

InControl 2 Appliance Setup Guide

for Appliance Software 2.13.1

(Last updated: 2023-12-22)

Contents

[Contents](#)

[1. Virtual Appliance](#)

[1.1 Introduction](#)

[1.2 Hardware Requirements](#)

[1.3 Installation on VMware ESXi](#)

[Compatibility](#)

[Networking](#)

[Creating InControl and DB VMs](#)

[1.4 Installation on Microsoft Hyper-V](#)

[Networking](#)

[Creating InControl and DB VMs](#)

[Uploading and Adding data storage to the VMs](#)

[Powering up VMs](#)

[1.5 Installation on AWS](#)

[1.5.1 Preparing AMIs](#)

[1.5.1.1 For general AWS regions](#)

[1.5.1.2 For AWS GovCloud](#)

[Uploading the images to S3 Bucket](#)

[Creating the required import role and policy](#)

[Importing the AMI to AWS](#)

[1.5.2 Setting up network](#)

[1.5.3 Setting up security groups](#)

[1.5.4 Setting up Route 53 Hosted private zone](#)

[1.5.5 Creating DNS update role](#)

[1.5.6 Launching instances](#)

[1.5.6.1 For general AWS regions](#)

[1.5.6.2 For AWS GovCloud](#)

[1.5.7 Associate Elastic IP address](#)

- [1.5.8 Reset control panel admin password on AWS](#)
 - [1.6 Installation on Google Cloud Platform](#)
 - [1.6.1 Uploading the image](#)
 - [1.6.2 Importing the image](#)
 - [1.6.3 Setting up the firewall](#)
 - [1.6.4 Creating the instances](#)
 - [1.7 Accessing the Control Panel](#)
 - [1.8 IP Address Configuration and Password Reset On the Console](#)
 - [1.8.1 How to change the VMs' IP on the Internal network?](#)
 - [1.9 Software License](#)
 - [1.10 Data Synchronization with Peplink InControl](#)
- [2. Hardware Appliance](#)
 - [2.1 Accessing Control Panel](#)
 - [2.2 License Key](#)
- [3. Input E-mail Delivery Settings](#)
- [4. Map Settings](#)
 - [Input Google Maps API Key](#)
 - [OpenStreetMap Settings](#)
- [5. Input FTP/SFTP Archive Server Settings](#)
- [6. Facebook App Settings \(for Captive Portal\)](#)
- [7. Setting up Devices to Report to InControl](#)
 - [Method 1: By Configuring Devices Individually - for Internet Isolated Environments](#)
 - [Method 2: By Configuring or Redirecting Devices from the Peplink InControl - for Internet-accessible Environments](#)
- [8. Logging Into InControl Appliance Web Site](#)
- [9. Importing Devices](#)
- [10. Creating an Organization, Group, and Adding Devices](#)
- [11. API Access](#)
- [12. Settings on Your Firewall](#)
 - [12.1 For Hardware Appliance's Management Port](#)
- [13. Upgrading InControl Virtual Appliance](#)
 - [13.1 Upgrading a system newer than 2.9.0](#)
 - [13.2 Upgrading a system earlier than 2.9.0](#)
 - [13.2.1 For VMware ESXi](#)
 - [13.2.2 For Microsoft Hyper-V and versions prior to 2.9.0](#)
- [14. Upgrading InControl Hardware Appliance](#)

15. Release Notes

[Release notes for 2.13.1](#)

[Release notes for 2.13.0.2](#)

[Release notes for 2.13.0.1](#)

[Release notes for 2.13.0](#)

[Release notes for 2.12.1.3](#)

[Release notes for 2.12.1](#)

[Release notes for 2.12.0](#)

[Release notes for 2.11.2](#)

[Release notes for 2.11.1](#)

[Release notes for 2.10.0](#)

[Release notes for 2.9.4.1](#)

[Release notes for 2.9.4](#)

[Release notes for 2.9.3.2](#)

[Release notes for 2.9.3.1](#)

[Release notes for 2.9.3](#)

[Release notes for 2.9.2.2](#)

[Release notes for DB-2021215](#)

[Release notes for 2.9.2.1](#)

[Release notes for 2.9.2](#)

[Release notes for 2.9.1.5](#)

[Release notes for 2.9.1.4](#)

[Release notes for 2.9.1.3](#)

[Release notes for 2.9.1.2](#)

[Release notes for 2.9.1.1](#)

[Release notes for 2.9.1](#)

[Release notes for 2.9.0.6](#)

[Release notes for 2.9.0.5](#)

[Release notes for 2.9.0.4](#)

[Release notes for 2.9.0.3](#)

[Release notes for 2.9.0.2](#)

[Release notes for DB-20210323](#)

[Appendix 1: Procedure for creating a Facebook App ID](#)

[Appendix 2: Procedure for preparing the data for setting up “Sign in with Apple”.](#)

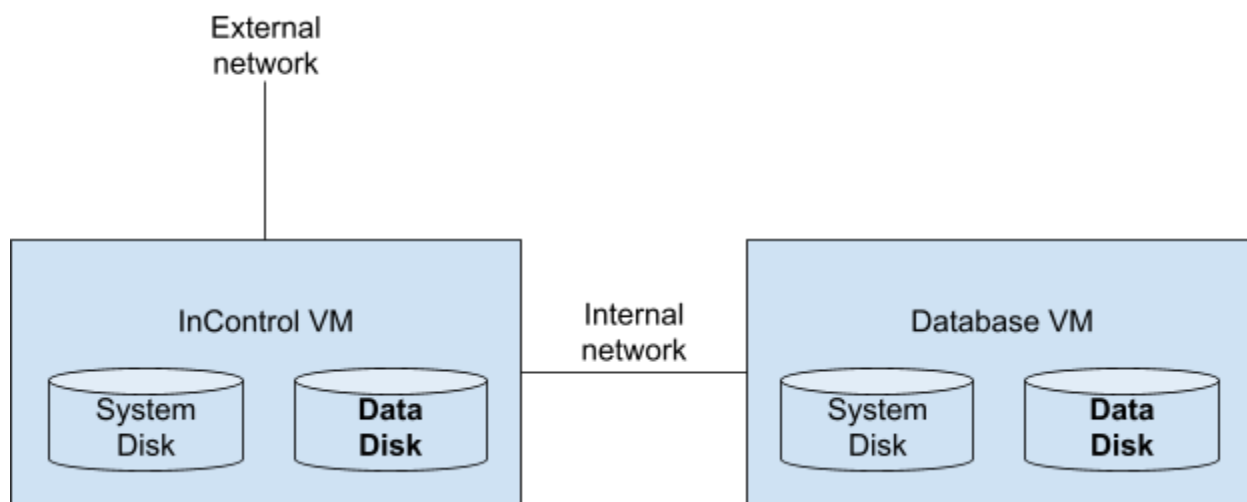
1. Virtual Appliance

1.1 Introduction

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

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

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



1.2 Hardware Requirements

For up to 100 devices

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

Data Disk Size	20 GB	100 GB
-----------------------	-------	--------

For up to 1000 devices

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

For up to 5000 devices

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

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

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

External archive server:

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

1.3 Installation on VMware ESXi

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.

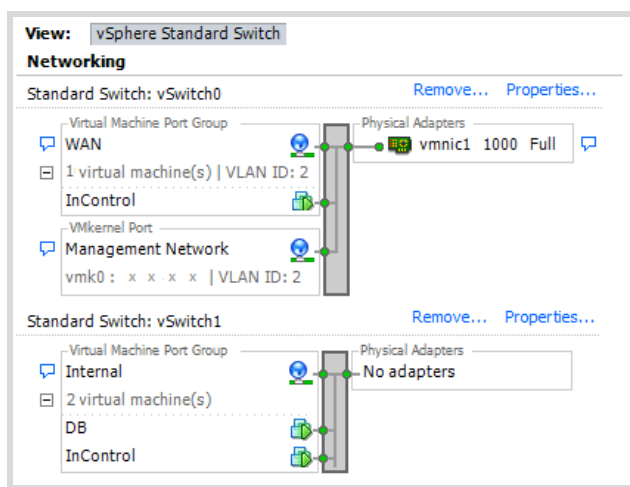
The "Internal" is for inter-InControl-DB communication, no physical adapter is needed. The second network adapter of the InControl VM and the single network adapter on the Database VM shall be assigned to this network.

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 [1.8](#)) and change the IC VM's Internal interface IP and the DB server setting on the control panel.

For the ESXi's web console, navigate to "Networking" > "Port groups".

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



Creating InControl and DB VMs

Step 1. Download the latest Virtual Appliance and Database Server Installation Image file from

<https://www.peplink.com/support/incontrol-appliance-images-downloads/>

Step 2. Extract the downloaded .zip files.

The extracted file names and sizes are as follows:

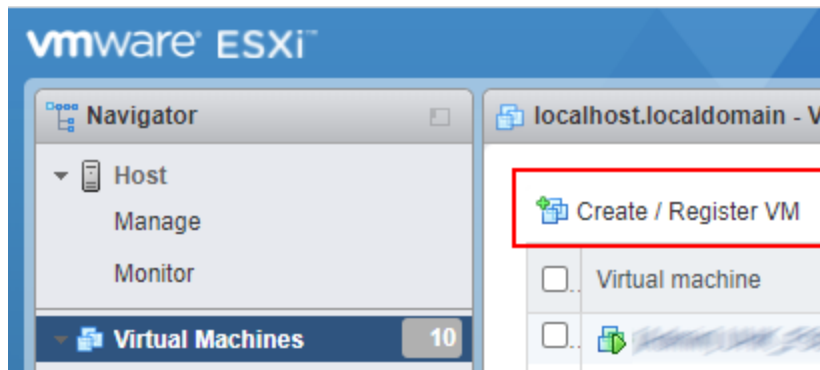
InControl-System-2.9.4.1-vmware.zip:

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

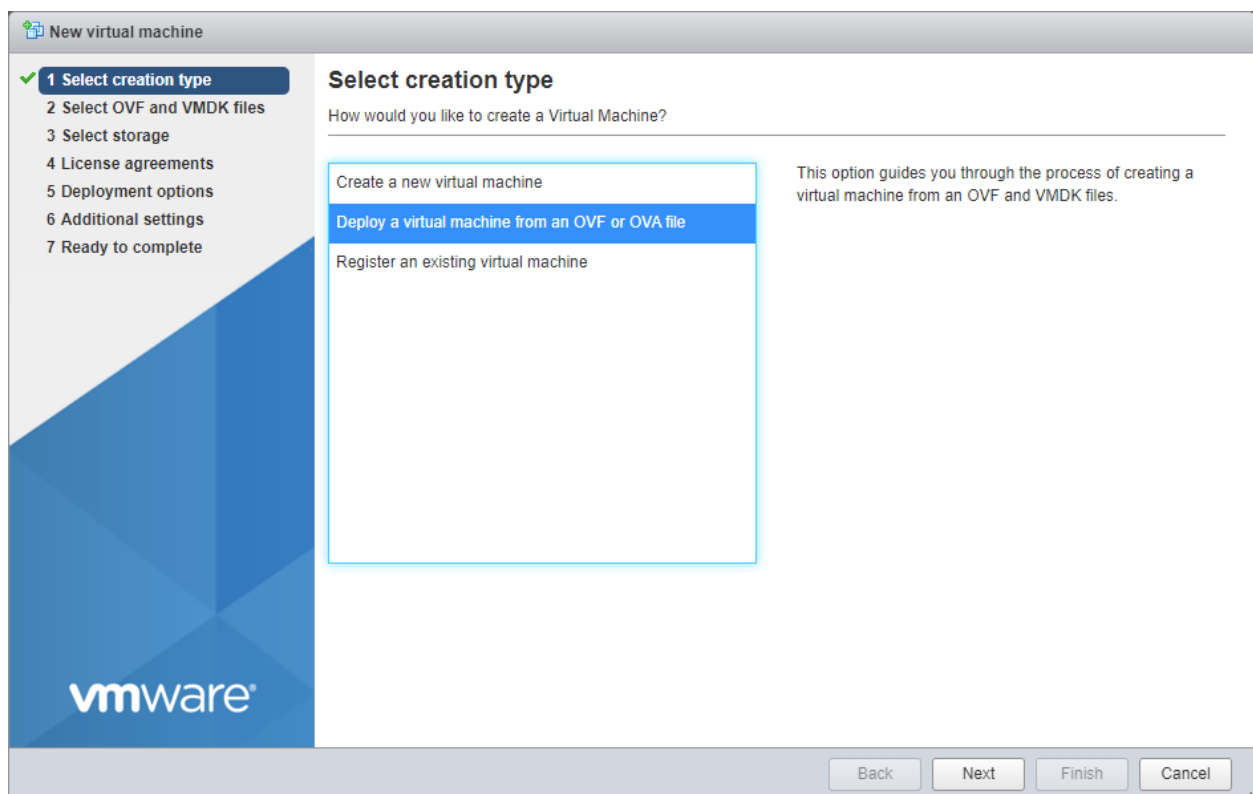
DB-System-20211215-vmware.zip:

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

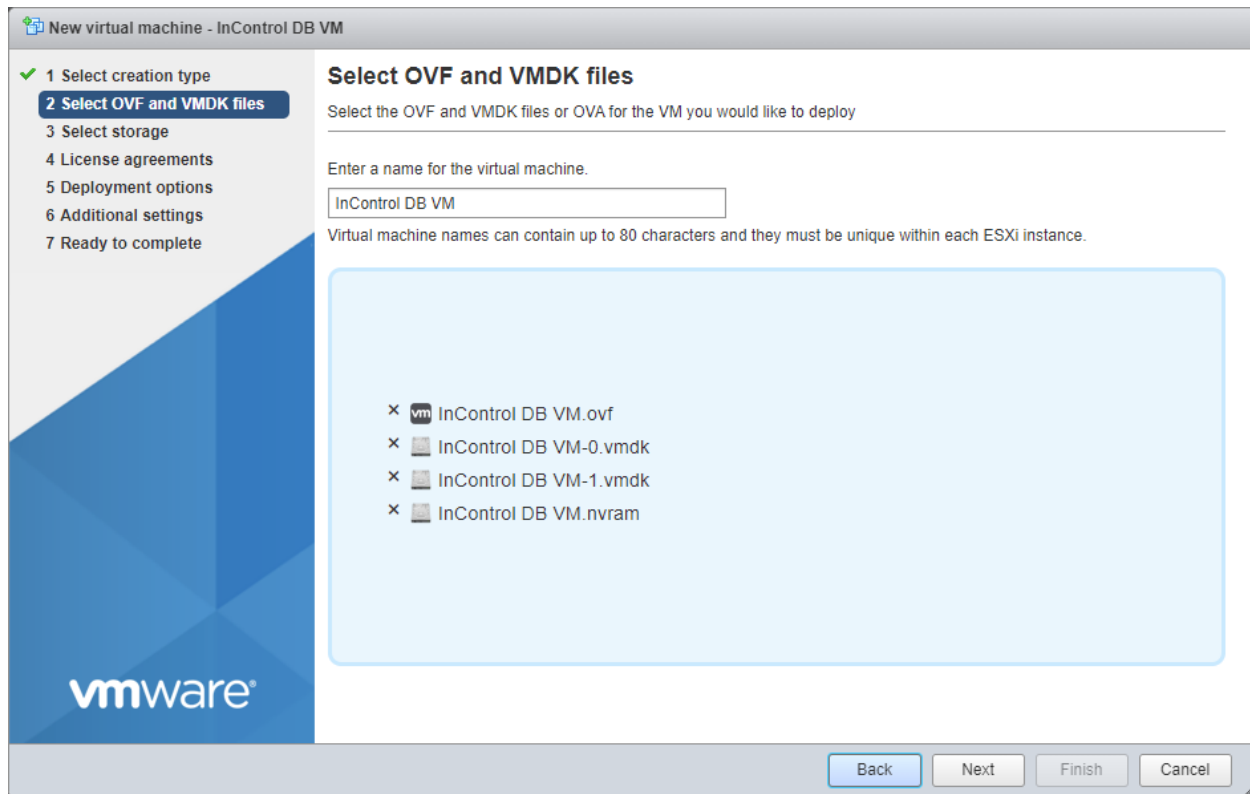
Step 3. On the ESXi web console, navigate to "Virtual Machines". Click the "Create / Register VM" button.



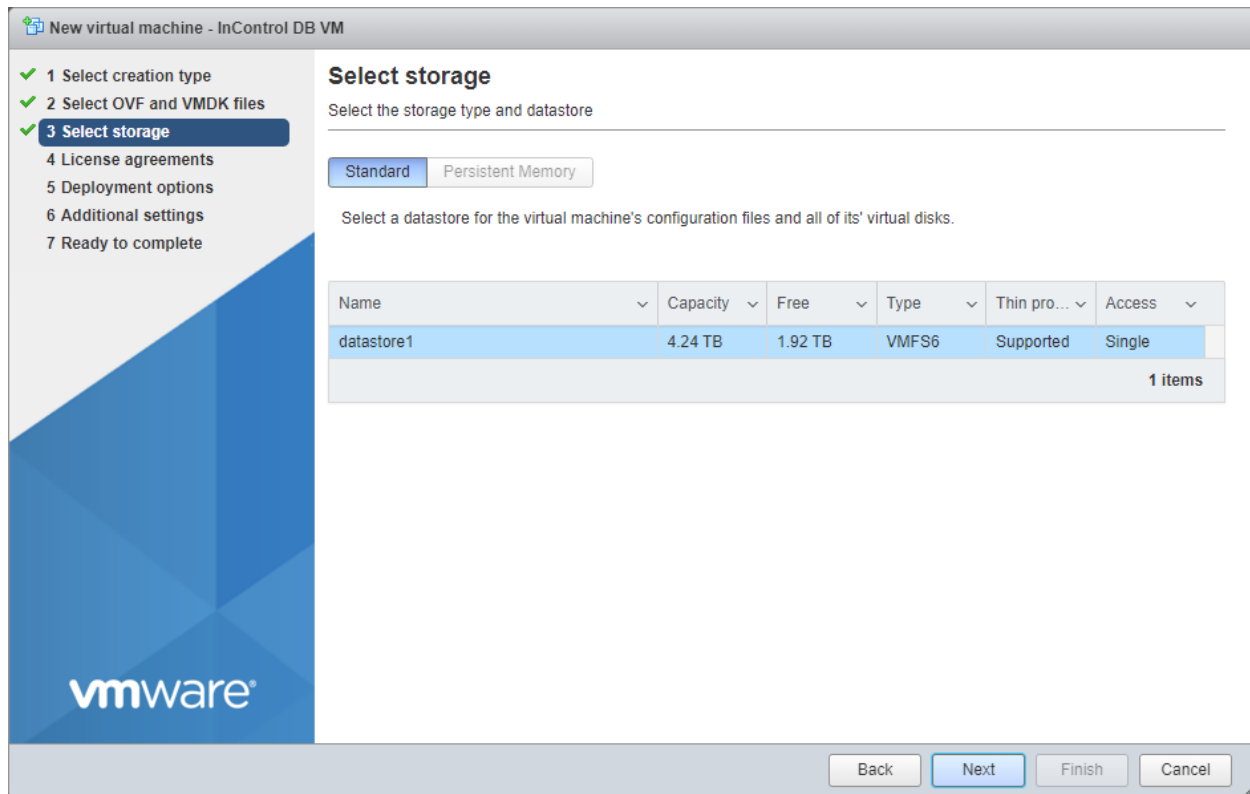
Step 4. Select the creation type "Deploy a virtual machine from an OVF or OVA file". Click "Next".



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



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



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

New virtual machine - InControl DB VM

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Ready to complete

Deployment options

Select deployment options

Network mappings	Internal <input type="text" value="Internal"/>
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick
Power on automatically	<input checked="" type="checkbox"/>

Back Next Finish Cancel

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.


New virtual machine - InControl DB VM

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

Product	InControl DB VM
VM Name	InControl DB VM
Files	InControl DB VM-0.vmdk InControl DB VM-1.vmdk InControl DB VM.nvram
Datastore	datastore1
Provisioning type	Thin
Network mappings	Internal: Internal
Guest OS Name	Unknown

 Do not refresh your browser while this VM is being deployed.

Back Next Finish Cancel

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 screenshot shows the 'New virtual machine - InControl IC VM' wizard in VMware Workstation. The left sidebar lists five steps: 1. Select creation type, 2. Select OVF and VMDK files, 3. Select storage, 4. Deployment options (highlighted), and 5. Ready to complete. The main area is titled 'Deployment options' and contains the instruction 'Select deployment options'. It features three sections: 'Network mappings' with dropdowns for 'WAN' and 'Internal' (both set to 'WAN' and 'Internal' respectively); 'Disk provisioning' with radio buttons for 'Thin' (selected) and 'Thick'; and 'Power on automatically' with a checked checkbox. At the bottom right are buttons for 'Back', 'Next', 'Finish', and 'Cancel'. The VMware logo is visible in the bottom left corner of the window.

