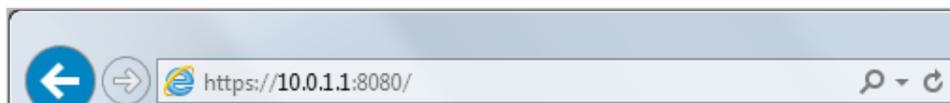


第四章 Web Setup Wizard

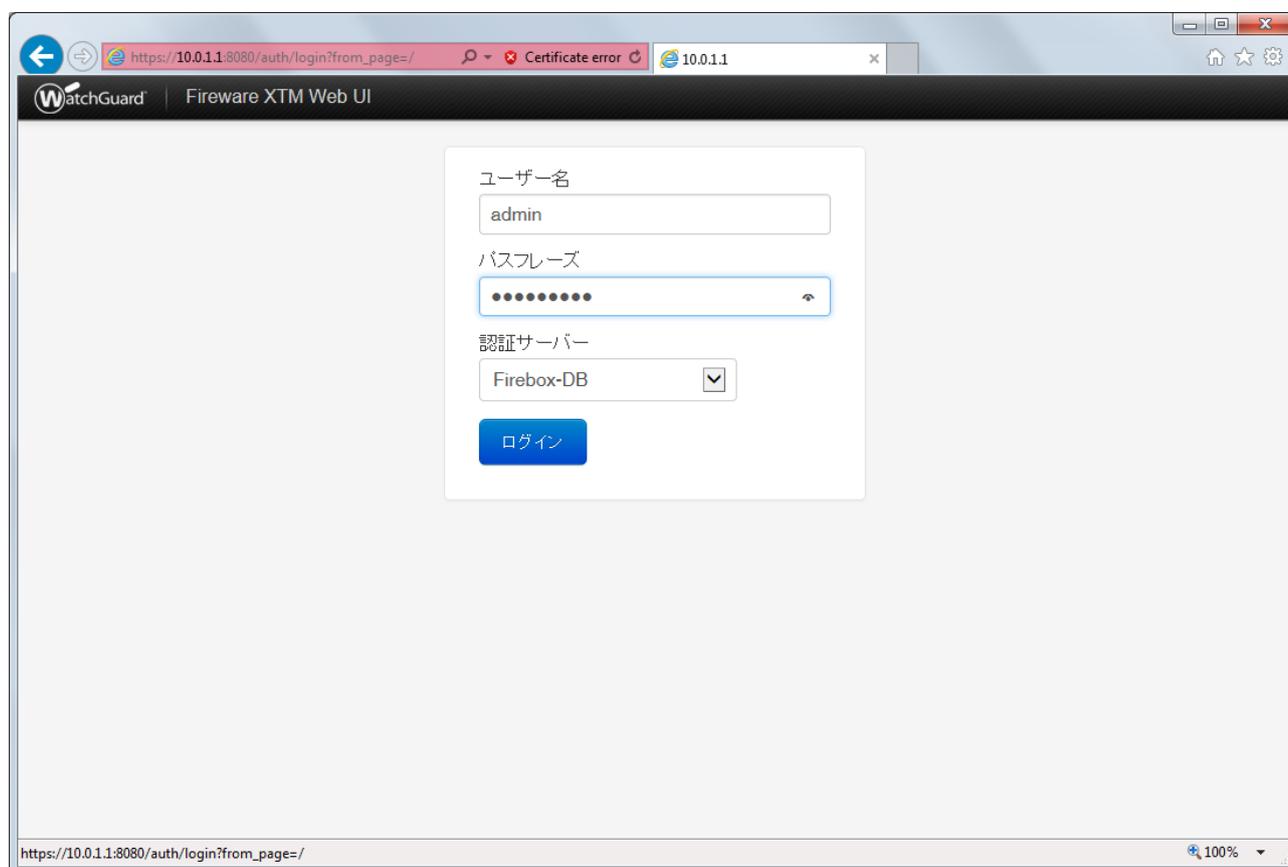
この章では、Web ブラウザだけで初期セットアップを行なえる、Web Setup Wizard の手順について解説します。

設定する PC とリセットしたデバイスの 1 番ポートを結線し、ブラウザのアドレスバーに <https://10.0.1.1:8080> を入力し、アクセスします。



証明書のセキュリティ警告が出てそのまま続行します。

するとログイン画面が表示されますのでユーザー名に「admin」、パスワードに「readwrite」を入力します。



Wizard が始まります。初期設定が目的なので「新しいデバイス構成の作成」にチェックして次へ。

Web Setup Wizard へようこそ

WatchGuard

このウィザードは WatchGuard XTM デバイスを設定するのに役立ちます。

Select a configuration type:

新しいデバイスの構成の作成

バックアップ イメージの復元

[その他の情報](#) [次へ](#)

