



Dimension

管理者ガイド



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	4
Dimension の導入.....	5
Dimension のデプロイ	5
デプロイ後	12
コンソール ログイン	12
IP アドレスの設定	13
初期セットアップ ウィザード	14
デバイスのログ送信設定	21
デバイスの設定	21
ポリシー単位でログを出力する設定	25
ユーザーの追加.....	28
読み取り専用ユーザーの作成.....	28
MSSP における運用	34
管理者メニュー リファレンス.....	42
管理者メニューについて.....	42
管理者メニューとは	42
モードの切り替え	43
Schedule Reports	44
レポートスケジュールの追加.....	44
Log Server Management.....	49
Status.....	49
Configuration	50
IP Address Mapping	56
Diagnostics	59
Database.....	61
Database Status	61
Process List.....	61
Log Messages.....	62

Status Report	62
User Management.....	64
ユーザーの追加	64
ユーザーの編集	67
ユーザーの削除	68
Active Directory を利用する	69
System Settings.....	70
Status.....	70
Configuration	73
Diagnostics	75
Dimension のアップグレード手順	78
事前準備	78
アップグレード手順	79
おわりに	81

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。

Dimension は、仮想マシン上に簡単に構築できる、セキュリティ可視化ツールです。

本書は、Dimension をすぐに始めることを目的としたスタートアップガイドであるとともに、Administration メニューの全項目を網羅した管理者リファレンスでもあります。

まずは導入がいかに容易か、ウォッチガードが提供する可視化がいかに簡単に実現できるか、さらには MSSP としてサービス展開が容易であり、いかにシンプルに管理できるかを実感していただければ幸いです。

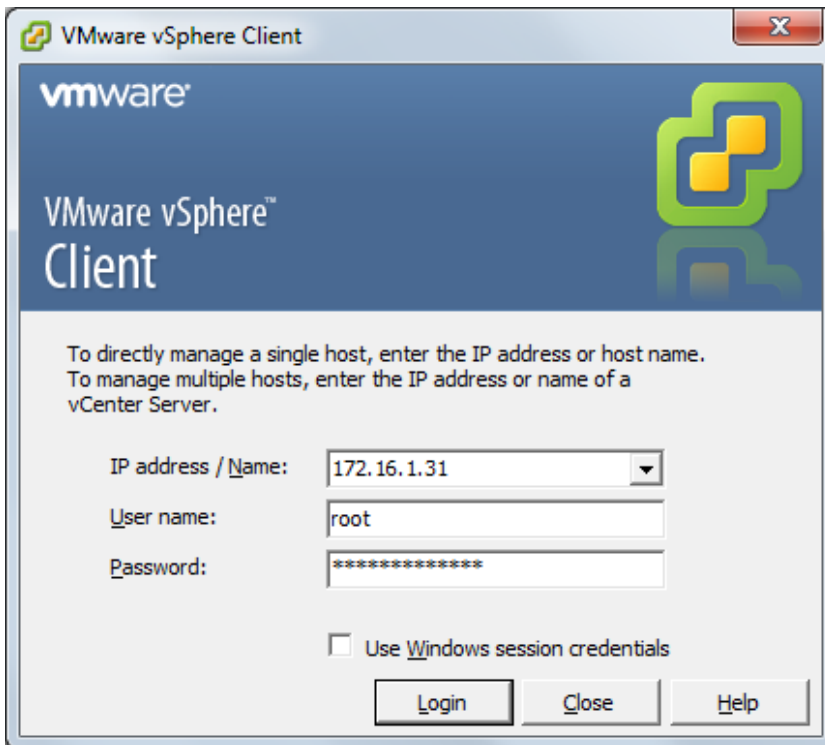
DIMENSION の導入

Dimension は VMWare と Hyper-V の両方に対応しています。

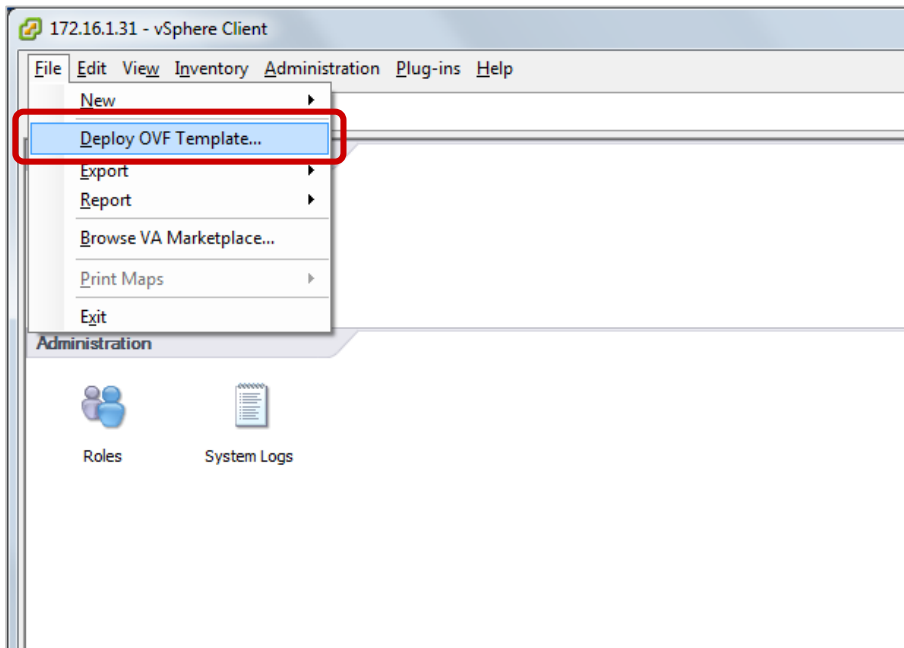
このガイドでは VMWare での導入方法を解説します。

Dimension のデプロイ

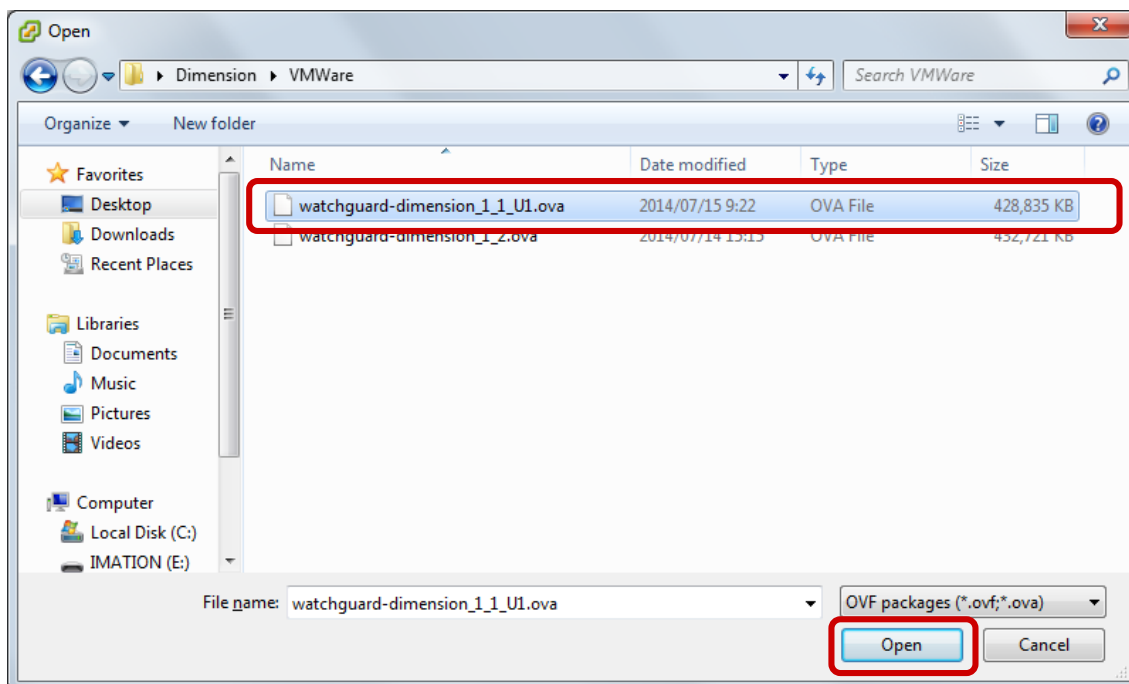
VMWare vSphere Client から VMWare サーバーに接続します。



