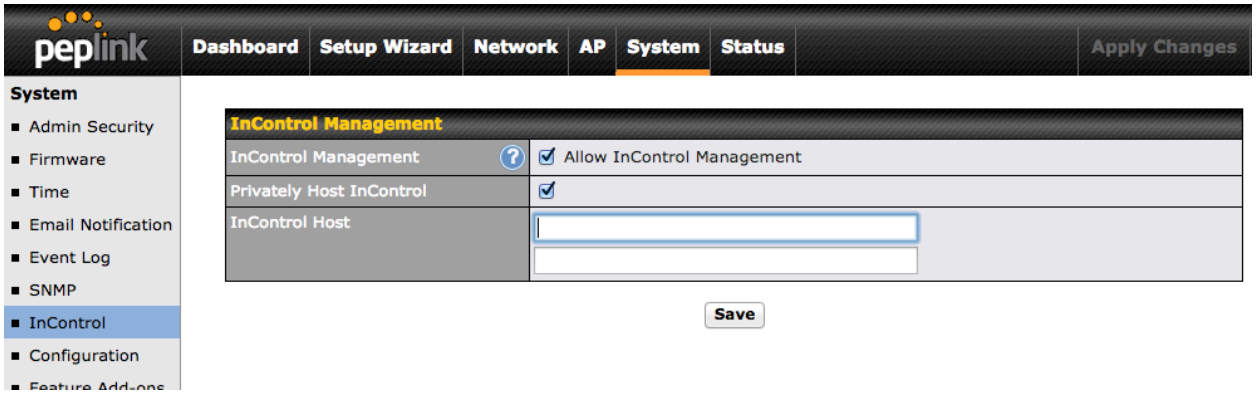


There are two ways to configure your Peplink devices to report to your InControl appliance instead of the Peplink InControl in the public cloud.

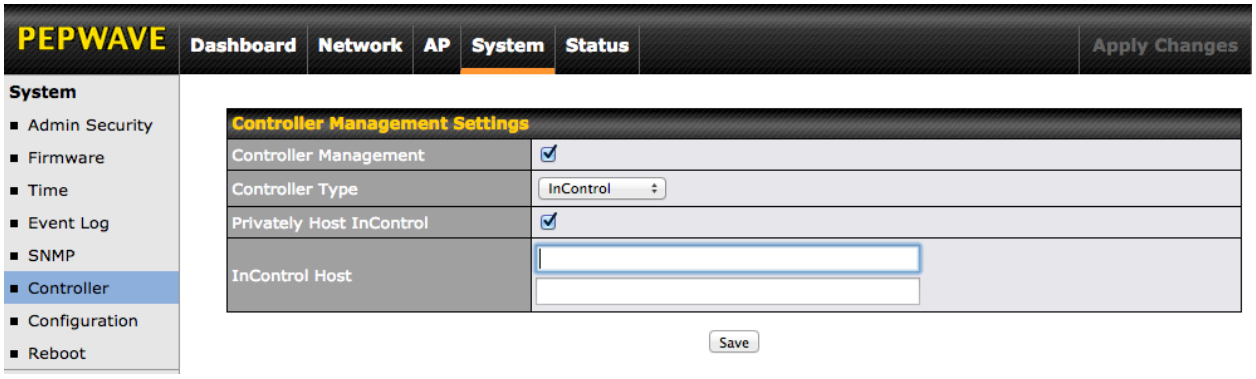
Method 1: By Configuring Devices Individually - for Internet Isolated Environments

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

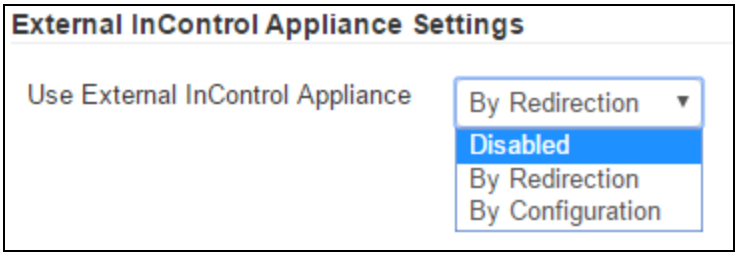


Input your InControl's IP address to the first InControl Host field.

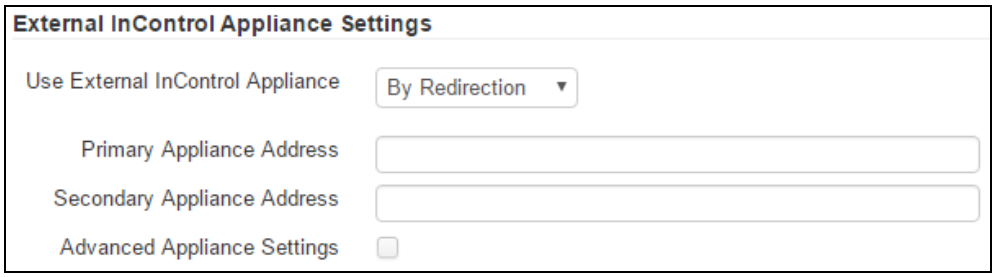
Method 2: By Configuring or Redirecting Devices from the Peplink InControl - for Internet-accessible Environments

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.



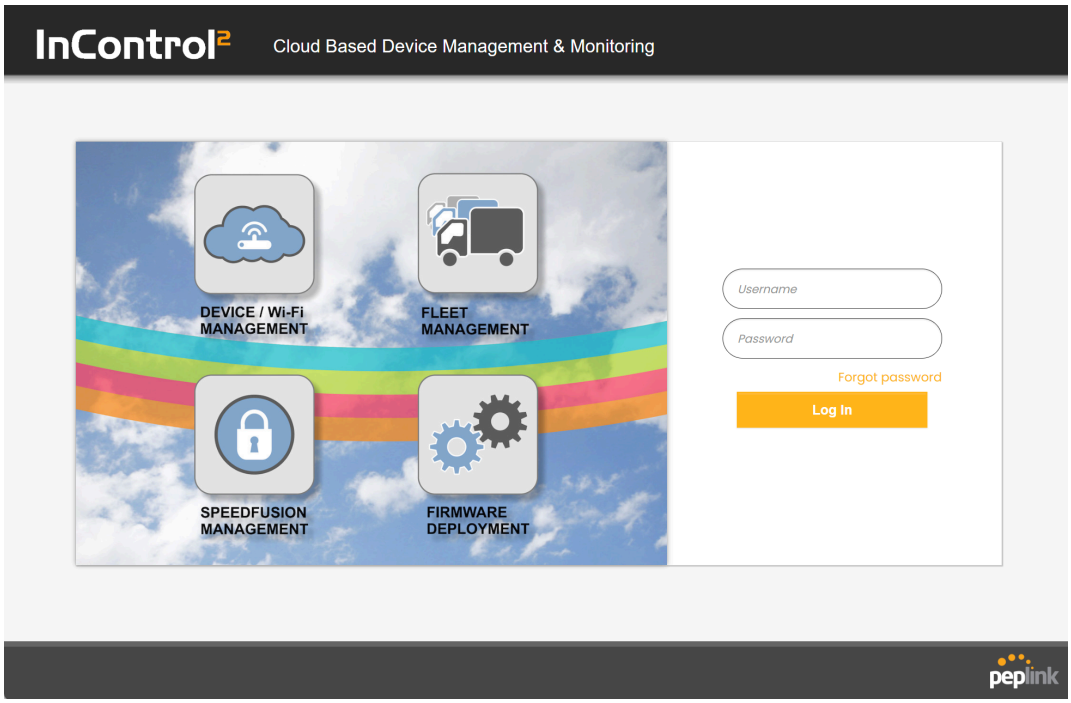
If you choose ***By Redirection***, devices will also connect to Peplink InControl first every time they start up. This option allows you to change your InControl Appliance's address easily in the future.



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

6. Logging Into InControl Appliance Website

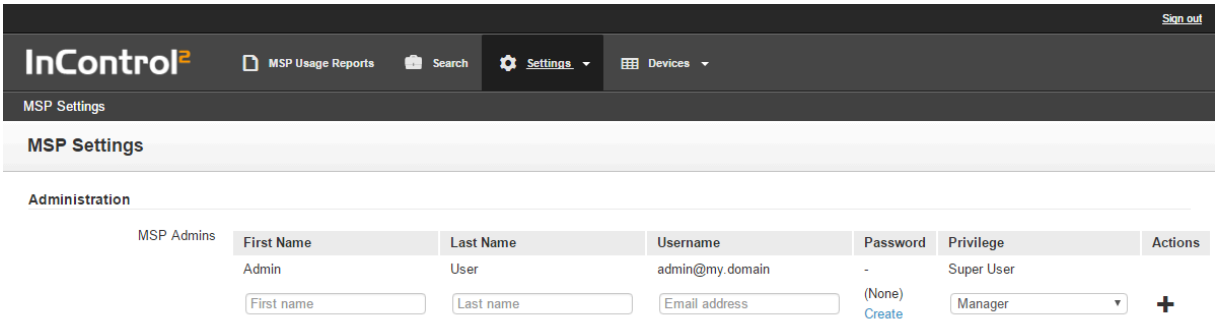


To access the InControl website, you must visit its hostname instead of its IP address. Your PC is required to resolve the hostname into the server IP address. You may add a local DNS record to your PC by editing its "`hosts`" file. It is "`%SystemRoot%\System32\drivers\etc\hosts`" for Windows or "`/etc/hosts`" 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`**.

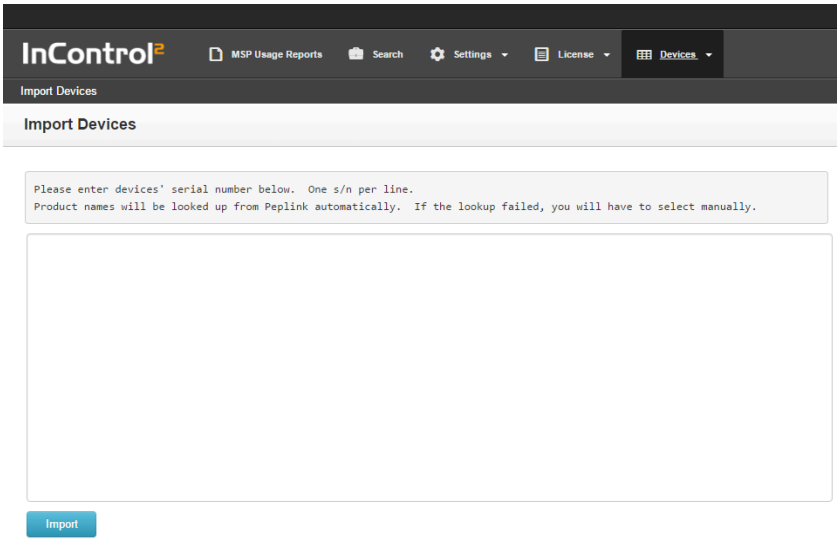
After logging into InControl, you will see an MSP (Managed Service Provider) administration page, which is for managing the InControl system. To manage MSP administrator accounts, navigate to Settings > MSP Settings.



7. Importing Devices

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

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



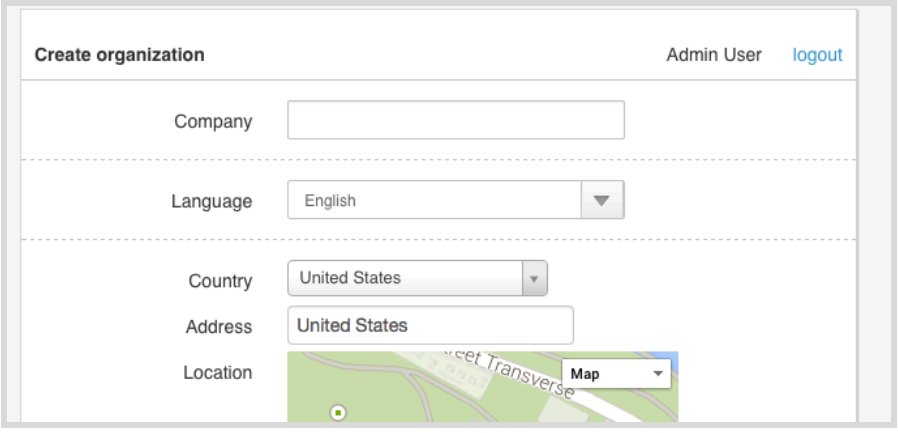
InControl Appliance will attempt to query the Peplink server what products the serial numbers are. If successful, the devices will be imported. If not, you will be prompted to select each device's product name.

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

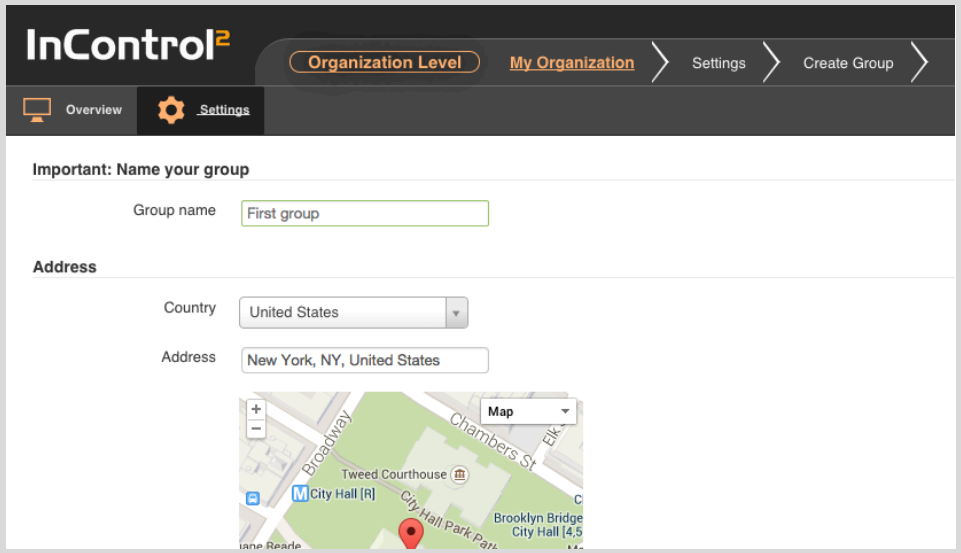
8. Creating an Organization, Group, and Adding Devices

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

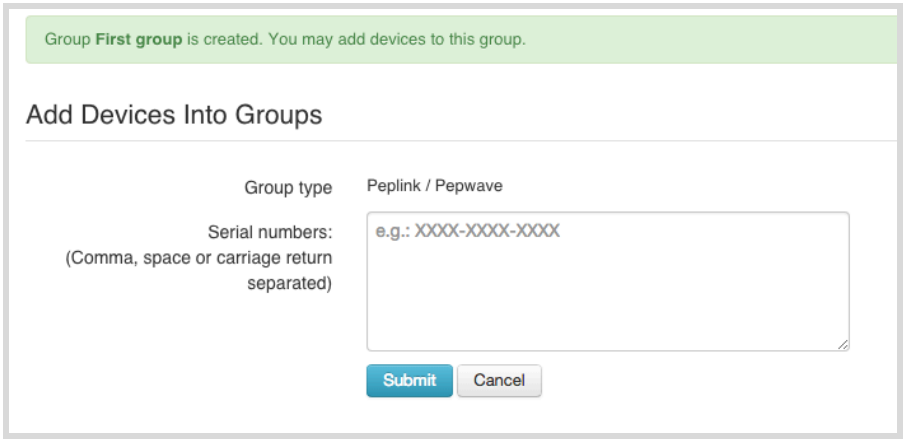
You may create more organizations by entering into an organization (e.g. "My Organization"). Then on the organization menu on the right of the screen, click "Create Organization".



