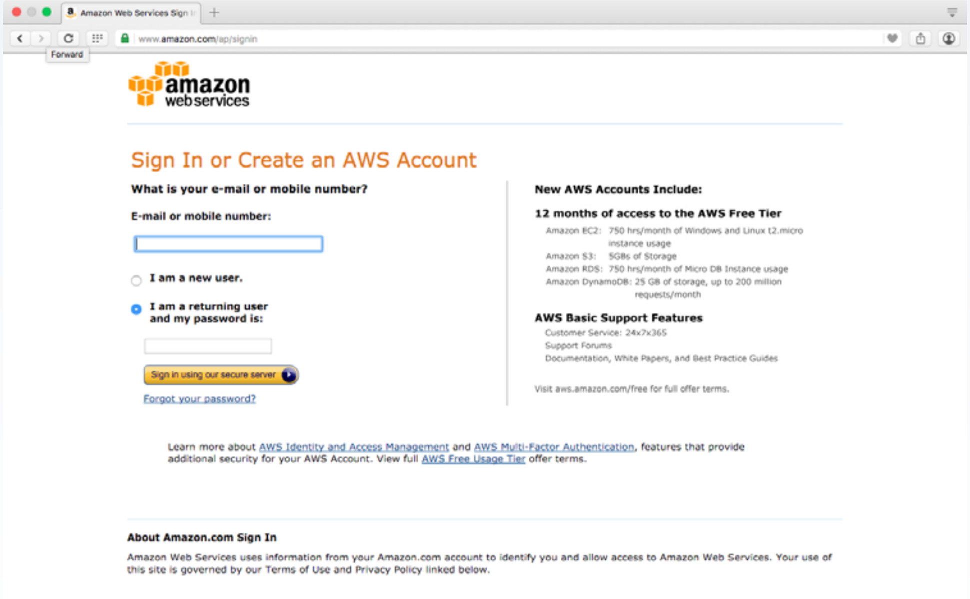
How to install Central WifiManager onto an Amazon AWS Cloud Instance

This document will guide you through the processes involved in setting up Central Wifi Manager in an AWS cloud.

Start off by signing up for a new AWS Account, or if you wish just can use your existing Amazon.com account to sign into AWS.



Sign In or Create an AWS Account

What is your e-mail or mobile number?

E-mail or mobile number:

○ I am a new user.

● I am a returning user and my password is:

Sign in using our secure server

Forgot your password?

New AWS Accounts Include:

12 months of access to the AWS Free Tier

Amazon EC2: 750 hrs/month of Windows and Linux t2.micro instance usage
Amazon S3: 5GBs of Storage
Amazon RDS: 750 hrs/month of Micro DB Instance usage
Amazon DynamoDB: 25 GB of storage, up to 200 million requests/month

AWS Basic Support Features

Customer Service: 24x7x365
Support Forums
Documentation, White Papers, and Best Practice Guides

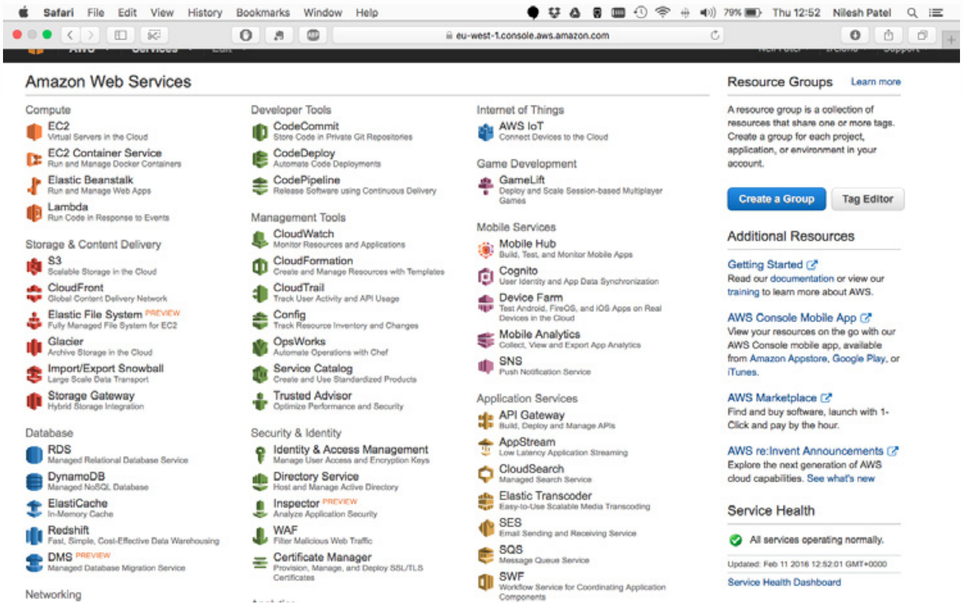
Visit aws.amazon.com/free for full offer terms.

Learn more about AWS Identity and Access Management and AWS Multi-Factor Authentication, features that provide additional security for your AWS Account. View full AWS Free Usage Tier offer terms.

About Amazon.com Sign In

Amazon Web Services uses information from your Amazon.com account to identify you and allow access to Amazon Web Services. Your use of this site is governed by our Terms of Use and Privacy Policy linked below.

Once logged in, you may select a datacentre near your region to minimise the latency between the CWM controller and your access points. You can do this by clicking in the top right-hand corner, between your name and the Support link and choosing the appropriate Amazon Datacentre. The under the Compute section select EC2.



