



# WatchGuard XTMv

## スタートアップガイド



ウォッチガード・テクノロジー・ジャパン株式会社

2014年8月 Rev-01

## 目次

はじめに .....	3
XTMv の導入.....	4
XTMv のデプロイ .....	4
デプロイに失敗するとき .....	11
初期セットアップ.....	12
XTMv デバイスの起動 .....	12
Web Setup Wizard の実行 .....	14
付録: Virtual Machine Port Group の作成.....	22
おわりに .....	26

## はじめに

この度は、ウォッチガード製品を選択していただき、誠にありがとうございます。

WatchGuard XTMv は仮想環境の中で仮想イメージとして動作する WatchGuard XTM デバイスです。通常の仮想技術同様、リソースの適正配分、導入の容易性を提供します。

本書は、XTMv の導入を目的としたスタートアップガイドです。使用されている画面のバージョンは、VMWare ESXi および vSphere Client が 5.5、XTMv は 11.9.1 です。

本書が可用性、管理の効率化、コスト削減を実現する XTMv の導入にお役に立てれば幸いです。

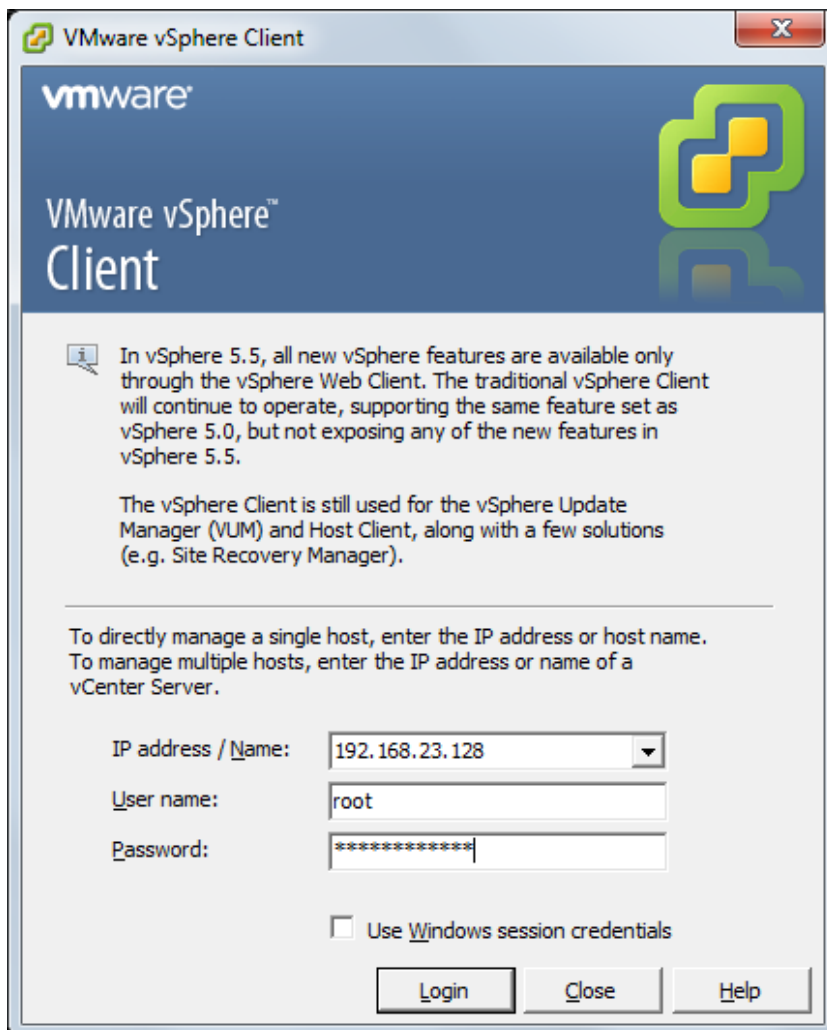
## XTMv の導入

XTMv は VMWare と Hyper-V の両方に対応しています。

このガイドでは VMWare での導入方法を解説します。

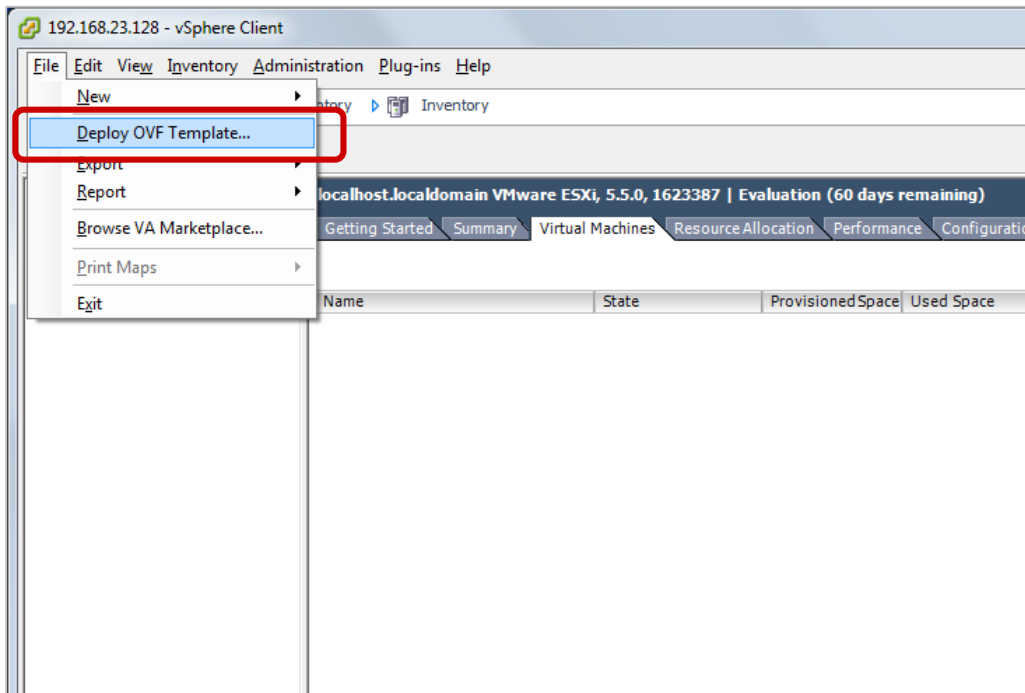
## XTMv のデプロイ

VMWare vSphere Client から VMWare サーバーに接続します。

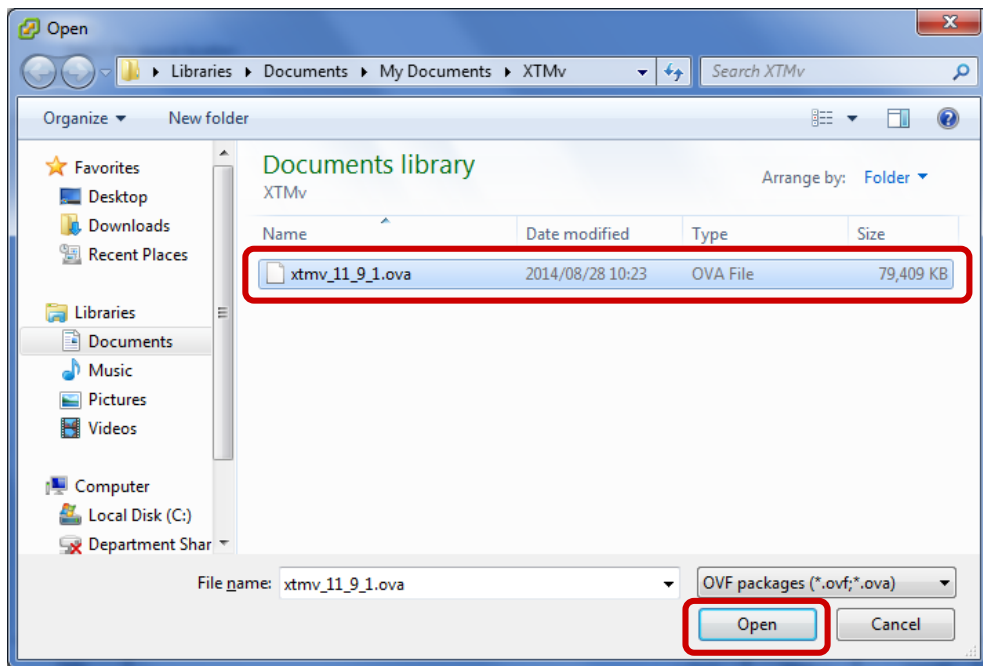


The screenshot shows the VMware vSphere Client login window. The title bar reads "VMware vSphere Client". The main area features the VMware logo and the text "VMware vSphere™ Client". Below this, there is an information icon and a message: "In vSphere 5.5, all new vSphere features are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0, but not exposing any of the new features in vSphere 5.5. The vSphere Client is still used for the vSphere Update Manager (VUM) and Host Client, along with a few solutions (e.g. Site Recovery Manager)." Below the message, there is a section for host management: "To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server." The form contains three input fields: "IP address / Name:" with the value "192.168.23.128", "User name:" with the value "root", and "Password:" with masked characters "\*\*\*\*\*". There is also a checkbox labeled "Use Windows session credentials" which is currently unchecked. At the bottom, there are three buttons: "Login", "Close", and "Help".

