Firebox® T40 / T40-W

HW Models: FS4AE5, FS4AE5W

DRAFT

Quick Start Guide

快速开始指南
Guide de démarrage rapide
Kurzanleitung
Guida introduttiva
クィックスタート・ガイド
빠른 설치 안내서
Guía Rápida
Guia de início rápido
快速設定手冊

WatchGuard® Technologies, Inc.

Activate Your Device

1. **Go to www.watchguard.com/activate**
2. Log in to your WatchGuard account, or create a new account*.

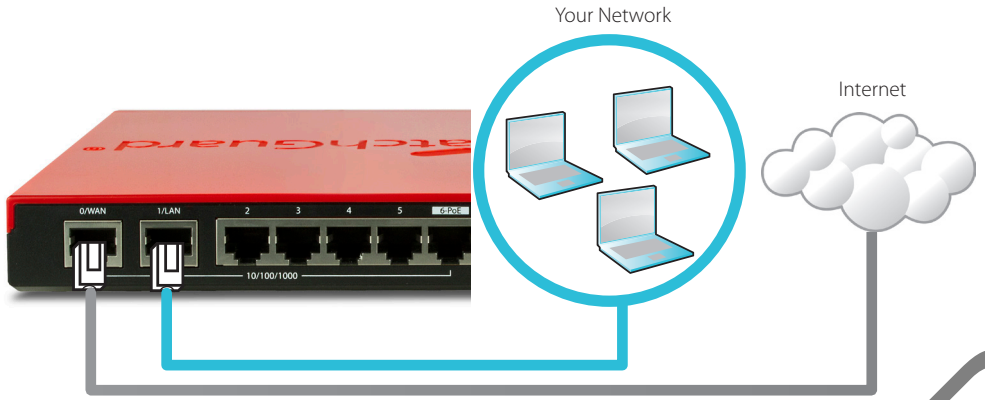
   *If you create a new account, return to www.watchguard.com/activate after you finish the account creation process.
3. Type the serial number for your device.
4. **During activation, select your setup method:**
   - **RapidDeploy QuickStart** – Automatically download and apply a QuickStart configuration 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.

DRAFT

RapidDeploy QuickStart Setup

1. Connect Your Device 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:

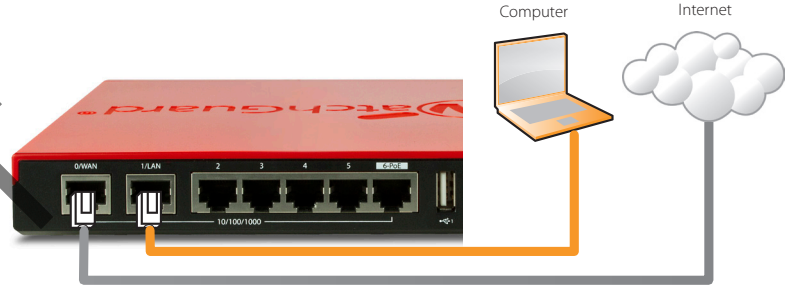
- Allows outbound TCP, UDP, and ping traffic
- Blocks all unrequested traffic from the external network
- Includes optimized security settings
- Uses licensed security services to protect the trusted and optional networks

DRAFT

Classic Activation Setup

1. Connect Your Device 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 TCP, UDP, and ping traffic
- 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:

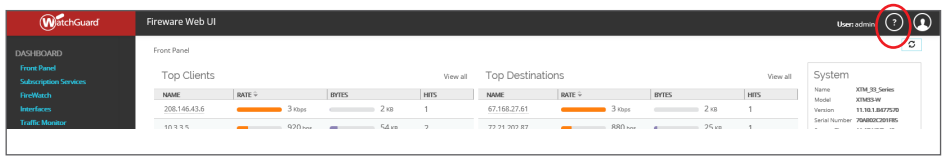
1. Log in to Fireware Web UI.
2. Select **System > Upgrade OS**.

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 the Firebox T35 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

Fail Over – Lights when there is a WAN failover from the primary external interface to the backup interface.

WAP - (Wireless models only) Lights when the device is activated as a wireless access point or as a wireless client.

Network interface status indicators – The Firebox T35 has five network interfaces. There are two status indicators for each interface.

Indicator	Indicator color	Interface Status
1000	Yellow	Link speed: 1000 Mbps
	Blinks*	Data sent and received
10/100	Green	Link speed: 10 Mbps or 100 Mbps
	Blinks*	Data sent and received

* Blink speed increases as the data flow increases

Status – Shows when there is a management connection to the device. The Status indicator is lit for 30 seconds after you connect to the device with the Fireware Web UI or the command line interface. It is also lit when the device is polled by WatchGuard System Manager.

Mode – Shows the status of the external network connection. If the device can connect to the external network and send traffic, the indicator is green. The indicator flashes if the device cannot connect to the external network and send traffic.

Attn – Lights when you start the device with the Reset button pressed.

Power (⏻) – The power indicator is lit when the device is on.

DRAFT

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.

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

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

激活设备

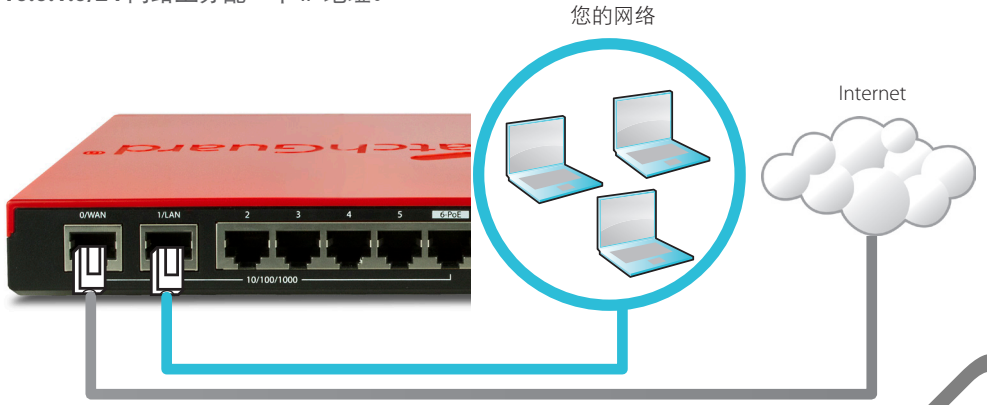
1. **转到 www.watchguard.com/activate**
2. 登录到您的 WatchGuard 帐户，或者创建一个新帐户*。
   *如果创建新帐户，请在完成帐户创建过程之后返回到 www.watchguard.com/activate 。
3. 输入设备的序列号。
4. **在激活期间，选择安装方法：**
   - **快速部署** – 自动下载快速部署配置文件并将其应用到您的设备，其中预配置了 WatchGuard 推荐的安全设置。
   - **常规激活** – 使用网页安装向导为您的设备创建基本配置。
5. 请根据您的实际安装方法选择本手册中对应的安装说明。