Amazon Web Services

Compute
EC2 – Virtual Servers in the Cloud
EC2 Container Service – Run and Manage Docker Containers
Elastic Beanstalk – Run and Manage Web Apps
Lambda – Run Code in Response to Events

Storage & Content Delivery
S3 – Scalable Storage in the Cloud
CloudFront – Global Content Delivery Network
Elastic File System PREVIEW – Fully Managed File System for EC2
Glacier – Archive Storage in the Cloud
Import/Export Snowball – Large Scale Data Transport
Storage Gateway – Hybrid Storage Integration

Database
RDS – Managed Relational Database Service
DynamoDB – Managed NoSQL Database
ElastiCache – In-Memory Cache
Redshift – Fast, Simple, Cost-Effective Data Warehousing
DMS PREVIEW – Managed Database Migration Service

Networking

Developer Tools
CodeCommit – Store Code in Private Git Repositories
CodeDeploy – Automate Code Deployments
CodePipeline – Release Software using Continuous Delivery

Management Tools
CloudWatch – Monitor Resources and Applications
CloudFormation – Create and Manage Resources with Templates
CloudTrail – Track User Activity and API Usage
Config – Track Resource Inventory and Changes
OpsWorks – Automate Operations with Chef
Service Catalog – Create and Use Standardized Products
Trusted Advisor – Optimize Performance and Security

Security & Identity
Identity & Access Management – Manage User Access and Encryption Keys
Directory Service – Host and Manage Active Directory
Inspector PREVIEW – Analyze Application Security
WAF – Filter Malicious Web Traffic
Certificate Manager – Provision, Manage, and Deploy SSL/TLS Certificates

Internet of Things
AWS IoT – Connect Devices to the Cloud

Game Development
GameLift – Deploy and Scale Session-based Multiplayer Games

Mobile Services
Mobile Hub – Build, Test, and Monitor Mobile Apps
Cognito – User Identity and App Data Synchronization
Device Farm – Test Android, FireOS, and iOS Apps on Real Devices in the Cloud
Mobile Analytics – Collect, View and Export App Analytics
SNS – Push Notification Service

Application Services
API Gateway – Build, Deploy and Manage APIs
AppStream – Low Latency Application Streaming
CloudSearch – Managed Search Service
Elastic Transcoder – Easy-to-Use Scalable Media Transcoding
SES – Email Sending and Receiving Service
SQS – Message Queue Service
SWF – Workflow Service for Coordinating Application Components

Resource Groups – Learn more

A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.

Create a Group | Tag Editor

Additional Resources

Getting Started
Read our documentation or view our training to learn more about AWS.

AWS Console Mobile App
View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.

AWS Marketplace
Find and buy software, launch with 1-Click and pay by the hour.

AWS re:Invent Announcements
Explore the next generation of AWS cloud capabilities. See what's new

Service Health

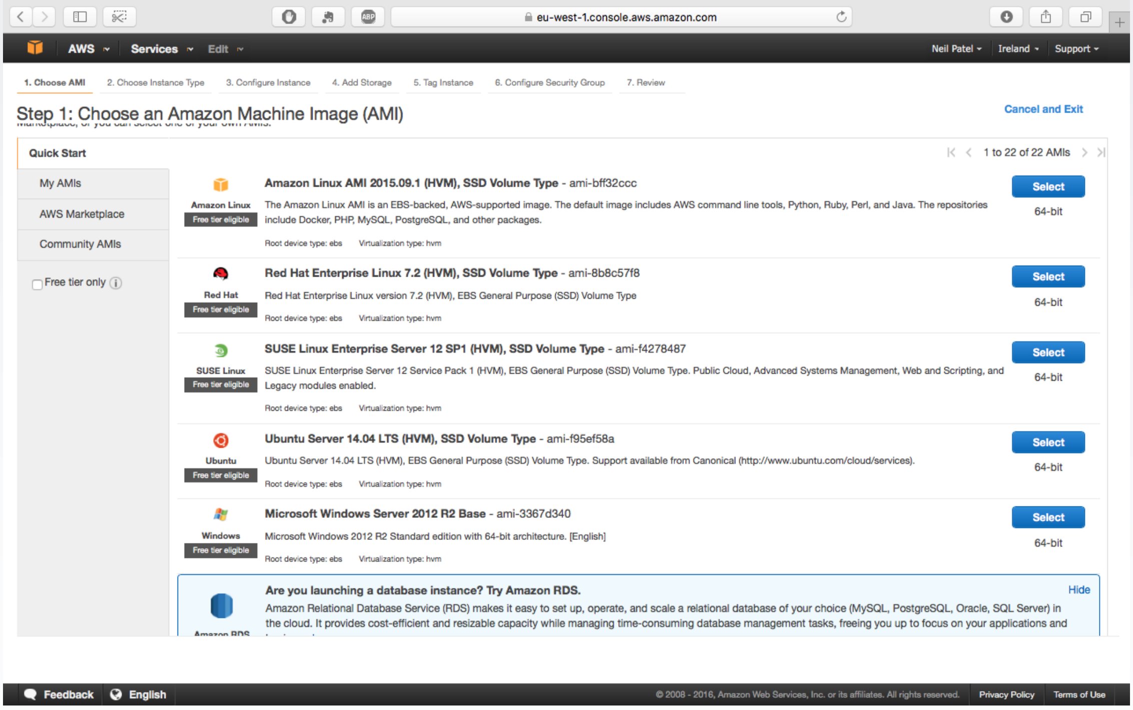
✓ All services operating normally.

Updated: Feb 11 2016 12:52:01 GMT+0000

Service Health Dashboard

Step 1

Scroll down and pick the appropriate Microsoft Windows Server instance, for this example I will select the Microsoft Windows Server 2012 R2 Base.



Step 1: Choose an Amazon Machine Image (AMI)

☐ Free tier only

Amazon Linux – Free tier eligible
Amazon Linux AMI 2015.09.1 (HVM), SSD Volume Type - ami-bff32ccc
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root device type: ebs Virtualization type: hvm
Select 64-bit

Red Hat – Free tier eligible
Red Hat Enterprise Linux 7.2 (HVM), SSD Volume Type - ami-8b8c57f8
Red Hat Enterprise Linux version 7.2 (HVM), EBS General Purpose (SSD) Volume Type
Root device type: ebs Virtualization type: hvm
Select 64-bit

SUSE Linux – Free tier eligible
SUSE Linux Enterprise Server 12 SP1 (HVM), SSD Volume Type - ami-f4278487
SUSE Linux Enterprise Server 12 Service Pack 1 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.
Root device type: ebs Virtualization type: hvm
Select 64-bit

Ubuntu – Free tier eligible
Ubuntu Server 14.04 LTS (HVM), SSD Volume Type - ami-f95ef58a
Ubuntu Server 14.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Root device type: ebs Virtualization type: hvm
Select 64-bit