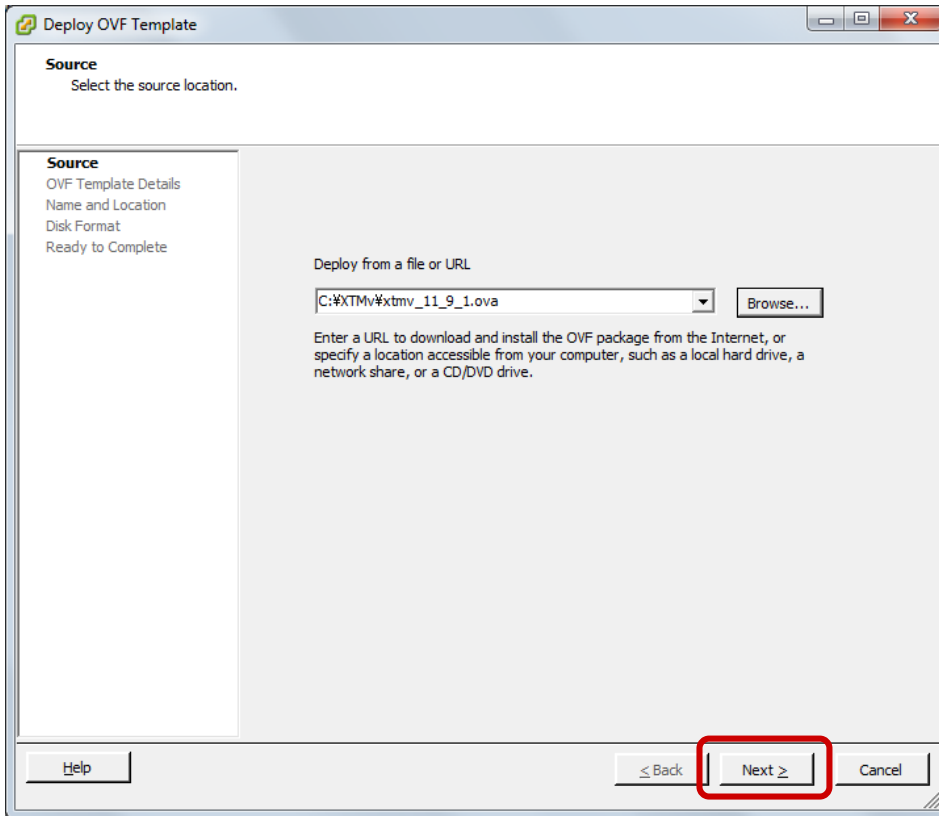
接続できたら、メニューの **File** - **Deploy OVF Template...** をクリックします。



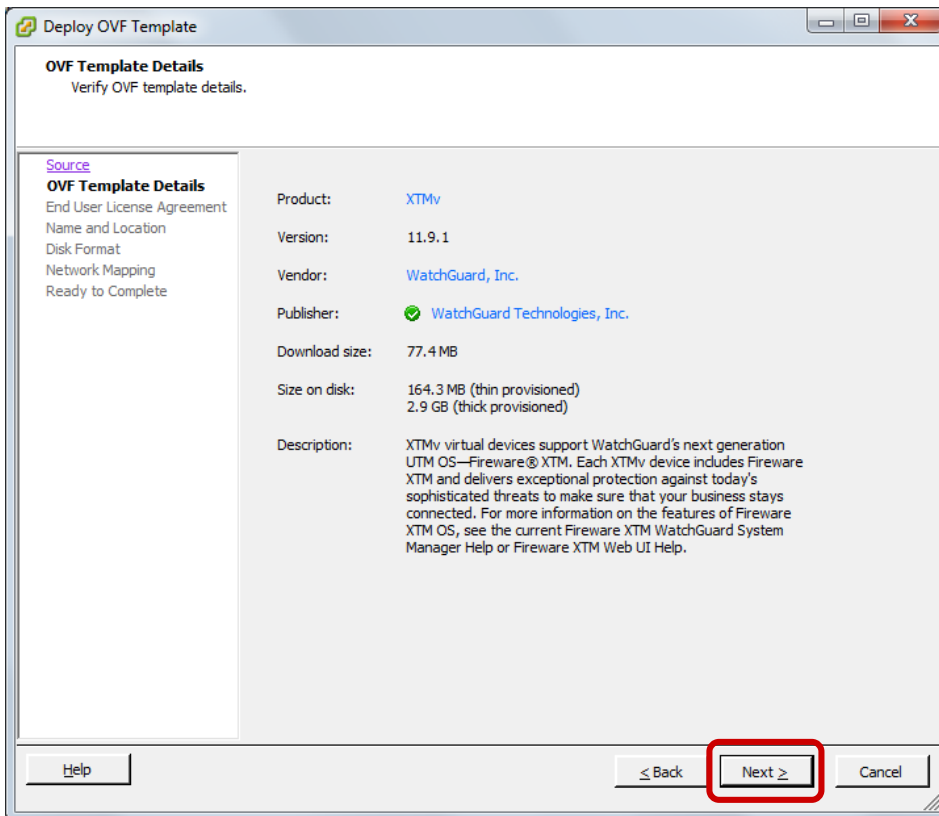
ダウンロードした XTMv の OVA ファイルを選択し、Open ボタンをクリックします。



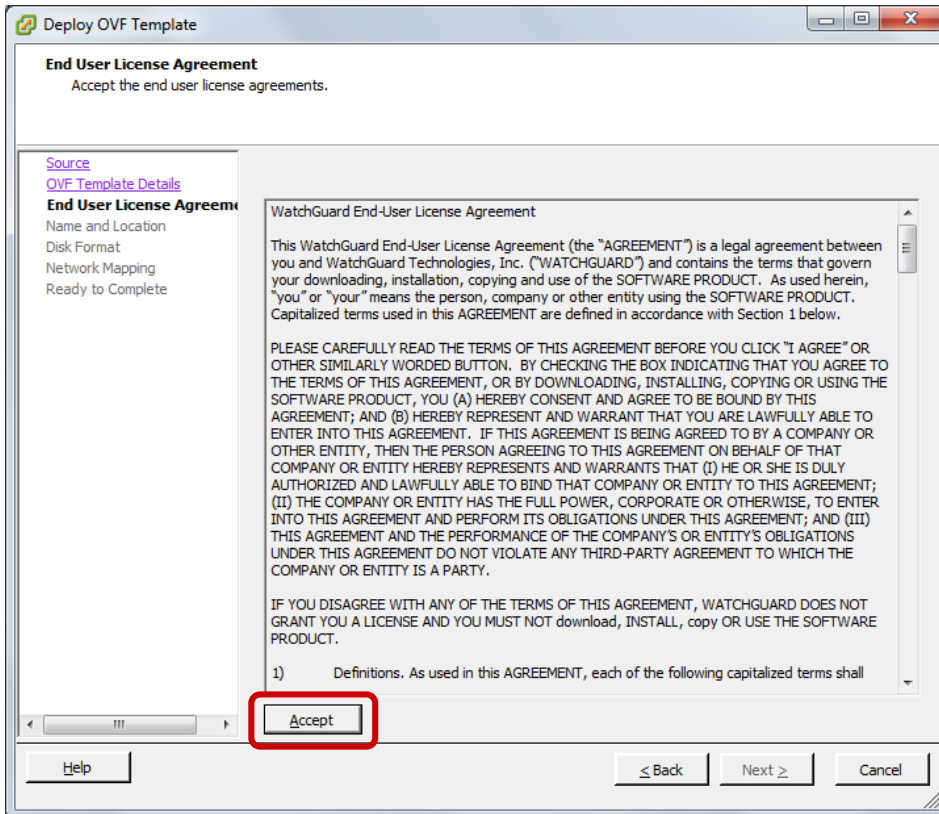
OVA ファイルのフルパスがテキストフィールドに入力されていることを確認し、Next ボタンをクリックします。



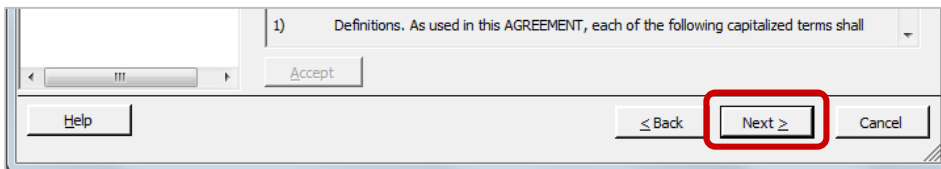
テンプレートの詳細情報が表示されるので、確認して Next ボタンをクリックします。