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.

9. 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://{SERVER_NAME}/api/ic2-api-doc` for the API documentation and testing tool.

10. Your Firewall Settings

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 and InTouch.
	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.
	Timeserver on UDP 123	Network time sync
	DNS resolver on UDP 53	DNS resolutions

11 Data Backup

InControl Virtual Appliance provides two types of backup: Essential data backup and full database data disk backup. You can choose either one of the following methods.

11.1 Essential Data Backup

The system performs automatic daily backups of all essential data, saving them as ".tgz" files available for download from the control panel. These files are crucial for system restoration, as they contain the control panel settings, the ICVA license, and all user data stored in the database (including devices, groups, organizations, users, and configurations), but exclude bulky report data.

System restoration using these backup files must be performed by Peplink personnel.

11.2 Disk Backup of the DB System

ICVA 2.14.0 or newer provides facilities for various virtualization platforms to create a consistent backup on the database VM data disk which stores all the user data.

For InControl VM's system and data disks, and database VM's system disk, you may simply create snapshots within your hypervisor. As the disks are not frequently written, the snapshots can be reliably used for restoration without file-system or file level integrity issues.

For database VM's data disk, as it is continuously written and a lot of data is cached in the memory, special arrangement is required when creating a snapshot of it.

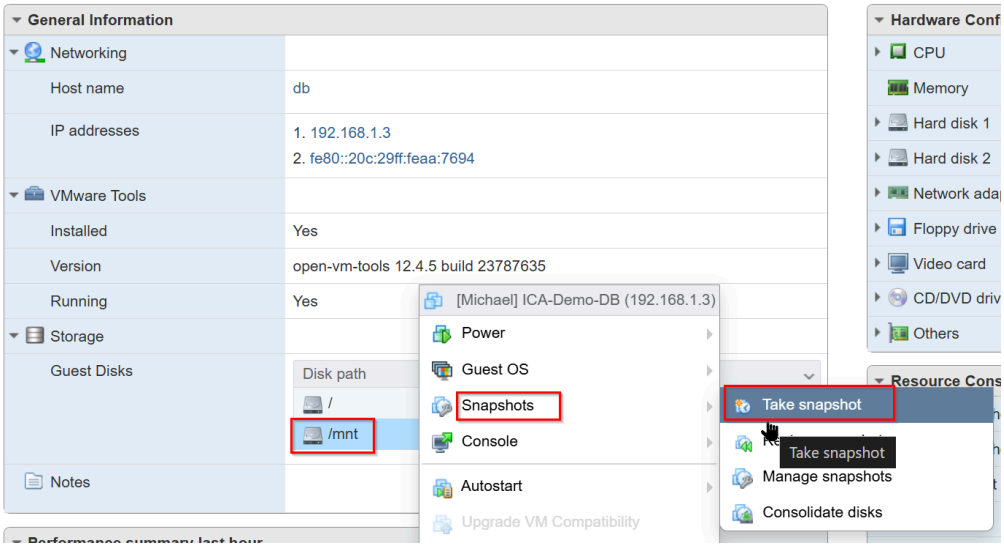
For VMware, when a snapshot creation is triggered, the DB VM can automatically write all cached data to the disk before a snapshot is actually made.

For AWS, the creation of snapshots for the database data disk must be triggered by pressing a button on the ICVA's control panel. When it is pressed, it will write the cached data to the memory and make an AWS API to create a snapshot for the database instance's data disk.

For the other hypervisors or platforms, you will also be required to implement an automation to trigger ICVA to freeze the data disk, trigger the hypervisor to create a snapshot, and trigger ICVA to thaw the disk.

11.2.1 VMware

For systems running VMware platforms, you can simply take a snapshot on the DB VM's disk "`/mnt`".



11.2.2 AWS

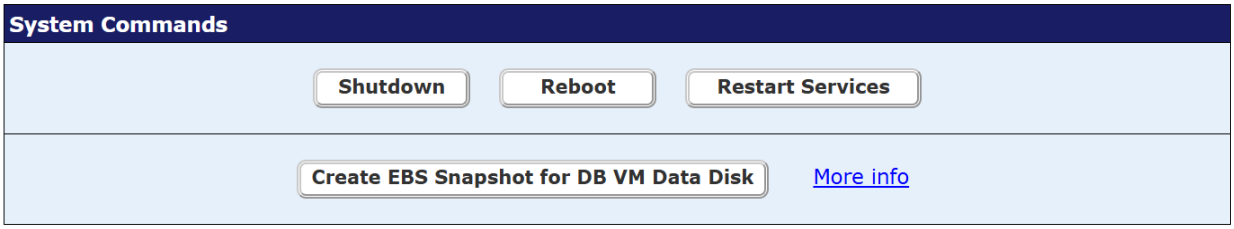
First time

On AWS, here is the procedure to create backups for the first time. (For consistency throughout this setup guide, "EC2 instances" and "EBS volumes" are called "VMs" and "disks" respectively below.

1. Navigate to **EC2** → **Instances**.
2. Select the **IC VM**.
3. Click **Actions** → **Image and templates** → **Create image**.
4. Uncheck "Reboot instance" and create the AMI.
5. Select the **DB VM**.

6. Click **Create image**.
7. During AMI creation:
    - Uncheck “Reboot instance”
    - **Remove the DB data disk** (the data volume should not be included in the AMI).
8. Create the AMI.
9. Click the “Create EBS Snapshot for DB VM Data Disk” button on ICVA's control panel to create a snapshot for the DB VM's data disk.

The “Create EBS Snapshot for DB VM Data Disk” button can be found in the System Commands section of the control panel.



Clicking it will trigger the creation of a snapshot of the DB VM’s data disk volume.

In order to make it work, please ensure the policy ***AllowSnapshotCreation*** is added to the role ***AutoDNSUpdatePeplink*** in IAM. Please refer to chapter 1.6.5 Creating a role for Route 53 DNS update and snapshot creation for details.

Create backups regularly

You may only repeat step 9 to back up the database VM’s data disk regularly, say, every day. To automate it, you might want to write a script or a scheduled task to trigger the snapshot creation by making an HTTP request to `https://{SERVER_NAME}:4443/create_snapshot_in_aws/` with the username and password passed in (e.g. for the `curl` command, use the parameter “`--user <username:password>`”).

When a DB VM’s firmware is updated or the data disk’s size has been enlarged, the database VM’s system disk will be modified. You should also follow steps 5 to 8 to create an AMI again.

You will have to follow step 1 to 4 to create an AMI for the InControl VM only when:

1. IC VM’s firmware is updated
2. Settings on the control panel have been updated.
3. Data disk size has been enlarged.

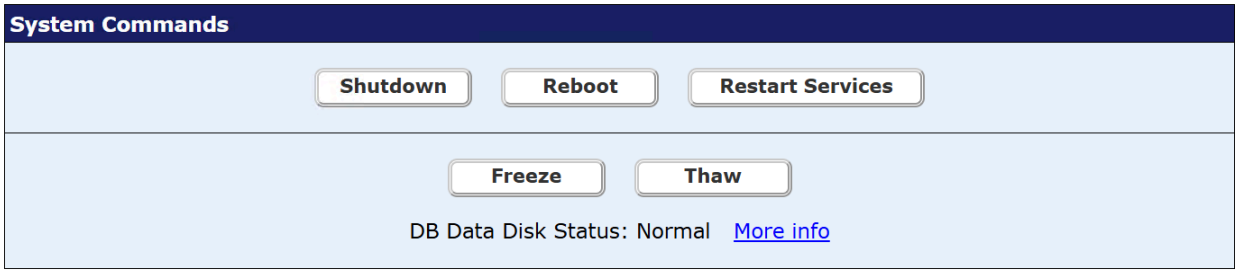
System restoration

For IC VM, simply restore it by launching the backed up AMI.

For DB VM, also restore it by launching the backed up AMI. But in the “Storage” section, click “Advanced”, click “Add a new volume”, and choose the backed up snapshot in the “Snapshot” field.

11.2.3 Hyper-V, GCE, and other virtualization platforms

For VMware, Hyper-V, GCE, and other virtualization platforms, a “Freeze” and “Thaw” buttons are displayed in the System Commands section of the control panel.



Before you trigger a snapshot or checkpoint (on Hyper-V) creation on the DB VM data disk in the virtualization platform, you may press the Freeze button to flush any data to the disk and free the disk. Note that you will be prompted to sign in again with “Basic Authentication” if you have not.

As freezing the disk will cause service interruption, the disk will automatically be thawed after 10 seconds. Or if you can also manually thaw the disk by pressing the Thaw button after you triggered a snapshot/checkpoint creation.

You may also want to write a script to automate the backup process. You can make an HTTP request to freeze the data disk, trigger a snapshot/checkbox creation, and make a second HTTP request to thaw the data disk. The URLs for freezing and thawing the DB VM data disk are

`https://{SERVER_NAME}:4443/freeze_dbvm_data/` and
`https://{SERVER_NAME}:4443/thaw_dbvm_data/`

respectively. You are required to pass the username and password in making the requests (e.g. for the `curl` command, use the parameter “`--user <username:password>`”).

12. High Availability (HA)

The InControl 2 Virtual Appliance software does not natively provide a High Availability (HA) solution. As a result, customers are expected to implement HA at the hypervisor level to ensure system uptime and resilience. This involves leveraging the built-in HA and replication features of your chosen virtualization platform to host the InControl (IC) VM and Database (DB) VM.

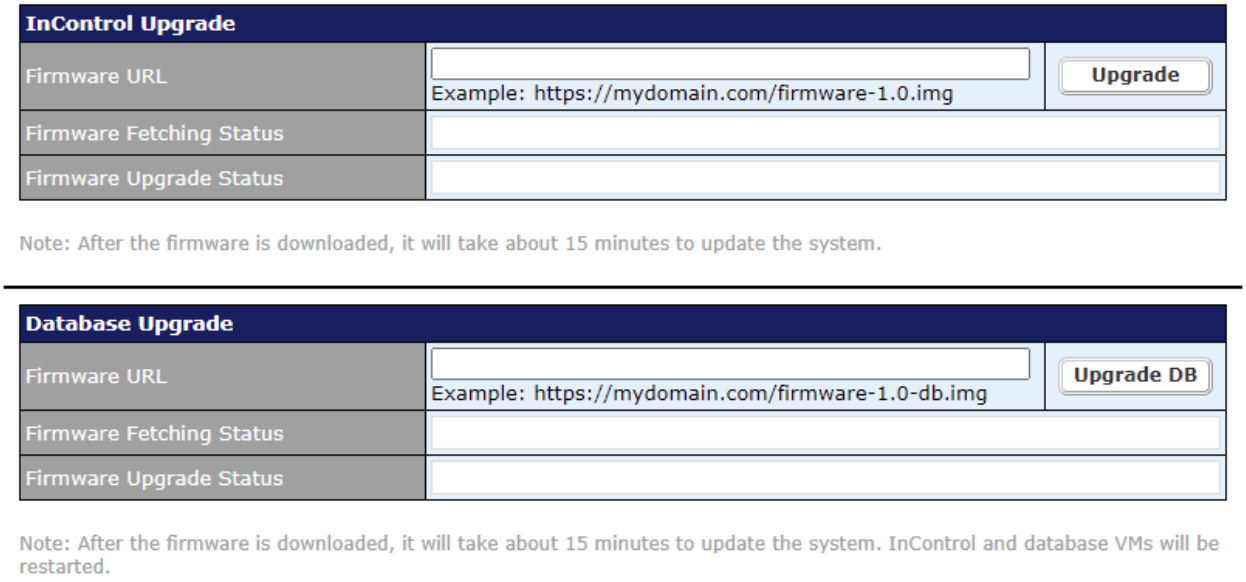
- **VMware ESXi:** Implement High Availability using **VMware High Availability (HA)** for automatic failover and **vSphere Replication** or **Storage vMotion** for data protection and migration.
- **Microsoft Hyper-V:** Utilize **Hyper-V Failover Clustering** for automatic failover and **Hyper-V Replica** for asynchronous replication of virtual machines to a secondary host.

The InControl appliance system also provides ways to create disk snapshots. You may rely on hypervisor-level automations to rebuild their system from these snapshots, allowing for rapid system restoration.

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/

IMPORTANT: Upgrade the DB VM to 20250520 or above before upgrading the IC VM to 2.14.0 or above.