Deployment options	
Select deployment options	
Network mappings	<div>WAN WAN</div> <div>Internal Internal</div>
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick
Power on automatically	<input checked="" type="checkbox"/>

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

1.4 Installation on Microsoft Hyper-V

Networking

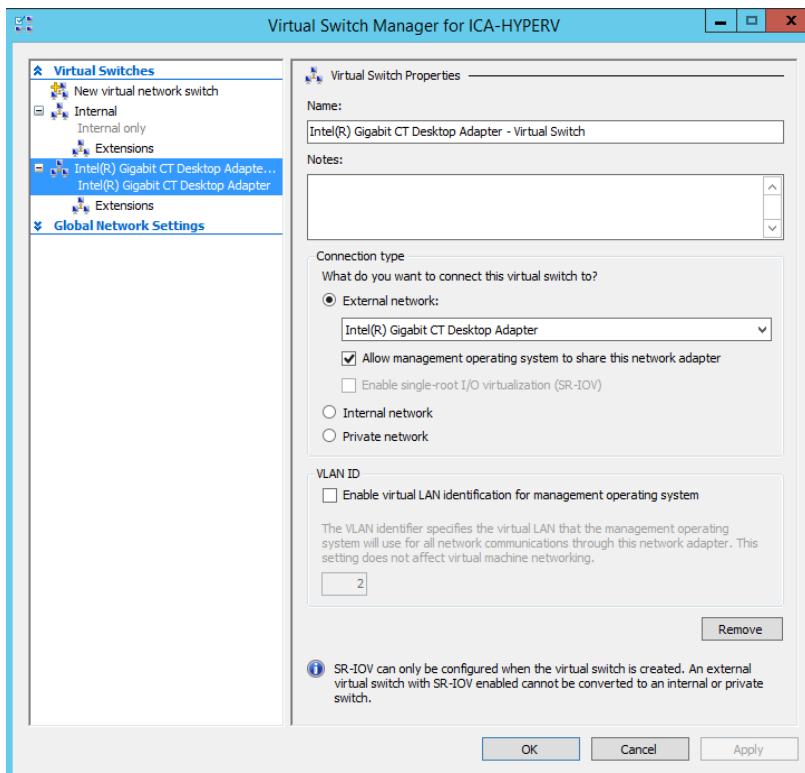
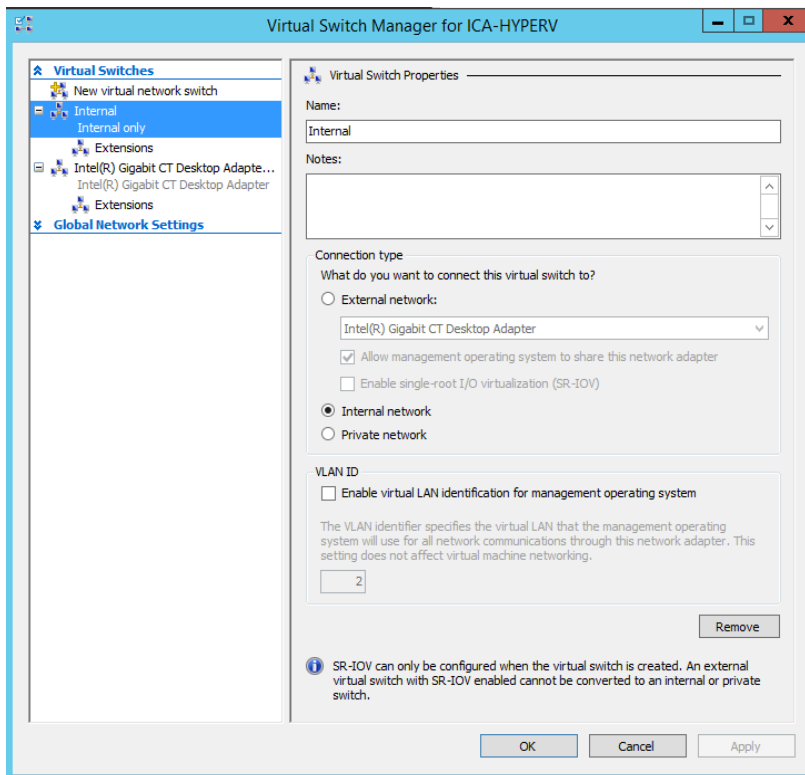
First of all, please create two networks on the Hyper-V host.

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

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

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

Note 2: As the "Internal" network segment is on the subnet 192.168.1.0/24 by default, the WAN interface cannot be on 192.168.1.0/24 too. You may change the subnet DB VM's "Internal" interface's IP on the console (see chapter [1.8](#)) and change the IC VM's Internal interface IP and the DB server setting on the control panel.



Creating InControl and DB VMs

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

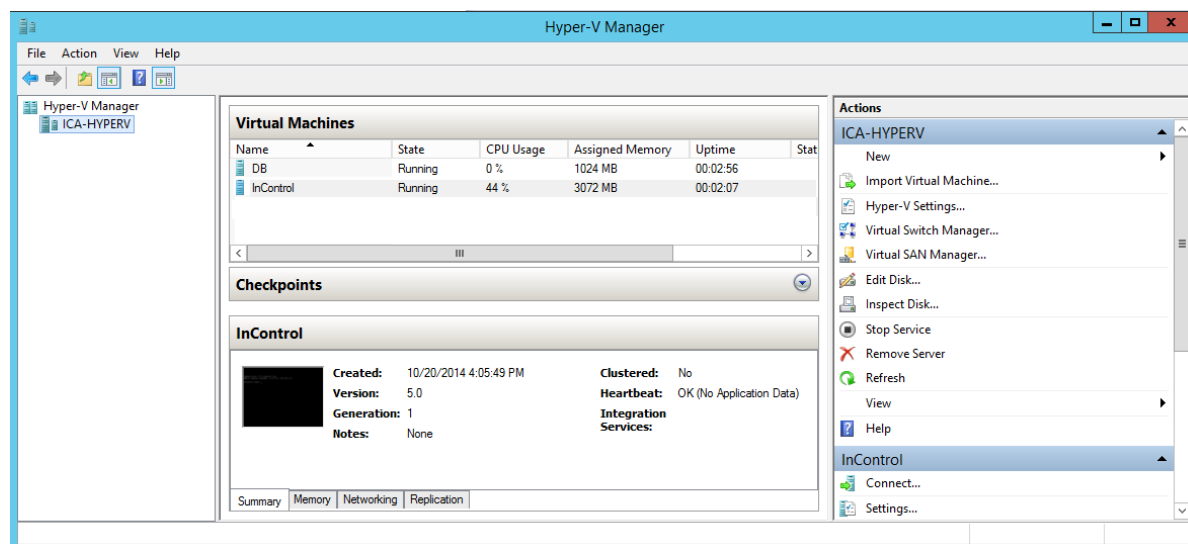
Download the latest Virtual Appliance and Database Server image files in .vhdx format from

<https://www.peplink.com/support/incontrol-appliance-images-downloads/>

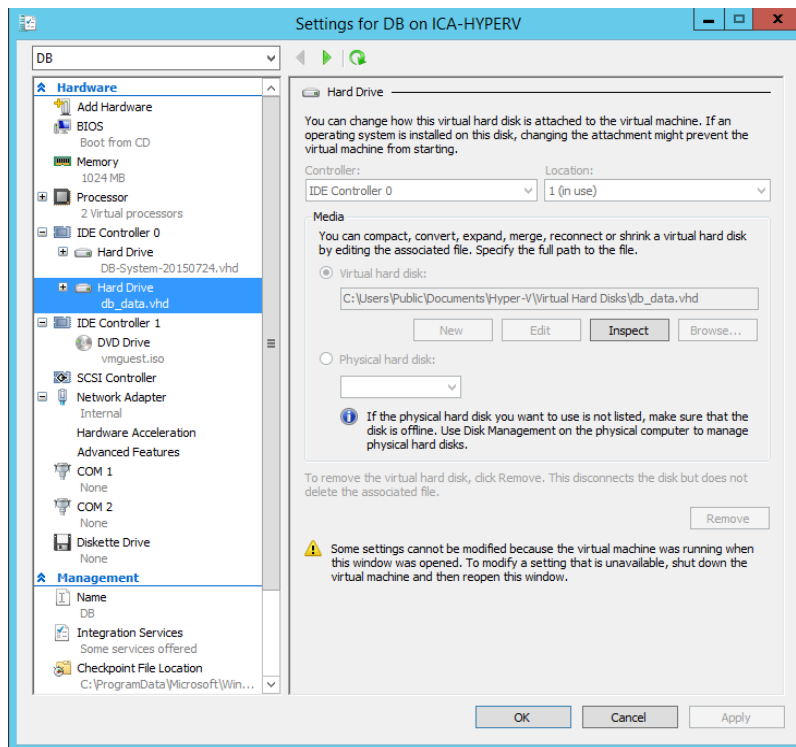
The .vhdx file names and sizes are as follow:

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

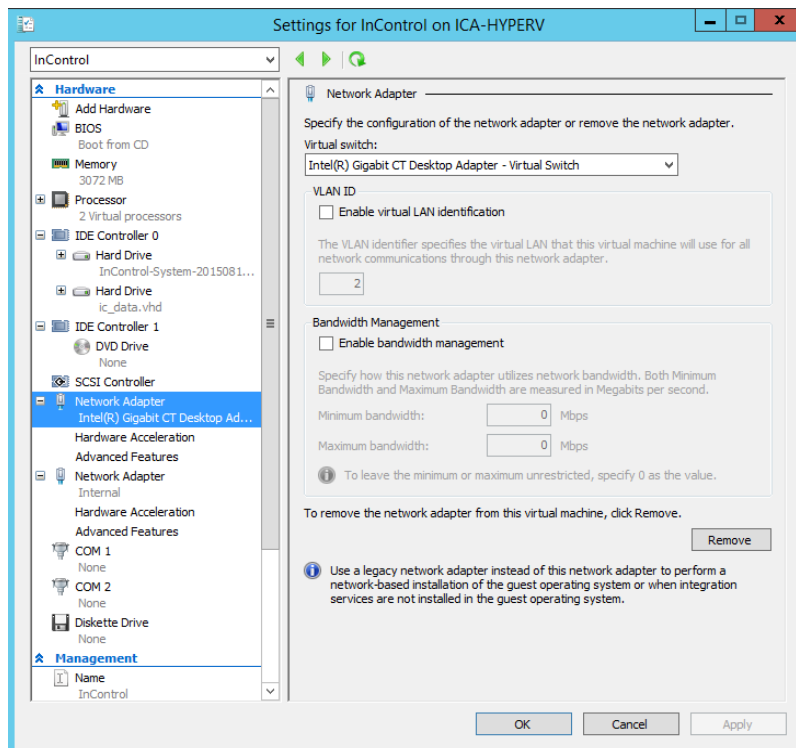
In the Hyper-V Manager, create two new Virtual Machines called `DB` and `InControl` for Ubuntu Linux (64 bit) guest operating systems. Our test was on first-generation VMs. For the DB VM, you need only one network connection on the Internal network. For the InControl VM, you'll need the WAN network and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



DB VM:



InControl VM:



Uploading and Adding data storage to the VMs

For the InControl VM, add the `InControl-System.vhd` on IDE (0:0) and create an empty 20GB disk on IDE (0:1). For the DB VM, follow the same but add 100 GB of disk storage for supporting 100 devices. See [Introduction - Minimum Hardware Requirements](#)

Choose VHDX - fixed-size data disks.

 New Virtual Hard Disk Wizard

×



Completing the New Virtual Hard Disk Wizard

Before You Begin

Choose Disk Format

Choose Disk Type

Specify Name and Location

Configure Disk

Summary

You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk.

Description:

Format:	VHD
Type:	fixed size
Name:	ic_data.vhd
Location:	C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks
Size:	20 GB

To create the virtual hard disk and close this wizard, click Finish.

< Previous

Next >

Finish

Cancel

After the installation, please perform a firmware update. Please refer to [chapter 13.1](#).

Powering up VMs

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

1.5 Installation on AWS

1.5.1 Preparing AMIs

1.5.1.1 For general AWS regions

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

1.5.1.2 For AWS GovCloud

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

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

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

Note: The file paths for AWS CLI commands should be specified in full with respect to your OS. E.g.

- **Windows:** `"file:///C:/Users/username/My Documents/trust-policy.json"`
- **Mac and Linux:** `"file:///Users/username/trust-policy.json"`

Uploading the images to S3 Bucket

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

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

Creating the required import role and policy

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

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

Then, run the following command to create the role:

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

(Please change the file path as described above.)

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

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

```

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

```

Then run the following command to create the role.

```

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

```

(Please change the file path as described above.)

Importing the AMI to AWS

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

db.json:

```

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

```

icva.json:

```

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

```

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

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

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

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

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

1.5.2 Setting up network

InControl virtual appliances require to be set up in a 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 login 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.

VPC > Subnets > subnet-02b8dc87d2190ab36 > Edit subnet settings

Edit subnet settings [Info](#)

Subnet

Subnet ID	Name
 subnet-02b8dc87d2190ab36	 subnet ic

Auto-assign IP settings [Info](#)

Enable the auto-assign IP settings to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

- ☒ Enable auto-assign public IPv4 address [Info](#)
- ☐ Enable auto-assign customer-owned IPv4 address [Info](#)
Option disabled because no customer owned pools found.

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”. Select the “Main” route of the VPC. In the Routes section, click the “Edit routes” button. Add a route where the Destination is “0.0.0.0/0” and the Target is the Internet gateway’s ID.

1.5.3 Setting up security groups

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

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

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

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

Protocol	Port	Source
TCP	3306	<i>The VPC's subnet address</i>
TCP	27017	<i>The VPC's subnet address</i>
TCP	6379	<i>The VPC's subnet address</i>
TCP	22	<i>The VPC's subnet address</i>
All ICMP (IPv4)	-	<i>The VPC's subnet address</i>

1.5.4 Setting up Route 53 Hosted private zone

Open the Route 53 > "Hosted zone". Click on **Create a new zone**.

Enter `peplink.icva` as the Domain name and select the Private zone option. In the next section, pick the region of your VPC and associate your InControl Virtual Appliance VPC with the private zone.

You can copy the domain name, as it will be used later.

Hosted zone configuration

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain name [Info](#)

This is the name of the domain that you want to route traffic for.

Valid characters: a-z, 0-9, ! * # \$ % & ' () * + , - / : ; < = > ? @ [\] ^ _ ` { | } . ~

Description - optional [Info](#)

This value lets you distinguish hosted zones that have the same name.

The description can have up to 256 characters. 29/256

Type [Info](#)

The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

☐ **Public hosted zone**
A public hosted zone determines how traffic is routed on the internet.

☒ **Private hosted zone**
A private hosted zone determines how traffic is routed within an Amazon VPC.

VPCs to associate with the hosted zone [Info](#)

To use this hosted zone to resolve DNS queries for one or more VPCs, choose the VPCs. To associate a VPC with a hosted zone when the VPC was created using a different AWS account, you must use a programmatic method, such as the AWS CLI.

For each VPC that you associate with a private hosted zone, you must set the Amazon VPC settings `enableDnsHostnames` and `enableDnsSupport` to true.

Region [Info](#)

US East (Ohio) [us-east-2]

VPC ID [Info](#)

Q vpc-075c036564d693572

Remove VPC

Add VPC

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

peplink.icva [Info](#)

▼ Hosted zone details

Hosted zone ID

Z0307012209DWNG9W7FTW

1.5.5 Creating DNS update role

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

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

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

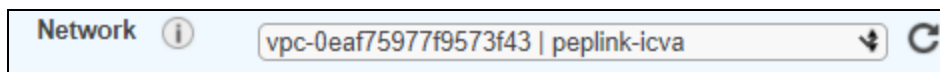
Navigate to **Identity and Access Management (IAM)** and select **Roles**. Click the **Create role** button. Choose **AWS service > EC2** and click **Next: Permission**. Select the policy ***AutoDNSUpdatePeplink*** that you just created. Click **Next: Tags**. Click **Next: Review**. On the **Review**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

1.5.6 Launching instances

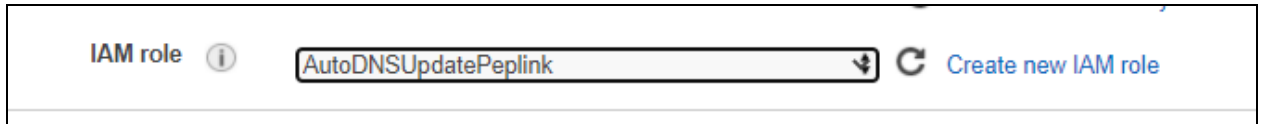
Please follow the instruction in [chapter 1.5.1](#) to prepare the AMI images in your account. You shall launch a DB instance first and then an InControl instance. If your setup is on AWS GovCloud, please jump to [chapter 1.5.6.2](#).

1.5.6.1 For general AWS regions

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



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



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

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

DB Instance	
AUTO_DNS_ZONE	<i>HOSTED_ZONE_ID</i>
AUTO_DNS_NAME	db.peplink.icva
Name	ICA DB

InControl instance	
AUTO_DNS_ZONE	<i>HOSTED_ZONE_ID</i>
AUTO_DNS_NAME	web.peplink.icva
Name	ICA IC

Click the **Configure Security Group** button.

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

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Proceed without a key pair

☒ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

Cancel
Launch Instances

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

```
https://ICA_public_address:4443
```

Please upgrade the firmware immediately. You may refer to [chapter 13.1](#).

1.5.6.2 For AWS GovCloud

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

Network ⓘ
vpc-0eaf75977f9573f43 | peplink-icva

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

IAM role ⓘ
AutoDNSUpdatePeplink
Create new IAM role

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

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ
Root	/dev/sda1	snap-04fd314d49a2812f2	25
EBS ▼	/dev/sdb ▼	Search (case-insensit	50

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

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

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

Click the **Configure Security Group** button.

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

Select an existing key pair or create a new key pair ×

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Proceed without a key pair ▼

☒ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

Cancel Launch Instances

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

```
https://ICA_public_address:4443
```

Please upgrade the firmware immediately. You may refer to [chapter 13.1](#).

1.5.7 Associate Elastic IP address

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

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

1.5.8 Reset control panel admin password on AWS

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

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

```
password=yournewpassword
```

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

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

1.6 Installation on Google Cloud Platform

1.6.1 Uploading the image

Browse to Google Cloud Storage menu and create a new bucket.

Name your bucket and select the planned installation region. All other default settings can be kept.



Choose where to store your data

This permanent choice defines the geographic placement of your data and affects cost, performance, and availability. [Learn more](#)

Location type

- ☒ Region
Lowest latency within a single region
- ☐ Dual-region
High availability and low latency across 2 regions
- ☐ Multi-region
Highest availability across largest area

Location


us-east1 (South Carolina) ▼


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


1.6.2 Importing the image

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


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

Name 
Name is permanent

Source 
Cloud Storage file

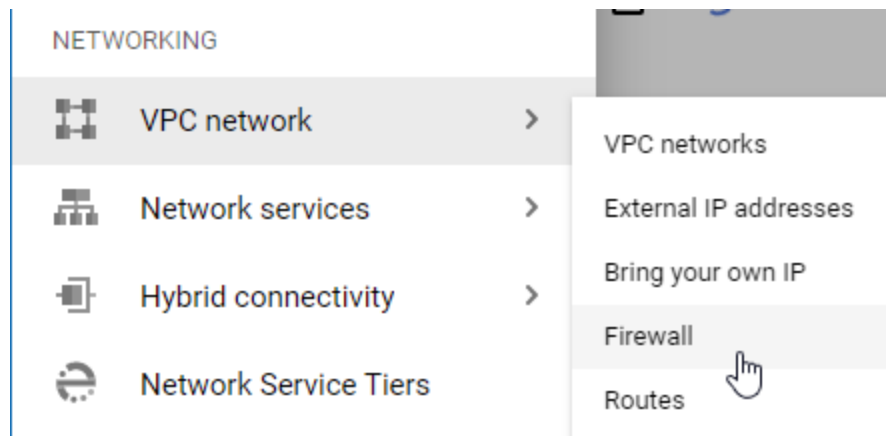
Cloud Storage file 
Your image source must use the .tar.gz extension and the file inside the archive must be named disk.raw. [Learn more](#)

☒

Location 
☐ Multi-regional
☒ Regional

1.6.3 Setting up the firewall

Browse to Networking / VPC Network / Firewall.



Click on Create Firewall rule:

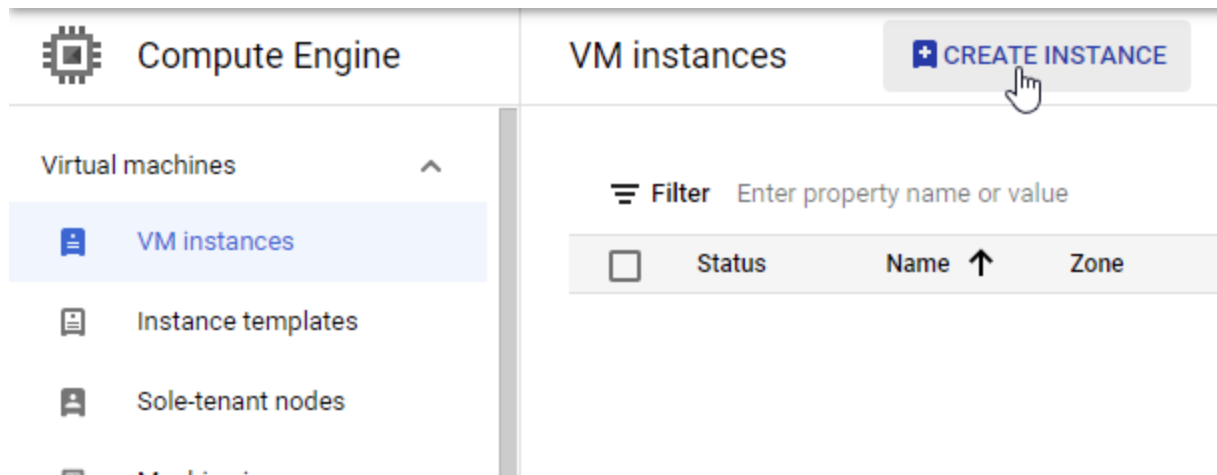
- Name your first rule “incontrol”
- Add a “Target tags” as “incontrol”
- Add a Source IP range from which your InControl instance will be reachable (eg: 0.0.0.0/0)
- Check TCP and paste the following: 80 , 443 , 2222 , 4443 , 5246
- Check UDP and paste the following: 53 , 5246
- Click on create

Now create a new firewall rule for DB:

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

1.6.4 Creating the instances

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



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

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

Boot disk

Select an image or snapshot to create a boot disk; or attach an existing disk. Can't find what y

Public images

Custom images

Snapshots

Existing disks

Show images from

My First Project

☐ Show deprecated images

Image

db

Created on Feb 24, 2021, 11:57:30 AM

Boot disk type ?

