



Firebox Cloud

Deployment Guide

Firebox Cloud for AWS and Microsoft Azure

About This Guide

The *Firebox Cloud Deployment Guide* is a guide for deployment of a WatchGuard Firebox Cloud virtual security appliance. For the most recent product documentation, see the *Fireware Help* on the WatchGuard website at <https://www.watchguard.com/wgrd-help/documentation/overview>. Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 10/26/2023

Copyright, Trademark, and Patent Information

Copyright © 1998-2023 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online at <https://www.watchguard.com/wgrd-help/documentation/overview>.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide.

The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter, @WatchGuard on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

Contents

Introduction to Firebox Cloud	7
About Firebox Cloud.....	7
Firebox Cloud Use Cases.....	8
Protect Virtual Servers.....	8
Branch Office VPN.....	8
Mobile VPN Gateway.....	8
About Microsoft Azure.....	9
About AWS.....	10
Firebox Cloud System Requirements	11
Firebox Cloud License Options	12
License Types.....	12
Licensed Security Services.....	13
Deploy Firebox Cloud on Microsoft Azure	16
Identify your Firebox Cloud Software Plan and License Type.....	16
Supported Instance Types.....	16
Create a Key Pair for SSH Authentication.....	17
Deploy Firebox Cloud.....	19
Find the Instance ID (VM ID).....	24
Activate your Firebox Cloud License.....	24
Run the Firebox Cloud Setup Wizard.....	25
Connect to Fireware Web UI.....	26
Add the Feature Key.....	27
Next Steps.....	28
Enable Feature Key Synchronization.....	28
Configure Firebox Cloud to Send Feedback to WatchGuard.....	28
Configure Firewall Policies and Services.....	29

Deploy Firebox Cloud on AWS	30
AWS Regions and Availability Zones	30
Supported Instance Types	31
Before You Begin	31
AWS Identity and Access Management (IAM)	31
Deployment Overview	32
Allocate or Associate an Elastic IP Address	33
Allocate an Elastic IP Address	33
Associate an Elastic IP Address	34
Create a VPC with Public and Private Subnets	34
Create an Instance of Firebox Cloud	35
Disable Source/Destination Checks	41
Assign an Elastic IP Address to the External Interface	41
Configure the Default Route	43
Verify the Instance Status	44
Find the Instance ID (VM ID)	44
Activate your Firebox Cloud License (BYOL Only)	44
Run the Firebox Cloud Setup Wizard	46
Connect to Fireware Web UI	47
Add the Feature Key (BYOL Only)	48
Next Steps	49
Enable Feature Key Synchronization	49
Configure Firebox Cloud to Send Feedback to WatchGuard	49
Configure Firewall Policies and Services	50
Troubleshooting	50
Firebox Cloud Feature Differences	51
Administration	51
Licensing and Services	51

Network Interfaces	51
Default Firebox Configuration	52
Fireware Features	52
View Firebox Cloud VM Information	55
VM Information in Fireware Web UI	55
The Front Panel Dashboard	55
The VM Information System Status Page	55
The Interfaces Dashboard	56
VM Information in Firebox System Manager	57
Use Firebox Cloud to Protect a Web Server	59
Step 1 – Launch an Instance of Firebox Cloud	59
Step 2 – Add A Static NAT Action	60
Step 3 – Add HTTP and HTTPS Proxy Policies	61
Add an HTTP-Proxy Policy	61
Add an HTTPS-Proxy Policy	62
Import a Proxy Server Certificate	64
Step 4 – Enable Subscription Services	65
Enable Gateway AntiVirus	65
Enable Intrusion Prevention Service (IPS)	65
Enable Botnet Detection	65
Enable Data Loss Prevention	66
Configure Geolocation	66
Enable Logging for Firebox Cloud	67
Configure Logging to WatchGuard Cloud	67
Configure Logging to Dimension	67
Open the Configuration File for a Firebox Cloud Instance	69
Download and Open the Configuration File	69
Download and Open the Diagnostic Log Message File	70

Changes that Require a Firebox Cloud Reboot	71
Administer Firebox Cloud with the CLI	72
Reset the Firebox to Factory-Default Settings	72
Add Firebox Cloud to WatchGuard Cloud (Cloud-Managed)	73
Before You Begin	73
Add a Firebox Cloud Device to WatchGuard Cloud	74
Upload the Payload and Connect the Firebox	78
Verify the Firebox Cloud Status	81
Additional Resources	82
Help Center and Technical Documentation	82
Technical Support	82
Troubleshooting	82
Monitor Your Firebox	82
Manage Users and Roles on Your Firebox	82
Firebox Upgrade, Downgrade, and Migration	82
Firebox Backup and Restore	82

Introduction to Firebox Cloud

The WatchGuard® Firebox security platform delivers unparalleled unified threat management, superior performance, ease of use, and value for your growing network. Fireware OS and WatchGuard security services give you fully integrated protection from spyware, viruses, worms, trojans, web-based exploits, and blended threats. From firewall and VPN protection, to secure remote access, WatchGuard devices support a broad range of network environments.

About Firebox Cloud

Firebox Cloud brings the proven features and services of the Firebox to the Amazon Web Services (AWS) and Microsoft Azure cloud computing platforms. Firebox Cloud uses the same powerful Fireware OS and most of the same subscription services available on other Firebox models. You can use Firebox Cloud to protect servers deployed on your private cloud, and you can use it as a secure VPN endpoint for connections to resources on your virtual network.

For greater visibility into the status of traffic and security on your virtual network, you can use WatchGuard Dimension to monitor Firebox Cloud. The Firebox Cloud BYOL license also includes a license for WatchGuard Cloud. After you activate a WatchGuard Cloud BYOL license, you can add the Firebox Cloud instance to your WatchGuard Cloud account. For information about how you can manage your Firebox Cloud instance as a cloud-managed device in WatchGuard Cloud, go to [Add Firebox Cloud to WatchGuard Cloud \(Cloud-Managed\)](#).

Firebox Cloud is available for AWS and Microsoft Azure cloud computing platforms.

Firebox Cloud Use Cases

You can use Firebox Cloud to protect any virtual network on AWS or Azure. These use cases describe some of the ways you can use Firebox Cloud to add security to your virtual network.

Protect Virtual Servers

To provide protection to one or more virtual servers that are accessible from the Internet, you can install a Firebox Cloud instance. Your instance of Firebox Cloud is then the gateway for inbound connections to your servers from the internet. You configure policies and security services on your instance of Firebox Cloud to control traffic to your virtual servers.

For a summary of how to configure policies and services on Firebox Cloud for inbound connections to a protected web server, go to [Use Firebox Cloud to Protect a Web Server](#).

Branch Office VPN

You can configure your Firebox Cloud as a branch office VPN (BOVPN) gateway endpoint so you can maintain a secure VPN connection between your virtual network resources and other networks protected by a Firebox or compatible VPN gateway endpoint. You can also configure your Firebox Cloud as a BOVPN over TLS Server or Client. Firebox Cloud supports all the same VPN features as other Firebox models.

Mobile VPN Gateway

You can also enable Firebox Cloud to accept VPN connections from SSL, IPSec, IKEv2, and L2TP mobile VPN clients, and configure policies to control user and group access to your protected AWS network resources.

About Microsoft Azure

Microsoft Azure is Microsoft's cloud computing platform that provides data management, compute, networking and performance services at a variable cost based on the resources you use. If you are new to Azure, you must understand the Azure terms and concepts in this section before you deploy Firebox Cloud.

Virtual Network (Vnet)

An Azure Virtual Network is a logically isolated private virtual network environment in the Azure cloud. Firebox Cloud, and the virtual servers it protects, are all virtual machines that you deploy in a Virtual Network.

Virtual Machine Image (VHD)

A VHD file is a virtual hard disk image that contains a VM image. Firebox Cloud is distributed as a VHD file that you can use to deploy one or more Firebox Cloud instances.

Storage Account

Microsoft Azure Storage is a Microsoft-managed cloud service that provides storage. The Firebox Cloud VHD is stored in a container in your Storage Account.

Resource

A manageable item available through Azure. For example, a virtual machine, storage account, and virtual machine are each resources.

Resource Group

A group of Azure resources that you manage as a group. When you add a storage account, you specify the resource group it belongs to. Each resource can belong to only one group.

Template

An Azure template is a JSON file that defines the resources and settings required to deploy an application. To deploy Firebox Cloud, you fill out the required settings and specify required resources defined in the Firebox Cloud template.

VM ID (Instance ID)

The VM ID, or instance ID, is a unique identifier associated with an Azure virtual machine instance. For Firebox Cloud you use the instance ID to activate your Firebox Cloud license on the WatchGuard website. The Instance ID is also the default admin passphrase you use to connect to Firebox Cloud to run the setup wizard.

Regions and Availability Zones

Microsoft Azure has several regions around the world. Each region contains several Availability Zones. You must specify the region when you deploy a Firebox Cloud instance.

About AWS

Amazon Web Services (AWS) is a flexible, on-demand, cloud services platform that provides compute power, networking, database storage, and other services at a variable cost based on the resources you use. If you are new to AWS, you must understand the AWS terms and concepts in this section before you deploy Firebox Cloud.

Amazon Virtual Private Cloud (VPC)

An Amazon VPC is a logically isolated private virtual network environment in the AWS cloud. Firebox Cloud, and the virtual servers it protects, are all virtual machines that you deploy in a VPC.

Amazon Elastic Compute Cloud (EC2)

Amazon EC2 is a virtual server hosting service that provides scalable computing capacity in the AWS cloud

Amazon Machine Image (AMI)

An AMI is a virtual machine template that you use to deploy a virtual server in AWS. Firebox Cloud is delivered as an .AMI file that you use to deploy Firebox Cloud in your AWS VPC.

EC2 Instance

To launch one or more EC2 instances, you use an .AMI file. Each instance is a copy of the .AMI that runs as a virtual server. When you launch a new instance, you select the instance type, which determines the amount of CPU, storage, and network capabilities assigned to the instance. Firebox Cloud runs as an EC2 instance in your Amazon VPC. Each instance has a unique Instance ID.

Elastic IP Address (EIP)

An Elastic IP address is a static public IP address that you can assign to an EC2 instance. First, you allocate an Elastic IP address to a VPC, and then you associate it with an EC2 instance in the VPC. For Firebox Cloud, you allocate an Elastic IP address for the external interface.

Security Group

The security group is a virtual firewall that controls which inbound and outbound traffic is allowed to reach the associated instances. In the security group, you define rules that control what traffic to allow. When you launch an instance, you must specify at least one security group.

AWS Regions and Availability Zones

AWS has multiple AWS Regions. Each region contains several Availability Zones. A VPC can contain subnets in different Availability Zones.

Firebox Cloud System Requirements

Firebox Cloud can run on Amazon Web Services (AWS) and Microsoft Azure cloud computing platforms.

Firebox Cloud CPU and memory requirements:

- Minimum CPU cores: 2
- Minimum total memory: 2048 MB
- Recommended minimum total memory: 4096 MB



4096 MB is required to enable Access Portal and IntelligentAV, and to use the Full signature set for IPS/Application Control.

WatchGuard recommends an instance that has at least 1024 MB of memory for each CPU core. For example, if the instance has four CPU cores, we recommend a minimum total memory of 4096 MB. Refer to the AWS and Azure documentation to identify instances that meet these requirements.



For Firebox Cloud with BYOL license, the Firebox Cloud model determines the maximum number of CPU cores. For more information, go to [Firebox Cloud License Options](#).



For a BYOL license, Azure automatically selects an instance size based on the License Type you select.

Firebox Cloud License Options

Firebox Cloud is available in both the [Microsoft Azure Marketplace](#) and [AWS Marketplace](#) with two license options.

License Types

Bring Your Own License (BYOL)

With this license option, you pay Microsoft or Amazon for the virtual machine instance and resources it uses. You then purchase a license for Firebox Cloud separately from an authorized WatchGuard reseller. For Firebox Cloud with a *BYOL* license, you must activate a license key for Firebox Cloud on the WatchGuard website. Then, add the feature key to your Firebox Cloud instance, which enables you to configure all the licensed features. This feature key is unique to that instance and has an expiration date. You can purchase a renewal from an authorized WatchGuard reseller.

After you activate the BYOL license, you can add the Firebox Cloud instance to your WatchGuard Cloud account.

For more information, go to [Add a Firebox to WatchGuard Cloud](#).

For information about how you can manage your Firebox Cloud instance as a cloud-managed device in WatchGuard Cloud, go to [Add Firebox Cloud to WatchGuard Cloud \(Cloud-Managed\)](#).

For information about feature keys, go to [About Feature Keys](#).



The feature key is valid only for the instance ID you specify when you activate the license. If you want to move your Firebox Cloud license to a different instance of Firebox Cloud, you must contact WatchGuard customer care to help you activate the license for a different instance ID.

You can purchase a Firebox Cloud for one of four models. The models are based on the maximum number of CPUs that Firebox Cloud uses. The maximum throughput of Firebox Cloud depends on both the Firebox Cloud model, and the VM size.

For Firebox Cloud with a BYOL, the model determines the maximum supported throughput rates.

Firebox Cloud Model	Maximum AWS vCPUs or Azure CPU Cores	VPN (Gbps)
Small	2	0.4
Medium	4	1.5
Large	8	3
Extra Large	Unrestricted	Unrestricted

If you deploy Firebox Cloud on a virtual machine with more CPUs than the Firebox Cloud model supports, Firebox Cloud uses only the supported maximum number of CPUs.

For details about the BYOL option for AWS, go to [WatchGuard Firebox Cloud \(BYOL\)](#). Cost can vary based on resources used, and by region.

Hourly / Pay As You Go (PAYG)

With this license option, the cost of the license for Firebox Cloud and all security services is included in the price charged by Amazon or Microsoft. This provides a perpetual license with no fixed expiration date. There is no need to purchase, activate, or renew a separate license from WatchGuard.

Both the Azure Firebox Cloud and AWS (PAYG) option includes a 30 day free trial. For the 30 day trial period, there are no hourly software charges but Azure and AWS infrastructure charges still apply. After the 30 day trial expires, the instance converts to a paid subscription.

For details about the PAYG option and associated costs for Azure, go to [WatchGuard Subscription Costs for Azure PAYG](#).

For details about the Hourly AWS option and associated costs, go to [WatchGuard Firebox Cloud \(Hourly\)](#).



To switch a Firebox Cloud instance from one license type to another, you must deploy a new instance and move the configuration to the new instance. For information about how to move a Firebox configuration, go to [Move a Configuration to a New Firebox](#).

Licensed Security Services

Firebox Cloud supports these WatchGuard security services:

- Access Portal (requires Fireware v12.1 or higher)
- Application Control
- APT Blocker
- Botnet Detection
- Data Loss Prevention

- DNSWatch (supported with a BYOL license only)
- Gateway AntiVirus / Intelligent AntiVirus
- Geolocation
- IntelligentAV (supported for BYOL licenses and PAYG instances, and requires 4GB of memory)
- Intrusion Prevention Service (IPS)
- Reputation Enabled Defense
- spamBlocker and Quarantine Server (requires Fireware v12.2 or higher)
- WatchGuard Cloud Visibility (supported with a BYOL license only)
- WebBlocker



Firebox Cloud with an Hourly / Pay As You Go license does not support WatchGuard Cloud or DNSWatch.

Deploy Firebox Cloud on Microsoft Azure

Before you create a Firebox Cloud virtual machine, you must create a Microsoft Azure account. When you set up your account, you specify billing information and the credentials you use to connect to the Microsoft Azure portal. Firebox Cloud requires a storage account. You can create a storage account before you deploy Firebox Cloud, or you can create one as part of the deployment.

Identify your Firebox Cloud Software Plan and License Type

When you create a Firebox Cloud VM in Azure, you select one of these two software plans.

Firebox Cloud (BYOL)

With the Bring Your Own License (BYOL) software plan, you purchase a Firebox Cloud license for a specified size, **Small**, **Medium**, **Large**, or **Extra Large**. The Firebox Cloud license defines the maximum number of Azure CPU cores that the Firebox Cloud VM can use.

When you create a Firebox Cloud (BYOL) VM, you select a **License Type**. To deploy your VM with appropriate resources, select the License Type that matches your Firebox Cloud license size.

Firebox Cloud (PAYG)

With the Pay As You Go (PAYG) software plan, you do not purchase a Firebox Cloud license. The PAYG option includes a 30 day free trial.