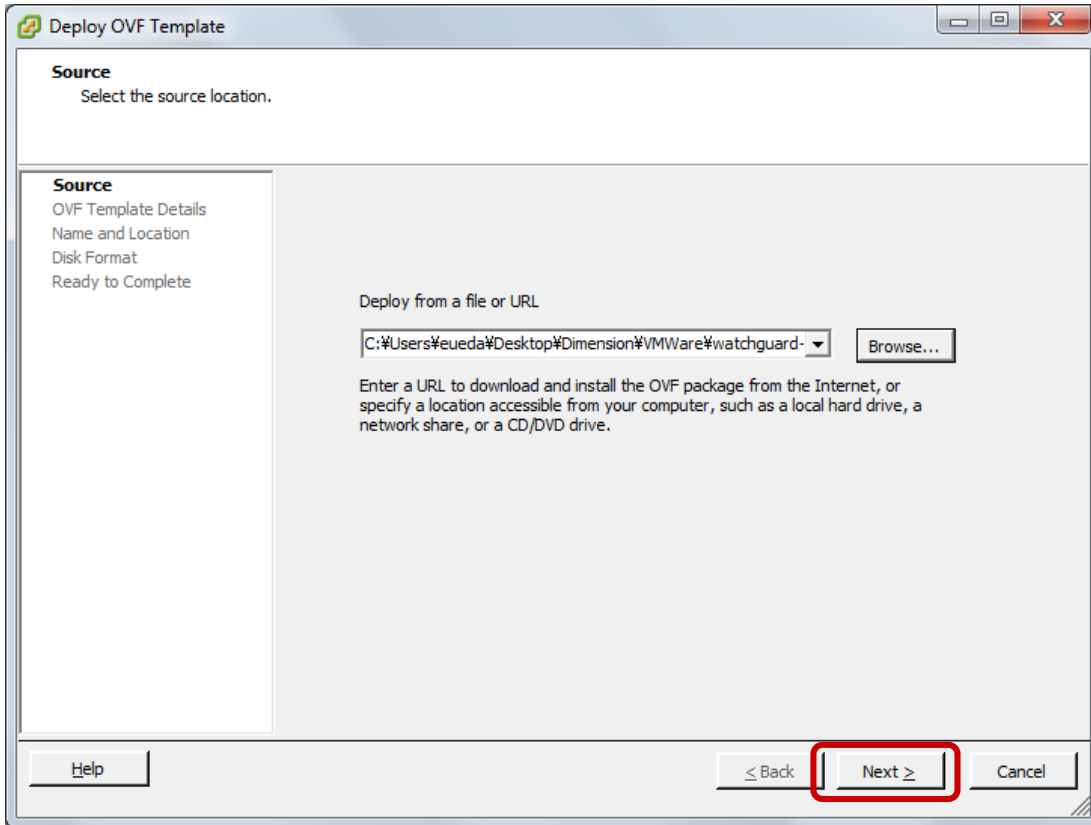
接続できたら、メニューの **File** - **Deploy OVF Template...** をクリックします。



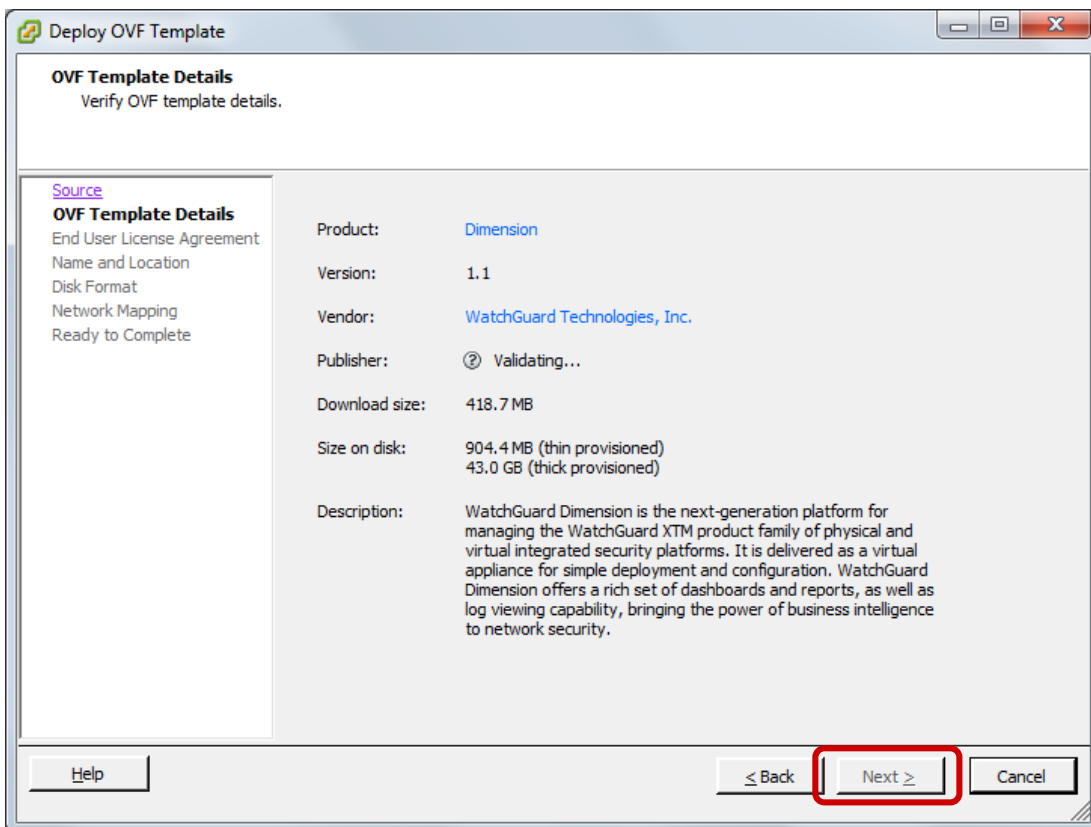
ダウンロードした OVA ファイルを指定し、Open をクリックします。



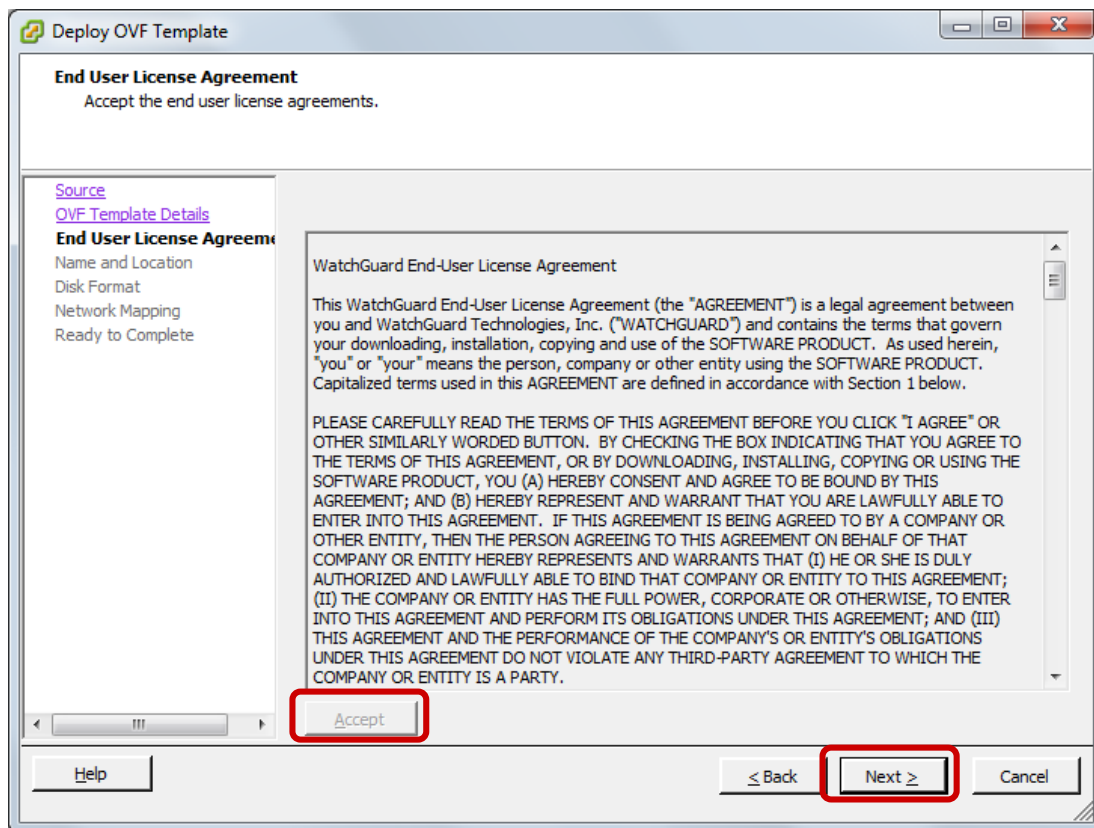
OVA ファイルのフルパスがテキストフィールドに入力されていることを確認し、Next をクリックします。