Balanced persistent disk

Size (GB) ?

25

- Expand the “Networking, disks, security, management, sole-tenancy” menu
✓ **NETWORKING, DISKS, SECURITY, MANAGEMENT, SOLE-TENANCY**
- 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”

Network interfaces ?

Network interface is permanent

Edit network interface ^

Network *
default

Subnetwork *
default (10.138.0.0/20)

Primary internal IP
db (10.138.0.3)

Alias IP ranges

+ ADD IP RANGE

External IP
None


DONE

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

Now create another new instance for the InControl:

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

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

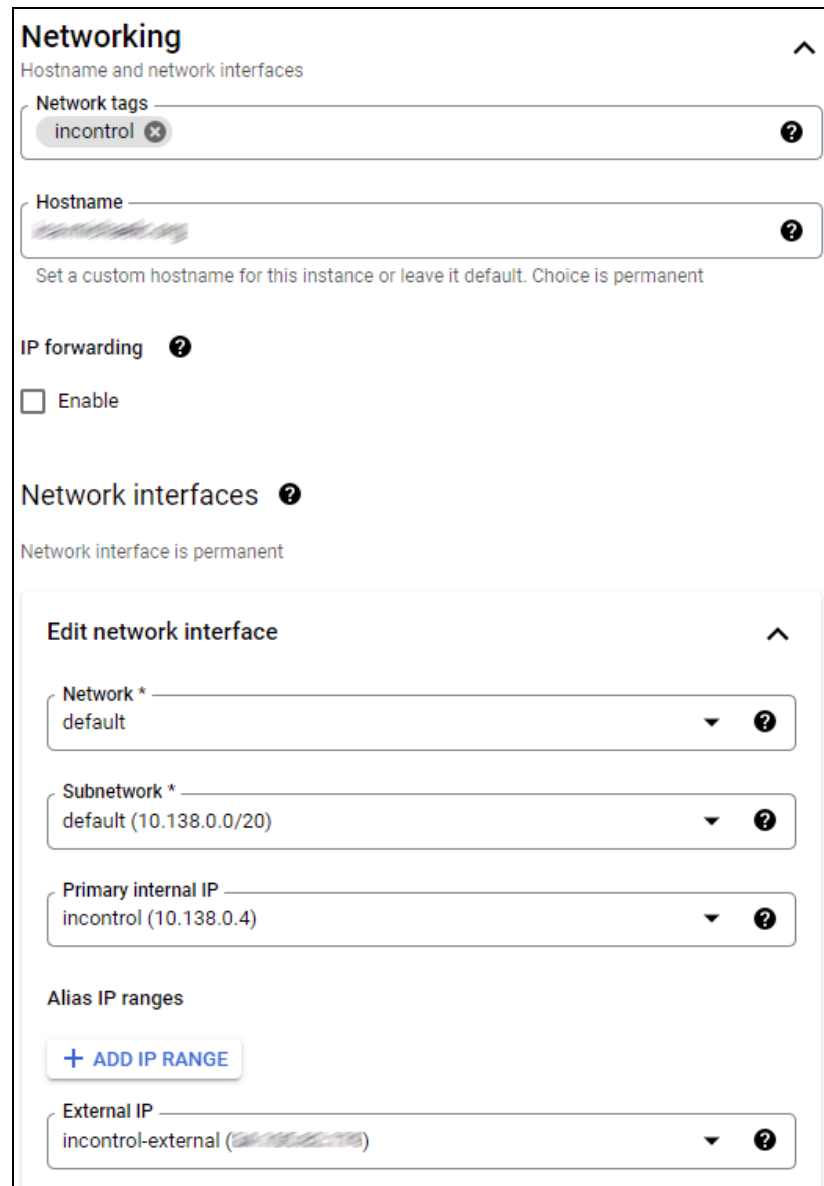
Hostname 

Set a custom hostname for this instance or leave it default. Choice is permanent

incontrol.xxxx.yyy

- 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.



Networking ^

Hostname and network interfaces

Network tags ?

incontrol ×

Hostname ?

[Redacted]

Set a custom hostname for this instance or leave it default. Choice is permanent

IP forwarding ?

☐ Enable

Network interfaces ?

Network interface is permanent

Edit network interface ^

Network * ?

default ▼

Subnetwork * ?

default (10.138.0.0/20) ▼

Primary internal IP ?

incontrol (10.138.0.4) ▼

Alias IP ranges

[+ ADD IP RANGE](#)

External IP ?

incontrol-external ([Redacted]) ▼

- 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.

Metadata

You can set custom metadata for an instance or project outside of the server-defined metadata. This is useful for passing in arbitrary values to your project or instance that can be queried by your code on the instance. [Learn more](#)

Key *	Value
<input type="text" value="db"/>	<input type="text" value="10.138.0.3"/>

- Click Create.

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

1.7 Accessing the Control Panel

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

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

System Control Panel

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

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

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

1.8 IP Address Configuration and Password Reset On the Console

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

InControl VM:

```
InControl 2.8.1
WAN IP address: 10.8.30.104/16

Control panel: https://10.8.30.104:4443/

incontrol login: setup
Password:
Last login: Thu Jun 13 09:25:10 UTC 2019 on tty1

      IP Settings
      =====

[WAN]
Connection Method: Static
      IP Address: 10.8.30.104
      Subnet Mask: 255.255.0.0
      Gateway: 10.8.8.1
      DNS Servers: 10.8.8.1

[Internal]
Connection Method: Static
      IP Address: 192.168.1.1
      Subnet Mask: 255.255.255.0

1: Change IP settings for WAN interface
2: Change IP settings for Internal interface
7: Reset control panel password
9: Abort
Choice:
```

Database VM

```
Ubuntu 14.04.6 LTS DB tty1

DB login: setup
Password:
Last login: Mon Jul 22 03:02:20 UTC 2019 on tty1

      IP Settings
      =====

[Internal]
Connection Method: static
      IP Address: 192.168.1.3
      Subnet Mask: 255.255.255.0

1: Change IP settings for Internal interface
9: Abort/Exit
Choice:
```

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

By default, the IP addresses of the InControl and database VMs are 192.168.1.1 and 192.168.1.3 respectively. 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	<input type="text" value="192.168.1.3"/>

1.9 Software License

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

License		
Server Name	<input type="text" value="incontrol.my.domain"/>	
License Key	<input type="text"/>	<input type="button" value="Submit"/>
Max. Allowed Number of Active Devices	50	
Expiry Date	n/a	

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

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

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

1.10 Data Synchronization with Peplink InControl

In order for the InControl Appliance to maintain the up-to-date warranty/subscription/PrimeCare date record, since version 2.9.0, the system automatically synchronizes devices' service expiration date records with Peplink InControl on the Internet every six hours. In addition, device's Feature Add-on activations, new product and model definitions, firmware releases, and captive portal default certificates are also synchronized at the same time.

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://{ICA_Address}/r/msp/device_management) and clicking the Synchronize button in the "Device Expiration Date Synchronization" section.

Device Expiration Date Synchronization

InControl Appliance system regularly attempts to connect to Peplink InControl public cloud and synchronize devices' warranty, subscription, and PrimeCare expiration dates. If this InControl Appliance is not connected to the Internet, or you want to initiate a synchronization manually, you can click the button below.

Synchronize

Last synchronized: 2021-03-04 08:53:11 GMT+0

If the web browser has an Internet connectivity to reach the public InControl, clicking the button will synchronize the data through the browser's connectivity to InControl automatically.

If the web browser does not have an Internet connectivity, the page will display some on-screen instructions. You will need to copy some encrypted messages from the ICVA and paste it to an InControl page (e.g. over a remote desktop session, email, etc.). The InControl page will let you copy another encrypted message. After you paste the message back to the ICVA page, the synchronization process will be completed.

2. Hardware Appliance

2.1 Accessing Control Panel

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

You can visit the control panel over its **Management port** or **WAN port** from a PC. The unit's management port's IP address is 192.168.5.10 by default. The WAN port IP address is

acquired from a DHCP server by default. You could find its IP address from the LCD panel. (Note that the WAN subnet must not be 192.168.1.0/24, 192.168.5.0/24, and 192.168.30.0/24.)

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

System Settings	
Product	InControl Appliance (Hardware)
Software Version	2.8.4
Serial Number	W334-F3U3-1188
Server Name	<input type="text" value="incontrol.my.domain"/>
Company Name	<input type="text" value="My Company"/>
Service Name	<input type="text" value="My Company InControl"/>
System Admin E-mail Address	<input type="text" value="ica@peplink.com"/>
Tech Support E-mail Address	<input type="text" value="support@peplink.com"/>
Notification E-mail Sender Name	<input type="text" value="My Company InControl"/>
Notification Sender E-mail Address	<input type="text" value="noreply@peplink.com"/>

2.2 License Key

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

License	
Server Name	<input type="text" value="incontrol.my.domain"/>
License Key	<input type="text"/> <input type="button" value="Submit"/>
Max. Allowed Number of Active Devices	100

3. Input E-mail Delivery Settings

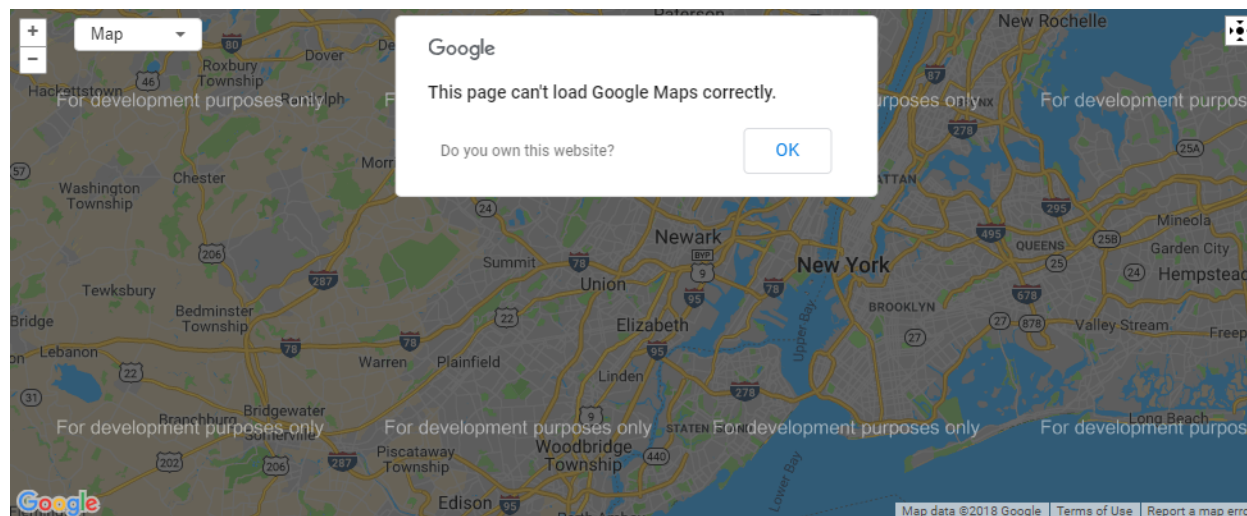
To create new accounts, the system has to be able to send confirmation emails to do account confirmation. So please configure the SMTP server settings, as well as the “Notification E-mail Sender Name” and “Notification Sender E-mail Address” in the System Settings above accordingly.

E-mail Delivery Settings		
SMTP Server	<input type="text" value="smtp.my.domain"/>	
SMTP Port	<input type="text" value="587"/>	
SMTP Username	<input type="text" value="smtp-user"/>	
SMTP Password	<input type="password" value="....."/>	
SMTP Authentication	<input type="text" value="Login (default) ▼"/>	
SMTP TLS Encryption	<input type="text" value="Enabled (default) ▼"/>	
SMTP HELO Domain	<input type="text" value="mydomain.com"/>	
Testing E-mail Address	<input type="text"/>	<input type="button" value="Test"/>
Testing E-mail Delivery Status	Note: Save E-mail Delivery Settings before testing.	

4. Map Settings

Input Google Maps API Key

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



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

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

If you do not want to use Google Maps, you may choose to display maps with the OpenStreetMap. The setting is available at Organization Settings.

OpenStreetMap Settings

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

5. Input FTP/SFTP Archive Server Settings

As a relational database is not good at storing bulky data, historical event log events, GPS locations, and cellular signal data are only kept in the MySQL database for 5 days. Before they are removed from the database, the system will archive the data to the archive server daily if an FTP or SFTP server is configured.

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

Below are data retention periods of various types of data:

Data	Retention period	
	without archive server	with archive server
Per-minute device usage	14 days	

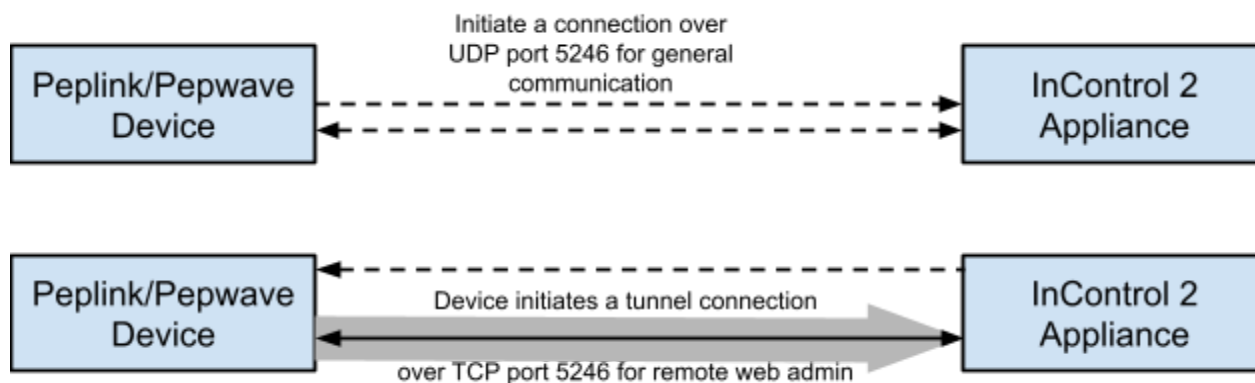
Hourly device usage	2 days	
Hourly client usage	1 month	
Daily client/device usage	60 days	
Monthly device usage	2 years	
Device online/offline history	6 months	
Social network user data	2 years	
Operation log	2 years	
Event log	30 days	1 year
GPS data	5 days	1 year
WAN Quality / Cellular reports	5 days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

6. Facebook App Settings (for Captive Portal)

Please refer to [Appendix 1](#) for how to acquire a Facebook app ID.

7. Setting up Devices to Report to InControl

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

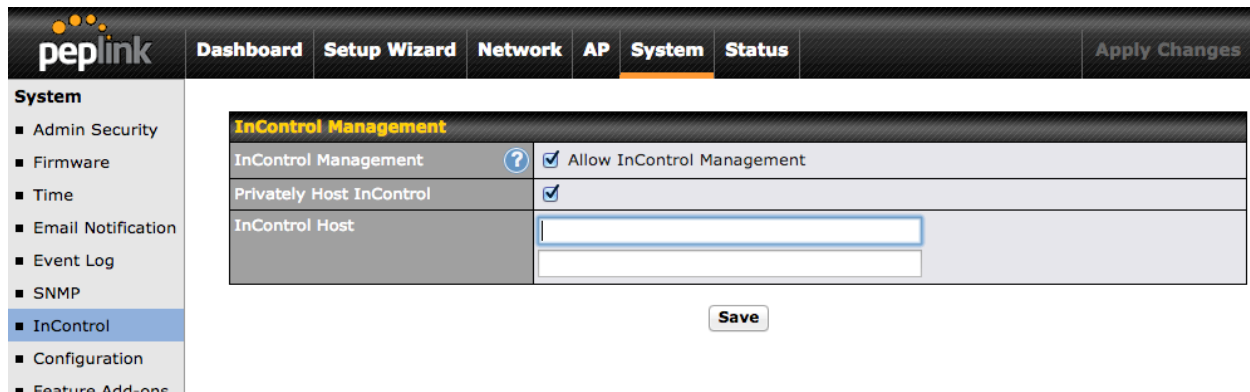


There are two ways to configure your Peplink/Pepwave devices to report to your InControl appliance instead of the Peplink InControl in the public cloud.

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

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

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

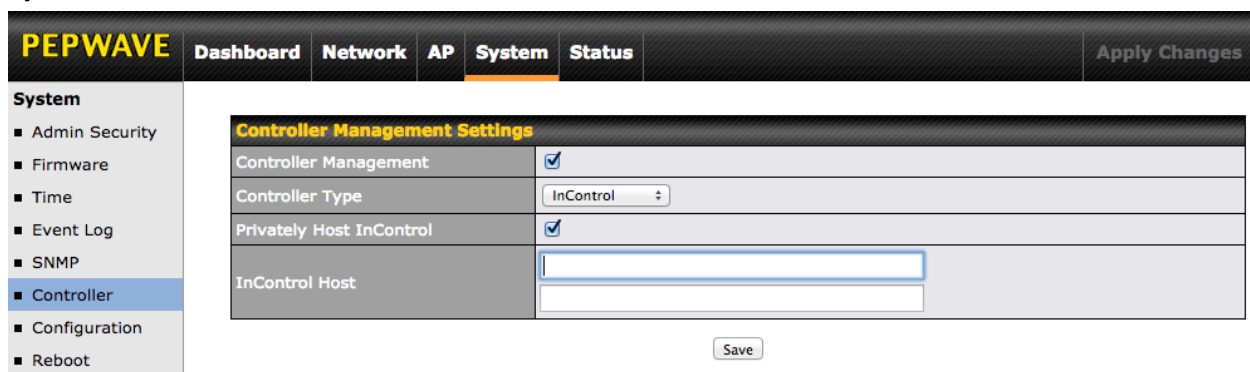


The screenshot shows the Peplink web admin interface. The top navigation bar includes 'peplink', 'Dashboard', 'Setup Wizard', 'Network', 'AP', 'System' (highlighted), and 'Status'. On the left, the 'System' menu is expanded, showing options like Admin Security, Firmware, Time, Email Notification, Event Log, SNMP, InControl (highlighted), Configuration, and Feature Add-ons. The main content area is titled 'InControl Management' and contains the following settings:

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

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

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



The screenshot shows the Pepwave web admin interface. The top navigation bar includes 'PEPWAVE', 'Dashboard', 'Network', 'AP', 'System' (highlighted), and 'Status'. On the left, the 'System' menu is expanded, showing options like Admin Security, Firmware, Time, Event Log, SNMP, Controller (highlighted), Configuration, and Reboot. The main content area is titled 'Controller Management Settings' and contains the following settings:

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

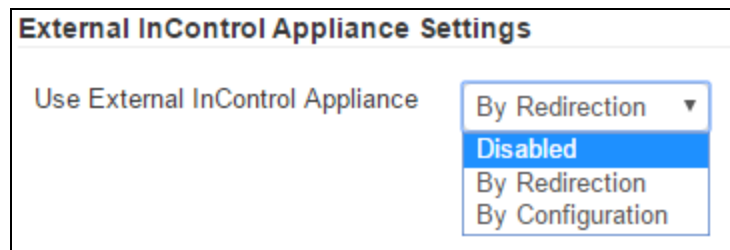
A 'Save' button is located at the bottom right of the configuration area.

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

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

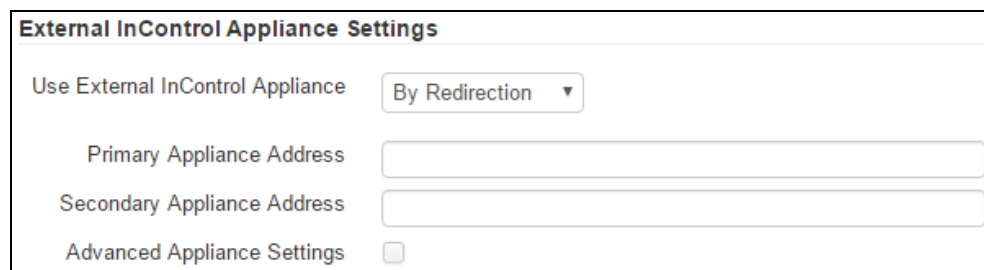
If your devices are accessible to both the Internet and your InControl appliance, you can follow this method. First, sign in to <https://incontrol2.peplink.com/>. Create an organization and a group by following the on-screen instructions. Add your devices to the group. Then go to the group-level **Device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



The screenshot shows the 'External InControl Appliance Settings' section with a dropdown menu open. The dropdown options are: 'By Redirection' (selected), 'Disabled', 'By Redirection', and 'By Configuration'.

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



The screenshot shows the 'External InControl Appliance Settings' form with 'By Redirection' selected. The form includes fields for 'Primary Appliance Address' and 'Secondary Appliance Address', and a checkbox for 'Advanced Appliance Settings'.