For more information about license options and trials, go to [Firebox Cloud License Options](#).

Supported Instance Types

Firebox Cloud supports these instance families:

- Av2
- Amv2
- Dv3
- Dv4
- Dsv3
- Dsv4
- F
- Fsv2

All Azure services that are part of the deployment are mandatory to run Firebox Cloud. To deploy your instance of Firebox Cloud on Azure, you must complete the following procedures.



For information about how to deploy load balancers with Firebox Cloud, go to [Deploy Firebox Cloud with Azure Load Balancers](#).

Create a Key Pair for SSH Authentication

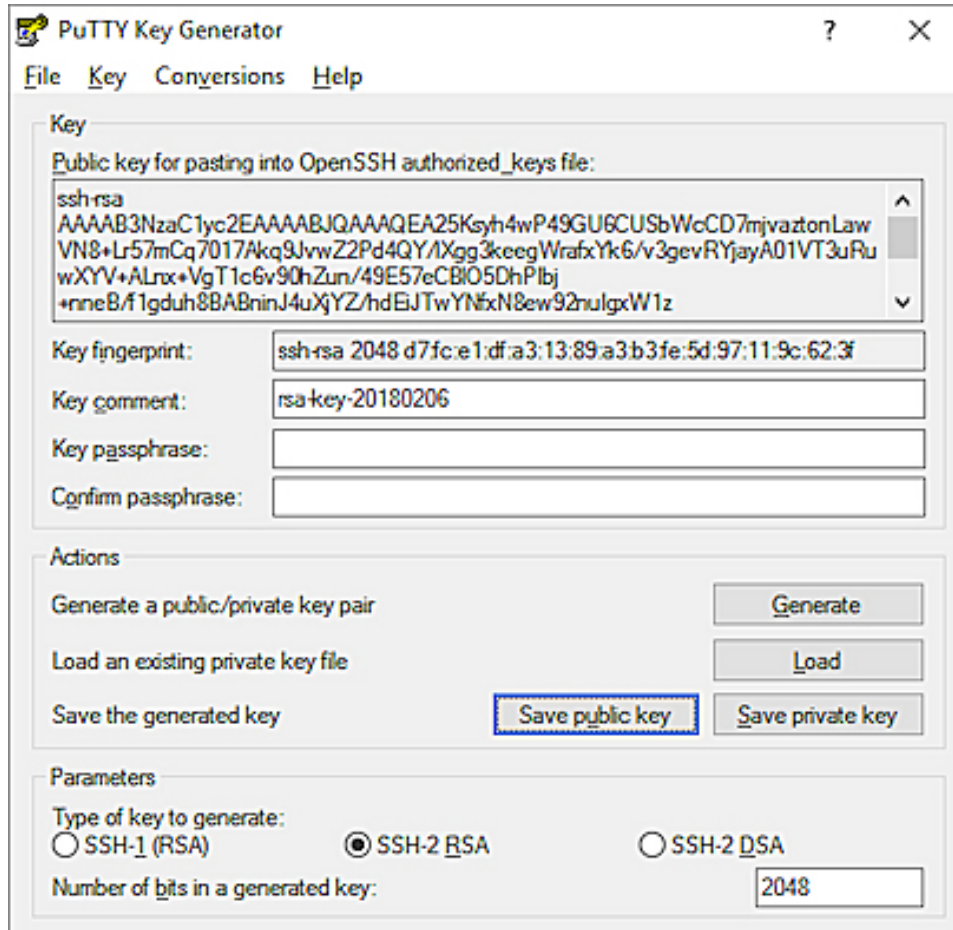
Before you create a Firebox Cloud instance, you must generate an SSH-2 RSA public key / private key pair. You can generate a new key pair when you configure your Firebox Cloud deployment, or you can use a tool such as `puttygen`, or `ssh-keygen` command in Linux to generate the key pair.

- Use the public key when you deploy your Firebox Cloud instance.
- Use the private key for ssh connections to the Fireware command line interface (CLI) for your Firebox Cloud instance.

To use the puttygen utility to generate an SSH-2 RSA key pair:

1. Download and install the PuTTYgen utility available from www.putty.org.
2. Start PuTTYgen.
3. Click **Generate**.
4. Move the mouse over the blank area to generate some randomness.

PuTTYgen uses the mouse movements as input to generate the key pair.



5. To save the generated public key to a file, click **Save public key**.
6. (Optional) Specify a passphrase to protect the private key file.
7. To save the generated private key to a file, click **Save private key**.

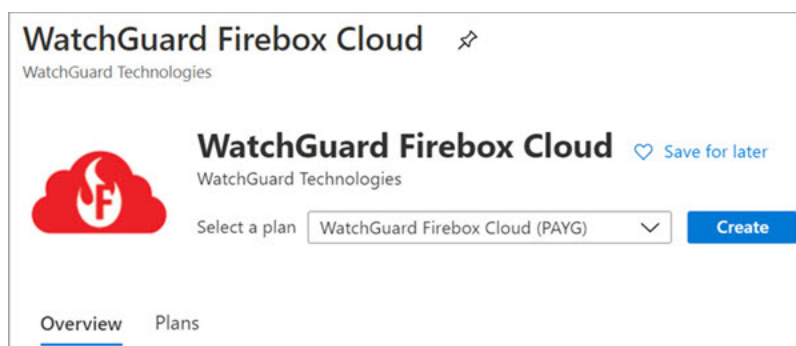


Save the private key in a secure location. You must provide the private key to connect to the Fireware command line interface.

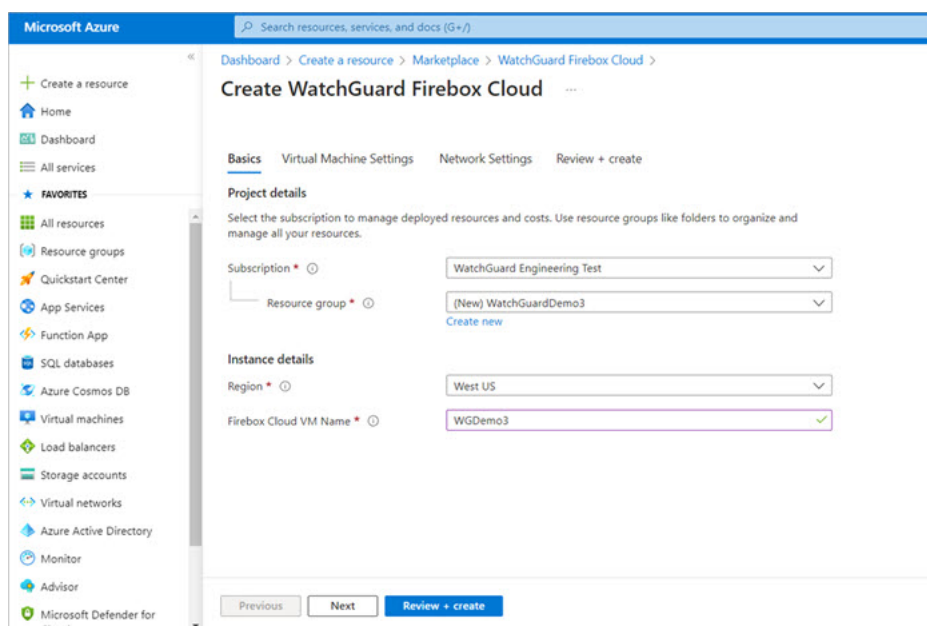
Deploy Firebox Cloud

To create the Firebox Cloud instance:

1. Log in to the Azure portal with your Microsoft Azure account credentials.
2. Click **Create a resource**.
The Azure Marketplace opens.
3. In the **Search services and marketplace** text box, enter **Firebox Cloud**.
4. Select **WatchGuard Firebox Cloud**.
The WatchGuard Firebox Cloud license options opens.



5. From the **Plan** drop-down list, select **WatchGuard Firebox Cloud (BYOL)** or **WatchGuard Firebox Cloud (PAYG)**.
6. Click **Create**.
The VM configuration steps opens.



7. On the **Basics** tab, specify basic information about your virtual machine.

Subscription

The name of the Azure subscription where the virtual machine and resources are stored. This is the account that Microsoft bills for VM use and storage.

Resource group

A resource group is a collection of resources that share the same lifecycle, permissions, and policies. All objects, such as networks and interfaces, and data for the Firebox Cloud instance will be associated with the resource group you specify. The resource group does not affect networking or connectivity from the Firebox to existing Azure resources.



Microsoft Azure does not support deployment of a managed application to a resource group with existing resources. You must create a new resource group or use an empty resource group.

Region

The Azure region for this Firebox Cloud instance.

Firebox Cloud VM Name

The name for the Firebox Cloud virtual machine in the Azure portal.

8. Click **Next**.

The *Virtual Machines Settings* configuration step opens if you are using the BYOL option, or the *VM Size and Key Data* section if you are using the PAYG option.

The screenshot shows the 'Create WatchGuard Firebox Cloud' wizard in the Microsoft Azure portal. The 'Virtual Machine Settings' tab is selected, displaying the following configuration options:

- Firebox Cloud License Type:** Small
- Size (Small):** 1x Standard A1 v2 (1 vcpu, 2 GB memory). A 'Change size' link is available.
- SSH public key source:** Generate new key pair
- Key pair name:** WGSSH Public Key
- Storage account:** (new) Storage account. A 'Create New' link is available.

At the bottom, there are three buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next : Network Settings >'.

9. In the **Virtual Machine Settings** step, specify virtual machine configuration details.*Firebox Cloud License Type and VM Size – for Firebox Cloud (BYOL)*

For a BYOL license, select the Firebox Cloud License Type. This is the Firebox Cloud license you purchased from WatchGuard or a WatchGuard reseller. Select **Small**, **Medium**, **Large** or **Extra Large**. After you select the License Type, an appropriate VM size is selected by default. To select a different size, click **Change size**. An Availability Set is created as part of the BYOL deployment.

Azure VM Tier and VM Size – for Firebox Cloud (PAYG)

For a PAYG license, select the Azure VM tier for the virtual machine. Select **Free Tier Eligible** or **Standard**. After you select the VM tier, an appropriate VM size is selected by default. To select a different size, click **Change size**.

SSH public key source

The public key for this Firebox. You can generate a new key pair, use an existing key stored in Azure, or use a tool such as `puttygen`, or `ssh-keygen` command in Linux to generate the key pair. You must use the private key associated with this public key to connect to the Firebox Cloud CLI.

Key pair name

The name for the key pair.

Storage account

The name of the storage account to store boot diagnostic log files. The storage account you select must not be in another resource group in your subscription. Boot diagnostic log files contain information that can help WatchGuard support troubleshoot issues.

- Click **Next**.

The screenshot shows the 'Create WatchGuard Firebox Cloud' wizard in the Azure portal, specifically the 'Network Settings' tab. The breadcrumb trail at the top reads: Dashboard > Create a resource > Marketplace > WatchGuard Firebox Cloud >. The page title is 'Create WatchGuard Firebox Cloud'. Below the title are four tabs: Basics, Virtual Machine Settings, Network Settings (which is selected), and Review + create. The 'Configure virtual networks' section contains the following fields:

- Virtual network ***: A dropdown menu showing '(new) vnet01' with a 'Create new' link below it.
- External (Public) subnet ***: A dropdown menu showing '(new) External (10.22.0.0/24)'.
- Trusted (Private) subnet ***: A dropdown menu showing '(new) Trusted (10.22.1.0/24)'.
- External Network Security Group ***: Three radio button options: 'None', 'Management Only' (which is selected), and 'Allow All'.

Below these fields are two informational messages in light blue boxes:

- A message with an information icon stating: 'A Network Security Group is not a set of policies on the Firebox Cloud.'
- A message with an information icon stating: 'This will only allow inbound access for Firebox Cloud Web UI, CLI, and WSM connections. All outbound connections are allowed. The security group policy can be modified post-deployment.'

At the bottom of the form are two more fields:

- Public IP address ***: A dropdown menu showing '(new) undefined' with a 'Create new' link below it.
- Domain name label ***: A text input field containing 'wgdemo3-63bda87333' with a green checkmark to its right.

At the very bottom of the form are three buttons: 'Previous', 'Next', and 'Review + create' (which is highlighted in blue).

- In the **Network Settings** step, specify required network configuration information.

Virtual network

The virtual network to use for this Firebox Cloud. By default, a new available address space with a /16 netmask is selected. You can use the default virtual network, edit the default virtual network, or choose another existing virtual network.

External (Public) subnet

Review and configure the subnet to use for the External (Public) network. By default, a new external network 10.7.0.0/24 is selected.

Trusted (Private) subnet

Review and configure the subnet to use for the Trusted (Private) network. By default, a new trusted network 10.7.1.0/24 is selected.

External Network Security Group

A network security group contains security rules that allow or deny inbound network traffic to, or outbound traffic from, the virtual machine. If you select **None**, no external network security group is applied. If you select **Management Only**, an external network security group is applied which allows inbound traffic on TCP 8080, TCP 4118, TCP 4117 for Web UI, CLI, and WatchGuard System Manager connections to the Firebox. If you select **Allow All**, all inbound traffic to the Firebox is allowed.

Public IP address

Select or create a public IP address to use for your Firebox Cloud external interface. For a new public IP address, specify a name, and select the SKU type (**Basic** or **Standard**). If you select a Basic SKU type, select the IP address assignment type, **Dynamic** or **Static**. If you select a **Standard** SKU type, select the routing preference, **Microsoft network** or **Internet**. For more information, go to [Routing Preference](#).



Inbound connections to a public IP address with the Standard SKU type fail until you create and associate a network security group and explicitly allow the desired inbound traffic. For more information, go to the article [IP address types and allocation methods in Azure](#) in the Microsoft Azure documentation.



To assign a secondary IP address, go to [Assign multiple IP addresses to virtual machines using the Azure portal](#).

Domain name label

Specify the DNS label for the Firebox Cloud public IP address. It must be all lowercase letters and numbers.

12. Click **Next**.
13. In the **Next: Review + Create** step, review the information, and correct any errors.
14. Click **Create**.

The deployment begins.

After the deployment is completed, you can go to the resource group or pin the VM to the Microsoft Azure dashboard.

Find the Instance ID (VM ID)

After you deploy your Firebox Cloud instance, you must find the Instance ID, also known as the VM ID. You will need this to activate your license, and to log in to the Fireware Web UI to run the Firebox Cloud Setup Wizard. You can find the instance ID in the name of the storage container for boot diagnostic logs.

To find the Firebox Cloud Instance ID:

1. In the Azure left navigation menu, select **Storage accounts**.
2. Click the name of the storage account associated with your Firebox Cloud instance.
3. In the **Data Storage** section, select **Containers**.
4. To find the boot diagnostic container, click the container to view its details.
5. On the container details page, in the **Location** field, the name of the boot diagnostic container is in the format:

```
<bootdiagnostics>-<vmname>-<vmid>
```

For example:

`bootdiagnostics-fbcloud-11111111-2222-3333-4444-f86331913a6d`, where `11111111-2222-3333-4444-f86331913a6d`, is the VMID.

6. Copy the VMID at the end of the container name.



You must have this instance ID to activate your Firebox Cloud license and to run the Firebox Cloud Setup Wizard.

Activate your Firebox Cloud License

For Firebox Cloud with a BYOL license, you must activate the Firebox Cloud serial number in the WatchGuard portal. Before you can activate Firebox Cloud, you must have the Firebox Cloud serial number you received from WatchGuard and you must know the Firebox Cloud Instance ID.

To activate your Firebox Cloud license:

1. Go to www.watchguard.com.
2. Click **Support**.
3. Click **Activate Products**.
4. Log in to your WatchGuard Customer or Partner portal account. If you do not have an account, you can create one.
5. If necessary, navigate to the Support Center and select **My WatchGuard > Activate Products**.
6. When prompted, provide your Firebox Cloud serial number and Instance ID.
7. When activation is complete, copy the feature key and save it to a local file.

For more information about how to activate your Firebox Cloud license, go to [Activate a WatchGuard Device or Feature](#).

Run the Firebox Cloud Setup Wizard

After you deploy Firebox Cloud, you can connect to Fireware Web UI through the public IP address to run the Firebox Cloud Setup Wizard. You use the wizard to set the administrative passphrases for Firebox Cloud.

