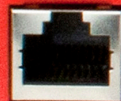




Firebox[®] M200 / M300

HW Models: ML3AE8



Quick Start Guide

快速开始指南

Guide de démarrage rapide

Kurzanleitung

Guida introduttiva

クイックスタート・ガイド

빠른 설치 안내서

Guía Rápida

Guia de início rápido

快速設定手冊

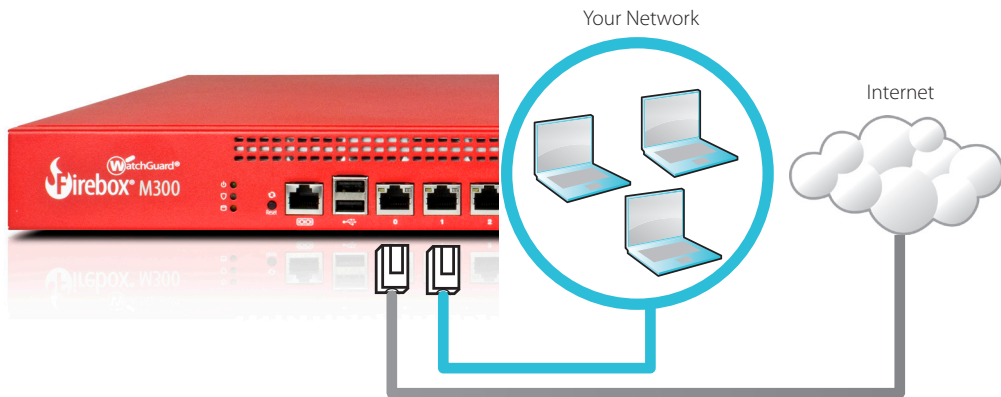
Activate Your Firebox

1. **Go to www.watchguard.com/activate**
2. Log in to your WatchGuard account, or create a new account*.
*If you create a new account, return to www.watchguard.com/activate after you finish the account creation process.
3. Type the serial number for your device.
4. **During activation, select your setup method:**
 - **RapidDeploy QuickStart** – Automatically download and apply a QuickStart configuration file to your device, pre-configured with security settings recommended by WatchGuard.
 - **Classic Activation** – Use the Web Setup Wizard to create a basic configuration file for your device.
5. Use the setup directions in this guide that match the method you selected.

RapidDeploy QuickStart Setup

1. Connect Your Firebox and Power it On

Make sure the computers on your network are configured to use DHCP. When you install your Firebox, it will assign an IP address on the **10.0.1.0/24** network.



2. Connect to the Web UI

- A. Go to **<https://10.0.1.1:8080>**
- B. You can safely ignore any certificate warnings you see because the device uses a self-signed certificate.
- C. Log in with the user account **admin** and the Admin (readwrite) passphrase you set during activation.

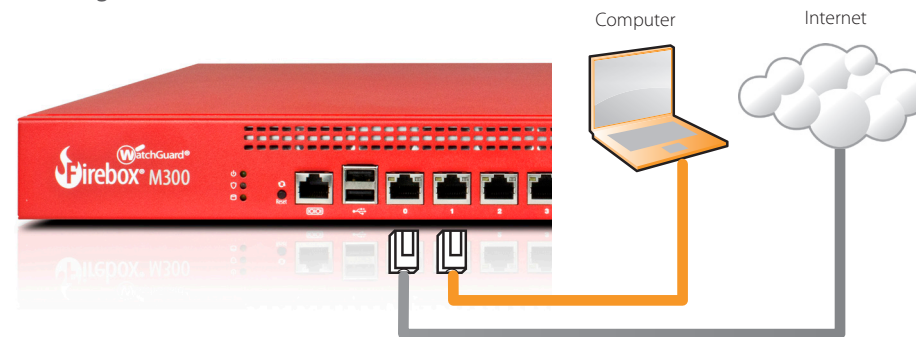
Your device has a basic configuration:

- Allows outbound TCP, UDP, and ping traffic
- Blocks all unrequested traffic from the external network
- Includes optimized security settings
- Uses licensed security services to protect the trusted and optional networks

Classic Activation Setup

1. Connect Your Firebox and Power it On

Make sure your computer is configured to use DHCP. When you connect to the Firebox, it will assign an IP address on the **10.0.1.0/24** network.



2. Connect to the Web UI

- A. Go to **<https://10.0.1.1:8080>**
- B. You can safely ignore certificate warnings, because the device uses a self-signed certificate.
- C. Log in with the user name **admin** and the passphrase **readwrite**.
- D. Follow the directions in the Web Setup Wizard to create a basic configuration file for a new device. Click *More Information* if you have questions.
- E. When the Wizard completes, log in to the Web UI with the **admin** user account and the Admin (readwrite) passphrase you set during the Wizard.
- F. Install the Firebox in your network.

Your device has a basic configuration:

- Allows outbound FTP, Ping, DNS, TCP, and UDP connections
- Blocks all unrequested traffic from the external network

- Inspects outgoing FTP, HTTP, and HTTPS traffic
- Uses licensed security services to protect the trusted and optional networks

Next Steps

Congratulations! You have finished basic setup of your Firebox. You can use the Web UI to view and edit your configuration and to manage and monitor your Firebox. Or, you can download and install WatchGuard System Manager (WSM) and use Policy Manager and the WSM suite of management and monitoring tools. Here are some recommendations to help you get started:

Verify your Internet connectivity

- With your Firebox installed in your network, make sure that your users can successfully browse the Internet.

Get the latest software

To upgrade the Firebox OS:

1. Log in to Fireware Web UI.
2. Select **System > Upgrade OS**.

To get the latest version of WSM, WatchGuard Dimension, VPN clients, and other software for your Firebox:

1. Go to www.watchguard.com/support and click **Download Software**.
2. Find the software downloads page for your Firebox model and select the software you want to install.

Explore the features and functions of your Firebox

Browse the Web UI or the tools in WatchGuard System Manager and click Help on any page or dialog box to learn more about the management, monitoring, and security features of your Firebox.


About the Device Status Lights


RJ45 interfaces

Interfaces 0 - 7 are RJ45 Ethernet interfaces that support link speeds of 10, 100, or 1000 Mbps. Each RJ45 interface has a pair of indicators. The right indicator shows the interface connection status. The left indicator shows interface activity.

Indicator	Indicator color	Interface Status
Connection (right)	Yellow	Link at 1000 Mbps
	Green	Link at 100 Mbps
	Not lit	Link at 10 Mbps, or no link
Activity (left)	Yellow, blinks	Power on, network activity
	Not lit	Power off, no connections

Storage () – When there is activity on the SD card, the storage indicator is yellow.

Arm/Disarm () – When the device is armed and ready to pass traffic, this indicator is green. When the device is powered on, but not ready to pass traffic, this indicator is red.

Power () – The power indicator on the left front of the device is green when the device is powered on.

Reset the Firebox to Factory-Default Settings

If you ever need to, you can restore your Firebox to its factory-default settings. For example, if you do not know your administrator account passphrase or you want to start over with RapidDeploy QuickStart, you can reset your device. Make sure you back up your device configuration before you reset your device in case you want to restore it in the future.

For more information, see the Hardware Guide for your Firebox, available at:

www.watchguard.com/help/documentation/hardware.asp

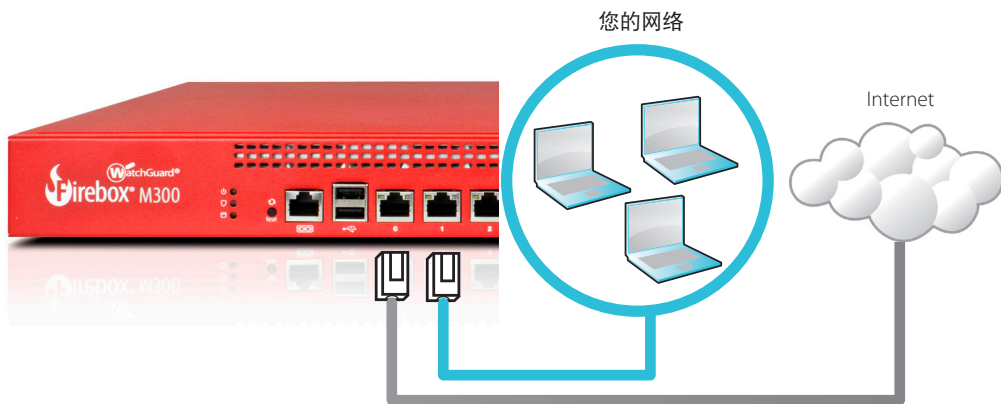
激活设备

1. 访问 www.watchguard.com/activate
2. 登录您的 WatchGuard 帐户，或者创建一个新帐户*。
*如果创建新帐户，请在完成帐户创建过程之后返回到 www.watchguard.com/activate。
3. 输入设备的序列号。
4. 在激活期间，选择设置方法：
 - **RapidDeploy QuickStart (RapidDeploy 快速部署)** – 自动下载快速部署配置文件并将其应用到您的设备，其中预配置了 WatchGuard 推荐的安全设置。
 - **Classic Activation (常规激活)** – 使用网络设置向导为您的设备创建一个基本的配置文件。
5. 请根据您选择的方法使用本手册中对应的设置说明。

RapidDeploy 快速部署设置

1. 连接您的设备并开启电源

确保网络中的计算机配置为使用 DHCP。在安装 Firebox 后，它将在 **10.0.1.0/24** 网络上分配一个 IP 地址。



2. 连接到网页管理界面

A. 访问 <https://10.0.1.1:8080>

B. 您可以安全地忽略看到的任何证书警告，因为该设备使用自签名证书。

C. 使用用户帐户 **admin** 和管理员密码 (readwrite) 登录。

您的设备具备基本配置：

- 允许出站 TCP、UDP 和 Ping 数据流

- 阻止来自外部网络的所有未请求的数据流

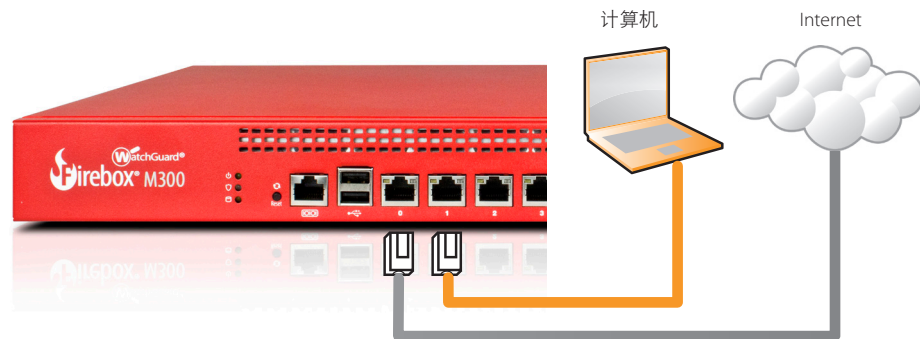
- 包含经过优化的安全设置

- 使用许可的安全服务来保护受信任的网络和可选网络

常规激活设置

1. 连接您的设备并开启电源

确保您的计算机配置为使用 DHCP。连接 Firebox 后，它将在 **10.0.1.0/24** 网络上分配一个 IP 地址。



2. 连接到网页管理界面

A. 访问 <https://10.0.1.1:8080>

B. 您可以安全地忽略证书警告，因为该设备使用自签名证书。

C. 以用户名 **admin** 和密码 **readwrite** 登录。

D. 按照网络设置向导中的说明为新设备创建一个基本的配置文件。如有问题，请单击“More Information”（更多信息）。

E. 在向导完成后，使用您在向导中设置的用户帐户 **admin** 和管理员密码 (readwrite) 登录网页管理界面。

F. 在您的网络中安装 Firebox。

您的设备具备基本配置：

- 允许出站 FTP、Ping、DNS、TCP 和 UDP 连接

- 阻止来自外部网络的所有未请求的数据流

- 检测传出 FTP、HTTP 和 HTTPS 流量

- 使用许可的安全服务来保护受信任的网络和可选网络

后续步骤

恭喜！您已经完成了 Firebox 的基本设置。您可以使用网页管理界面查看和编辑配置，以及管理和监控您的 Firebox。或者，您也可以下载并安装 WatchGuard 系统管理器（WSM），使用策略管理器和 WSM 管理与监控工具套件。下面是帮助您入门的一些建议：