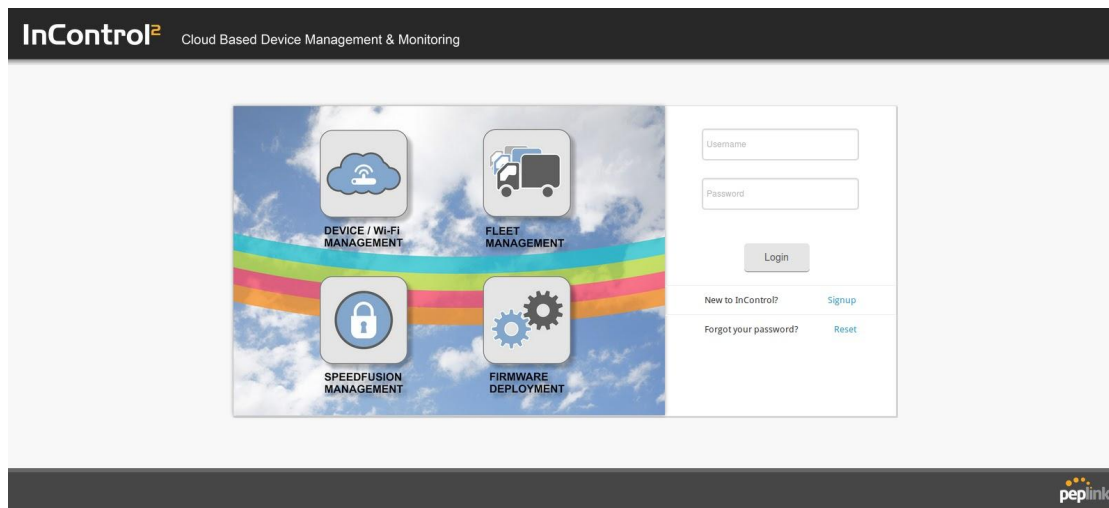
If you choose **By Configuration**, your InControl Appliance address(es) will be saved persistently to your devices. After your devices receive the setting, they will connect to your InControl Appliance directly on startup without connecting to Peplink InControl. The appliance address will be lost if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



The screenshot shows the 'External InControl Appliance Settings' form with 'By Configuration' selected. The form includes fields for 'Primary Appliance Address' and 'Secondary Appliance Address', a checkbox for 'Fail over to Peplink InControl in Public Cloud', and a checkbox for 'Advanced Appliance Settings'. A note is displayed: 'Note: If this field left blank, devices will be configured to connect to Peplink InControl in the public cloud'.

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

8. Logging Into InControl Appliance Web Site

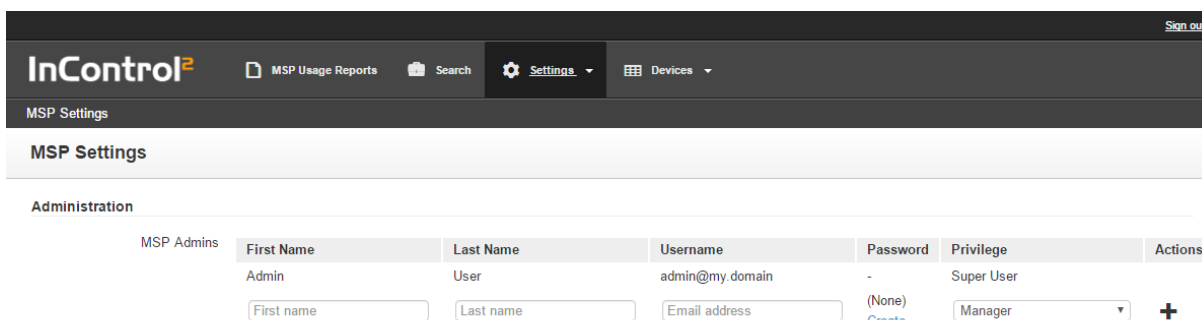


To access the InControl website, you must visit its hostname instead of its IP address. Your PC is required to resolve the hostname into the server IP address. You may add a local DNS record to your PC by editing its “hosts” file. It is “%SystemRoot%\System32\drivers\etc\hosts” for Windows or “/etc/hosts”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

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

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

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



The screenshot shows the InControl 2 web interface. The top navigation bar includes 'InControl²', 'MSP Usage Reports', 'Search', 'Settings' (selected), and 'Devices'. Below the navigation bar, the 'MSP Settings' section is active. Under 'Administration', there is a table for 'MSP Admins'.

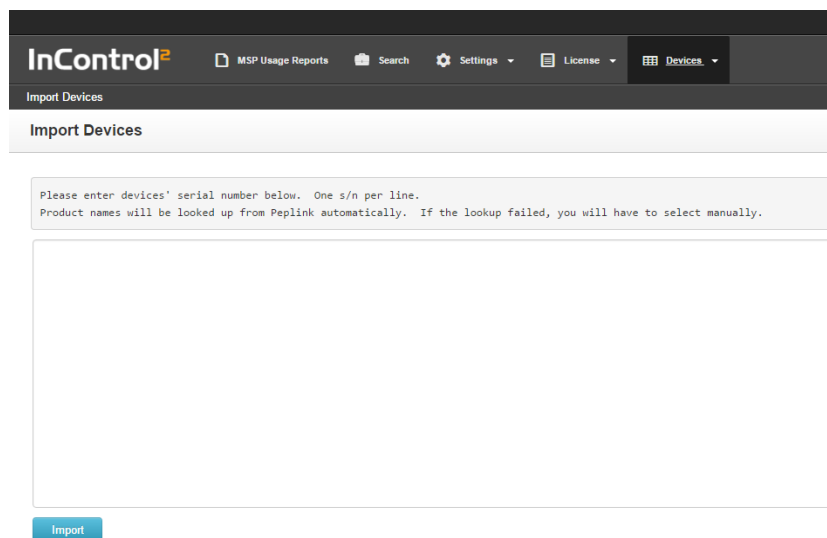
First Name	Last Name	Username	Password	Privilege	Actions
Admin	User	admin@my.domain	-	Super User	
<input type="text" value="First name"/>	<input type="text" value="Last name"/>	<input type="text" value="Email address"/>	<input type="text" value="(None)"/> Create	<input type="text" value="Manager"/>	+

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

9. Importing Devices

Before organization administrators can add devices 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.



The screenshot shows the 'Import Devices' page in the InControl 2 web interface. The top navigation bar includes 'InControl²', 'MSP Usage Reports', 'Search', 'Settings', 'License', and 'Devices' (selected). Below the navigation bar, the 'Import Devices' section is active. A text area for entering serial numbers is shown, with a message: 'Please enter devices' serial number below. One s/n per line. Product names will be looked up from Peplink automatically. If the lookup failed, you will have to select manually.' Below the text area is an 'Import' button.

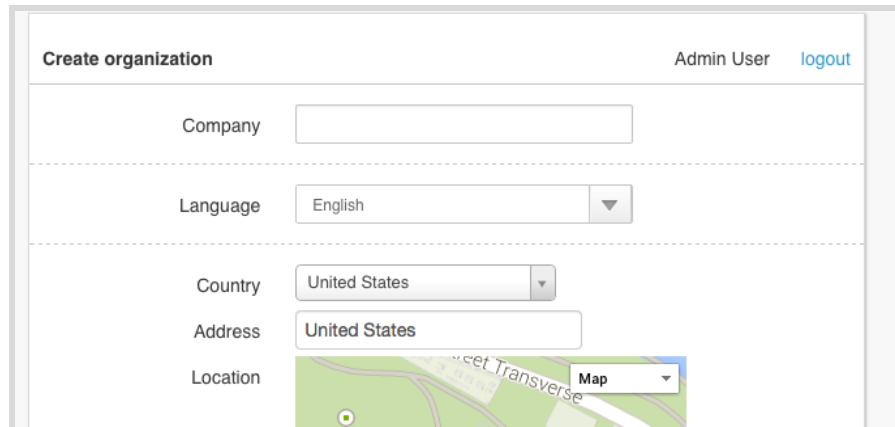
InControl Appliance will attempt to query the Peplink server what products the serial numbers are. If successful, the devices will be imported. If not, you will be prompted to select each device's product name.

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

10. Creating an Organization, Group, and Adding Devices

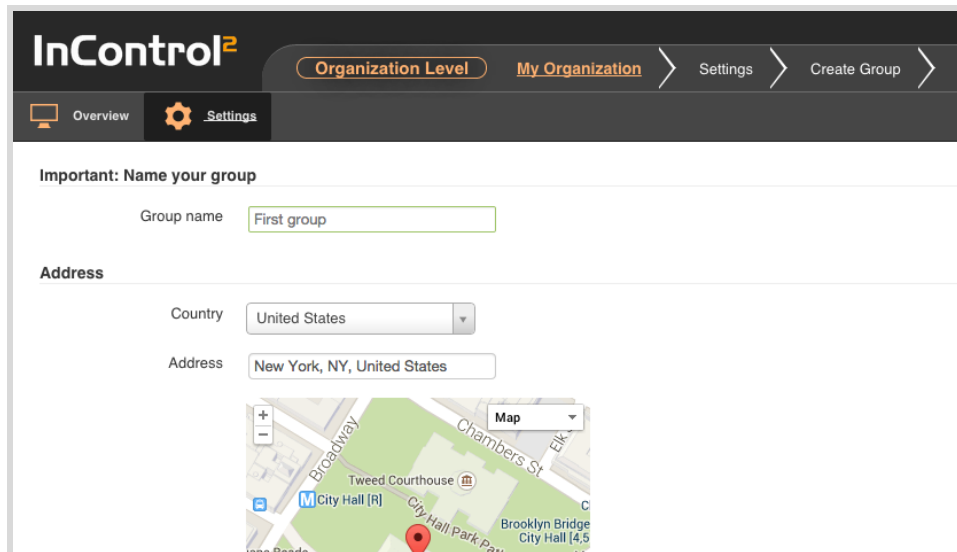
An organization is pre-created which is called “My Organization”. You can find it on the MSP Reports page.

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



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

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



The screenshot shows the 'Create Group' page. At the top, there's a navigation bar with 'InControl²' and tabs for 'Organization Level', 'My Organization', 'Settings', and 'Create Group'. Below the navigation bar, there's a sidebar with 'Overview' and 'Settings' (selected). The main content area has a heading 'Important: Name your group' and a 'Group name' text input field with 'First group' entered. Below that, there's an 'Address' section with a 'Country' dropdown menu set to 'United States' and an 'Address' text input field with 'New York, NY, United States' entered. At the bottom, there's a map input with a 'Map' button. The map shows a street view of New York City with a red pin.

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

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

Add Devices Into Groups

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

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

11. API Access

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

12. Settings on Your Firewall

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

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

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

12.1 For Hardware Appliance's Management Port

Direction	Protocol	Purpose
Inbound	TCP 8000	Non-secure web accesses to control panel (optional)
Outbound	download.peplink.com on TCP 443	ICA firmware download
	UDP 53	DNS resolution for ICA firmware download (not required since 2.8.2)

13. Upgrading InControl Virtual Appliance

13.1 Upgrading a system newer than 2.9.0

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

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

Note: After the firmware is downloaded, it will take about 15 minutes to update the system.

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

Note: After the firmware is downloaded, it will take about 15 minutes to update the system. InControl and database VMs will be restarted.

You can find the firmware URLs from

<https://www.peplink.com/support/incontrol-appliance-images-downloads/>

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

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

13.2 Upgrading a system earlier than 2.9.0

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

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

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

13.2.1 For VMware ESXi

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

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

The extracted file names and sizes are as follows:

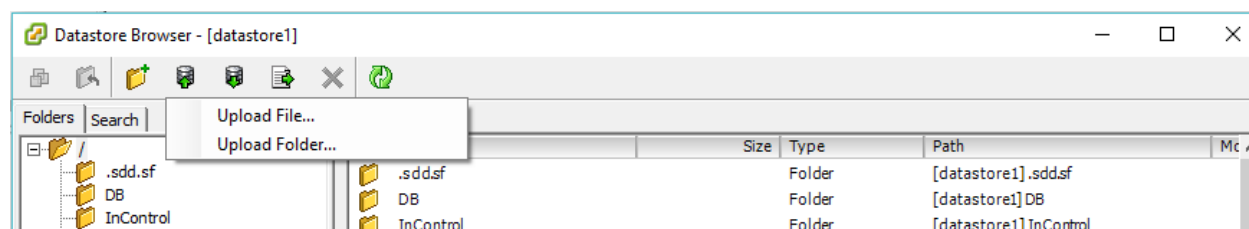
InControl-System-2.9.0.2-vmrk.tgz:

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

DB-System-20210323-vmrk.tgz:

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

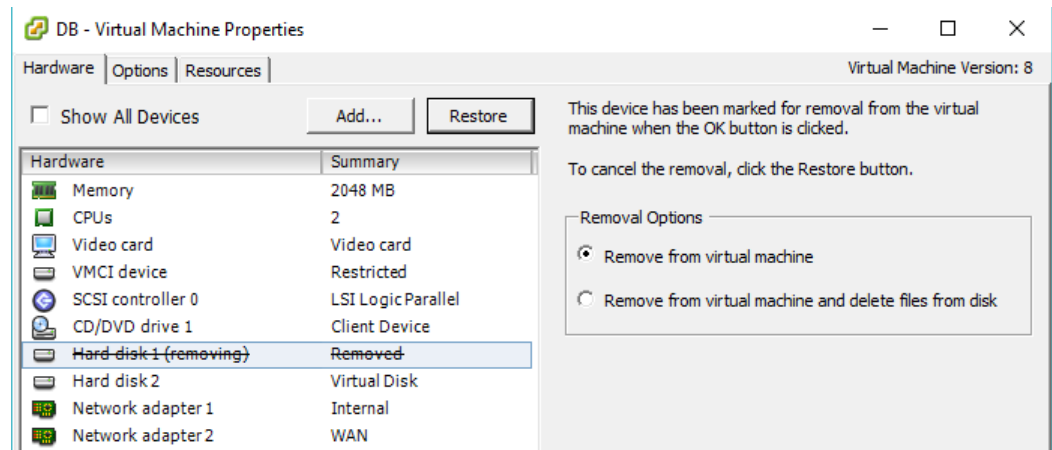
Step 3. Start the Datastore Browser in the vSphere Client. Use it to upload the InControl-System*.vmrk and DB-System-*.vmrk files to folders, say, “InControl” and “Database” in the datastore respectively. After finishing uploading the two files, the two files will be shown as one item in the Datastore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



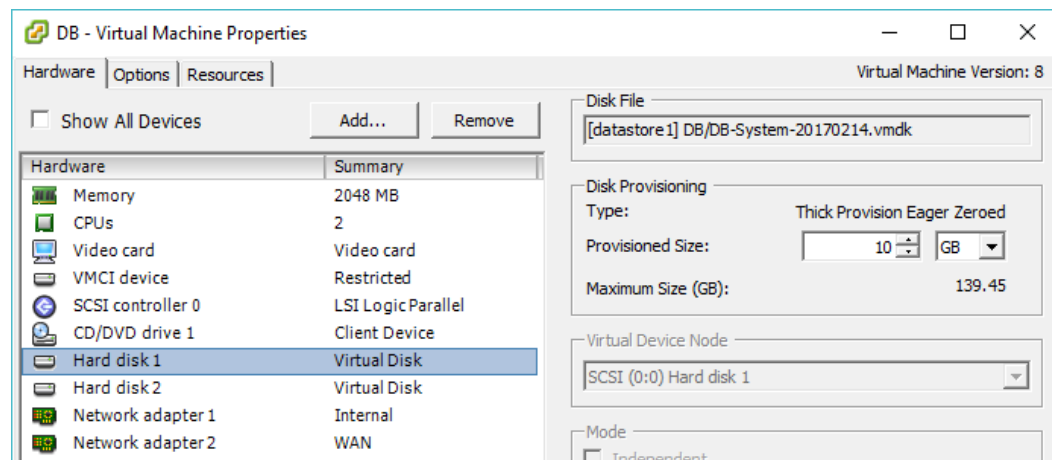
Step 4. Restart VMs in the following order:

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"

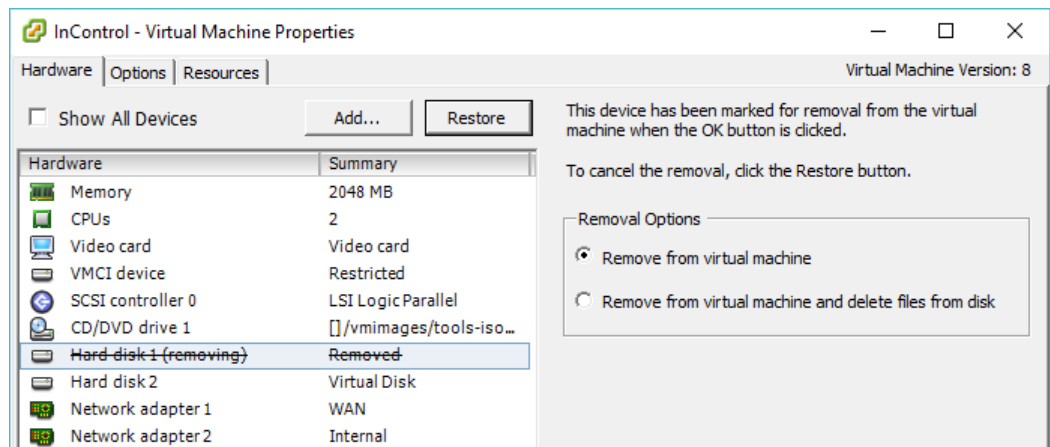


4. Open DB VM Properties again
 - Select 'Add...' > "Existing virtual disk..." > Browse and select the disk file "DB-System-20210323.vmdk"
 - Select SCSI 0:0 Hard disk as the Virtual Device Node



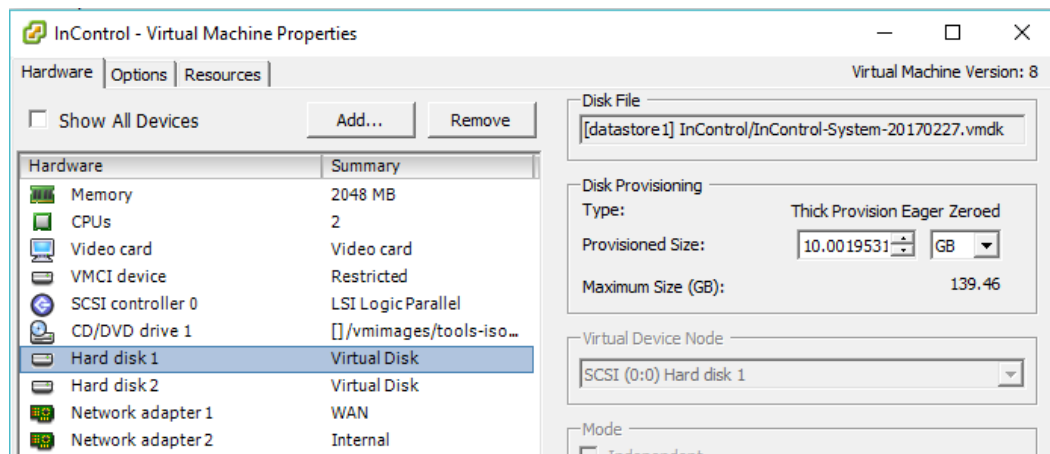
5. Start DB VM
6. Open InControl VM Properties
 - Identify and select the system hard disk (usually "Hard disk 1")
 - Select the "Remove from virtual machine" radio button (without deleting it)

- 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

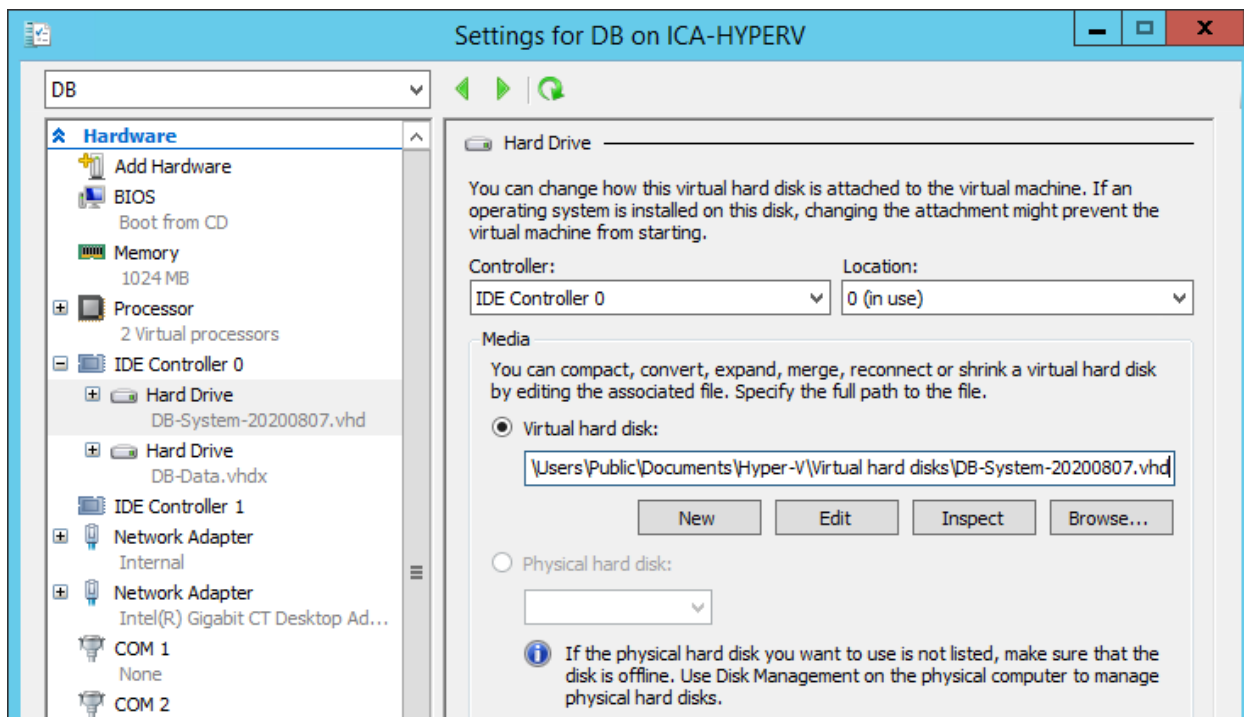
Step 1. Download the Virtual Appliance 2.9.0.2 and Database Server 202103223 image files in .vhd format from <https://www.peplink.com/support/incontrol-appliance-images-downloads/>