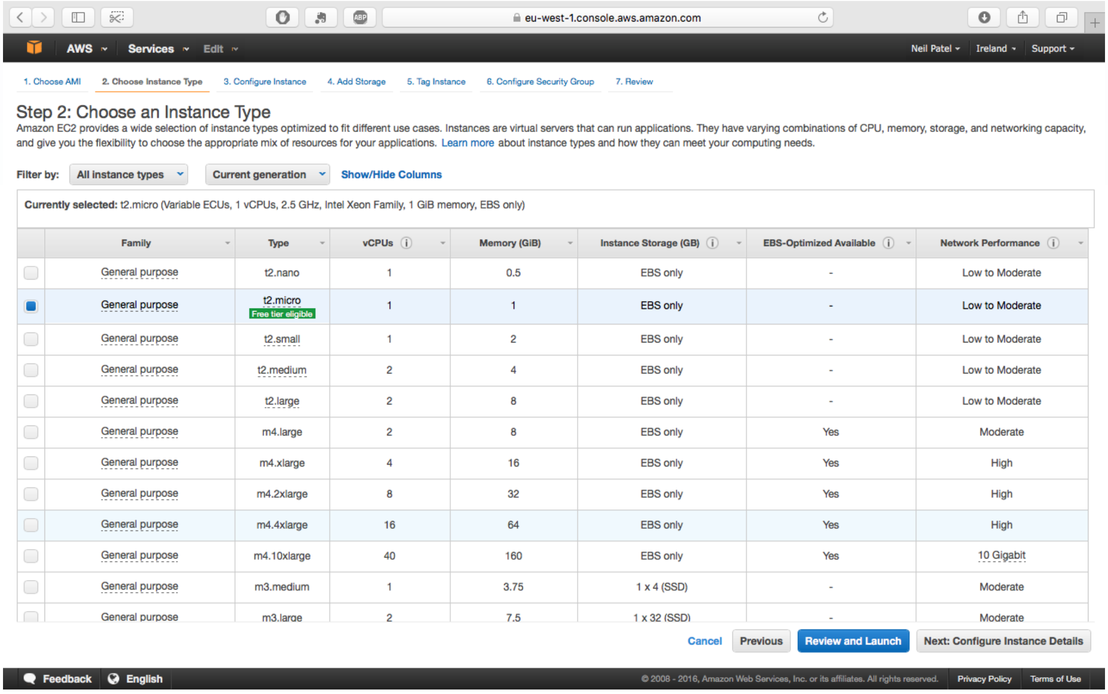
Windows – Free tier eligible
Microsoft Windows Server 2012 R2 Base - ami-3367d340
Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]
Root device type: ebs Virtualization type: hvm
Select 64-bit

Amazon RDS
Are you launching a database instance? Try Amazon RDS.
Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale a relational database of your choice (MySQL, PostgreSQL, Oracle, SQL Server) in the cloud. It provides cost-efficient and resizable capacity while managing time-consuming database management tasks, freeing you up to focus on your applications and

© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step 2

Since we will only be running a limited number of Access Points I have selected the General purpose, t2.micro instance. This free micro instance has 1 virtual CPU, 1GB of memory, and is Free tier eligible. Then Click Next.



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types | Current generation

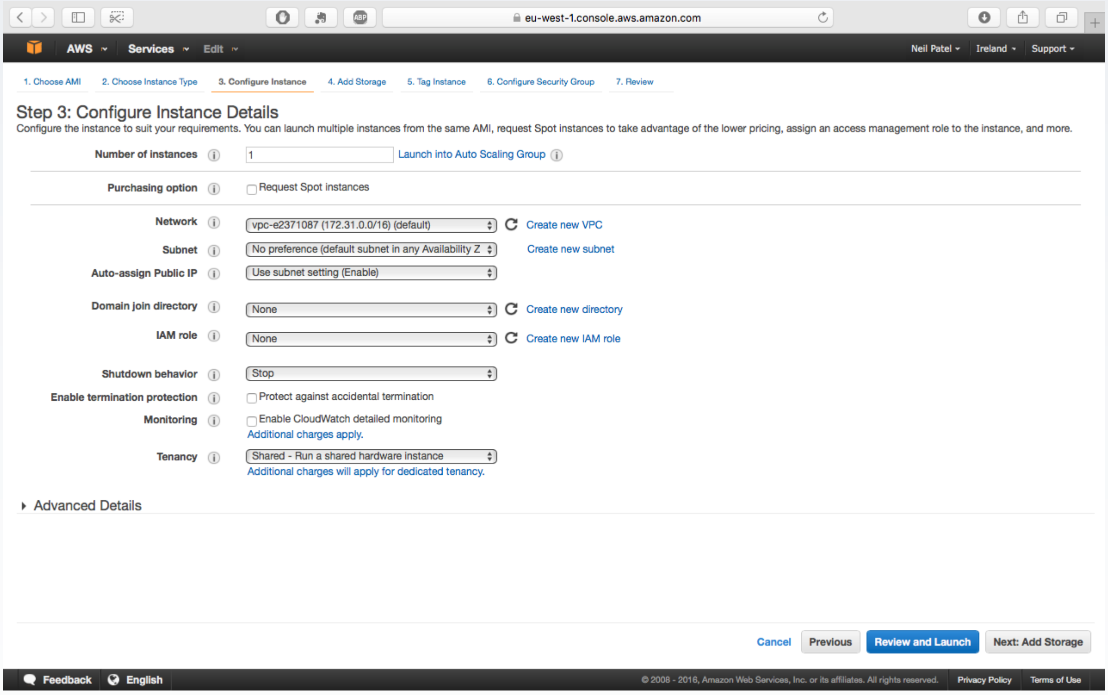
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
☐	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
■	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
☐	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
☐	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
☐	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
☐	General purpose	m4.large	2	8	EBS only	Yes	Moderate
☐	General purpose	m4.xlarge	4	16	EBS only	Yes	High
☐	General purpose	m4.2xlarge	8	32	EBS only	Yes	High
☐	General purpose	m4.4xlarge	16	64	EBS only	Yes	High
☐	General purpose	m4.10xlarge	40	160	EBS only	Yes	10 Gigabit
☐	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
☐	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate

© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step 3

Configure Instance Details. Leave all settings as default. You may want to check Enable termination protection - Protect against accidental termination, which makes sure you don't delete the instance by accident (this can be enabled/disabled in the future). Then Click Next.