验证您的 Internet 连接

- 在网络中安装 Firebox 之后，确保您的用户可以成功浏览 Internet。

获取最新版本的软件

升级 Firebox 操作系统：

1. 登录 Fireware 网页管理界面。
2. 选择 **System > Upgrade OS**（系统 > 升级操作系统）。

获取最新版本的 WSM、WatchGuard Dimension、VPN 客户端

和其他 Firebox 软件：

1. 访问 www.watchguard.com/support 并单击“Download Software”（下载软件）。
2. 找到您的 Firebox 型号的软件下载页面并选择想要安装的软件。

探索 Firebox 的特性和功能

浏览网页管理界面或 WatchGuard 系统管理器，单击任意页面或对话框的上的“Help”（帮助），详细了解 Firebox 的管理、监控和安全功能。

关于设备状态指示灯

RJ45 接口

接口 0 - 7 为 RJ45 以太网接口，支持 10、100 或 1000 Mbps 的链路速度。每个 RJ45 接口都配有一对指示灯。右侧的指示灯显示接口连接状态。左侧的指示灯显示接口活动。

指示灯	指示灯颜色	接口状态
连接（右侧）	黄色	链路速度为 1000 Mbps
	绿色	链路速度为 100 Mbps
	不亮	链路速度为 10 Mbps 或无链路
活动（左侧）	黄色，闪烁	已开启，有网络活动
	不亮	已关闭，无连接

存储 (🔋) – 在 SD 卡活动期间，存储指示灯显示为黄色。

防护/解除防护 (🛡️) – 当设备处于防护状态并可通过数据流时，此指示灯显示为绿色。当设备处于开启状态，但尚不能通过数据流时，此指示灯显示为红色。

电源 (🔌) – 当设备处于开启状态时，位于设备左前方的电源指示灯显示为绿色。

将 Firebox 重置为出厂默认设置

如果需要，可以将 Firebox 重置为其出厂默认设置。例如，如果您不知道管理员帐户的密码或者想要使用“RapidDeploy 快速部署”方式重新配置，可以重置设备。

如需了解更多信息，请参阅 Firebox 硬件指南，网址为：

www.watchguard.com/help/documentation/hardware.asp

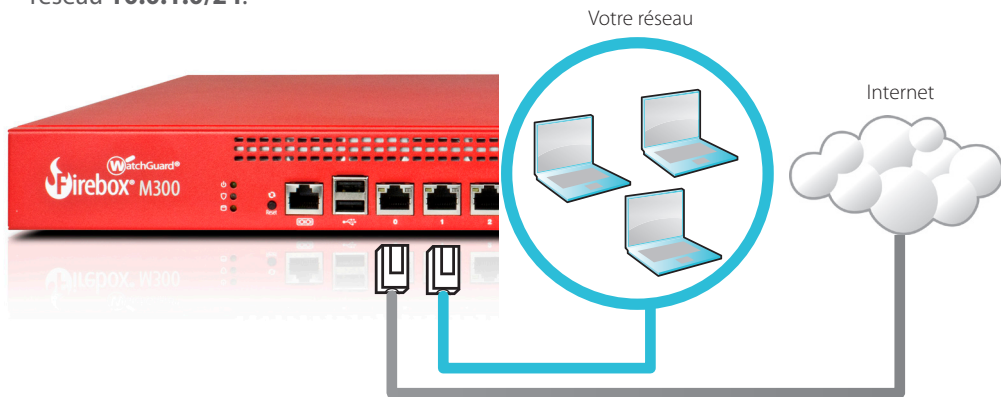
Activation de votre appliance Firebox

1. **Rendez-vous à l'adresse www.watchguard.com/activate**
2. Connectez-vous à votre compte WatchGuard ou créez un nouveau compte*.
*Si vous créez un nouveau compte, retournez à l'adresse www.watchguard.com/activate à la fin du processus de création du compte.
3. Saisissez le numéro de série de votre appareil.
4. **Lors de l'activation, sélectionnez votre méthode de configuration :**
 - **RapidDeploy QuickStart** : téléchargement et application automatiques d'un fichier de configuration QuickStart sur votre appareil. Ce fichier est pré-configuré avec les paramètres de sécurité recommandés par WatchGuard.
 - **Classic Activation** : utilisation de l'Assistant de configuration Web pour générer un fichier de configuration de base pour votre appareil.
5. Suivez les instructions de configuration correspondant à la méthode sélectionnée.

Configuration RapidDeploy QuickStart

1. Branchement et mise sous tension de votre appareil

Assurez-vous que les ordinateurs de votre réseau sont configurés pour utiliser le protocole DHCP. Lorsque vous installez votre appliance Firebox, elle attribue une adresse IP sur le réseau **10.0.1.0/24**.



2. Connexion à l'interface utilisateur Web

A. Rendez-vous à l'adresse <https://10.0.1.1:8080>

- B. Votre appareil utilisant un certificat auto-signé, vous pouvez, sans risque, ignorer les avertissements liés aux certificats.
- C. Connectez-vous avec le compte utilisateur **admin** et le mot de passe Admin (readwrite) que vous avez définis lors de l'activation.

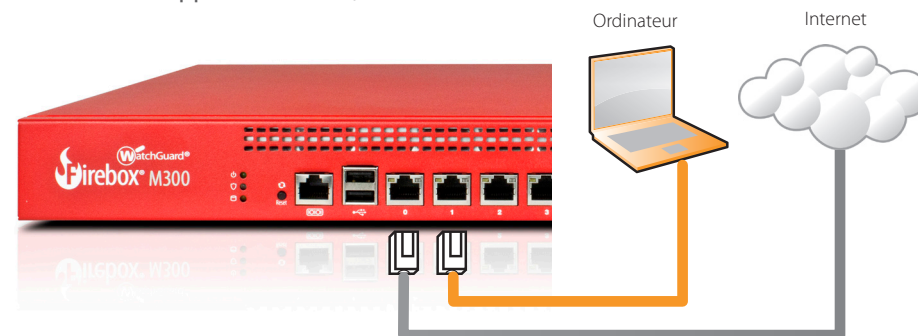
Votre appareil présente une configuration de base :

- Trafic sortant TCP, UDP et Ping autorisés.
- Blocage de tout le trafic non demandé en provenance du réseau externe.
- Paramètres de sécurité optimisés.
- Utilisation de services de sécurité sous licence pour protéger les réseaux approuvés et en option

Configuration Classic Activation

1. Branchement et mise sous tension de votre appliance Firebox

Assurez-vous que votre ordinateur est configuré pour utiliser le protocole DHCP. Lorsque vous connectez votre appliance Firebox, elle attribue une adresse IP sur le réseau **10.0.1.0/24**.



2. Connexion à l'interface utilisateur Web

A. Rendez-vous à l'adresse <https://10.0.1.1:8080>

- B. Votre appareil utilisant un certificat auto-signé, vous pouvez, sans risque, ignorer les avertissements liés aux certificats.
- C. Connectez-vous avec le nom d'utilisateur **admin** et le mot de passe **readwrite**.
- D. Suivez les instructions de l'Assistant de configuration Web pour générer un fichier de configuration pour un nouvel appareil. Si vous avez des questions, cliquez sur *Plus d'informations*.
- E. Une fois que l'Assistant a terminé, connectez-vous à l'interface utilisateur Web avec le nom d'utilisateur **admin** et le mot de passe Admin (readwrite) que vous avez définis dans l'Assistant.
- F. Installez l'appliance Firebox sur votre réseau.

Votre appareil présente une configuration de base :

- Autorisation des connexions sortantes FTP, Ping, DNS, TCP et UDP.
- Blocage de tout le trafic non demandé en provenance du réseau externe.

- Inspection du trafic sortant FTP, HTTP et HTTPS.
- Utilisation de services de sécurité sous licence pour protéger les réseaux approuvés et en option.

Étapes suivantes

Félicitations ! Vous avez à présent terminé la configuration de base de votre appliance Firebox. Vous pouvez utiliser l'interface utilisateur Web pour consulter et modifier votre configuration, mais aussi pour gérer et contrôler votre appliance. Autrement, vous pouvez télécharger et installer WatchGuard System Manager (WSM) et utiliser Policy Manager et la suite WSM d'outils de gestion et de surveillance. Voici quelques recommandations pour débiter :

Vérifiez votre connectivité Internet

- Une fois votre appliance Firebox installée sur votre réseau, assurez-vous que vos utilisateurs peuvent naviguer correctement sur Internet.

Procurez-vous le logiciel le plus récent

Pour mettre à niveau le système d'exploitation de l'appliance Firebox :

1. Connectez-vous à l'interface utilisateur Web de Fireware.
2. Sélectionnez **System > Upgrade OS (Système > Mise à niveau du système d'exploitation)**.

Pour obtenir la toute dernière version de WSM, de WatchGuard Dimension, des clients VPN et d'autres logiciels pour votre appliance Firebox :

1. Rendez-vous à l'adresse www.watchguard.com/support et cliquez sur Download Software (Téléchargements de logiciels).
2. Recherchez la page des téléchargements de logiciels pour votre modèle d'appliance Firebox et sélectionnez le logiciel à installer.

Examen des caractéristiques et fonctions de votre appliance Firebox

Accédez à l'interface utilisateur Web ou aux outils de WatchGuard System Manager et cliquez sur l'icône d'Aide d'une page ou d'une boîte de dialogue pour en savoir plus sur les fonctions de gestion, de surveillance et de sécurité de votre appliance Firebox.


À propos des témoins d'état de l'appareil


Ports RJ45

Les interfaces 0 à 7 sont des ports Ethernet RJ45 qui prennent en charge des vitesses de 10, 100 ou 1 000 Mbps. Chaque port RJ45 comporte deux indicateurs. Celui de droite indique l'état de la connexion de l'interface. Celui de gauche indique l'activité de l'interface.

Indicateur	Couleur de l'indicateur	État de l'interface
Connexion (droit)	Jaune	Liaison à 1 000 Mbps
	Vert	Liaison à 100 Mbps
	Éteint	Liaison à 10 Mbps ou aucune liaison
Activité (gauche)	Jaune, clignotant	Sous tension, activité réseau
	Éteint	Hors tension, aucune connexion

Storage (Stockage) () : lorsque la carte SD est active, l'indicateur de stockage est jaune.

Arm/Disarm (Activation/désactivation) () : lorsque l'appareil est activé et prêt à transmettre du trafic, cet indicateur passe au vert. Lorsque l'appareil est sous tension mais qu'il n'est pas prêt à transmettre du trafic, cet indicateur est rouge.

Power (Alimentation) () : situé à l'avant gauche, l'indicateur d'alimentation est vert lorsque l'appareil est sous tension.

Rétablissement des paramètres d'usine de l'appliance Firebox

En cas de besoin, vous pouvez réinitialiser votre appliance Firebox sur ses paramètres d'usine. Par exemple, vous pouvez réinitialiser votre appareil si vous ne connaissez pas le mot de passe de votre compte administrateur ou si vous souhaitez recommencer à l'aide de RapidDeploy QuickStart.