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

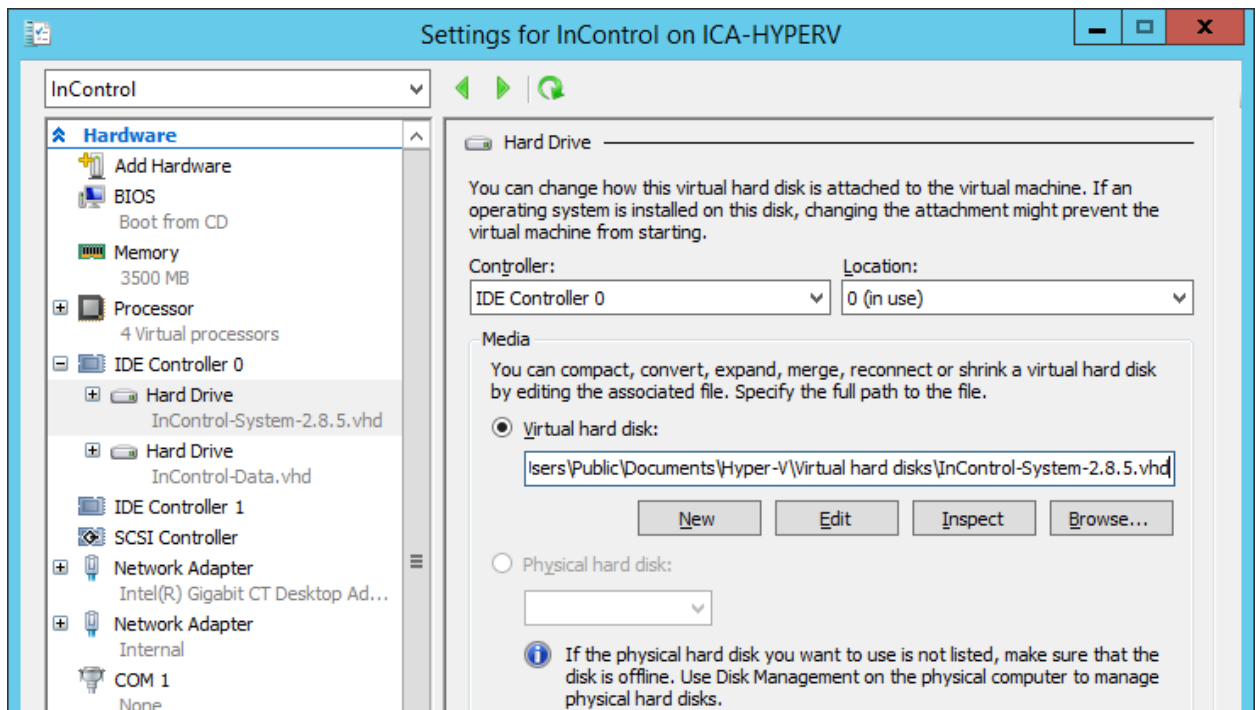
File name	Size (Bytes)
InControl-System-2.9.0.2.vhd	25,035,800,576
DB-System-20210323.vhd	25,035,800,576

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.vhd file. The "Location" for IDE Controller should be 0.



4. Start DB VM.
5. Open InControl VM settings. Identify and select the system hard disk.
Replace the virtual hard disk with the newly downloaded
InControl-System-2.9.0.2.vhdx file. The "Location" for IDE Controller
should be 0.



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

14. Upgrading InControl Hardware Appliance

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

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

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

Note: Upgrading firmware will take about 25 mins.

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

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

15. Release Notes

Release notes for 2.13.1

What's new

- When changing password, users cannot pick the last 10 used passwords.
- InTouch
 - Web-based InTouch: add two compatibility options.
 - InTouch profiles can be accessible by some InTouch users only.
- Reports
 - Wi-Fi Report > SSID Usage: added per-SSID client usage.
 - Group-level Usage Reports > Daily: clicking a date will show per-device per-WAN usage.
 - Daily usage reports: the date range changed from 32 to up to 45 days.
 - Performance Test: location and speed data are now recorded in test results.
- Custom map markers can be uploaded on the Organization and Group Settings screen. They can be chosen for devices' markers in Device Details > Edit screen.

- Added group-level operation log. Available to group administrators too.
- Outbound Firewall Rules: added a checkbox option for including router-generated traffic.
- The organization and group level option “Auto Update Captive Portal SSL Certificate” has been reset to disabled. Users will need to manually enable it. Balance and MAX firmware 8.4.1 or above are now required.
- Improved eSIM activation status report.
- Added display of live vehicle status data collected from OBD-II interface on Device Details.
- Added support for multiple subnets in the LAN_NETWORK_LIST field to group-level Device IP Settings.

Release notes for 2.13.0.2

What's new

- Fixed: system could not boot up on NVME-based storage
- Implemented an HTML5 cross-origin resource sharing (CORS) policy that allows accesses from its own server name only.

Release notes for 2.13.0.1

What's new

- Fixed device date synchronization
- Fixed update of web admin SSL certificate
- Fixed Startlink and Wi-Fi mesh event logging
- Fixed outbound policy
- Fixed SSID usage report.
- Updated the diagnostic reports.

Release notes for 2.13.0

What's new

- Supported running on Azure. (Installation guide is to be updated.)
- Auto GPS follow (31138)
- Added Starlink support. For supported models, if Starlink support is enabled on the WAN Settings page on the web admin, the Device Details screen will display any Starlink status and controls.
- Added options to Group and Organization Settings to allow viewers to see all settings.
- If a FusionHub license becomes invalid due to some changes on the virtual machine, administrators are allowed to renew its license without reinstalling the FusionHub.

- Captive portal: added support of bandwidth limit after data quota reached for the remaining time quota.
- When creating a group, group-level settings can be cloned from an existing group.
- When creating an organization, two-factor authentication will be required for all users by default.
- Inbound Firewall rules: added SaaS to the Source drop-down menu.
- Outbound Policy rules: added "Access Control List", "Client Type" and "Client Associated SSID" to the Source drop-down menu.
- On the User Organizations page, users can remove themselves from an organization or group.
- Connection tests: logging and notifications can optionally be enabled when a test fails.
- Added support of applying an eSIM activation code.
- Added support of displaying LoRaWAN status in Device Details.
- Device-level per-minute bandwidth and usage report: added a button to export the report as an image.
- Device Details > Map: supported to "Download as GPX" for a date range.
- AP-controller-managed devices' details screen: added a hyperlink to the controller's Remote Web Admin page.
- Notifications: added Starlink and High System Temperature.
- InTouch SSH profile: a warning is displayed if the key is not passphrase protected.
- SIM pool: added carrier quota settings to "All Carriers".
- Clients: added CSV file download.
- Added advanced group and organization firmware update schedule settings for higher flexibility.
- Added Netflow settings to Device System Management.
- When disabling Email Notifications, subscription settings are now preserved.
- Devices' routes are now shown on Device Details pages and can be searched by IP address on the "User Organizations" page.
- Added custom handshake port option for manually added devices in SpeedFusion configurations.
- If APs are connected to a router that is with GPS location data, the APs will appear at the same location as the router on the map. (Requires Balance/MAX firmware 8.4.1 or above and AP firmware 3.9.4 or above.)

Release notes for 2.12.1.3

What's new

- Added Starlink support. Supported gathering information from Starlink dishes that are connected to Peplink's Ethernet WANs. Supported stowing, unstowing, and rebooting the dishes.
- Added WAN over VLAN support to Connection Tests.
- Added a "Security" option in InTouch RDP profiles.

- Fixed auto certificate management
- Fixed DHCP reservation configuration
- Fixed: devices' uptimes sometime are not shown or are outdated.
- Fixed domain validations in Firewall Rules > Content Blocking.
- Fixed WAN up/down history in CSV format
- Added Detailed Engineering Data in Cellular WANs.
- Captive portal: quota reset logic for guest accounts.
- External captive portal: added support for authenticating guests with the HotspotSystem and an LDAP server.

Release notes for 2.12.1

What's new

- The organization-level option "Show Service Expiration Dates and Notices to non-MSP users only" now applies to organization and group users only. MSP users can always see the dates and notices.
- Fixed: did not synchronize time only with the configured time server.
- Device Details:
 - In the Configuration Backup table, you can now apply a configuration backup back to the device by simply clicking an "Apply" button.
 - Routes are now shown on Device Details.
 - For SD Switches, added "Bridge ID" and "Root ID".
 - Added Synergy mode support.
- Device Details > Map:
 - added support to display the GPS location in a day range.
 - added an option to change markers to half-size.
- Added group-level Certificate Management for SpeedFusion/IPsec VPN, Web Admin, Captive Portal, MediaFast, OpenVPN, and LoRaWAN.
- The map on the WAN quality reports now respects the "Follow GPS location" setting.
- SIM pool: added weekly bandwidth quota.
- SpeedFusion VPN configuration:
 - Improved error messages.
 - Multiple users can now edit unrelated profiles.
 - Disabled profiles no longer block device re-use in active profiles.
 - Improved UI allows users to see which profiles have been edited and are not yet saved/deleted.
 - Added TCP Ramp Up support. (requires firmware 8.3)
 - Fixed: "Send all Traffic to Hub" was not selecting the primary tunnel when multiple sub-tunnels were active.

- Client Details of SD Switches: added per-VLAN usages.
- Client Details of Balance/MAX: add hourly client usage.
- Logging settings: added support for multiple profiles and device selection.
- Added LoRaWAN configuration support.
- LAN Network Settings > Bonjour Forwarding: now profiles of the same Service Network Name but different Service Network Type, Client Network Type, and Client Network Name are now allowed.
- Added notification type "Configuration Rolled Back".
- SSID Profiles: added support of "Radius MAC Authentication", "Radius Source Network Address", and WPA 3 Enterprise (requires firmware 8.3).
- The Clients table's columns are now customizable.
- Captive portal profile
 - Increased the font size of the Check box and Connect button labels.
 - Split the "General Button and Link Color" setting into two.
 - Added title text font size and style customization.
- Device System Management: disallowed some web admin port values that modern web browsers do not allow or support.
- Device-level Internet and Device Availability figures can now be downloaded as CSV.
- Added a Remote Assistance option for turning it off automatically after a number of days. (requires firmware 8.3).
- Device list: improved the responsiveness for long device listings.
- Fixed: IP addresses in Switch port details > Clients were sorted in alphabetical order, not sorted in the IP-address way.
- Pressing the ESC key on any popup now closes the popup.

Release notes for 2.12.0

What's new

- Added support of syncing device expiration dates in air-tight network environments.
- MSP > Search: added device search by an ICCID/IMSI
- Organization Settings
 - Security: added an option for choosing which users are allowed to make API calls to the organization.
 - Warranty and Subscription Renewal Reminders can not only be sent to users but also to specified email addresses as well.
 - For uploaded logos in PNG format and with a transparent background, a background color can now be chosen.
 - Organization Administrators can no longer make changes to Super Organization Administrators.

- Organization listing screen that is shown after logging in (for users with access to multiple organizations):
 - Search results can now be downloaded as a CSV file.
 - For group users, the organization name is now linked to a page that lists all accessible groups.
- Group Settings:
 - Organization Administrators can now control the visibility or editability of some settings to Group Administrators.
 - Added a group-level user role "InTouch User". InTouch users are allowed to use the InTouch services to access InTouch-enabled client devices only.
- Group creation: added an option to include device tags in cloning settings.
- Device listing: devices can now be filtered by WAN types.
- Device Details:
 - Inactive SIMs can now be made active in their icon tooltip.
 - Wi-Fi Mesh SSIDs are now displayed.
- Firmware can now be applied to devices that have never been reported online.
- SpeedFusion VPN:
 - PepVPN is now named "SpeedFusion VPN".
 - Fixed: after moving a device from one group to another in the same organization, all topology profiles were created as organization-level even if they are also in the same group.
 - Added group-level SpeedFusion VPN route isolation settings.
- SIM pools:
 - Added pause buttons to SIM pools. Pressing a button will stop using the SIM cards in the pool to route user traffic.
 - Added daily and yearly quota support.
- VLAN Networks:
 - Added DHCP Reservation settings.
 - Networks can now be cloned.
- Firewall Rule Sets: added "Content Blocking" settings.
- Firewall log: more than 100,000 entries can now be displayed.
- Device System Management: added Event Log settings.
- Captive Portal Settings > E-mail Access Mode, add an optional field "Allowed E-mail Domains".
- Captive portal reports: added a "Client Types" report.
- SD Switch:
 - Added "Loop Protection" settings to port levels.
 - In the port listing, editing multiple ports' settings on one screen is supported.
- Connection Up/Down History: added monthly connection availability figures.
- Per-minute reports: added SIM-slot/type selection (require firmware 8.3.0).
- InTouch SSH profiles: the username field now becomes optional.
- In creating/editing Connection Test profiles, WAN names are auto-suggested.
- System Tools > "WAN Performance Analysis Server": WAN addresses are now displayed.

- Added IoT product support.
- Improved the speed of adding many serial numbers at once.

Release notes for 2.11.2

What's new

- On the Device Details pages, modules' product code is now displayed.
- Fixed a bug with the bulk configurator. The help texts for the "Preserve..." settings have been revised.
- Added an HTTP-POST-based API for updating InControl Appliance's web server SSL certificate. See [https://\[ICA_ADDR\]:4443/cert.cgi](https://[ICA_ADDR]:4443/cert.cgi).
- Fixed a system stability issue that might occur every 6 hours. The more online devices a system has, the higher chance the issue might occur.
- Fixed: RDP, VNC, SSH, and Telnet-based InTouch connections could not establish.
- Fixed a stability issue with ICA for GCE that has been enabled with auto SSL certificate renewal.

Release notes for 2.11.1

What's new

- The user interface for updating cellular module firmware has been enhanced. You may initiate an update by going to a device list, selecting devices, clicking the Actions menu, and selecting "Update cellular module firmware..."
- Added a new group-level user role called "InTouch". InTouch users can see InTouch devices and access them only.
- Captive portal: supported sending OTP codes with SMS using Twilio Verify.
- Device details:
 - SIM icons are added to cellular WANs to indicate which SIM cards are detected and being used.
 - Labels are added to indicate whether outbound policy and firewall rules are being managed by InControl.
 - In case no signal information can be displayed for cellular WANs' SCC2 band, a tooltip is added to explain.
- On group-level event log pages, a "Log Archive Download" link is added for downloading the log archive of all devices in the group.
- Connection up/down history: all up and down time stamps are linkified. Clicking them will open the corresponding event log messages in a new browser tab.
- In defining an AWS Transit Gateway connection, its ASN is now user-definable and is no longer fixed to a predefined value.
- Because of a software error, some groups' firmware policies saved before early this year were not actually saved. Their firmware management option is now disabled. On the

organization-level firmware policy page, if any groups are affected, they will be listed in the section “Group-level Policies Need to be Reviewed”.

- Fixed: When moving groups to an organization, users were not inherited.

(The followings are the changes of 2.11.0. No firmware 2.11.0 had been released.)

- Added Connection Test: users can now schedule SpeedTest, HTTP download tests, and ping tests over devices’ wired/wireless WAN or OpenVPN connections. See group-level “Network Settings” and “Reports” menus. Require firmware 8.3.0 and 3.9.3 or above for Balance/MAX and AP One respectively.
- Added USB-to-serial adapter support to serial-port-based InTouch. Require firmware 8.3.0 or above.
- Added support of automatic renewals of default captive portal SSL certificate without needing to update firmware from time to time. See the group-level Device System Management screen. Require firmware 8.3.0 and 3.9.3 or above for Balance/MAX and AP One respectively.
- Added DHCP relay settings in VLAN Networks for Balance, MAX, and AP One in router mode.
- Added a column “IP Settings for Balance, MAX, and AP One” to the VLAN Networks table.
- In creating a group, added a cloning option for notification settings.
- In notification settings, added an option for including devices’ notes in online/offline emails.
- Allow configuring the “Follow another device’s GPS location...” setting for multiple selected devices on the device management screen.
- Organizations on the “My organizations and groups” screen can now be sorted in a few new ways.
- Added an organization-level device management screen for organization viewers.

Release notes for 2.10.0

What’s new

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

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

- In captive portal profiles, you can now optionally put one of three special variables to the “General Description” field. The variables’ values defined in the control panel will be displayed in the General Description field on the captive portal login page. This feature is for displaying a time-limited notice in all captive portals in the system without needing to modify every single captive portal profile every time. (InControl virtual appliance only.)

Release notes for 2.9.4.1

What’s new

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

Release notes for 2.9.4

What’s new

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

Release notes for 2.9.3.2

What’s new

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

Release notes for 2.9.3.1

What's new

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

Release notes for 2.9.3

What's new

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

Release notes for 2.9.2.2

What's new

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

Release notes for DB-2021215

Here are the changes since DB-20210323:

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

Release notes for 2.9.2.1

What's new

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

Release notes for 2.9.2

What's new

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

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

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

Release notes for 2.9.1.5

What's new

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

Release notes for 2.9.1.4

What's new

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

Release notes for 2.9.1.3

What's new

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

Release notes for 2.9.1.2

What's new

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

Release notes for 2.9.1.1

What's new

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

Release notes for 2.9.1

What's new

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

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

Release notes for 2.9.0.6

What's new

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

Release notes for 2.9.0.5

What's new

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

Release notes for 2.9.0.4

What's new

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

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

Release notes for 2.9.0.3

What's new

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

Release notes for 2.9.0.2

IMPORTANT

This release requires Database VM version 20201214 or above.

What's new

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

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

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

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

Release notes for DB-20210323

Here are the changes since DB-20201013:

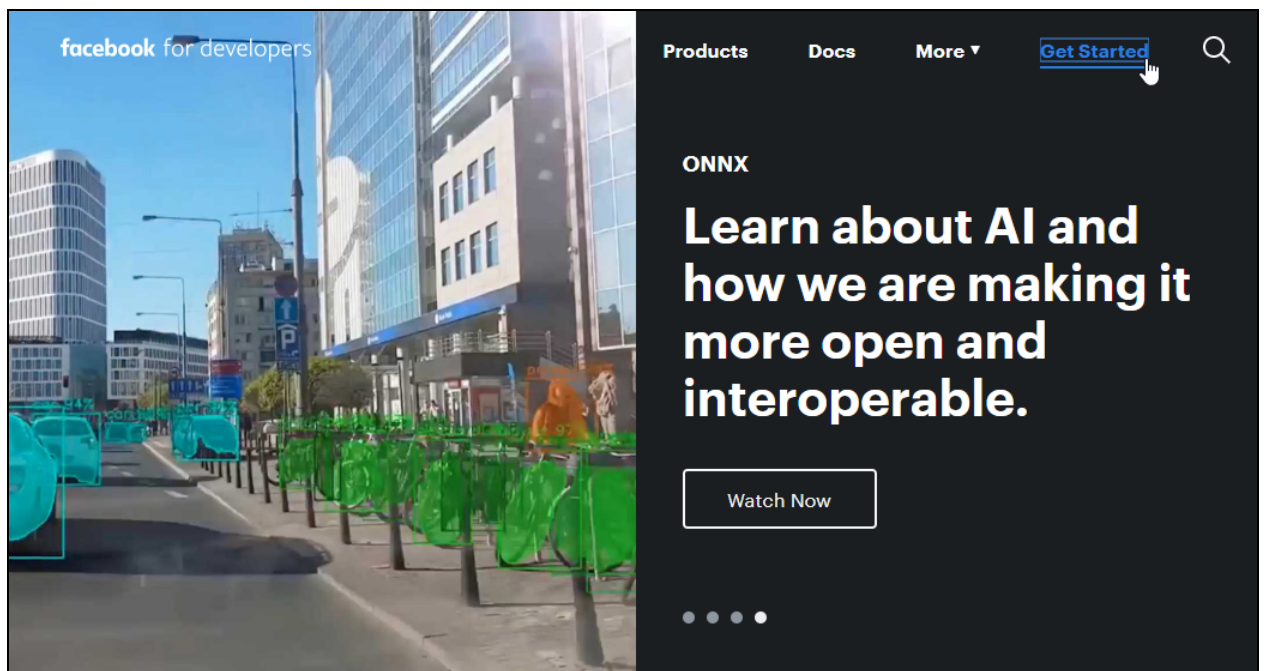
- Both InControl and Database VMs support could be upgraded by issuing a firmware URL to the InControl VM's control panel since the next release. No system disk image replacement on the hypervisor will be required.
- Added support of running on Amazon Web Services and Google Compute Platform.

Appendix 1: Procedure for creating a Facebook App ID

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

Below is a procedure for Facebook app ID creation:

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



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

×


1 Register

2 Verify

3 First App

4 Tell Us About You

Welcome to Facebook for Developers



Create a Facebook for Developers account

Next

By proceeding, you agree to receive marketing related electronic communications from Facebook, including news, events, updates, and promotional emails. You may unsubscribe at any time in Developer Settings.

✓ Register — 2 Verify — 3 First App — 4 Tell Us About You

×

Verify your account

Use your phone number to verify your account.?