DRAFT

快速部署安装向导

1. 将您的设备连接好网线后开启电源

确保网络中的电脑被配置为使用 DHCP方式自动获取IP地址。在启动 Firebox 设备后，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. **在浏览器地址栏输入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. 用您的账户 **admin** 以及在激活过程中设置的账户（readwrite）密码登录。

您的设备有一个基本配置：

- 允许从内网向外发起 TCP、UDP 和 Ping 数据流
- 自动阻止来自外部网络的所有未经允许的数据流
- 包含优化过的安全设置
- 使用许可的安全服务来保护受信任的网络和可选网

常规激活操作

1. 将您的设备连接好网线后开启电源

确保网络中的电脑被配置为使用 DHCP方式自动获取IP地址。连接 Firebox 设备后，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. **在浏览器地址栏输入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. 以管理员账号 **admin** 和管理员配置密码 **readwrite** 登录。

D. 按照网页安装向导中的说明为新设备创建基本配置文件。如果有问题，请单击“*更多信息*”(*More Information*)。

E. 在向导完成后，使用 **admin** 账户和您在向导中设置的账户密码（readwrite）登录到网页管理界面。

F. 在您的网络中安装 Firebox设备。

您的设备有一个基本配置：

- 允许从内网向外发起 TCP、UDP 和 Ping 数据流
- 自动阻止来自外部网络的所有未经允许的数据流

DRAFT

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

后续步骤

恭喜！您已经完成了 Firebox 的基本安装。您可以使用网页管理界面查看和编辑您的配置，并管理和监控您的 Firebox 。或者，您可以下载和安装 WatchGuard 系统管理器（WSM），使用政策管理器和 WSM 管理套件和监控工具。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 设备之后，检查您的用户可以成功浏览网页。

获取最新版本软件

要升Firebox 操作系 ：

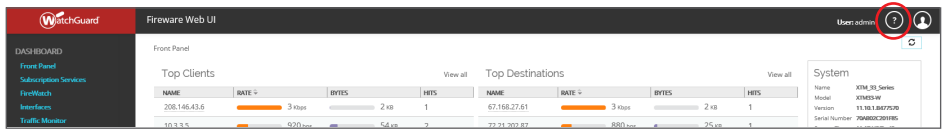
1. 登录 Fireware 网页管理界面。
2. 选择系统 > 升级操作系统。

要获取 Firebox 上最新版本的 WSM、WatchGuard Dimension、VPN 客户端和其他软件：

1. 转到 **www.watchguard.com/support** 并单击下载软件。
2. 找到 Firebox T30/T50 的软件下载页面并选择您想安装的软件。

浏览 Firebox 的特性和功能

浏览网页管理界面或 WatchGuard 系统管理器，点击任意页面或对话框的上的帮助，了解 Firebox 的管理、监控和安全功能。



关于设备状态指示灯

Fail Over故障转移 – 当 WAN 从主要外部接口向备份接口进行故障转移时亮起。

WAP –（仅无线机型）当设备作为无线接入点或无线客户端时亮起。

网络接口状态指示灯 – Firebox T35 有5个网络接口。每个接口有两个状态指示灯。

指示灯	指示灯颜色	接口状态
1000	黄色	链路速度：1000 Mbps
	闪烁*	发送和接收数据
10/100	绿色	链路速度：10 Mbps 或 100 Mbps
	闪烁*	发送和接收数据

*闪烁速度会随着数据流量的增加而加快

Status状态 – 当设备有管理连接时将亮起。在用Fireware网页管理界面或命令行界面连接上设备后，状态指示灯将持续亮30秒。当 WatchGuard System Manager 轮询设备时也会亮起。

Mode模式 – 显示外部网络连接的状态。如果设备可以连接到外部网络并发送数据流，则该指示灯为绿色。如果设备无法连接到外部网络和发送数据流，则该指示灯闪烁。

Attn注意 – 在重启设备时按下“重置”(Reset) 按钮，此灯闪烁。

Power电源 (⏻) – 当设备处于开启状态时，电源指示灯亮。

DRAFT

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，如果您忘记了您的管理员帐户密码或者想用快速部署方式重新安装设备，您可以重置您的设备。

欲了解更多信息，请通过下面的网址浏览Firebox设备的硬件指南（“Hardware Guide”）：

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

DRAFT

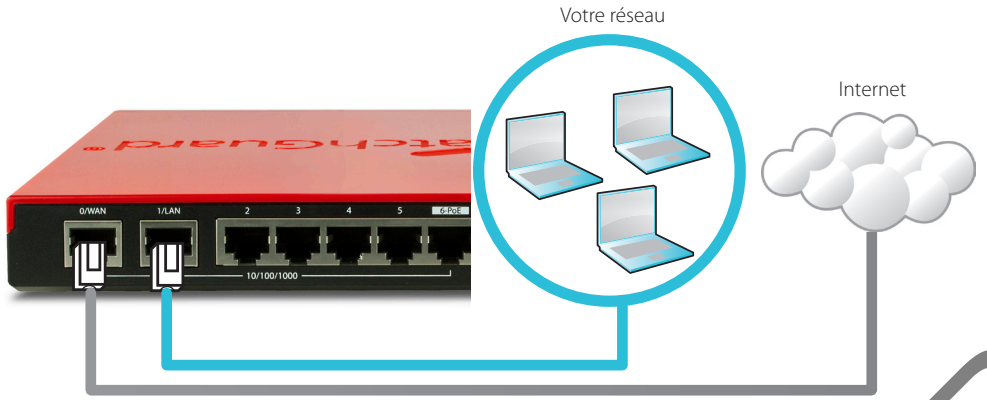
Activation de votre appareil

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 de 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 Firebox, il 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 appareil

Assurez-vous que votre ordinateur est configuré pour utiliser le protocole DHCP. Lorsque vous connectez votre Firebox, il 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 le Firebox dans votre réseau.