Pour en savoir plus, reportez-vous au Guide du matériel pour votre appliance Firebox, disponible à l'adresse suivante :

www.watchguard.com/help/documentation/hardware.asp

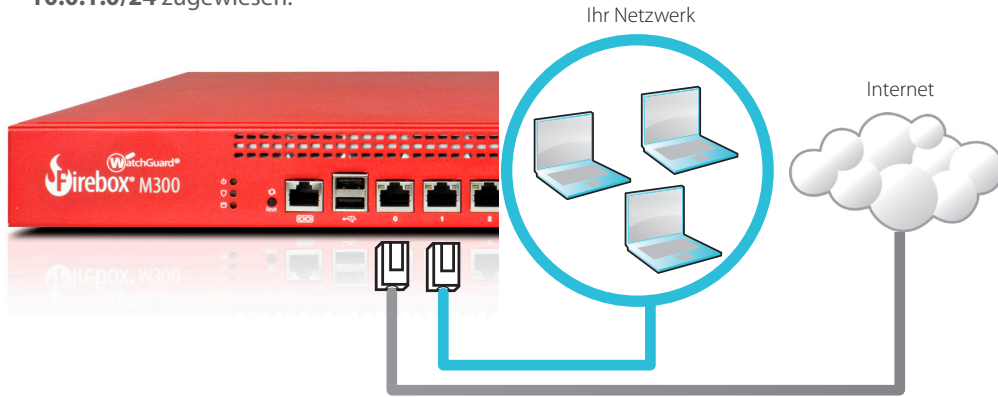
Firebox aktivieren

1. **Rufen Sie die Website www.watchguard.com/activate auf.**
2. Melden Sie sich bei Ihrem WatchGuard-Account an oder erstellen Sie ein neues Konto*.
*Falls Sie ein neues Konto erstellen, kehren Sie nach erfolgreichem Abschluss zur Seite www.watchguard.com/activate zurück.
3. Geben Sie die Seriennummer Ihres Geräts ein.
4. **Wählen Sie bei der Aktivierung eines der folgenden Setup-Verfahren aus:**
 - **RapidDeploy-Schnellstart** – Sie können automatisch eine Schnellstart-Konfigurationsdatei auf Ihr Gerät herunterladen und ausführen. Hierbei sind die von WatchGuard empfohlenen Sicherheitseinstellungen bereits vorkonfiguriert.
 - **Klassische Aktivierung** – Erstellen Sie mithilfe des Web-Setup-Assistenten eine Basiskonfigurationsdatei für Ihr Gerät.
5. Folgen Sie den Setup-Anweisungen in diesem Handbuch für das von Ihnen gewählte Verfahren.

Setup mit RapidDeploy-Schnellstart

1. Firebox anschließen und einschalten

Stellen Sie sicher, dass die Computer in Ihrem Netzwerk für die Verwendung von DHCP konfiguriert sind. Wenn Sie Ihre Firebox installieren, wird eine IP-Adresse im Netzwerk **10.0.1.0/24** zugewiesen.



2. Verbindung zum Web-Interface herstellen

- A. **Rufen Sie die Website <https://10.0.1.1:8080> auf.**
- B. Eventuell angezeigte Zertifikatswarnungen können Sie ignorieren, da das Gerät ein selbstsigniertes Zertifikat verwendet.
- C. Melden Sie sich mit dem Benutzerkonto **admin** und dem Admin-Kennwort (**readwrite**) an, das Sie während der Aktivierung festgelegt haben.

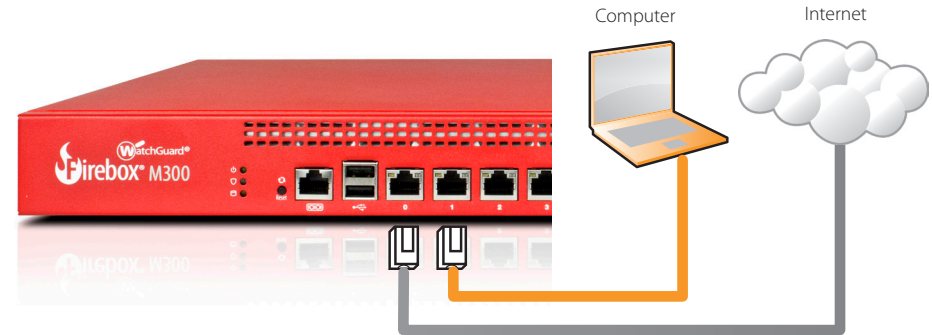
Ihr Gerät verfügt über die folgende Basiskonfiguration:

- Unterstützung für ausgehenden TCP-, UDP- und Ping-Datenverkehr
- Blockierung von nicht angefordertem Datenverkehr aus dem externen Netzwerk
- Bereitstellung optimierter Sicherheitseinstellungen
- Verwendung lizenzierter Sicherheitsdienste zum Schutz vertrauenswürdiger und optionaler Netzwerke

Setup mit klassischer Aktivierung

1. Firebox anschließen und einschalten

Stellen Sie sicher, dass Ihr Computer für die Verwendung von DHCP konfiguriert ist. Wenn Sie eine Verbindung zu Ihrer Firebox herstellen, wird eine IP-Adresse im Netzwerk **10.0.1.0/24** zugewiesen.



2. Verbindung zum Web-Interface herstellen

- A. **Rufen Sie die Website <https://10.0.1.1:8080> auf.**
- B. Eventuell angezeigte Zertifikatswarnungen können Sie ignorieren, da das Gerät ein selbstsigniertes Zertifikat verwendet.
- C. Melden Sie sich mit dem Benutzernamen **admin** und dem Kennwort **readwrite** an.
- D. Folgen Sie den Anweisungen im Web-Setup-Assistenten, um eine Basiskonfigurationsdatei für ein neues Gerät zu erstellen. Klicken Sie bei weiteren Fragen auf *More Information*.
- E. Melden Sie sich nach Abschluss des Assistenten mit dem Benutzerkonto **admin** und dem Admin-Kennwort (**readwrite**), das Sie mit dem Assistenten festgelegt haben, an der Web-Schnittstelle an.
- F. Installieren Sie die Firebox in Ihrem Netzwerk.

Ihr Gerät verfügt über die folgende Basiskonfiguration:

- Unterstützung von ausgehenden FTP-, Ping-, DNS-, TCP- und UDP-Verbindungen
- Blockierung von nicht angefordertem Datenverkehr aus dem externen Netzwerk

- Prüfung von ausgehendem FTP-, HTTP- und HTTPS-Datenverkehr
- Verwendung lizenzierter Sicherheitsdienste zum Schutz vertrauenswürdiger und optionaler Netzwerke

Weitere Schritte

Herzlichen Glückwunsch! Sie haben das Basis-Setup für Ihre Firebox abgeschlossen. Über das Web-Interface können Sie Ihre Konfiguration anzeigen lassen sowie bearbeiten und Ihre Firebox verwalten und überwachen. Alternativ können Sie den WatchGuard System Manager (WSM) herunterladen und installieren und den Policy Manager und die WSM-Suite mit Management- und Überwachungstools verwenden. Tipps für den Start:

Internetverbindung überprüfen

- Stellen Sie sicher, dass Ihre Nutzer nach der Installation der Firebox im Netzwerk problemlos im Internet navigieren können.

Neueste Software implementieren

So führen Sie ein Upgrade des Firebox-Betriebssystems durch:

1. Melden Sie sich beim Firewall-Web-Interface an.
2. Wählen Sie die Option **System > Upgrade OS** aus.

So rufen Sie die neueste Version von WSM, WatchGuard Dimension, VPN-Clients und anderer Software für die Firebox ab:

1. Rufen Sie die Website www.watchguard.com/support auf, und klicken Sie auf „Download Software“.
2. Gehen Sie auf die Seite mit den Software-Downloads für Ihr Firebox-Modell und wählen Sie die zu installierende Software aus.

Erkunden der Merkmale und Funktionen der Firebox

Durchsuchen Sie das Web-Interface oder die Tools in WatchGuard System Manager und klicken Sie auf einer beliebigen Seite oder in einem beliebigen Dialogfeld auf „Help“, um weitere Informationen zu den Verwaltungs-, Überwachungs- und Sicherheitsmerkmalen Ihrer Firebox zu erhalten.


Informationen zu den Statusanzeigen des Geräts


RJ45-Schnittstellen

Schnittstellen 0–7 sind RJ45-Ethernet-Schnittstellen, die Verbindungsgeschwindigkeiten von 10, 100, oder 1.000 Mbit/s unterstützen. Jede RJ45-Schnittstelle verfügt über ein Anzeigenpaar. Die rechte Anzeige signalisiert den Verbindungsstatus der Schnittstelle. Die linke Anzeige signalisiert die Schnittstellenaktivität.

Anzeige	Farbsignal	Schnittstellenstatus
Verbindung (rechts)	Gelb	Verbindung mit 1.000 Mbit/s
	Grün	Verbindung mit 100 Mbit/s
	Leuchtet nicht	Verbindung mit 10 Mbit/s oder keine Verbindung
Aktivität (links)	Gelb, blinkt	Eingeschaltet, Netzwerkaktivität
	Leuchtet nicht	Ausgeschaltet, keine Verbindung

Storage () – Wenn auf der SD-Karte Aktivität stattfindet, leuchtet die Speicheranzeige gelb.

Arm/Disarm () – Wenn das Gerät aktiv und bereit ist, Daten zu übertragen, leuchtet diese Anzeige grün. Wenn das Gerät eingeschaltet, jedoch nicht bereit ist, Daten zu übertragen, leuchtet diese Anzeige rot.

Power () – Diese Anzeige links auf der Vorderseite des Geräts leuchtet grün, wenn das Gerät eingeschaltet ist.

Zurücksetzen der Firebox auf die Standard-Werkseinstellungen

Falls erforderlich, lassen sich jederzeit die Werkseinstellungen Ihrer Firebox wiederherstellen. Sie können Ihr Gerät beispielsweise zurücksetzen, wenn Sie Ihr Kennwort für das Administratorkonto vergessen haben oder den RapidDeploy QuickStart durchführen möchten.

Weitere Informationen finden Sie im Hardwarehandbuch für Ihre Firebox. Sie finden es unter:
www.watchguard.com/help/documentation/hardware.asp

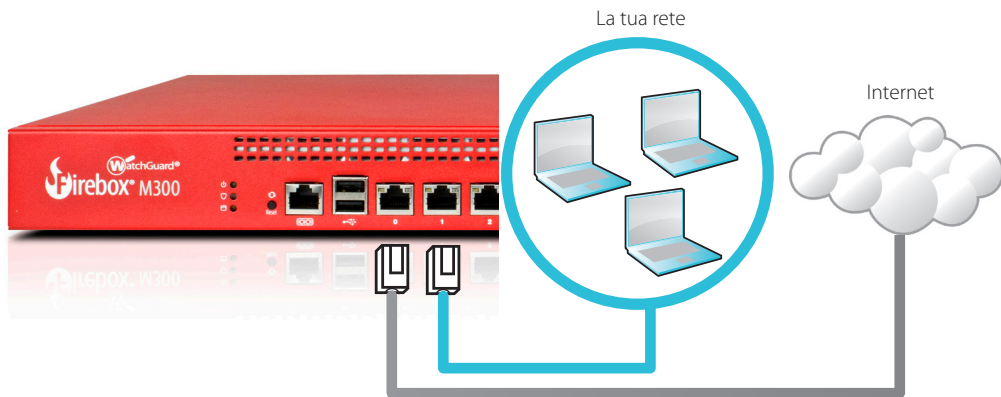
Attivazione di Firebox

1. **Vai su www.watchguard.com/activate**
2. Accedi al tuo account WatchGuard, oppure creane uno nuovo*.
*Se crei un nuovo account, ritorna a www.watchguard.com/activate dopo aver terminato la procedura di creazione dell'account.
3. Digita il numero di serie del tuo dispositivo.
4. **Durante l'attivazione, seleziona il metodo di installazione preferito:**
 - **RapidDeploy QuickStart** – Scarica automaticamente e applica il file di configurazione sul tuo dispositivo, con le impostazioni di sicurezza consigliate da WatchGuard.
 - **Attivazione classica** – Utilizza la procedura guidata, attraverso l'interfaccia di gestione via Web, per creare il file di configurazione base per il tuo dispositivo.
5. Utilizza le istruzioni per l'installazione contenute in questa guida, corrispondenti al metodo selezionato.

Impostazione di RapidDeploy QuickStart

1. Collegamento e accensione di Firebox

Assicurati che i computer collegati alla rete siano configurati per utilizzare il protocollo DHCP. Quando installi il tuo Firebox, questo assegnerà al computer un indirizzo IP nella sottorete **10.0.1.0/24**.