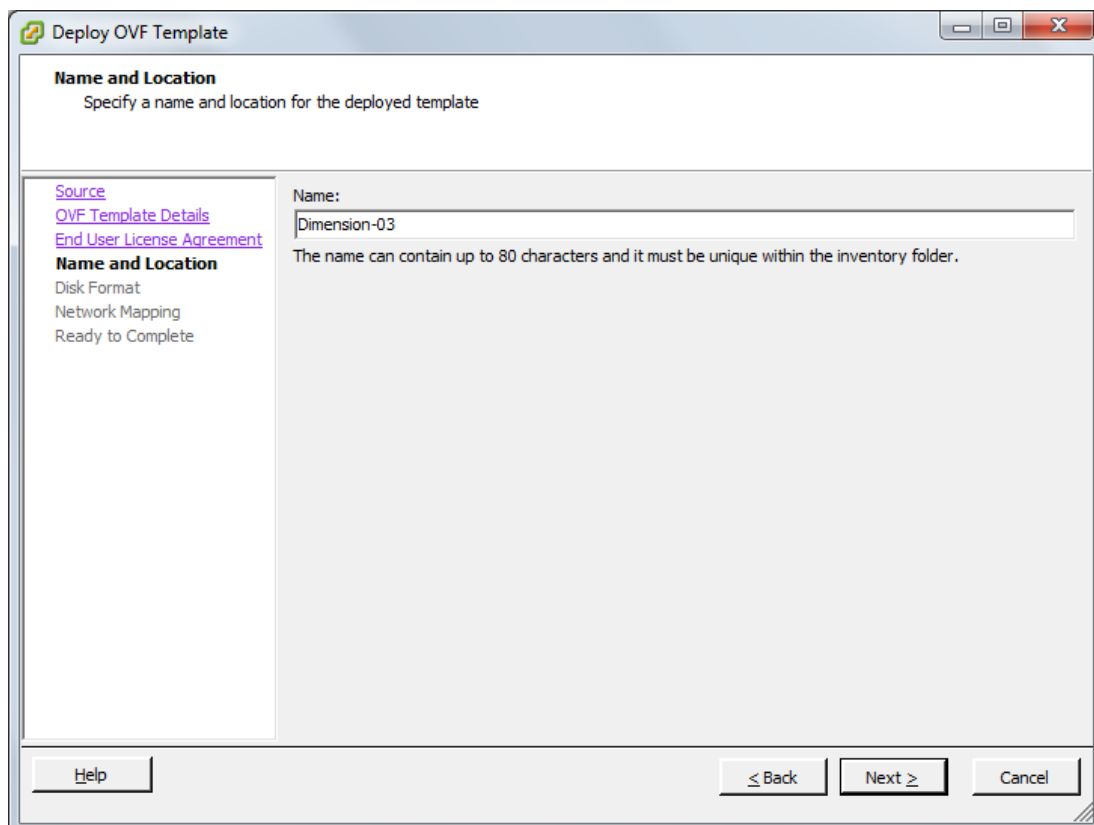
テンプレートの詳細情報が表示されるので、確認して Next をクリックします。



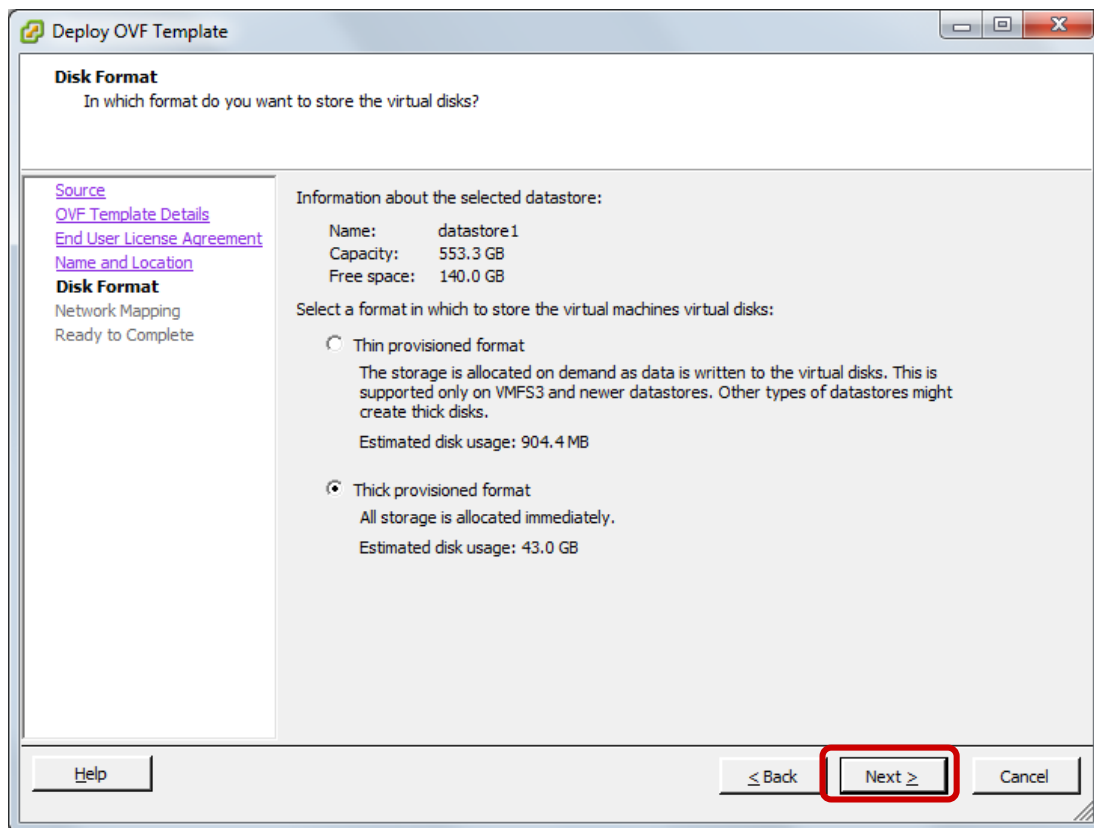
End User License Agreement は Accept ボタンをクリックして Next ボタンをクリックします。



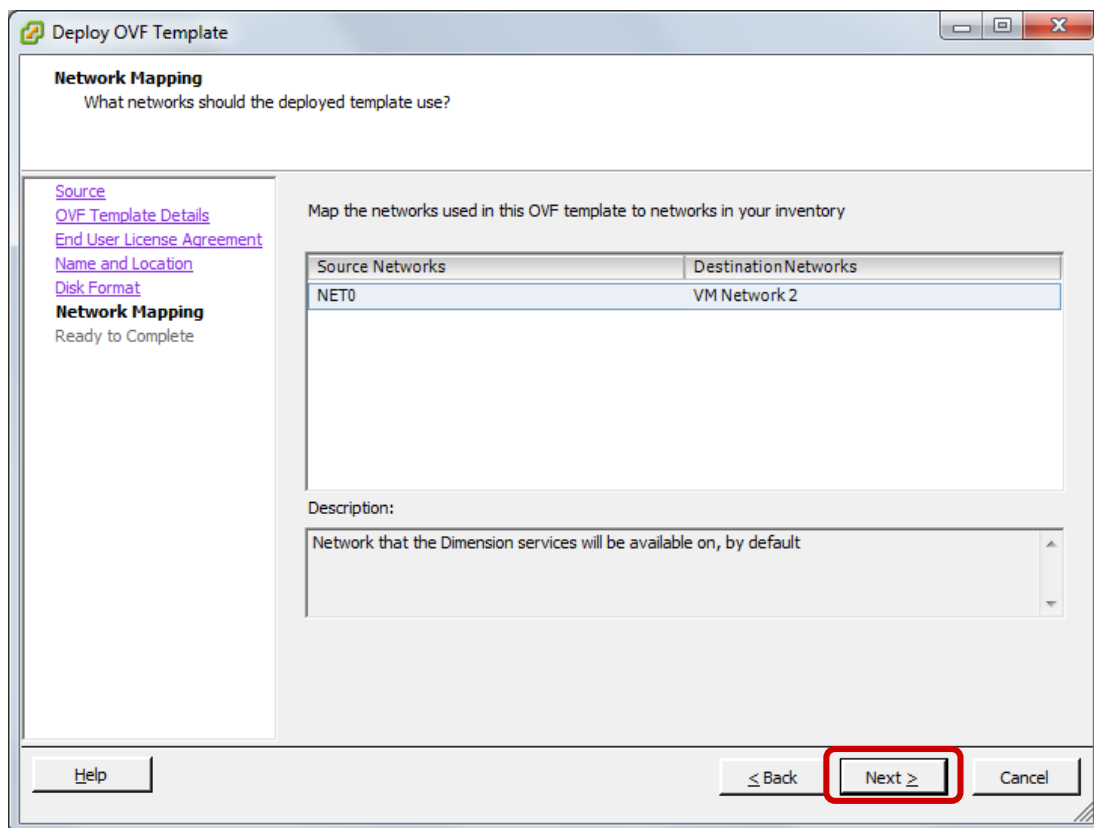
次にデプロイされる仮想マシンに名前を付けます。実際のサーバー名ではなく、vSphere Client 上のインベントリで表示される名前を入力します。



