STORMSHIELD

TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK SECURITY FOR CLOUD - AMAZON WEB SERVICES

Document version : 1.0

Reference : snentno_SNS_For_Cloud_Amazon_Web_Services

Table of contents

Introduction

This document will guide you through the main steps towards setting up your Stormshield Network Security for Cloud on Amazon Web Services (AWS).

Before you start…

Please make sure you have completed the following steps before you start deploying your Stormshield Network Security for Cloud instance.

Choose the EC2 instance type matching your needs

Your Cloud UTM will be deployed on an EC2 instance. Several choices of EC2 instance types will be offered to you, depending on the resources you need.

Here are the minimal requirements to run your Cloud UTM:

Required RAM	Required Drive Space	Virtual CPUs
2 GB	10 GB	1 – 4

The M3 Medium (m3.medium) instance type will be the best choice for standard deployments.

Get your Cloud UTM license

Once deployed, your Cloud UTM will require a software license to run properly. The license you need will depend on the number of servers your Cloud UTM will protect.

Number of protected EC2 servers	Required Stormshield Network Security for Cloud license
1 to 5	VS5
6 to 10	VS10
More than 10	VU

Please contact your Stormshield Network distributor to order a license for your Cloud UTM. If you don't already have a distributor, you can use our partner locator website.

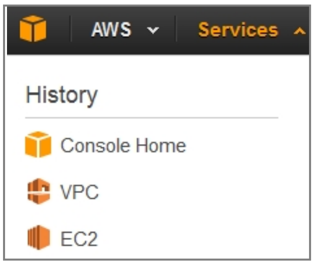
Create an "Allow All" Security Group in your AWS Console

As your Stormshield Network Security for Cloud will provide security to your network by itself, the Amazon Web Services network filter to and from your Cloud UTM instance should be deactivated.

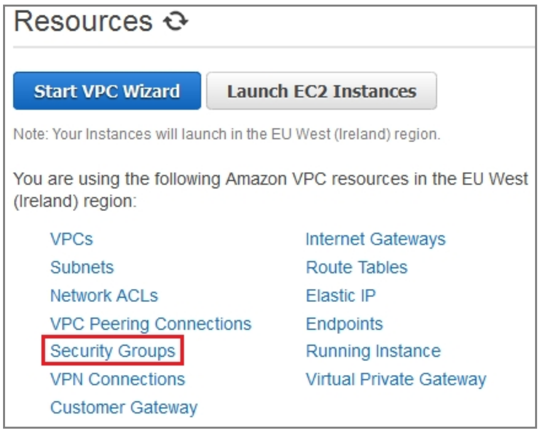
In order to do this, create a Security Group allowing all traffic. This Security Group will later be attached to your Stormshield Network Security for Cloud instance.

1. Log in to your AWS Console (https://console.aws.amazon.com).

2. In the **Services** menu, select the **VPC** section.



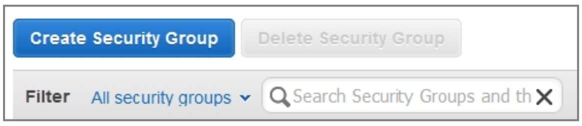
3. In the **Resources** menu, select **Security Groups**.



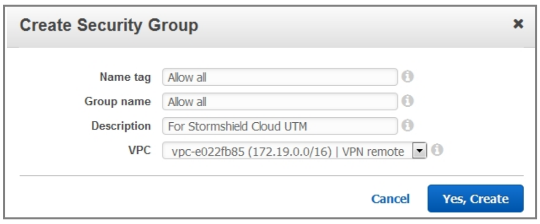
Note: Your Instances will launch in the EU West (Ireland) region.

You are using the following Amazon VPC resources in the EU West (Ireland) region:

4. Create a new Security Group.

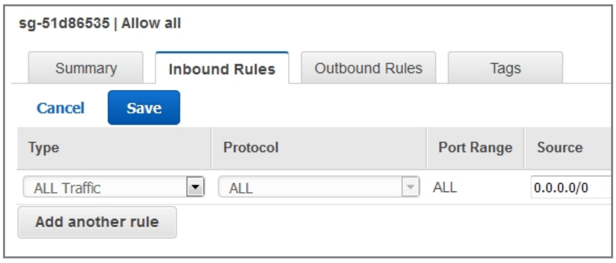


5. Name this new Security Group, select your VPC and click on "**Yes, Create**".



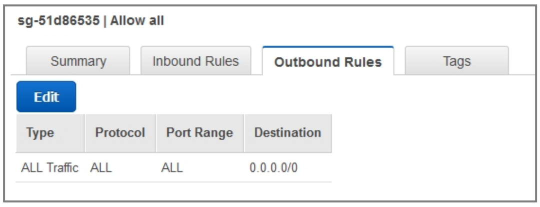
Name tag: Allow all
Group name: Allow all
Description: For Stormshield Cloud UTM
VPC: vpc-e022fb85 (172.19.0.0/16) | VPN remote

6. In the *Inbound* tab of this Security Group, click on **Edit**, select **All Traffic**, indicate 0.0.0.0/0 as **Source** and click on **Save**.


sg-51d86535 | Allow all

Type	Protocol	Port Range	Source
ALL Traffic	ALL	ALL	0.0.0.0/0

7. The *Outbound* tab should already be set to allow all outbound traffic. If it isn't, perform the same actions as for Inbound traffic.


sg-51d86535 | Allow all

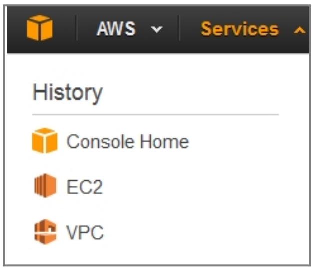
Type	Protocol	Port Range	Destination
ALL Traffic	ALL	ALL	0.0.0.0/0

Your Security Group is now ready to be used during the creation of your Stormshield Network Security for Cloud instance.

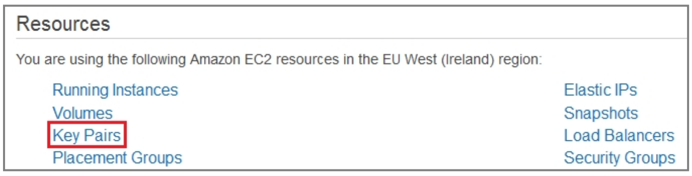
Create a Key Pair in your AWS Console

To secure SSH access to your Stormshield Network Security for Cloud instance, please select an existing Key Pair when creating the instance. If no such Key Pair exists or if you want to use a new one for this instance, you can create it as follows:

1. In the menu **Services**, select **EC2**

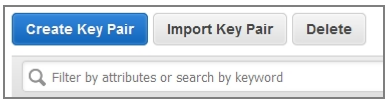


2. In the **Resources** menu, select **Key Pairs.**


Resources

You are using the following Amazon EC2 resources in the EU West (Ireland) region:

3. Click on **Create Key Pair** and provide a name for this new Key Pair.

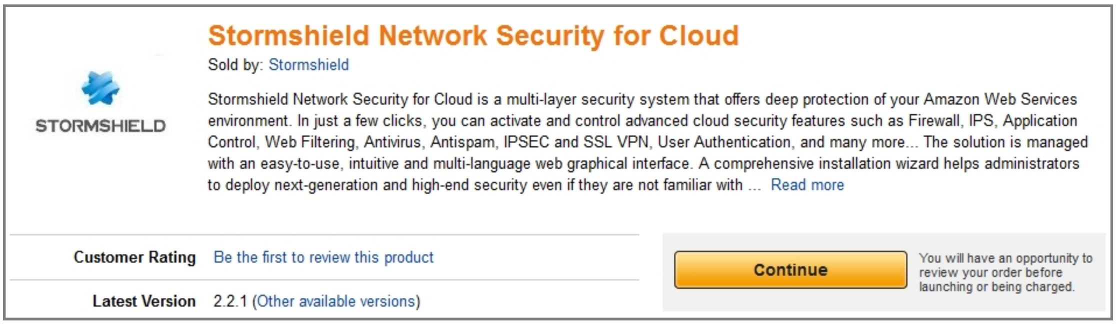


4. Download the Key Pair provided in *pem* format and store it in a safe place on your computer.

Deploying your Cloud UTM

1. Click on the following link: Stormshield Network Security for Cloud

2. Once you've reached the Product Description page, click on **Continue**.


Stormshield Network Security for Cloud

Sold by: Stormshield

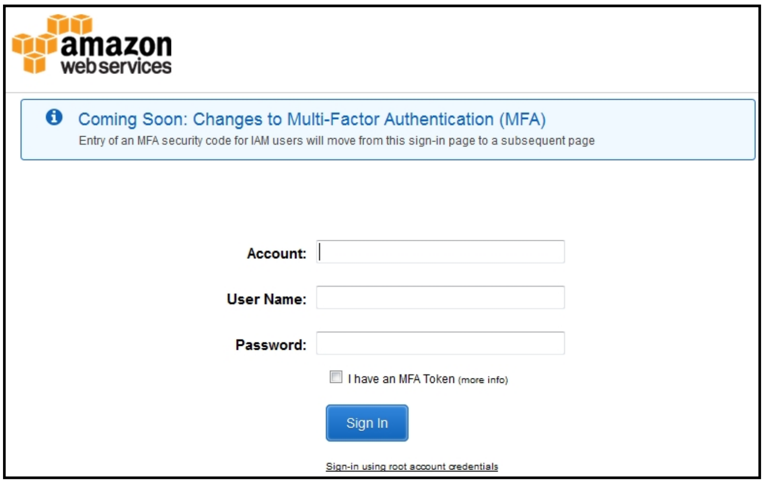
Stormshield Network Security for Cloud is a multi-layer security system that offers deep protection of your Amazon Web Services environment. In just a few clicks, you can activate and control advanced cloud security features such as Firewall, IPS, Application Control, Web Filtering, Antivirus, Antispam, IPSEC and SSL VPN, User Authentication, and many more... The solution is managed with an easy-to-use, intuitive and multi-language web graphical interface. A comprehensive installation wizard helps administrators to deploy next-generation and high-end security even if they are not familiar with ... Read more

Customer Rating Be the first to review this product

Latest Version 2.2.1 (Other available versions)

You will have an opportunity to review your order before launching or being charged.

3. If not already done, **Sign in** using your Amazon.com account.



amazon webservices

Coming Soon: Changes to Multi-Factor Authentication (MFA)

Entry of an MFA security code for IAM users will move from this sign-in page to a subsequent page

Account:

User Name:

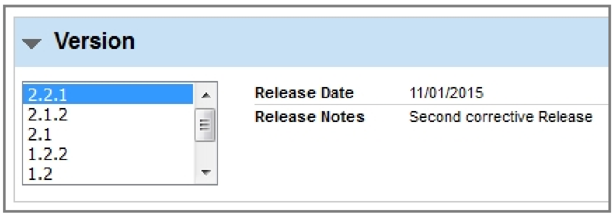
Password:

□ I have an MFA Token (more info)

Sign In

Sign-in using root account credentials

4. If you don't want to deploy the last available version of the Stormshield Network software, select the version you want in the **Version** section.



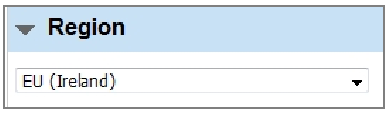
Version

2.2.1
2.1.2
2.1
1.2.2
1.2

Release Date	11/01/2015
Release Notes	Second corrective Release

5. The region where you will deploy the EC2 instance running your Cloud UTM might have an impact on several factors, including:
   - AWS charges for this Instance,
   - Network performance,
   - Local legislation

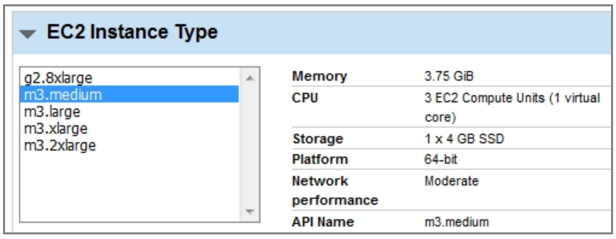
You must deploy your Cloud UTM in the region where your protected AWS servers and VPC are already deployed. Select the region in the **Region** section.



Region

EU (Ireland)

6. In the **EC2 Instance Type** section, select the EC2 Instance Type you need (see Choose the EC2 instance Type matching your needs).