End User License Agreement は Accept ボタンをクリックします。

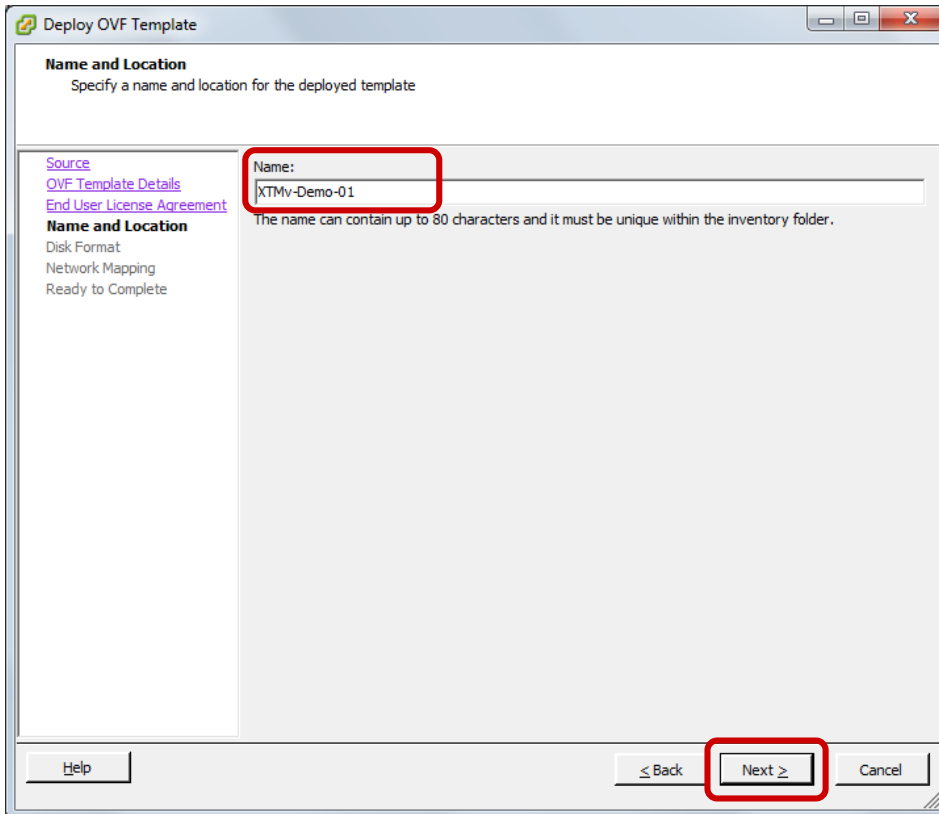


アクティブになった Next ボタンをクリックします

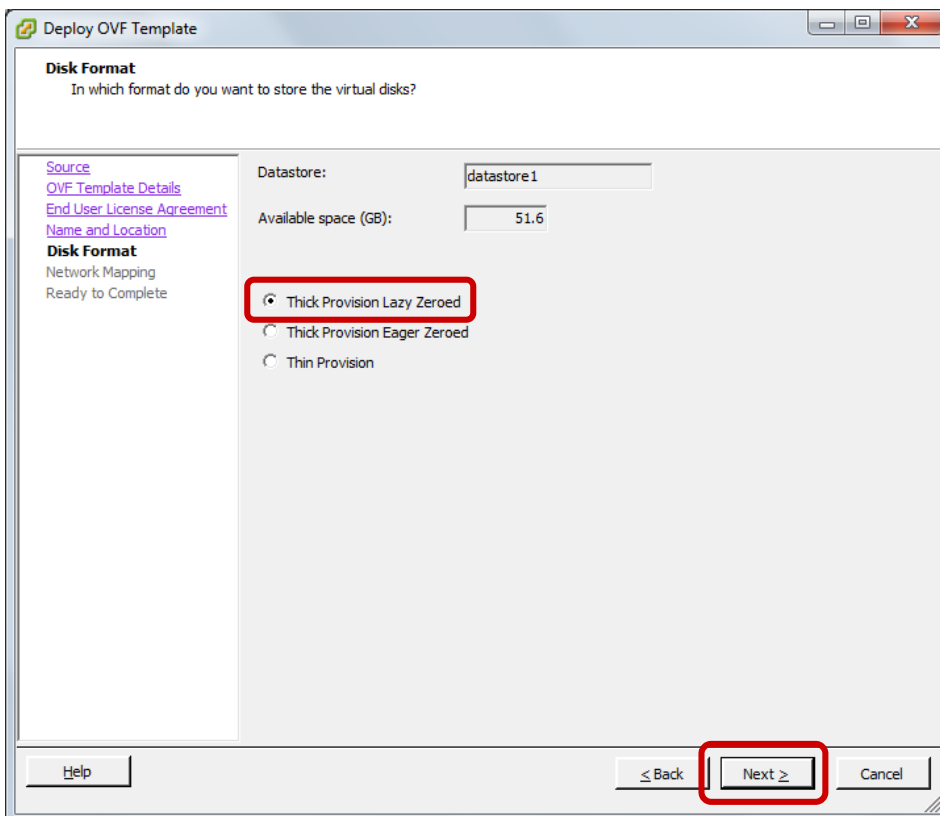


次にデプロイされる仮想マシンに名前をつけます。

実際のホスト名ではなく、vSphere Client 上のインベントリで表示される名前を入力します。



次にディスクの設定です。Thin か Thick を選択して次へ進みます。Thick プロビジョニングが推奨です。

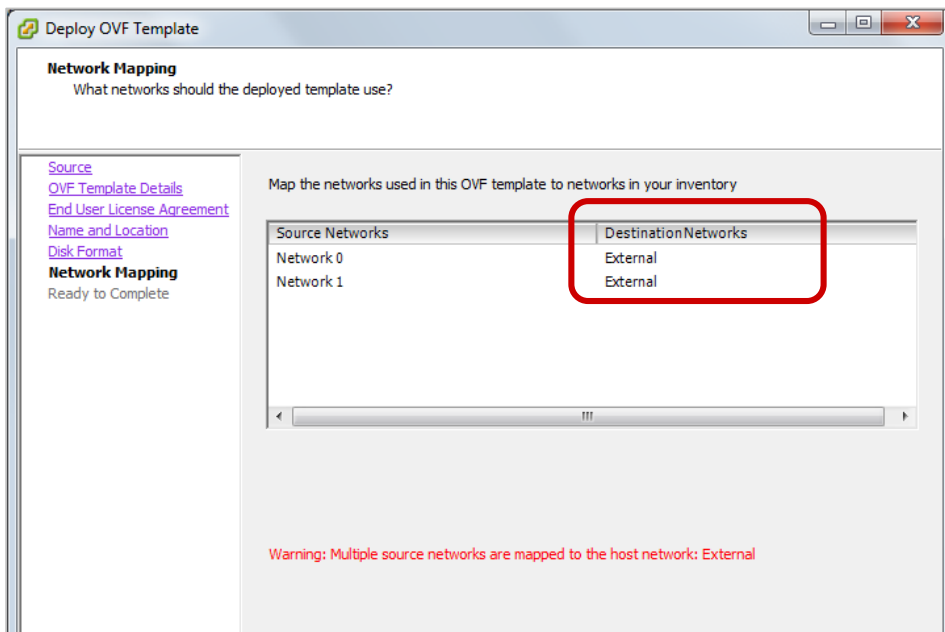




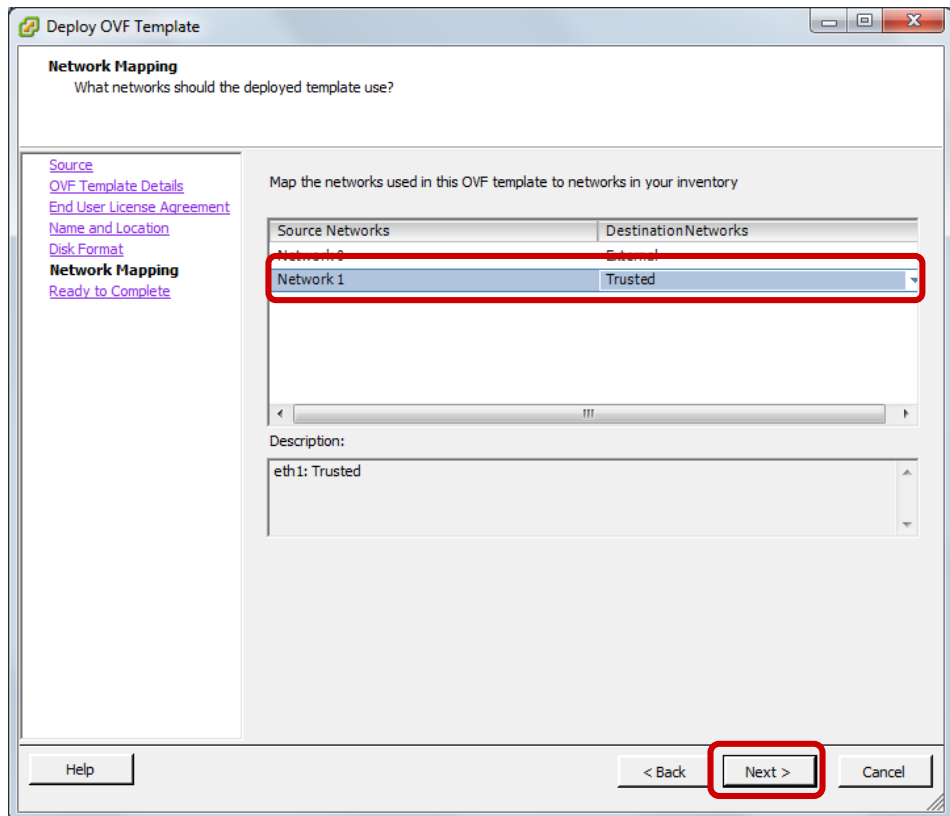
次にネットワークの設定画面です。Destination Networks が同じインターフェースを指しているとアラートが表示されます。

※ここが External 又は Trusted にならない場合は手でポートグループを作成します。

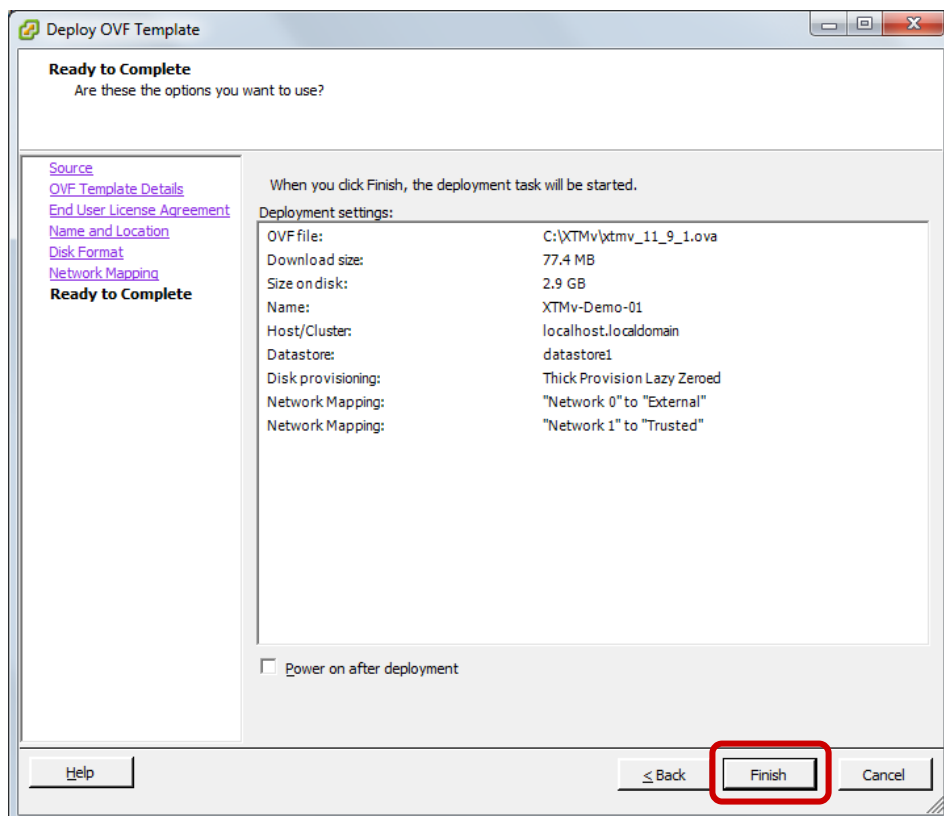
「付録: Virtual Machine Port Group の作成」をご参照ください。