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

DRAFT

Étapes suivantes

Félicitations ! Vous avez à présent terminé la configuration de base de votre Firebox. Vous pouvez utiliser l'interface utilisateur Web pour consulter et modifier votre configuration, mais aussi pour gérer et contrôler votre Firebox. 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 débuter :

Vérifiez votre connectivité Internet

- Une fois votre Firebox installé dans 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 du 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 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 le Firebox T30/T50 et sélectionnez le logiciel à installer.

Examen des fonctions de votre 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 Firebox.

DRAFT

À propos des témoins d'état de l'appareil

Fail Over (**Basculement**) : s'allume en cas de basculement WAN depuis l'interface externe principale vers l'interface de secours.

WAP (modèles sans fil uniquement) : s'allume lorsque l'appareil est activé en tant que point d'accès sans fil ou en tant que client sans fil.

Indicateurs d'état des interfaces réseau : le Firebox T35 possède cinq interfaces réseau. Chaque interface comporte deux indicateurs d'état.

Indicateur	Couleur de l'indicateur	État de l'interface
1 000	Jaune	Vitesse des liens : 1 000 Mbps
	Clignote*	Données envoyées et reçues
10/100	Vert	Vitesse des liens : 10 Mbps ou 100 Mbps
	Clignote*	Données envoyées et reçues

* La vitesse de clignotement augmente avec le débit du flux de données

Status (**État**) : indique qu'il y a une connexion de gestion avec l'appareil. L'indicateur d'état s'allume pendant 30 secondes après avoir connecté l'appareil à l'interface utilisateur Web de Fireware ou à l'interface de ligne de commande. Il s'allume également lorsque l'appareil est sondé par WatchGuard System Manager.

Mode : indique l'état de la connexion du réseau externe. Si l'appareil peut se connecter au réseau externe et envoyer du trafic, cet indicateur est vert. Si l'appareil ne peut pas se connecter au réseau externe et envoyer du trafic, cet indicateur clignote.

Attn : s'allume lorsque vous démarrez l'appareil tout en maintenant le bouton Reset (Réinitialiser) enfoncé.

Power (**Alimentation**) (⏻) : l'indicateur d'alimentation s'allume lorsque l'appareil est sous tension.

Rétablissement des paramètres d'usine du Firebox

En cas de besoin, vous pouvez réinitialiser votre 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 Firebox, disponible à l'adresse suivante :

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

DRAFT

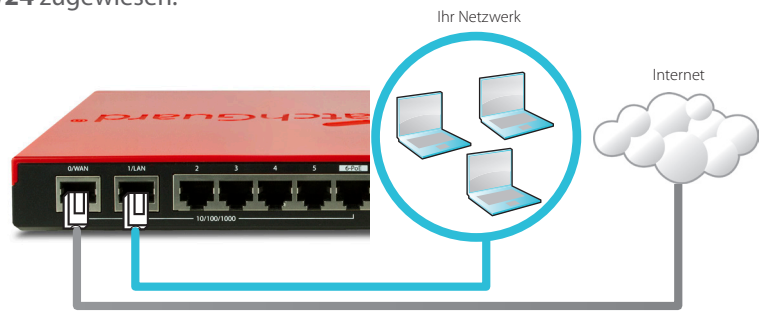
Gerät aktivieren

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. Gerät 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. Etwaig 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. Gerät 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 für ausgehenden TCP-, UDP- und Ping-Datenverkehr
- 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

DRAFT

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 Fireware Web UI 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 die Firebox T30/T50, und wählen Sie die zu installierende Software aus.

Merkmale und Funktionen der Firebox erkunden

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.

DRAFT

Informationen zu den Statusanzeigen des Geräts

Fail Over – Diese Anzeige leuchtet bei WAN-Failover zwischen der primären externen Schnittstelle und der Backup-Schnittstelle.

WAP (nur bei Drahtlosmodellen) – Diese Anzeige leuchtet, wenn das Gerät als Wireless Access Point oder als drahtloser Client aktiviert wurde.

Statusanzeigen der Netzwerkschnittstellen – Die Firebox T35 verfügt über fünf Netzwerkschnittstellen. Für jede Schnittstelle gibt es zwei Statusanzeigen.

Anzeige	Farbsignal	Schnittstellenstatus
1000	Gelb	Verbindungsgeschwindigkeit: 1000 MBit/s
	Blinkt*	Daten werden gesendet und empfangen
10/100	Grün	Verbindungsgeschwindigkeit: 10 MBit/s oder 100 MBit/s
	Blinkt*	Daten werden gesendet und empfangen

* Bei zunehmendem Datenverkehr erhöht sich die Blinkfrequenz

Status – Zeigt an, ob eine Verwaltungsverbindung zum Gerät besteht. Die Statusanzeige leuchtet 30 Sekunden lang, nachdem Sie über das Fireware-Web-Interface oder das Kommandozeileninterface die Verbindung zum Gerät hergestellt haben. Sie leuchtet außerdem, wenn das Gerät vom WatchGuard System Manager abgefragt wird.

Mode – Zeigt den Status der externen Netzwerkverbindung an. Die Anzeige leuchtet grün, wenn das Gerät eine Verbindung zum externen Netzwerk herstellen und Datenverkehr senden kann. Die Anzeige blinkt, wenn das Gerät keine Verbindung zum externen Netzwerk herstellen und keinen Datenverkehr senden kann.

Attn – Diese Anzeige leuchtet, wenn Sie das Gerät mit gedrückter Reset-Taste starten.