Country

United States (+1) ▾

Phone Number

123456789

Get Confirmation Code

Send as Text

Send via Phone Call

Confirmation Code

Enter Confirmation Code

Verify

You can also verify your account by [adding a credit card](#)

✕

✓ Register

✓ Verify

3 First App

4 Tell Us About You

Welcome to Facebook for Developers

Lets get started with your first app

App Name

My first app

You can change the name now or later

Contact Email

peplink@gmail.com

Used for important updates about your app

By proceeding you agree to the Facebook Platform Policy and the Facebook Data Policy.

Next

✓ Register — ✓ Verify — ✓ First App — 4 Tell Us About You

Which of these best describe what you do

</>

Developer

📊

Analyst

🎓

Student

🏷️

Marketer

💼

Product Manager

👤

Other

🔗

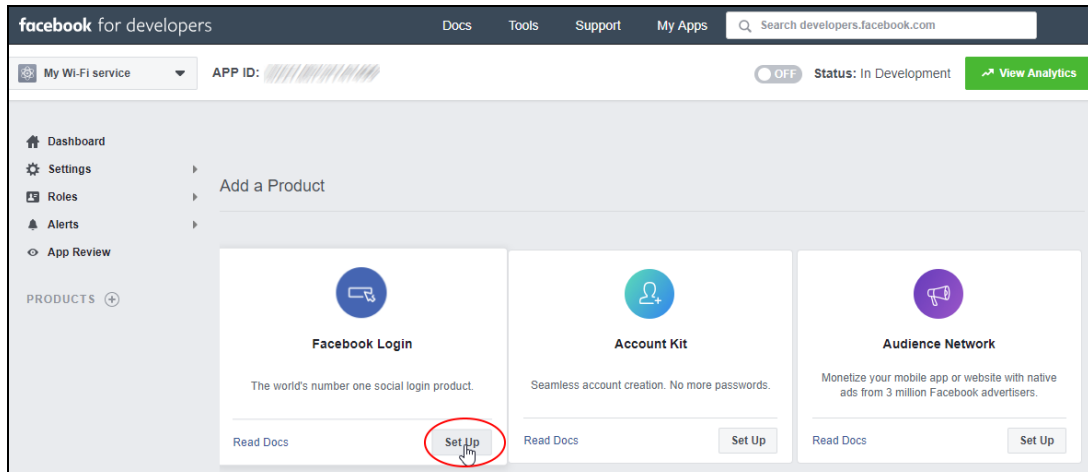
Owner/Founder

Welcome to your Facebook for Developers Dashboard

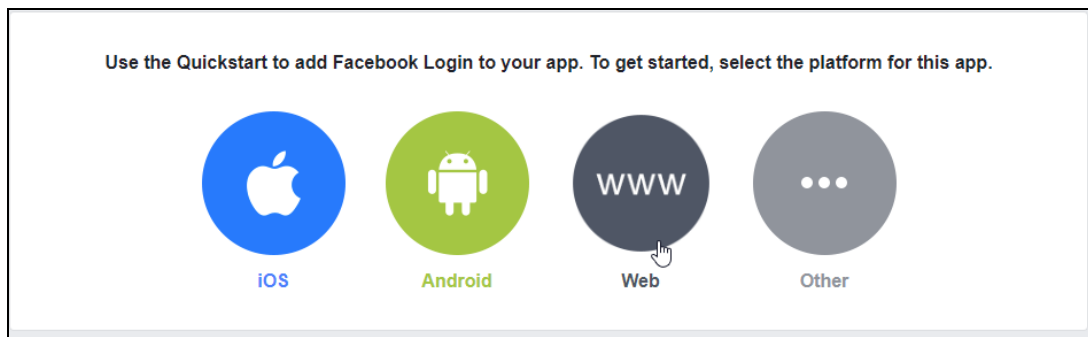
Your app dashboard is where you can get an overview of your app, edit app settings, and configure new products.

Add Your First Product

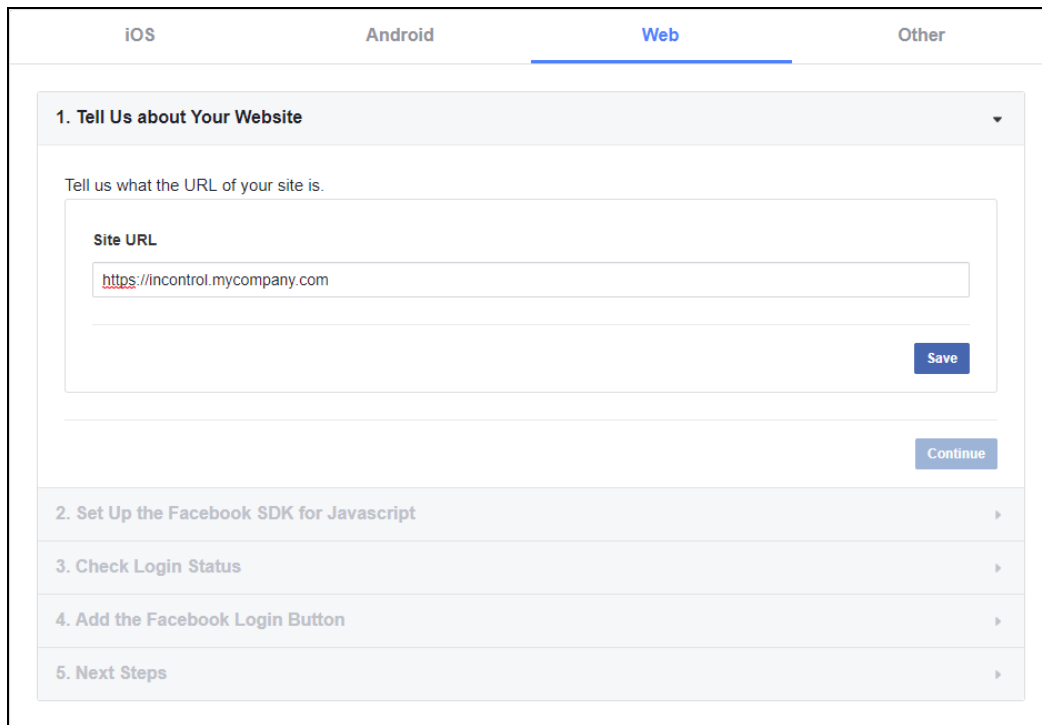
3. Click the “Set Up” button on the “Facebook Login” control



4. Click “Web”



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



iOS Android **Web** Other

1. Tell Us about Your Website

Tell us what the URL of your site is.

Site URL

<https://incontrol.mycompany.com>

Save

Continue

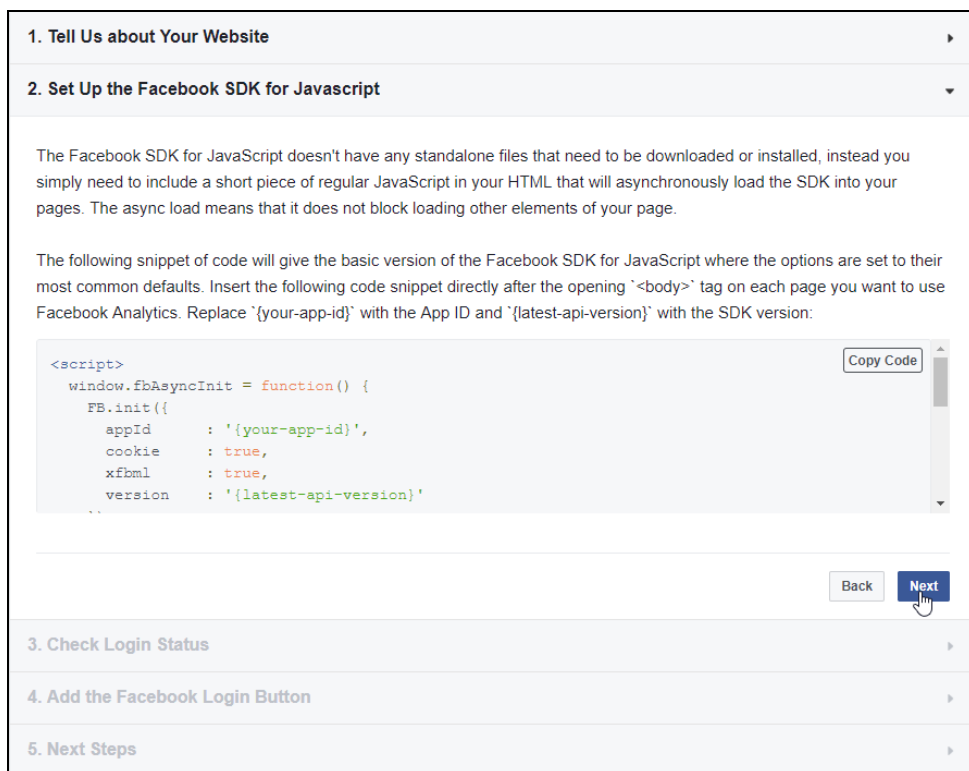
2. Set Up the Facebook SDK for Javascript

3. Check Login Status

4. Add the Facebook Login Button

5. Next Steps

6. Click "Next".



1. Tell Us about Your Website

2. Set Up the Facebook SDK for Javascript

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

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

```
<script>
window.fbAsyncInit = function() {
  FB.init({
    appId      : '{your-app-id}',
    cookie     : true,
    xfbml     : true,
    version    : '{latest-api-version}'
  });
};
(function(d, s, id) {
  var js, fjs = d.getElementsByTagName(s)[0];
  if (d.getElementById(id)) return;
  js = d.createElement(s); js.id = id;
  js.src = '//connect.facebook.net/{latest-api-version}/sdk.js';
  fjs.parentNode.insertBefore(js, fjs);
}(document, 'script', 'facebook-jssdk'));
```

Copy Code

Back Next

3. Check Login Status

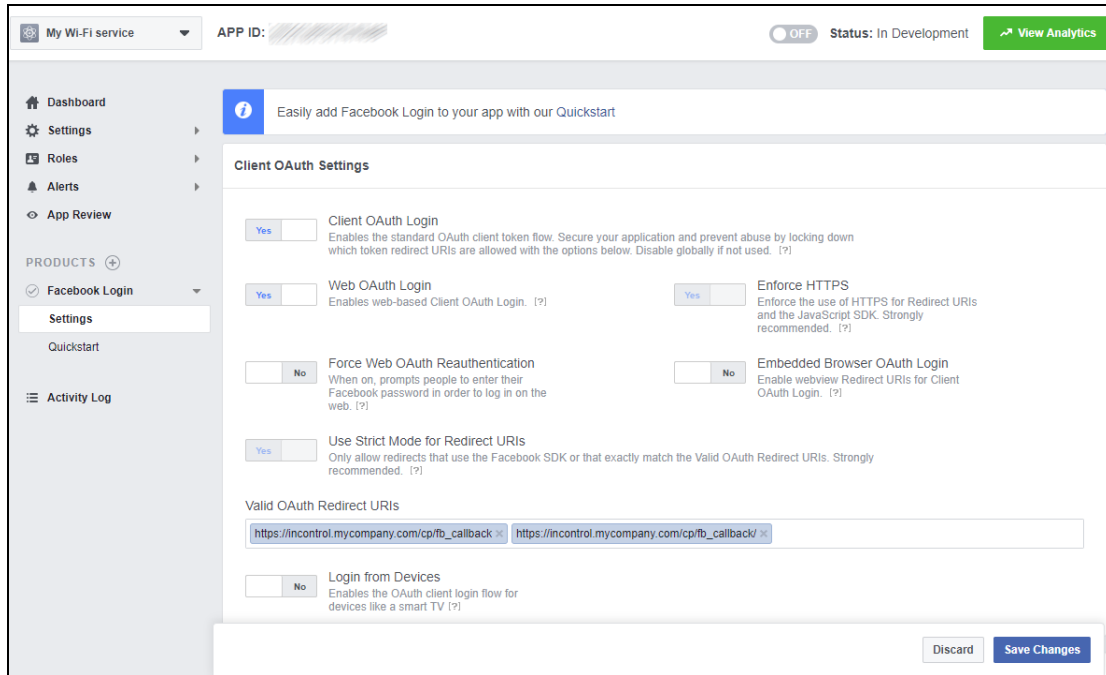
4. Add the Facebook Login Button

5. Next Steps

7. Input the following URLs into the “Valid OAuth Redirect URIs” field:

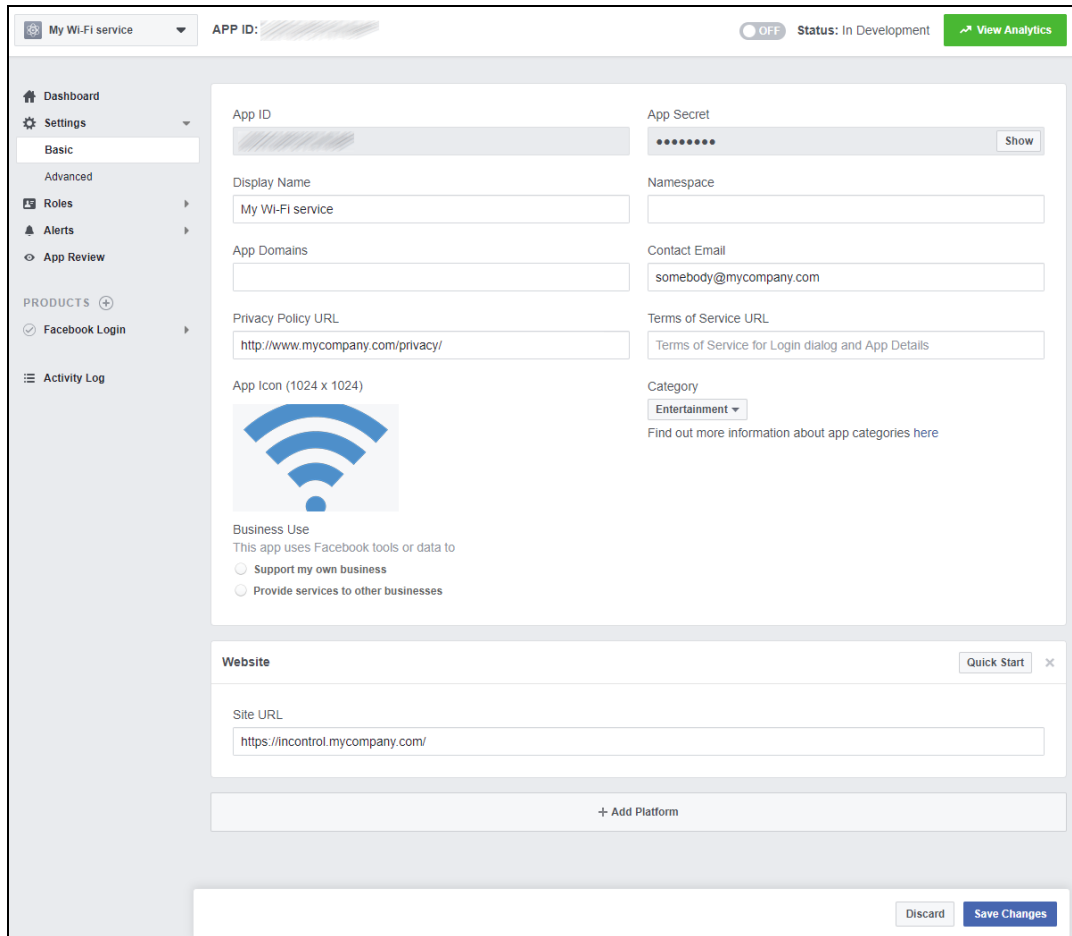
`https://[InControl_URL]/cp/fb_callback` and

`https://[InControl_URL]/cp/fb_callback/`



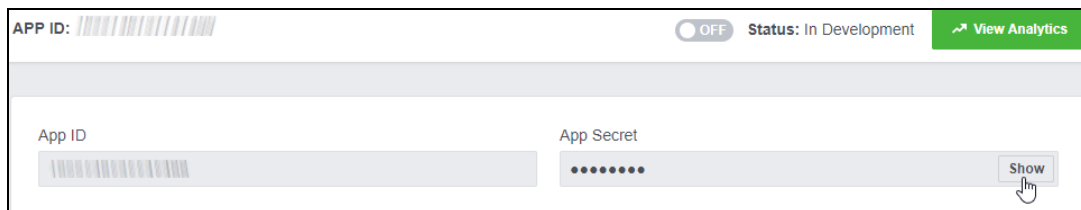
The screenshot shows the 'Client OAuth Settings' page for a Facebook Login integration. The left sidebar contains navigation links: Dashboard, Settings, Roles, Alerts, App Review, and a PRODUCTS section with Facebook Login (selected), Settings, Quickstart, and Activity Log. The main content area has a top bar with 'My Wi-Fi service', 'APP ID', a toggle switch (OFF), 'Status: In Development', and a 'View Analytics' button. Below this is an information banner about adding Facebook Login. The 'Client OAuth Settings' section includes several toggle switches: 'Client OAuth Login' (Yes), 'Web OAuth Login' (Yes), 'Enforce HTTPS' (Yes), 'Force Web OAuth Reauthentication' (No), 'Embedded Browser OAuth Login' (No), 'Use Strict Mode for Redirect URIs' (Yes), and 'Login from Devices' (No). Each toggle has a descriptive text and a help link. At the bottom, the 'Valid OAuth Redirect URIs' field contains two entries: 'https://incontrol.mycompany.com/cp/fb_callback' and 'https://incontrol.mycompany.com/cp/fb_callback/'. At the very bottom right are 'Discard' and 'Save Changes' buttons.

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



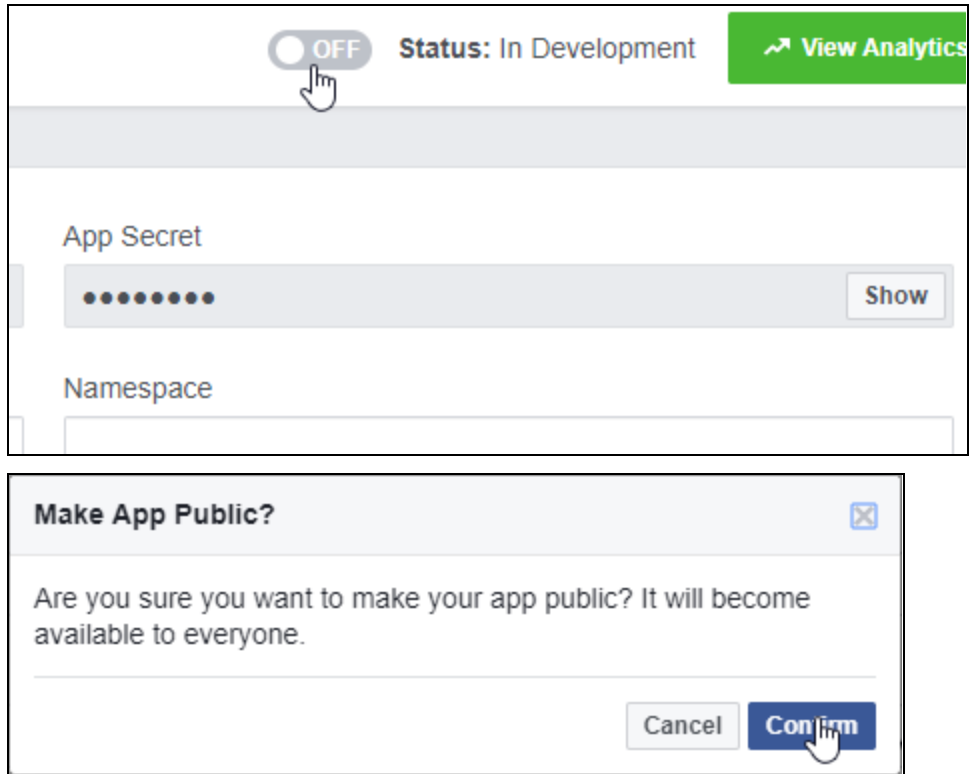
The screenshot shows the Facebook App Settings page for an application named "My Wi-Fi service". The page is divided into several sections. At the top, there's a header with the app name, a status toggle (OFF), and a "View Analytics" button. Below this, the "App ID" and "App Secret" fields are visible, with the App Secret field having a "Show" button. The main settings area includes fields for "Display Name" (filled with "My Wi-Fi service"), "Namespace", "App Domains", "Contact Email" (filled with "somebody@mycompany.com"), "Privacy Policy URL" (filled with "http://www.mycompany.com/privacy/"), "Terms of Service URL" (filled with "Terms of Service for Login dialog and App Details"), and "App Icon (1024 x 1024)" (showing a Wi-Fi icon). There's also a "Business Use" section with two radio buttons: "Support my own business" (selected) and "Provide services to other businesses". At the bottom, there's a "Website" section with a "Site URL" field (filled with "https://incontrol.mycompany.com/"). The page ends with "Discard" and "Save Changes" buttons.

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



This screenshot is a close-up of the top section of the Facebook App Settings page. It shows the "APP ID:" field with a long alphanumeric string, the "App ID" field with the same string, and the "App Secret" field with a masked string of dots. A mouse cursor is clicking the "Show" button next to the App Secret field. The status toggle (OFF) and "View Analytics" button are also visible at the top right.