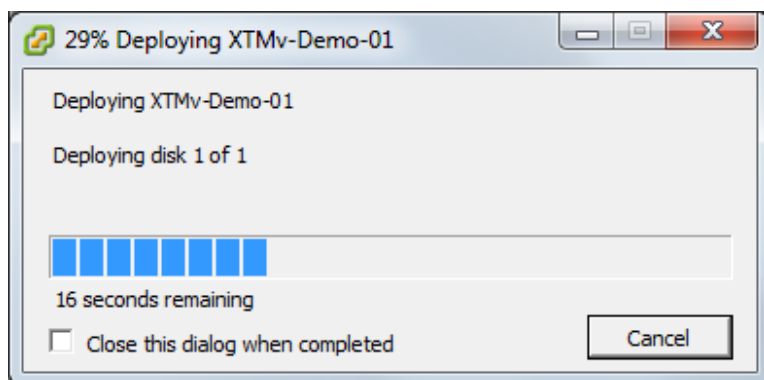
Destination Networks は Network0 には External、Network1 には Trusted を指定して、Next ボタンをクリックします。



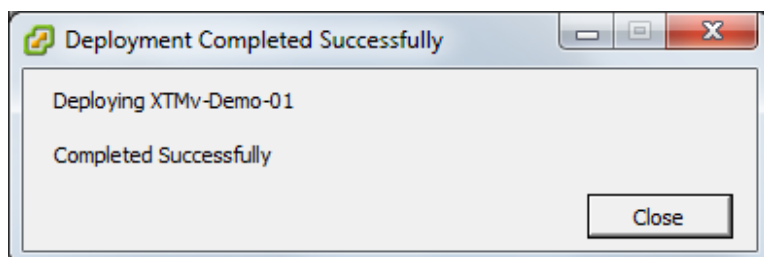
次に進むと設定のサマリーが表示されます。確認して Finish ボタンをクリックします。



デプロイが始まります。進行中はプログレスバーで進捗が表示されます。



Completed Successfully と表示されれば完了です。



## デプロイに失敗するとき

デプロイに失敗する場合は OVFTOOL を使って OVA ファイルを OVF ファイルに展開し、デプロイ時に OVF ファイルを指定してください。

コマンドラインは次のとおりです。(OVF ファイルは OVA ファイルの拡張子を変えるだけです)

```
ovftool.exe OVA ファイル OVF ファイル
```

以下は実行例です。

```
PROMPT> ovftool.exe C:\XTMv\xtmv_11_9_1.ova C:\XTMv\OVF\xtmv_11_9_1.ovf
Opening OVA source: C:\XTMv\VMWare\xtmv_11_9_1.ova
The manifest validates
Source is signed but could not verify certificate (possibly self-signed)
Opening OVF target: C:\XTMv\OVF\xtmv_11_9_1.ovf
Writing OVF package: C:\XTMv\OVF\xtmv_11_9_1.ovf
Transfer completed
Completed successfully
```

OVFTOOL の入手先:

<https://my.vmware.com/jp/web/vmware/details?productId=352&downloadGroup=OVFTOOL350>

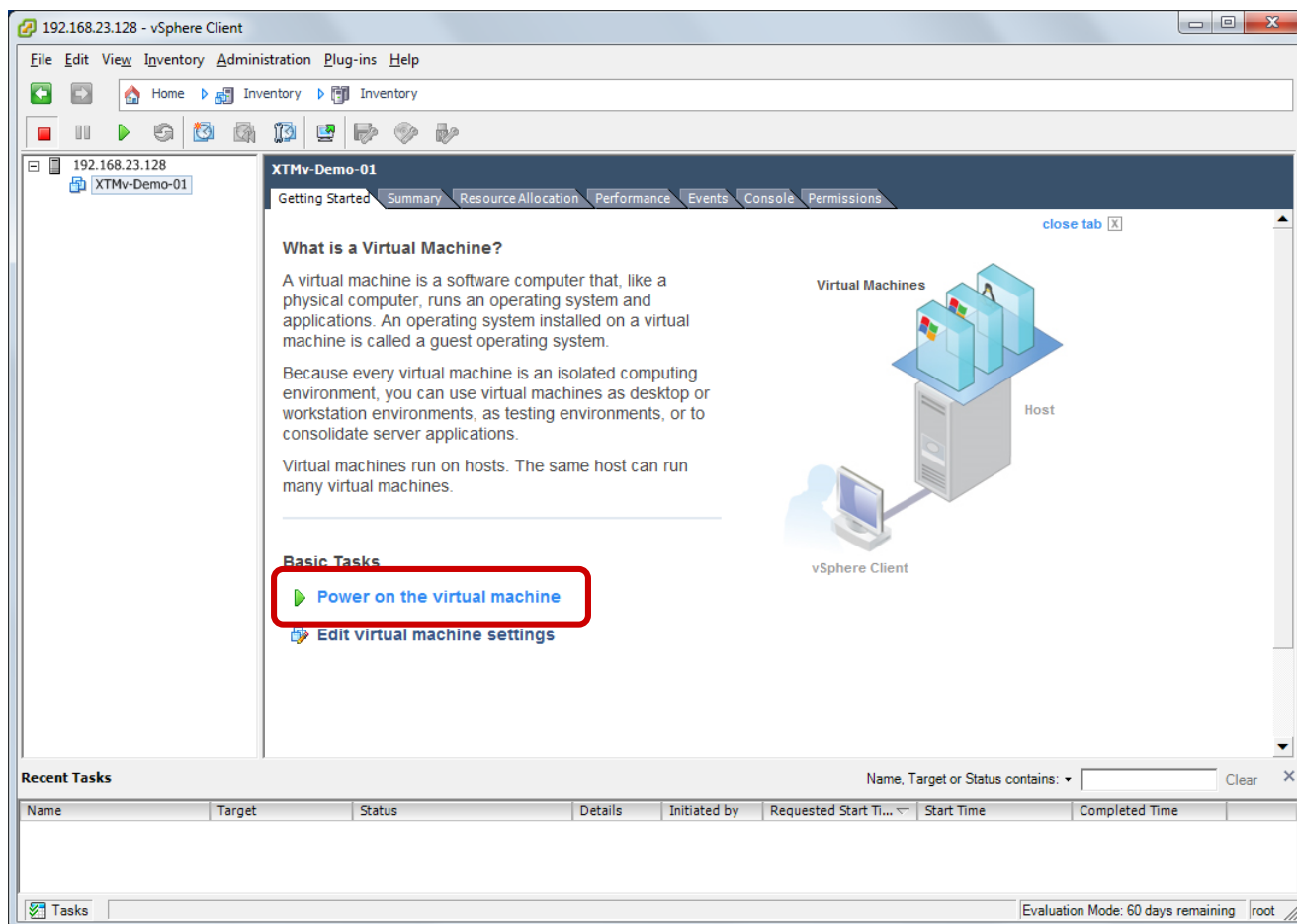
## 初期セットアップ

XTMv は仮想アプライアンスですが、一度起動してしまえば扱いはほとんど実機と変わりません。  
デプロイ後の初期設定は以下のとおりです。

- アクティブなインターフェースは External と Trusted の 2 ポート
- Trusted インターフェースの IP アドレスは 10.0.1.1
- External インターフェースは DHCP で IP アドレスを取得
- どちらのポートからでも Web Setup Wizard で設定することが可能 (この点は実機と異なる)
- admin アカウントのデフォルトパスワードは readwrite

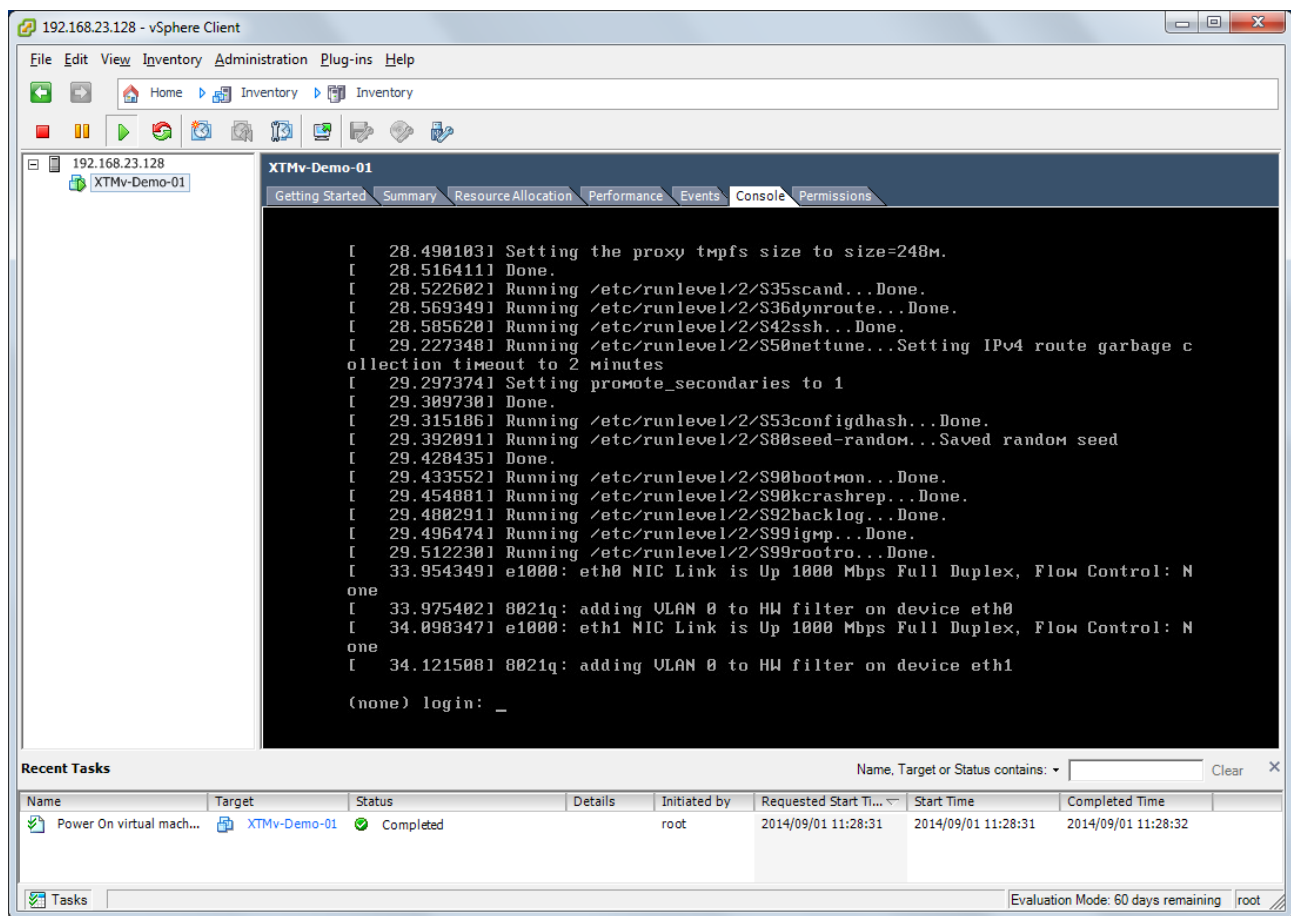
## XTMv デバイスの起動

Web Setup Wizard で基本的な設定を施しますが、その前にデプロイした XTMv デバイスを起動しましょう。  
vSphere Client のインベントリに表示されている XTMv デバイスを Power On します。