Ein/Aus (⏻) – Diese Anzeige leuchtet, 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 del dispositivo

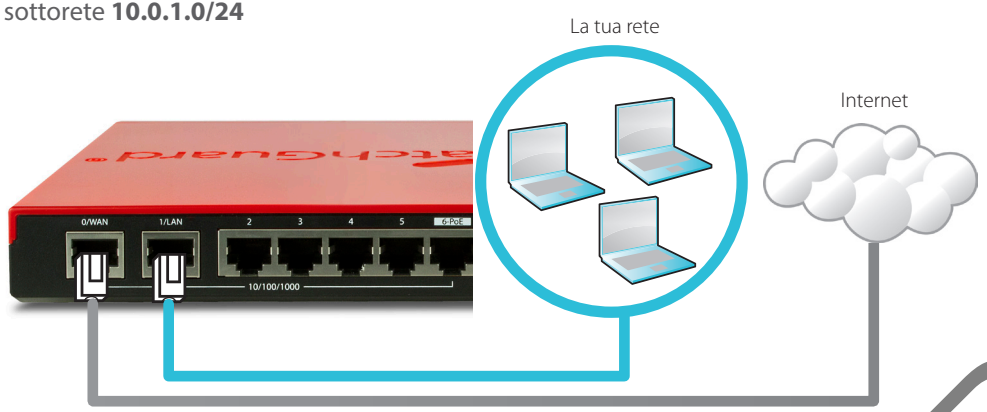
1. **Vai su www.watchguard.com/activate**
2. Accedi al tuo account WatchGuard, oppure creane uno nuovo*.
   *Se crei un nuovo account, ritorna a www.watchguard.com/activate dopo aver terminato la procedura di creazione dell'account.
3. Digita il numero di serie del tuo dispositivo.
4. **Durante l'attivazione, 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.

DRAFT

Impostazione di RapidDeploy QuickStart

1. Collegamento e accensione del dispositivo

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**



2. Collegamento 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.

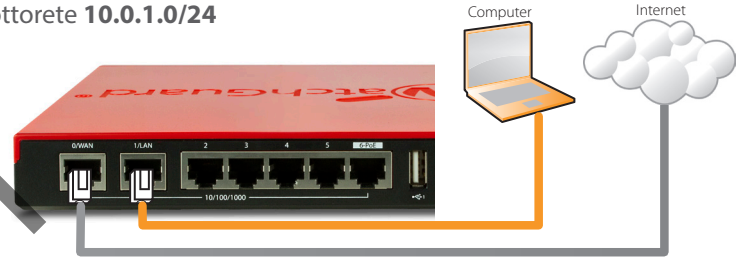
Il dispositivo contiene una configurazione di base:

- 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

1. Collegamento e accensione del dispositivo

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**



2. Collegamento 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 il traffico TCP e UDP in uscita, e il ping
- 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

DRAFT

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:

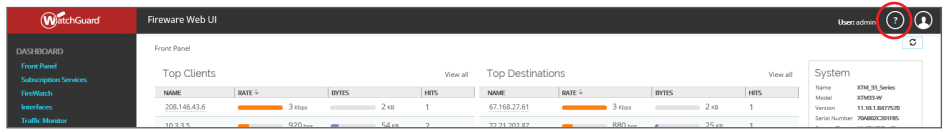
1. Accedi all'interfaccia utente Web Fireware.
2. Seleziona **System > Upgrade OS**.

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 T30/T50 e seleziona il software che desideri installare.

Esplorazione delle caratteristiche e delle funzionalità di 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.



DRAFT

Informazioni sulle spie di stato del dispositivo

Fail Over – Si accende in caso di failover WAN dall'interfaccia esterna primaria all'interfaccia di backup.

WAP – (Solo nei modelli wireless) Si accende quando il dispositivo viene attivato come un punto di accesso wireless o un come un client wireless.

Indicatori di stato della scheda di rete – Firebox T35 ha cinque interfacce di rete. Per ogni scheda sono disponibili due indicatori di stato.

Indicatore	Colore dell'indicatore	Stato dell'interfaccia
1000	Giallo	Velocità collegamento: 1000 Mbps
	Lampeggi*	Dati inviati e ricevuti
10/100	Verde	Velocità collegamento: 10 Mbps o 100 Mbps
	Lampeggi*	Dati inviati e ricevuti

* La velocità di lampeggio aumenta insieme all'incremento del flusso di dati

Stato – Si accende quando viene stabilita una connessione per la gestione del dispositivo. L'indicatore di stato si accende per 30 secondi una volta collegatisi al dispositivo mediante l'interfaccia utente basata sul web di Fireware o l'interfaccia a riga di comando. Si accende anche quando il dispositivo viene sondato da WatchGuard System Manager.

Modo – Mostra lo stato della connessione alla rete esterna. Se il dispositivo può collegarsi alla rete esterna e inviare traffico, l'indicatore è verde. Se il dispositivo non può collegarsi alla rete esterna e inviare traffico, l'indicatore lampeggia.

Attn – Si accende quando il dispositivo viene avviato premendo il pulsante Reset.

Alimentazione (⏻) – L'indicatore dell'alimentazione si accende quando il dispositivo viene 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

DRAFT

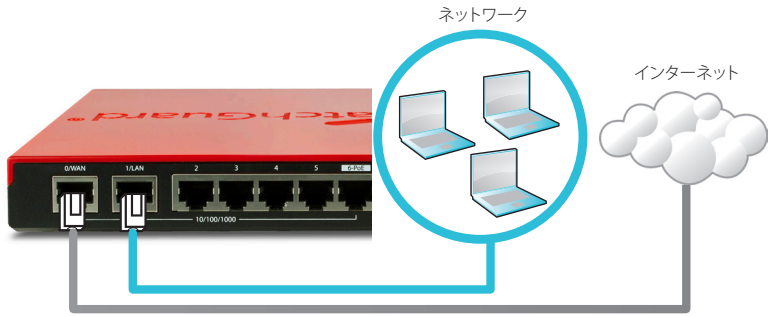
デバイスのアクティベーションを行う

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

A. **https://10.0.1.1:8080にアクセスします。**

B. 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。

C. 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**と管理用パスフレーズ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

A. **https://10.0.1.1:8080にアクセスします。**

B. 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。

C. ユーザー名**admin**とパスフレーズ**readwrite**でログインします。

D. 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。

E. 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**と管理用パスフレーズreadwriteでウェブUIにログインします。

F. 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
- 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

DRAFT

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 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。