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 11.1 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:

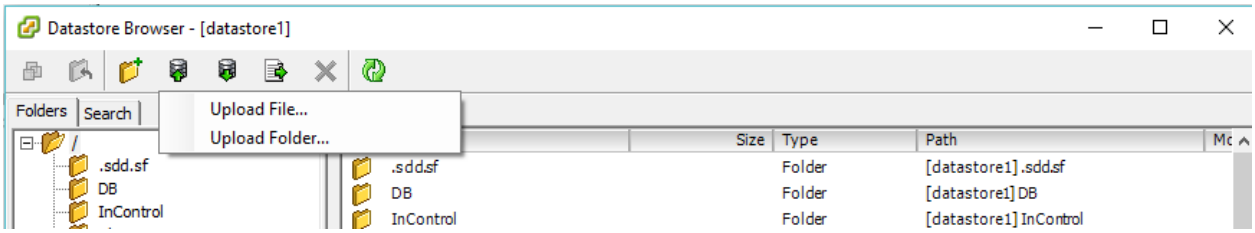
InControl-System-2.9.0.2-vmdk.tgz:

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:

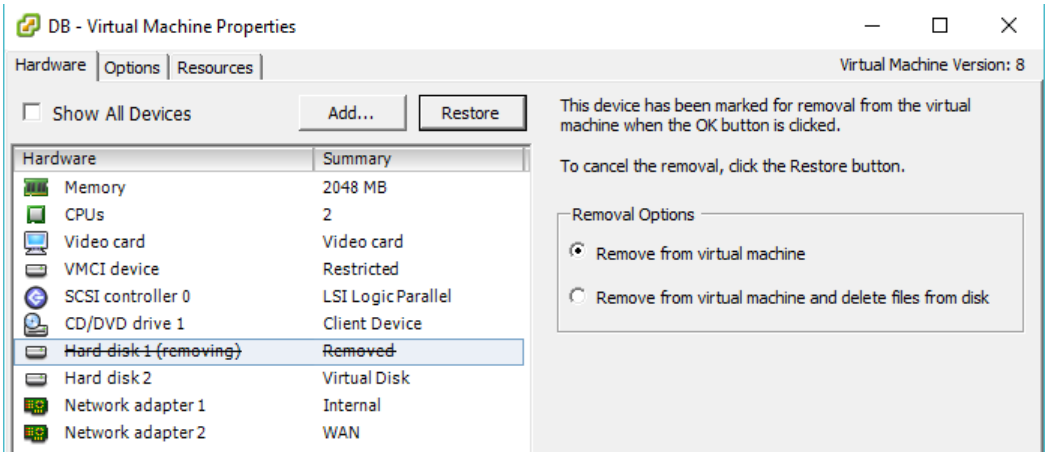
File name	Size (Bytes)
DB-System-20210323-vmdk/DB-System-20210323-flat.vmdk	26,843,545,600
DB-System-20210323-vmdk/DB-System-20210323.vmdk	660

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.



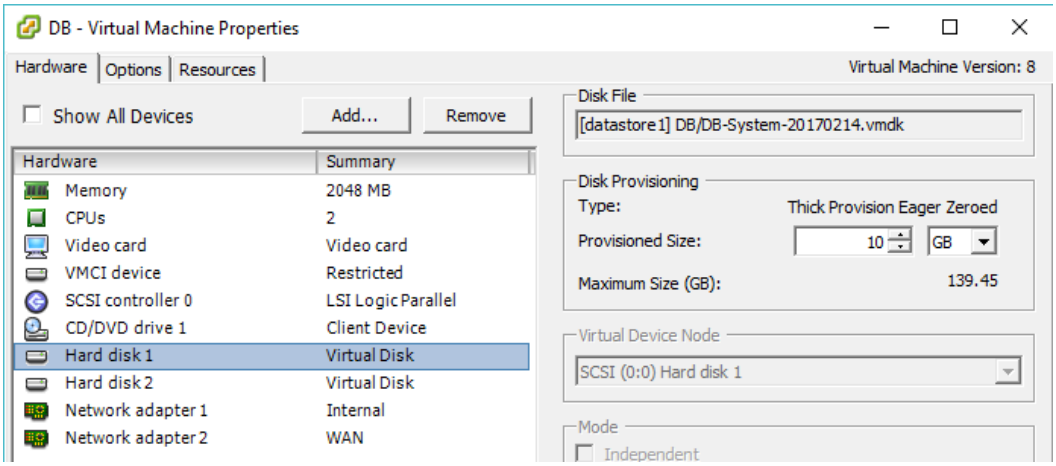
Step 4. Restart VMs in the following order:

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"

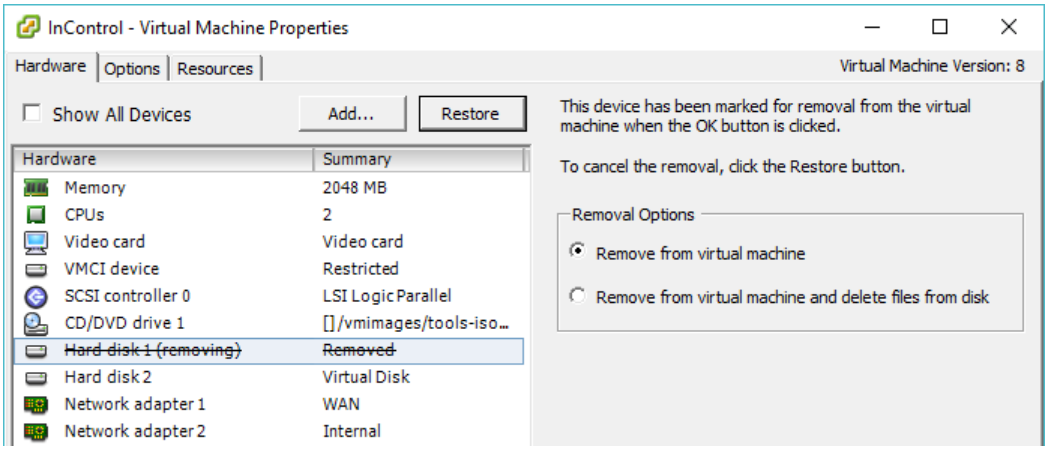


4. Open DB VM Properties again
    - Select 'Add…" > "Existing virtual disk…" > Browse and select the disk file "DB-System-20210323.vmdk"

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

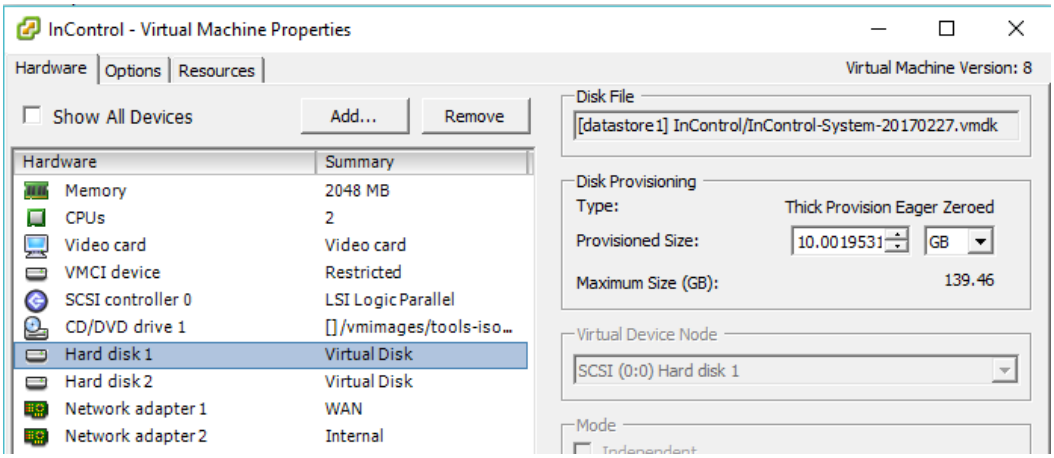


5. Start DB VM
6. Open InControl VM Properties
   - Identify and select the system hard disk (usually "Hard disk 1")
   - Select the "Remove from virtual machine" radio button (without deleting it)
   - Press "OK"



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

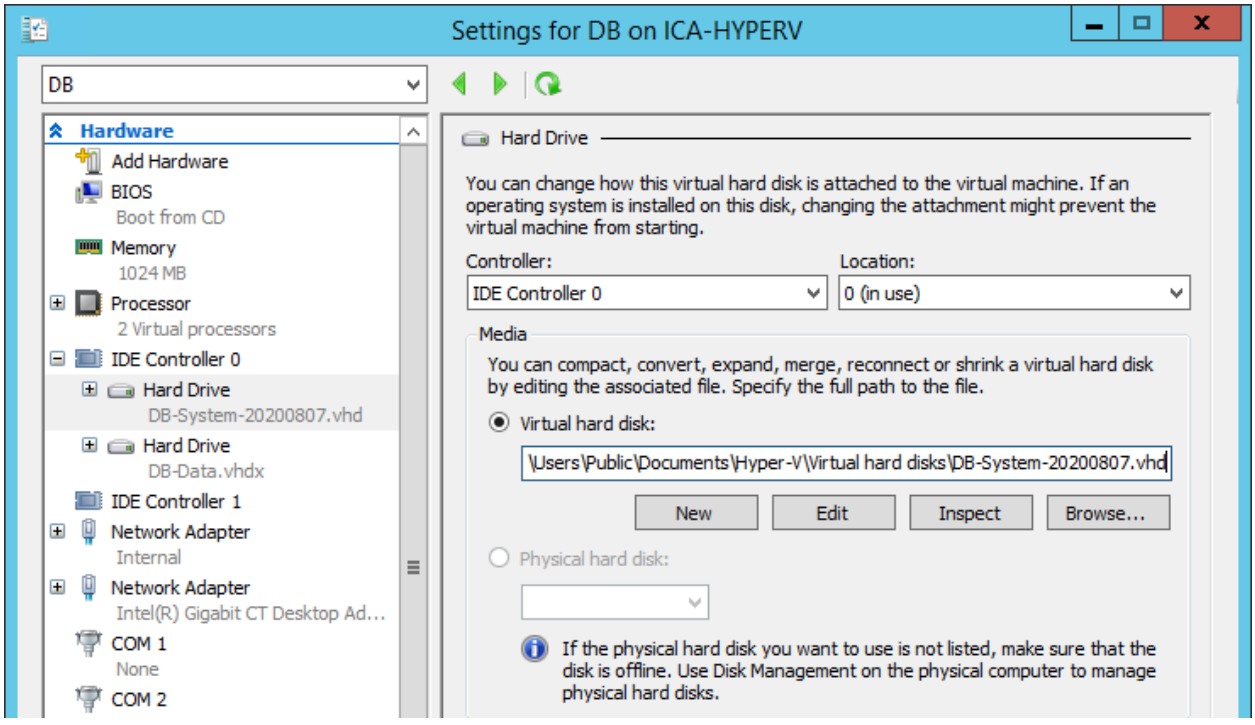
Step 1. Download the Virtual Appliance 2.9.0.2 and Database Server 202103223 image files in `.vhdx` format from https://www.peplink.com/support/incontrol-appliance-images-downloads/

Decompress the .vhdx.gz files into .vhdx files. The .vhdx file names and sizes are as follows:

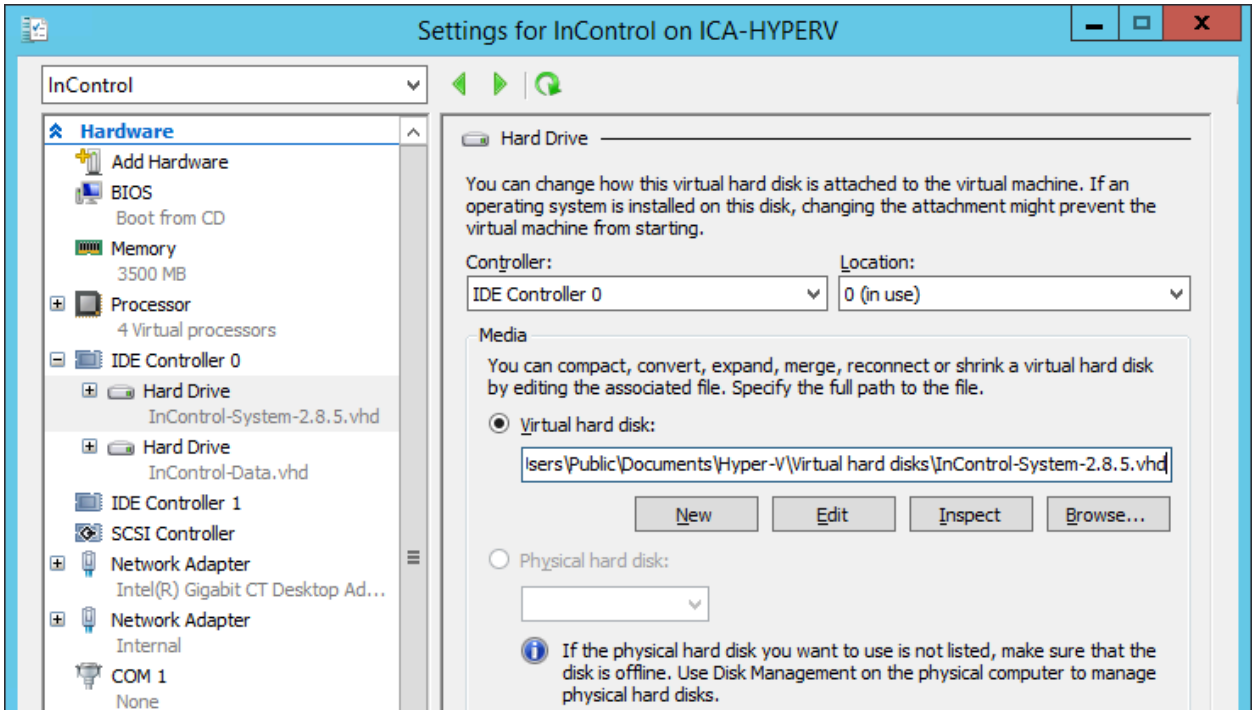
File name	Size (Bytes)
InControl-System-2.9.0.2.vhdx	25,035,800,576
DB-System-20210323.vhdx	25,035,800,576

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. Release Notes

Release notes for 2.14.2.7

- Mitigated the Dirty Frag (CVE-2026-43284, CVE-2026-43500) and Fragnesia (CVE-2026-46300) vulnerabilities.

Release notes for 2.14.2.6

- Mitigated the Copy Fail vulnerability (CVE-2026-31431).

Release notes for 2.14.2.5

- When the web server certificate and private key are uploaded to the control panel but they do not correspond to each other, an error message will now be displayed.
- Fixed: error in saving the web server certificate on the control panel.
- Fixed: “Sign-in with Open ID” did not work in some circumstances.