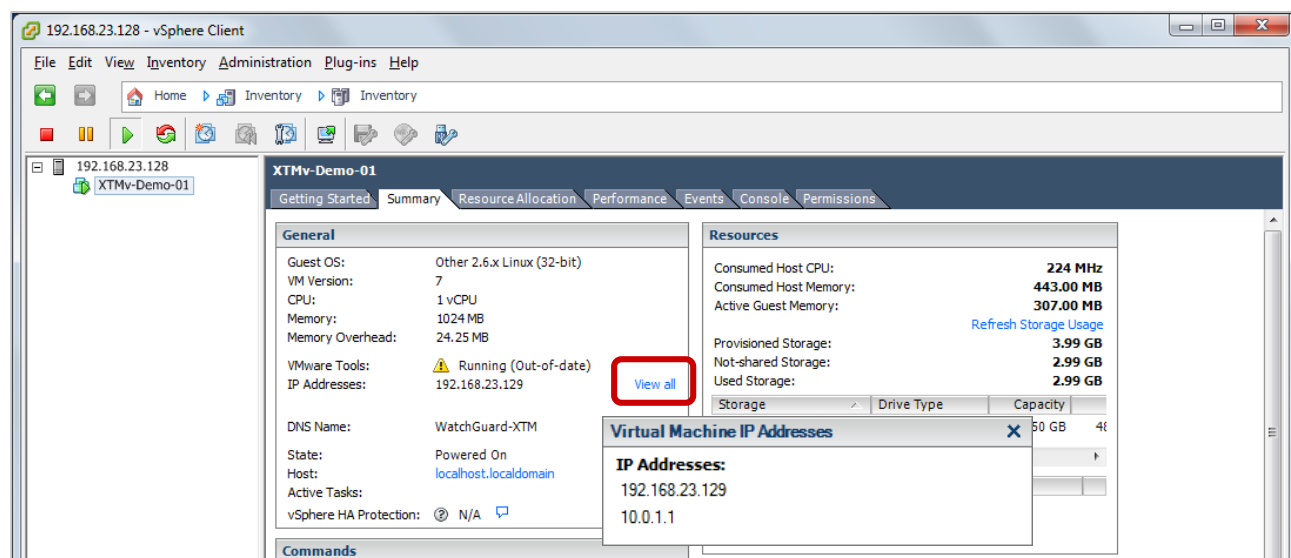


コンソールタブをクリックすると、起動途中のメッセージを確認することができます。

ログインプロンプトが表示されたら起動したことが分かります。



Summary タブをから、初期状態で設定されている IP アドレスが分かりますので、このアドレスにブラウザでアクセスし、Web Setup Wizard を実行します。



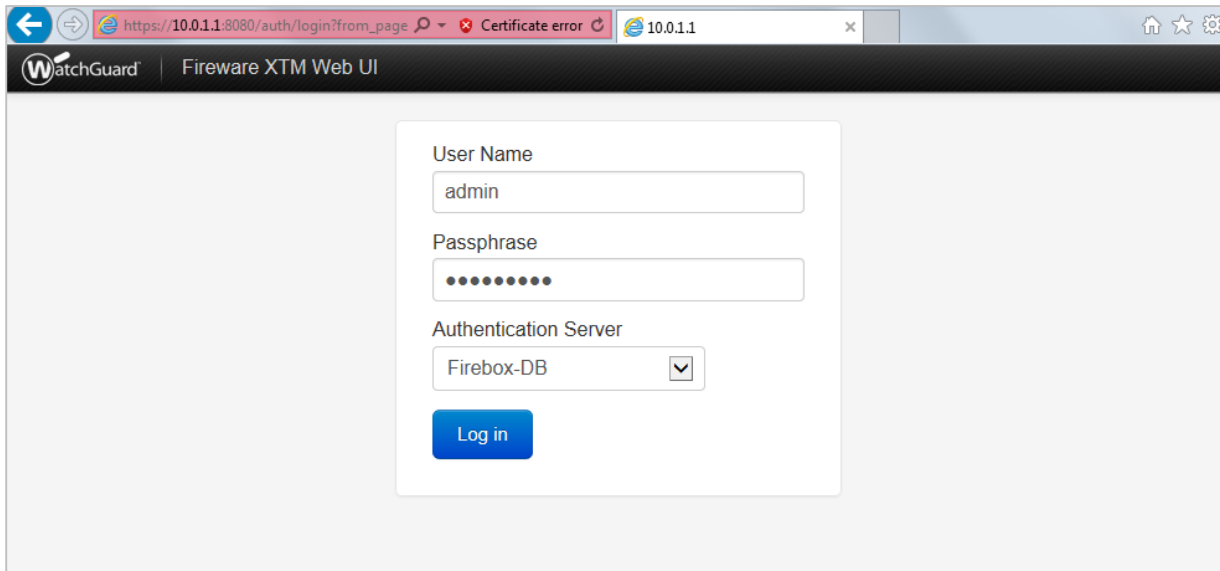
## Web Setup Wizard の実行

15 分以内に Wizard を完了しないと、タイムアウトして設定内容が保存されません。

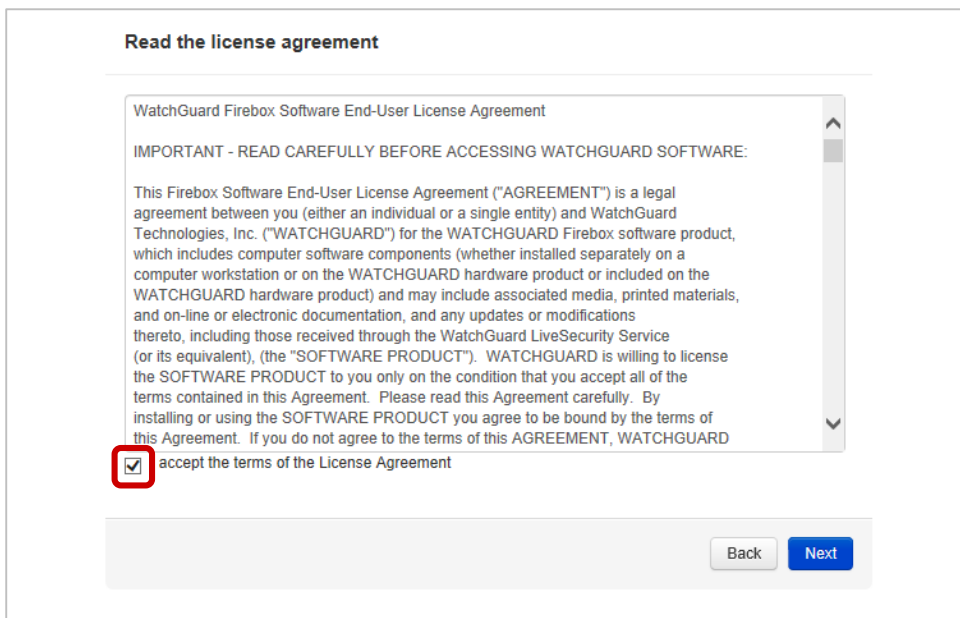
最低限の設定内容を決めておき、製品の Activate を完了させ、ライセンスキーを取得しておいてください。

Web Setup Wizard を開始するには、ブラウザで <https://<XTMv の IP アドレス>:8080> にアクセスします。

User Name は admin、Passphrase は readwrite を入力し、Log in ボタンをクリックします。



License Agreement には同意のチェックをして Next。



External ポートの設定になりますが、詳細な設定は Wizard ではなく、設定後、WebUI もしくは WSM で行ったほうがよいので、ここではデフォルトで進みます。

### Configure the external interface of your XTM device

Select the method your XTM device uses to set its external IP address:

DHCP  
 PPPoE  
 Static

[More Information](#)

デフォルトのまま Next。

### Configure the external interface for DHCP

If you want to manually assign the IP address and use DHCP just to give this assigned address to the XTM device, select the **Use IP address** radio button and enter the IP address in the adjacent field. The **Client** and **Host Name** fields are optional.

Obtain an IP address automatically  
 Use IP address

Leasing Time

Client

Host Name

[More Information](#)

DNS サーバーの設定画面になります。社内に指定の DNS サーバーがあれば入力します。

### Configure the DNS and WINS servers

Some Fireware XTM features require Windows Internet Name Service (WINS) and Domain Name System (DNS) server IP addresses. Access to these servers must be available from the trusted interface of the XTM device and is used for: The XTM device uses the DNS server shown here to resolve names to IP addresses for IPSec VPNs and for the spamBlocker, Gateway AV, and IPS features to operate correctly. The WINS and DNS entries are used by DHCP clients on the trusted or optional networks, and by Mobile VPN users to resolve DNS queries.

Domain Name

DNS Servers

WINS Servers

[More Information](#)

Trusted 側で DHCP サーバーを有効にする場合、Enable the DHCP server on this interface にチェックを入れ、IP アドレス範囲を入力します。

### Configure the trusted interface

Type an available IP address from your internal, private network to use for the trusted interface. This IP address becomes the trusted interface address.