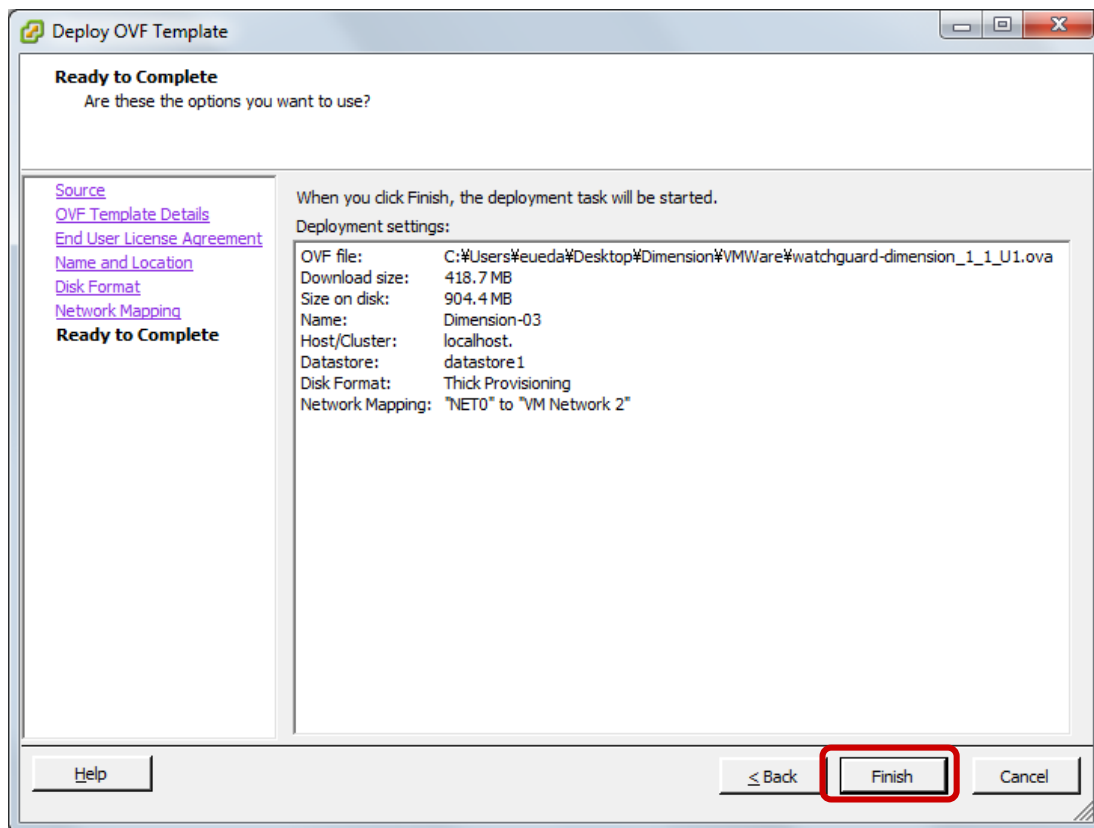
次にディスクの設定です。どちらかを選択して次へ進みます。Thick プロビジョニングが推奨です。



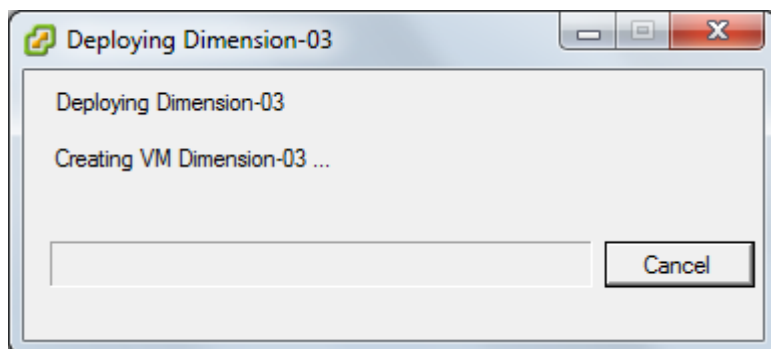
次にネットワーク・インターフェースの設定です。複数のインターフェースがある場合は、どのインターフェースにバインドするか選択する必要があります。



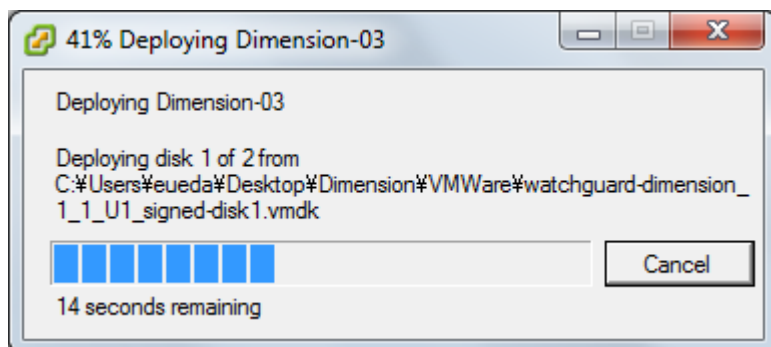
次に進むと、設定のサマリーが表示されますので、確認して次に進みます。



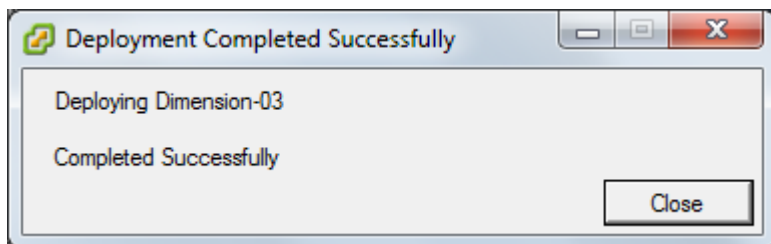
デプロイが始まります。



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みてください。

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:\Dimension\watchguard-dimension_1_1_U1.ova C:\Dimension\watchguard-  
dimension_1_1_U1.ovf  
  
Opening OVA source: C:\Dimension\VMWare\watchguard-dimension_1_1_U1.ova  
  
The manifest validates  
  
Source is signed but could not verify certificate (possibly self-signed)  
  