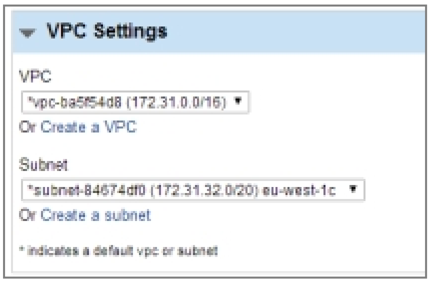


EC2 Instance Type

g2.8xlarge
m3.medium
m3.large
m3.xlarge
m3.2xlarge

Memory	3.75 GiB
CPU	3 EC2 Compute Units (1 virtual core)
Storage	1 x 4 GB SSD
Platform	64-bit
Network performance	Moderate
API Name	m3.medium

7. Set your **VPC Settings** to insert your Cloud UTM into your AWS infrastructure.



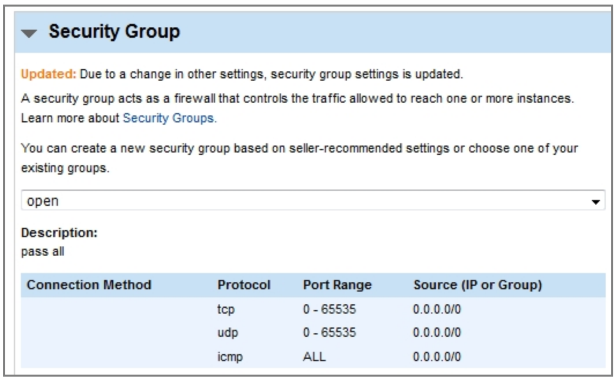
VPC Settings

VPC
*vpc-ba5f54d8 (172.31.0.0/16)
Or Create a VPC

Subnet
*subnet-84674df0 (172.31.32.0/20) eu-west-1c
Or Create a subnet

* indicates a default vpc or subnet

8. In the **Security Group** section, select the previously created Security Group allowing all inbound and outbound traffic (*Allow all* in the example).



Security Group

Updated: Due to a change in other settings, security group settings is updated.

A security group acts as a firewall that controls the traffic allowed to reach one or more instances. Learn more about Security Groups.

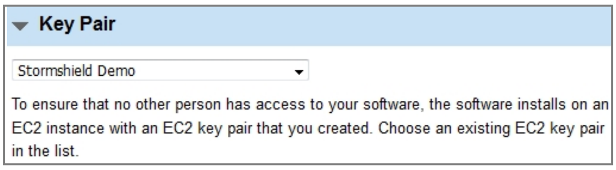
You can create a new security group based on seller-recommended settings or choose one of your existing groups.

open

Description:
pass all

Connection Method	Protocol	Port Range	Source (IP or Group)
	tcp	0 - 65535	0.0.0.0/0
	udp	0 - 65535	0.0.0.0/0
	icmp	ALL	0.0.0.0/0

9. Select the Key Pair you want to install on your instance.

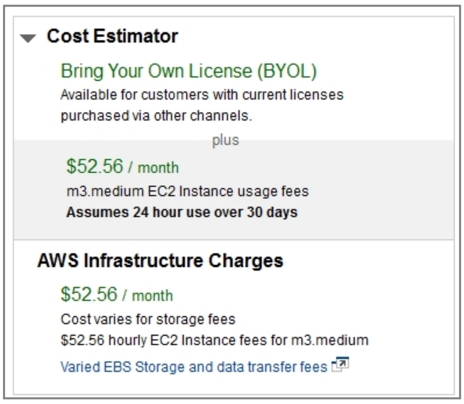


Key Pair

Stormshield Demo

To ensure that no other person has access to your software, the software installs on an EC2 instance with an EC2 key pair that you created. Choose an existing EC2 key pair in the list.

10. Check your **Monthly estimate** . This represents AWS Infrastructure Fees for the EC2 Instance Type and the Region you selected.



Cost Estimator

Bring Your Own License (BYOL)
Available for customers with current licenses purchased via other channels.

plus

$52.56 / month
m3.medium EC2 Instance usage fees
Assumes 24 hour use over 30 days

AWS Infrastructure Charges

$52.56 / month
Cost varies for storage fees
$52.56 hourly EC2 Instance fees for m3.medium
Varied EBS Storage and data transfer fees

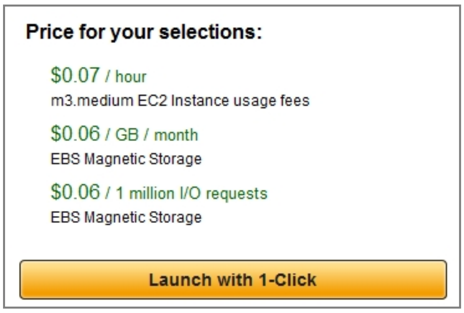
IMPORTANT

EBS Storage is not included in these fees. Stormshield Network Security for Cloud will require 10 GB of EBS storage.