1. Connessione all'interfaccia di gestione via Web

- A. Vai all'indirizzo **<https://10.0.1.1:8080>**
- B. Puoi ignorare l'avviso di sito web non sicuro dovuto al certificato SSL, perché il dispositivo utilizza un certificato auto-firmato.
- C. Accedi con l'account utente **admin** e la passphrase di amministratore (readwrite) impostata durante l'attivazione.

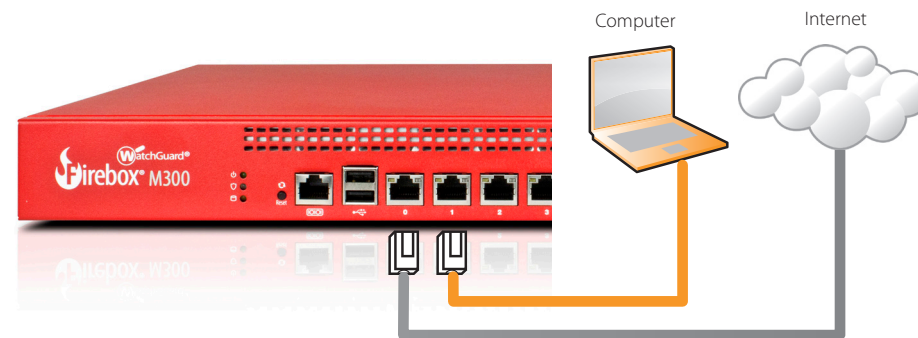
Il dispositivo contiene una configurazione di base:

- Consente il traffico TCP e UDP in uscita, e il ping
- Blocca tutto il traffico non richiesto dalla rete esterna
- Include impostazioni di sicurezza ottimizzate
- Utilizza i servizi di sicurezza concessi in licenza per proteggere le reti affidabili e opzionali

Impostazioni di attivazione classiche

2. Collegamento e accensione di Firebox

Verifica che il computer in uso sia configurato per utilizzare il protocollo DHCP. Quando installi il tuo Firebox, questo assegnerà al computer un indirizzo IP nella sottorete **10.0.1.0/24**.



3. Connessione all'interfaccia di gestione via Web

- A. Vai all'indirizzo **<https://10.0.1.1:8080>**
- B. Puoi ignorare tranquillamente qualsiasi avviso di certificato visualizzato perché il dispositivo utilizza un certificato autofirmato.
- C. Accedi con il nome utente **admin** e la passphrase **readwrite**.
- D. Per creare un file di configurazione di base per il nuovo dispositivo, segui le indicazioni contenute nella procedura guidata per l'installazione basata sul Web. In caso di domande, fai clic su *Ulteriori informazioni*.
- E. Una volta completata la procedura guidata, accedi all'interfaccia di gestione via Web con l'account utente **admin** e la password (readwrite), impostata durante la procedura guidata.
- F. Installa il Firebox nella tua rete.

Il dispositivo contiene una configurazione di base:

- Consente le connessioni in uscita FTP, Ping, DNS, TCP e UDP
- Blocca tutto il traffico non richiesto dalla rete esterna
- Ispeziona il traffico in uscita FTP, HTTP e HTTPS

- Utilizza i servizi di sicurezza concessi in licenza per proteggere le reti affidabili e opzionali

Passaggi successivi

Congratulazioni! L'installazione di base di Firebox è completata. Per visualizzare e modificare la configurazione in uso e per gestire e monitorare Firebox, utilizza l'interfaccia di gestione via Web. In alternativa, è possibile scaricare e installare WatchGuard System Manager (WSM) e utilizzare Policy Manager e la suite di strumenti gestionali e di monitoraggio WSM. Di seguito alcuni consigli utili per iniziare:

Verifica della connessione a Internet

- Dopo avere installato Firebox nella tua rete, verifica che gli utenti possano navigare in Internet senza problemi.

Aggiornamento del software

Per aggiornare il sistema operativo Firebox:

1. Accedi all'interfaccia utente Web Firewall.
2. Seleziona **System > Upgrade OS**.

Per ottenere l'ultima versione di WSM, WatchGuard Dimension, client VPN e altro software per Firebox:

1. Vai su www.watchguard.com/support e fai clic su Download Software.
2. Cerca la pagina per scaricare il software di Firebox e seleziona il software che desideri installare.

Esplorazione delle caratteristiche e delle funzionalità del Firebox

Per ulteriori informazioni sulle funzionalità di gestione, monitoraggio e sicurezza di Firebox, sfogliare l'interfaccia utente basata sul web o gli strumenti di WatchGuard System Manager e fare clic su ? o su qualsiasi altra pagina o finestra di dialogo.


Informazioni sulle spie di stato del dispositivo

Interfacce RJ45

Le interfacce 0 - 7 sono interfacce Ethernet RJ45 che supportano velocità di collegamento di 10, 100 o 1000 Mbps. Ogni interfaccia RJ45 ha una coppia di indicatori. L'indicatore di destra mostra lo stato di connessione dell'interfaccia. L'indicatore di sinistra mostra l'attività dell'interfaccia.

Indicatore	Colore dell'indicatore	Stato dell'interfaccia
Connessione (destra)	Giallo	Collegamento a 1000 Mbps
	Verde	Collegamento a 100 Mbps
	Spento	Collegamento a 10 Mbps, o nessun collegamento
Attività (sinistra)	Giallo, lampeggiante	Accensione, attività della rete
	Spento	Spegnimento, nessuna connessione

Archiviazione () – Quando la scheda SD è attiva, l'indicatore di archiviazione è giallo.

Attivazione/Disattivazione () – Quando il dispositivo è attivo e pronto a trasmettere traffico, questo indicatore è verde. Quando il dispositivo è acceso, ma non è ancora pronto a trasmettere traffico, questo indicatore è rosso.

Alimentazione () – L'indicatore dell'alimentazione a sinistra è verde quando il dispositivo è acceso.

Ripristino delle impostazioni di fabbrica predefinite di Firebox

Se necessario, è possibile ripristinare le impostazioni di fabbrica di Firebox. Per esempio, il dispositivo può essere ripristinato se non conosci la passphrase dell'account administrator o se desideri ricominciare la procedura con RapidDeploy QuickStart.

Per maggiori informazioni, consulta la Guida all'hardware del tuo Firebox, disponibile all'indirizzo:

www.watchguard.com/help/documentation/hardware.asp

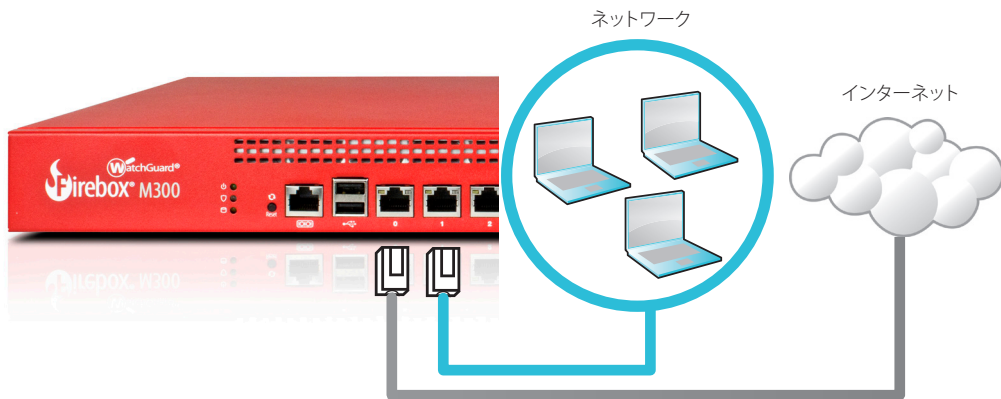
デバイスのアクティベーションを行う

1. www.watchguard.com/activate にアクセスします。
2. 登録済みの WatchGuard アカウントにログインするか、新しいアカウントを作成します*。
* 新しいアカウントを作成する場合は、アカウントの作成が完了してからもう一度 www.watchguard.com/activate にアクセスしてください。
3. デバイスのシリアル番号を入力します。
4. アクティベーションの実行時にセットアップ方法を選択します。
 - **RapidDeploy QuickStart** – QuickStart 設定ファイルを自動的にダウンロードしてデバイスに適用します。このファイルは、WatchGuard で推奨しているセキュリティ設定を事前に設定したものです。
 - **従来のアクティベーション** – ウェブセットアップ・ウィザードを使用して、デバイスの基本設定ファイルを作成します。
5. 選択した方法に応じて、本ガイドのいずれかのセットアップ手順に従います。

RapidDeploy QuickStart によるセットアップ

1. デバイスを接続して電源を入れる

ネットワーク上のコンピュータが DHCP を使用するように設定されていることを確認します。Firebox のインストール時に、**10.0.1.0/24** ネットワーク上の IP アドレスが割り当てられます。



2. WebUI に接続する

- https://10.0.1.1:8080 にアクセスします。**
- Firebox デバイスは自己署名証明書を使用するため、証明書に関する警告は無視してかまいません。
- アクティベーションの実行時に設定したユーザー・アカウント **admin** と管理用パスワード **readwrite** でログインします。

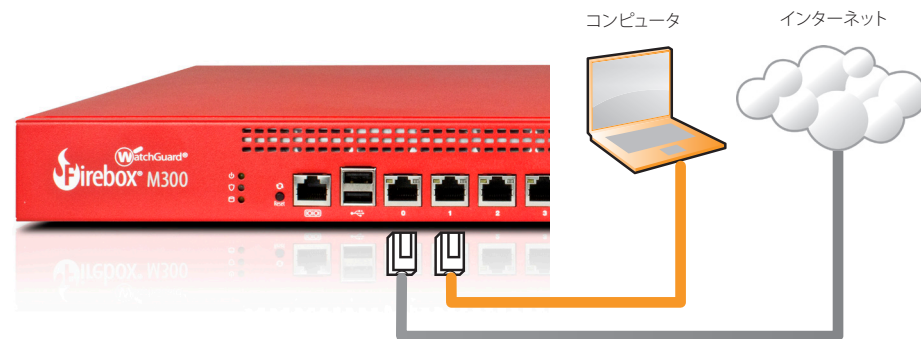
デバイスの基本設定は次のとおりです。

- ・アウトバウンドの TCP、UDP、および ping トラフィックを許可
- ・外部ネットワークからのすべての要求されないトラフィックをブロック
- ・セキュリティ設定を最適化
- ・信頼できるネットワークとオプション ネットワーク保護のため、ライセンス式セキュリティ サービスを使用

従来のアクティベーションによるセットアップ

1. デバイスを接続して電源を入れる

コンピュータが DHCP を使用するように設定されていることを確認します。Firebox への接続時に、**10.0.1.0/24** ネットワーク上の IP アドレスが割り当てられます。



2. WebUI に接続する

- https://10.0.1.1:8080 にアクセスします。**
- Firebox デバイスは自己署名証明書を使用するため、証明書に関する警告は無視してかまいません。
- ユーザー名 **admin** とパスワード **readwrite** でログインします。
- ウェブセットアップ・ウィザードの手順に従って、新しいデバイスの基本設定ファイルを作成します。詳しい手順を確認する場合は、[More Information] をクリックしてください。
- ウィザードが完了したら、ウィザードで設定したユーザー・アカウント **admin** と管理用パスワード **readwrite** でウェブ UI にログインします。

- ネットワークに Firebox をインストールします。

デバイスの基本設定は次のとおりです。

- ・アウトバウンド FTP、Ping、DNS、TCP、UDP 接続を可能にする
- ・外部ネットワークからのすべての要求されないトラフィックをブロック

- ・ 外部に向けた FTP、HTTP、HTTPS トラフィックを検査
- ・ 信頼できるネットワークとオプション ネットワーク保護のため、ライセンス式セキュリティ サービスを使用

次のステップ

おめでとうございます。これで Firebox の基本セットアップが完了しました。Web UI を使って、設定の閲覧と編集、および Firebox の管理 / 監視が可能です。また、WatchGuard System Manager (WSM) をダウンロードしてインストールし、Policy Manager や WSM スイートに含まれる管理 / 監視ツールを利用することもできます。それらの作業の手始めとして、いくつかの推奨事項を次に示します。