使用許諾契約の条項に同意して次へ。

使用許諾契約を読む

In accordance with the substantive laws of Washington excluding the 1900 United National Convention on Contracts for the International Sale of Goods, as amended This is the entire AGREEMENT between us relating to the SOFTWARE PRODUCT, and supersedes any prior purchase order, communications, advertising or representations concerning the SOFTWARE PRODUCT AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS AGREEMENT; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT AND; (C) THIS AGREEMENT AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of this AGREEMENT will be valid unless it is in writing

使用許諾契約に同意します

[戻る](#) [次へ](#)

以降、各種ネットワークやポリシーをできる画面になりますが、すべての設定項目は初期セットアップ後に変更可能ですので、設定が決まっていなくてもデフォルトのまま進んでいただいて構いません

外部インターフェイスは DHCP(デフォルトのまま)を選択し次へ。

XTM デバイスの 外部インターフェイスの構成

XTM デバイスが外部 IP アドレスを設定する際に使用する方法を選択してください:

DHCP
 PPPoE
 静的

その他の情報 戻る 次へ

次へ。

DHCP 用外部インターフェイスの構成

手動で IP アドレスを割り当て、そのアドレスを XTM デバイスに設定するためだけに DHCP を使用する場合には、**IP アドレスの使用**ラジオ ボタンを選択して、隣のフィールドに IP アドレスを入力します。**クライアント**および**ホスト名**フィールドの入力は任意です。

IP アドレスの自動取得
 IP アドレスの使用

リース時間

クライアント

ホスト名

その他の情報 戻る 次へ

DNS サーバーの指定です。後から設定できますが、プロバイダもしくはシステム部門指定の IP アドレスが決まっていたら入力して次へ。

DNS サーバーおよび WINS サーバーの構成

Fireware XTM の機能の中には、Windows Internet Name Server (WINS) および Domain Name System (DNS) のサーバーの IP アドレスを要求するものがあります。これらのサーバーへのアクセスは、Firebox の信頼済みインターフェイスから行える必要があります。次の目的で使用されます: IPSec VPNI に対して IP アドレスへの名前解決を提供し、spamBlocker、Gateway AV、および IPS 機能が正しく動作するように、XTM デバイスはここに示す DNS サーバーを使用します。WINS の入力内容および DNS の入力内容は、信頼済みネットワークまたは任意ネットワーク上の DHCP クライアントや、Mobile VPN ユーザーが DNS クエリを解決するために使用されません。

ドメイン名

DNS サーバー

WINS サーバー

[その他の情報](#)

信頼済みインターフェイス(現在接続しているポート)の設定です。

DHCP を有効にしてよければこのまま次へ。開始/終了 IP を変更しても構いません。

DHCP を有効にたくない場合はチェックを外して次へ。

信頼済みインターフェイスの構成

信頼済みインターフェイス用に、内部のプライベート ネットワークから利用可能な IP アドレスを入力します。この IP アドレスは信頼済みインターフェイスとなります。

IP アドレス /

このインターフェイス上で DHCP サーバーを有効にする

開始 IP

終了 IP

信頼済みインターフェイスの IP アドレスを変更する場合、Fireware XTM Web UI に接続するために、ブラウザアドレスバー内で新しい IP アドレスを使用する必要があります。例えば、信頼済みインターフェイス IP アドレスを 172.16.0.1 に変更する場合、接続するためには <https://172.16.0.1:8080> を使用する必要があります。また、新しい信頼済みネットワーク IP サブネット範囲に入るように、コンピュータの IP アドレスも変更する必要があります。

[その他の情報](#)

パスワードの設定です。status ユーザーは設定の読み取り専用のアカウント、admin ユーザーは設定が保存できる管理者アカウントです。それぞれを 8 文字以上の英数字で設定します。
status と admin は同じパスワードを使用することはできません。

デバイス用のパスワードの作成

デバイスには 2 つのビルトイン ユーザー アカウントがあります：

管理者は読み書き権限を持ちます。
ステータスは読み取りのみの権限を持ちます。

それぞれのアカウントで使用するパスワードを入力します。
それぞれのパスワードは 8 ～ 32 文字を含む必要があります。

ユーザー名	ステータス (読み取りのみ)
パスワード	●●●●●●
パスワードの確認	●●●●●●
ユーザー名	管理者 (読み書き)
パスワード	●●●●●●
パスワードの確認	●●●●●●

[その他の情報](#) 戻る 次へ

リモート管理の有効化はしないで次へ。(後からポリシーの編集画面で変更できます)