IMPORTANT

This amount includes AWS fees only. The SN license is not issued by AWS, as the Stormshield Network Security Cloud is provided with a Bring Your Own License (BYOL) model. The SN software license must be ordered from your distributor (see **Get your Cloud UTM license**).

11. Click on **Launch with 1-Click**.



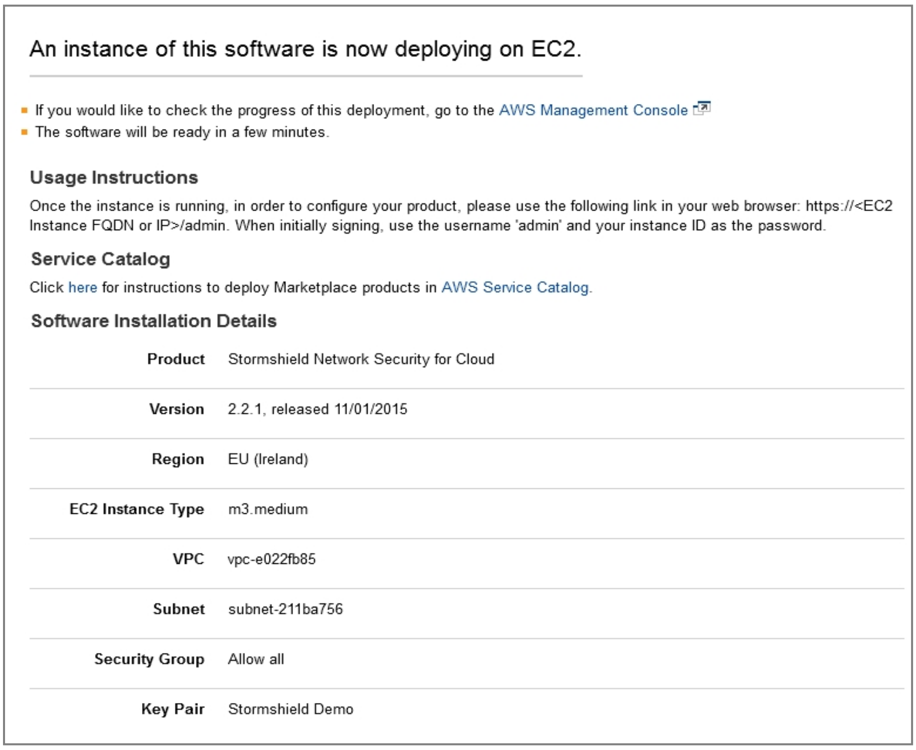
Price for your selections:

$0.07 / hour
m3.medium EC2 Instance usage fees

$0.06 / GB / month
EBS Magnetic Storage

$0.06 / 1 million I/O requests
EBS Magnetic Storage

12. Your instance is now ready to be deployed.



An instance of this software is now deploying on EC2.

- If you would like to check the progress of this deployment, go to the AWS Management Console
- The software will be ready in a few minutes.

Usage Instructions

Once the instance is running, in order to configure your product, please use the following link in your web browser: https://<EC2 Instance FQDN or IP>/admin. When initially signing, use the username 'admin' and your instance ID as the password.

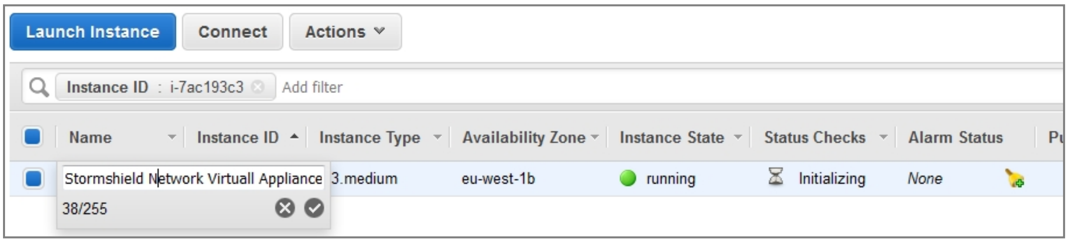
Service Catalog

Click here for instructions to deploy Marketplace products in AWS Service Catalog.