Release notes for 2.14.2.4

- Enhanced the security of the control panel.
- Fixed: errors may be generated when the system is under heavier load in some circumstances.
- Fixed: in the MSP-level system usage report, the figures in the organization usage report were not updated. An error email was sent to the system administrators.

Release notes for 2.14.2.2

- Fixed: a data synchronization with Peplink InControl never completes.
- Fixed: when a device was upgraded to or downgraded from firmware version 8.5.4, the visibility of the Remote Web Admin and InTouch Settings menus was incorrectly managed when the high security mode was set for Remote Web Admin and InTouch.

Release notes for 2.14.2.1

- Fixed: data synchronization with Peplink InControl failed silently.
- Fixed a typo on the control panel.

Release notes for 2.14.2

- **Breaking change:** The web server certificate update page (`https://{SERVER_NAME}/cert.cgi`) and the sample certificate update shell script (`upload_cert.sh`) have been updated.
- Provided a control panel option to select an even higher security level when establishing Remote Web Admin and InTouch tunnels with devices running firmware 8.5.4 or above.
- Enhanced the security of Remote Web Admin and InTouch secure tunnels (in both high compatibility and security modes).
- ICVA backup files are now encrypted.
- Added a Remote Web Admin and InTouch support option in the control panel.
- Fixed snapshot creation issues on VMware.
- On AWS, more metrics are reported to CloudWatch.
- Added LLDP configuration. See group-level Network Settings menu. With LLDP enabled, on the Clients pages, the name of the Ethernet port that a client is attached to will be displayed.
- Added group-level Serial-port-based InTouch configuration, serial port events, and notifications.
- Group-level Radio Settings
  - Added Wi-Fi 7 (802.11be, 6GHz) support.
  - Added assisted roaming settings for guiding Wi-Fi clients to stronger signal APs for improved connectivity.
  - Revamped Wi-Fi channel scanning schedule settings.
  - Added “Disconnect Clients” option.
- SpeedFusion configuration > Advanced Link Settings: converted tunnel and subtunnel settings from one single page to tabs. Search is more granular.
- Added Peplink eSIM data plan management.
- In the device listing CSV file, added SpeedFusion Connect and Peplink eSIM fields.
- In the maps of Device Details, and Group and Organization overview pages, a location search UI control is added.
- Devices can be added by a CSV file.
- In group-level Usage Reports, added a device count column.
- In Group Settings > Advanced Settings, the group-level Operation Log page can be hidden from group administrators and/or viewers.
- Added a note field to every Site Survey report.
- Added “Custom Route Advertising” settings to “Route Advertising”.
- Added a webhook which will be triggered when a Site Survey or Connection Test report is created.
- Captive portal

    - Added a guest session console for guests to check their data or time usage or status.
    - Added an inactive timeout setting.
- Added API endpoints for provisioning serial-port-based InTouch profiles without needing the devices to appear online first.
- Added API endpoints for generating captive portal tokens programmatically.
- Added a name field to MAC addresses in grouped MAC address profiles.
- In Device System Management, added Time Sync settings.
- Added Auto Airplane Mode setting in Geofencing for groups containing Peplink MBX. When a selected device exceeds a certain speed or altitude, its cellular WANs will automatically be disabled.
- In connection test notification emails, a link to the test profile page is added to the connection test result.
- When Email Notification is disabled, the subscription settings are now preserved and can be restored when the notification option is re-enabled.

Release notes for DB-20260224

Here are the changes since DB-20250520:

- On AWS, various metrics are posted to CloudWatch. E.g. CPU Utilization, Swap
- Fixed snapshot creation issues on VMware.

Release notes for 2.14.1.3

- **Breaking change**: added a new set of username and password for downloading the ICVA backups. The original username and password are no longer accepted. See the “Backup Download Password” field on the control panel.
- Improved the reliability in generating ICVA diagnostic reports.
- Added an option in the control panel to disable Remote Web Admin and InTouch.
- Fixed an AWS EC2 snapshot creation problem for some EC2 instance types.
- Fixed a SpeedFusion VPN configuration bug. If one or more devices have never been online, the hub device list failed to load.

Release notes for 2.14.1.2

- A problem that occurred during system startup has been resolved, which previously affected the system if the password for web management, FTP, or SMTP included an ampersand (&).
- Resolved the two-factor authentication email code issue, which began in version 2.14.0.

- On AWS, various metrics are posted to CloudWatch. E.g. CPU Utilization, Swap
- Fixed: the number of SFTP connections to the archive server kept increasing.

Release notes for DB-20251229

Here are the changes since DB-20250520:

- Fixed the MongoBleed (CVE-2025-14847) vulnerability.
- Fixed: failed to create EBS snapshots in AWS.

Release notes for 2.14.1.1

Please read the breaking change in 2.14.1 below.

What's new

- Enhanced memory allocations to the core and API services. Improved system stability.
- Added API for querying a device's details by a serial number.
- Fixed: remote web admin did not work for some devices for ICVA with a legacy license.
- Improved support for the latest Peplink SD Switches.
- Added the data disk's usage information to the SNMP OID `.1.3.6.1.4.1.2021.9`.

Release notes for 2.14.1

Breaking change

Since InControl 2.14.1, the system utilizes the OpenMapTiles API for map loading, replacing the previously used Google Maps JavaScript API. This change allows map tiles to be sourced from various providers, including Google Maps and HERE Maps.

Consequently, if you are providing a Google Maps API key to display maps, you must now enable the "Map Tiles API" within the Google Cloud Console. This is a mandatory step to ensure Google Maps loads correctly in InControl 2.14.1 and all subsequent versions.

What's new

- Added a token-based API for looking up organization, group, and device ID of a serial number.
- Added HERE Map support. Added option to choose the API service to use for displaying the maps, satellite view, and geocoding.
- Supported WAN configurations on major settings.

- Device System Management: added an option to turn Bluetooth off on all devices.
- Added "All" VLAN selection to trunk ports.
- Dynamic location source is now indicated (e.g. GPS, Starlink, Google Maps Geolocation API, etc.)
- HTTP/S Notifications (Webhook): notification to be received can now be selected.
- Outbound Policy > Weighted Balance: added SpeedFusion VPN connection support.
- InTouch Settings can now be copied to another device in the same organization or group.
- MSP, organization, and group-level device list: devices can be selected by providing a serial number list.
- Captive portal: added an option for preventing immediate closure of the captive portal after signing in on Android devices. (34868, 34867)
- User organizations page: search result is now bookmarkable.
- Device Details > Starlink status: an indicator is displayed when the Starlink service quota exceeded.
- Notification settings: added info tip to every notification type.
- In Wi-Fi radio settings, removed the "Auto" channel width selection.
- Added an API endpoint for changing device tags one in one operation. (`device_hashtag`)
- Site survey: add a Download as CSV link.
- WAN usage data is no longer captured from access points in bridge mode.
- Organization user roles are now hidden from group-level settings.
- Wi-Fi SSID settings: the MFP option is now always enabled in WPA3-Enterprise mode.
- Check cellular module support before downgrading device firmware.
- Captive portals:
  - Guest account mode: expired guest accounts can now be reactivated.
  - Guest account mode: all columns and expired users are now included in the guest account CSV file.
  - Supported right-to-left languages.
- In doing eSIM discovery, the number of profile retrieved and installed are now displayed.

Release notes for 2.14.0.3

What's new

- Fixed an issue with the SpeedFusion usage reports.
- Fixed a potential data synchronization failure error with the public InControl if the system is managing many devices.
- Fixed an hourly report generation error.
- Updated Content Security Policy.

Release notes for 2.14.0.2

What's new

- Fixed: in captive portal profiles, if a landing page is configured to an address outside the InControl, guests will not be able to reach the landing page during sign-ins. They will be stuck on the "signing in" screen.
- TLSv1.3 is enabled for web requests.

Release notes for 2.14.0.1

What's new

- Fixed: boot up process stalls in some situations.
- Fixed: WAN connection history shows up events only.
- InTouch: added support of the HTTP request method "PATCH".

Release notes for 2.14.0

IMPORTANT: it requires DB VM version DB-20250520 or above. It is preferred to upgrade the DB VM before upgrading the IC VM.

What's new

- The OS is upgraded to Ubuntu 24.04.
- Added support of creating data disk backups for the DB VM data disk. See chapter 11 Data Backup for details.
- Added an MSP-level API to look up the organization ID of multiple serial numbers. See the API documentation at `https://{SERVER_NAME}/api/ic2-api-doc/`.
- Supported sending emails in SMTP TLS mode.
- Send MSP and organization level operation log to a syslog server.
- If IP-based InTouch is enabled, Remote Web Admin URLs will be changed to the format "`https://{SN}-ic.{SERVER_NAME}/`". This change fixes a compatibility issue with POTS Adapter web admin.
- Added Starlink data pools.
- Added bandwidth throttling in SIM pools.
- Added site survey on cellular networks.
- Added a new device online state "Appeared Online Today" for devices without a care plan.
- Added organization-wide grouped networks.

- Device Details:
  - Included any system messages displayed on devices' web admin.
  - When the "Find My Peplink" option is enabled, the device's web admin server SSL will automatically be managed too.
- Device list: added a "Hide expiration notices" checkbox.
- "Grouped MAC Addresses" replaces "Access Control List". Added "Ingress ACL" and "Port-based 802.1x Authentication" configurations.
- SpeedFusion VPN configuration:
  - Added detailed loading status, for organizations with many devices.
  - Greatly reduce saving time when profiles contain large numbers of devices and/or connections.
  - Added "TCP Traffic Optimization" setting.
- SSID profile > "Last 8 octets of LAN MAC as key": added an uppercase option.
- Added "Colombia" to the Operating Country field in Wi-Fi Radio Settings.
- Administrators can temporarily disable a user from accessing their organization or group. MSP Administrators can disable a user from accessing the system.
- Notifications: Added POTS Adapter and DHCP Server events. Added Power Supply Change option to MAX Adapter.
- Web-based InTouch profiles: added Username and Password fields for HTTP Basic authentication.
- WAN Quality Reports: added a "Throughput" option to include per-minute bandwidth figures on the chart.
- Device System Management:
  - A random web admin password can be regenerated automatically every month.
  - Added "Timeout" and "Source Network Address" for RADIUS and TACACS+ settings.
  - Added additional SNMP Trap settings.
- Docker scripts are now run when devices report online.
- Added the Actions menu item "Ignore Starlink Obstruction Outage" on the device management screen.
- FusionHub licenses: the "Auto Renew" buttons' states will be persistent and not be auto-disabled after the licenses' hardware identifiers are renewed.
- Firewall rule set > Content Blocking: added a logging option.
- Added an "IGMP Fast Leave" option to the latest SD Switches' port settings screens.
- Captive portal:
  - E-mail access mode: outgoing emails can optionally be sent to a "cc" address.
  - Supported the latest Google Analytics ID format.
  - Prevented the pop-up browser from closing immediately on Android devices.
- External captive portal: added the "Authentication Protocol", "Popup Handling", and "Logout Hostname" settings to profiles.

- Added Japanese localization.
- Fixed: SIM data usage of synergy controllers is now ignored from SIM pools.
- Changed: the "Top Client Device Manufacturers" table in Device/Wi-Fi Reports is only available for the last 31 days

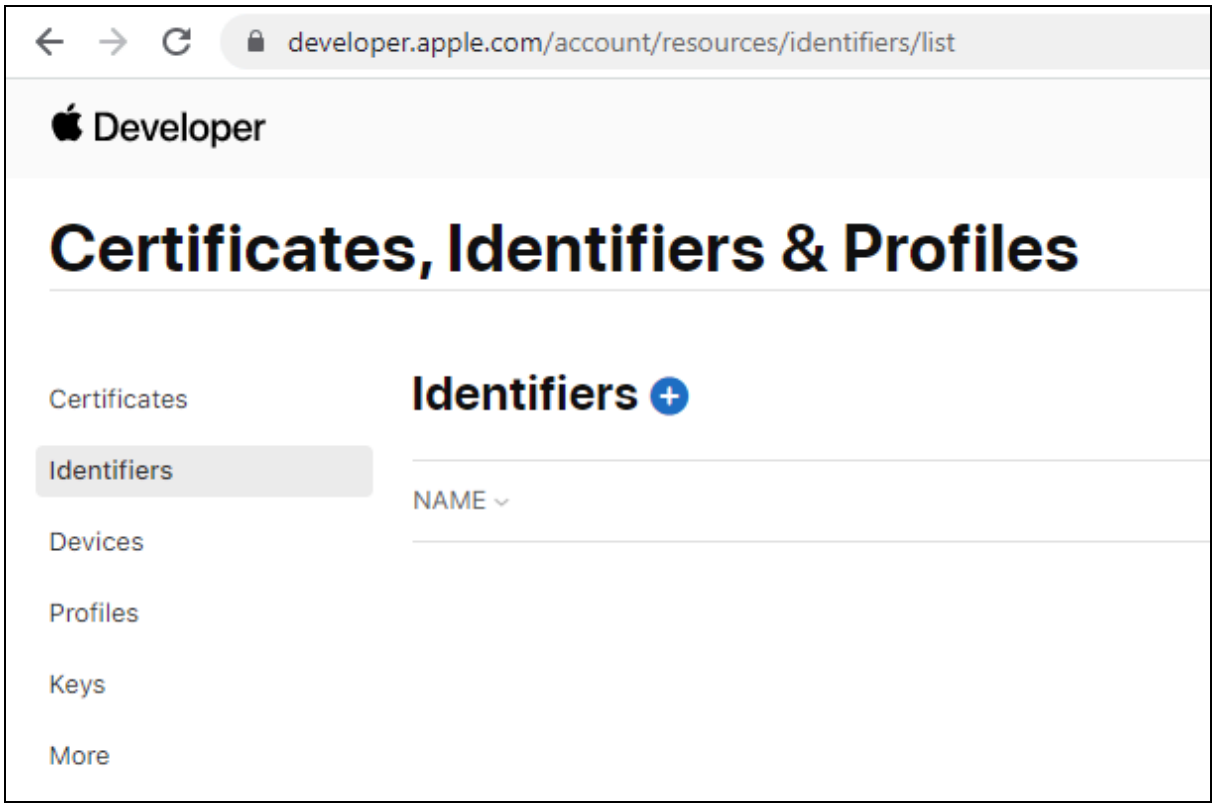
Release notes for DB-20250520

Here are the changes since DB-20240410:

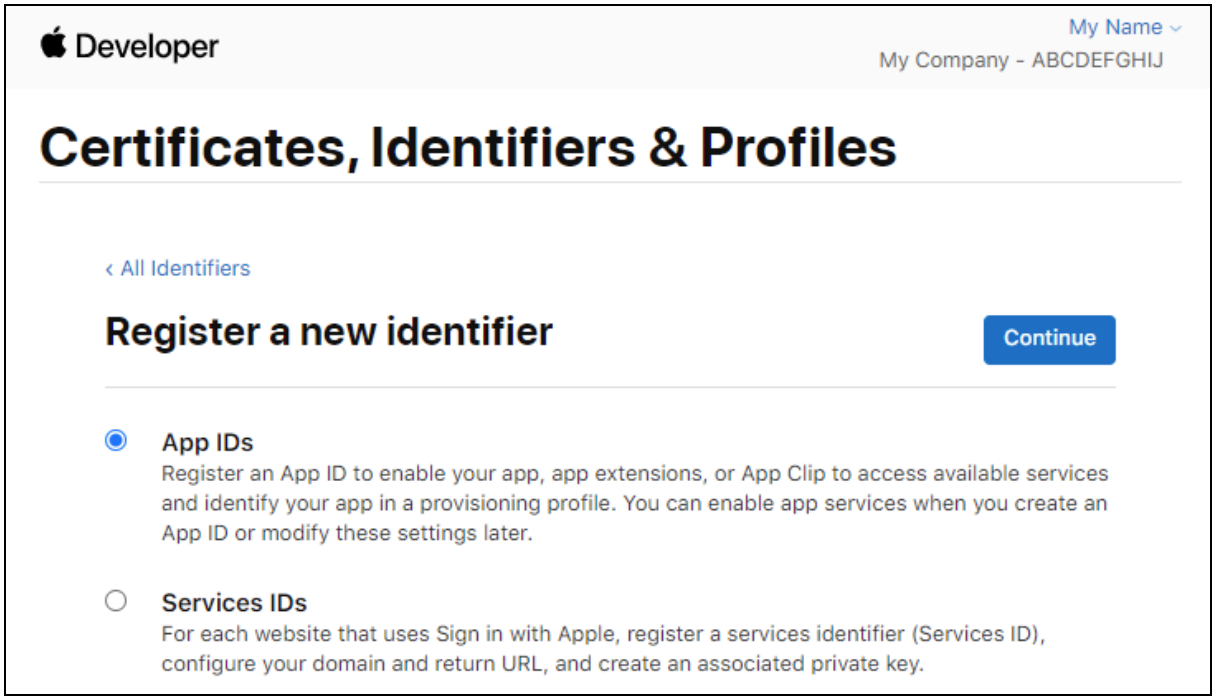
- The OS is upgraded to Ubuntu 24.04.
- Supported freezing and thawing the database VM data disk through the control panel or API. See chapter 11 Data Backup for details.

Appendix 1: Procedure for preparing the data for setting up "Sign in with Apple".

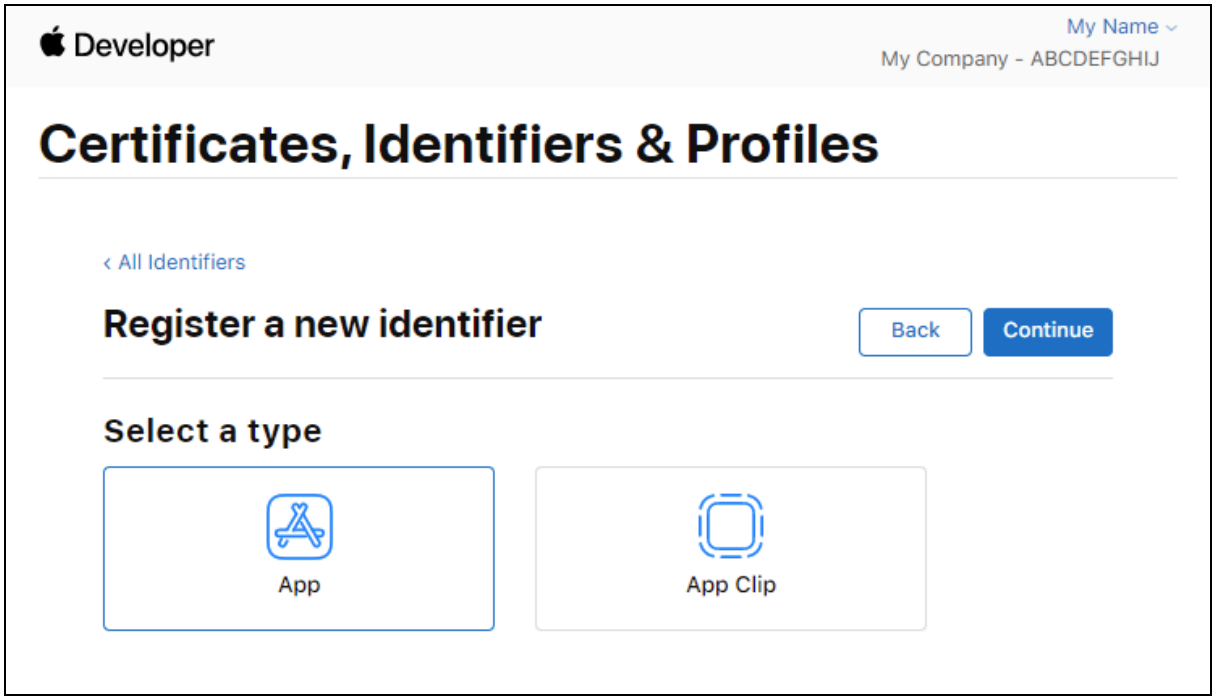
Login to https://developer.apple.com/account/resources/identifiers/list with your Apple Developer account.



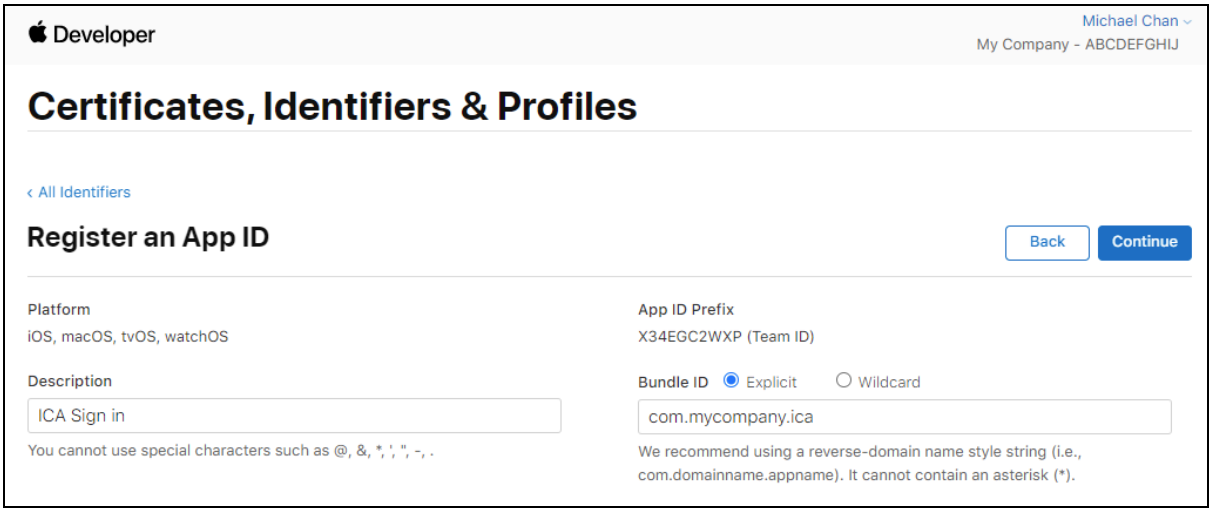
Press the "+" icon.



Select “App IDs”. Press Continue

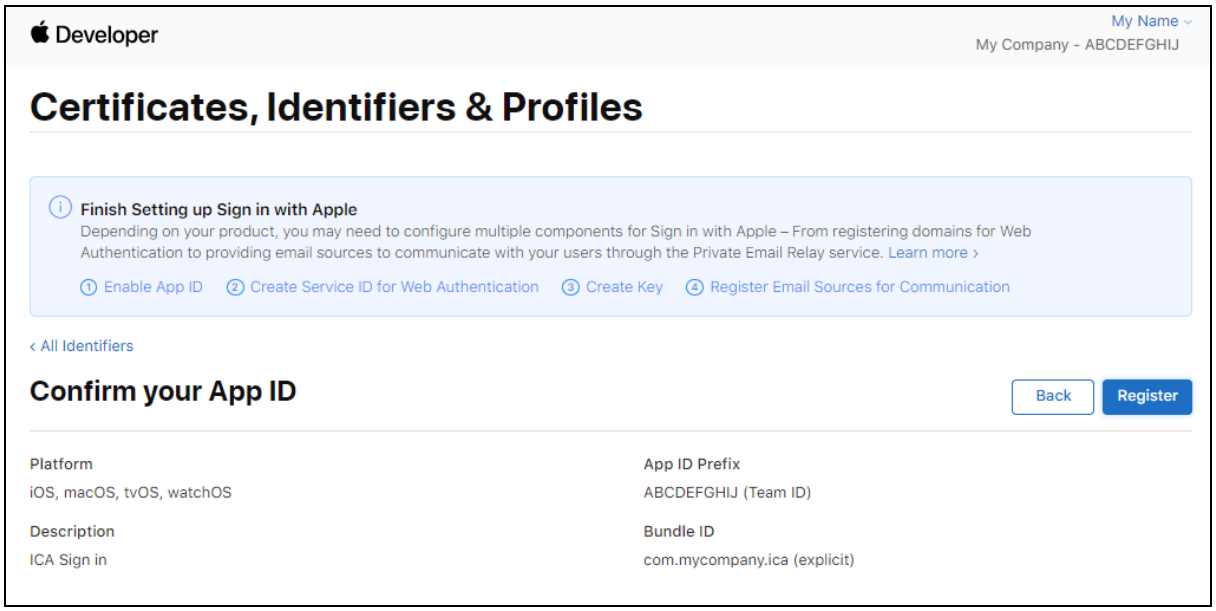


Select “App” and press Continue.

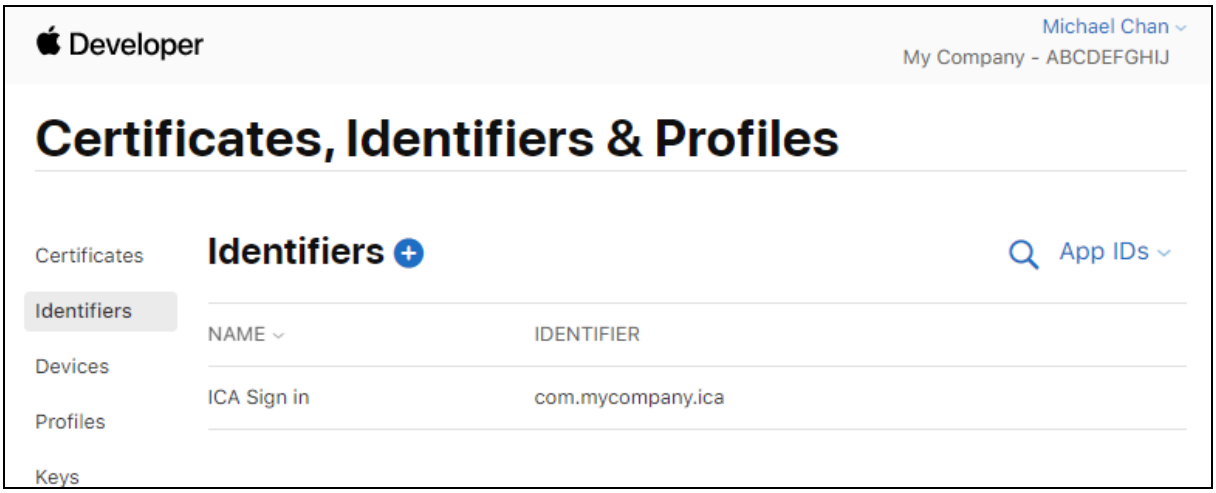


Enter “ICA Sign in” in the Description box. Choose “Explicit” and input a Bundle ID. Replace “com.mycompany.ica” with an identifier you decide.