インターネット接続を確認する

- ・ ネットワークにインストールした Firebox で、ユーザーがインターネットを正常に閲覧できることを確認します。

最新のソフトウェアを入手する

Firebox OS をアップグレードする手順は次のとおりです。

1. Firewall Web UI にログインします。
2. **System > Upgrade OS** を選択します。

Firebox 用に、最新版の WSM、WatchGuard Dimension、VPN clients、

その他のソフトウェアを入手するには：

1. www.watchguard.com/support にアクセスし、Download Software をクリックします。
2. お使いのモデルに対応したソフトウェア ダウンロード ページを探し、インストールするソフトウェアを選択します。

Firebox の機能について調べる

WatchGuard System Manager のウェブ UI やツールを参照し、それぞれのページまたはダイアログ ボックスで [Help] をクリックして、Firebox の管理、監視、およびセキュリティの機能の詳細を確認してください。

デバイスのステータス・ライトについて

RJ45 インターフェイス

インターフェイス 0 ～ 7 は RJ45 イーサネット・インターフェイスで、10、100、または 1000 Mbps のリンク速度をサポートします。RJ45 インターフェイスにはそれぞれ、ペアのインジケータがあります。右側のインジケータはインターフェイスの接続ステータスを示し、左側のインジケータはインターフェイスのアクティビティを示します。

インジケータ	インジケータの色	インターフェイスのステータス
接続（右）	黄色	リンク速度 1000 Mbps
	緑色	リンク速度 100 Mbps
	消灯	リンク速度 10 Mbps、またはリンクなし
アクティビティ（左）	黄色の点滅	電源オン、ネットワーク・アクティビティ
	消灯	電源を切る、接続なし

Storage () – SD カードに対するアクティビティがある場合は黄色に点滅します。

Arm/Disarm () – デバイスの電源が入った状態で、トラフィックを送受信する準備ができている場合は緑色に点灯します。デバイスの電源が入っていても、トラフィックを送受信する準備ができていない場合は赤色に点灯します。

Power () – デバイス前面の左側にあるインジケータは、デバイスの電源が入っているときに点灯します。

Firebox の設定を工場出荷時の状態に戻す

必要に応じて、Firebox の設定を工場出荷時の状態に戻すことができます。たとえば、管理者アカウントのパスワードを忘れた場合や、RapidDeploy QuickStart でセットアップをやり直したい場合に、デバイスをリセットすることができます。

詳細については、下記のサイトでお使いの Firebox 向けのハードウェア・ガイドを参照してください。

www.watchguard.com/help/documentation/hardware.asp

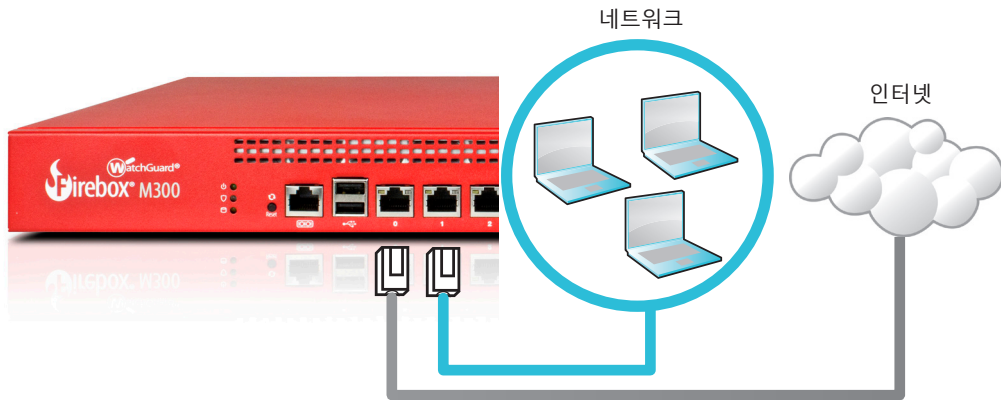
장치 활성화

1. www.watchguard.com/activate로 이동합니다.
2. WatchGuard 계정으로 로그인하거나 새 계정을 만듭니다*.
*새 계정을 만들 경우 계정 생성 과정을 마친 후 www.watchguard.com/activate로 돌아가십시오.
3. 장치의 일련 번호를 입력합니다.
4. 활성화 과정을 진행하는 중에 원하는 설정 방법을 선택합니다.
 - **RapidDeploy QuickStart** – WatchGuard에서 권장하는 보안 설정으로 사전 구성된 QuickStart 구성 파일을 자동으로 다운로드하여 장치에 적용합니다.
 - **Classic Activation** – Web Setup Wizard를 사용하여 장치에 대한 기본 구성 파일을 만듭니다.
5. 이 가이드에서 선택한 방법에 맞는 설정 지침을 따릅니다.

RapidDeploy QuickStart 설정

1. 장치 연결 및 전원 켜기

네트워크에 있는 컴퓨터가 DHCP를 사용하도록 설정되어 있는지 확인합니다. Firebox를 설치할 때 **10.0.1.0/24** 네트워크의 IP 주소가 자동 할당됩니다.



2. Web UI에 연결

- https://10.0.1.1:8080**로 이동합니다.
- 장치에서 자체 서명된 인증서를 사용하기 때문에 인증서 경고는 안심하고 무시하시면 됩니다.
- 사용자 계정 **admin**과 활성화 과정에서 설정한 Admin 암호(readwrite)를 사용하여 로그인합니다.

장치가 기본적으로 다음과 같이 구성됩니다.

- 아웃바운드 TCP, UDP 및 Ping 트래픽 허용
- 외부 네트워크에서 들어오는 요청되지 않은 트래픽 모두 차단
- 최적화된 보안 설정 포함
- 라이선스가 있는 보안 서비스를 사용하여 신뢰할 수 있고 선택적인 네트워크를 보호합니다.

Classic Activation 설정

1. 장치 연결 및 전원 켜기

컴퓨터가 DHCP를 사용하도록 설정되어 있는지 확인합니다. Firebox에 연결할 때 **10.0.1.0/24** 네트워크의 IP 주소가 자동으로 할당됩니다.



2. Web UI에 연결

- https://10.0.1.1:8080**로 이동합니다.
- 장치에서 자체 서명된 인증서를 사용하기 때문에 인증서 경고는 안심하고 무시하시면 됩니다.
- 사용자 이름 **admin**과 암호 **readwrite**를 사용하여 로그인합니다.
- Web Setup Wizard의 지침을 따라 새 장치에 대한 기본 구성 파일을 만듭니다. 질문이 있을 경우 *More Information*을 클릭합니다.
- 마법사가 완료되면 사용자 계정 **admin**과 마법사를 진행하는 도중 설정한 Admin 암호(readwrite)를 사용하여 Web UI에 로그인합니다.
- 네트워크에 Firebox를 설치합니다.

장치가 기본적으로 다음과 같이 구성됩니다.

- 아웃바운드 FTP, Ping, DNS, TCP 및 UDP 연결 허용
- 외부 네트워크에서 들어오는 요청되지 않은 트래픽 모두 차단

- 나가는 FTP, HTTP 및 HTTPS 트래픽 검사
- 라이선스가 있는 보안 서비스를 사용하여 신뢰할 수 있고 선택적인 네트워크를 보호합니다.

다음 단계

축하합니다! Firebox 기본 설정을 완료하였습니다. Web UI를 사용하여 구성을 보고 편집할 수 있으며 Firebox를 관리하고 모니터링할 수 있습니다. 또는 WatchGuard System Manager(WSM)를 다운로드한 후 설치하여 Policy Manager와 WSM 관리 및 모니터링 도구 제품군을 사용할 수도 있습니다. 시작할 때 도움이 되는 몇 가지 권장 사항은 다음과 같습니다.

인터넷 연결 상태 확인

- 네트워크에 설치된 Firebox에서 사용자가 성공적으로 인터넷을 탐색할 수 있는지 확인하십시오.

최신 소프트웨어 다운로드

Firebox OS를 업그레이드하려면 다음과 같이 하십시오.

1. Fireware Web UI에 로그인합니다.
2. **System > Upgrade OS**를 선택합니다.

최신 버전의 WSM, WatchGuard Dimension, VPN 클라이언트 및 기타 Firebox용 소프트웨어를 다운로드하려면 다음과 같이 하십시오.

1. www.watchguard.com/support로 이동하여 Download Software를 클릭합니다.
2. Firebox 모델의 소프트웨어 다운로드 페이지를 찾아 설치하고자 하는 소프트웨어를 선택합니다.

Firebox의 기능 살펴보기

Web UI 또는 WatchGuard System Manager의 도구를 살펴보고 어떠한 페이지나 대화 상자에서든 Help를 클릭하면 Firebox의 관리, 모니터링 및 보안 기능에 대한 자세한 내용을 볼 수 있습니다.

장치 상태 표시등 정보

RJ45 인터페이스

인터페이스 0 - 7은 10Mbps, 100Mbps 또는 1000Mbps 링크 속도를 지원하는 RJ45 이더넷 인터페이스입니다. 각 RJ45 인터페이스에는 한 쌍의 표시등이 있습니다. 오른쪽 표시등은 인터페이스 연결 상태를 표시합니다. 왼쪽 표시등은 인터페이스 활동을 표시합니다.

표시등	표시등 색상	인터페이스 상태
연결(오른쪽)	노란색	1000Mbps 링크 속도
	녹색	100Mbps 링크 속도
	켜져 있지 않음	10 Mbps 링크 속도, 또는 링크가 없음
활동(왼쪽)	노란색, 깜박임	전원 켜짐, 네트워크 활동
	켜져 있지 않음	전원 꺼짐, 연결 안 됨

Storage (☐) - SD 카드에 활동이 있는 경우, 스토리지 표시등이 노란색으로 켜집니다.

Arm/Disarm (☑) - 장치가 작동 설정되어 트래픽을 전달할 준비가 된 경우, 이 표시등이 녹색으로 켜집니다. 장치의 전원이 켜졌으나 트래픽을 전달할 준비가 되지 않은 경우, 이 표시등이 빨간색으로 켜집니다.

Power (Ⓢ) - 장치의 전원이 켜지면, 장치 왼쪽 앞면의 전원 표시등이 녹색으로 켜집니다.

Firefox를 공장 초기 설정으로 리셋

필요할 경우 Firefox를 공장 초기 설정으로 되돌릴 수 있습니다. 예를 들어, 관리자 계정 암호를 모르거나 RapidDeploy QuickStart로 다시 시작하고자 하는 경우 장치를 리셋할 수 있습니다.

자세한 내용은 사용하시는 Firefox용 하드웨어 가이드를 참조하십시오. 이 가이드는 다음에서 확인할 수 있습니다.

www.watchguard.com/help/documentation/hardware.asp

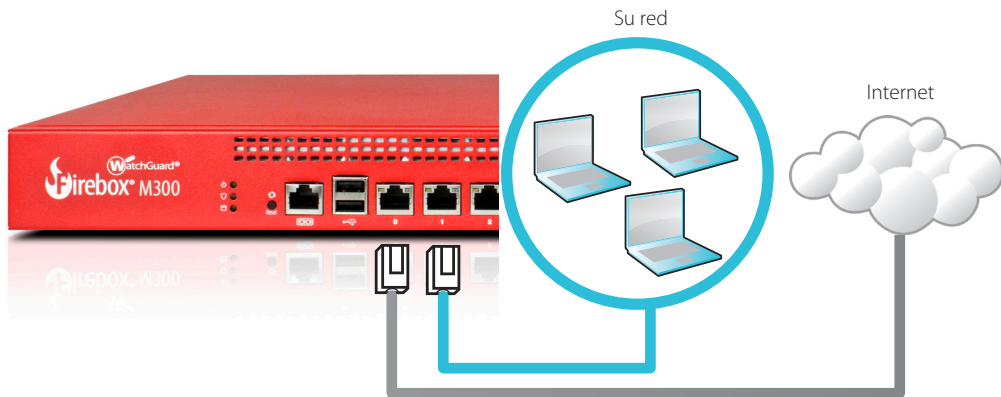
Active su Firefox

1. **Visite www.watchguard.com/activate**
2. Inicie sesión con su cuenta de WatchGuard o cree una cuenta nueva*.
*Si usted crea una cuenta nueva, regrese a www.watchguard.com/activate luego de finalizar el proceso de creación de la cuenta.
3. Ingrese el número de serie de su dispositivo.
4. **Durante la activación, seleccione su método de instalación:**
 - **Inicio rápido de RapidDeploy:** automáticamente descargue y aplique un archivo de configuración de inicio rápido en su dispositivo, configurado previamente con la configuración de seguridad recomendada por WatchGuard.
 - **Activación clásica:** use el asistente de instalación web para crear un archivo de configuración básico para su dispositivo.
5. Use las directivas de instalación de esta guía que correspondan al método que seleccionó.