IP Address  /

Enable the DHCP server on this interface

Starting IP

Ending IP

If you change the trusted interface IP address, you must use the new IP address in your browser address bar to connect to the Fireware XTM Web UI. For example, if you change the trusted interface IP address to 172.16.0.1, then you must use https://172.16.0.1:8080 to connect. You must also change your computer's IP address so that it is in the new trusted network IP subnet range.

[More Information](#)



status および admin のパスワードを設定します。

### Create passphrases for your device

Your device has two built-in user accounts:

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

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

User name	status (read-only)
Passphrase	<input type="password"/>
Confirm passphrase	<input type="password"/>
User name	admin (read-write)
Passphrase	<input type="password"/>
Confirm passphrase	<input type="password"/>

[More Information](#)

デバイス名を入力します。WSM や WebUI でデバイスに接続した際に表示される名前です。他の項目も任意に設定します。

### Add contact information for your device

**Contact Information**

Contact information for a device helps you to identify this device when you manage multiple devices.

Device Name	<input type="text" value="XTMv"/>
Device Location	<input type="text" value="Tokyo"/>
Contact Person	<input type="text"/>

**Device Feedback**

Device feedback helps WatchGuard improve products and features. The feedback that your device sends to WatchGuard includes information about how your device is used, but does not include identifying information about your company or your company data.

Send device feedback to WatchGuard

[More Information](#)

タイムゾーンを設定します。日本であれば「Osaka, Sapporo, Tokyo」を選択します。

### Set the time zone

Select the time zone for the physical location of your XTM device. The time zone setting controls the date and time that appear in the log file and on tools such as LogViewer, WatchGuard Reports, and WebBlocker.

Timezone

[More Information](#)

Online Activation はすでにフィーチャーキー(ライセンスキー)を取得しているのでスキップします。

### Online Activation

Configuration is complete. If the external interface of your XTM device has a connection to the Internet, the Wizard can automatically activate your device on the WatchGuard web site and download and install the feature key that enables all features for your device. Type a friendly name to identify this device. Then, type the account credentials you use to log in to the WatchGuard web site.

Friendly Name

Serial Number

User Name

Password

New to WatchGuard? [Click here to create an account](#)

[More Information](#)

Add the feature key を選択して Next。

**Activation**

Would you like to upload the feature key that enables all features for your device? To do this in this wizard, you must have downloaded the feature key from your WatchGuard account to a local file after you activated this device.

Add the feature key

Skip this step

[More Information](#)

テキストエリアにフィーチャーキーを貼り付けて Next。

**Add the feature key**

Paste your feature key into the box below.

```
Serial Number: V1C502728DA89
License ID: V1C502728DA89
Name: 08-27-2014_23:32
Model: XTMv-DC
Version: 2
Feature: APP_CONTROL@May-29-2015
Feature: AUTHENTICATED_USER#0
Feature: AV@May-29-2015
Feature: BOVPN_TUNNEL#10000
Feature: FIREWARE_XTM
Feature: FW_SPEED#0
Feature: IPS@May-29-2015
Feature: LIVESECURITY@May-29-2015
Feature: MUVPN_USER#0
Feature: RED@May-29-2015
```

[More Information](#)

設定のサマリーが表示されるので、確認して Next。

**Summary**

Review your configuration below.

Activation	Successful
Feature Key	Manually Applied
External Interface	Using DHCP - Obtain an IP address automatically
Trusted Interface	10.0.1.1/24 - Using DHCP
Time Zone	(GMT+09:00) Osaka, Sapporo, Tokyo

To apply these settings, click Next

Back Next

最後に Setup is Complete!と表示されます。

**Setup is Complete!**

Your device now has a basic configuration that allows outbound TCP, UDP, and ping traffic, and blocks all unrequested external traffic.

**Update your device**

We recommend that you upgrade your device to the latest Fireware XTM OS. Check for updates at the [WatchGuard Support Center](#)

**Manage your device**

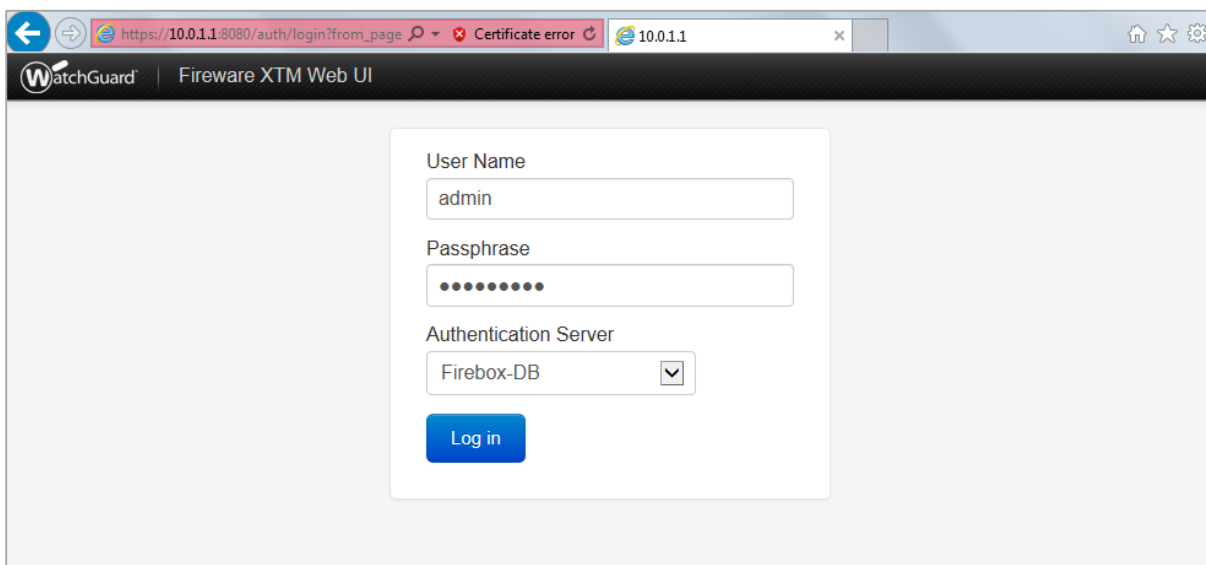
The **WatchGuard Web UI** lets you configure and manage your device from any browser on your network. **WatchGuard System Manager** is our suite of Windows-based management tools, which gives you access to clustering, detailed reporting, and other enterprise-level features.

Launch the Web UI <https://<External IP Address>:8080> Download WatchGuard System Manager <https://www.watchguard.com/archive/softwarecenter.asp>

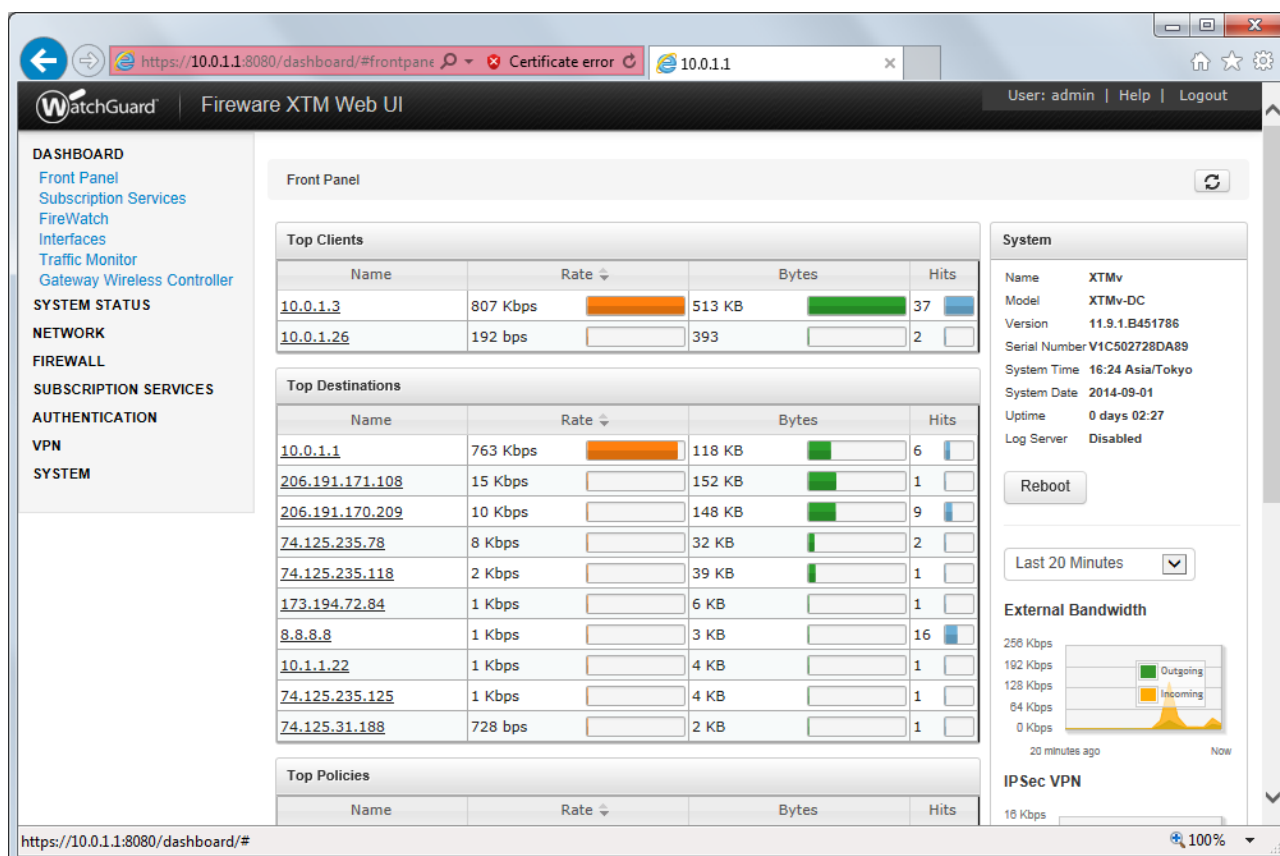
この画面までいくと、XTMv デバイスは自動的に再起動がかかり、利用できるようになります。