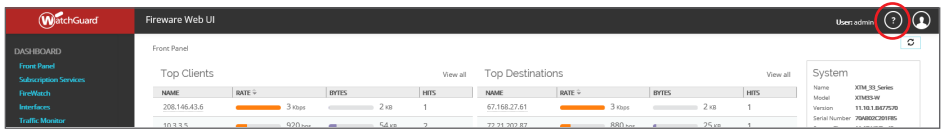
1. Fireware Web UI にログインします。
2. **System > Upgrade OS** を選択します。

Firebox 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. Firebox T30/T50 向けのソフトウェア・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

Firebox の管理、監視、およびセキュリティの機能の詳細については、ウェブ UI または WatchGuard System Manager で確認できます。それぞれのページやダイアログ・ボックスで **[Help]** をクリックしてください。



デバイスのステータス・ライトについて

Fail Over – プライマリ外部インターフェイスからバックアップ・インターフェイスへのWANフェイルオーバーの発生時に点灯します。

WAP - （無線モデルのみ）デバイスを無線アクセス・ポイントまたは無線クライアントとしてアクティベートした場合に点灯します。

ネットワーク・インターフェイスのステータス・インジケータ – Firebox T35には5つのネットワーク・インターフェイスがあります。それらのインターフェイスのそれぞれに2種類のステータス・インジケータがあります。

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
1000	黄色	リンク速度: 1000 Mbps
	点滅*	データを送受信
10/100	緑色	リンク速度: 10 Mbpsまたは 100 Mbps
	点滅*	データを送受信

* データの量が多いほど高速に点滅します

Status – デバイスへの管理接続のステータスを示します。このインジケータは、Fireware Web UIまたはコマンドライン・インターフェイスでデバイスに接続したときに、30秒間点灯します。また、WatchGuard System Managerによるデバイスのポーリング時にも点灯します。

Mode – 外部ネットワーク接続のステータスを示します。外部ネットワークに接続してトラフィックを送信できる場合、このインジケータは緑色になります。外部ネットワークに接続してトラフィックを送信することができない場合は点滅します。

Attn – デバイスの起動時にリセット・ボタンを押すと点灯します。

Power (⏻) – デバイスの電源が入っているときに点灯します。

DRAFT

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フレーズを忘れた場合や、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

DRAFT

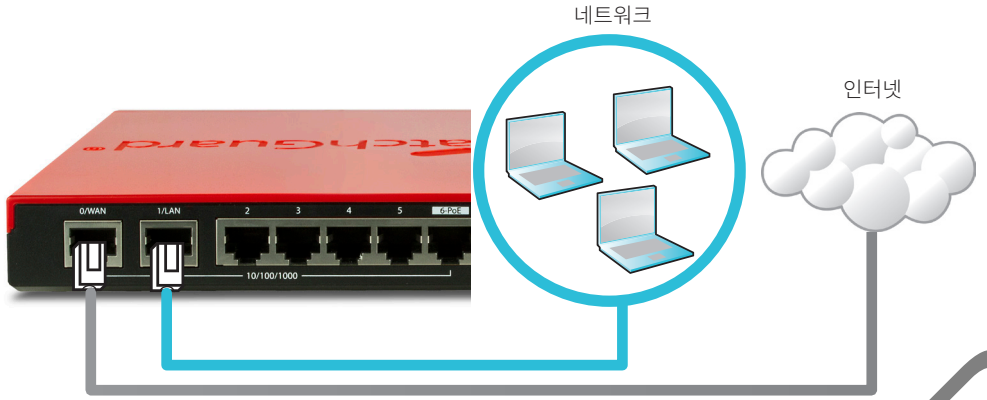
장치 활성화

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

A. **https://10.0.1.1:8080으로 이동합니다.**

B. 장치에서 자체 서명된 인증서를 사용하기 때문에 인증서 경고는 안심하고 무시하시면 됩니다.

C. 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

A. **https://10.0.1.1:8080으로 이동합니다.**

B. 장치에서 자체 서명된 인증서를 사용하기 때문에 인증서 경고는 안심하고 무시하시면 됩니다.

C. 사용자 이름 **admin**과 암호 **readwrite**를 사용하여 로그인합니다.

D. Web Setup Wizard의 지침을 따라 새 장치에 대한 기본 구성 파일을 만듭니다. 질문이 있을 경우 *More Information*을 클릭합니다.

E. 마법사가 완료되면 사용자 계정 **admin**과 마법사를 진행하는 도중 설정한 Admin 암호(readwrite)를 사용하여 Web UI에 로그인합니다.

F. 네트워크에 Firebox를 설치합니다.

장치가 기본적으로 다음과 같이 구성됩니다.

- 아웃바운드 TCP, UDP 및 Ping 트래픽 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.

DRAFT

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 OS를 선택합니다.

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

1. **www.watchguard.com/support**로 이동하고 **Download Software**를 클릭합니다.
2. Firebox T30/T50 의 소프트웨어 다운로드 페이지를 찾아 설치하고자 하는 소프트웨어를 선택합니다.

Firebox의 특징 및 기능 살펴보기

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

장치 상태 표시등 정보

Fail Over – 기본 외부 인터페이스에서 백업 인터페이스로의 WAN 페일오버가 발생할 경우 켜집니다.

WAP - (무선 모델 전용) 장치가 무선 액세스 포인트 또는 무선 클라이언트로 활성화된 경우에 켜집니다.

네트워크 인터페이스 상태 표시등 – Firebox T35에는 다섯 가지 네트워크 인터페이스가 있습니다. 각 인터페이스마다 상태 표시등이 두 개씩 있습니다.

표시등	표시등 색상	인터페이스 상태
1000	노란색	링크 속도: 1000Mbps
	깜박임*	데이터 송수신
10/100	녹색	링크 속도: 10Mbps 또는 100Mbps
	깜박임*	데이터 송수신

* 데이터 흐름 속도가 빨라질수록 깜박임 속도도 빨라집니다.

Status – 장치에 대한 관리 연결이 있음을 표시합니다. 이 상태 표시등은 사용자가 Fireware Web UI 또는 명령줄 인터페이스를 사용하여 장치에 연결한 후 30초간 켜집니다. WatchGuard System Manager에서 장치를 폴링한 경우에도 켜집니다.