リモート管理を有効にする

このデバイスのリモートコンピュータからの管理を許可する

リモートホスト IP アドレス

Web Setup Wizard が自動的に"WatchGuard"と呼ばれるポリシーを作成します。このポリシーによって、信頼済みネットワークまたは任意ネットワーク上の任意のコンピュータから、XTM デバイスに接続して管理することが許可されます。離れた場所(信頼済みや任意のネットワーク上にはない、あらゆるコンピュータ)から XTM デバイスを管理する場合は、ここにリモート IP アドレスを追加してポリシーを変更することができます。

[その他の情報](#) 戻る 次へ

デバイス名を入力し次へ。

デバイスの連絡先情報の追加

連絡先情報

デバイスの連絡先情報は、複数のデバイスを管理する場合に、このデバイスを識別するのに役立ちます。

デバイス名

デバイスの場所

担当者

デバイスフィードバック

デバイスフィードバックは WatchGuard が製品および機能を改善するのに役立ちます。デバイスが WatchGuard に送信するフィードバックは、どのようにデバイスが使用されるかについての情報が含まれますが、お客様の会社または会社データを特定する情報は含まれません。

デバイスフィードバックを WatchGuard に送信

その他の情報

タイムゾーンは「(GMT+09:00)大阪、札幌、東京」を選択して次へ。

タイムゾーンの設定

XTM デバイスが設置された地域のタイムゾーンを選択します。タイムゾーン設定は、ログファイルや、LogViewer、WatchGuard Reports、WebBlocker などのその他のツールに表示される日付・時間を制御します。

タイムゾーン

その他の情報

オンラインライセンス登録はスキップしてください。

※ 設定済みの機器を再セットアップする際には、ライセンスが保持されていることがあり、その場合ライセンス登録やフィーチャーキーの入力の画面は表示されず、セットアップが完了します

オンラインライセンス登録

構成は完了です。XTM デバイスの外部インターフェイスがインターネットに接続されている場合、ウィザードは自動的に WatchGuard のウェブサイト上でデバイスを起動して、デバイスのすべての機能を有効にする機能キーをダウンロードおよびインストールします。このデバイスを識別するには、わかりやすい名前を入力します。次に、WatchGuard Web サイトのログインに使用するアカウント認証情報を入力します。

わかりやすい名前

シリアル番号

ユーザー名

パスワード

WatchGuard は初めてお使いですか? [アカウントを作成するにはここをクリックしてください](#)

[その他の情報](#)

有効化の画面になります。機能キーを追加 を選んで次へ。

有効化

デバイスのすべての機能を有効にする機能キーをアップロードしますか? このウィザードでこれを行うには、このデバイスを有効化した後、ローカルファイルに WatchGuard アカウントから機能キーをダウンロードしておく必要があります。

機能キーを追加

この手順をスキップ

[その他の情報](#)

あらかじめ取得しておいた機能キーをテキストボックスに貼り付けて、次へ。

機能キーを追加

下記のボックスに、使用する機能キーを貼り付けてください。

```
Feature: FW_RULE#0
Feature: FW_SPEED#200
Feature: FW_USERS#0
Feature: IPS@Feb-10-2018
Feature: L2TP_USER#5
Feature: LIVESECURITY@Feb-10-2018
Feature: MUVPN_USER#5
Feature: RED@Feb-10-2018
Feature: SESSION#15000
Feature: SPAMBLOCKER@Feb-10-2018;UC17Q63WEU2Q2UGD54HB
Feature: SSLVPN_USER#5
Feature: VLAN#10
Feature: VPN_SPEED#30
Feature: WEBBLOCKER@Feb-10-2018
Expiration: never
```

その他の情報

戻る 次へ

最後に設定のサマリーが表示されますので、内容を確認して次へ。

概要

下記の構成を確認します。

有効化	成功
機能キー	手動で適用
外部インターフェイス	DHCP の使用 - IP アドレスの自動取得
信頼済みインターフェイス	10.0.1.1/24 - DHCP の使用
タイムゾーン	(GMT+09:00) 大阪、札幌、東京

これらの設定を適用するには、[次へ] をクリックします

戻る 次へ

設定が保存されます。

設定の保存

セットアップ完了が表示されます。

設定は完了です。

デバイスの基本構成が完了しました。これにより、アウトバウンド TCP、UDP、および ping トラフィックが許可され、要求していないすべての外部トラフィックがブロックされるようになります。

デバイスを更新
デバイスを最新の Fireware XTM OS にアップグレードすることを推奨します。アップデートを [WatchGuard サポートセンター](#) でチェックしてください

デバイスの管理
WatchGuard Web UI はネットワーク上の任意のブラウザからデバイスを設定し管理することを可能にします。WatchGuard System Manager は、Windows ベースの管理ツールのセットで、これによって、クラスタ、詳細なレポートや、他のエンタープライズレベルの機能にアクセスすることができます。

Web UI を起動 WatchGuard System Manager をダウンロードする
<https://10.0.1.1:8080> <https://www.watchguard.com/archive/softwarecenter.asp>