もし 15 分以内に Wizard を完了させないと、Summary のページで Next ボタンをクリックすると、瞬時にログイン画面にリダイレクトされてしまいます。その場合は最初からやり直してください。

再起動したら、<https://<Wizardで設定したIPアドレス>:8080> にアクセスし、User Name は admin、Passphrase は Wizard で設定した admin のパスワードを入力して Log in します。



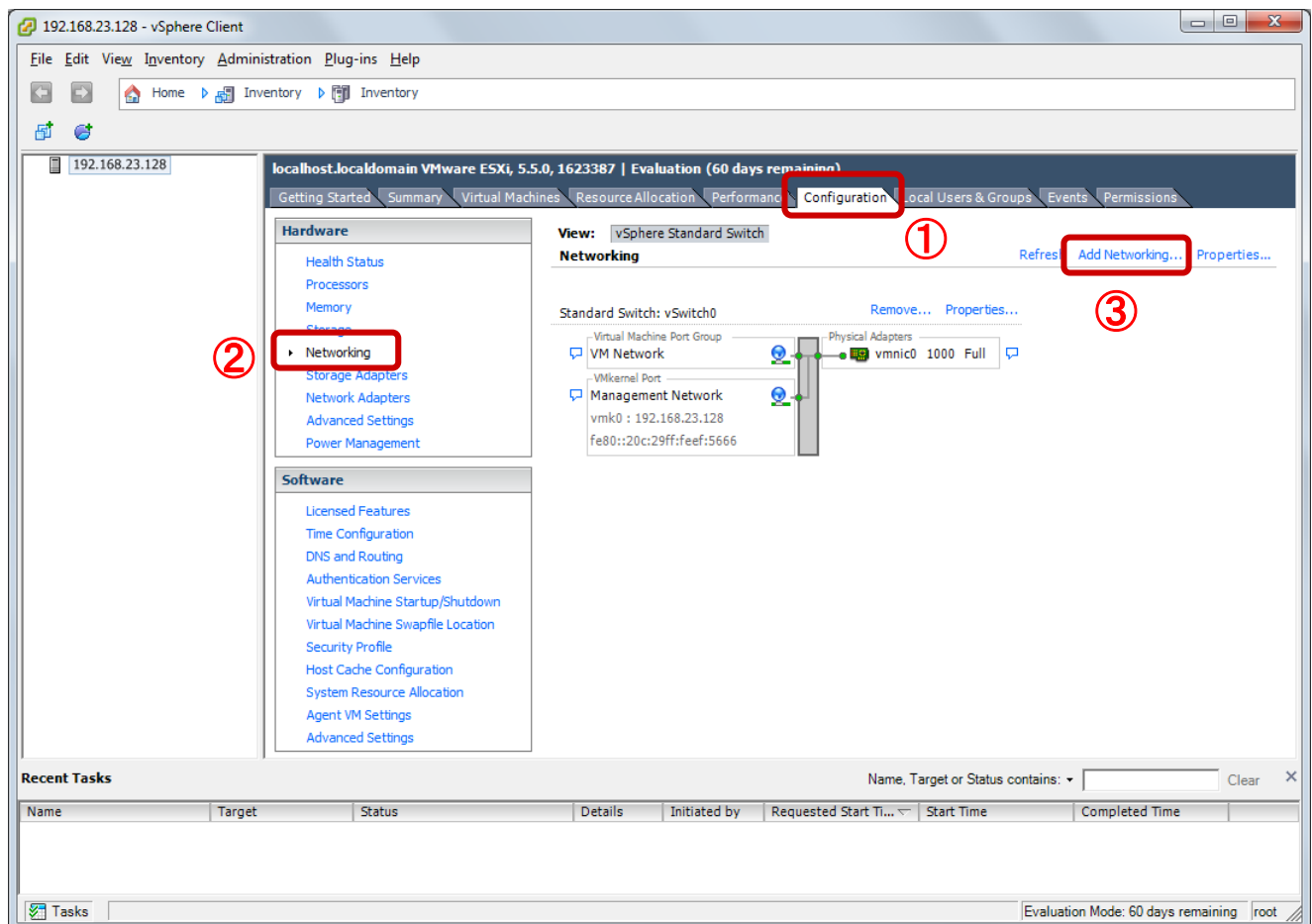
ログインでき、以下のように Front Panel が表示されたら初期設定は完了です。



## 付録: Virtual Machine Port Group の作成

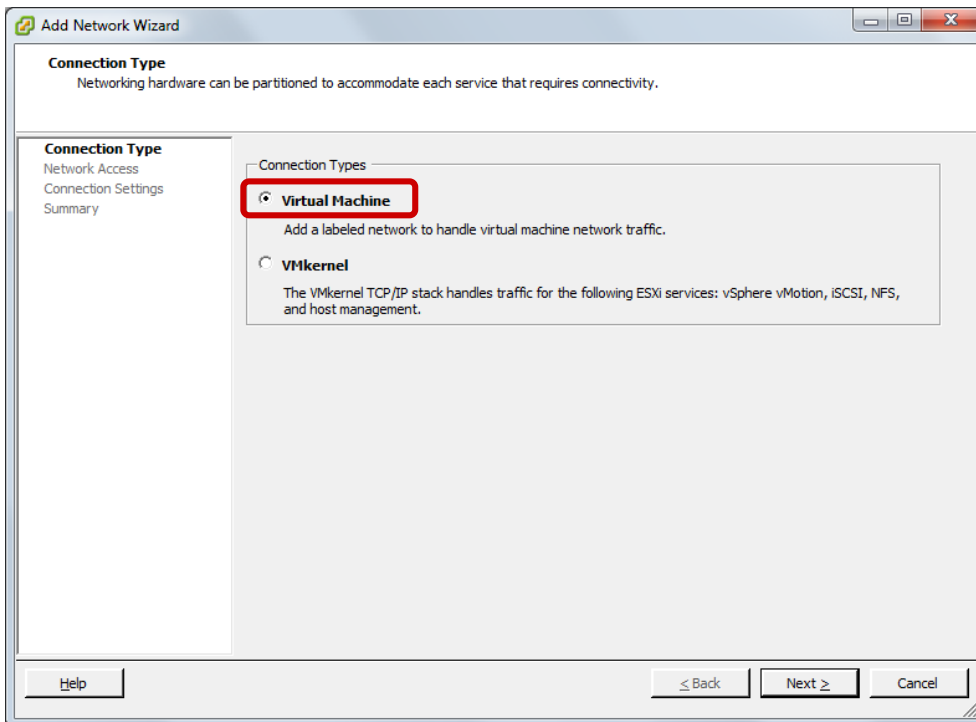
この作業は XTMv のデプロイ前に実施して、デプロイのウィザード中に Network Mapping でポートを指定してもよいですし、デプロイ後に実施してマッピングの設定をしても結構です。

- ① Configurations タブを選択します
- ② 左側 Hardware メニューの Networking をクリックします
- ③ 右上の Add Networking... をクリックします。