To run the Firebox Cloud Setup Wizard:

1. Connect to Fireware Web UI for your Firebox Cloud with the public IP address:
`https://<eth0_public_IP>:8080`
2. Log in with the default Administrator account user name and passphrase:
 - User name – **admin**
 - Passphrase – The Firebox Cloud Instance ID
The Firebox Cloud Setup Wizard welcome page opens.
3. Click **Next**.
The setup wizard starts.
4. Review and accept the End-User License Agreement. Click **Next**.

The screenshot shows the 'Create passphrases for your Firebox Cloud' page in the Fireware Web UI. The page has a red header with the WatchGuard logo and a dark grey header with 'Fireware Web UI' and a user profile icon. The main content area has a title 'Create passphrases for your Firebox Cloud' and a subtitle 'Your Firebox Cloud has two built-in user accounts:'. Below this, it lists the privileges for 'admin' (read-write) and 'status' (read-only). It then instructs the user to 'Type the passphrase to use with each account' and 'Each passphrase must contain between 8 and 32 characters.' There are two sets of input fields: one for 'status (read-only)' and one for 'admin (read-write)', each with a 'Passphrase' field and a 'Confirm passphrase' field. At the bottom right, there are 'BACK' and 'NEXT' buttons.

5. Specify new passphrases for the built-in **status** and **admin** user accounts.
6. Click **Next**.
The configuration is saved to Firebox Cloud and the wizard is complete.




WatchGuard does not store any sensitive customer information in the Firebox Cloud configuration or on the Azure cloud-based platform.

Connect to Fireware Web UI

To connect to Fireware Web UI and administer Firebox Cloud:

1. Open a web browser and go to the public IP address for your instance of Firebox Cloud at:
`https://<eth0_public_IP>:8080`
2. Log in with the *admin* user account. Make sure to specify the passphrase you set in the Firebox Cloud Setup Wizard.

By default, Firebox Cloud allows more than one user with Device Administrator credentials to log in at the same time. To prevent changes by more than one administrator at the same time, the configuration is

locked by default. To unlock the configuration so you can make changes, click .

If you prefer to allow only one Device Administrator to log in at the same time, select **System > Global Settings** and clear the **Enable more than one Device Administrator to log in at the same time** check box.



Microsoft Azure automatically terminates your management connection to Firebox Cloud after 30 minutes of inactivity. To avoid unexpected disconnection of your management session, do not set the Management Session **Idle Timeout** in the Fireware **Authentication > Settings** page to a value higher than 30 minutes.

Add the Feature Key

If you have received or downloaded the Firebox Cloud feature key to a local file, in the Feature Key Wizard select **Yes I have a local copy of the feature key** and paste the feature key into the wizard.

If you activated a Firebox Cloud license in the WatchGuard portal, your feature key is available directly from WatchGuard. You must add this feature key to the Firebox Cloud configuration to enable all functionality and configuration options on Firebox Cloud.




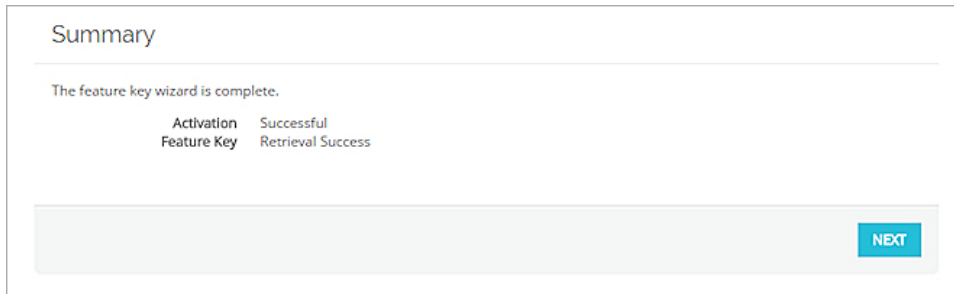
After you add the feature key, Firebox Cloud automatically reboots with a new serial number.

To add the feature key, from Fireware Web UI:

1. Select **System > Feature Key**.

The Feature Key Wizard page opens.

2. To unlock the configuration file, click .
3. To download and install the feature key, click **Next**.
4. On the **Summary** page, verify that your feature key was successfully installed.
When your feature key has been installed, Feature Key Retrieval Success appears on the Summary page.



5. Click **Next**.

The wizard completes and Firebox Cloud reboots with a new serial number.

Next Steps

After you run the setup wizard and add the feature key you can use Fireware Web UI or Policy Manager to configure the settings for Firebox Cloud.

Enable Feature Key Synchronization

Enable Firebox Cloud to automatically check for feature key updates when services are about to expire.

To enable feature key synchronization, in Fireware Web UI:

1. Select **System > Feature Key**.
2. Select the **Enable automatic feature key synchronization** check box.
3. Click **Save**.

To enable feature key synchronization, in Policy Manager:

1. Connect to Firebox Cloud in WatchGuard System Manager.
2. Open Policy Manager.
3. Select **System > Feature Keys**.
4. Select the **Enable automatic feature key synchronization** check box.
5. Click **Save**.

Configure Firebox Cloud to Send Feedback to WatchGuard

To enable Firebox Cloud to send feedback, in Fireware Web UI:

1. Select **System > Global Settings**.
2. Select the **Send device feedback to WatchGuard** check box.
3. Select the **Send Fault Reports to WatchGuard daily** check box.

To enable Firebox Cloud to send feedback, in Policy Manager:

1. Connect to Firebox Cloud in WatchGuard System Manager.
2. Open Policy Manager.
3. Select **Setup > Global Settings**.

4. Select the **Send device feedback to WatchGuard** check box.
5. Select the **Send Fault Reports to WatchGuard daily** check box.

Configure Firewall Policies and Services

The default WatchGuard and WatchGuard Web UI policies allow management connections from any computer on the trusted, optional, or external networks.



We strongly recommend that you do not allow management connections from the external network, and that you edit the WatchGuard and WatchGuard Web UI policies to remove the *Any-External* alias from the From list after you complete initial configuration.

To allow management from only a specific computer on the external network, you can add the address of that management computer to the From list in these policies.

Configure other policies and services as you would for any other Firebox.



Firebox Cloud does not support every Fireware feature. For a summary of the differences between Firebox Cloud and other Firebox models, go to [Firebox Cloud Feature Differences](#).

Deploy Firebox Cloud on AWS

WatchGuard Firebox Cloud brings the proven protection of Firebox UTM appliances to public cloud environments and enables organizations to extend their security perimeter to protect business critical assets in Amazon Web Services. Under the [AWS Shared Responsibility Model](#), security in the cloud falls to the customer. For this reason, it is crucial that administrators take every step possible to defend their data and deflect cyber criminals. Firebox Cloud can quickly and easily be deployed to protect a Virtual Private Cloud (VPC) from attacks such as Botnets, cross-site scripting, SQL injection attempts, and other intrusion vectors.

AWS Regions and Availability Zones

AWS has multiple AWS Regions. Each region contains several Availability Zones. A VPC can contain subnets in different Availability Zones.

Regions available in AWS:

- Africa (Cape Town) – af-south-1
- Asia Pacific (Hong Kong) – ap-east-1
- Asia Pacific (Tokyo) – ap-northeast-1
- Asia Pacific (Seoul) – ap-northeast-2
- Asia Pacific (Osaka) – ap-northeast-3
- Asia Pacific (Mumbai) – ap-south-1
- Asia Pacific (Singapore) – ap-southeast-1
- Asia Pacific (Sydney) – ap-southeast-2
- Asia Pacific (Jakarta) – ap-southeast-3
- AWS GovCloud (US-East) – us-gov-east-1
- AWS GovCloud (US-West) – us-gov-west-1
- Canada (Central) – ca-central-1
- Europe (Frankfurt) – eu-central-1
- Europe (Ireland) – eu-west-1
- Europe (London) – eu-west-2
- Europe (Milan) – eu-south-1
- Europe (Paris) – eu-west-3
- Europe (Stockholm) – eu-north-1
- Middle East (Bahrain) – me-south-1
- South America (São Paulo) – sa-east-1
- US East (N. Virginia) – us-east-1
- US East (Ohio) – us-east-2

- US West (N. California) – us-west-1
- US West (Oregon) – us-west-2



If you deploy a Firebox Cloud instance with the following instructions, each virtual machine instance is available in a single region and single availability zone.



AWS accounts have default quotas, or limits, for each AWS service. For information, go to [AWS Service Quotas](#).

Supported Instance Types

Firebox Cloud supports these instance sizes and families:

- M4
- M5
- C4
- C5

For detailed information about supported EC2 instance types for Firebox Cloud (BYOL) and Firebox Cloud (Hourly) specific to selected regions, go to the Firebox Cloud product information in the [AWS Marketplace](#).

Before You Begin

Deployment of Firebox Cloud on AWS requires familiarity with AWS. We recommend you have familiarity with networking, cloud networking, and network security.

For more information about how to get started with AWS, go to:

<http://docs.aws.amazon.com/gettingstarted/latest/awsgsg-intro/gsg-aws-intro.html>

For information about the AWS Management Console, go to:

<http://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/getting-started.html>

AWS Identity and Access Management (IAM)

Before you can use Firebox Cloud, you must create an AWS account. When you set up your AWS account, you specify billing information and the security credentials you use to connect to the AWS Management Console.

AWS IAM is a web service that enables you to securely control access to AWS resources. You use IAM to control who is authenticated and authorized to use resources. When you first create your AWS account, you begin with a root user, which is a single sign-in identity that has complete access to all AWS services and resources in the account. Because of this access, we recommend you do not use the root user for your Firebox Cloud deployment or operations. The root user should only be used to create your first IAM user.

To enable an IAM user to launch an instance with an IAM role or to attach or replace an IAM role for an existing instance, you must grant the user permission to use the following API actions:

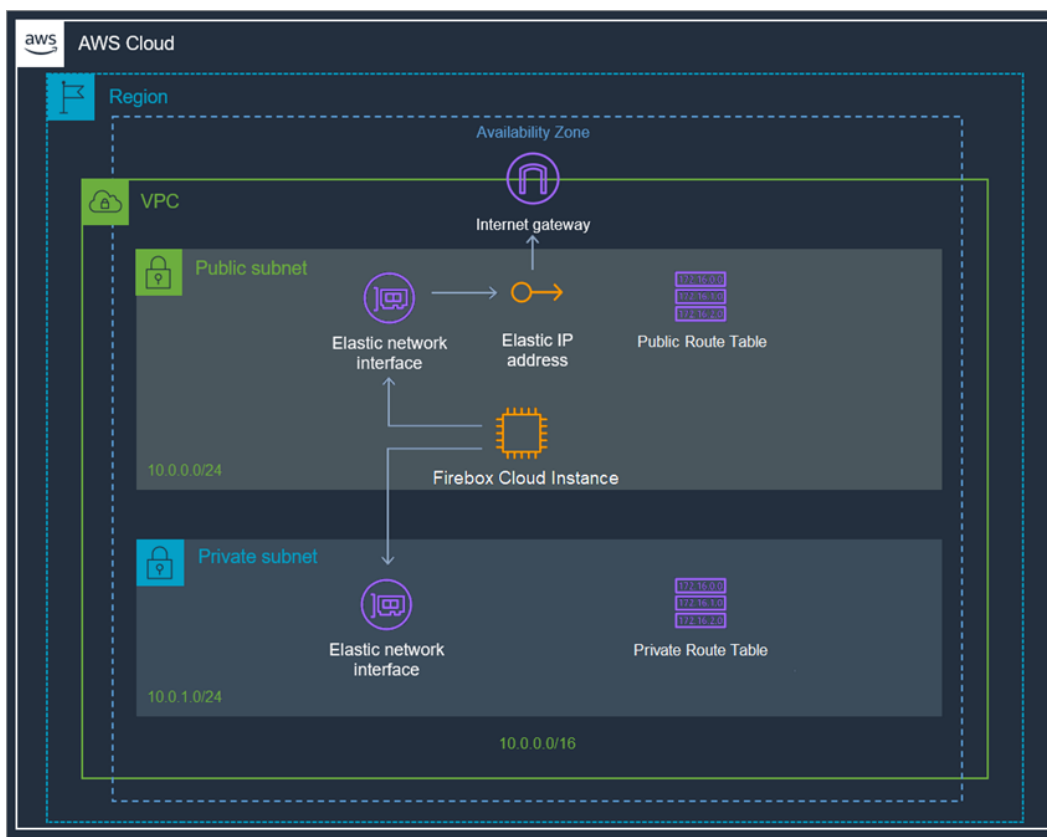
- iam:PassRole
- ec2:AssociateIamInstanceProfile
- ec2:ReplaceIamInstanceProfileAssociation

For more information about roles for Amazon EC2, go to [IAM Roles for Amazon EC2](#).

For more information about policies and permissions, go to [Policies and Permissions in IAM](#).

Deployment Overview

This diagram shows a basic Firebox Cloud deployment on AWS.



All AWS services that are part of the deployment are mandatory to run Firebox Cloud. To deploy your instance of Firebox Cloud on AWS, you must complete these procedures:

Allocate an Elastic IP address

Allocate an Elastic IP address from Amazon's pool of public IPv4 addresses, or from a custom IP address you brought to your AWS account.

Create a Virtual Private Cloud (VPC)

Use the VPC Wizard to create a VPC with public and private subnets.

Create an instance of Firebox Cloud

Launch an EC2 instance for Firebox Cloud with these properties:

- **VPC Configuration** – VPC with Public and Private Subnets
- **AMI** – WatchGuard Firebox Cloud
- **Instance Type** – If you select Firebox Cloud with a BYOL license, make sure to select the instance type that has the same number of vCPUs as the Firebox Cloud license you purchased
- **Network** – A VPC with public and private subnets
- **Interfaces** – Eth0 must use a public subnet; Eth1 must use a private subnet
- **Storage** – Keep the default size
- **Security Group** – Allow all inbound traffic

Disable the Source/Destination checks for Firebox Cloud

For your Firebox Cloud to function as a NAT device for your VPC, you must disable the source/destination check for the instance of Firebox Cloud.

Assign an Elastic IP address to the instance of Firebox Cloud

Assign an Elastic IP (EIP) address to the eth0 interface for your instance of Firebox Cloud.

Configure the default route for the private network

Change the routing for the private subnet so that it uses the instance of Firebox Cloud as the default gateway.

Check instance status

Check the state of the instance of Firebox Cloud to verify that it has powered up, that it has a public IP address and DNS server assigned, and the correct security group is configured.

Each of these procedures is described in detail in the next sections. Deployment will take approximately 20 minutes.

Allocate or Associate an Elastic IP Address

Before you create a VPC, you must allocate or associate an elastic IP to the external interface. You can either select an existing elastic IP, or allocate an elastic IP from Amazon's pool of IPv4 addresses.

Allocate an Elastic IP Address

To allocate an elastic IP:

1. Log in to the AWS Management Console at aws.amazon.com.
2. From the top navigation bar, select **Services > Compute > EC2**.
The EC2 Dashboard page opens.
3. In the **Network & Security** section, select **Elastic IPs**.
4. Click **Allocate Elastic IP address**.
The Allocate Elastic IP address page opens with Amazon's pool of IPv4 addresses selected.
5. Click **Allocate** and record your allocated elastic IP address.

Associate an Elastic IP Address

To associate an existing elastic IP address:

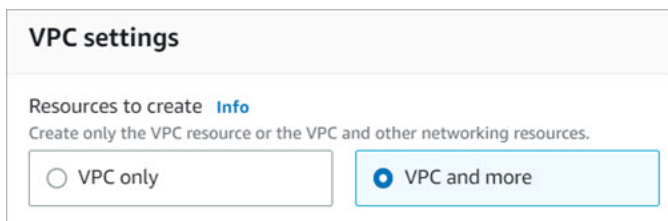
1. Log in to the AWS Management Console at aws.amazon.com.
2. From the top navigation bar, select **Services > Compute > EC2**.
The EC2 Dashboard page opens.
3. In the **Network & Security** section, select **Elastic IPs**.
4. Select the check box next to the elastic IP address you want to associate.
5. Select the **Actions** drop-down list. Click **Associate Elastic IP address**.
The Associate Elastic IP address page opens.
6. In the **Resource type** section, select **Network interface**.
7. In the **Network interface** drop-down list, select a network interface.
8. In the **Private IP address** drop-down list, select a private IP address.
9. Click **Associate**.

Create a VPC with Public and Private Subnets

If you do not already have a VPC with public and private subnets, you must create one.