自動的に再起動がかかり、設定した内容で起動します。3~4 分お待ちください。

再度 <https://10.0.1.1:8080> にアクセスし、ウィザードで設定したパスワードでログインしてください。

以下のように Web UI のダッシュボードが表示されれば問題なく設定できています。

WatchGuard Fireware XTM Web UI ユーザー: admin | ヘルプ | ログアウト

ダッシュボード
フロントパネル
サブスクリプションサービス
FireWatch
インターフェイス
トラフィックモニタ
ゲートウェイワイヤレスコントローラ
システム ステータス
ネットワーク
ファイアウォール
サブスクリプションサービス
認証
VPN
システム

フロントパネル

トップクライアント

名前	レート	バイト	ヒット
10.0.1.2	6 Kbps	1 KB	1

上位宛先

名前	レート	バイト	ヒット
10.0.1.1	6 Kbps	1 KB	1

上位ホスト

名前	レート	バイト	ヒット
WatchGuard Web UI	6 Kbps	1 KB	1

送信先ポート

名前	レート	バイト	ヒット
8080	6 Kbps	1 KB	1

システム

名前 XTM_2_Series-W
モデル XTM26-W
バージョン 11.9.4.B463675
シリアル番号 70A705EE6FDC8
システム時間 14:19 Asia/Tokyo
システム日付 2015-01-19
稼働時間 0 days 01:05
Log Server Disabled

再起動

過去 20 分

外部帯域幅

16 Kbps
12 Kbps
8 Kbps
4 Kbps
0 Kbps

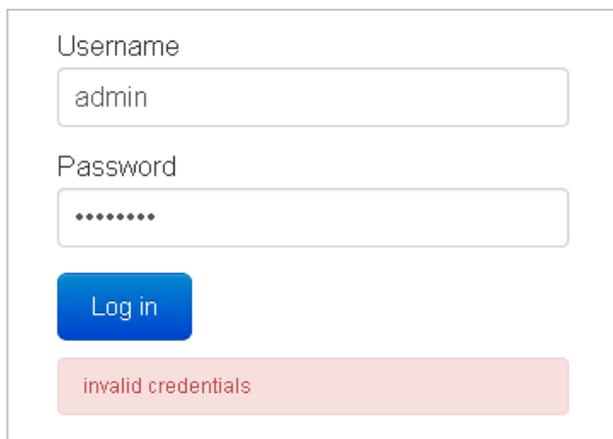
20 分前 現在

初期セットアップは以上で完了です。

付録 :トラブルシューティング

エラー表示やアクセスできないなどの症状がある場合に参考にしてください。

ログイン後に“invalid credentials”と表示される

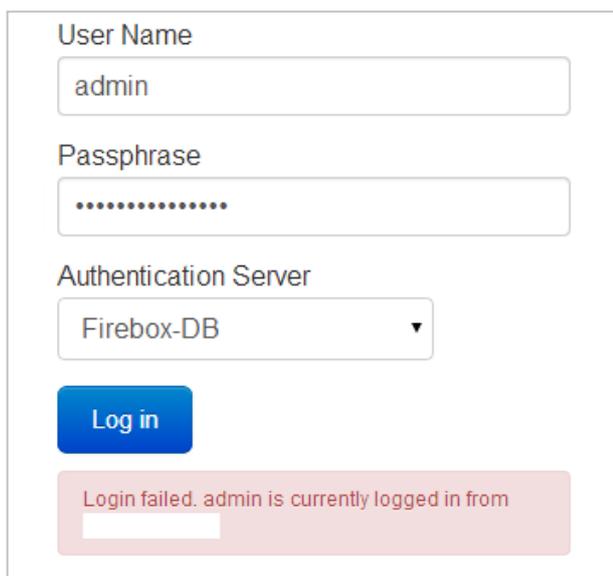


A screenshot of a login form. It has two input fields: 'Username' with the text 'admin' and 'Password' with seven dots. Below the fields is a blue 'Log in' button. At the bottom, a red error message box displays the text 'invalid credentials'.

原因と対策:

1. Web ブラウザにキャッシュ/クッキー情報が残っている可能性があります
⇒Web ブラウザを再起動して接続し直す
2. Firebox/XTM デバイス内部のプロセスが正常に起動していない可能性があります
⇒デバイスの再起動
3. 初期セットアップに失敗している可能性があります
⇒再度手順に沿って初期セットアップを実施

ログイン後に“Login failed. admin is currently logged in from x.x.x.x”と表示される



A screenshot of a login form. It has three input fields: 'User Name' with the text 'admin', 'Passphrase' with ten dots, and 'Authentication Server' with a dropdown menu showing 'Firebox-DB'. Below the fields is a blue 'Log in' button. At the bottom, a red error message box displays the text 'Login failed. admin is currently logged in from' followed by a white redacted area.