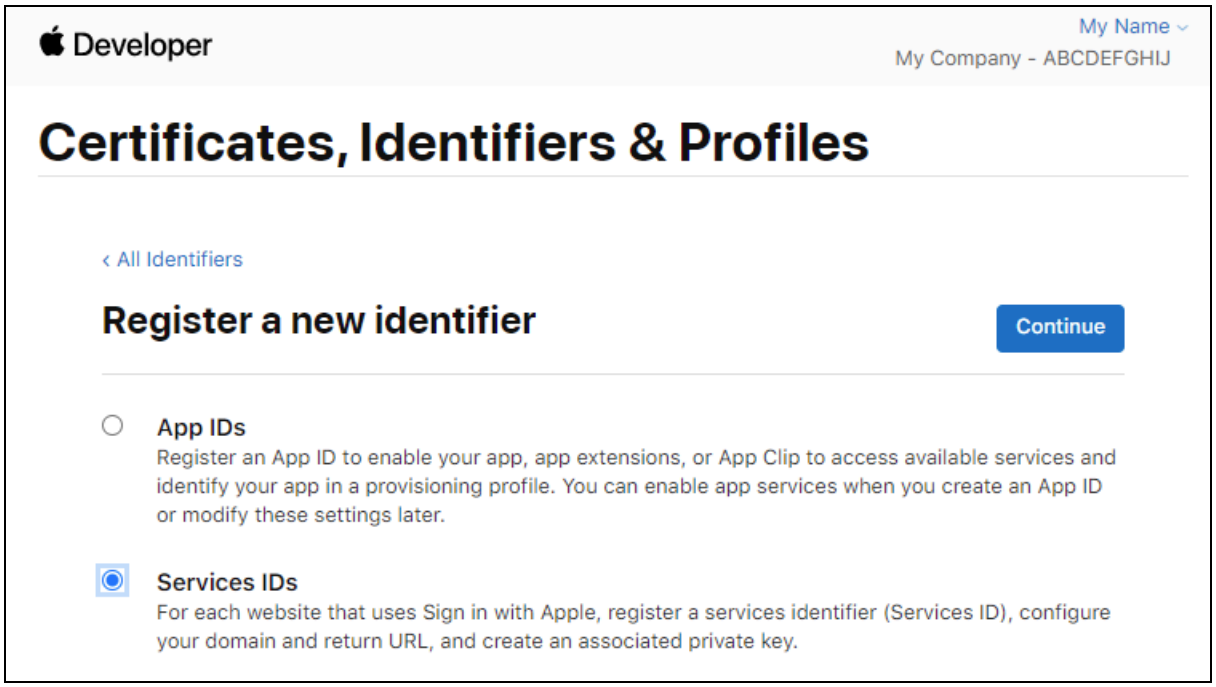
Scroll down and select “Sign in with Apple”. Press Continue



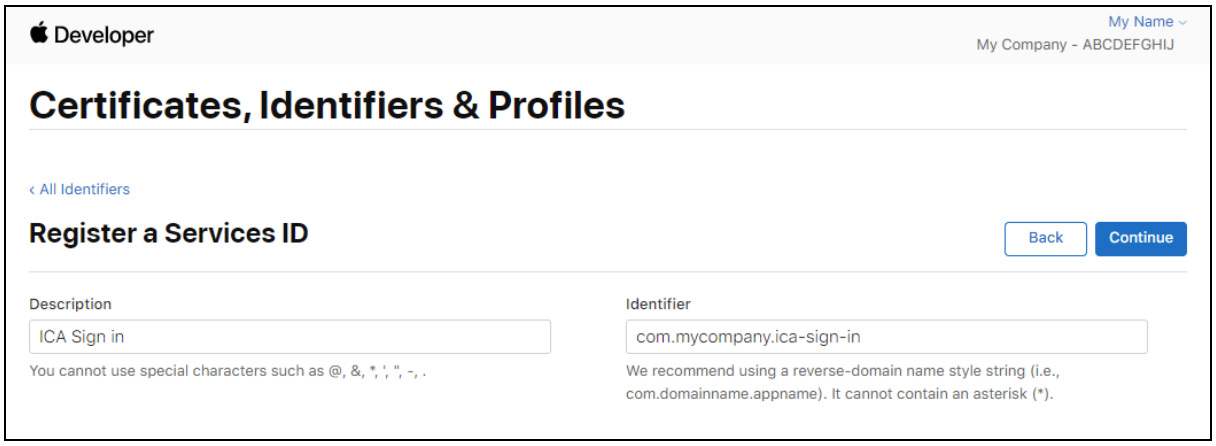
Press Register.



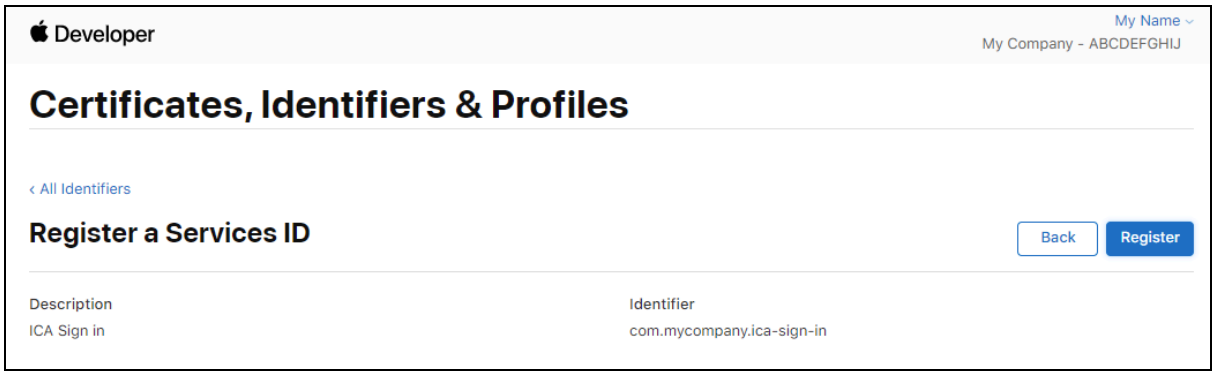
Press the “+” icon again.



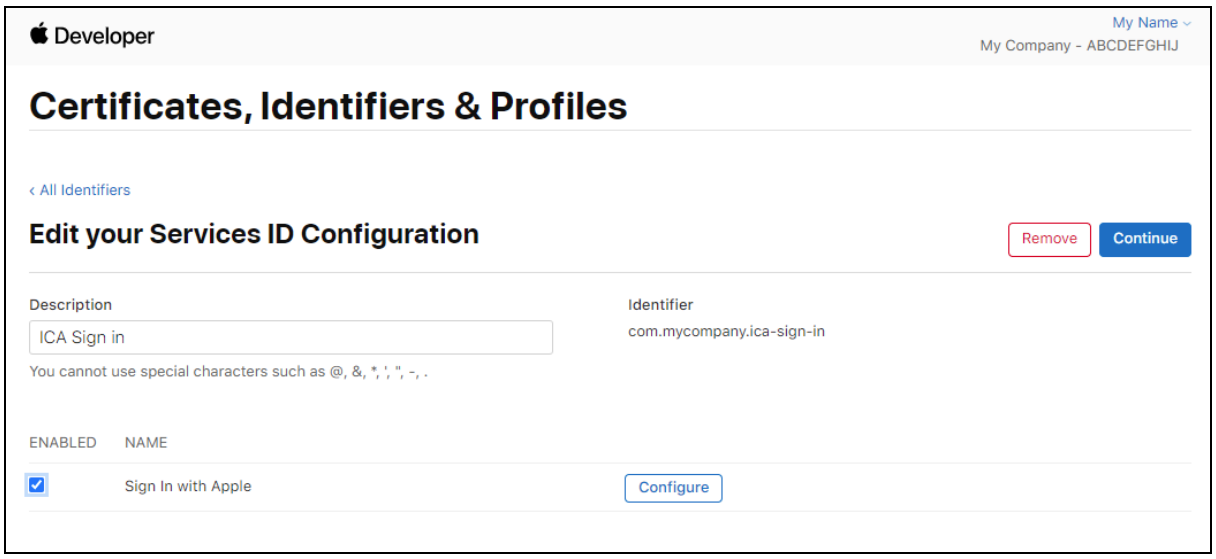
Select “Services IDs” and press Continue.



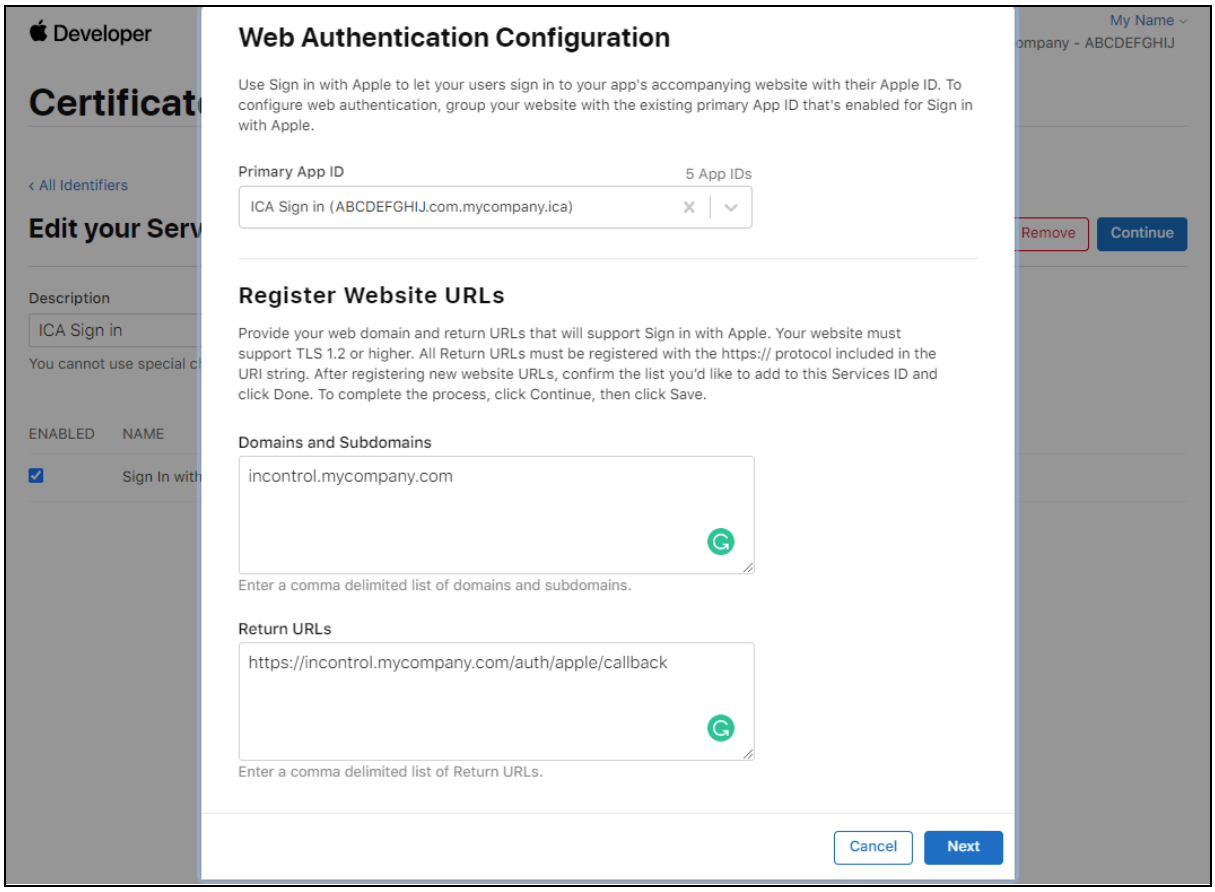
Replace “`com.mycompany.ica-sign-in`” with an identifier you decide. This is your “**Service ID**”. Record this down.



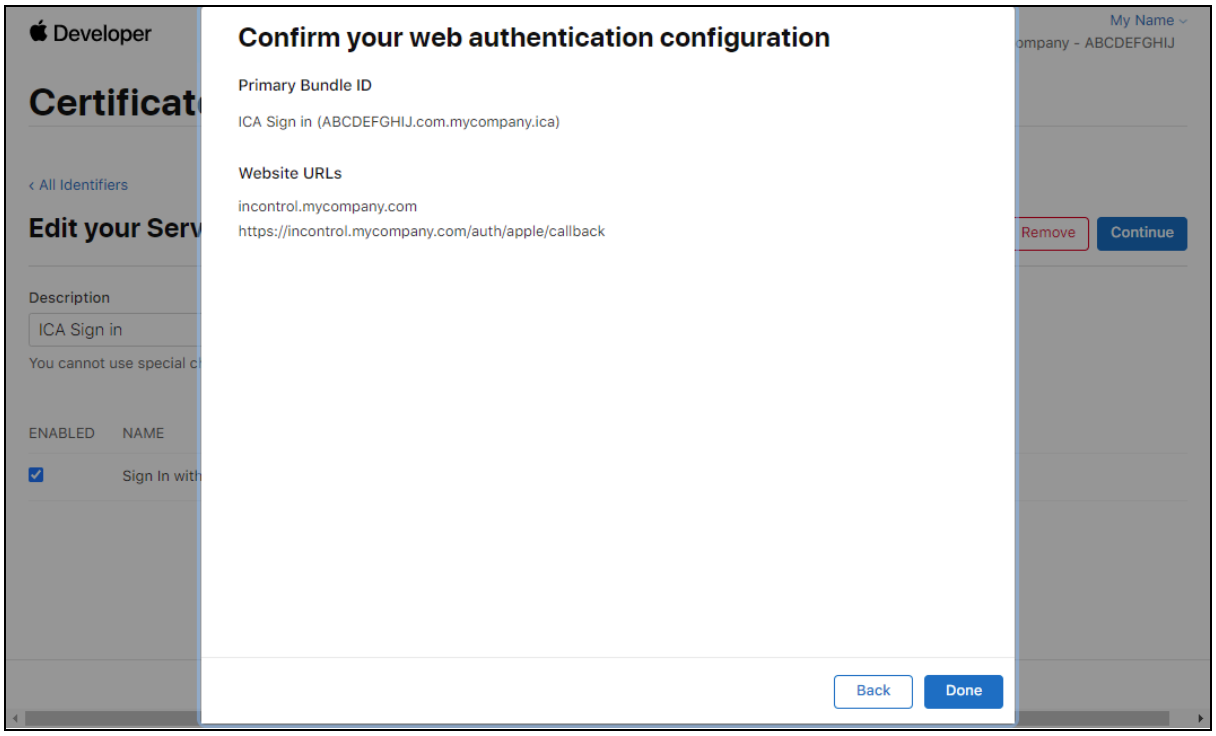
Press Register.



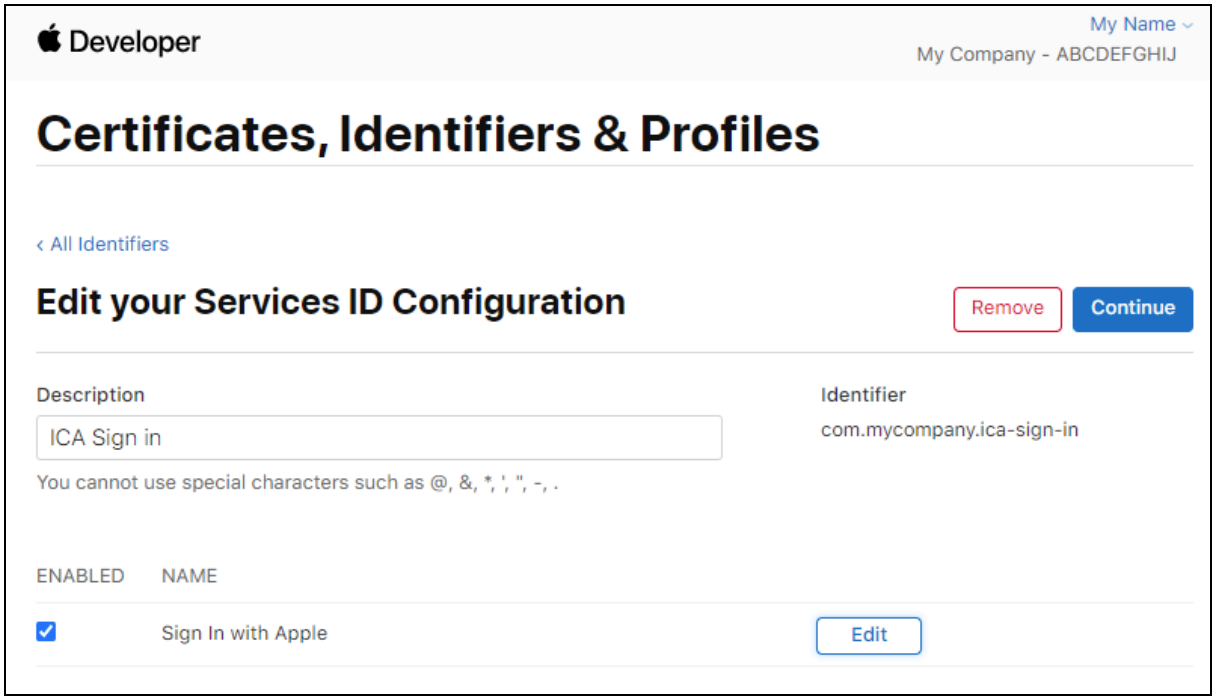
Press Configure.