Instalación del inicio rápido RapidDeploy

1. Conecte o Firebox e ligue-o

Asegúrese de que los equipos de su red estén configurados para usar DHCP. Cuando instale su Firebox, este le asignará una dirección IP en la red **10.0.1.0/24**.



2. Conéctese a la Interfaz de Usuario Web

A. Vaya a <https://10.0.1.1:8080>

- B. De manera segura, puede ignorar cualquier certificado de advertencia que vea debido a que el dispositivo usa un certificado con firma automática.
- C. Inicie sesión con la cuenta de usuario **admin** y la frase de contraseña de Administrador (readwrite) que estableció durante la activación.

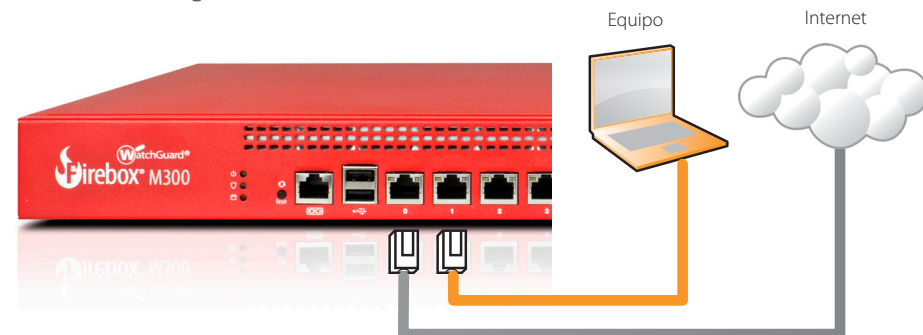
Su dispositivo tiene una configuración básica:

- Permite tráfico ping, UDP y TCP saliente.
- Bloquea todo el tráfico no solicitado de la red externa
- Incluye configuración de seguridad optimizada
- Usa servicios de seguridad con licencia para proteger las redes confiables y opcionales.

Instalación de activación clásica

1. Conecte o Firebox e ligue-o

Asegúrese de que su equipo esté configurado para usar DHCP. Cuando se conecte a su Firebox, este le asignará una dirección IP en la red **10.0.1.0/24**.



2. Conéctese a la Interfaz de Usuario Web

A. Vaya a <https://10.0.1.1:8080>

- B. De manera segura, puede ignorar cualquier certificado de advertencia debido a que el dispositivo usa un certificado con firma automática.
- C. Inicie sesión con el nombre de usuario **admin** y la frase de contraseña **readwrite**.
- D. Siga las directivas en el asistente de instalación web para crear un archivo de configuración básico para un dispositivo nuevo. Haga clic en *Más información* si tiene preguntas.
- E. Cuando el asistente finalice, inicie sesión en la interfaz de usuario web con la cuenta de usuario **admin** y la frase de contraseña de Administrador (readwrite) que estableció durante el asistente.

F. Instale el Firebox en su red

Su dispositivo tiene una configuración básica:

- Permite conexiones UDP, TCP, DNS, ping y FTP salientes.
- Bloquea todo el tráfico no solicitado de la red externa
- Inspecciona tráfico HTTPS, HTTP y FTP saliente.
- Usa servicios de seguridad con licencia para proteger las redes confiables y opcionales.

Próximos pasos

¡Felicitaciones! Ha finalizado la instalación básica de su Firebox. Puede usar la interfaz de usuario web para ver y editar su configuración, y para administrar y controlar su Firebox. O bien, puede descargar e instalar WatchGuard System Manager (WSM) y usar la función Policy Manager y el conjunto de herramientas de gestión y supervisión de WSM. A continuación, presentamos algunas recomendaciones para ayudarlo a comenzar:

Verifique su Conexión a Internet

- Con su Firebox instalado en su red, asegúrese de que sus usuarios puedan navegar correctamente en Internet.

Obtenga el Software más Reciente

Para actualizar el SO Firebox:

1. Inicie sesión en la interfaz de usuario web de Fireware.
2. Seleccione **System (Sistema) > Upgrade OS (Actualizar SO)**.
Para obtener la versión más reciente de WSM, WatchGuard Dimension, clientes de VPN y otras aplicaciones de software para su Firebox:

1. Visite www.watchguard.com/support y haga clic en Download Software (Descargar software).

2. Encuentre la página de descargas de software para su modelo de Firebox y seleccione el software que desee instalar.

Explore las características y funciones de su Firebox


Explore la interfaz de usuario web o las herramientas de WatchGuard System Manager y haga clic en Help (Ayuda) en cualquier página o cuadro de diálogo para aprender más sobre las características de seguridad, control y gestión de su Firebox.


Acerca de las luces de estado del dispositivo


Interfaces de RJ45

Las interfaces de 0 a 7 son interfaces de Ethernet que soportan velocidades de enlace de 10, 100 o 1000 Mbps. Cada interfaz de RJ45 tiene un par de indicadores. El indicador de la derecha muestra el estado de conexión de la interfaz. El indicador de la izquierda muestra la actividad de la interfaz.

Indicador	Color del indicador	Estado de interfaz
Conexión (derecha)	Amarillo	Enlace a 1000 Mbps
	Verde	Enlace a 100 Mbps
	Sin iluminación	Enlace a 10 Mbps o sin enlace
Actividad (izquierda)	Amarillo, parpadea	Encendido, actividad de red
	Sin iluminación	Apagado, sin conexiones

Almacenamiento (): cuando hay actividad en la tarjeta Compact Flash, el indicador de almacenamiento se enciende de color amarillo.

Armar/Desarmar (): cuando el dispositivo está armado y listo para transmitir tráfico, este indicador se muestra verde. Cuando el dispositivo está encendido, pero no está listo para transmitir tráfico, este indicador se muestra rojo.

Encendido (): el indicador de encendido ubicado en la parte frontal izquierda del dispositivo se muestra verde cuando el dispositivo está encendido.

Restablecimiento del Firebox a la configuración predeterminada de fábrica

Si alguna vez lo necesita, puede restaurar su Firebox a la configuración predeterminada de fábrica. Por ejemplo, si no conoce la frase de contraseña de su cuenta de administrador o quiere comenzar de nuevo con el inicio rápido RapidDeploy, puede restablecer su dispositivo.

Para obtener más información, consulte la guía de hardware de su Firebox, disponible en: www.watchguard.com/help/documentation/hardware.asp

Ative o dispositivo

1. **Acesse www.watchguard.com/activate**

2. Faça login na conta WatchGuard ou crie uma conta nova*.

*Se for criar uma conta nova, volte a www.watchguard.com/activate depois de concluído o processo de criação de conta.

3. Insira o número de série do dispositivo.

4. **Durante a ativação, selecione o método de configuração:**

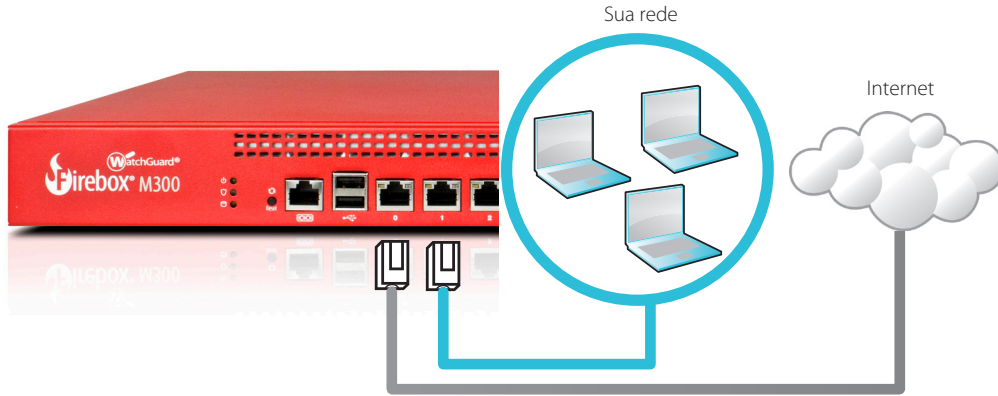
- **RapidDeploy QuickStart** – baixe e aplique automaticamente um arquivo de configuração QuickStart no dispositivo, pré-configurado com as configurações de segurança recomendadas pela WatchGuard.
- **Ativação clássica** – use o Assistente de Configuração pela Web para criar um arquivo de configuração básica para o dispositivo.

5. Use as orientações de configuração neste guia que correspondam ao método selecionado.

Configuração RapidDeploy QuickStart

1. Conecte o dispositivo e ligue-o

Certifique-se de que os computadores da rede estejam configurados para usar DHCP. Ao instalar o Firebox, ele atribuirá um endereço IP na rede **10.0.1.0/24**.



2. Conecte à interface de usuário da web

A. Acesse <https://10.0.1.1:8080>

- B. É seguro ignorar os avisos de certificado exibidos porque o dispositivo usa um certificado autoassinado.
- C. Faça login com a conta de usuário **admin** e a senha do Admin (readwrite) definida durante a ativação.

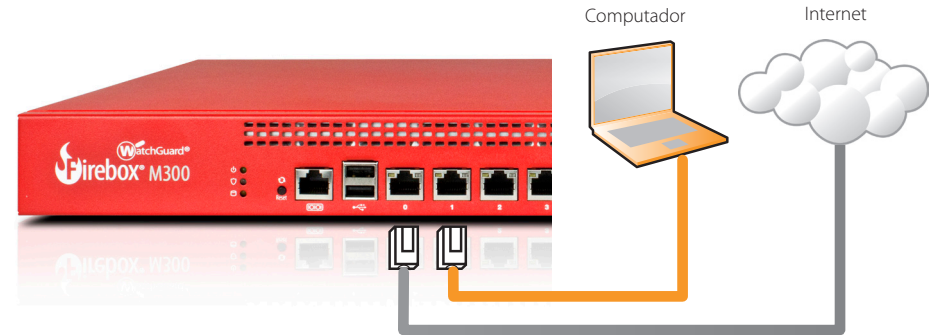
O dispositivo tem uma configuração básica:

- Permite TCP, UDP e tráfego de ping de saída
- Bloqueia todo tráfego não solicitado da rede externa
- Contém configurações de segurança otimizadas
- Usa serviços de segurança licenciados para proteger as redes opcionais e confiáveis

Configuração de ativação clássica

1. Conecte o dispositivo e ligue-o

Certifique-se de que o computador esteja configurado para usar DHCP. Ao conectar-se ao Firebox, ele atribuirá um endereço IP na rede **10.0.1.0/24**.



2. Conecte à interface de usuário da web

A. Acesse <https://10.0.1.1:8080>

- B. É seguro ignorar os avisos de certificado porque o dispositivo usa um certificado autoassinado.
- C. Faça login com o nome de usuário **admin** e a senha **readwrite**.
- D. Siga as instruções no Assistente de Configuração da Web para criar um arquivo de configuração básica para o dispositivo. Em caso de dúvidas, clique em *Mais informações*.
- E. Na conclusão do assistente, faça login na interface de usuário da web com a conta de usuário **admin** e a senha do Admin (readwrite) definida durante o Assistente.
- F. Instale o Firebox na rede.

