

# EDF-G1002 クイック設定ガイド

本ガイドは、EDF-G1002 の初期接続を迅速に行い、IPS（産業用侵入防御システム）機能を正しく有効化することで、機器をネットワーク攻撃から保護するための手順を分かりやすくご案内します。

## Step 1: ハードウェア接続とログイン

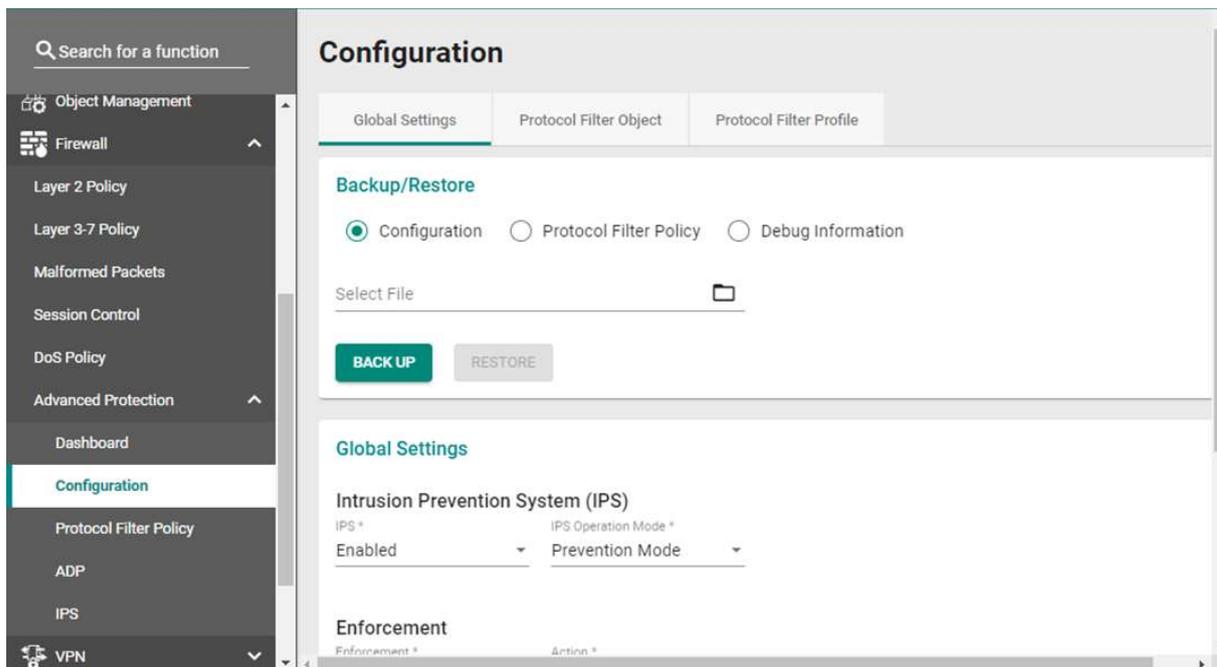
設定を開始する前に、接続が正しいことを確認してください：

1. **接続：** PC を EDF-G1002 の LAN ポートに接続します。
2. **PC の IP アドレス設定：** PC の IP アドレスが機器と同じネットワーク（例：192.168.127.100）になっていることを確認してください。
3. **Web ブラウザを開き、アドレス欄に初期 IP アドレス「192.168.127.254」を入力します。**
  - **初期ユーザー名：** admin
  - **初期パスワード：** moxa

## Step 2: IPS 機能の有効化とライセンス確認

ログイン後：

1. 左側メニューの [Firewall] → [Advanced Protection] → [Global Setting] をクリックして設定画面に進みます。
2. IPS 機能を [Enable (有効)] に切り替えます。



3. 同じ画面内の [Dashboard] セクションで「Expiration Date (有効期限)」が有効期間内であることを確認します。

**⚠ 重要備註:**

IPS のライセンスが期限切れになった場合でも、IPS 機能は（最後に更新されたシグネチャに基づき）引き続き動作し、ネットワークの遮断や防御機能の消失は発生しません。ただし、最新のシグネチャをダウンロードできなくなるため、常に最新の脅威に対応するには定期的なライセンス更新をおすすめします。

💡 画面イメージは別途ご参照ください

## Step 3: 防御モードの選択（重要）

IPS ページでは「Prevention (防御)」と「Detection (検知)」の2つのモードを選択できます。それぞれの違いは以下の通りです。

### A. Detection Mode (検知モード)

- **動作:** 攻撃を検知すると、ログに記録し警告を出しますが、通信自体は遮断しません。
- **メリット:** 生産ラインの通信に影響を与えないため、安定稼働を確保できます。
- **推奨:** 導入初期や、正常な通信が誤検知される可能性がある場合は、まずこのモードで1~2週間様子を見てください。

## B. Prevention Mode (防御モード)

- **動作:** 悪意のあるパケットを検出すると、即座に通信を遮断（ブロック）します。
- **メリット:** ウイルスや攻撃の侵入を未然に防ぎ、最高レベルのセキュリティを実現します。
- **推奨:** 運用環境の通信が正常であることを確認したら、このモードに切り替えて自動的な防御を行ってください。

以上