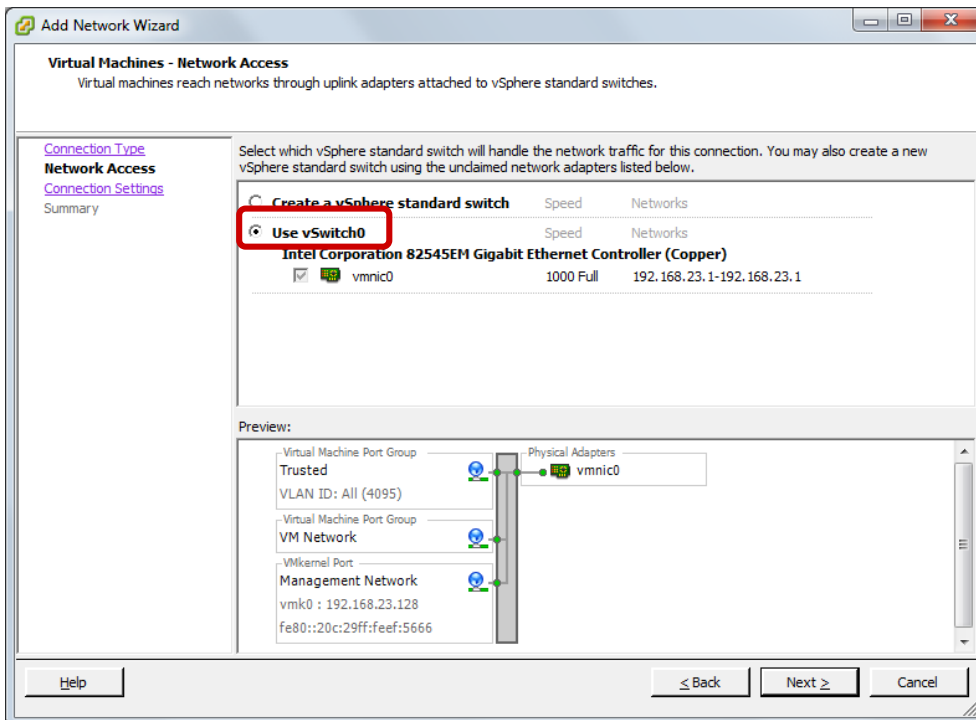


Add Network Wizard が開始します。

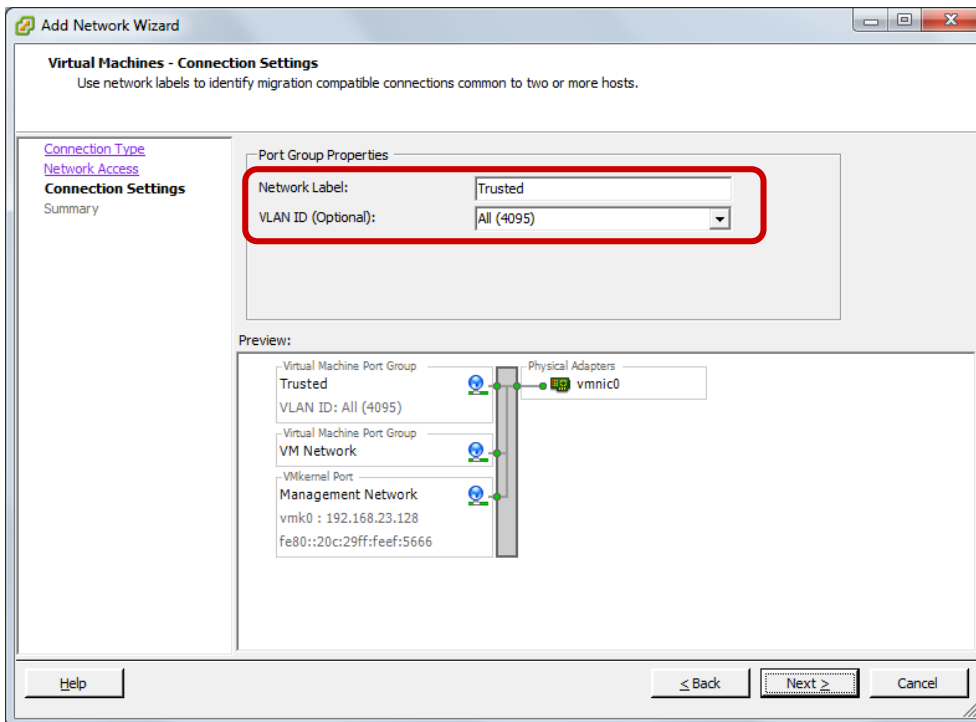
Virtual Machine を選択し、Next。



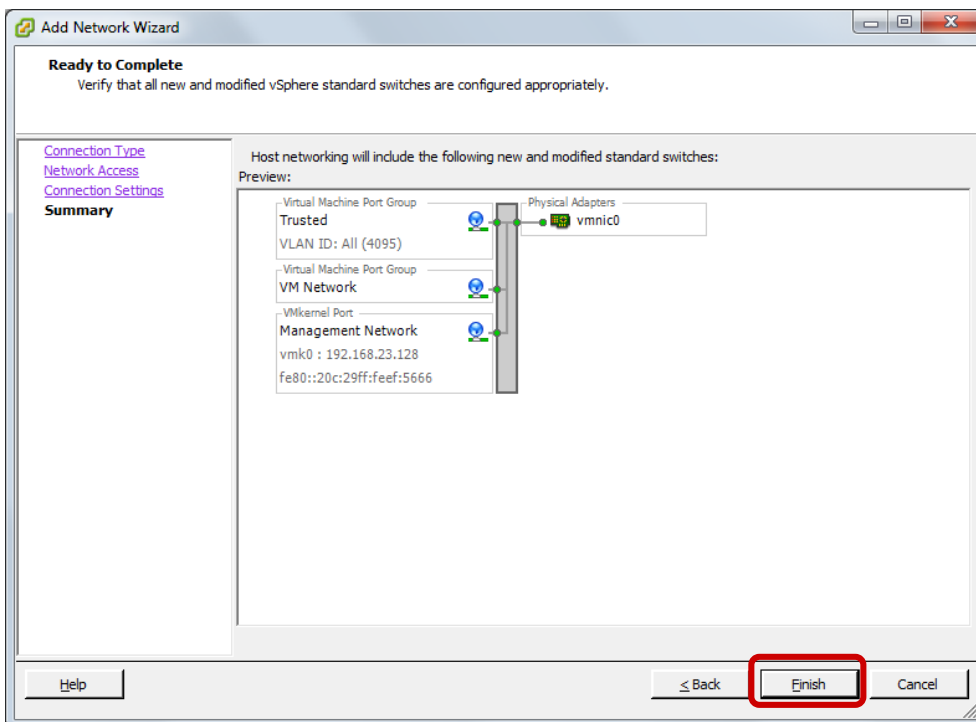
Use vSwitch0 (既存の vSwitch)を選択し、Next。



Network Label を Trusted、VLAN ID は All(4095)を選択し、Next。

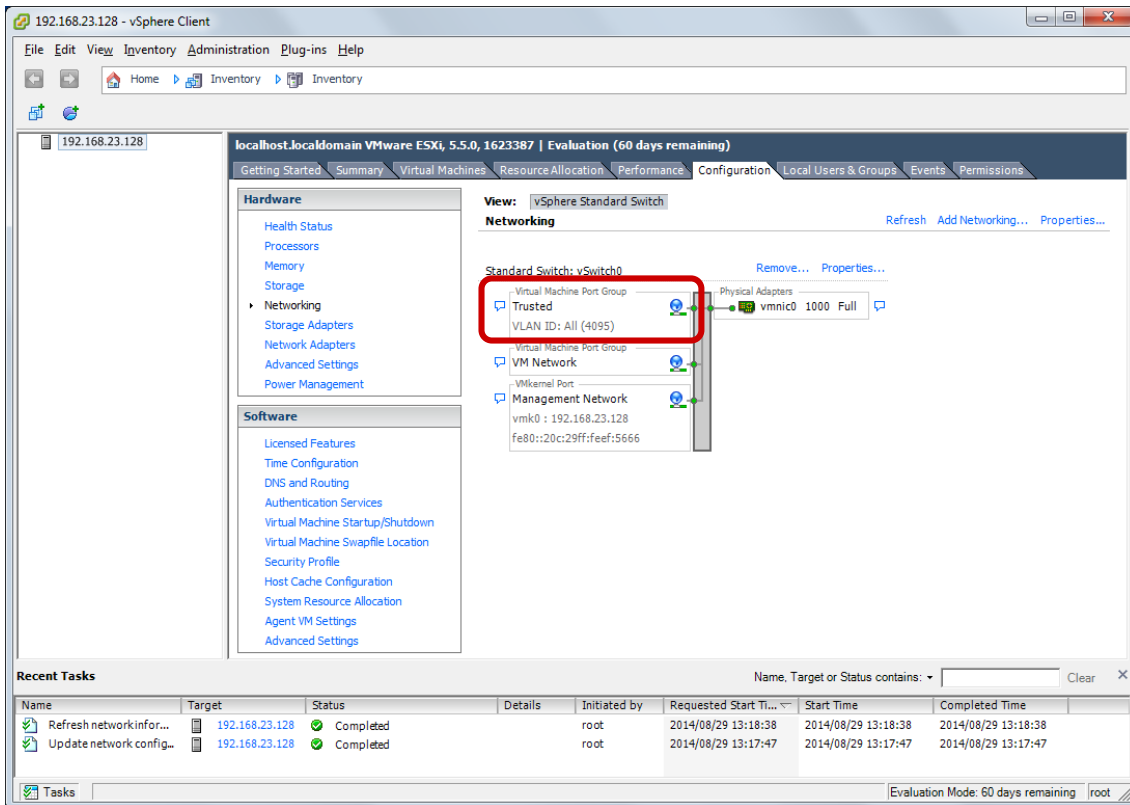


Finish をクリックして完了します。

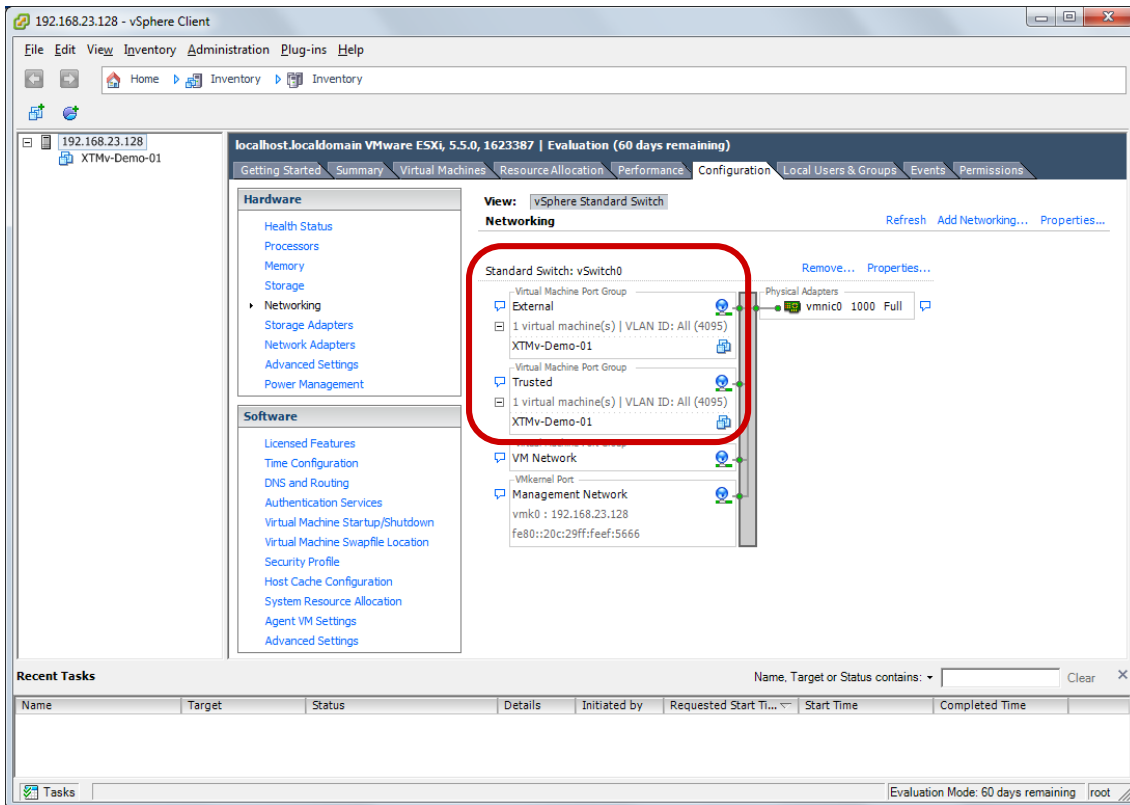




Trusted が追加されました。



同様の手順で External も追加します。追加後は以下ようになります。



以上です。

## おわりに

WatchGuard XTMv スタートアップガイドをご活用いただき、ありがとうございます。

本書を通して XTMv の導入がいかに容易か、実感していただけたと思います。

XTMv が御社のサービス可用性向上、管理の効率化、コスト削減、セキュリティ向上にお役に立てれば幸いです。