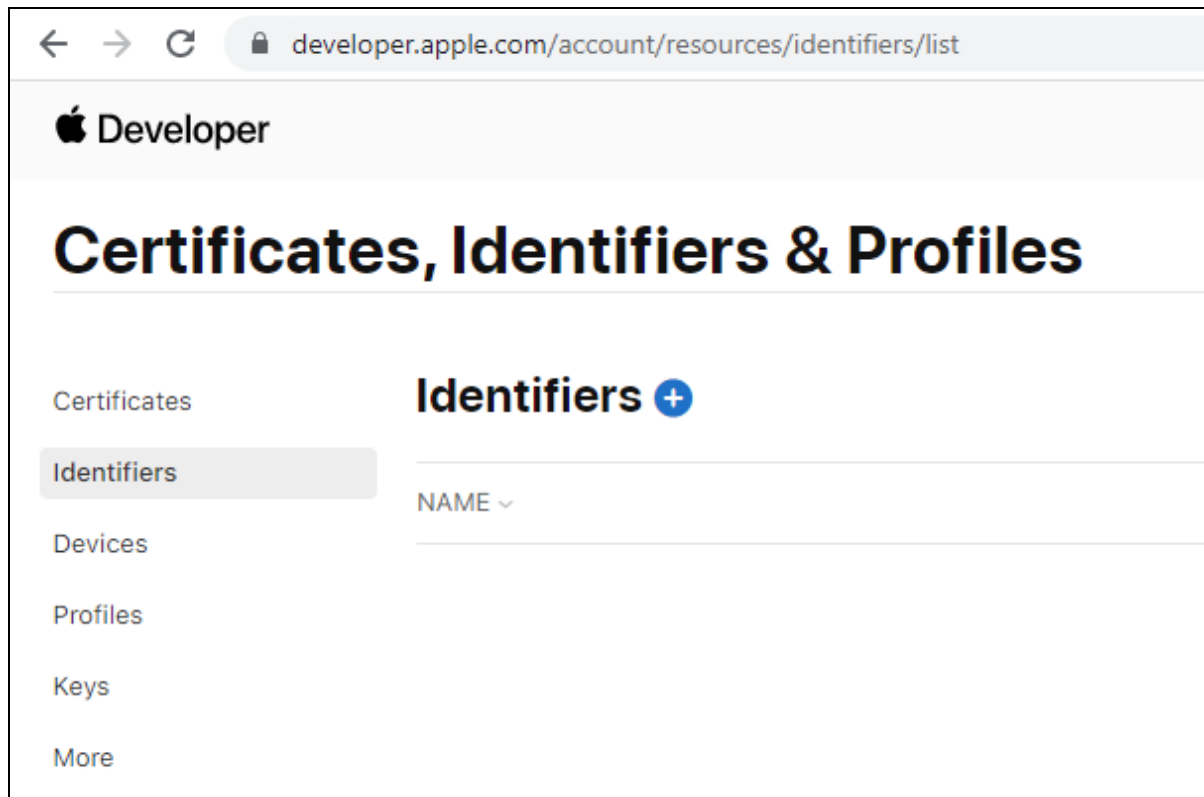
10. Finally, click the OFF switch and click Confirm to make the app public.



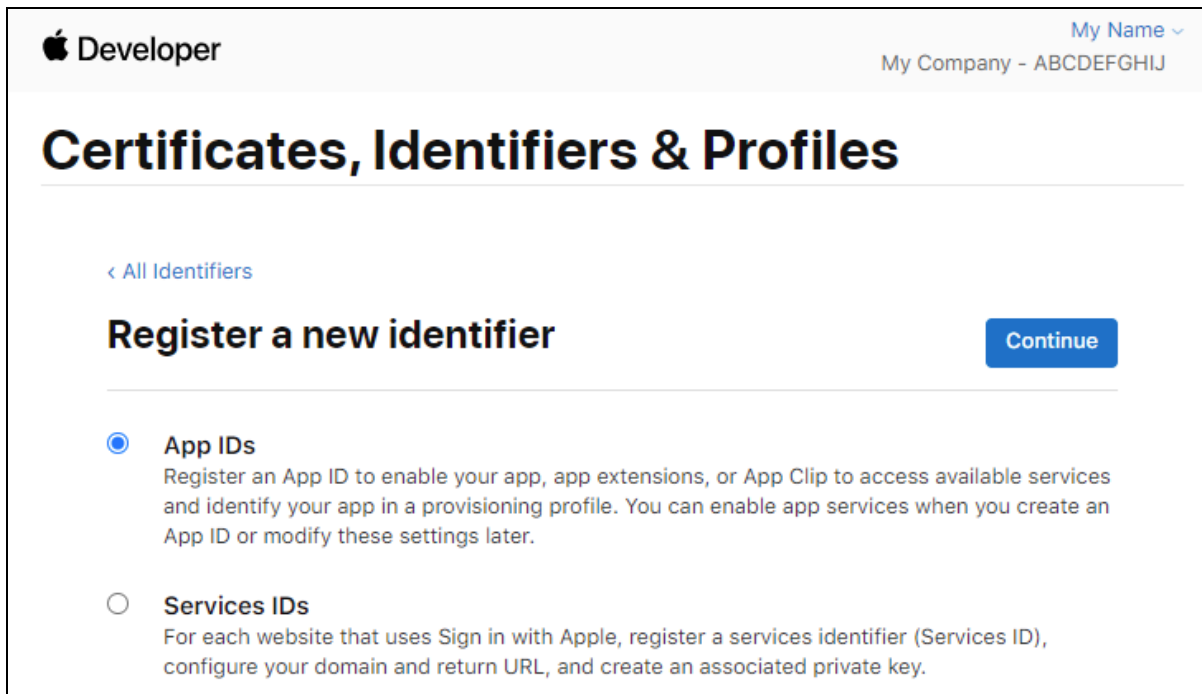
The screenshot displays the Peplink InControl 2 app configuration interface. At the top, there is a toggle switch labeled 'OFF' with a hand cursor pointing to it, indicating it should be turned off. To the right of the toggle, the status is 'Status: In Development'. Further right is a green button labeled 'View Analytics'. Below this, there is a section for 'App Secret' with a masked input field (represented by dots) and a 'Show' button. Below that is a 'Namespace' input field. A modal dialog titled 'Make App Public?' is open in the foreground. The dialog contains the text: 'Are you sure you want to make your app public? It will become available to everyone.' At the bottom of the dialog are two buttons: 'Cancel' and 'Confirm'. A hand cursor is pointing to the 'Confirm' button.

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

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



Press the “+” icon.



Apple Developer My Name ▾
My Company - ABCDEFGHIJ

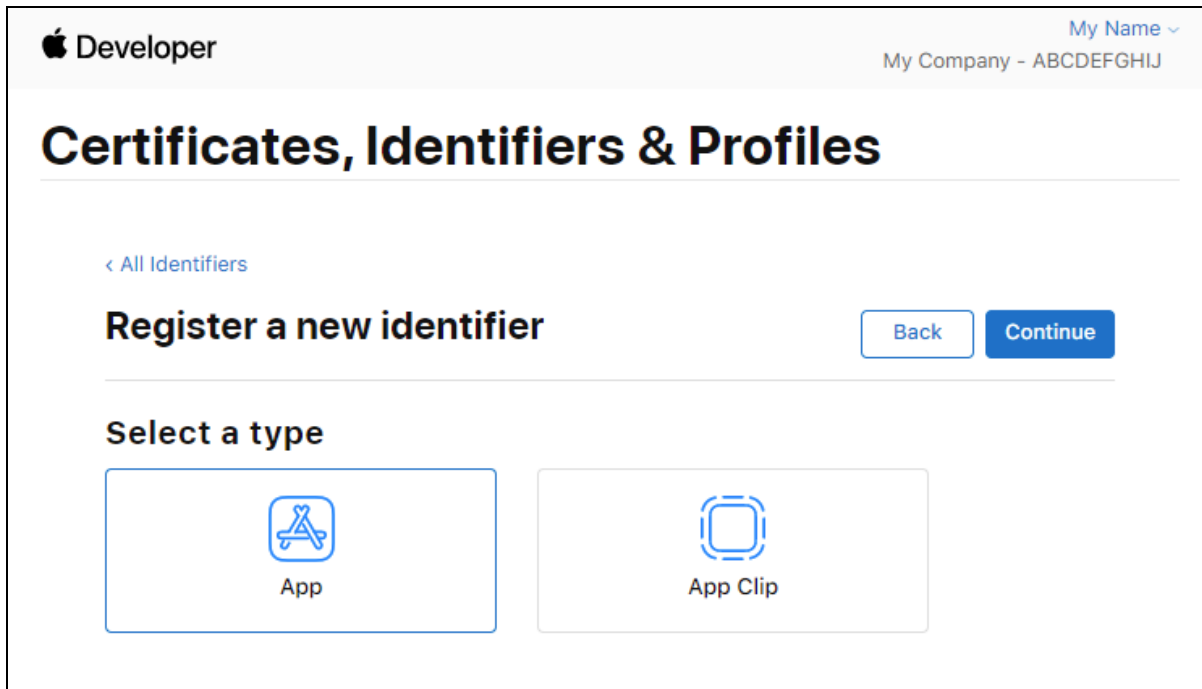
Certificates, Identifiers & Profiles

[< All Identifiers](#)

Register a new identifier Continue

- ☒ **App IDs**
Register an App ID to enable your app, app extensions, or App Clip to access available services and identify your app in a provisioning profile. You can enable app services when you create an App ID or modify these settings later.
- ☐ **Services IDs**
For each website that uses Sign in with Apple, register a services identifier (Services ID), configure your domain and return URL, and create an associated private key.

Select "App IDs". Press Continue




Apple Developer My Name ▾
My Company - ABCDEFGHIJ


Certificates, Identifiers & Profiles

[< All Identifiers](#)

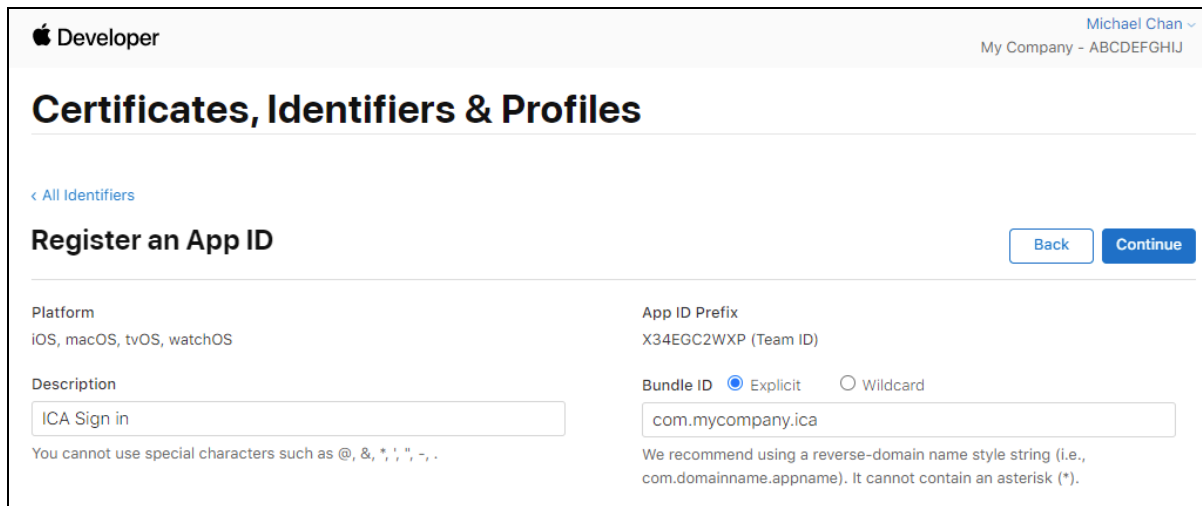
Register a new identifier Back Continue

Select a type


App


App Clip

Select "App" and press Continue.



Apple Developer Michael Chan ▾
My Company - ABCDEFGHIJ

Certificates, Identifiers & Profiles

[← All Identifiers](#)

Register an App ID Back Continue

Platform
iOS, macOS, tvOS, watchOS

App ID Prefix
X34EGC2WXP (Team ID)

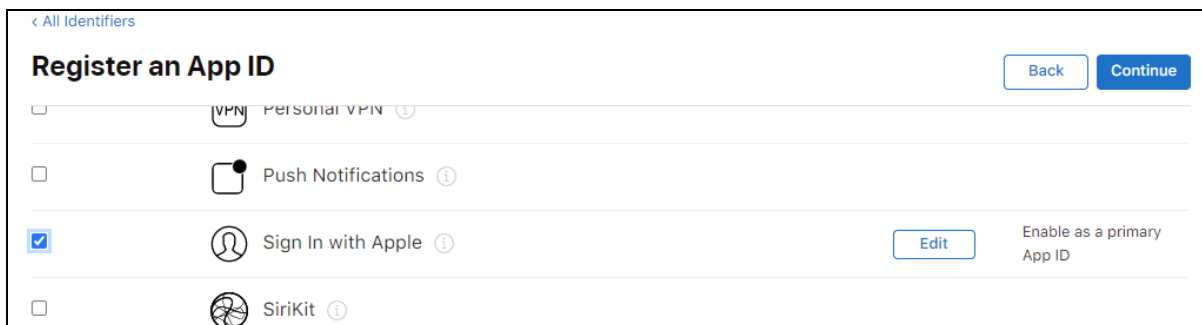
Description
ICA Sign in

Bundle ID ☒ Explicit ☐ Wildcard
com.mycompany.ica

You cannot use special characters such as @, &, *, ' , " , - , .





We recommend using a reverse-domain name style string (i.e., com.domainname.appname). It cannot contain an asterisk (*).

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




[← All Identifiers](#)


Register an App ID Back Continue

- ☐  Personal VPN ⓘ
- ☐  Push Notifications ⓘ
- ☒  Sign In with Apple ⓘ Edit Enable as a primary App ID
- ☐  SiriKit ⓘ

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

 My Name ▾
My Company - ABCDEFGHIJ

Certificates, Identifiers & Profiles

 **Finish Setting up Sign in with Apple**
Depending on your product, you may need to configure multiple components for Sign in with Apple – From registering domains for Web Authentication to providing email sources to communicate with your users through the Private Email Relay service. [Learn more >](#)
[1 Enable App ID](#) [2 Create Service ID for Web Authentication](#) [3 Create Key](#) [4 Register Email Sources for Communication](#)

[< All Identifiers](#)

Confirm your App ID

Platform
iOS, macOS, tvOS, watchOS


App ID Prefix
ABCDEFGHIJ (Team ID)

Description
ICA Sign in

Bundle ID
com.mycompany.ica (explicit)


[Back](#) [Register](#)


Press Register.

 Michael Chan ▾
My Company - ABCDEFGHIJ

Certificates, Identifiers & Profiles

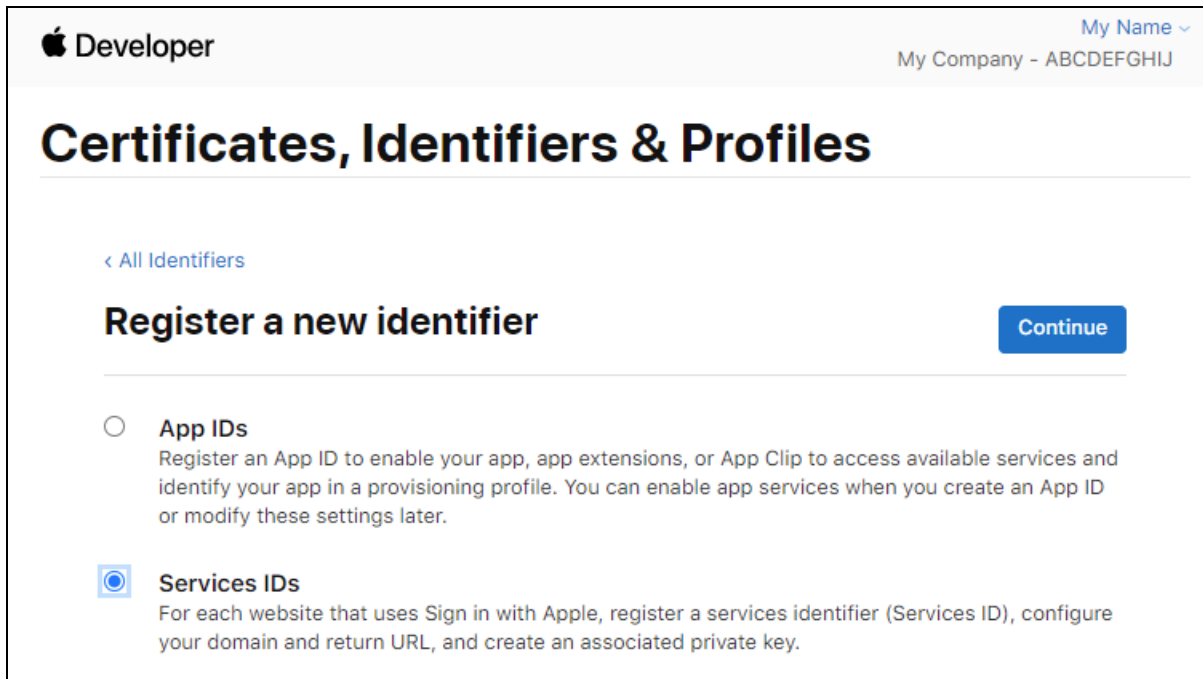
Certificates

Identifiers 

 App IDs ▾

	NAME ▾	IDENTIFIER
Identifiers	ICA Sign in	com.mycompany.ica
Devices		
Profiles		
Keys		

Press the “+” icon again.



Apple Developer My Name ▾
My Company - ABCDEFGHIJ

Certificates, Identifiers & Profiles

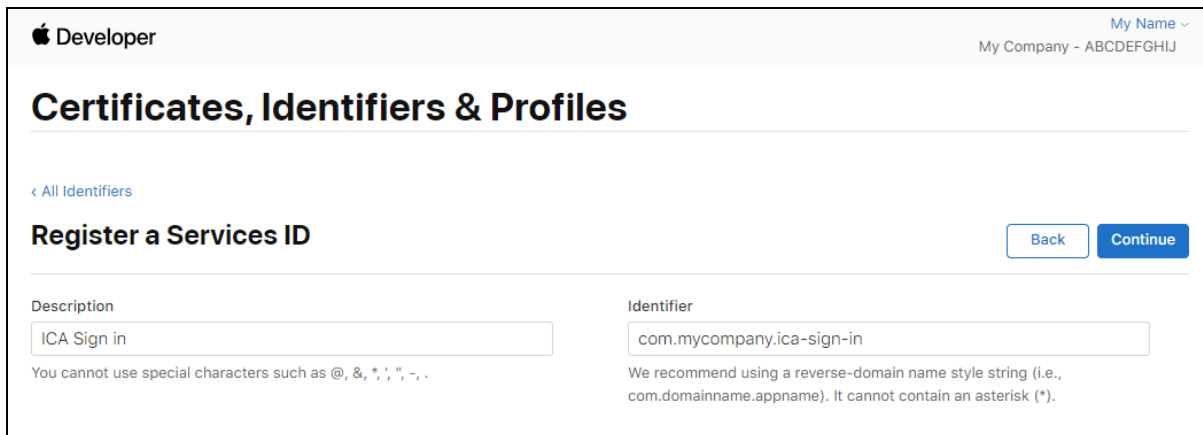
[< All Identifiers](#)

Register a new identifier Continue

☐ **App IDs**
Register an App ID to enable your app, app extensions, or App Clip to access available services and identify your app in a provisioning profile. You can enable app services when you create an App ID or modify these settings later.

☒ **Services IDs**
For each website that uses Sign in with Apple, register a services identifier (Services ID), configure your domain and return URL, and create an associated private key.

Select “Services IDs” and press Continue.



Apple Developer My Name ▾
My Company - ABCDEFGHIJ


Certificates, Identifiers & Profiles


[< All Identifiers](#)

Register a Services ID Back Continue

<p>Description</p> <input type="text" value="ICA Sign in"/> <p><small>You cannot use special characters such as @, &, *, ' , " , - , .</small></p>	<p>Identifier</p> <input type="text" value="com.mycompany.ica-sign-in"/> <p><small>We recommend using a reverse-domain name style string (i.e., com.domainname.appname). It cannot contain an asterisk (*).</small></p>
--	---

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

 Developer

My Name 

My Company - ABCDEFGHIJ

Certificates, Identifiers & Profiles


[< All Identifiers](#)


Register a Services ID

Back Register

Description	Identifier
ICA Sign in	com.mycompany.ica-sign-in

Press Register.