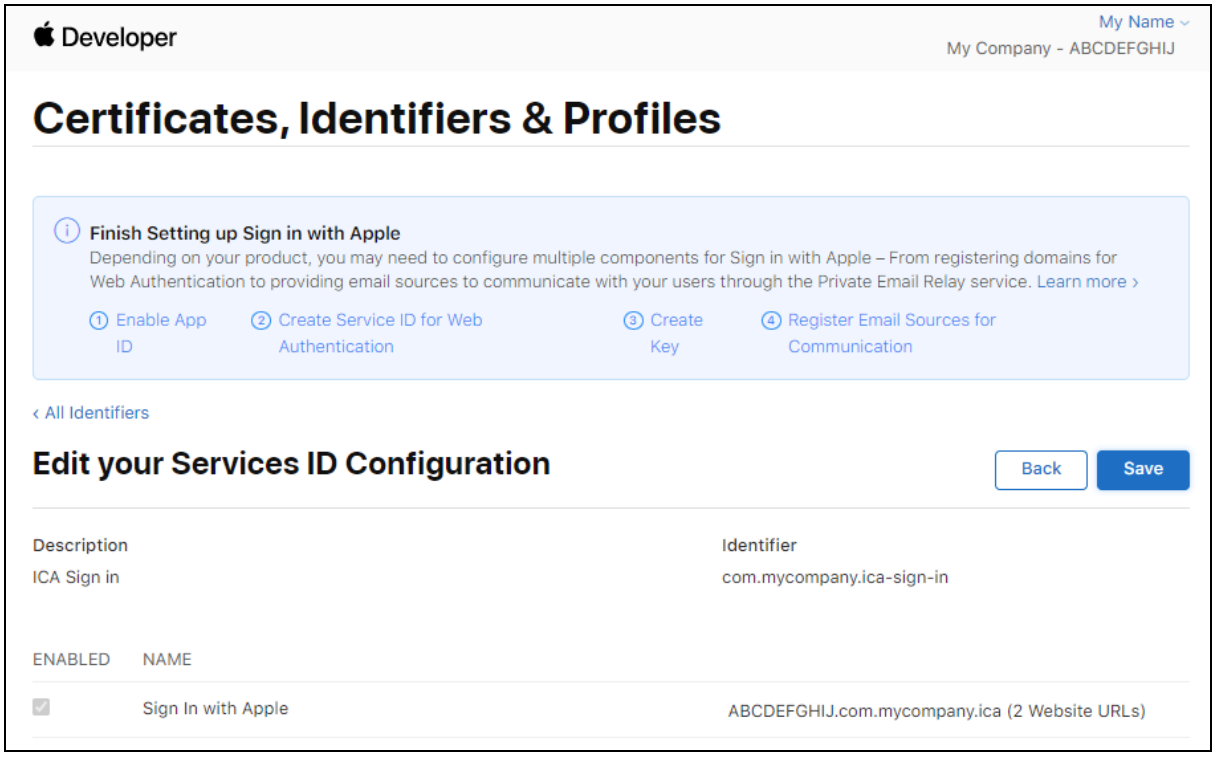
Replace "`incontrol.mycompany.com`" with your InControl's Server Name. The return URLs shall be "`https://{your_server_name}/auth/apple/callback`".



Press Done.

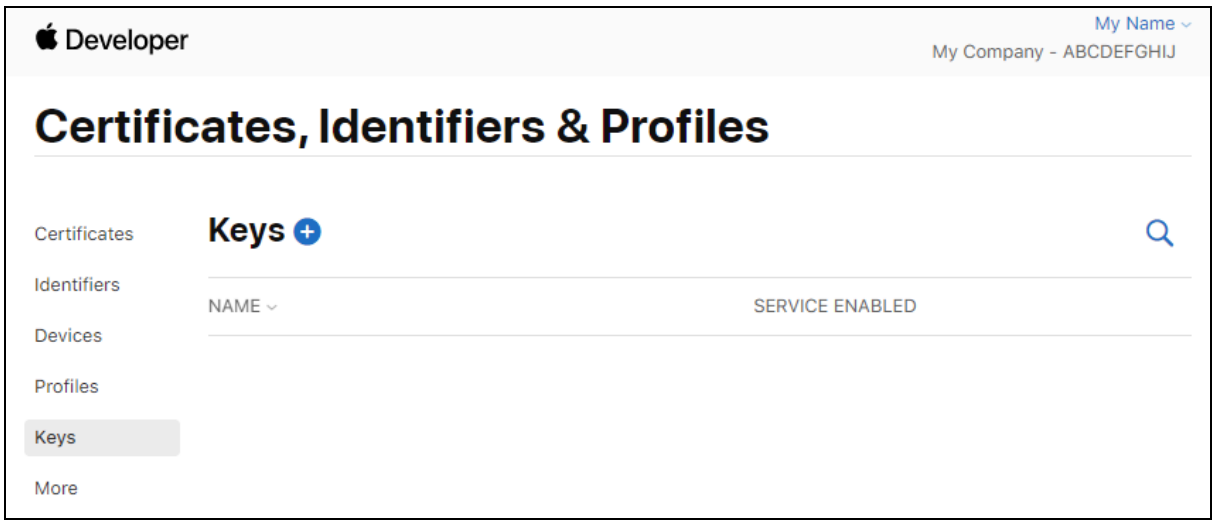


Press Continue.

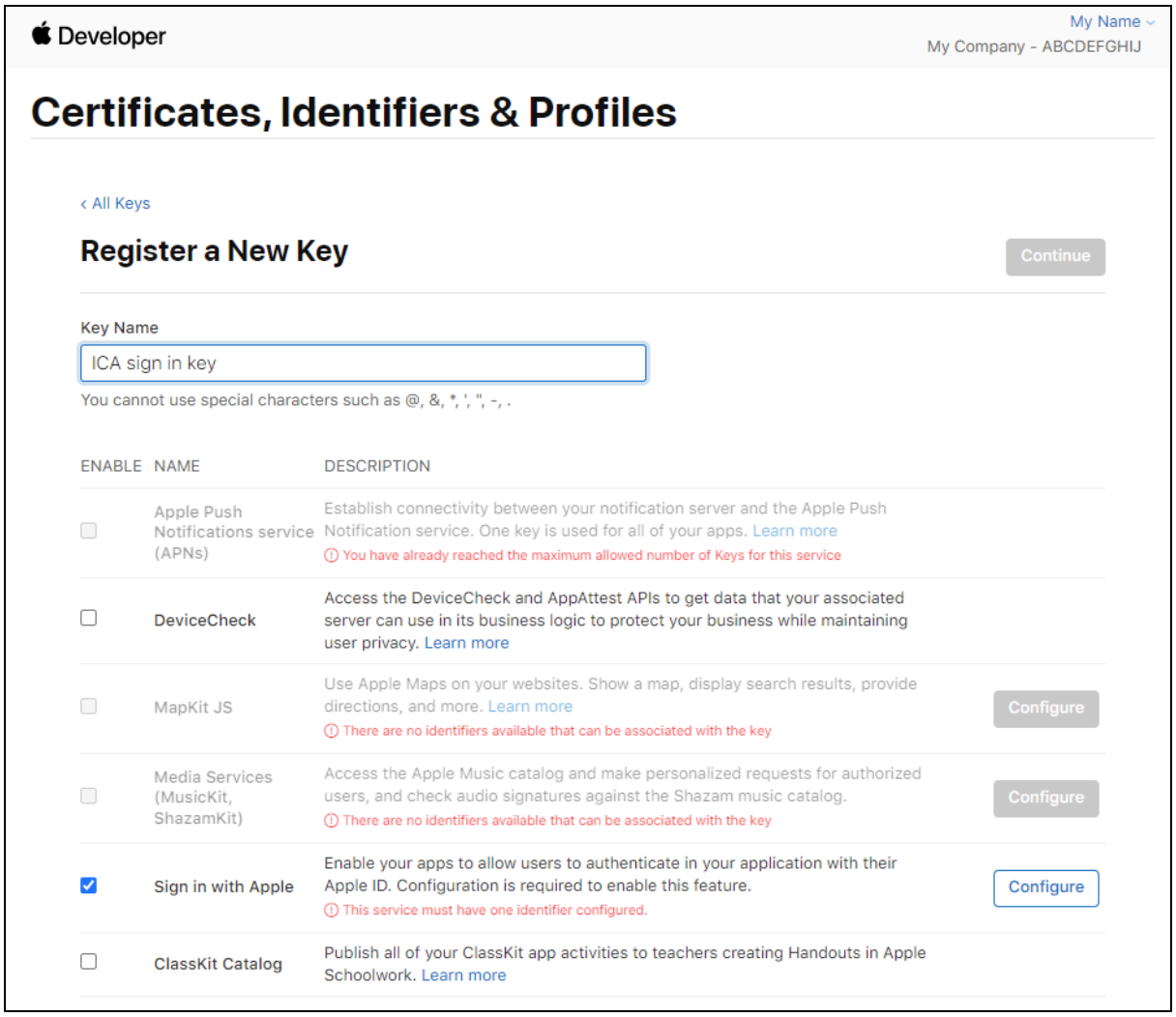


Press Save to save the Services ID.

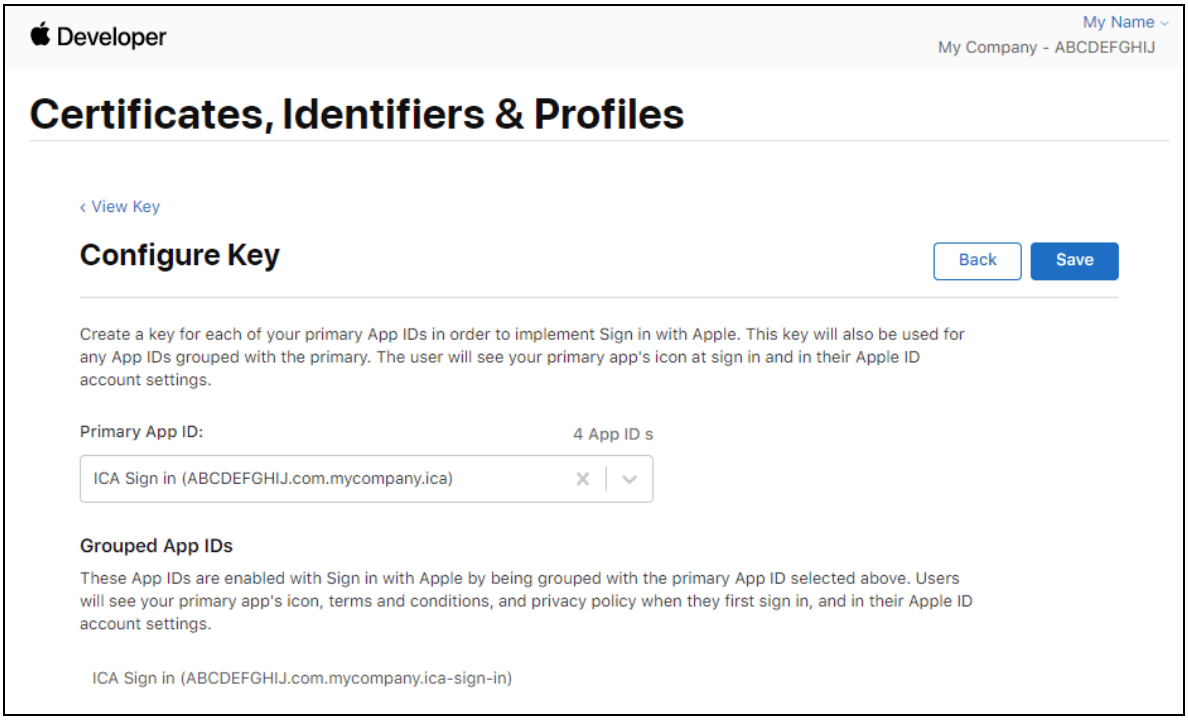
Then press the “Keys” item on the right navigation bar.