Mode – 외부 네트워크 연결 상태를 표시합니다. 장치가 외부 네트워크에 연결하여 트래픽을 송신할 수 있을 경우 표시등은 녹색으로 켜집니다. 장치가 외부 네트워크에 연결하여 트래픽을 송신할 수 없을 경우에는 표시등이 깜박입니다.

Attn – Reset 버튼을 누른 상태로 장치를 시작할 때 켜집니다.

Power (⏻) – 장치가 켜지면 전원 표시등이 켜집니다.

DRAFT

Firebox를 공장 초기 설정으로 리셋

필요할 경우 Firebox를 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 Firebox용 하드웨어 가이드를 참조하십시오. 이 가이드는 다음에서 확인할 수 있습니다.

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

Active su dispositivo

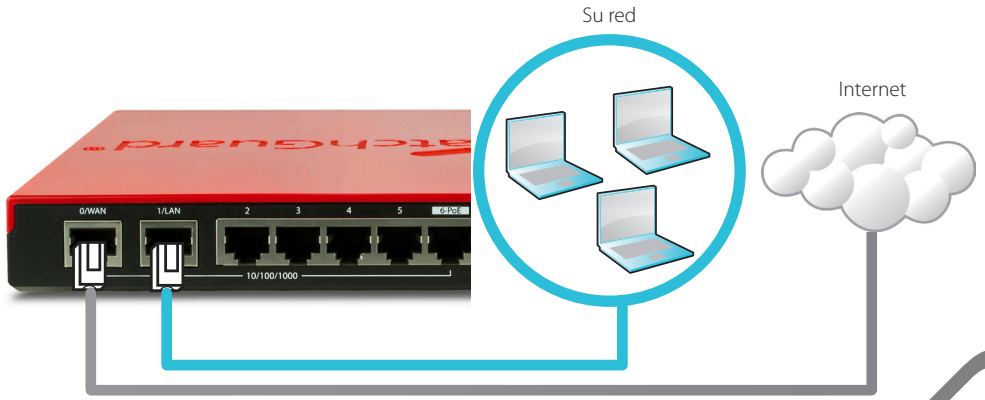
1. **Visite www.watchguard.com/activate**
2. Inicie sesión con su cuenta de WatchGuard o cree una cuenta nueva*.
   *Si usted crea una cuenta nueva, regrese a www.watchguard.com/activate luego de finalizar el proceso de creación de la cuenta.
3. Ingrese el número de serie de su dispositivo.
4. **Durante 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.

DRAFT

Instalación del inicio rápido RapidDeploy

1. Conecte su dispositivo y enciéndalo

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 confiablesy opcionales.

Instalación de activación clásica

1. Conecte su dispositivo y enciéndalo

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 tráfico ping, UDP y TCP saliente
- 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 confiablesy opcionales.

DRAFT

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 otro software para su Firebox:

1. Visite **www.watchguard.com/support** y haga clic en **Download Software (Descargas de software)**.
2. Encuentre la página de descargas de software para el Firebox T30/T50 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.

DRAFT

Acerca de las luces de estado del dispositivo

Conmutación por error: las luces se encienden cuando hay una conmutación por error de WAN de la interfaz externa principal a la interfaz de copia de seguridad.

WAP: (únicamente en modelos inalámbricos) las luces se encienden cuando el dispositivo está activado como punto de acceso inalámbrico o como cliente inalámbrico.

Indicadores de estado de la interfaz de la red: el Firebox T35 tiene cinco interfaces de red. Hay dos indicadores de estado para cada interfaz.

Indicador	Color del indicador	Estado de interfaz
1000	Amarillo	Velocidad de vínculo: 1000 Mbps
	Las luces parpadean*	Datos enviados y recibidos
10/100	Verde	Velocidad de vínculo: 10 Mbps o 100 Mbps
	Las luces parpadean*	Datos enviados y recibidos

* La velocidad de parpadeo de las luces aumenta a medida que el flujo de datos aumenta

Estado: muestra cuando hay una conexión de administración al dispositivo. El indicador de estado está iluminado durante 30 segundos después de que usted se conecta al dispositivo con la interfaz de usuario web de Fireware o con la interfaz de línea de comandos. También está iluminado cuando WatchGuard System Manager realiza un sondeo en el dispositivo.

Modo: muestra el estado de la conexión de red externa. Si el dispositivo se puede conectar a la red externa y enviar tráfico, el indicador se muestra de color verde. El indicador se enciende y apaga de forma intermitente si el dispositivo no se puede conectar a la red externa y enviar tráfico.

Attn: las luces se encienden cuando enciende el dispositivo con el botón para reiniciar apretado.

Encendido (⏻): el indicador de encendido está iluminado 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

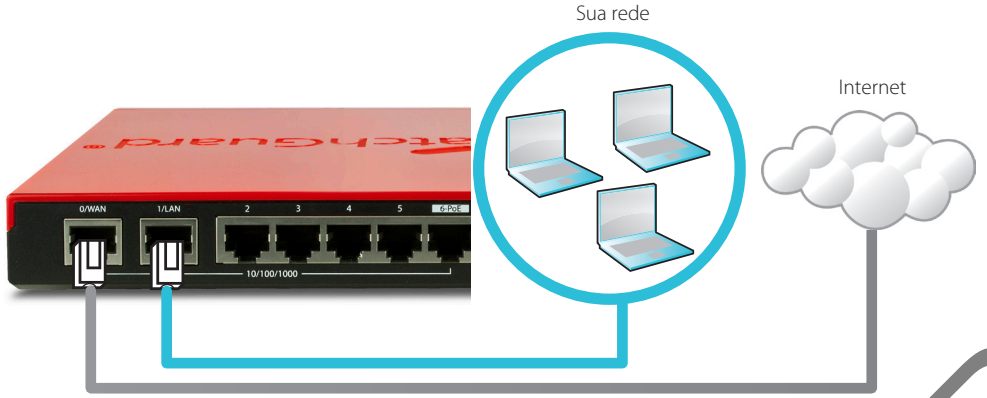
1. **Acesse www.watchguard.com/activate**
2. Faça login na conta WatchGuard ou crie uma conta nova*.
   *Se for criar uma conta nova, volte a www.watchguard.com/activate depois de concluído o processo de criação de conta.
3. Insira o número de série do dispositivo.
4. **Durante a ativação, selecione 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.