 Developer

My Name 

My Company - ABCDEFGHIJ

Certificates, Identifiers & Profiles

[< All Identifiers](#)

Edit your Services ID Configuration

Remove Continue

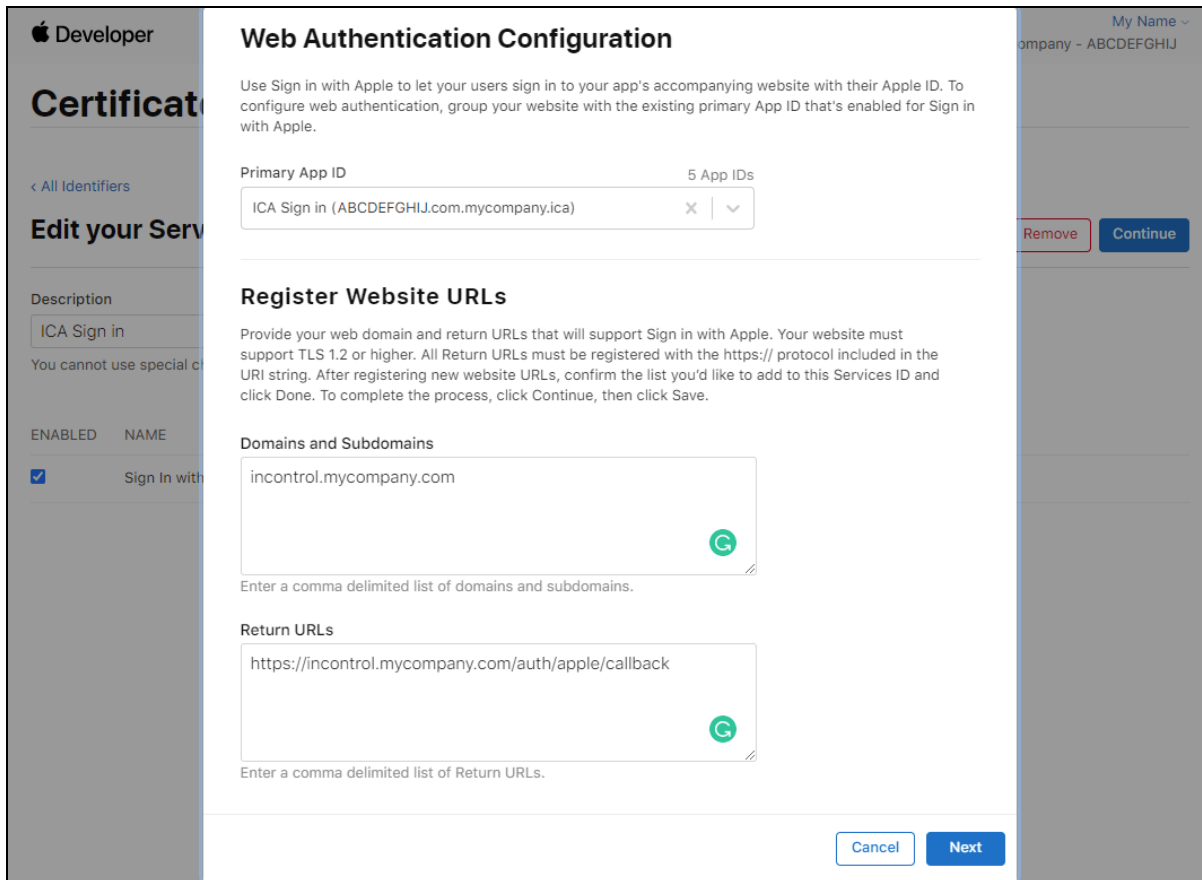
Description	Identifier
<input type="text" value="ICA Sign in"/>	com.mycompany.ica-sign-in

You cannot use special characters such as @, &, *, ' , " , - , .

ENABLED	NAME
<input checked="" type="checkbox"/>	Sign In with Apple

Configure

Press Configure.



Web Authentication Configuration

Use Sign in with Apple to let your users sign in to your app's accompanying website with their Apple ID. To configure web authentication, group your website with the existing primary App ID that's enabled for Sign in with Apple.

Primary App ID: ICA Sign in (ABCDEFGHIJ.com.mycompany.ica) 5 App IDs

Register Website URLs

Provide your web domain and return URLs that will support Sign in with Apple. Your website must support TLS 1.2 or higher. All Return URLs must be registered with the https:// protocol included in the URI string. After registering new website URLs, confirm the list you'd like to add to this Services ID and click Done. To complete the process, click Continue, then click Save.

Domains and Subdomains

incontrol.mycompany.com

Enter a comma delimited list of domains and subdomains.

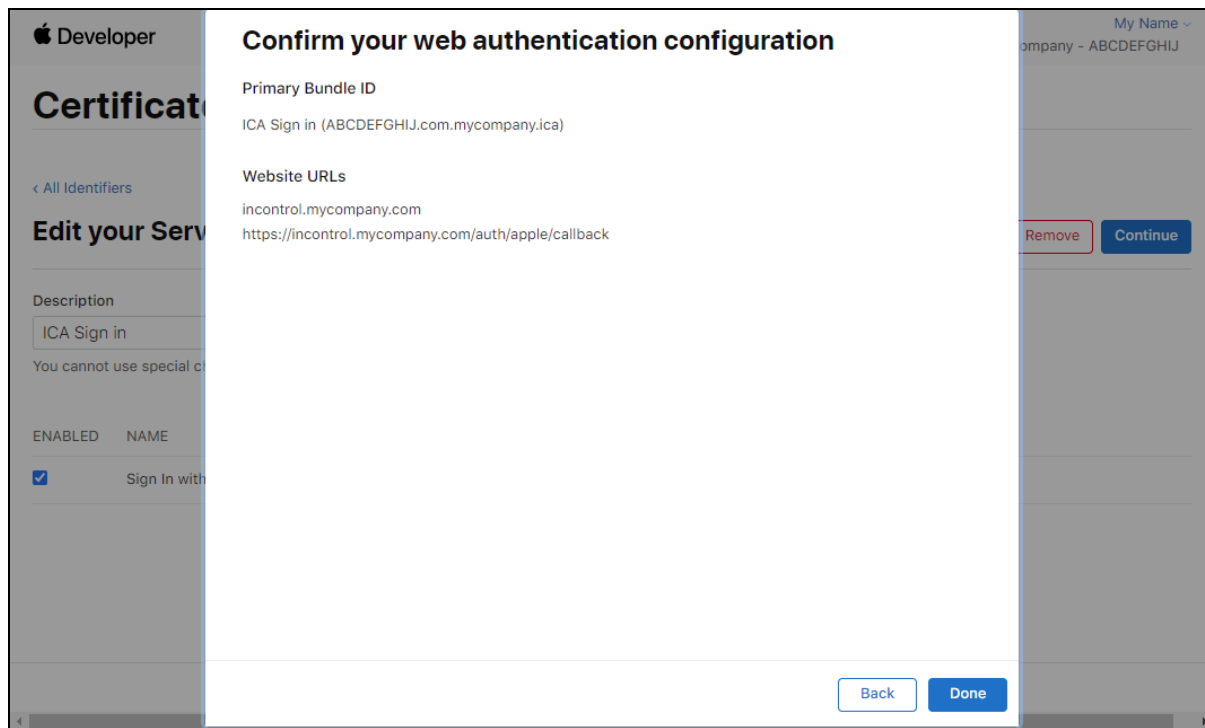
Return URLs

https://incontrol.mycompany.com/auth/apple/callback

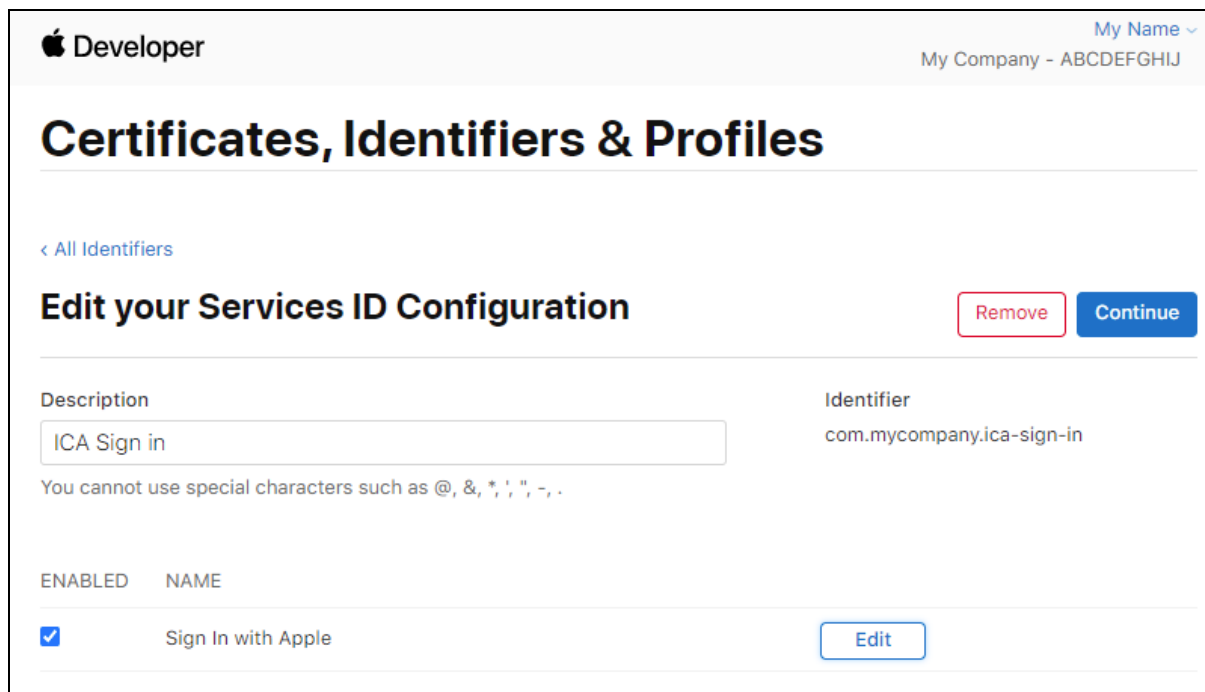
Enter a comma delimited list of Return URLs.

Buttons: Cancel, Next, Remove, Continue


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.

 Developer My Name ▾
My Company - ABCDEFGHIJ

Certificates, Identifiers & Profiles

 **Finish Setting up Sign in with Apple**
Depending on your product, you may need to configure multiple components for Sign in with Apple – From registering domains for Web Authentication to providing email sources to communicate with your users through the Private Email Relay service. [Learn more >](#)

① Enable App ID

② Create Service ID for Web Authentication

③ Create Key

④ Register Email Sources for Communication

[< All Identifiers](#)


Edit your Services ID Configuration Back Save

Description	Identifier
ICA Sign in	com.mycompany.ica-sign-in

ENABLED	NAME
<input checked="" type="checkbox"/>	Sign In with Apple
	ABCDEFGHIJ.com.mycompany.ica (2 Website URLs)


Press Save to save the Services ID.

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

 Developer My Name ▾
My Company - ABCDEFGHIJ

Certificates, Identifiers & Profiles

Certificates

Keys + 

Identifiers

NAME ▾ SERVICE ENABLED


Devices

Profiles

Keys

More

Press the “+” icon.

 My Name ▾
My Company - ABCDEFGHIJ

Certificates, Identifiers & Profiles

[< All Keys](#)

Register a New Key Continue



Key Name

ICA sign in key

You cannot use special characters such as @, &, *, ' , ", -, .

ENABLE	NAME	DESCRIPTION	
<input type="checkbox"/>	Apple Push Notifications service (APNs)	Establish connectivity between your notification server and the Apple Push Notification service. One key is used for all of your apps. Learn more ⓘ You have already reached the maximum allowed number of Keys for this service	
<input type="checkbox"/>	DeviceCheck	Access the DeviceCheck and AppAttest APIs to get data that your associated server can use in its business logic to protect your business while maintaining user privacy. Learn more	
<input type="checkbox"/>	MapKit JS	Use Apple Maps on your websites. Show a map, display search results, provide directions, and more. Learn more ⓘ There are no identifiers available that can be associated with the key	Configure
<input type="checkbox"/>	Media Services (MusicKit, ShazamKit)	Access the Apple Music catalog and make personalized requests for authorized users, and check audio signatures against the Shazam music catalog. ⓘ There are no identifiers available that can be associated with the key	Configure
<input checked="" type="checkbox"/>	Sign in with Apple	Enable your apps to allow users to authenticate in your application with their Apple ID. Configuration is required to enable this feature. ⓘ This service must have one identifier configured.	Configure
<input type="checkbox"/>	ClassKit Catalog	Publish all of your ClassKit app activities to teachers creating Handouts in Apple Schoolwork. Learn more	

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

 My Name 
My Company - ABCDEFGHIJ

Certificates, Identifiers & Profiles



[< View Key](#)

Configure Key

Back Save

Create a key for each of your primary App IDs in order to implement Sign in with Apple. This key will also be used for any App IDs grouped with the primary. The user will see your primary app's icon at sign in and in their Apple ID account settings.

Primary App ID: 4 App ID s



ICA Sign in (ABCDEFGHIJ.com.mycompany.ica)  

Grouped App IDs


These App IDs are enabled with Sign in with Apple by being grouped with the primary App ID selected above. Users will see your primary app's icon, terms and conditions, and privacy policy when they first sign in, and in their Apple ID account settings.





ICA Sign in (ABCDEFGHIJ.com.mycompany.ica-sign-in)

Select "ICA Sign in". Press Save.

 My Name 
My Company - ABCDEFGHIJ

Certificates, Identifiers & Profiles

 **Finish Setting up Sign in with Apple**
Depending on your product, you may need to configure multiple components for Sign in with Apple – From registering domains for Web Authentication to providing email sources to communicate with your users through the Private Email Relay service. [Learn more >](#)

[< All Keys](#)



Register a New Key

Back Register

Key Name
ICA sign in key

ENABLE	NAME	DESCRIPTION
<input checked="" type="checkbox"/>	Sign in with Apple	Enable your apps to allow users to authenticate in your application with their Apple ID. Configuration is required to enable this feature.

Press Register.

 My Name 
My Company - ABCDEFGHIJ

Certificates, Identifiers & Profiles

[< All Keys](#)

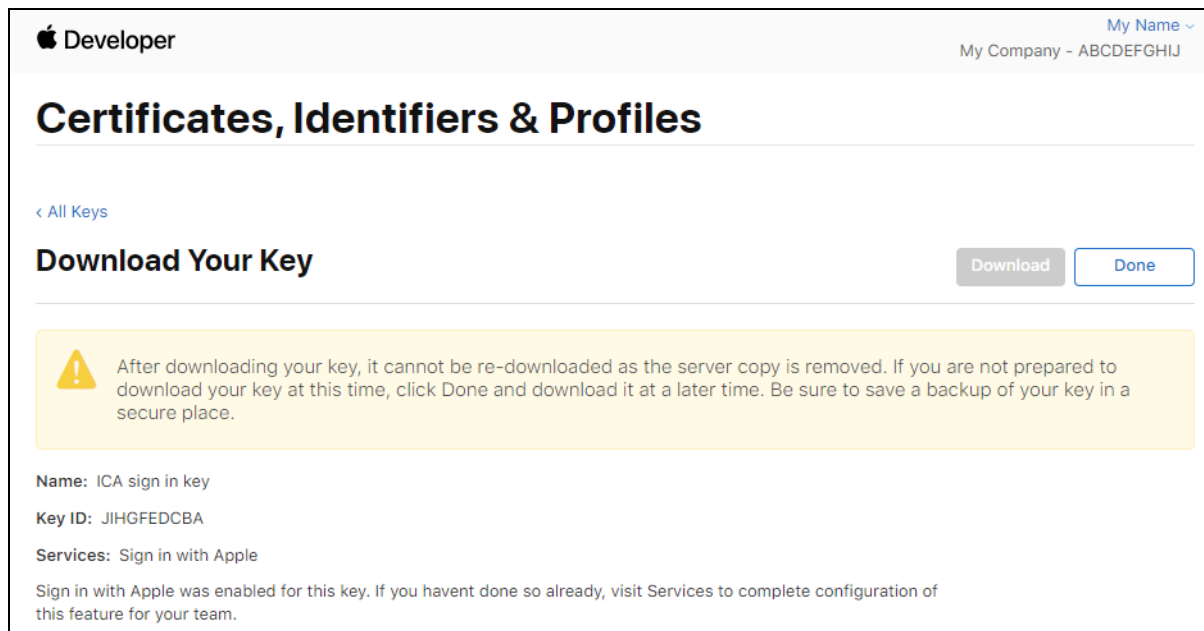
Register a New Key Continue

Key Name

You cannot use special characters such as @, &, *, ' ", -, .

ENABLE	NAME	DESCRIPTION	
<input type="checkbox"/>	Apple Push Notifications service (APNs)	Establish connectivity between your notification server and the Apple Push Notification service. One key is used for all of your apps. Learn more ⓘ You have already reached the maximum allowed number of Keys for this service	
<input type="checkbox"/>	DeviceCheck	Access the DeviceCheck and AppAttest APIs to get data that your associated server can use in its business logic to protect your business while maintaining user privacy. Learn more	
<input type="checkbox"/>	MapKit JS	Use Apple Maps on your websites. Show a map, display search results, provide directions, and more. Learn more ⓘ There are no identifiers available that can be associated with the key	Configure
<input type="checkbox"/>	Media Services (MusicKit, ShazamKit)	Access the Apple Music catalog and make personalized requests for authorized users, and check audio signatures against the Shazam music catalog. ⓘ There are no identifiers available that can be associated with the key	Configure
<input checked="" type="checkbox"/>	Sign in with Apple	Enable your apps to allow users to authenticate in your application with their Apple ID. Configuration is required to enable this feature.	Edit
<input type="checkbox"/>	ClassKit Catalog	Publish all of your ClassKit app activities to teachers creating Handouts in Apple Schoolwork. Learn more	

Press Continue.



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

Press Done only after you have downloaded the key.

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

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

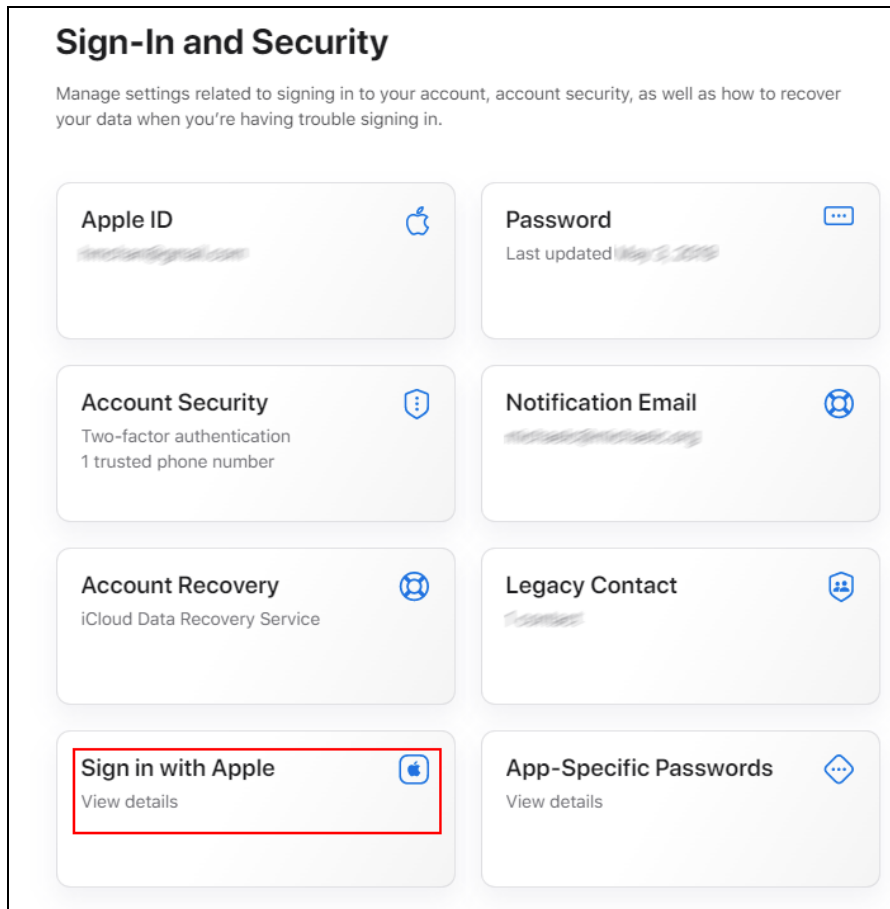
Note: when your users sign in to your InControl with Apple for the first time, they will be asked to choose whether to hide their email address from your InControl on Apple’s website. It is a privacy feature of the Apple sign-in.

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

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

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

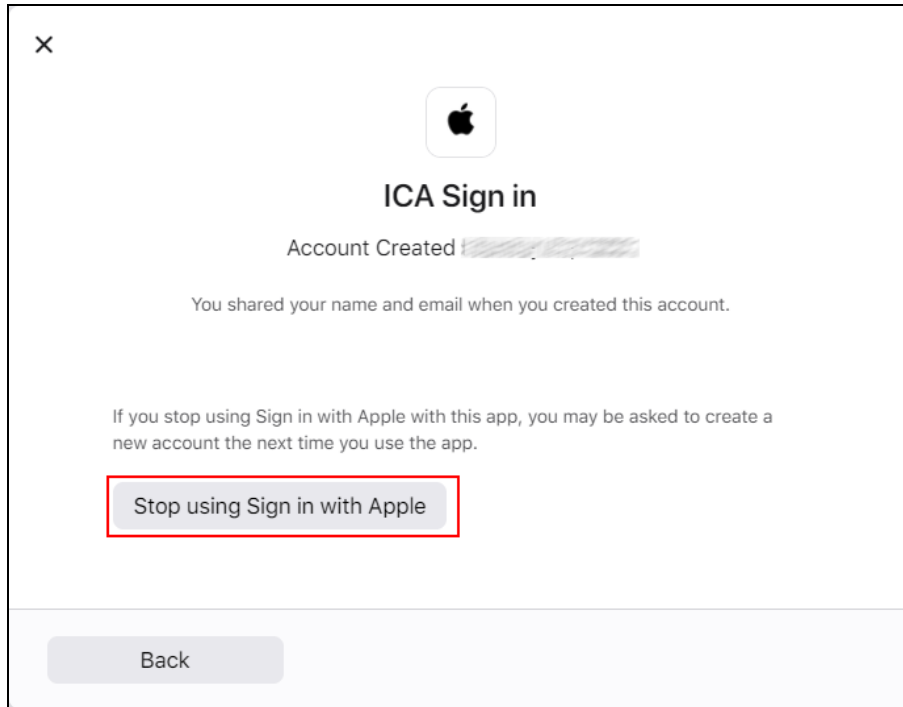
1. Login to <https://appleid.apple.com>
2. Choose "Sign in with Apple"



3. Select "ICA Sign in"



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



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

Now their account is well set.