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-e2371087 (172.31.0.0/16) (default) Create new VPC

Subnet: No preference (default subnet in any Availability Z Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

Domain join directory: None Create new directory

IAM role: None Create new IAM role

Shutdown behavior: Stop

Enable termination protection: □ Protect against accidental termination

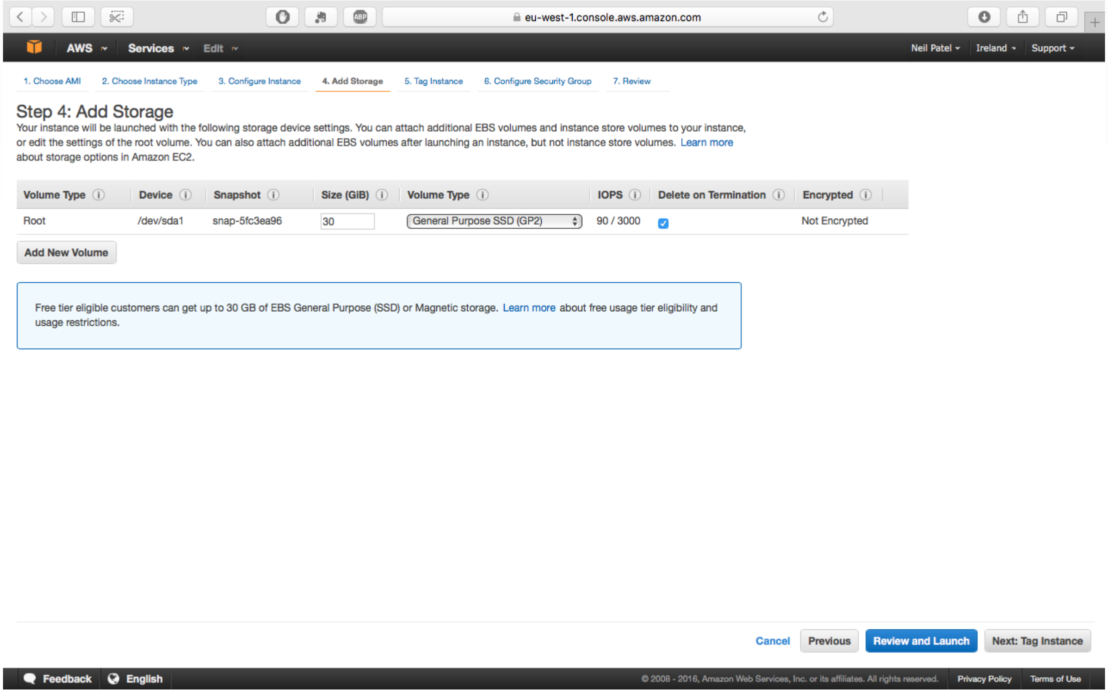
Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

Advanced Details

Step 4

You may add extra Storage capacity , but AWS provides up to 30 GB of EBS Storage.



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

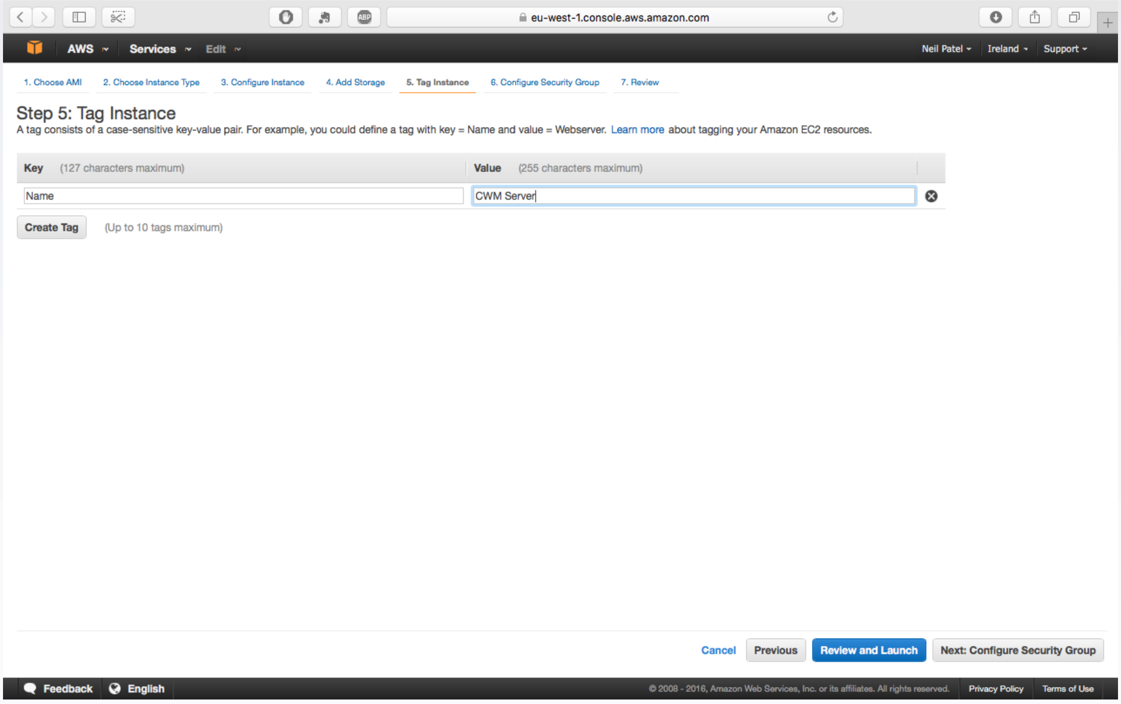
Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/sda1	snap-5fc3ea96	30	General Purpose SSD (GP2)	90 / 3000	☑	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Step 5

Tag Instance. Enter the optional tag to help identify the instance, it is not required in our implementation.