To use the VPC Wizard to create a VPC:

1. Log in to the AWS Management Console at aws.amazon.com.
2. From the top navigation bar, select **Services > Networking & Content Delivery > VPC**.
The VPC Dashboard page opens.
3. Click **Create VPC**.
4. In the **VPC settings** section, select **VPC and more**.



VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☐ VPC only ☒ VPC and more

5. In the **Name tag auto-generation** section, you can edit the name tag of individual resources, or auto-generate the name tags. Clear the **Auto-generate** check box to edit the name tags of your VPC and subnets.

6. In the **IPv6 CIDR block** section, select **Amazon-provided IPv6 CIDR block** for the VPC.
7. Configure the Availability Zone for each subnet. Make sure that the public subnet and private subnet are in the same zone.
8. (Optional). If you use two or more availability zones, you can customize the order of the availability zones. For more information, go to [Regions and Zones](#).
9. Configure at least one public and one private subnet for each Availability Zone the VPC is in. You can use the default public and private subnets or select other subnets. AWS requires that each subnet must include enough space for a least 16 IP addresses.
10. Configure the NAT gateways, VPC endpoints, and DNS options.
11. Click **Create VPC**.

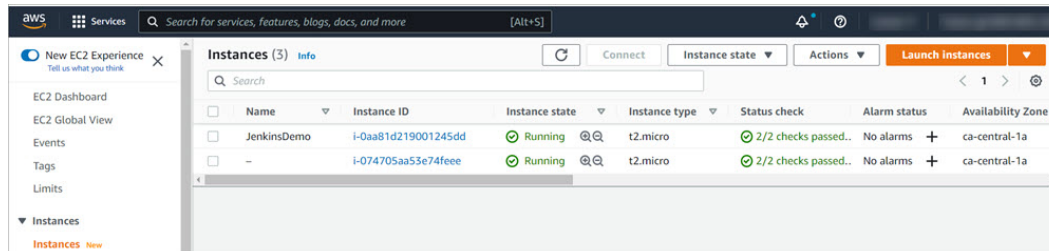
The wizard creates the VPC.

Create an Instance of Firebox Cloud

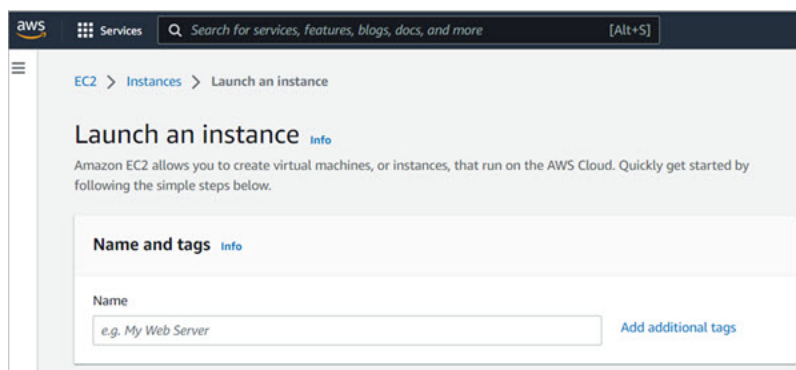
From the EC2 dashboard, you can create an EC2 instance for Firebox Cloud.

To launch an instance of Firebox Cloud:

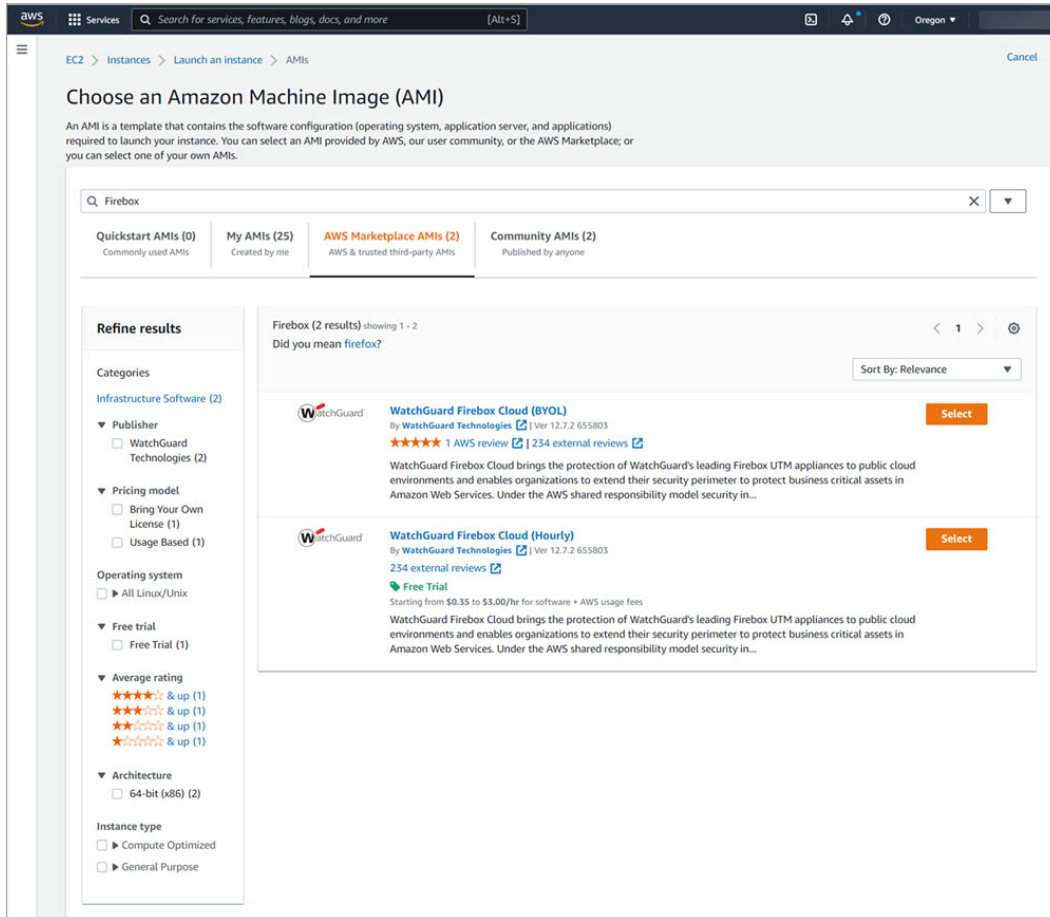
1. Log in to the AWS Management Console at aws.amazon.com.
2. From the top navigation bar, select **Services > Compute > EC2**.
The EC2 Dashboard page opens.
3. From the navigation menu, in the **Instances** section, click **Instances**.
4. Click **Launch instances**.



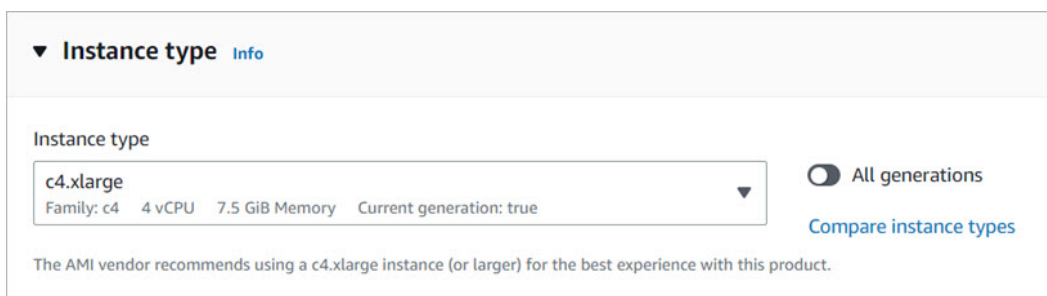
5. In the **Name** text box, enter a name for your instance.



- In the **Application and OS Images (Amazon Machine Image)** search text box, enter **Firebox** and select the **AWS Marketplace AMIs** tab.



- Select WatchGuard Firebox Cloud Hourly or BYOL.
- Click **Continue**.
- In the **Instance type** section, select the AWS instance type from the drop-down list or from the **Compare instance types** page. If you selected Firebox Cloud with a BYOL license, select an instance that has the number of vCPUs your Firebox Cloud license supports.
 - For information about the maximum number of vCPUs supported for each Firebox Cloud model, go to [Firebox Cloud License Options](#).
 - For information about supported EC2 instance types for Firebox Cloud (BYOL) and Firebox Cloud (Hourly), go to the Firebox Cloud product information in the [AWS Marketplace](#).



▼ Instance type [Info](#)

Instance type

c4.xlarge
Family: c4 4 vCPU 7.5 GiB Memory Current generation: true

☒ All generations [Compare instance types](#)

The AMI vendor recommends using a c4.xlarge instance (or larger) for the best experience with this product.

10. In the **Key pair (login)** section, select or create a key pair for SSH authentication. The key pair is needed only for ssh connections to the Fireware command line interface (CLI) for Firebox Cloud. You do not need the key pair to connect to Fireware Web UI. If you proceed without a key pair, you can log in to Fireware Web UI, but you cannot connect to the CLI from outside of the VPC.
 - a. To use an existing key pair, select a key pair from the drop-down list.
 - b. To create a new key pair, select **Create new key pair**.
The Create key pair dialog box opens.
 - c. In the **Key pair name** text box, type a name for the new key pair.
 - d. Click **Create key pair**.
The .PEM file that contains the private key is downloaded.
 - e. Save the private key to a location that is secure and accessible. You cannot download the private key file again.

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

Enter key pair name

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

⚠

When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Cancel

Create key pair

Save the private key file in a secure location. You must provide the private key to connect to the Fireware command line interface.

11. In the **Network settings** section, click **Edit**.
 - a. From the **VPC** drop-down list, select your VPC.
 - b. From the **Subnet** drop-down list, select the public subnet to use for eth0.
 - c. From the **Auto-assign public IP** drop-down list, select **Disable**.
 - d. In the **Firewall (security groups)** section, select **Create security group**. By default, the instance uses a security group that functions as a basic firewall. Because Firebox Cloud is a firewall, you must add a new security group that allows all traffic, and assign that security group to this EC2 instance.
 - e. Edit the **Security group name** and **Description**.
 - f. In the **Inbound Security Groups Rules** section, configure an existing security group rule or add a new security group rule. Make sure that the security group rule selected allows all traffic. From the **Type** drop-down list, select **All traffic**.

Firebox Cloud Deployment Guide

38

Inbound Security Group Rules

▼ Security group rule 1 (All, All, 0.0.0.0/0, Example) Remove

Type Info	Protocol Info	Port range Info
All traffic ▼	All	All
Source type Info	Source Info	Description - optional Info
Anywhere ▼	<input type="text" value="Add CIDR, prefix list or security"/> 0.0.0.0/0 ✕ :::/0 ✕	Example

12. To add a second interface, expand the **Advanced network configuration** section.
 - **Description** – Type a description for the new network interface.
 - **Subnet** – The subnet in which to create the new network interface. For the primary network interface (eth0), this is the subnet used to launch the instance. If you enter an existing network interface for eth0, the instance is launched in the subnet where the network interface is located.
 - **Security groups** – The security group in your VPC to associate with the network interface.
 - **Primary IP** – A private IPv4 address from the range of your subnet. Leave blank to allow Amazon EC2 to select a private IPv4 address.
 - **Secondary IP** – One or more additional private IPv4 addresses from the range of your subnet. Select **Manually assign** and enter an IP address or select **Automatically assign** to allow Amazon EC2 select an IP address, and enter a value to indicate the number of IP addresses to add.
 - **IPv6 IPs** – An IPv6 address from the range of the subnet. Select **Manually assign** and enter an IP address or select **Automatically assign** to allow Amazon EC2 select an IP address, and enter a value to indicate the number of IP addresses to add.
 - **IPv4 Prefixes** – The IPv4 prefixes for the network interface.
 - **IPv6 Prefixes** – The IPv6 prefixes for the network interface.
 - **Delete on termination** – Select **Yes** or **No** to delete the network interface when the instance is deleted.

▼ Advanced network configuration

Network interface 1

Device index Info 0	Network interface Info New interface ▼	Description Info My Primary ENI
Subnet Info subnet-0caef682aa645382b IP addresses available: 250	Security groups Info New security group	Primary IP Info <input type="text"/>
Secondary IP Info Select ▼	IPv6 IPs Info Select ▼	IPv4 Prefixes Info Select ▼ <small>The selected instance type does not support IPv4 prefixes.</small>
IPv6 Prefixes Info Select ▼ <small>The selected instance type does not support IPv6 prefixes.</small>	Delete on termination Info Select ▼	Elastic Fabric Adapter Info <input type="checkbox"/> Enable <small>EFA is only compatible with certain instance types.</small>

13. In the **Configure Storage** section, use the default storage size (5 GB).
14. Review the **Summary** side panel. Click **Launch instance**.

▼ Summary

Number of instances [Info](#)
1

[Software Image \(AMI\)](#)
WatchGuard Firebox Cloud (BYOL...[read more](#))
ami-00d28a301ad3d1b63

[Virtual server type \(instance type\)](#)
c4.xlarge

[Firewall \(security group\)](#)
New security group

[Storage \(volumes\)](#)
1 volume(s) - 5 GiB

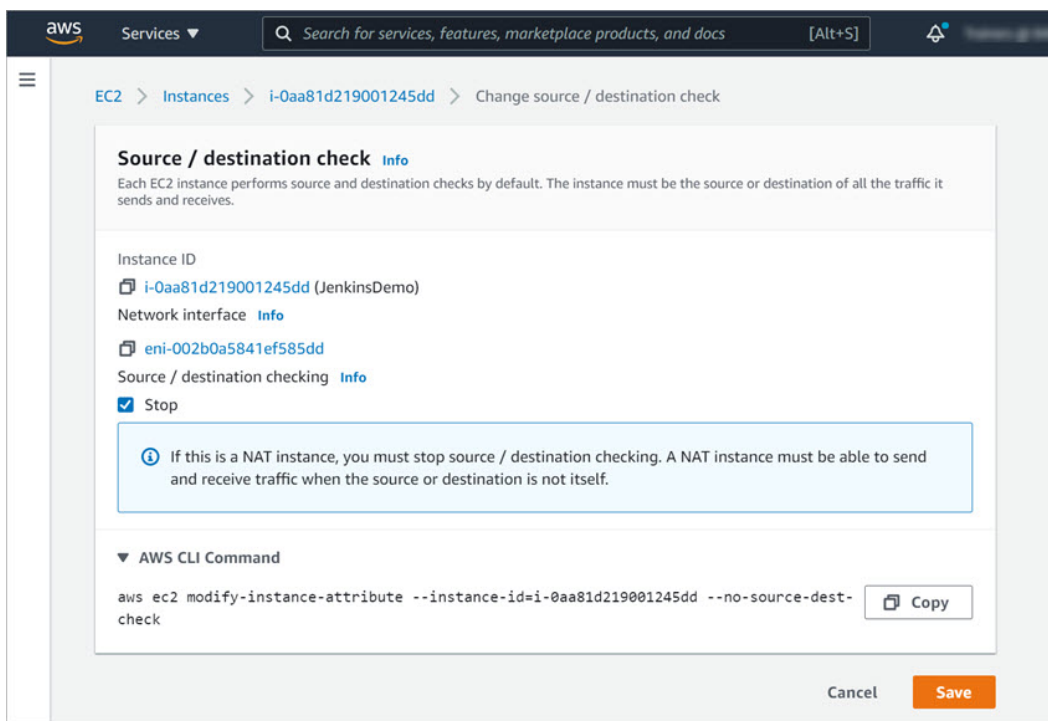
Cancel **Launch instance**

Disable Source/Destination Checks

By default, each EC2 instance completes source/destination checks. For the networks on your VPC to successfully use your instance of Firebox Cloud for NAT, you must disable the source/destination check for the network interfaces assigned to the instance of Firebox Cloud.

To disable source/destination checks for the public interface:

1. From the EC2 Management Console, select **Instances > Instances**.
2. Select the check box next to the instance of Firebox Cloud.
3. Select **Actions > Networking > Change source/destination check**.
The Source / destination check page opens.
4. Select the **Stop** check box.
5. Click **Save**.