Opening OVF target: C:\Dimension\VMWare\watchguard-dimension_1_1_U1.ovf  
  
Writing OVF package: C:\Dimension\VMWare\watchguard-dimension_1_1_U1.ovf  
  
Transfer Completed  
  
Completed successfully
```

OVFTOOL の入手先:

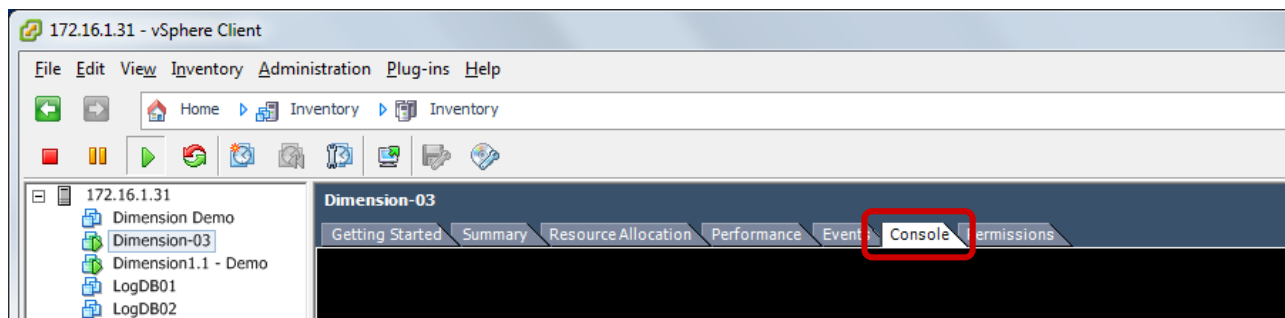
<https://my.vmware.com/jp/web/vmware/details?productId=352&downloadGroup=OVFTOOL350>

デプロイ後

コンソール ログイン

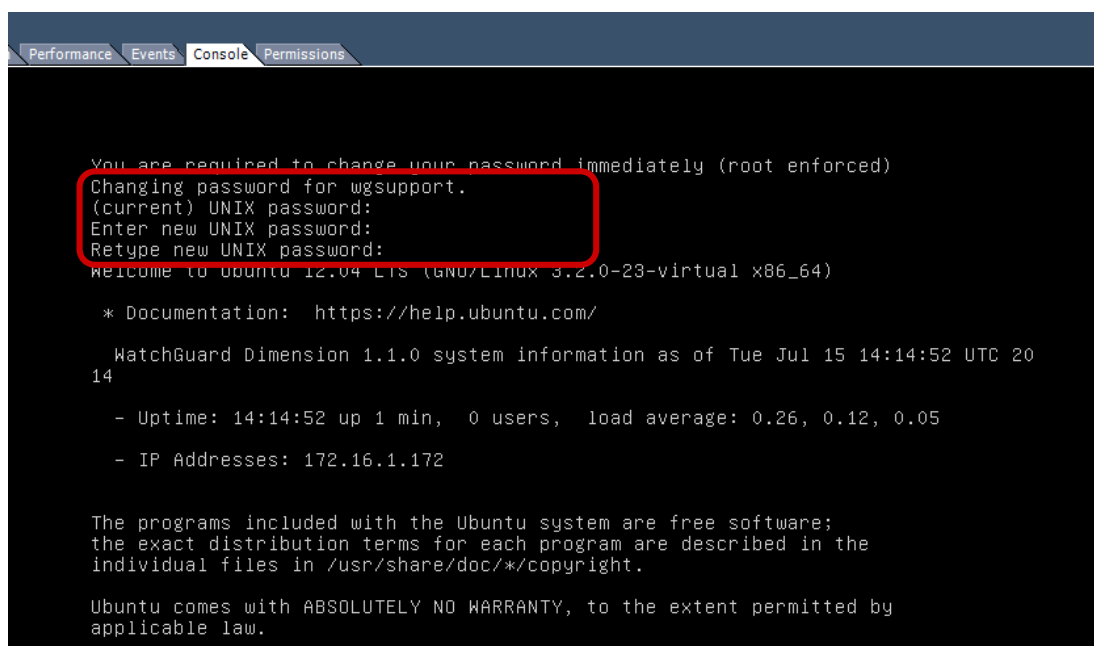
デプロイした仮想マシンを選択し、Power On します。

仮想マシンのコンソールタブを選択すると、起動する様子が確認できます。



コンソールにログインするには、ログインに wgsupport、初期パスワードは readwrite を入力します。

ログインするとすぐにパスワード変更が促されますので、旧パスワードと新パスワードを入力します。



この後、Dimension にウェブブラウザでアクセスして、初期設定を行ないます。

アクセスする方法は 2 種類あります。

1. VMWare のコンソールから Dimension のコマンドラインで IP アドレスを静的なものに設定し、その IP アドレスでアクセスすることができます。
2. DHCP サーバーが存在していれば、Dimension は起動した段階で IP アドレスを自動取得します。自動取得した IP アドレスにブラウザでアクセスすれば、セットアップウィザードを実行できます。また、そのウィザード中に IP アドレスを静的なものに設定することもできます。

IP アドレスの設定

IP アドレスを設定するには、Dimension の付属コマンドを利用します。コマンドラインの文法は以下のとおりです。

```
/opt/watchguard/dimension/bin/wg_ip_addr.sh -i IPアドレス -m ネットマスク(ビット指定) -g  
ゲートウェイ
```

実行例:

```
wgsupport@localhost:~$ /opt/watchguard/dimension/bin/wg_ip_addr.sh -i 172.16.1.1  
83 -m 24 -g 172.16.1.1  
Method: Static IP  
Static IP: 172.16.1.183  
Mask: 24  
Gateway: 172.16.1.1  
wgsupport@localhost:~$ _
```

vSphere Client の Summary タブを選択すると、IP アドレスはコマンドで設定したものになっていることを確認できます。

The screenshot shows the vSphere Client interface for a virtual machine named "Dimension-03". The "Summary" tab is selected, displaying various system details. The "IP Addresses" field is highlighted with a red box, showing the value "172.16.1.183". Other visible details include the Guest OS (Ubuntu Linux (64-bit)), VM Version (7), CPU (2 vCPU), Memory (2048 MB), and State (Powered On). The "Resources" section shows host CPU and memory usage, and the "Network" section shows the VM is connected to "VM Network 2".

Field	Value
Guest OS	Ubuntu Linux (64-bit)
VM Version	7
CPU	2 vCPU
Memory	2048 MB
Memory Overhead	110.62 MB
IP Addresses	172.16.1.183
State	Powered On
Host	localhost
Active Tasks	

Consumed Host CPU	9 MHz
Consumed Host Memory	353.00 MB
Active Guest Memory	0.00 MB
Provisioned Storage	45.00 GB
Not-shared Storage	43.00 GB
Used Storage	43.00 GB

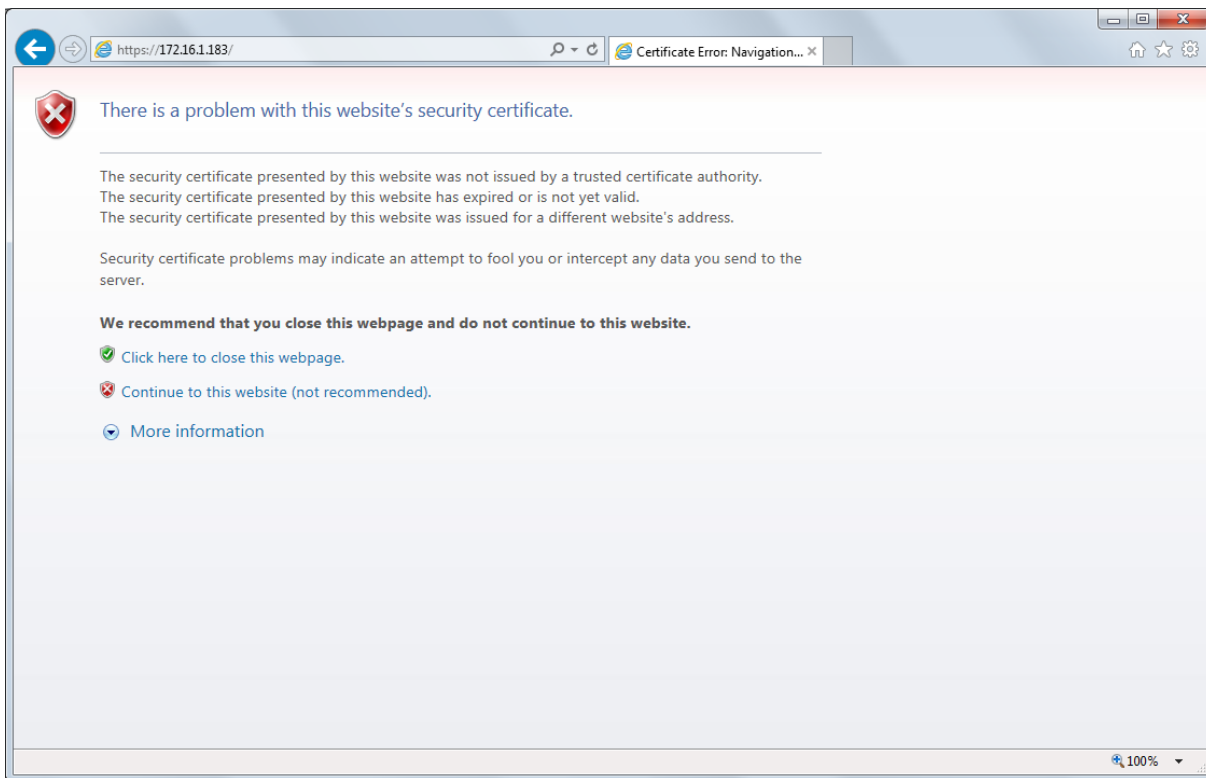
Network	Type
VM Network 2	Standard switch network

初期セットアップ ウィザード

ウェブブラウザで、Dimension に接続します。IP アドレスは DHCP で取得したもの、もしくはコンソールからコマンドで設定したならその IP アドレスを使います。

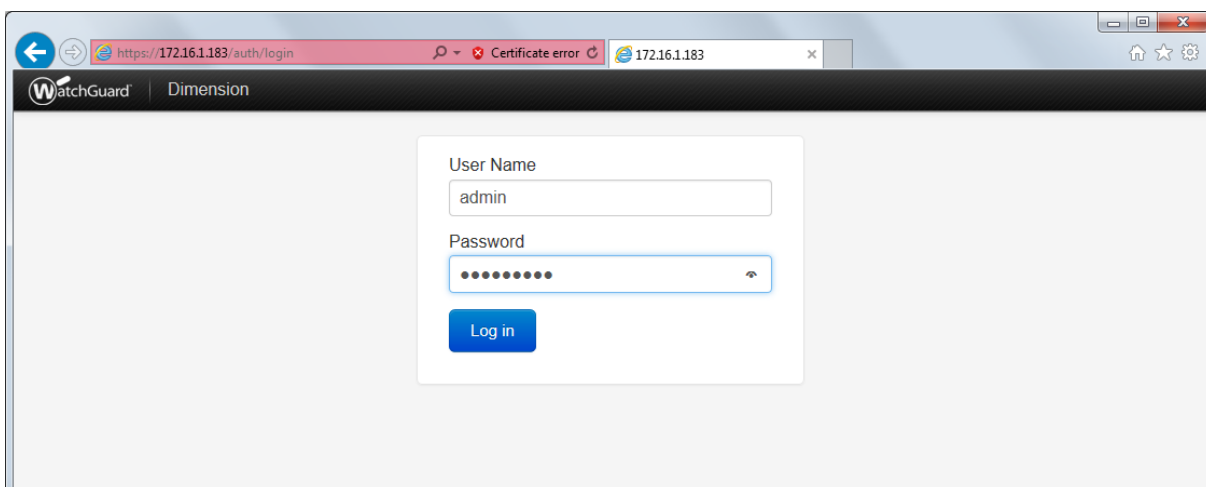
https://<IP アドレス>

証明書の警告が表示されますが、続けます。



ログイン画面になります。

User Name は admin、Password(初期) は readwrite を入力し、ログインします。



ログイン後、すぐに Setup Wizard が始まります。Next をクリックします。