Step 5: Tag Instance

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	CWM Server

(Up to 10 tags maximum)

© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step 6

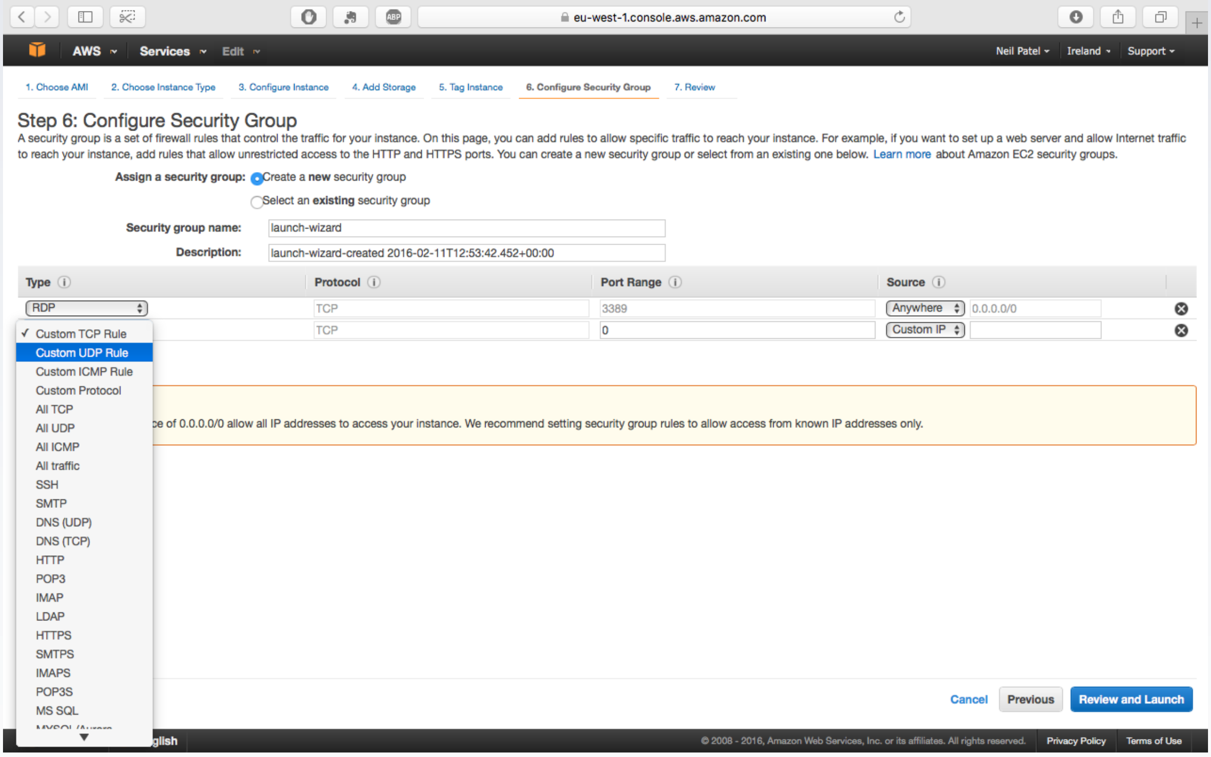
Configure Security Group. AWS uses a software firewall to protect the virtual server. To open the relevant firewall ports to enable CWM to communicate with your remote Access Points.

1. Assign a security group: Create a new security group

2. Security group name: CWM Configuration

3. Description: (Enter the optional controller description)

Type	Protocol	Port Range	Source
RDP	TCP	3389	Anywhere 0.0.0.0/0
SNMP	UDP	161-162	Anywhere 0.0.0.0/0
Syslog	UDP	514	Anywhere 0.0.0.0/0
Listen Port	UDP	8090	Anywhere 0.0.0.0/0
Service POrt	UDP	64768	Anywhere 0.0.0.0/0
FTP	TCP	9000	Anywhere 0.0.0.0/0
ALG-FTP	TCP	54000-54999	Anywhere 0.0.0.0/0