DRAFT

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 TCP, UDP e tráfego de ping de saída
- Bloqueia todo tráfego não solicitado da rede externa
- Inspeciona o tráfego de saída de FTP, HTTP e HTTPS
- Usa serviços de segurança licenciados para proteger as redes opcionais e confiáveis

DRAFT

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 softwares para o Firebox:

1. Acesse **www.watchguard.com/support** e clique em **Download Software (Baixar software)**.
2. Localize a página de downloads de software do Firebox T30/T50 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.

DRAFT

Sobre as luzes de estado do dispositivo

Fail Over – acende quando existe um failover de WAN a partir da interface externa principal para a interface de backup.

WAP – (somente modelos sem fio) acende quando o dispositivo é ativado como um ponto de acesso sem fio ou um cliente sem fio.

Indicadores de estado da interface de rede – o Firebox T35 tem cinco interfaces de rede. Existem dois indicadores de status de cada interface.

Indicador	Cor do indicador	Estado da interface
1.000	Amarelo	Velocidade do link: 1.000 Mbps
	Intermitente*	Dados enviados e recebidos
10/100	Verde	Velocidade do link: 10 Mbps ou 100 Mbps
	Intermitente*	Dados enviados e recebidos

* A velocidade da intermitência aumenta proporcionalmente ao aumento do fluxo de dados

Status – indica que existe uma conexão de gerenciamento com o dispositivo. O indicador Status acende por 30 segundos depois de conectar ao dispositivo pela interface de usuário da web do Fireware ou pela interface de linha de comando. Ela também acende quando o dispositivo é sondado pelo WatchGuard System Manager.

Mode – indica o status da conexão de rede externa. Se o dispositivo puder se conectar com a rede externa e enviar tráfego, a luz ficará verde. O indicador piscará se o dispositivo não puder se conectar com a rede externa e enviar tráfego.

Attn – acende ao iniciar o dispositivo com o botão Reset pressionado.

Power (⏻) – o indicador de alimentação acende 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

DRAFT

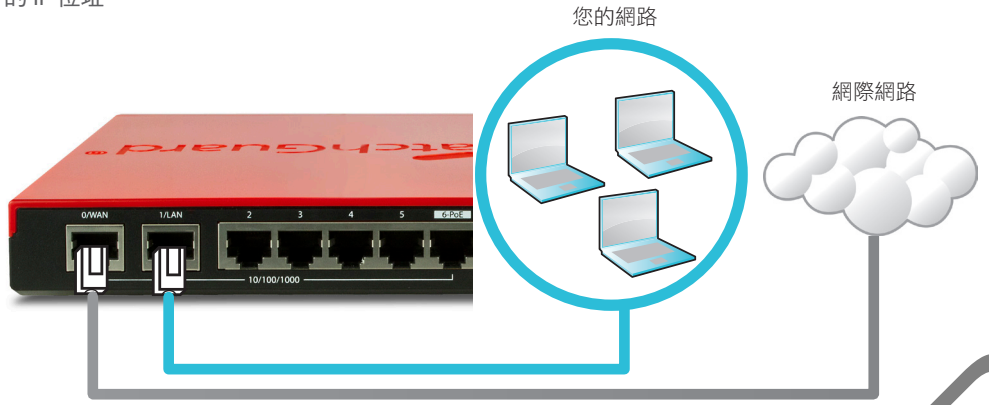
啟動您的裝置

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

A. **請前往 https://10.0.1.1:8080**

B. 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。

C. 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 量

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

A. **請前往 https://10.0.1.1:8080**

B. 您可以安全地忽略憑證警告，因為裝置使用自我簽署憑證。

C. 請利用使用者名稱 **admin** 與通行詞組 **readwrite** 登入。

D. 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*)。

E. 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。

F. 在您的網路中安裝 Firebox。

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

DRAFT

- 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 量

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：

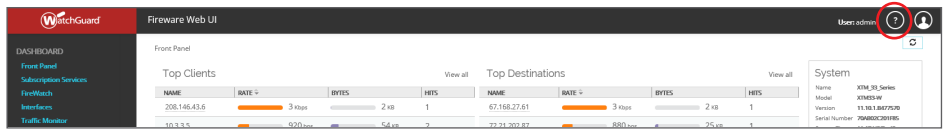
1. 登入 Fireware Web UI。
2. 選取 **[System] (系統) > [Upgrade OS] (升級 OS)**。

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

1. 移至 **www.watchguard.com/support** 並按一下 **[Download Software] (下載軟體)**。
2. 尋找 Firebox T30/T50 的軟體下載頁面，並選取您要安裝的軟體。

探索 Firebox 的功能與作用

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

容錯移轉 (Fail Over) – 當有從主要外部介面到備份介面的 WAN 容錯移轉時，此燈號會亮起。

WAP - (僅無線模式) 當裝置啟動為無線基地台或啟動為無線用戶端時，此燈號會亮起。

網路介面狀態指示燈 – Firebox T35 有五個網路介面。每個介面有兩個狀態指示燈。

指示燈	指示燈色彩	介面狀態
1000	黃色	連結速度：1000 Mbps
	閃爍*	資料傳送與接收
10/100	綠色	連結速度：10 Mbps 或 100 Mbps
	閃爍*	資料傳送與接收

* 當資料流量增加時，閃爍速度會變快

狀態 (Status) – 顯示連到裝置的管理連線。當您使用 Fireware Web UI 或命令列介面連線到裝置時，Status (狀態) 指示燈會亮起 30 秒。當裝置由 WatchGuard System Manager (WatchGuard 系統管理員) 輪詢時，它也會亮起。

模式 (Mode) – 顯示外部網路連線的狀態。若裝置可以連線到外部網路並傳送流量，此指示燈是綠色的。若裝置無法連線到外部網路並傳送流量，此指示燈會閃爍。

注意 (Attn) – 當您按下 [重設] 按鈕啟動裝置時會亮起。

電源 (Power) （⏻）– 當裝置電源開啟時，電源指示燈會亮起。

DRAFT

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

DRAFT

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 C22.2 No.60950-1-07, Second Edition 2014-10
- UL 60950-1, Second Edition 2014-10-14
- IEC 60950-1, 2005+A1:2009+A2:2013
- 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.
- You must disconnect the AC power cord from the Firebox before you remove the cover of the Firebox for any reason.
- There is risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the manufacturer's instructions.