O dispositivo tem uma configuração básica:

- Permite conexões de saída de FTP, Ping, DNS, TCP e UDP
- Bloqueia todo tráfego não solicitado da rede externa

- Inspecciona o tráfego de saída de FTP, HTTP e HTTPS
- Usa serviços de segurança licenciados para proteger as redes opcionais e confiáveis

Próximas etapas

Parabéns! Você concluiu a configuração básica do Firebox. Use a interface de usuário da web para editar as configurações e para gerenciar e monitorar o Firebox. Ou você pode fazer o download e instalar o WatchGuard System Manager (WSM) e usar o Policy Manager e o conjunto WSM de ferramentas de gerenciamento e monitoramento. Eis algumas recomendações para ajudar no início:

Verifique a conectividade com a internet

- Com o Firebox instalado na rede, certifique-se de que os usuários consigam navegar na internet.

Obtenha o software mais recente

Para atualizar o Firebox OS:

1. Faça login na interface de usuário da web do Fireware.
2. Selecione **System > Upgrade OS (Sistema > Atualizar SO)**.

Para obter a versão mais recente do WSM, do WatchGuard Dimension, dos clientes VPN

e outros software para o seu Firebox:

1. Acesse www.watchguard.com/support e clique em Download Software (Baixar software).
2. Encontre a página de downloads de software do modelo do Firebox e selecione o software que deseja instalar.

Explore os recursos e as funções do Firebox


Abra a interface de usuário da web ou as ferramentas no WatchGuard System Manager e clique em Help (Ajuda) em qualquer página ou caixa de diálogo para saber mais sobre os recursos de gerenciamento, monitoramento e segurança do Firebox.


Sobre as luzes de estado do dispositivo


Interfaces RJ45

As interfaces 0 a 7 são interfaces Ethernet RJ45 que suporta velocidades de link de 10, 100 ou 1.000 Mbps. Cada interface RJ45 tem um par de indicadores. O indicador direito mostra o estado de conexão da interface. O indicador esquerdo mostra a atividade da interface.

Indicador	Cor do indicador	Estado da interface
Conexão (direita)	Amarelo	Link a 1.000 Mbps
	Verde	Link a 100 Mbps
	Apagado	Link a 10 Mbps ou sem link
Atividade (esquerda)	Amarelo, pisca	Ligado, atividade de rede
	Apagado	Desligado, sem conexões

Storage (Armazenamento) () – Quando há atividade no cartão SD, o indicador de armazenamento fica amarelo.

Arm/Disarm (Armar/Desarmar) () – Quando o dispositivo está armado e pronto para passar tráfego, esse indicador fica verde. Quando o dispositivo está ligado, mas não está pronto para passar tráfego, esse indicador fica vermelho.

Power (Ligado/Desligado) () – O indicador ligado/desligado na frente à esquerda do dispositivo fica verde quando o dispositivo está ligado.

Redefina o Firebox com as configurações padrão de fábrica

Se for necessário, é possível restaurar as configurações padrão de fábrica do Firebox. Por exemplo, se não souber a senha da conta do administrador ou quiser reiniciar o RapidDeploy QuickStart, você pode redefinir o dispositivo.

Para obter mais informações, consulte o guia de hardware do seu Firebox, disponível em: www.watchguard.com/help/documentation/hardware.asp

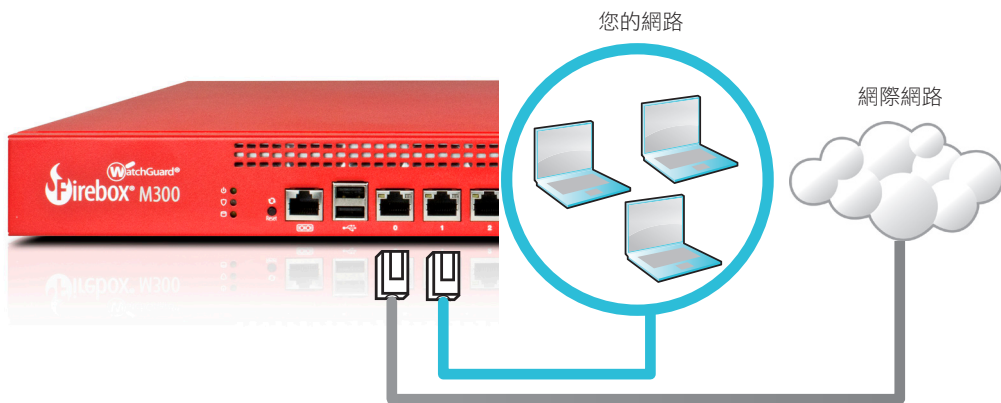
啟動您的裝置

1. 請前往 www.watchguard.com/activate
2. 登入您的 WatchGuard 帳戶，或是建立新的帳戶*。
*如果您建立新的帳戶，請在帳戶建立程序完成後返回 www.watchguard.com/activate
3. 輸入您的裝置序號。
4. 在啟用期間，選取您的安裝方法：
 - **RapidDeploy QuickStart** (快速部署快速啟動) - 自動下載並套用 QuickStart 設定檔案到您的裝置，使用 WatchGuard 建議的資訊安全設定預先設定。
 - **Classic Activation** (傳統啟用) - 使用「網頁安裝精靈」為您的裝置建立基本設定。
5. 使用此指南中符合您所選方法的安裝程式指示。

RapidDeploy QuickStart (快速部署快速啟動) 安裝程式

1. 連接您的裝置並開啟電源

確定您網路上的電腦已設定為使用 DHCP。當您安裝 Firebox 時，它將會指派 **10.0.1.0/24** 網路上的 IP 位址。



2. 連線到 Web UI

- 請前往 **<https://10.0.1.1:8080>**
- 您可以安全地忽略看到的任何憑證警告，因為裝置使用自我簽署憑證。
- 以您在啟用期間所設定的使用者帳戶 **admin** 與 Admin (readwrite) 密碼登入。

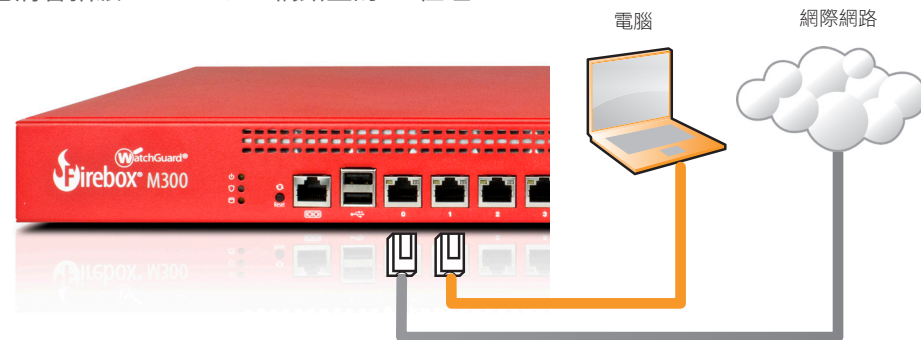
您的裝置會有下列基本設定：

- 允許連出的 TCP、UDP 與 Ping 流量
- 封鎖來自外部網路所有的流量
- 包含最佳化的資訊安全設定
- 使用授權的資訊安全服務以保護信任和選用的網路

Classic Activation (傳統啟用) 安裝程式

1. 連接您的裝置並開啟電源

請確定您的電腦已設定為使用 DHCP。連線到 Firebox 時，它將會指派 **10.0.1.0/24** 網路上的 IP 位址。



2. 連線到 Web UI

- 請前往 **<https://10.0.1.1:8080>**
- 您可以安全地忽略憑證警告，因為裝置使用自我簽署憑證。
- 請利用使用者名稱 **admin** 與密碼 **readwrite** 登入。
- 請遵循「Web 安裝精靈」中的指示，建立新裝置的基本設定檔案。若您有問題，請按一下 [More Information] (更多資訊)。
- 當精靈完成時，請使用您在精靈期間設定的 **admin** 使用者帳戶與 Admin (readwrite) 密碼登入 Web UI。
- 在您的網路中安裝 Firebox。

您的裝置會有下列基本設定：

- 允許對外的 FTP、Ping、DNS、TCP 及 UDP 連線
- 封鎖來自外部網路所有的流量
- 檢查 FTP 下載、HTTP 及 HTTPS 傳輸

- 使用授權的資訊安全服務以保護信任和選用的網路

接下來的步驟

恭喜！您已經完成 Firebox 的基本安裝。您可以使用 Web UI 檢視及編輯設定，並管理及監視您的 Firebox。或者，您可以下載並安裝 WatchGuard System Manager (WSM)，並使用管理與監控工具的 Policy Manager 以及 WSM 套件。以下是協助您開始使用的一些建議：

驗證您的網際網路連線

- 在網路中安裝 Firebox 之後，請確認您的使用者可以順利瀏覽網際網路。

取得最新的軟體

升級 Firebox OS：

1. 登入 Fireware Web UI。
2. 選取 **[System] (系統) > [Upgrade OS] (升級 OS)**。

若要取得最新版本的 WSM、WatchGuard Dimension、VPN 客戶端，以及其他 Firebox 軟體：

1. 前往 www.watchguard.com/support 並按一下 [Download Software] (下載軟體)。
2. 尋找您的 Firebox 型號所對應的軟體下載頁面，並選取您要安裝的軟體。

探索 Firebox 特色與功能

瀏覽 Web UI 或是 WatchGuard System Manager 中的工具，並按一下任何頁面或對話方塊上的 [Help] (說明)，了解更多關於 Firebox 管理、監視與安全功能的詳細資訊。

關於裝置狀態燈號

RJ45 介面

介面 0-7 是 RJ45 乙太網路介面，它們支援 10、100 或 1000 Mbps 的連結速度。每個 RJ45 介面都有一組指示燈。右邊的指示燈會顯示介面連線狀態。左邊的指示燈會顯示介面活動。

指示燈	指示燈色彩	介面狀態
連線 (右邊)	黃色	以 1000 Mbps 的速度連結
	綠色	以 100 Mbps 的速度連結
	未亮起	以 10 Mbps 的速度連結或無連結
活動 (左邊)	黃色，閃爍	電源開啟，網路活動
	未亮起	電源關閉，無連線

Storage (儲存裝置) (☐) - 當 Compact Flash 上有活動進行，儲存裝置指示燈會是黃色。

Arm/Disarm (防護/解除防護) (☑) - 當裝置已受到防護且準備好傳輸流量，此指示燈會是綠色。當裝置電源已開啟，但尚未準備好傳輸流量，此指示燈會是紅色。

Power (電源) (⏻) - 當裝置電源已開啟，裝置左前方的電源指示燈會是綠色。

將 Firebox 重設為預設設定

若您需要，可以將 Firebox 還原為出廠預設值。例如，若您不知道系統管理員帳戶密碼，或是想要以 RapidDeploy QuickStart (快速部署快速啟動) 重新開始，您可以重設裝置。

如需詳細資訊，請參閱 Firebox 硬體手冊，網址是：

www.watchguard.com/help/documentation/hardware.asp

Notices:

All WatchGuard products are designed and tested to meet strict safety requirements. These requirements include product safety approvals and other global compliance standards. Please read the following instructions carefully before operating the product, and refer to them as needed to ensure the continued safe operation of your product. Additional information can be found in the Hardware Guide located on the WatchGuard website:

<http://www.watchguard.com/help/documentation/hardware.asp>

Product Safety Certification

The WatchGuard product is safety certified under the following standards:

- CAN/CSA C 22.2 No. 60950-1-07+A1:2011+A2:2014
- UL 60950-1:2007 R10.14
- IEC 60950-1:2005 (Second Edition) + Am 1:2009 + Am 2:2013
- EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

Safety Warning

- Do not place objects on the power cord.
- Do not obstruct the ventilation openings. These openings prevent overheating of the machine.
- Never push objects of any kind into slots or openings on this equipment. Making a contact with a voltage point or shorting out a part may result in fire or electrical shock.
- When removing or installing an appliance, follow the general installation safety instructions.

Disclaimer

WatchGuard shall not be held liable if the end user alters, modifies, or repairs any WatchGuard hardware appliance.