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group

○ Select an **existing** security group

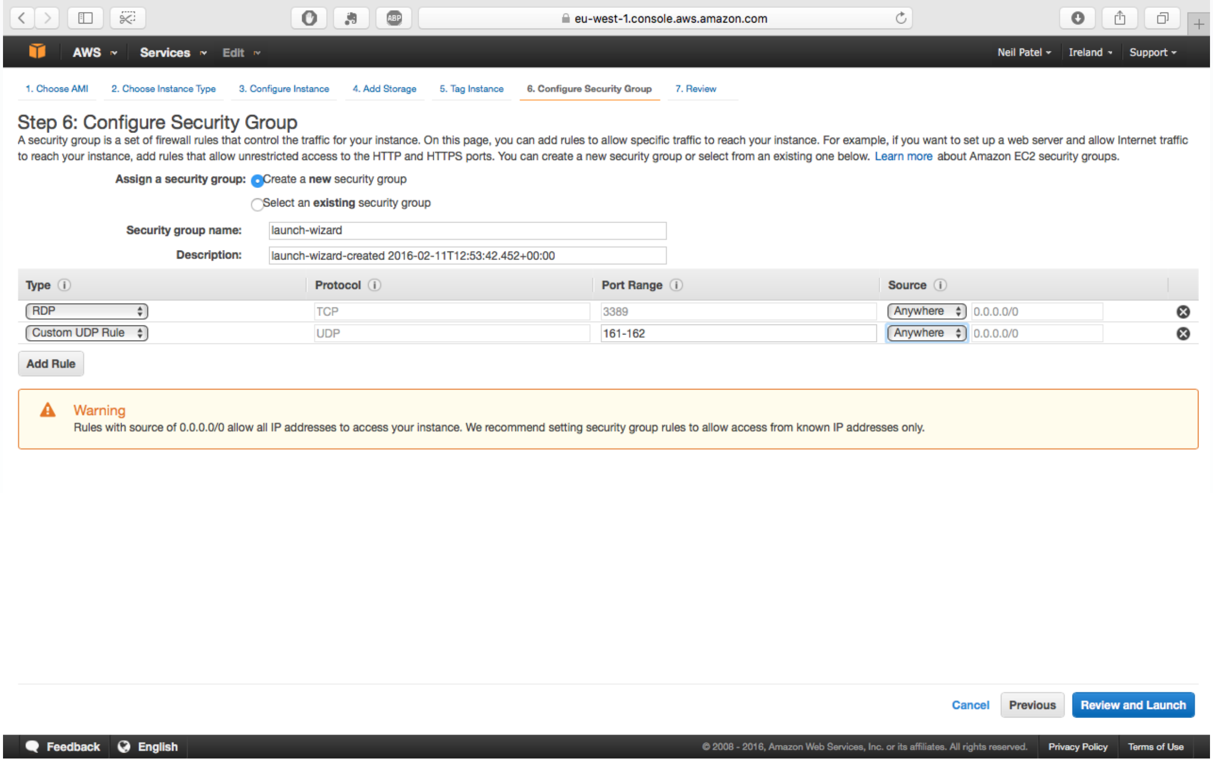
Security group name: launch-wizard

Description: launch-wizard-created 2016-02-11T12:53:42.452+00:00

Type	Protocol	Port Range	Source	
RDP	TCP	3389	Anywhere 0.0.0.0/0	⊗
	TCP	0	Custom IP	⊗

ce of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel
Previous
Review and Launch
glish
© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group

○ Select an **existing** security group

Security group name: launch-wizard

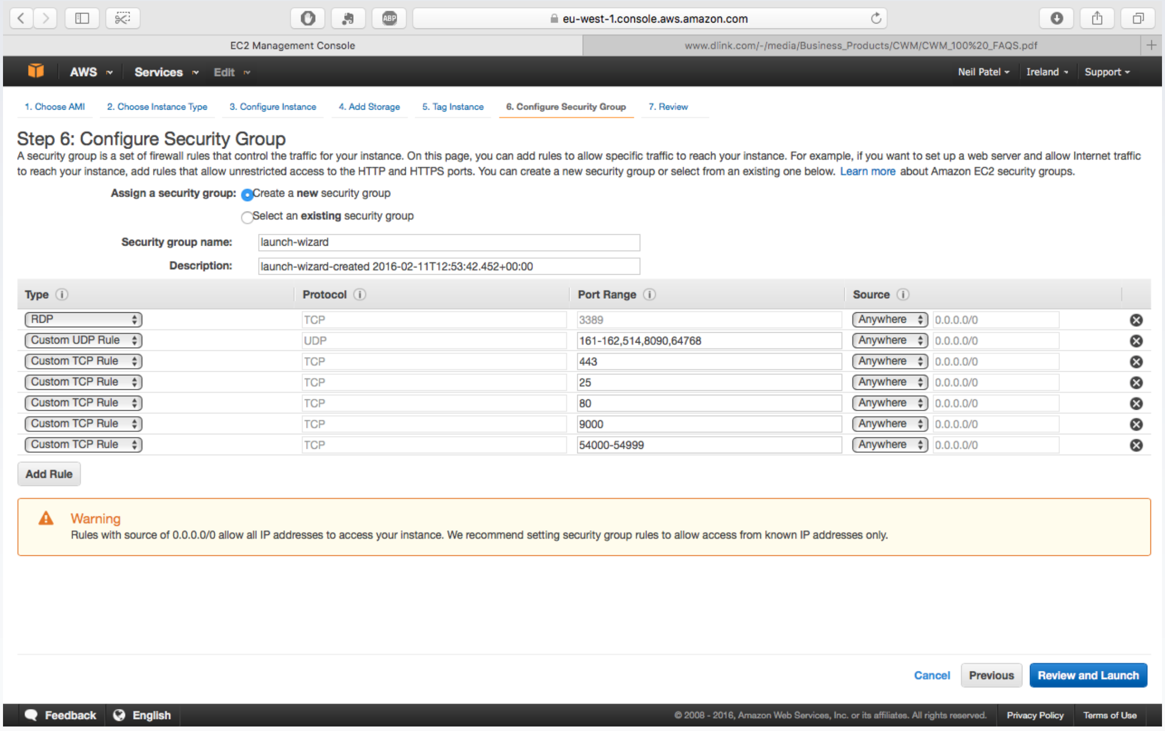
Description: launch-wizard-created 2016-02-11T12:53:42.452+00:00

Type	Protocol	Port Range	Source	
RDP	TCP	3389	Anywhere 0.0.0.0/0	⊗
Custom UDP Rule	UDP	161-162	Anywhere 0.0.0.0/0	⊗

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel
Previous
Review and Launch
Feedback
English
© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: launch-wizard

Description: launch-wizard-created 2016-02-11T12:53:42.452+00:00

Type	Protocol	Port Range	Source	
RDP	TCP	3389	Anywhere 0.0.0.0/0	☒
Custom UDP Rule	UDP	161-162,514,8090,64768	Anywhere 0.0.0.0/0	☒
Custom TCP Rule	TCP	443	Anywhere 0.0.0.0/0	☒
Custom TCP Rule	TCP	25	Anywhere 0.0.0.0/0	☒
Custom TCP Rule	TCP	80	Anywhere 0.0.0.0/0	☒
Custom TCP Rule	TCP	9000	Anywhere 0.0.0.0/0	☒
Custom TCP Rule	TCP	54000-54999	Anywhere 0.0.0.0/0	☒