Assign an Elastic IP Address to the External Interface

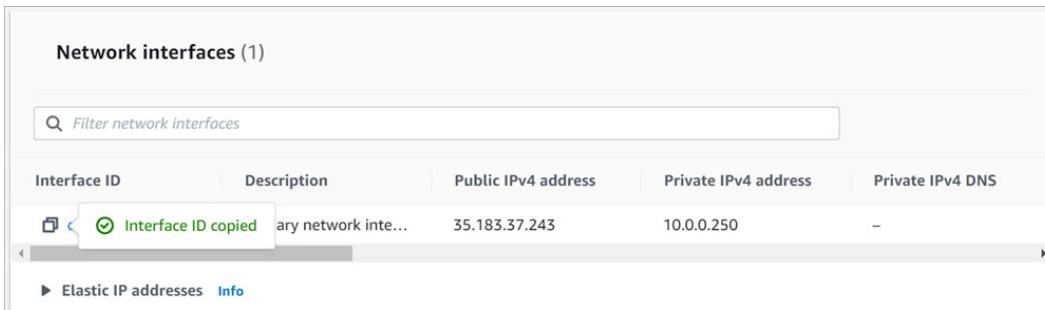
You must assign an Elastic IP (EIP) address to the eth0 interface for the instance of Firebox Cloud. To make sure you assign it to the correct interface, find and copy the eth0 interface ID for your instance of Firebox Cloud.

To find the eth0 interface ID for your instance of Firebox Cloud:

1. From the EC2 Dashboard, select **Instances**.
2. Select the instance of Firebox Cloud.

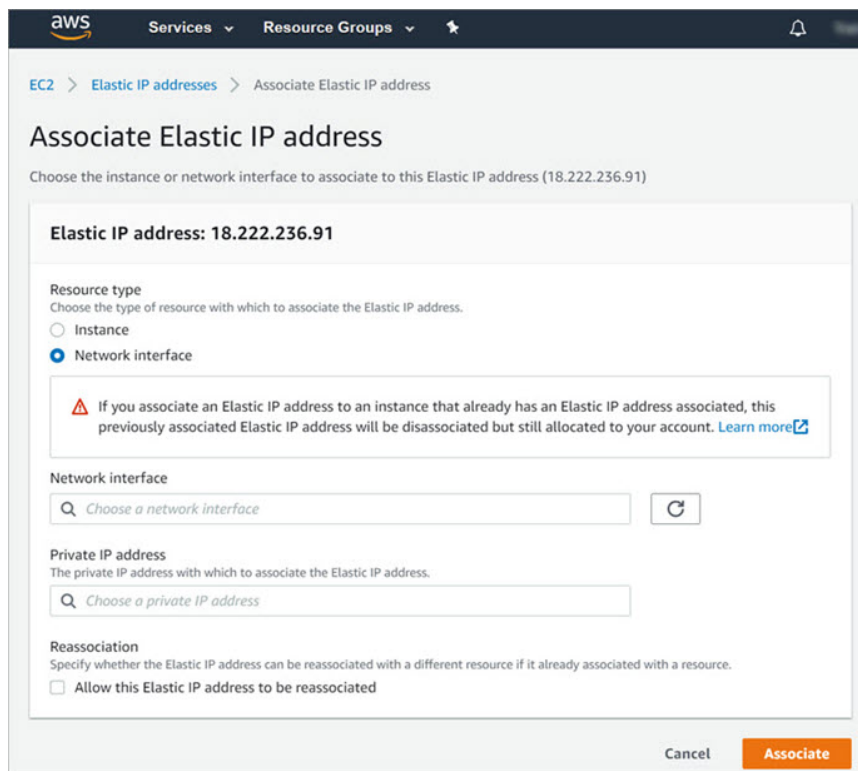
The instance details appear.

3. Select the **Networking** tab.
4. In the **Network interfaces** section, copy the **Interface ID** from the **Primary network interface**.
The Interface ID copied confirmation is displayed.



To associate the Elastic IP address with the eth0 interface:

1. From the EC2 Management Console, select **Network & Security > Elastic IPs**.
2. Select an available Elastic IP address.
3. Select **Actions > Associate Elastic IP Address**.
The Associate Elastic IP Address page opens.



4. In the **Resource type** settings, select **Network interface**.
5. In the **Network Interface** text box, paste the Interface ID for eth0.
6. Click **Associate**.

You can now use the EIP address to connect to Fireware Web UI for your instance of Firebox Cloud.

To connect to Fireware Web UI, open a web browser and go to `https://<eth0_EIP>:8080`.

Configure the Default Route

To enable Firebox Cloud to control outbound traffic from the private network connected to eth1, you must change the route table for the private subnet so that it uses Firebox Cloud as the default gateway.

To find the network interface ID of the private network:

1. On the EC2 dashboard, select **Network & Security > Network Interfaces**.
2. Find the private network interface for your instance ID. It is the interface that does not have a public IP address assigned.
3. Copy the network interface ID.

To edit the route table:

1. Select **Services > VPC**.
2. In the **Virtual Private Cloud** section, select **Route tables**.
3. To find the interface for the private network, select each route table for your VPC one at a time.
The route table details appear, with the interface information for each route table.
4. To view the routes for each network, select the **Routes** tab.
5. On the **Routes** tab for the private network, click **Edit routes**.

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	nat-xxxxxxxxxxxx	blackhole	No

6. In the **Target** text box, paste the Interface ID over the NAT Gateway ID.

The route status changes from Black Hole to Active.

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	eni-04988b4753857713c	active	No

7. Click **Save routes**.

Verify the Instance Status

After you finish all the steps to deploy your instance of Firebox Cloud, review the instance details on the EC2 **Instances** page to verify that:

- Public IP address and Public DNS server are assigned
- The security group to allow all traffic is assigned



If you delete the Firebox Cloud VM, make sure you delete the associated resources to avoid additional charges.

Find the Instance ID (VM ID)

After you deploy your Firebox Cloud instance, you must find the Instance ID, also known as the VM ID. You will need this to activate your license, and to log in to the Fireware Web UI to run the Firebox Cloud Setup Wizard.

To find the Firebox Cloud Instance ID:

1. From the EC2 Management Console, select **Instances > Instances**.
2. Open your instance.
3. Copy the Instance ID.



You must have this instance ID to activate your Firebox Cloud license and to run the Firebox Cloud Setup Wizard.

Activate your Firebox Cloud License (BYOL Only)

For Firebox Cloud with a BYOL license, you must activate the Firebox Cloud serial number in the WatchGuard portal. Before you can activate Firebox Cloud, you must have the Firebox Cloud serial number you received from WatchGuard and you must know the Firebox Cloud Instance ID.

To activate your Firebox Cloud license:

1. Go to www.watchguard.com.
2. Click **Support**.
3. Click **Activate Products**.
4. Log in to your WatchGuard Customer or Partner portal account. If you do not have an account, you can create one.
5. If necessary, navigate to the Support Center and select **My WatchGuard > Activate Products**.

6. When prompted, provide your Firebox Cloud serial number and Instance ID.
7. When activation is complete, copy the feature key and save it to a local file.

Run the Firebox Cloud Setup Wizard

After you deploy Firebox Cloud, you can connect to Fireware Web UI through the public IP address to run the Firebox Cloud Setup Wizard. You use the wizard to set the administrative passphrases for Firebox Cloud.

To run the Firebox Cloud Setup Wizard:

1. Connect to Fireware Web UI for your Firebox Cloud with the public IP address:
`https://<eth0_public_IP>:8080`
2. Log in with the default Administrator account user name and passphrase:
 - User name – **admin**
 - Passphrase – The Firebox Cloud Instance ID
The Firebox Cloud Setup Wizard welcome page opens.
3. Click **Next**.
The setup wizard starts.
4. Review and accept the End-User License Agreement. Click **Next**.

WatchGuard Fireware Web UI User: ?

Create passphrases for your Firebox Cloud

Your Firebox Cloud has two built-in user accounts:

- admin has read-write privileges.
- status has read-only privileges.

Type the passphrase to use with each account.
Each passphrase must contain between 8 and 32 characters.

User name: status (read-only)

Passphrase:

Confirm passphrase:

User name: admin (read-write)

Passphrase:

Confirm passphrase:

5. Specify new passphrases for the built-in **status** and **admin** user accounts.
6. Click **Next**.
The configuration is saved to Firebox Cloud and the wizard is complete.




WatchGuard does not store any sensitive customer information in the Firebox Cloud configuration or on the AWS cloud-based platform.

Connect to Firewall Web UI

To connect to Firewall Web UI and administer Firebox Cloud:

1. Open a web browser and go to the public IP address for your instance of Firebox Cloud at:
`https://<eth0_public_IP>:8080`
2. Log in with the *admin* user account. Make sure to specify the passphrase you set in the Firebox Cloud Setup Wizard.

By default, Firebox Cloud allows more than one user with Device Administrator credentials to log in at the same time. To prevent changes by more than one administrator at the same time, the configuration is

locked by default. To unlock the configuration so you can make changes, click .

If you prefer to allow only one Device Administrator to log in at the same time, select **System > Global Settings** and clear the **Enable more than one Device Administrator to log in at the same time** check box.

Add the Feature Key (BYOL Only)

If you activated a Firebox Cloud license in the WatchGuard portal, your feature key is available directly from WatchGuard. You must add this feature key to the Firebox Cloud configuration to enable all functionality and configuration options on Firebox Cloud.




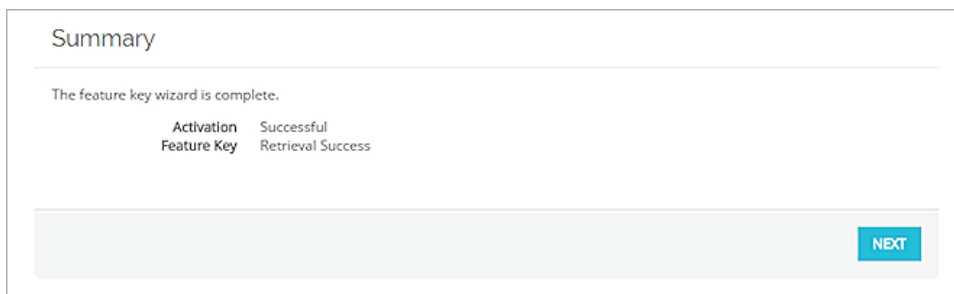
After you add the feature key, Firebox Cloud automatically reboots with a new serial number.

To add the feature key, from Fireware Web UI:

1. Select **System > Feature Key**.

The Feature Key Wizard page opens.

2. To unlock the configuration file, click .
3. To download and install the feature key, click **Next**.
4. On the **Summary** page, verify that your feature key was successfully installed.
When your feature key has been installed, Feature Key Retrieval Success appears on the Summary page.



5. Click **Next**.

The wizard completes and Firebox Cloud reboots with a new serial number.

Next Steps

After you run the setup wizard and add the feature key you can use Fireware Web UI or Policy Manager to configure the settings for Firebox Cloud.

Enable Feature Key Synchronization

Enable Firebox Cloud to automatically check for feature key updates when services are about to expire.

To enable feature key synchronization, in Fireware Web UI:

1. Select **System > Feature Key**.
2. Select the **Enable automatic feature key synchronization** check box.
3. Click **Save**.

To enable feature key synchronization, in Policy Manager:

1. Connect to Firebox Cloud in WatchGuard System Manager.
2. Open Policy Manager.
3. Select **System > Feature Keys**.
4. Select the **Enable automatic feature key synchronization** check box.
5. Click **Save**.

Configure Firebox Cloud to Send Feedback to WatchGuard

To enable Firebox Cloud to send feedback, in Fireware Web UI:

1. Select **System > Global Settings**.
2. Select the **Send device feedback to WatchGuard** check box.
3. Select the **Send Fault Reports to WatchGuard daily** check box.

To enable Firebox Cloud to send feedback, in Policy Manager:

1. Connect to Firebox Cloud in WatchGuard System Manager.
2. Open Policy Manager.
3. Select **Setup > Global Settings**.

4. Select the **Send device feedback to WatchGuard** check box.
5. Select the **Send Fault Reports to WatchGuard daily** check box.

Configure Firewall Policies and Services

The default WatchGuard and WatchGuard Web UI policies allow management connections from any computer on the trusted, optional, or external networks.



We strongly recommend that you do not allow management connections from the external network, and that you edit the WatchGuard and WatchGuard Web UI policies to remove the *Any-External* alias from the From list after you complete initial configuration.

To allow management from only a specific computer on the external network, you can add the address of that management computer to the From list in these policies.

Configure other policies and services as you would for any other Firebox.



Firebox Cloud does not support every Fireware feature. For a summary of the differences between Firebox Cloud and other Firebox models, go to [Firebox Cloud Feature Differences](#).

Troubleshooting

If you experience issues with your Firebox Cloud deployment on AWS, check to make sure that you have followed the procedures in the [Deployment Overview](#) section:

- Allocate an Elastic IP address
- Create a Virtual Private Cloud (VPC)
- Create an instance of Firebox Cloud
- Disable the Source/Destination checks for Firebox Cloud
- Configure the default route for the private network
- Check the instance status. With instance status monitoring, you can check if Amazon EC2 has detected any problems with the health of your instance and set up an Amazon CloudWatch alarm. For more information, go to [Status checks for your instances](#).

Firebox Cloud Feature Differences

Because Firebox Cloud is optimized to protect servers in a virtual private cloud, some setup requirements, configuration options, and available features are different from other Firebox models. This section summarizes the differences between Firebox Cloud and other Fireboxes.

Administration

You use Fireware Web UI, WatchGuard System Manager, or WatchGuard Cloud to manage a Firebox Cloud instance. You can use WatchGuard Cloud or WatchGuard Dimension to monitor the traffic and security status of the networks your Firebox protects. You can use Dimension Command to manage a Firebox Cloud instance that runs Fireware v11.12.4 or higher.

To add a Firebox Cloud instance to WatchGuard Cloud, the Firebox Cloud instance must have a BYOL license.

To manage Firebox Cloud from Policy Manager or a WatchGuard Management Server you must install WatchGuard System Manager v12.2 or higher.

Licensing and Services

For Firebox Cloud with a *BYOL* license, you must activate a license key for Firebox Cloud on the WatchGuard website, and add the feature key to your instance of Firebox Cloud. For more information, go to [Deploy Firebox Cloud on AWS](#) or [Deploy Firebox Cloud on Microsoft Azure](#).

Most supported features and services are included with Firebox Cloud. Some security services are supported only for Firebox Cloud with a BYOL license. For information about license options and supported services, go to [Firebox Cloud License Options](#).

Network Interfaces

Firebox Cloud supports two to eight interfaces. It supports one external interface (eth0), and up to seven private interfaces (eth1-eth7). All Firebox Cloud interfaces use DHCP to request an IP address. Because you must configure all network interface IP addresses and settings in AWS or Azure, you cannot configure the network interfaces in Fireware Web UI. The **Network > Interfaces** configuration page is not visible in Fireware Web UI for Firebox Cloud.

For Firebox Cloud on AWS, you assign an Elastic IP (EIP) address to the external interface. For Firebox Cloud on Azure, you can configure the external interface with a dynamic or static IP address. The internal IP addresses are assigned based on the private networks assigned to your Firebox Cloud instance in AWS or Azure.



Firebox Cloud supports one or more secondary IP addresses on the external interface in Fireware v12.1 and higher.

Default Firebox Configuration

When you launch an instance of Firebox Cloud, it automatically starts with a default configuration. For Firebox Cloud with a BYOL license, you must get a feature key to enable configuration of all features.

The Firebox Cloud Setup Wizard runs the first time you connect to Fireware Web UI. In the wizard you accept the End User License Agreement and choose new passphrases.

After you run the setup wizard, the default configuration for Firebox Cloud is different from other Firebox models in these ways:

- All interfaces use DHCP to obtain an IPv4 primary IP addresses
- Firebox Cloud allows more than one Device Administrator to connect at the same time
- You can connect to any interface for administration with Fireware Web UI
- The default policies allow management connections and pings to Firebox Cloud, but do not allow outbound traffic from private subnets through Firebox Cloud
- Licensed subscription services are not configured by default

The default WatchGuard and WatchGuard Web UI policies allow management connections from any computer on the trusted, optional, or external networks.



We strongly recommend that you do not allow management connections from the external network, and that you edit the WatchGuard and WatchGuard Web UI policies to remove the *Any-External* alias from the From list after you complete initial configuration.

To allow management from only a specific computer on the external network, you can add the address of that management computer to the From list in these policies.

Fireware Features

Firebox Cloud supports most policy and security features available on other Firebox models. It supports a subset of networking features appropriate for the AWS environment. For supported features, the available configuration settings are the same as for any other Firebox. Most features and options that are not supported for Firebox Cloud do not appear in Fireware Web UI.