WatchGuard Dimension Setup Wizard

Before you begin, make sure you have this information:

Setting up the System

1. Host name for Dimension
2. IPv4 address settings for eth0 interface

Setting up the Log Server

1. Administrator passphrase
2. Log Encryption Key

Do not power off Dimension before the Setup Wizard completes.

ホスト名、IP アドレス、ネットマスク、デフォルトゲートウェイ、DNS サーバー、ドメイン名(必要に応じて)を入力し、Next をクリックします。

System Information

Host Name

IP Address Method

IPv4 Address / Mask /

Default Gateway

DNS Server

Domain Name (Optional)

We recommend that you specify a static IPv4 address for Dimension. This is the default IP address that you use to connect to Dimension.

Admin ユーザー(管理者)のパスワードを変更します。

Set Administrator Passphrase

Administrator User Name

Administrator Passphrase

Confirm Passphrase

The Administrator passphrase gives you read-write access to Dimension, so you can modify your settings. The Administrator passphrase must have at least 8 characters.

ログサーバーの暗号化キーを入力します。

これはデバイスからログサーバーに送信する設定に必要なになります。

Log Server Settings

Encryption Key

Confirm Encryption Key

The Encryption key is used to establish a secure connection between your Dimension Log Server and your XTM devices or WatchGuard servers.

最後に設定のサマリーが表示されますので、確認します。

Review Dimension Settings

System Information	Host name: logsrv03 IPv4 address: 172.16.1.100/24 Default Gateway: 172.16.1.1 DNS Server: 172.16.1.10 Domain Name: domain.name
Administrator Passphrase	Administrator passphrase set