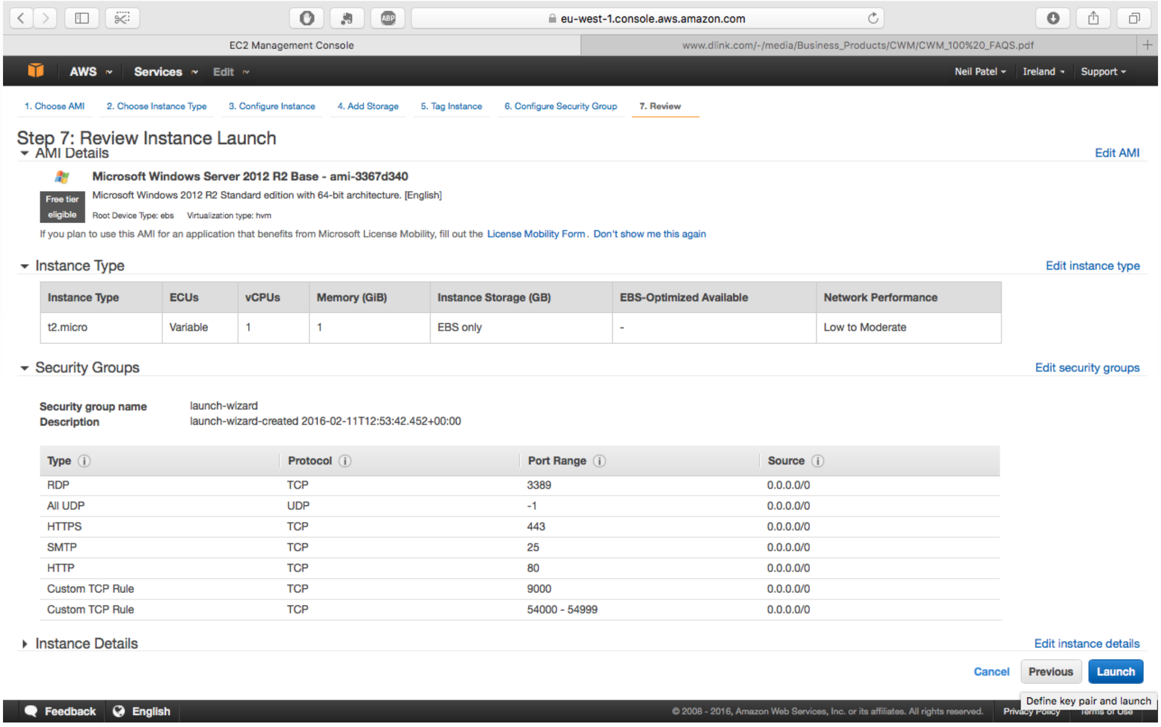
Add Rule

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel
Previous
Review and Launch
Feedback
English
© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Step 7

Review Instance Launch. Use this page to review your configuration, and when ready, click Launch.



Step 7: Review Instance Launch

AMI Details — Edit AMI

Microsoft Windows Server 2012 R2 Base - ami-3367d340
Free tier eligible
Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]
Root Device Type: ebs Virtualization type: hvm
If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the License Mobility Form. Don't show me this again

Instance Type — Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups — Edit security groups

Security group name launch-wizard
Description launch-wizard-created 2016-02-11T12:53:42.452+00:00

Type	Protocol	Port Range	Source
RDP	TCP	3389	0.0.0.0/0
All UDP	UDP	-1	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
SMTP	TCP	25	0.0.0.0/0
HTTP	TCP	80	0.0.0.0/0
Custom TCP Rule	TCP	9000	0.0.0.0/0
Custom TCP Rule	TCP	54000 - 54999	0.0.0.0/0

Instance Details — Edit instance details

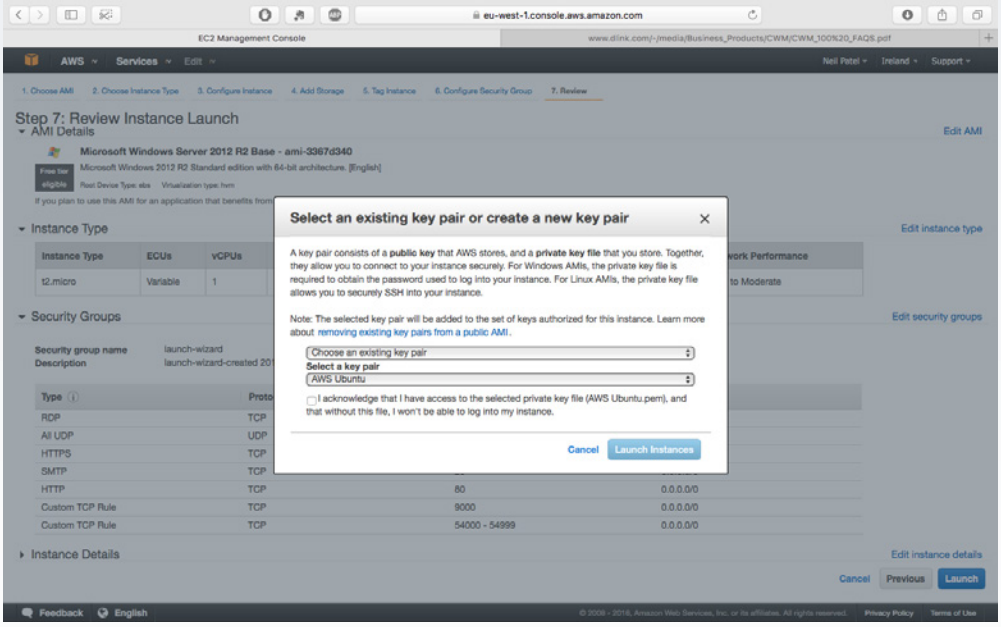
Cancel
Previous
Launch
Define key pair and launch
Feedback
English
© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Step 8

You will be prompted to Select an existing key pair or create a new key pair. An AWS Key Pair allows you to securely connect to your AWS instance.

Enter a Key Pair name, and click Download Key Pair.

Important: Ensure you have saved the .pem file to a safe place on your computer, 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.

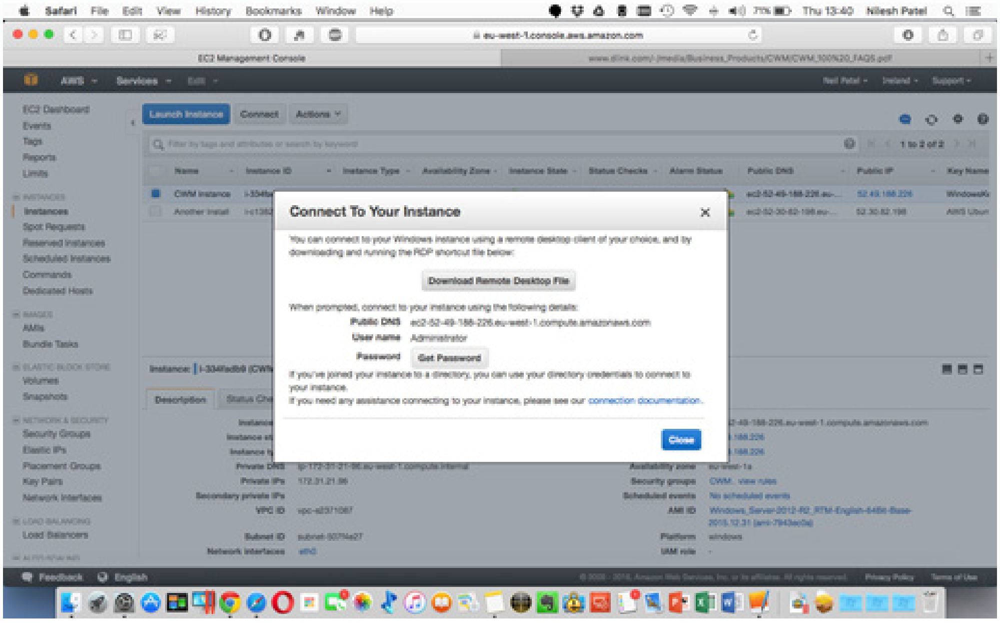
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair

Select a key pair: AWS Ubuntu

□ I acknowledge that I have access to the selected private key file (AWS Ubuntu.pem), and that without this file, I won't be able to log into my instance.

Download the shortcut to the Remote Desktop File.



Connect To Your Instance

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

When prompted, connect to your instance using the following details:

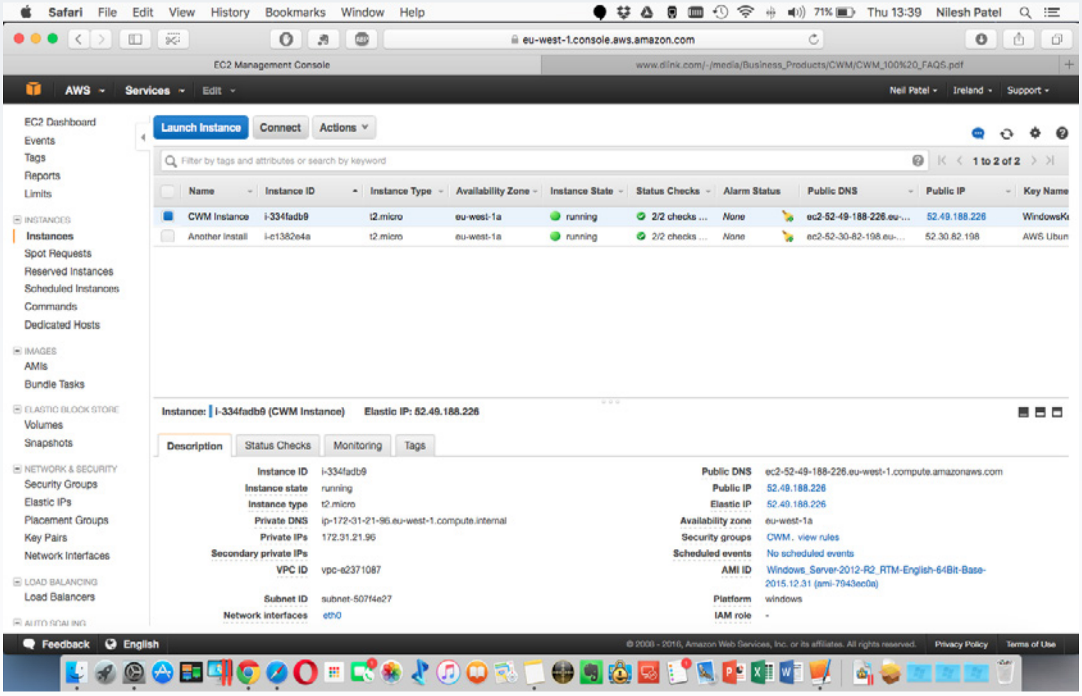
Public DNS: ec2-52-49-188-226.eu-west-1.compute.amazonaws.com

User name: Administrator

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

If you need any assistance connecting to your instance, please see our connection documentation.

Click on **Get Password** (it takes a few minutes for the instance to be launched before the password is available). **Browse** and navigate to the private key file you created when you launched the instance. Select the file and choose Open to copy the entire contents of the file into contents box. Click **Decrypt Password**, and the console displays the default administrator password for the Windows instance. Make a note of the default administrator password, or copy it to the clipboard. You need this password to connect to the instance.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP	Key Name
CWM Instance	i-334fadb9	t2.micro	eu-west-1a	running	2/2 checks ...	None	ec2-52-49-188-226.eu-...	52.49.188.226	WindowsK
Another Install	i-c1382e4a	t2.micro	eu-west-1a	running	2/2 checks ...	None	ec2-52-30-82-198.eu-...	52.30.82.198	AWS Ubun

Instance: i-334fadb9 (CWM Instance)   Elastic IP: 52.49.188.226

Instance ID	i-334fadb9	Public DNS	ec2-52-49-188-226.eu-west-1.compute.amazonaws.com
Instance state	running	Public IP	52.49.188.226
Instance type	t2.micro	Elastic IP	52.49.188.226
Private DNS	ip-172-31-21-96.eu-west-1.compute.internal	Availability zone	eu-west-1a
Private IPs	172.31.21.96	Security groups	CWM. view rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-e2371087	AMI ID	Windows_Server-2012-R2_RTM-English-64Bit-Base-2015.12.31 (ami-7943ec0a)
Subnet ID	subnet-507f4e27	Platform	windows
Network interfaces	eth0	IAM role	-

- If you opened the .rdp file, you'll see the Remote Desktop Connection dialog box.
- If you saved the .rdp file, navigate to the downloads directory, and open the .rdp file to display the dialog box.

You may get a warning that the publisher of the remote connection is unknown. If you are using Remote Desktop Connection from a Windows PC, choose Connect to connect to your instance.

When prompted, log in to the instance, using the administrator account for the operating system and the password that you recorded or copied previously. If your Remote Desktop Connection already has an administrator account set up, you might have to choose the Use another account option and enter the user name and password manually.

For more information about D-Link: www.dlink.com

D-Link European Headquarters. D-Link (Europe) Ltd., D-Link House, Abbey Road, Park Royal, London, NW10 7BX.

Updated June 2016