Networking features not supported:

- Drop-in mode and Bridge mode
- DHCP server and DHCP relay (all interfaces are DHCP clients)
- PPPoE
- IPv6
- Multi-WAN (includes sticky connections and policy-based routing)
- ARP entries
- Link Aggregation
- VLANs
- FireCluster
- Bridge interfaces
- DNS forwarding and conditional DNS forwarding

Policies and Security Services not supported:

- Explicit-proxy and Proxy Auto-Configuration (PAC) files
- Quotas
- DNSWatch (supported with a BYOL license only)
- Network Discovery
- Mobile Security

Authentication features not supported:

- Hotspot



Firebox Cloud supports Single Sign-On (SSO) in Fireware v12.2 or higher.

System Administration features not supported:

- Logon disclaimer for device management connections
- USB drive for backup and restore

Other features not supported:

- Gateway Wireless Controller
- Mobile VPN with SSL **Bridge VPN Traffic** option
- SD-WAN

Features you cannot configure from Fireware Web UI:

- Change the logging settings for default packet handling options
- Edit the name of an existing policy
- Add a custom address to a policy
- Use a host name (DNS lookup) to add an IP address to a policy
- Add or edit a secondary PPPoE interface



It is possible to configure some features, such as IPv6 routes, that are not supported for Firebox Cloud. This does not enable the unsupported feature, but does no harm.

View Firebox Cloud VM Information

You can view information about the Firebox Cloud virtual machine in Fireware Web UI and Firebox System Manager.

VM Information in Fireware Web UI

For Firebox Cloud, some pages in Fireware Web UI include information about the Firebox Cloud virtual machine and virtual interfaces.

The Front Panel Dashboard

For Firebox Cloud, the **Front Panel** dashboard page includes this information about the Firebox Cloud instance:

- Instance ID – The virtual machine identifier
- Instance Type – The type of AWS or Azure virtual machine instance
- Availability Zone – The AWS Availability Zone or Azure region where the Firebox Cloud virtual machine is deployed

The VM Information System Status Page

The **System Status > VM Information** page includes more details about the Firebox Cloud virtual machine.

The VM Information for Firebox Cloud for AWS includes:

- Instance ID – The virtual machine identifier
- Instance Type – The type of AWS virtual machine instance
- Availability Zone – The AWS Availability Zone
- Public Hostname – The public host name of the Firebox Cloud virtual machine
- Public IPv4 Address – The public IPv4 address for the external interface
- Security Group – The AWS security group
- Public Key – The public key for this Firebox Cloud virtual machine

The VM Information for Firebox Cloud for Azure includes:

- VM ID – The virtual machine ID. This is the same as the Instance ID on the Front Panel.
- VM Size – The Azure VM size. This is the same as the Instance Type on the Front Panel.
- Location – The Azure region. This is the same as the Availability Zone on the Front Panel.
- Public Hostname – The host name for the Firebox Cloud instance external interface
- Public IPv4 Address – The public IPv4 address for the external interface

The Interfaces Dashboard

The **Interfaces** Dashboard page includes information about the status of virtual network interfaces associated with each Firebox Cloud interface. The content shown in the **Detail** tab varies slightly for Firebox Cloud on AWS or Azure.

For Firebox Cloud on AWS, the **Interfaces** Dashboard page includes this information:

- Interface ID – The elastic network interface (eni) ID
- Public Hostname – The public DNS host name for the external interface
- Public IPv4 address – The public IPv4 address for the external interface
- Local Hostname – The private DNS host name for the network interface
- Device Number – The interface number
- VPC ID – The ID of the VPC where the instance of Firebox Cloud is deployed
- Link Status – The link status of each interface (Up or Down)
- DNS Servers – The list of DNS servers that generate the public IPv4 address

Bandwidth

Detail

Interfaces

External (eth0)

Enabled

Yes

Link Status

Up

Zone

External

IPv4 Address

10.0.0.211/24

Gateway

10.0.0.1

MAC Address

0A:64:65:EC:24:55

Interface ID

eni-ca27849a

Public Hostname

ec2-52-38-221-202.us-west-2.compute.amazonaws.com

Public IPv4

52.38.221.202

Local Hostname

ip-10-0-0-211.us-west-2.compute.internal

Device Number

0

VPC ID

vpc-40508c27

Enabled

Yes

Link Status

Up

Trusted (eth1)

Enabled

Yes

Link Status

Up

Zone

Trusted

IPv4 Address

10.0.1.253/24

Gateway

10.0.1.1

MAC Address

0A:B3:D5:CD:05:37

Interface ID

eni-58278408

Local Hostname

ip-10-0-1-253.us-west-2.compute.internal

Device Number

1

VPC ID

vpc-40508c27

Enabled

Yes

Link Status

Up

DNS Servers

- 10.0.0.2

The Interfaces Dashboard for a Firebox Cloud instance on AWS

For Firebox Cloud on Azure, the **Interfaces** Dashboard page includes this information:

- Public IPv4 address – The public IPv4 address for the external interface
- Local IPv4 address – The private IPv4 address for the external interface
- Device Number – The interface number
- Link Status – The link status of each interface (Up or Down)
- DNS Servers – The list of DNS servers that generate the public IPv4 address

The screenshot shows the 'Interfaces' dashboard with tabs for 'Bandwidth' and 'Detail'. The 'Detail' tab is active. It lists two interfaces: 'External (eth0)' and 'Trusted (eth1)'. Each interface has a table of configuration details. The 'External (eth0)' interface is enabled, has a link status of 'Up', and is in the 'External' zone. It has a public IPv4 address of 40.80.153.5 and a local IPv4 address of 10.0.0.5. The 'Trusted (eth1)' interface is also enabled, has a link status of 'Up', and is in the 'Trusted' zone. It has a local IPv4 address of 10.0.1.5. Below the interfaces, there is a section for 'DNS Servers' with a single entry: 168.63.129.16.

External (eth0)		Enabled	Yes
Link Status	Up	Link Status	Up
Zone	External	Public IPv4	40.80.153.5
IPv4 Address	10.0.0.5/24	Local IPv4	10.0.0.5
Gateway	10.0.0.1	Device Number	0
MAC Address	00:0D:3A:31:65:6A		

Trusted (eth1)		Enabled	Yes
Link Status	Up	Link Status	Up
Zone	Trusted	Local IPv4	10.0.1.5
IPv4 Address	10.0.1.5/24	Device Number	1
Gateway	0.0.0.0		
MAC Address	00:0D:3A:33:18:CD		

DNS Servers

- 168.63.129.16

The Interfaces Dashboard for a Firebox Cloud instance on Azure

You can also view some information about the virtual machine in Firebox System Manager, as described in the next section.

VM Information in Firebox System Manager

To use Firebox System Manager to monitor Firebox Cloud, you must install WatchGuard System Manager v12.2 or higher. When you use Firebox System Manager to manage Firebox Cloud, the **VM Information** tab shows information about the Firebox Cloud virtual machine.

The VM Information for Firebox Cloud for AWS includes:

- Instance ID – The virtual machine identifier
- Instance Type – The type of AWS virtual machine instance
- Availability Zone – The AWS Availability Zone

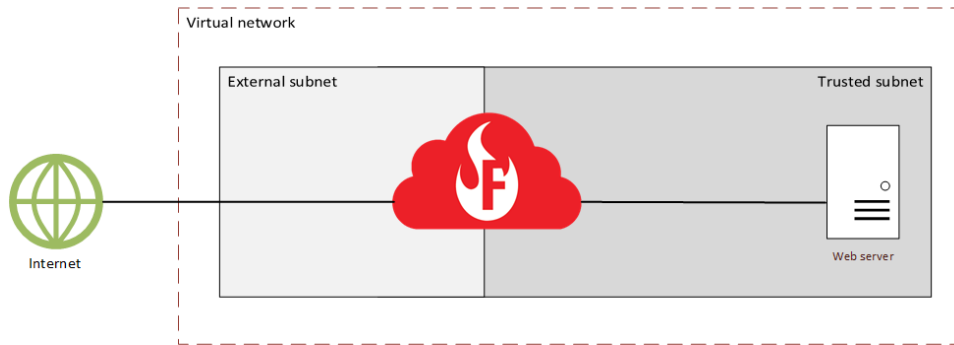
- Public Hostname – The public host name of the Firebox Cloud virtual machine
- Public IPv4 Address – The public IPv4 address for the external interface
- Security Group – The AWS security group
- Public Key – The public key for this Firebox Cloud virtual machine

The VM Information for Firebox Cloud for Azure includes:

- VM ID – The virtual machine ID. This is the same as the Instance ID on the Front Panel.
- VM Size – The Azure VM size. This is the same as the Instance Type on the Front Panel.
- Location – The Azure region. This is the same as the Availability Zone on the Front Panel.
- Public Hostname – The host name for the Firebox Cloud instance external interface
- Public IPv4 Address – The public IPv4 address for the external interface

Use Firebox Cloud to Protect a Web Server

You can configure the proxy policies and subscription services in your Firebox Cloud configuration file to protect a web server on the virtual network connected to your Firebox Cloud instance.



For more information about Firebox Cloud features, go to:

- [Introduction to Firebox Cloud](#)
- [Firebox Cloud Feature Differences](#)

Step 1 – Launch an Instance of Firebox Cloud

To protect a web server with Firebox Cloud, you must launch an instance of Firebox Cloud in the same virtual network as the web server you want to protect. You must assign a public IP address to eth0 of the Firebox Cloud instance. This is the public IP address of Firebox Cloud. The web server to protect must be on the private subnet of the virtual network where you deploy the instance of Firebox Cloud.

For detailed steps to launch and configure a Firebox Cloud instance on AWS or Azure, go to:

- [Deploy Firebox Cloud on AWS](#)
- [Deploy Firebox Cloud on Microsoft Azure](#)

After you deploy the instance of Firebox Cloud, connect to it with Fireware Web UI at the public IP address of the Firebox external interface:

```
https://<eth0_public_IP>:8080
```

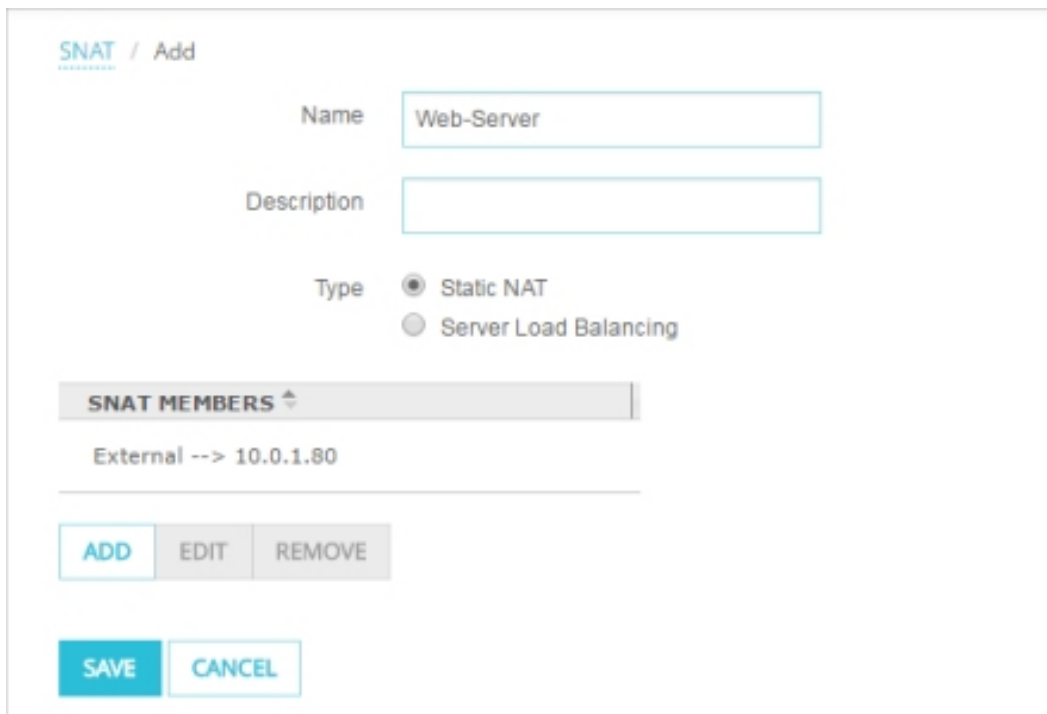
After you have connected to Fireware Web UI for your instance of Firebox Cloud, you can configure your Firebox Cloud.

Step 2 – Add A Static NAT Action

Add a static NAT action for traffic from the external interface to the internal IP address of the web server. You can then use the static NAT action in policies that allow traffic to your web server.

To add a static NAT action, from Fireware Web UI:

1. Select **Firewall > SNAT**.
2. Add a static NAT action that allows traffic from the external interface to the private IP address of the web server. In Fireware v12.2 or higher, you can also specify an FQDN in the static NAT action.



The screenshot shows the 'SNAT / Add' configuration page in the Fireware Web UI. The page has a light blue header with the text 'SNAT / Add'. Below the header, there are two text input fields: 'Name' with the value 'Web-Server' and 'Description' which is empty. Below these fields is a 'Type' section with two radio buttons: 'Static NAT' (which is selected) and 'Server Load Balancing'. Below the radio buttons is a section titled 'SNAT MEMBERS' with a small upward arrow icon. Under this section, the text 'External --> 10.0.1.80' is displayed. Below the 'SNAT MEMBERS' section are three buttons: 'ADD' (highlighted in blue), 'EDIT', and 'REMOVE'. At the bottom of the form are two buttons: 'SAVE' (highlighted in blue) and 'CANCEL'.

3. Click **Save**.

Step 3 – Add HTTP and HTTPS Proxy Policies

After you add the static NAT action, to allow HTTP and HTTPS traffic to the web server, you can add proxy policies that use the new static NAT action. You also clone the predefined proxy actions for each policy and create user-defined proxy actions that you can edit.

Add an HTTP-Proxy Policy

To allow HTTP traffic through Firebox Cloud to the web server over port 80, you must add an HTTP-proxy policy to the Firebox Cloud configuration.

To add the HTTP-Proxy policy, from Fireware Web UI:

1. Select **Firewall > Firewall Policies**.
2. Click **Add Policy**.
3. Select **Proxies**.
4. Select the **HTTP-proxy** and the **HTTP-Server.Standard** proxy action.
5. Click **Add Policy**.
By default, the policy allows traffic from Any-External to Any-Trusted.
6. From the policy **To** list, remove **Any-Trusted**, then click **Add**.
7. From the **Member type** drop-down list, select **Static NAT** and select the static NAT action you added. Click **OK**.

The static NAT action is added to the policy.

The screenshot shows the 'Firewall Policies / Add' configuration page. The 'Name' field is set to 'HTTP-proxy' and the 'Enable' checkbox is checked. The 'Connections are' dropdown is set to 'Allowed'. The 'Policy Type' is 'HTTP-proxy'. Below this, there is a table with two columns: 'PORT' and 'PROTOCOL'. The 'PORT' row is set to '80' and the 'PROTOCOL' row is set to 'TCP'. The 'FROM' section shows 'Any-External' as the source. The 'TO' section shows 'Web-Server (SNAT)' with the action 'External --> 10.0.1.80'. At the bottom of each section, there are 'ADD' and 'REMOVE' buttons.

To select a user-defined proxy action for HTTP traffic:

1. Select the **Proxy Action** tab.
2. From the **Proxy Action** drop-down list, select **Clone the current proxy action**.
A user-defined proxy action based on the predefined proxy action is created and assigned to the policy. The cloned proxy action has a number appended to the name. For example, HTTP-Server.Standard.1.
3. Click **Save**.

Add an HTTPS-Proxy Policy

To allow secure web traffic (HTTPS) to your web server, you must also add an HTTPS-proxy policy that allows HTTPS connections to the server over port 443. In the proxy configuration, you clone the predefined HTTPS proxy action and enable inspection of HTTPS content.

To add the HTTPS-proxy policy, from Fireware Web UI:

1. Select **Firewall > Firewall Policies**.
2. Click **Add Policy**.
3. Select **Proxies**.
4. Select the **HTTPS-proxy** and the **HTTPS-Server.Standard** proxy action.
5. Click **Add Policy**.
By default, the policy allows traffic from Any-External to Any-Trusted.
6. From the **To** list, remove **Any-Trusted**, then click **Add**.
7. From the **Member type** drop-down list, select **Static NAT** and select the static NAT action you added. Click **OK**.
The static NAT action is added to the policy.