Disclaimer

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

DRAFT

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 C22.2 No.60950-1-07, Second edition 2014-14
- UL 60950-1, Second Edition 2014-10-14
- IEC 60950-1:2005+A1:2009+A2:2013
- 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 Schlitze 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 C22.2 No.60950-1-07, Second edition 2014-14
- UL 60950-1, Second Edition 2014-10-14
- IEC 60950-1:2005+A1:2009+A2:2013
- 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).

DRAFT

Federal Communication Commission Interference Statement

Operations in the 5.15-5.25GHz band are restricted to indoor usage only. This equipment has been tested and found to comply with the limits for a Class B 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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement: (Wireless)

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Europe – EU Declaration of Conformity (Wireless)

This device complies with the essential requirements of the RED 2014/53/EU. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the RED 2014/53/EU:

EN 60950-1 - Safety of Information Technology Equipment

EN 50385 - Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)

EN 300 328 - Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the RED Directive

EN 301 893 - Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the RED Directive

EN 301 489-1 - Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 - Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2.4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 5GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

AT	BE	BG	CZ	DK
EE	FR	DE	IS	IE
IT	EL	ES	CY	LV
LI	LT	LU	HU	MT
NL	NO	PL	PT	RO
SI	SK	TR	FI	SE
CH	UK	HR		

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 R0HS 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

DRAFT

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-247 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(B)/NMB-3(B)

Ce dispositif est conforme à la norme CNR-247 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.

Warning:

This device is not to be mounted or installed on ceilings.

Attention:

Cet appareil ne doit pas être monté ou installé au plafond.

DRAFT

Caution: (Wireless)

The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

Avertissement:

Les dispositifs fonctionnant dans la bande 5150-5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

For Mobile Device Usage (Wireless)

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20cm de distance entre la source de rayonnement et votre corps.

France (Wireless)

Les dispositifs fonctionnant dans la bande 5150-5250 MHz est réservé à une utilisation en intérieur pour réduire le risque de brouillage préjudiciable aux systèmes mobiles par satellite utilisant les mêmes canaux;

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。

VCCI-A

Taiwan Class A Notice:

警告使用者：這是甲類產品，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。

警示 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

設備名稱： 網路伺服器 Equipment name　　型號（型式）：MS3AE5,MS3AE5W,MS5AE5,MS5AE5W Type designation (Type)

單元Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
電路板總成 PCBA	○	○	○	○	○	○
電源供應器 Power Supply	○	○	○	○	○	○
金屬機構件 ME metal part	○	○	○	○	○	○
塑膠機構件 ME plastic part	○	○	○	○	○	○
配件(例: 電源線等) Accessory (cable, etc.)	○	○	○	○	○	○

備考1.〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note 1："Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2.〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note 2："○" indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3.〝—〞係指該項限用物質為排除項目。

Note 3：The "–" indicates that the restricted substance corresponds to the exemption.

DRAFT

Taiwan NCC

低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

電磁波曝露量MPE標準值(MPE) 1mW/cm2，送測產品實值為0.338 mW/cm2

無線資訊傳輸設備避免影響附近雷達系統之操作

Mexico Notice:

La operación de este equipo está sujeta a las siguientes dos condiciones:
(i) es posible que este equipo o dispositivo no cause interferencia perjudicial y
(ii) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

Declaration of Conformity

WatchGuard Technologies, Inc.
505 Fifth Ave. S., Suite 500
Seattle, WA 98104 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 Model: Firebox T35-W and Firebox T35, Hardware Model: MS3AE5W and MS3AE5

EU Directive(s):

Low Voltage (2006/95/EC)
Electromagnetic Compatibility (2004/108/EC)
RoHS (2002/95/EC)
WEEE Directive 2002/96/EC
REACH EC 1907/2006
The Radio Equipment Directive (2014/53/EU)

Common Standard(s):

EN 60950-1:2006+A11+A1+A12	Safety for ITE
EN55032:2012/AC:2013	Class A Emissions for ITE
EN 55024:2010	Immunity for ITE
EN 50385:2002	
EN 61000-3-2:2014	Class A
EN 61000-3-3:2013	
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	
EN 61000-4-11:2004	

Wireless Standard(s):

EN 301 489-1 v2.1.1	EMC and Radio Spectrum Matters
EN 301 489-17 v3.1.1	EMC and Radio Spectrum Matters
EN 300 328 v2.1.1	Radio Spectrum Matters
EN 301 893 v2.2.1	Broadband Radio Access Networks

This device complies with Directive 2014/53/EU issued by the Commission of the European Community.

Manufacturer / Hersteller:	WatchGuard Technologies 505 5th Ave S. Suite 500, Seattle, WA 98104 USA
Radio Equipment / Funkanlage:	Wireless Access Point
Type Designation / Typenbezeichnung:	Firebox T35-W and Firebox T35
Specifications / Technische Daten:	802.11a,b,g,n,ac (2.4Ghz & 5GHz)
Intended Purpose / Verwendungszweck:	Indoor Access Point
Equipment Class / Betriebsmittel der Klasse:	Class II

The above device complies with the essential requirements and other relevant provisions to Directive 2014/53/EU when used for its intended purpose. This equipment may be operated in the USA, Canada, & Europe Union.

Warning! This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

The frequency and maximum transmitted power limit in EU are listed as belows,
2412 - 2472 MHz: 20 dBm
5150 - 5350 MHz: 20 dBm

Restrictions: France les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux

Warnung! Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen. In diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen

Einschränkungen: Frankreich –Geräte, die im Band 5150-5250 MHz ist nur für den Innenbereich, um das Risiko von Störungen des mobilen Satelliten-Systeme, die die gleichen Kanäle

Laurence Huang

Signature
Full Name: Laurence Huang
Position: Manufacturing Program Manager

Date: July 21, 2017

DRAFT

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.

DRAFT

DRAFT

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-T350-001_082617 Rev A