Software Installation Details

Product	Stormshield Network Security for Cloud
Version	2.2.1, released 11/01/2015
Region	EU (Ireland)
EC2 Instance Type	m3.medium
VPC	vpc-e022fb85
Subnet	subnet-211ba756
Security Group	Allow all
Key Pair	Stormshield Demo

13. In the AWS console, you can now edit the **Name** of your instance.



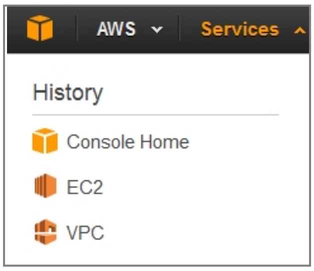
Instance ID : i-7ac193c3

☐	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Pu
☐	Stormshield Network Virtuall Appliance 38/255		3.medium	eu-west-1b	● running	Initializing	None	

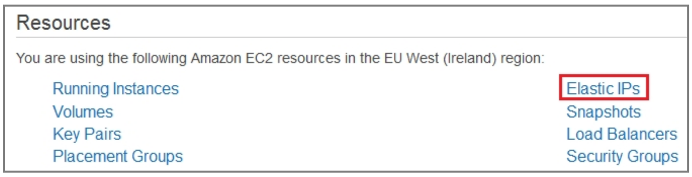
Allocate a public IP address to your instance

To enable remote administration of the firewall, you must define a public IP address (Elastic IP) and assign it to the firewall.

1. In the menu **Services**, select **EC2**

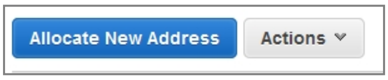


2. In the **Resources** menu, select **Elastic IPs.**

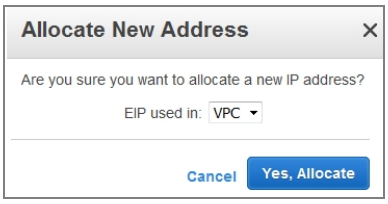

Resources

You are using the following Amazon EC2 resources in the EU West (Ireland) region:

3. Click on **Allocate New Address**



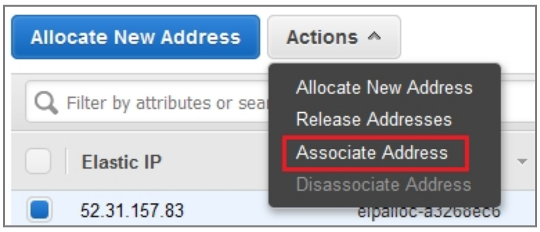
4. Select **VPC** for allocation and confirm (**Yes, Allocate**)


Allocate New Address

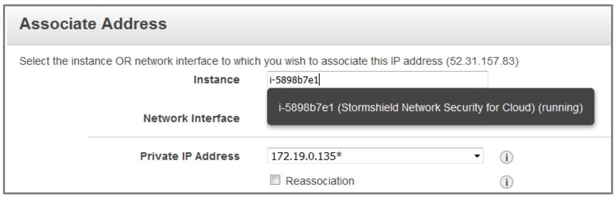
Are you sure you want to allocate a new IP address?

EIP used in: VPC

5. Select the newly created IP address and click on **Actions** > **Associate Address**



6. In the **Instance** field, select your Stormshield Network Security for Cloud new instance and click on **Associate**.


Associate Address

Select the instance OR network interface to which you wish to associate this IP address (52.31.157.83)

Instance: i-5898b7e1

i-5898b7e1 (Stormshield Network Security for Cloud) (running)

Network Interface

Private IP Address: 172.19.0.135*

□ Reassociation

7. You can access the Stormshield Network Administration Console with your web browser using the link *https://<EC2 Instance FQDN or IP>/admin*, where *<EC2 Instance FQDN or IP>* is the FQDN or IP of the EC2 instance running Stormshield Network Security for Cloud.

8. The default login is **admin**, and the default password is your EC2 instance ID (available in the EC2 Instances console).

   NOTE

   You will be prompted to change the **admin** account password at the first logon on your Stormshield Network Security for Cloud instance.

9. You can now set up your Stormshield Network Security for Cloud instance. Do not forget to install your license (see **Get your Cloud UTM license**) as soon as possible.