To select a user-defined proxy action and enable inspection of HTTPS content:

1. Select the **Proxy Action** tab.
2. From the **Proxy Action** drop-down list, select **Clone the current proxy action**.

A user-defined proxy action based on the predefined proxy action is created and assigned to the policy. The cloned proxy action has a number appended to the name. For example, HTTPS-Server.Standard.1.

Firewall Policies / Add

Name: ☒ Enable

Settings | Application Control | Traffic Management | **Proxy Action** | Scheduling | Advanced

Proxy Action

HTTPS Proxy Action Settings

Name:

Description:

General | **Content Inspection** | Domain Names | WebBlocker | Proxy and AV Alarms

Content Inspection

☒ Enable Content Inspection

Content Inspection applies only to Domain Name rules with the Inspect action and to WebBlocker categories you select to inspect.

When Content Inspection is enabled you can download the Proxy Authority certificate from the Certificate Portal at <http://<Firebox IP address>:4126/certportal>

☐ Allow SSLv3

Proxy Action:

3. In the **HTTPS Proxy Action Settings** section, select the **Content Inspection** tab.
4. Select the **Enable Content Inspection** check box.
5. From the **Proxy Action** drop-down list, select the user-defined HTTP proxy action you created when you cloned the HTTP proxy action in the HTTP-Proxy policy. For example, select **HTTP-Server.Standard.1**.
6. Click **Save**.

Import a Proxy Server Certificate

If you enable inspection of HTTPS content, the HTTPS proxy intercepts the HTTPS request and starts a new connection to the destination HTTPS server on behalf of the client. The HTTPS proxy in your Firebox Cloud configuration sends a self-signed certificate to the client that originated the connection. To avoid certificate errors in the web browser for users that connect to the server with HTTPS, you must get the proxy server certificate and key pair from the web server and import it to Firebox Cloud as a proxy server certificate.

To import the certificate, from Fireware Web UI:

1. Select **System > Certificates**.
2. Select **Import Certificate**.
3. For the **Certificate Function**, select **Proxy Server**.
4. Import the certificate file from your web server.
5. Save the configuration.

For more information, go to [Manage Device Certificates \(Web UI\)](#) in *Fireware Help*.

Step 4 – Enable Subscription Services

Firebox Cloud includes activated subscription services you can use to control network traffic. Follow the instructions in these procedures to enable subscription services for the HTTP and HTTPS proxy policies.

Enable Gateway AntiVirus

Gateway AntiVirus works with the SMTP, POP3, HTTP, FTP, and TCP-UDP proxies. When a new virus is identified, the features that make the virus unique are recorded. These recorded features are known as the signature. Gateway AntiVirus uses these signatures to find viruses when content is scanned by the proxy.

To enable Gateway AntiVirus in the user-defined HTTP-proxy action assigned to your HTTP-proxy policy, from Fireware Web UI:

1. Select **Subscription Services > Gateway AV**.
The Gateway AntiVirus Activation Wizard starts automatically if Gateway AntiVirus is not already enabled.
2. Complete the wizard.

Enable Intrusion Prevention Service (IPS)

Intrusion Prevention Service (IPS) provides real-time protection from threats, such as spyware, SQL injections, cross-site scripting, and buffer overflows.

To enable IPS, from Fireware Web UI:

1. Select **Subscription Services > IPS**.
2. Select the **Enable Intrusion Prevention** check box.
3. Make sure that IPS is enabled in the HTTP-proxy and HTTPS-proxy policies you added.

Enable Botnet Detection

The Botnet Detection subscription service uses a feed of known botnet site IP addresses gathered by Reputation Enabled Defense (RED). These known botnet sites are added to the Blocked Sites List that enables Firebox Cloud to block these sites at the packet level.

To enable Botnet Detection, from Fireware Web UI:

1. Select **Subscription Services > Botnet Detection**.
2. Select the **Block traffic from suspected botnet sites** check box.
3. Click **Save**.

Enable Data Loss Prevention

The Data Loss Prevention (DLP) service enables you to detect, monitor, and prevent accidental unauthorized transmission of confidential information outside your network or across network boundaries. You can use the built-in PCI Audit or HIPAA Audit sensors, or create your own sensor.

For example, to enable Data Loss Prevention for PCI compliance, from Fireware Web UI:

1. Select **Subscription Services > Data Loss Prevention**.
2. Select the **Enable Data Loss Prevention** check box.
3. Select the **Policies** tab.
4. Configure the **HTTP-proxy** and **HTTPS-proxy** to use the **PCI Audit Sensor**.
5. Click **Save**.

The default Data Loss Prevention sensors monitor and send log messages when they detect data that matches the rules enabled in the sensor. To change the action for the sensor, you can clone the sensor and then edit the settings in the new sensor.

Configure Geolocation

The Geolocation subscription service uses a database of IP addresses and countries to identify the geographic location of connections through the Firebox. Geolocation is enabled by default. You can configure Geolocation to block connections to or from specific regions.



If your internal network configuration includes IP addresses outside the reserved private IP address ranges defined in RFC 1918, RFC 5737, or RFC 3330, make sure to look up the geolocation of the IP addresses in your network before you block a country.

To look up the geolocation of an IP address, from Fireware Web UI:

1. Select **Dashboard > Geolocation > Lookup**.
2. Specify the IP address to look up.

To select the countries to block, from Fireware Web UI:

1. Select **Subscription Services > Geolocation**.
2. Select the **Enable Geolocation** check box.
3. Select countries to block on a map or from a list.
4. If there are sites you want to allow in the blocked countries, configure exceptions.
5. Save the configuration.

For more information about how to select countries and configure exceptions, go to [Configure Geolocation](#) in *Fireware Help*.

Enable Logging for Firebox Cloud

You can enable Firebox Cloud to send log messages to WatchGuard Cloud or WatchGuard Dimension™. Both WatchGuard Cloud and Dimension are virtual visibility and management solutions you can use to view Firebox log data in real-time, track it across your network, view the source and destination of the traffic, view log message details of the traffic, monitor threats to your network, and view reports of the traffic.

Configure Logging to WatchGuard Cloud

To enable Firebox Cloud to send log messages to WatchGuard Cloud, you can add your Firebox Cloud to WatchGuard Cloud. When you enable WatchGuard Cloud, the Firebox sends log messages to WatchGuard Cloud in addition to any other log servers you configure. After you activate a Firebox Cloud license on the WatchGuard portal, you can add the Firebox Cloud instance to your WatchGuard Cloud account.

For more information, go to [Add a Firebox to WatchGuard Cloud](#).

For information about how you can manage your Firebox Cloud instance as a cloud-managed device in WatchGuard Cloud, go to [Add Firebox Cloud to WatchGuard Cloud \(Cloud-Managed\)](#).



Firebox Cloud is not supported for WatchGuard Cloud with a PAYG license.

Configure Logging to Dimension

If you have an instance of Dimension, you can configure Firebox Cloud to send log messages to Dimension.

To configure Firebox Cloud to send log messages to your instance of Dimension:

1. Select **System > Logging**.
2. Select the **Send log messages to these WatchGuard Log Servers** check box.
3. In the **Log Servers** list, add the IP address of your instance of Dimension.
If your instance of Dimension is behind another Firebox, specify the external IP address of the Firebox that protects your instance of Dimension.
4. Type and confirm the **Authentication Key** for your instance of Dimension.
5. Click **Save**.

If your instance of Dimension is behind another Firebox, make sure that the configuration file of the Firebox that protects Dimension includes a **WG-Logging** policy to allow traffic from the external interface to a static NAT action that translates the public IP address of the Firebox to the private IP address of Dimension.

For more information about Dimension, go to these Video Tutorials:

- [Dimension Kernel Upgrade in Hyper-V](#) (11 minutes)
- [Dimension Kernel Upgrade in VMware ESXi](#) (11 minutes)

For more information about how to configure the logging settings, go to [Fireware Help](#).

Open the Configuration File for a Firebox Cloud Instance

From Fireware Web UI, you can download your Firebox Cloud configuration to a compressed file. This can be useful if you want to open the configuration file in Policy Manager but cannot connect to the Firebox from Policy Manager.

Before you can open a configuration file in offline mode, you must download the configuration file from your Firebox.

From Fireware Web UI, there are two methods to download the configuration file for your Firebox Cloud instance:

- Download the configuration file, `config.xml`
- Download the diagnostic log message file, `support.tgz`

Download and Open the Configuration File

You download the configuration file, `config.xml`, in a compressed (.GZ) file format. Before you can open the configuration file with Policy Manager, you must use a utility such as Winzip or 7-Zip to extract the contents of the .GZ file to a location on your computer.

After you extract the files, you can open the configuration file from Policy Manager for this Firebox Cloud instance.

To download and open the configuration file, from Fireware Web UI:

1. Select **System > Configuration File**.
The Configuration File page opens.
2. Click **Download the Configuration File**.
The browser downloads the .GZ file.
3. Open the compressed file and extract the contents.



To open a Firebox Cloud configuration file with Policy Manager, you must extract the `vmhost.json` file and the `config.xml` file into the same folder. Both files are necessary to open the configuration file in Policy Manager.

4. In Policy Manager, with an existing configuration file open, select **File > Open > Configuration File**.

Download and Open the Diagnostic Log Message File

The diagnostic log message file, `support.tgz`, includes the configuration file for your Firebox Cloud instance. Before you download the diagnostic log message file, make sure that diagnostic logging is enabled on your device. For more information about how to enable diagnostic logging, go to [Set the Diagnostic Log Level](#).

To download the diagnostic log message file `support.tgz`, from Fireware Web UI:

1. Select **System Status > Diagnostics**.
2. Click **Download a Support Log File**.

The browser downloads the file.



The configuration file, `config.xml`, is located inside the compressed diagnostic log file, `support.tgz`. The default location is `\support\config\config.xml.gz`.

To open the configuration file:

1. Extract the `config.xml` file from `config.xml.gz`.
2. Copy `vmhost.json` from `\support\networking\vmhost.json` to the `\support\config` folder.
3. Rename `vmhost.json` to `config_vmhost.json`.
4. In Policy Manager, with an existing configuration file open, select **File > Open > Configuration File**.

Changes that Require a Firebox Cloud Reboot

If you change the configuration of the network interfaces assigned to your Firebox Cloud instance in AWS or Azure, a reboot might be required for the Firebox to recognize the change. You can restart Firebox Cloud from the AWS console, or from Fireware Web UI.



If you add interfaces to a Firebox Cloud instance, you must reboot Firebox Cloud twice for new interfaces to receive IP addresses.

The types of changes that require a reboot depend on the version of Fireware.

Fireware v12.4 and Higher

In Fireware v12.4 and higher, you must reboot the Firebox after you add or remove a network interface.

If you make changes to an interface that Firebox Cloud already uses, a reboot is not required. Firebox Cloud detects the change within five minutes after you save the change in AWS or Azure.

Fireware v12.3.x and Lower

In Fireware v12.3.x and lower, you must reboot the Firebox after you:

- Add or remove a network interface
- Change interface configuration
- Manually assign an elastic IP address to an interface

To restart Firebox Cloud from Fireware Web UI:

1. Connect to Fireware Web UI.
2. On the **Front Panel** page, click **Reboot**.

If you added an interface, repeat these steps to restart Firebox Cloud a second time.

Administer Firebox Cloud with the CLI

For most Firebox Cloud administration tasks, we recommend that you use Fireware Web UI. You can also use the Fireware command line interface (CLI) to administer your instance of Firebox Cloud. To connect to the Fireware CLI you must have a terminal client that supports SSH2 and public key authentication.



If you did not specify a key pair when you launched your instance of Firebox Cloud, you cannot connect to Firebox Cloud with the Fireware CLI.

To connect to your Firebox Cloud with the Fireware CLI, use an SSH terminal client and specify these settings:

- User name – The Device Administrator user name that you use to log in to Fireware Web UI
- Private key – The private key file for your instance of Firebox Cloud
- Address – The public IP address of Eth0 for your instance of Firebox Cloud
- Port – 4118

For information about how to use the CLI to manage Fireware, go to the [Fireware Command Line Interface Reference](#).

Reset the Firebox to Factory-Default Settings

If you want to run the Web Setup Wizard again for a Firebox Cloud instance, you can use the CLI to reset the virtual machine to factory default settings.

To reset the Firebox to factory-default settings:

1. Log in to the CLI with the admin account.
2. Run the command `restore factory-default`.



When you reset a Firebox Cloud instance with a BYOL license to factory-default settings, this also resets the Firebox serial number. To restore the serial number, you must add the device feature key to the Firebox configuration.

Add Firebox Cloud to WatchGuard Cloud (Cloud-Managed)

Applies To: Cloud-managed Fireboxes¹

The Firebox Cloud Bring Your Own License (BYOL) also includes a license for WatchGuard Cloud. After you activate a Firebox Cloud BYOL license, you can add the Firebox Cloud instance to your WatchGuard Cloud account.

Firebox Cloud is available for Amazon Web Services (AWS) and Microsoft Azure cloud computing platforms.

To manage Firebox Cloud from WatchGuard Cloud, you must add Firebox Cloud as a cloud-managed device and then upload a payload to your Firebox Cloud instance.



Because Firebox Cloud is optimized to protect servers in a virtual private cloud, some setup requirements, configuration options, and available features are different from other Firebox models. For more information, go to [Firebox Cloud Feature Differences](#).

Before You Begin

Before you add a Firebox Cloud instance to WatchGuard Cloud, make sure that:

- You have purchased a Firebox Cloud BYOL license.
- You have deployed the AWS or Azure instance.
- You have your Instance ID, also known as the VM ID. You need this to activate your license, and to log in to Fireware Web UI to run the Firebox Cloud Setup Wizard.
- You have activated the Firebox Cloud instance in your WatchGuard Portal account.
- The Firebox Cloud instance is allocated to a Subscriber account (Service Providers only). For more information, go to [Firebox Allocation](#).

To add a Firebox Cloud instance as cloud-managed, it must meet these requirements:

Runs Fireware v12.7.1 or higher

For a Firebox Cloud instance to successfully connect to WatchGuard Cloud as cloud-managed, it must run Fireware v12.7.1 or higher.

The version of Fireware originally manufactured on the device appears in the **Device Information** section of the **Product Details** page in the WatchGuard Portal.

¹This topic applies to Fireboxes you configure in WatchGuard Cloud.

If your Firebox uses a lower version of Fireware, you must first set up the Firebox as a locally-managed device and upgrade it to Fireware to v12.7.1 or higher before you can add it as a cloud-managed device. For information about Fireware upgrade methods, go to [Firebox Upgrade, Downgrade, and Migration](#).


Uses factory-default settings

If you previously configured the Firebox Cloud instance as locally-managed, you must reset it to factory-default settings before it can connect to WatchGuard Cloud as a cloud-managed device. For the steps to reset your Firebox Cloud instance, go to [Changes that Require a Firebox Cloud Reboot](#).

Add a Firebox Cloud Device to WatchGuard Cloud


When you add a Firebox Cloud instance to WatchGuard Cloud as a cloud-managed device, you configure the device name, time zone, and device passwords. Network settings are configured by Microsoft AWS or Microsoft Azure.


To add Firebox Cloud to WatchGuard Cloud as a cloud-managed device:

1. Log in to your WatchGuard Cloud account.
2. For Service Provider accounts, from Account Manager, select **My Account**.
3. Select **Manage > Devices** or **Configure > Devices**.
4. Click **Add Device**.
A list of activated Fireboxes opens.
5. Click the **Name** of the Firebox you want to add or click .
A confirmation dialog box opens.
6. Click **Add Device**.
The Add Device to WatchGuard Cloud page opens.

Add Device to WatchGuard Cloud

Your Firebox was added to WatchGuard Cloud.
Select how you want to manage your Firebox configuration.

Device Management 


Cloud Management 

What is cloud management?
When a Firebox is cloud-managed, you manage the device configuration in WatchGuard Cloud. You can also monitor live status, and see log messages and reports for the devices. **If you currently manage the device configuration in WSM, Fireware Web UI, or the Command Line Interface, your configuration will be replaced with the cloud-managed configuration.**
For more information, see [Firebox Monitoring and Configuration Features](#).