Hinweise Zur Sicherheit

Alle WatchGuard Produkte werden entwickelt und getestet, um strenge Sicherheitsanforderungen zu erfüllen. Diese Anforderungen umfassen Produktsicherheit Zulassungen und andere globale Compliance- Standards. Bitte lesen Sie die folgenden Anweisungen sorgfältig, bevor Sie das Produkt, und bezeichnen sie als notwendig, um den sicheren Betrieb des Geräts zu gewährleisten. Weitere Informationen finden Sie in der elektronischen Hardware Guide.

Die WatchGuard Produkt ist Sicherheit unter den folgenden Normen zertifiziert:

- CAN/CSA C 22.2 No. 60950-1-07+A1:2011+A2:2014
- UL 60950-1:2007 R10.14
- IEC 60950-1:2005 (Second Edition) + Am 1:2009 + Am 2:2013
- EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

Sicherheitshinweis

- Legen Sie keine Gegenstände auf das Netzkabel.
- Verdecken Sie nicht die Lüftungsöffnungen. Diese Öffnungen verhindern eine Überhitzung der Maschine
- Stecken Sie niemals Gegenstände jeglicher Art in die Schlitz- oder Öffnungen des Geräts stecken. Der Kontakt mit einem spannungsführenden Punkt oder das Kurzschließen eines Bauteils kann zu einem Brand oder elektrischen Schlag führen.
- Beim Entfernen oder Installieren eines Gerätes, nach den allgemeinen Installation Sicherheitshinweise.

Aviso De Seguridad

Todos los productos WatchGuard están diseñados y probados para satisfacer estrictos requisitos de seguridad. Estos requisitos incluyen la homologación de productos de seguridad y otras normas de cumplimiento global. Por favor, lea atentamente las siguientes instrucciones antes de utilizar el producto, y se refieren a ellos como sea necesario para garantizar el funcionamiento seguro y continuo de su producto. Información adicional se puede encontrar en la Guía del usuario electrónica.

Certificación de seguridad del producto

El producto tiene certificación de seguridad WatchGuard bajo las siguientes normas:

- CAN/CSA C 22.2 No. 60950-1-07+A1:2011+A2:2014
- UL 60950-1:2007 R10.14
- IEC 60950-1:2005 (Second Edition) + Am 1:2009 + Am 2:2013
- EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

Advertencia de seguridad

- No coloque objetos sobre el cable de alimentación.
- No obstruya las aberturas de ventilación. Estas aberturas evitan el sobrecalentamiento de la máquina.
- Nunca introduzca objetos de ningún tipo en las ranuras o aberturas del equipo. El contacto con puntos de voltaje o el cortocircuito de una pieza podría provocar un incendio o una descarga eléctrica.
- Al extraer o instalar un electrodoméstico, siga las instrucciones generales de instalación de seguridad.

CE Notice:



The CE symbol on your WatchGuard Technologies equipment indicates that it is in compliance with the Electromagnetic Compatibility (EMC) directive and the Low Voltage Directive (LVD) of the European Union (EU).

Federal Communication Commission Interference Statement



This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the device.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. RoHS Statement

The member states of the European Union approved directive 2002/95/EC, Restrictions of Hazardous Substances ("RoHS directive") that became valid on July 1, 2006. It states that all new electrical and electronic equipment put on the market within the member states must not contain certain hazardous materials. This device complies with the European Union's RoHS directive 2002/95/EC and similar regulations that may be adopted by other countries for European Sales.

WEEE Statement

WEEE is a general set of requirements dictated in the EU Directive 2002/96/EC. This Directive mandated that member EU countries enact regulations governing the Waste of Electrical and Electronic Equipment (WEEE). The Directive, and its individual transpositions into specific country laws and legislation, is aimed at the reduction of WEEE through reuse, recovery, and recycling of WEEE.

WatchGuard is working in partnership with our European Union (EU) distribution partners to ensure that our products are in compliance with the WEEE statutes, and that the recovery of our product per the specific EU country legislative requirements is seamless for our product's end users. If you have a WatchGuard product that is at its end of life and needs to be disposed of, please contact WatchGuard Customer Care Department at:

U.S. Customers: 877.232.3531 International Customers: +1.206.613.0456

WatchGuard is reasonably confident that our products do not contain any substances or hazardous materials presently banned by any legislation, and do not present a risk due to hazardous materials. WEEE recovery professionals should also note that these products do not have any materials that are of particular high value in their individual form.

REACH

The new EU chemicals policy REACH (Registration, Evaluation, Authorization and restriction of Chemicals) came into effect on June 1, 2007. REACH is Europe's new chemicals legislation, which is applicable in all 27 EU Member States as well as the EFTA European Economic Area (EEA). REACH creates a new system for gathering information, assessing risks to human health and the environment, and authorizing or restricting the marketing and use of chemicals produced or supplied in the EEA. REACH has an impact on EEA producers and importers of finished products and users of chemicals in the course of industrial or professional activities.

WatchGuard supports the overall REACH objective of improving the protection of human health and the environment and will meet all applicable REACH requirements. WatchGuard is strongly committed to working with our customers and supply chain to define and implement the REACH requirements and ensure a smooth transition to compliance.

One of the REACH requirements is that manufacturers and importers have the duty to register substances they are producing or importing. In accordance with the regulations, the products of WatchGuard do not need to be registered for the following reasons:

- WatchGuard does not import more than 1 metric ton per year of a substance as defined by REACH.
- WatchGuard products are non-chemical products that are not designed to release any substance under normal and reasonably predictable application.
- Our products do not contain the listed substances at more than 0.1% by weight of the whole product/part.

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. CAN ICES-3(A)/NMB-3(A)

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Japan VCCI Notice (Class A ITE)

これはVCCI評議会の基準に基づくクラスA製品です。本製品がラジオやテレビ受信機の近くで使用されている場合は、電波障害を引き起こすことがあります。インストールして、取扱説明書に従って機器を使用しています。

Taiwan Class A Notice:

警告使用者：這是A類產品，應使用並正確安裝。本產品可能會造成無線電干擾，在這種情況下，用戶可能需要採取適當的措施。

警告 本電池如果更換不正確會有爆炸的危險，請勿自行更換電池

Mexico Notice:

La operación de este equipo está sujeta a las siguientes dos condiciones:

- 1) es posible que este equipo o dispositivo no cause interferencia perjudicial y
- 2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su propia operación no deseada.

Korea Notice:

사용자안내문

기 종 별	사 용 자 안 내 문
A 급 기기 (업무용 방송통신기자재)	이 기기는 업무용(A 급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다. 목적으로 합니다.

DECLARATION OF CONFORMITY

WatchGuard Technologies, Inc.
505 Fifth Ave. S., Suite 500
Seattle, WA 98104-3892 USA

WatchGuard Technologies Inc. hereby declares that the product(s) listed below conform to the European Union directives and standards identified in this declaration.

Product(s):

WatchGuard Models: Firebox M200 and Firebox M300
Hardware Model: ML3AE8

EU Directive(s):

Low Voltage (2014/35/EC)
Electromagnetic Compatibility (2014/30/EU)
RoHS(2011/65/EC)
WEEE Directive 2002/96/EC
REACH EC 1907/2006

Standard(s):

Safety: EN60950-1:2006+A11:2009+A1+A12:2011+A2:2013
Emission: EN 55032:2012+AC: 2013 Class A
FCC Part 15 Subpart B Class A
ICES-003: Issue 5:2012 + Update:2014 Class A
CISPR 32: 2015 Class A
VCCI-CISPR 32: 2016/ CISPR 32:2015
AS/NZS CISPR 32:2015 Class A
EN 61000-3-2:2014 Class A
EN 61000-3-3:2013
Immunity: EN 55024: 2010 + A1:2015
EN 61000-4-2:2009
EN 61000-4-3:2006+A1:2008+A2:2010
EN 61000-4-4:2012
EN 61000-4-5:2014
EN 61000-4-6:2014+AC:2015
EN 61000-4-8:2010
EN 61000-4-11:2004

Signature:

Laurence Huang



Full Name: Laurence Huang
Position: Manufacturing Program Manager
Date: 09 Aug 2017

Limited Hardware Warranty

This Limited Hardware Warranty (the “Warranty”) applies to the enclosed hardware product, not including any associated software, which is licensed pursuant to a separate end-user license agreement and warranty (the “Product”). BY USING THE PRODUCT, YOU (either an individual or a single entity) AGREE TO THE TERMS HEREOF. If you do not agree to these terms, please return this package, along with proof of purchase, to the authorized dealer from which you purchased it for a full refund. WatchGuard Technologies, Inc. (“WatchGuard”) and you agree as set forth below or on the reverse side of this card, as applicable.

1. **LIMITED WARRANTY.** WatchGuard warrants that upon delivery and for one (1) year thereafter (the “Warranty Period”): (a) the Product will be free from material defects in materials and workmanship, and (b) the Product, when properly installed and used for its intended purpose and in its intended operating environment, will perform substantially in accordance with WatchGuard applicable specifications.

This warranty does not apply to any Product that has been: (i) altered, repaired or modified by any party other than WatchGuard except for the replacement or inclusion of specified components authorized in, and performed in strict accordance with, documentation provided by WatchGuard; or (ii) damaged or destroyed by force majeure events, accidents, power spikes or similar events or by any intentional, reckless or negligent acts or omissions of any party. You may have additional warranties with respect to the Product from the manufacturers of Product components. However, you agree not to look to WatchGuard for, and hereby release WatchGuard from any liability for, performance of, enforcement of, or damages or other relief on account of, any such warranties or any breach thereof.

2. **REMEDIES.** If any Product does not comply with the WatchGuard warranties set forth in Section 1 above, WatchGuard will, following the receipt of the product you claim is defective and at its option, either (a) repair the Product, or (b) replace the Product with a like or similar product; provided, that you will be responsible for returning the Product and for all costs of shipping and handling. Repair or replacement of the Product shall not extend the Warranty Period. Any Product, component, part or other item replaced by WatchGuard becomes the property of WatchGuard. WatchGuard shall not be responsible for return of or damage to any software, firmware, information or data contained in, stored on, or integrated with any returned Products.
3. **DISCLAIMER AND RELEASE.** THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 1 AND 2 ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF

PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD OR FROM PRODUCT LIABILITY, STRICT LIABILITY OR OTHER THEORY, AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE PRODUCT).

4. **LIMITATION AND LIABILITY.** WATCHGUARD’S LIABILITY (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) WITH REGARD TO ANY PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF ANY AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) FOR COST OF COVER OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF PROFITS, BUSINESS, OR DATA) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF ANY AGREED REMEDY.
5. **MISCELLANEOUS PROVISIONS.** This Warranty will be governed by the laws of the state of Washington, U.S.A., without reference to its choice of law rules. The provisions of the 1980 United Nations Convention on Contracts for the International Sales of Goods, as amended, shall not apply. You agree not to directly or indirectly transfer the Product or use of the product or associated documentation to any country to which such transfer would be prohibited by the U.S. Export laws and regulations. If any provision of this Warranty is found to be invalid or unenforceable, then the remainder shall have full force and effect and the invalid provision shall be modified or partially enforced to the maximum extent permitted by law to effectuate the purpose of this Warranty. This is the entire agreement between WatchGuard and you relating to the Product, and supersedes any prior purchase order, communications, advertising or representations concerning the Product AND BY USING THE PRODUCT YOU AGREE TO THESE TERMS. IF THE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS BY USING THE PRODUCT REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THE WARRANTY ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS WARRANTY; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THE WARRANTY AND PERFORM ITS OBLIGATIONS UNDER THE WARRANTY AND; (C) THE WARRANTY AND THE PERFORMANCE OF THE ENTITY’S OBLIGATIONS UNDER THE WARRANTY DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of the Warranty will be valid unless it is in writing and is signed by WatchGuard.

WATCHGUARD TECHNICAL SUPPORT

1.877.232.3531
(U.S. and Canada)

+1.206.613.0456
(all other countries)

www.watchguard.com/support

ADDRESS: 505 Fifth Avenue South, Suite 500, Seattle, WA 98104

WEB: www.watchguard.com • **U.S. SALES:** 1.800.734.9905 • **INTERNATIONAL SALES:** +1.206.613.0895

© 2017 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Fireware, and LiveSecurity are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners.
P.N. 352-5150-001 Rev C 092817