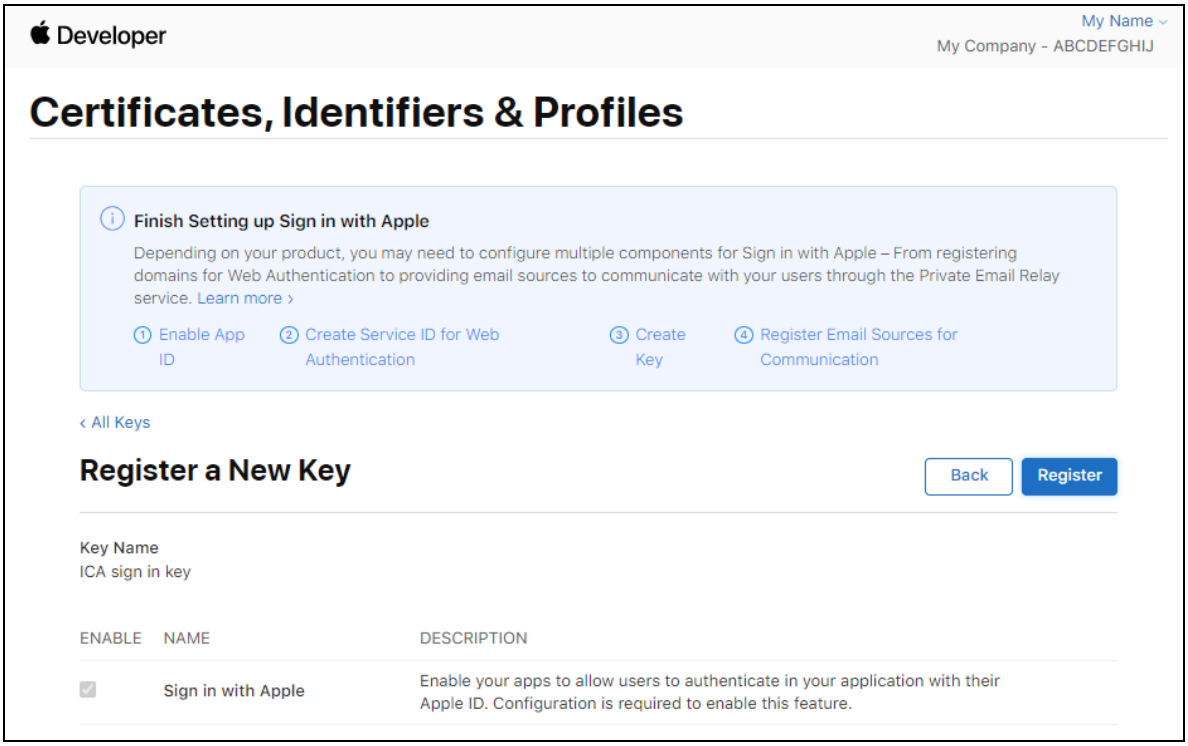
Press the “+” icon.



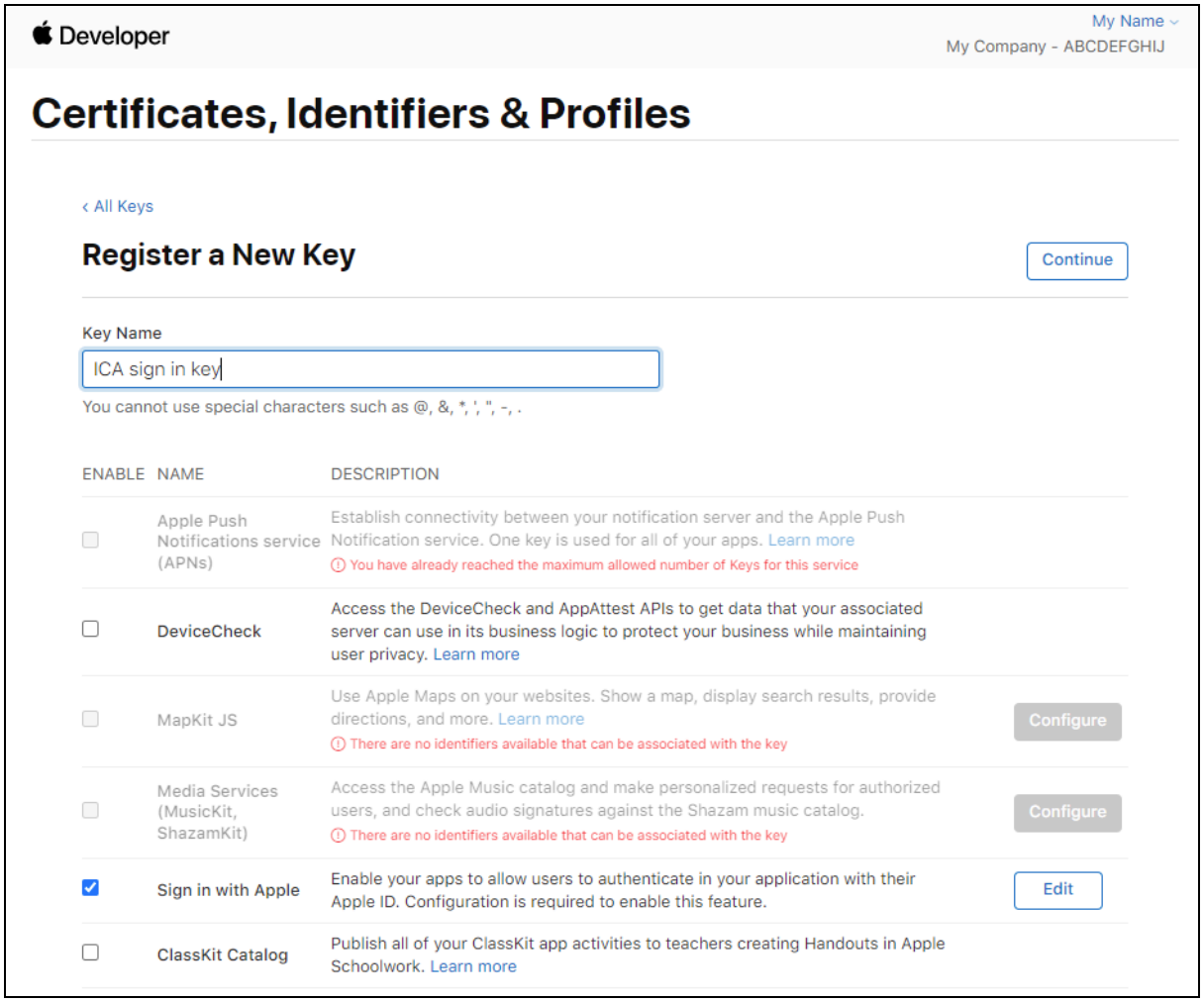
Input “ICA sign in key” in the Key Name field. Select “Sign in with Apple”. Press Configure.



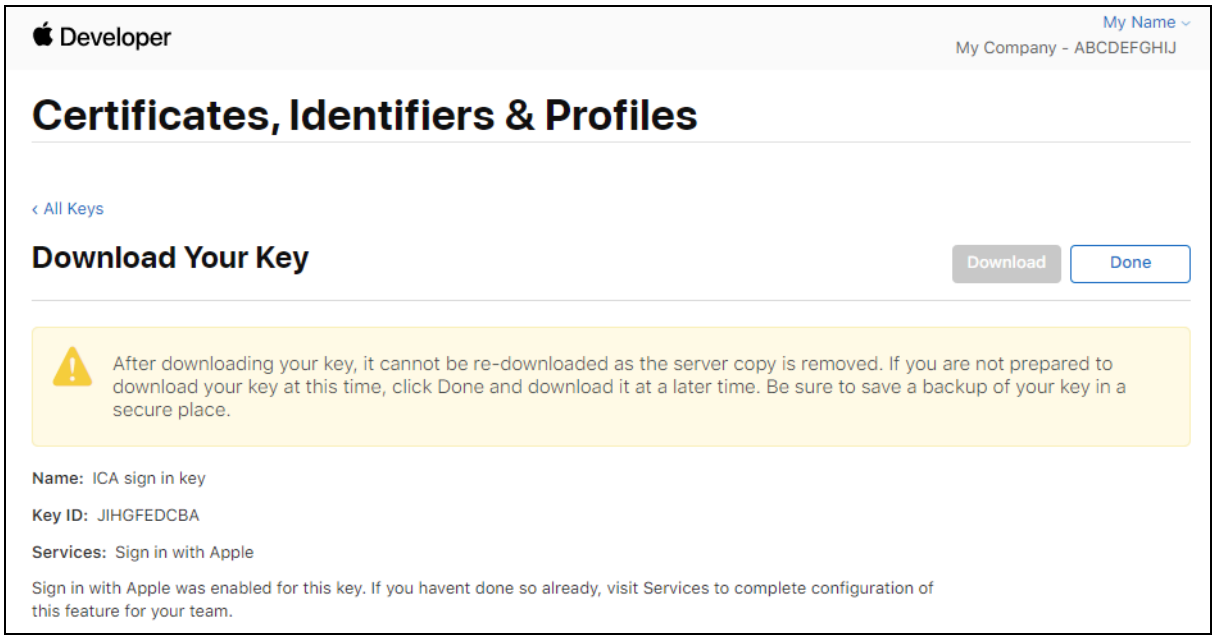
Select “ICA Sign in”. Press Save.



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 in 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.

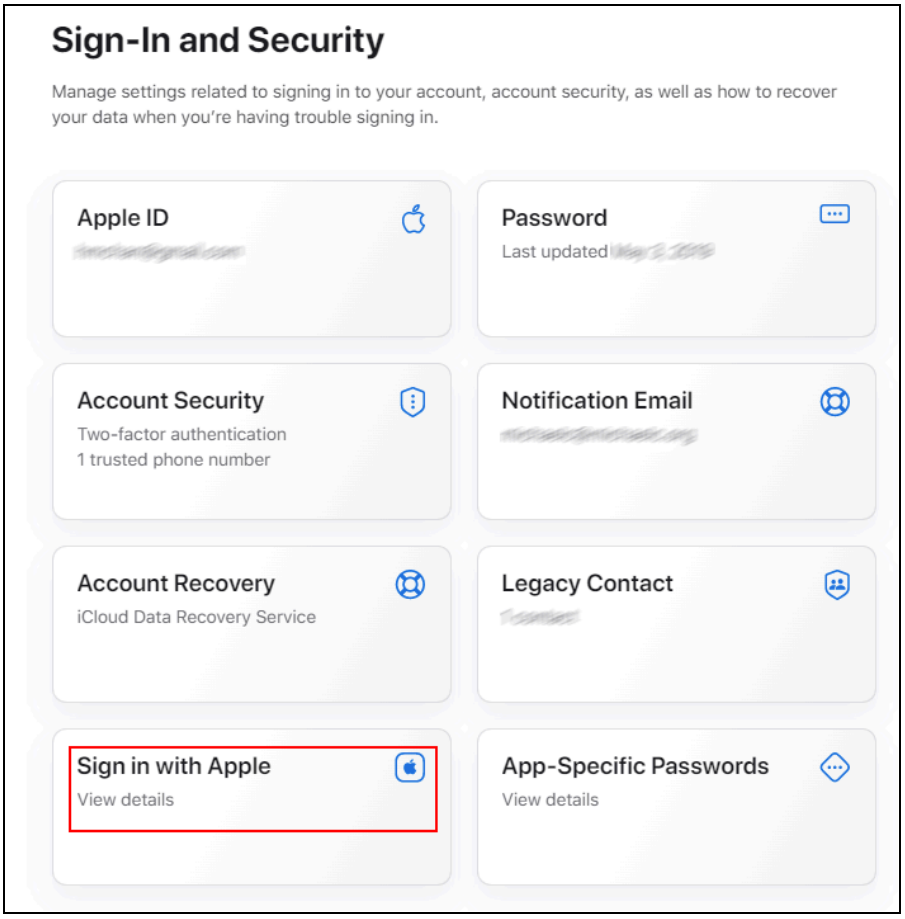
Note: when your users sign in to your InControl with Apple for the first time, they will be asked to choose whether to hide their email address from your InControl on Apple's website. It is a privacy feature of the Apple sign-in.

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.

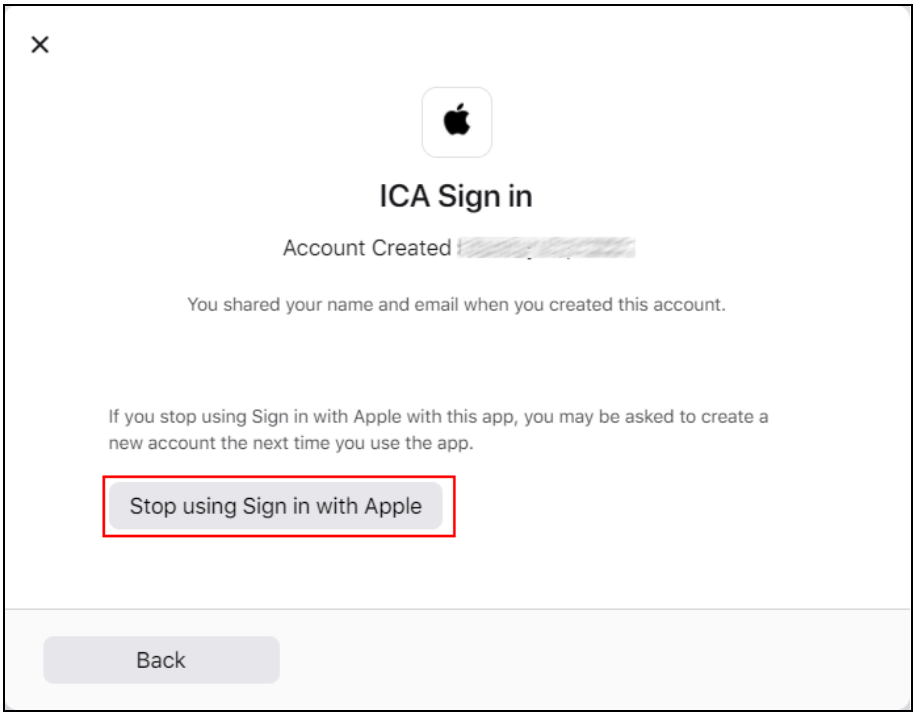
In case they have mistakenly chosen “Hide My Email”, you may either add their Apple-generated email address to the organization/group or advise them to follow the following procedure to change their preference:

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.

Appendix 2: Procedure for setting up authentication with Okta

Step 1. Visit Okta signup page. Choose the one of the two “Okta Platform” plans and sign up for an account. If you have already got an Okta account, skip this.

Step 2. Follow the instructions in this article for how to create an OAuth 2.0 app in Okta.
The Sign-in redirect URI is `https://{ICVA_SERVER_NAME}/auth/openid/callback`

Step 3. Assign users to your Okta OAuth 2.0 app

1. In the Admin Console, go to "Applications" > "Applications"
2. Click your created Okta OAuth 2.0 app
3. Click "Assignments"
4. Click the "Assign" button and select "Assign to People"
5. Select people that allowed to access your Okta OAuth 2.0 app

Step 4: Follow the instructions in this article to get the Okta OpenID Connect Well-Known URL.

Step 5: Visit the ICVA's control panel, scroll down to the "Authentication Settings" section. Enable the "Sign-in with Open ID" option. Fill in the 5 fields accordingly. Fill in the "Okta OpenID Connect Well-Known URL" into the "OpenID Configuration URL" field.