NEXT Cancel

DEVICE DETAILS

Name: Milton2
Model: FireboxV Sm...
Serial Number: FVE...



7. Select **Cloud Management**.
8. Click **Next**.
9. Configure Firebox system settings:
 - **Name** – The name to identify the Firebox in WatchGuard Cloud.
 - **Time Zone** – The time zone of the location where the Firebox is installed.
 - **Device Folder** – Select the folder that you want to add your device to. [Device Folders](#) help you to view status and summarized data for groups of devices.

If you only have one root folder, the folder list does not appear.

The screenshot shows the WatchGuard web interface for adding a device to the cloud. The top navigation bar includes 'Dashboard', 'Monitor', 'Configure' (active), and 'Administration'. The main heading is 'Add Device to WatchGuard Cloud'. Below this, the section 'Begin Setting Up Your Firebox' prompts the user to 'Specify the Firebox name and select the time zone.' The 'Name' field contains 'Corporate Firebox Boston'. The 'Time Zone' dropdown is set to '(GMT-08:00) Pacific Time (US & Canada)'. A message states: 'Select the time zone where your Firebox is located. The time zone setting controls the date and time that appear in the log messages and reports for your Firebox.' Below this, another instruction says: 'Select the folder you would like to add your Firebox to.' A folder selection menu is open, showing a tree structure: 'Corporate' (selected), 'Baltimore', 'Boston', 'San Francisco', 'Seattle', and another 'Boston' entry. At the bottom, there are three buttons: 'BACK', 'NEXT' (highlighted), and 'Cancel'.

10. Click **Next**.
11. Set Firebox device passwords for connections to Fireware Web UI on the Firebox. Device passwords must be 8-32 characters long, and must contain uppercase and lowercase letters, at least one number, and at least one symbol.



The admin password you specify here is used to encrypt the payload. You must use the same admin password when you upload the payload in the Firebox Cloud Web Setup Wizard.


Add Device to WatchGuard Cloud

Set the Status and Admin Passwords

Set passwords for the built-in status and admin user accounts. These users can log in to Fireware Web UI on this device.


Status Password

Password for status account (8-32 characters) *



Admin Password

Password for admin account (8-32 characters) *





To keep your device secure, make sure you do not use the default passphrases for the admin account (readwrite) and status account (readonly). We recommend you specify unique passphrases for each Firebox you manage and change them frequently.



For a cloud-managed Firebox, you can use Fireware Web UI to recover the Firebox connection to WatchGuard Cloud. You cannot use Fireware Web UI to modify the Firebox configuration.

12. Click **Next**.

13. Click **Download Payload**.

A dialog box opens for you to save the payload file to your default download folder in your browser. The package has a TGZ extension. For example, `package_FVE1028C0754`.



Record the location where you saved the payload file. In the next section, you will upload the payload in the Fireware Web UI to connect your Firebox Cloud instance to WatchGuard Cloud.

Add Device to WatchGuard Cloud

Download Payload to Virtual Firebox

To enable a virtual Firebox, you must download the encrypted payload. The payload includes:

- Verification code
- Admin and status passwords
- Initial configuration
- Feature key

DOWNLOAD PAYLOAD

✓ Payload download complete

The payload is now encrypted with your admin password and your virtual Firebox was added to WatchGuard Cloud.

The next step is to upload the payload to your virtual Firebox.

DONE

Your device is now added to WatchGuard Cloud, but not yet connected. You must now upload the payload to your Firebox Cloud instance in the Fireware Web UI.

Upload the Payload and Connect the Firebox

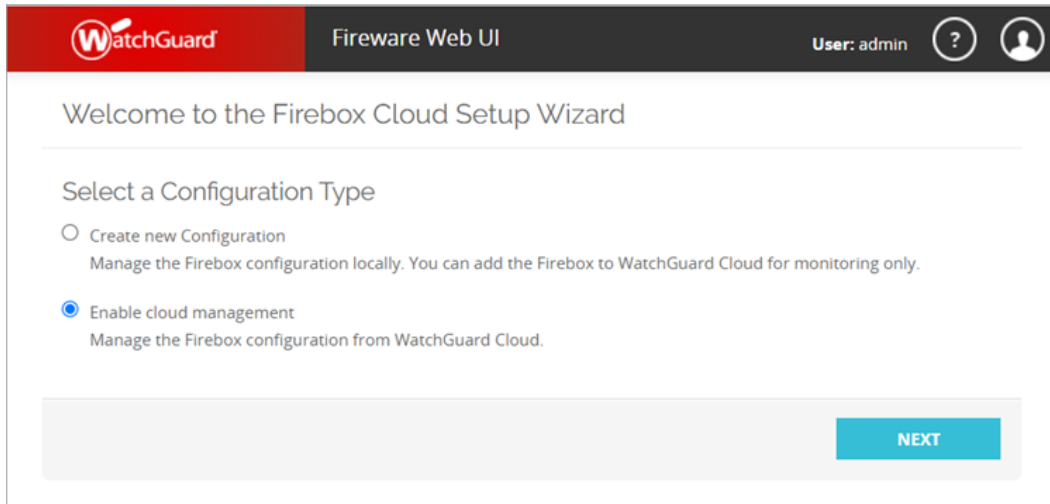
Before you can manage Firebox Cloud in WatchGuard Cloud, you must upload the payload you downloaded from WatchGuard Cloud.

The payload includes:

- Verification code
- Admin and status passwords
- Initial configuration
- Feature key

To upload the payload and connect your Firebox Cloud instance to WatchGuard Cloud:

1. Open a web browser and go to `https://<eth0_public_IP>:8080`.
2. Log in with the default administrator account user name and password:
 - Username – admin
 - Password – the Firebox Cloud Instance ID
3. Select **Enable cloud management**.



WatchGuard Fireware Web UI User: admin

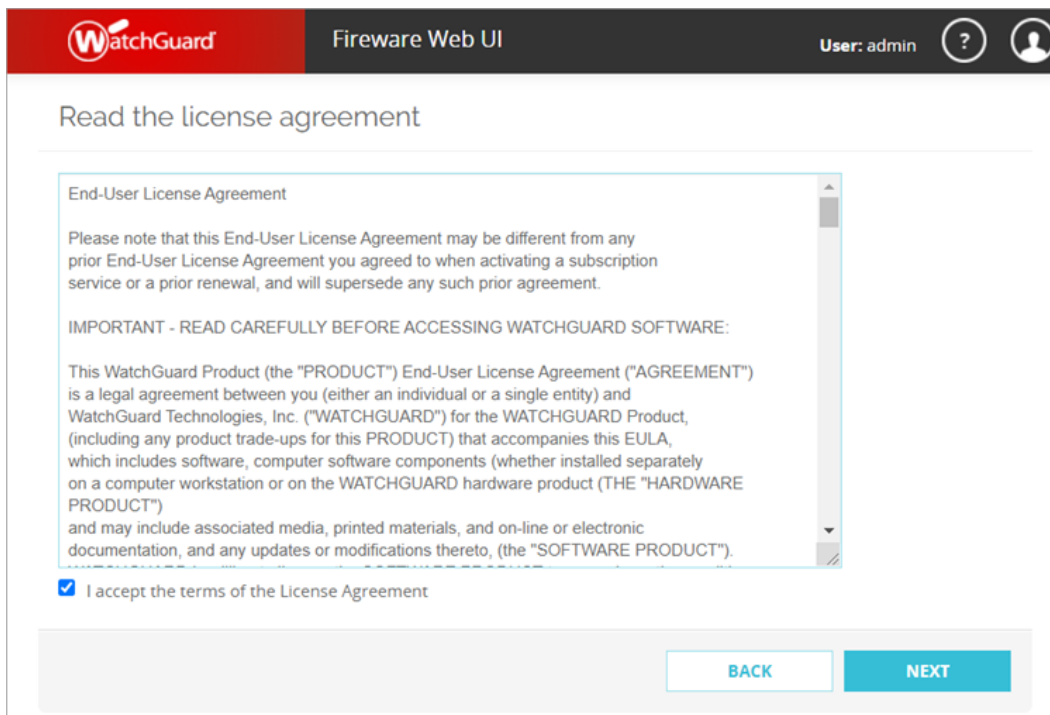
Welcome to the Firebox Cloud Setup Wizard

Select a Configuration Type

- ☐ Create new Configuration
Manage the Firebox configuration locally. You can add the Firebox to WatchGuard Cloud for monitoring only.
- ☒ Enable cloud management
Manage the Firebox configuration from WatchGuard Cloud.

NEXT

4. Click **Next**.
5. Accept the terms of the License Agreement.



WatchGuard Fireware Web UI User: admin

Read the license agreement

End-User License Agreement

Please note that this End-User License Agreement may be different from any prior End-User License Agreement you agreed to when activating a subscription service or a prior renewal, and will supersede any such prior agreement.

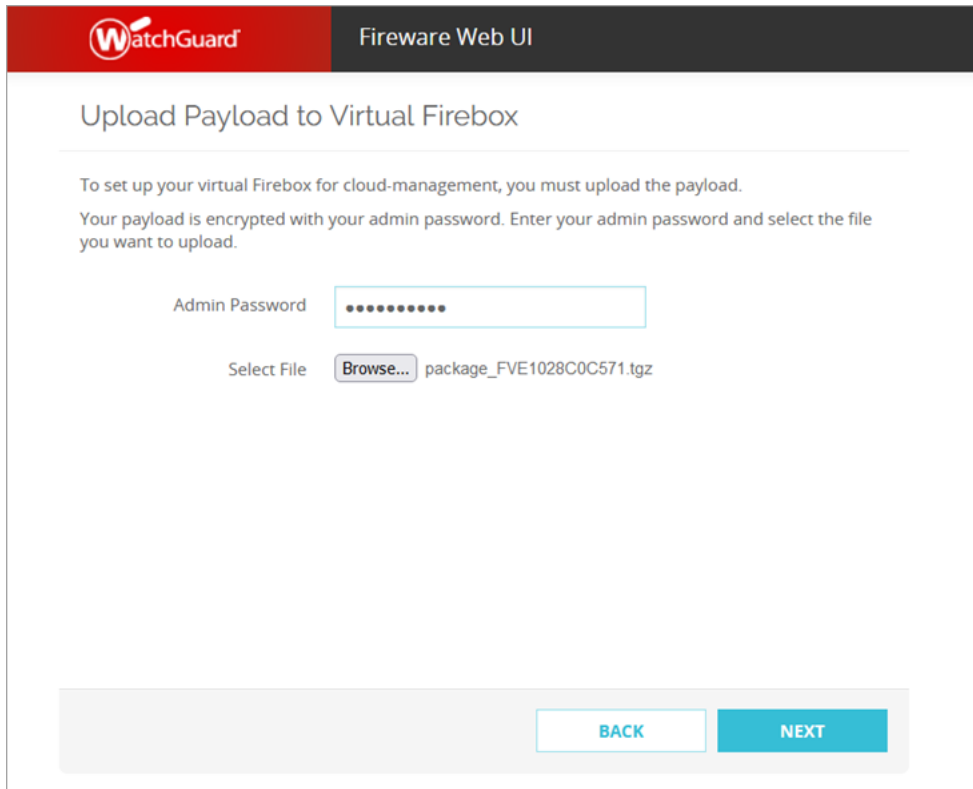
IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:

This WatchGuard Product (the "PRODUCT") End-User License Agreement ("AGREEMENT") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD Product, (including any product trade-ups for this PRODUCT) that accompanies this EULA, which includes software, computer software components (whether installed separately on a computer workstation or on the WATCHGUARD hardware product (THE "HARDWARE PRODUCT")) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, (the "SOFTWARE PRODUCT").

☒ I accept the terms of the License Agreement

BACK NEXT

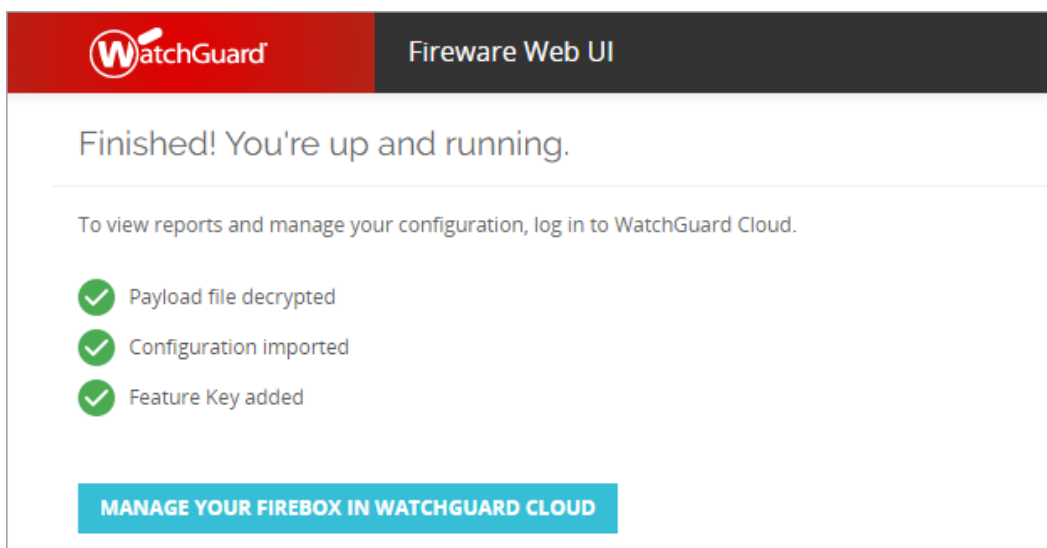
6. Click **Next**.
7. Upload the payload.
 - a. Type the admin password you created in the Add Device Wizard in WatchGuard Cloud. This password is used to decrypt the payload.
 - b. Click **Browse**, navigate to the location where you saved the payload, and select the payload file.



The screenshot shows the 'Upload Payload to Virtual Firebox' interface in the Fireware Web UI. The header includes the WatchGuard logo and 'Fireware Web UI'. The main heading is 'Upload Payload to Virtual Firebox'. Below this, instructions state: 'To set up your virtual Firebox for cloud-management, you must upload the payload. Your payload is encrypted with your admin password. Enter your admin password and select the file you want to upload.' There is a text input field for 'Admin Password' with masked characters. Below it, a 'Select File' section shows a 'Browse...' button and the filename 'package_FVE1028C0C571.tgz'. At the bottom right, there are 'BACK' and 'NEXT' buttons.

8. Click **Next**.

The payload file uploads and applies changes to the Firebox. When the process finishes, you see a message.



Verify the Firebox Cloud Status

After you upload the payload and connect Firebox Cloud in the Fireware Web UI, log in to WatchGuard Cloud to verify the connection status and other summary information on the Device Settings page and the Deployment History page.



Because AWS or Azure controls the networking information for Firebox Cloud, the Networking and Live Status Monitoring sections in WatchGuard Cloud do not show the same level of detail as physical Fireboxes or FireboxV.


For more information, go to:

- [WatchGuard Cloud Device Summary](#)
- [Monitor Live Status for Cloud-Managed Fireboxes](#)

Additional Resources

This guide described how to set up a Firebox Cloud on AWS or Microsoft Azure. After you launch and successfully connect to your instance of Firebox Cloud, use these resources to learn more about how to configure the supported features and services.

Help Center and Technical Documentation

- *Fireware Help* – From Fireware Web UI, click  for context-sensitive help, or go to [WatchGuard Help Center](#).
- Complete Fireware documentation – For the complete set of documentation for Fireware and related software go to the WatchGuard [Technical Documentation](#) page.

Technical Support

- If you require assistance with your Firebox Cloud instance, including how to handle fault conditions, go to [Support Information](#).
- For information about Support tiers and targeted response times, go to [Compare Support Levels](#).

Troubleshooting

- *Fireware Help* – For Fireware troubleshooting documentation, go to [Troubleshooting](#).

Monitor Your Firebox

- *Fireware Help* – For more information about how to monitor your Firebox Cloud instance, go to [Monitor your Firebox](#).

Manage Users and Roles on Your Firebox

- *Fireware Help* – For Firebox users and roles information, go to [Manage Users and Roles on Your Firebox](#).

Firebox Upgrade, Downgrade, and Migration

- *Fireware Help* – For Firebox upgrade, downgrade, and migration information, go to [Firebox Upgrade, Downgrade, and Migration](#).

Firebox Backup and Restore

- *Fireware Help* – For Firebox backup and restore information, go to [Firebox Backup and Restore](#).