Log Server	Encryption key set Database location: /var/opt/watchguard/dimension/data/db

Review your settings. To change any settings, click **Back**. You cannot make changes after you click **Next**.

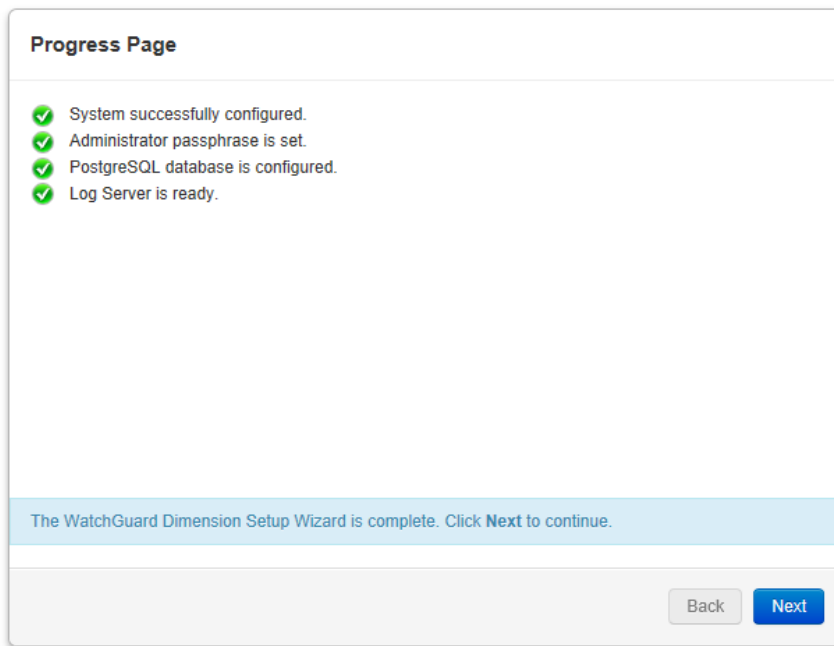
Next をクリックすると、システム設定やデータベース、ログサーバーの設定が行われます。

Progress Page

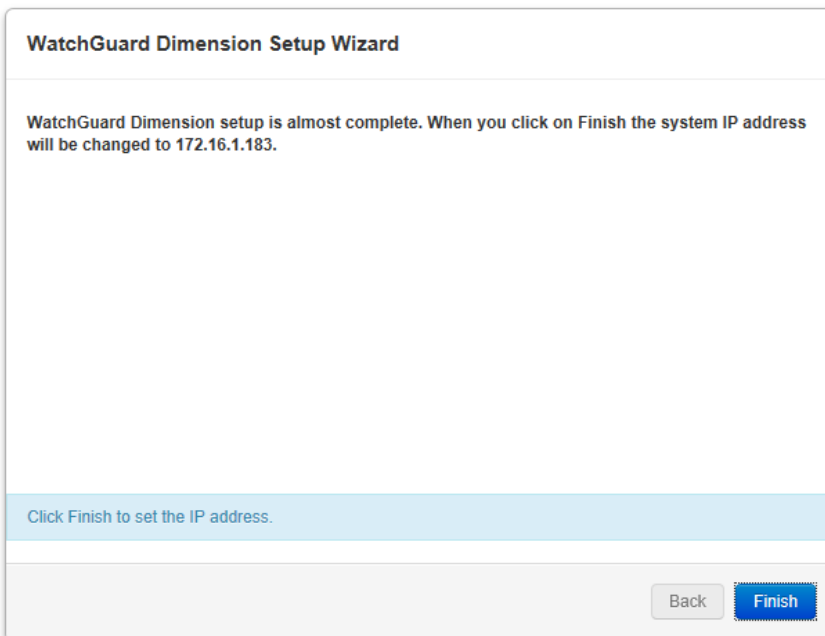
- ✔ System successfully configured.
- ✔ Administrator passphrase is set.
- PostgreSQL database
- Log Server

WatchGuard Dimension setup is in progress.
Do not power off Dimension before the Setup Wizard completes.

処理が最後まで進んだら Next をクリックします。



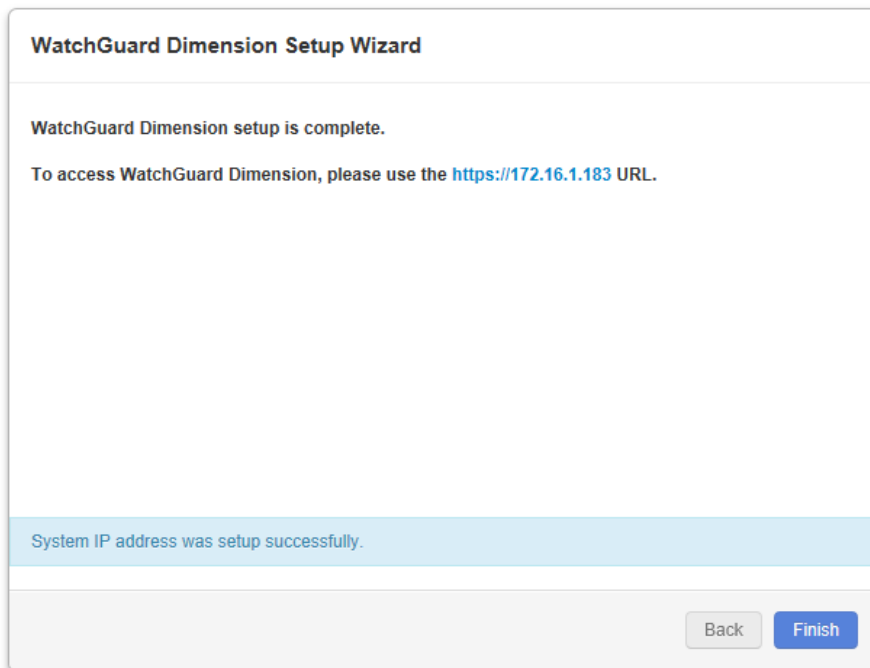
Finish ボタンをクリックします。



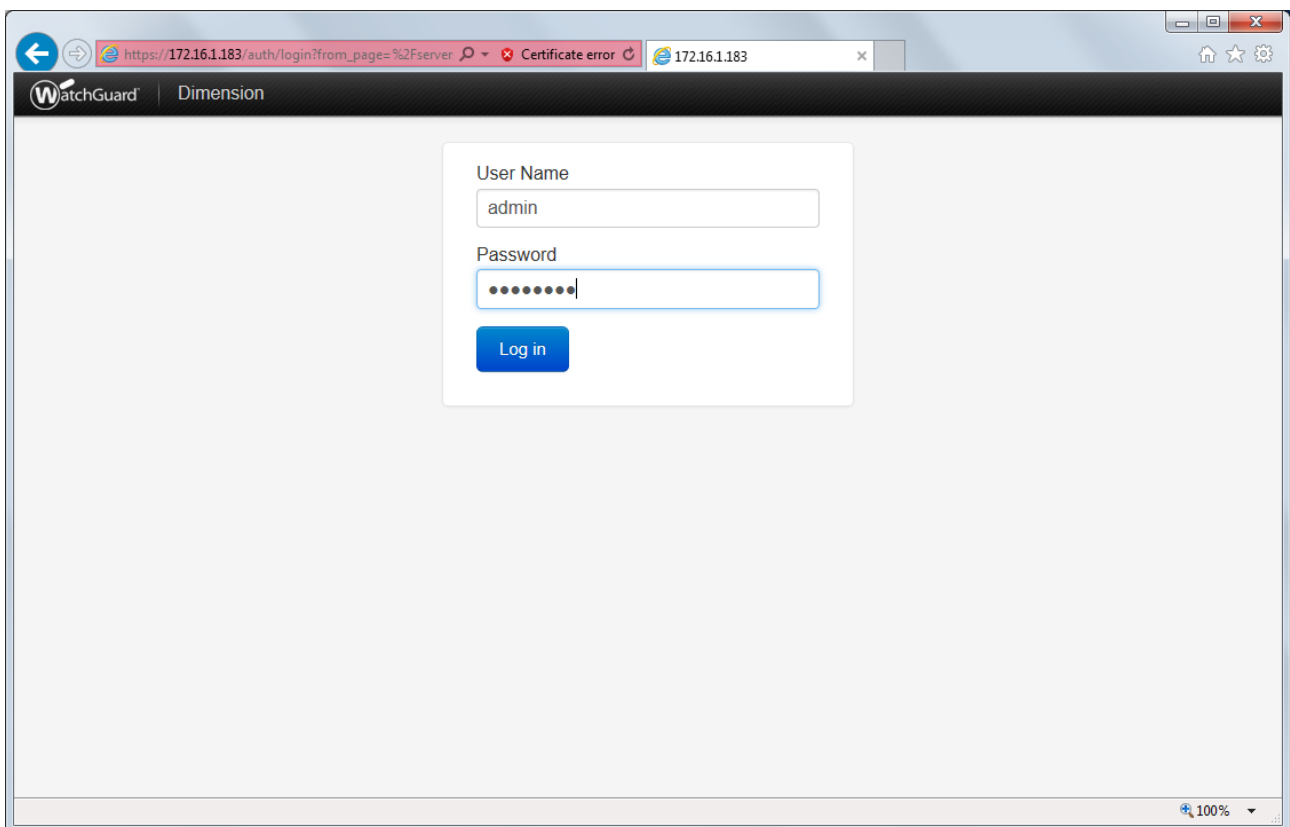
Setup Wizard の最後の画面になります。

To access WatchGuard Dimension, please use the <https://<設定後の IP アドレス>> URL.
と表示されます。

Dimension の仮想マシンは再起動しなくても、Wizard で設定した内容が反映されます。

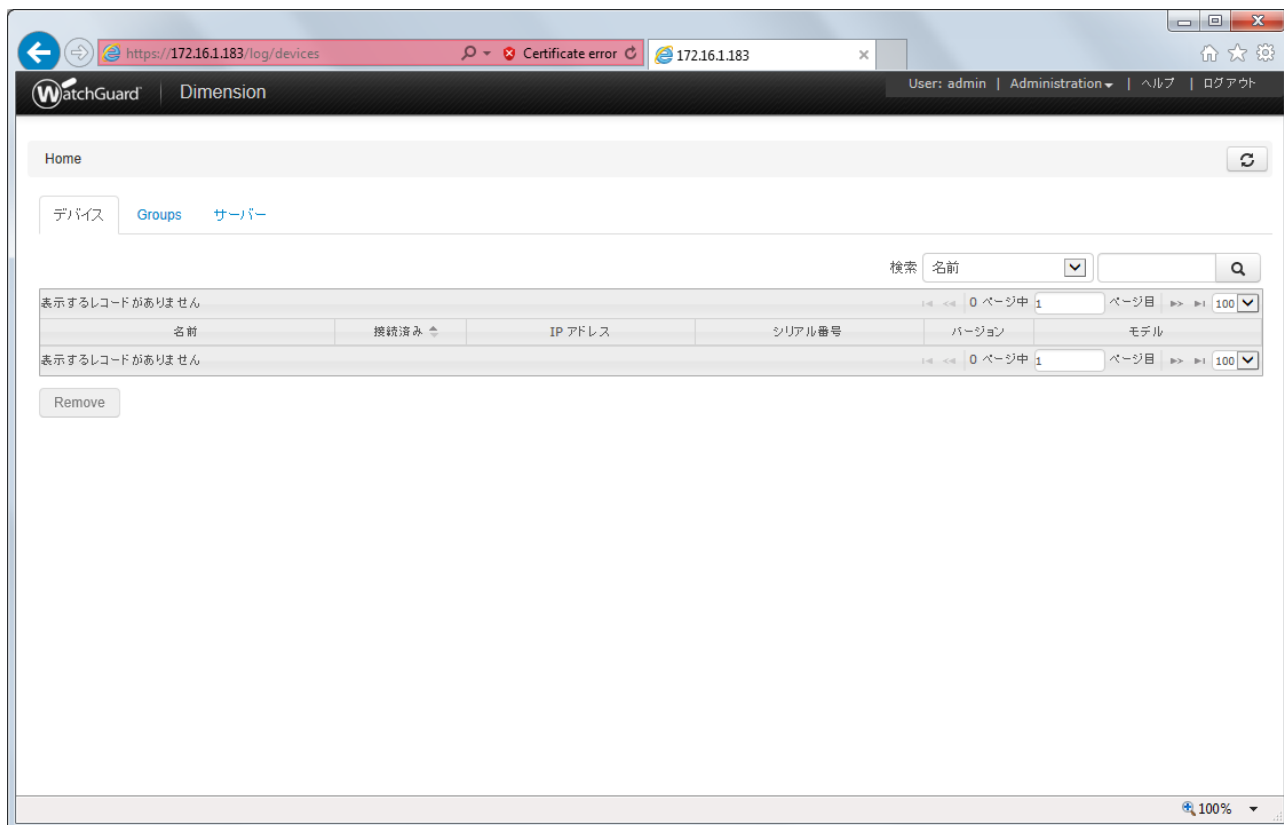


設定した URL にアクセスするとログイン画面が表示されますので、admin アカウントでログインします。



ログインすると Dimension の Home ページになり、デバイス一覧が表示されます。

Setup Wizard 後はまだ登録されているデバイスがないので、何も表示されていない状態です。



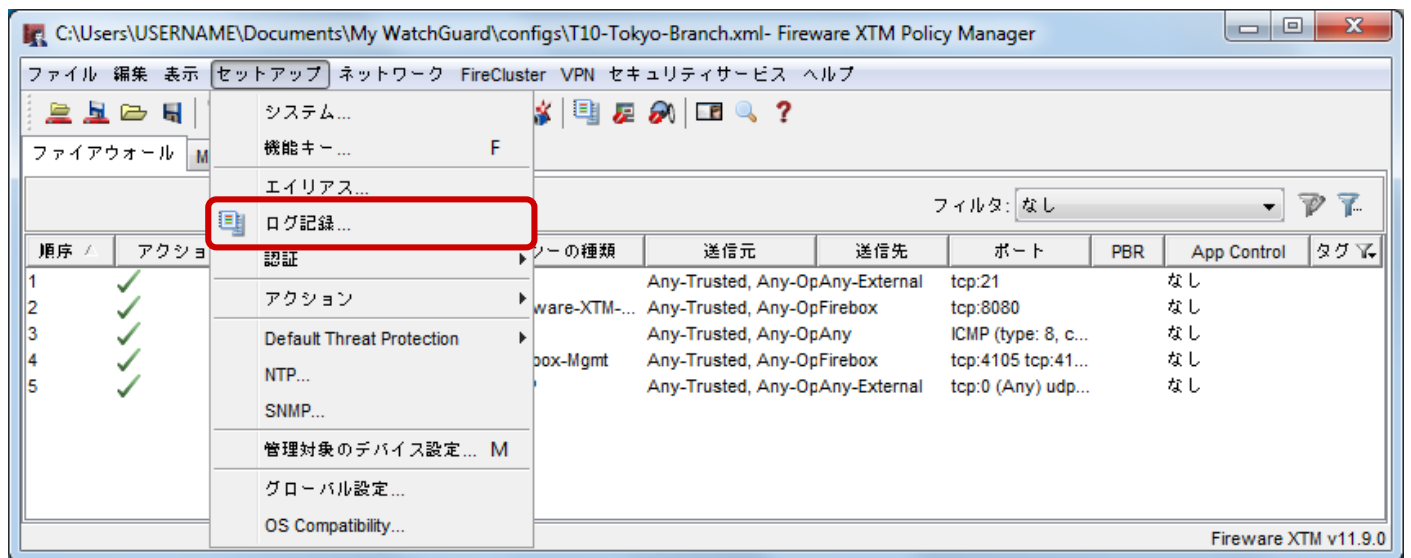
デバイスのログ送信設定

Dimension の設定が完了したら、さっそくデバイスからログを送信してみましょう。

デバイスの設定

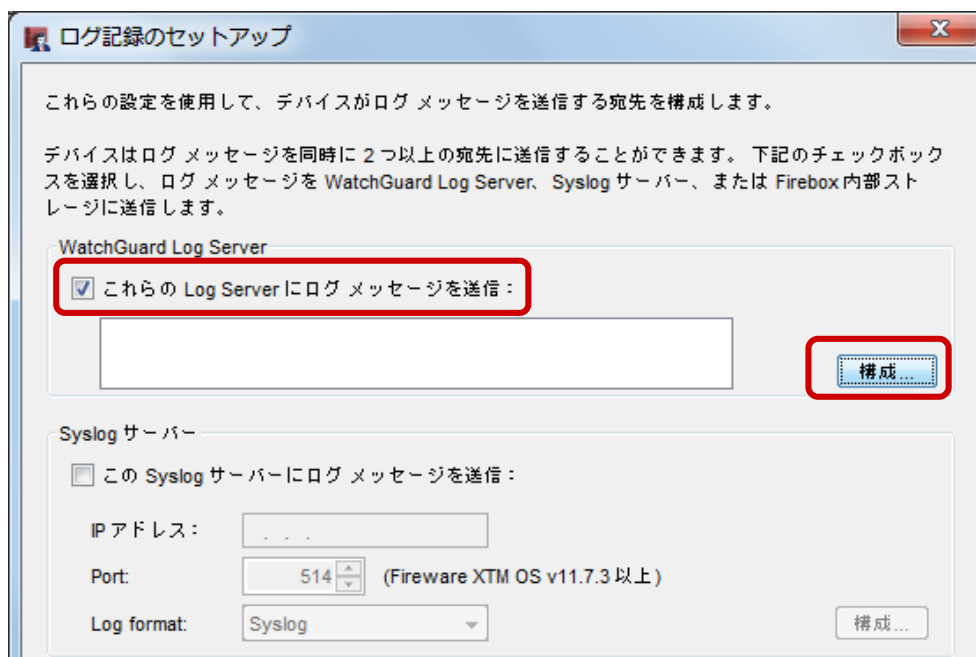
デバイス側で Dimension のログサーバーを指定して、ログを送信する設定が必要です。

メニューから、**セットアップ** – **ログ記録** をクリックします。

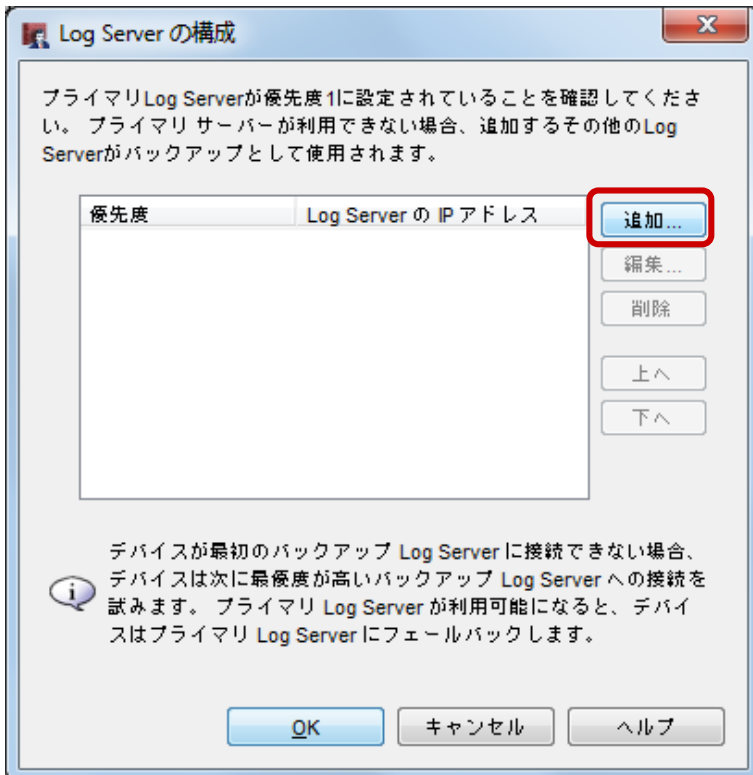


ログ記録のセットアップ画面が表示されます。

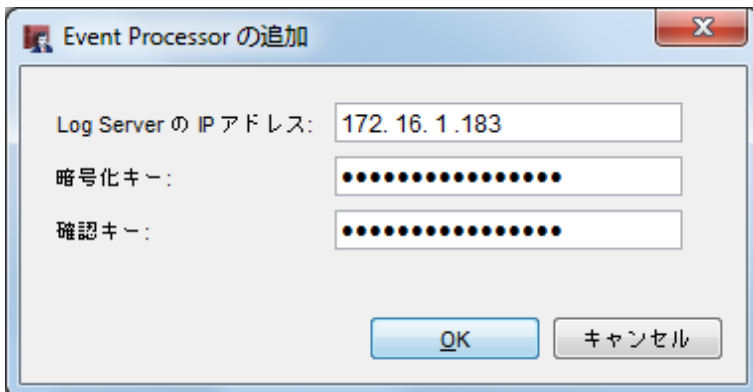
「これらの Log Server にログ メッセージを送信:」にチェックをし、構成ボタンをクリックします。



Log Server の構成画面で追加ボタンをクリックします。

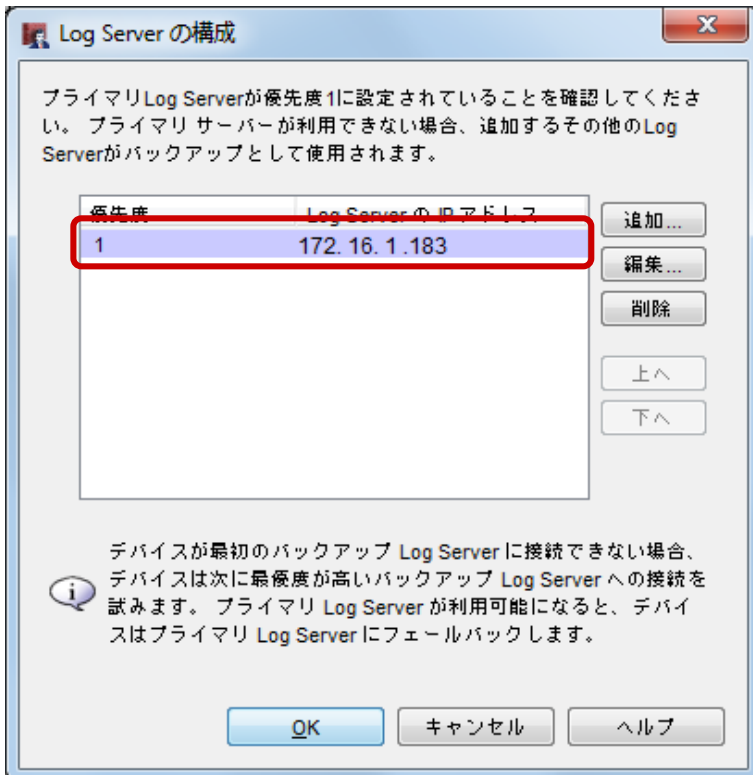


Log Server の IP アドレスと暗号化キーを入力します。

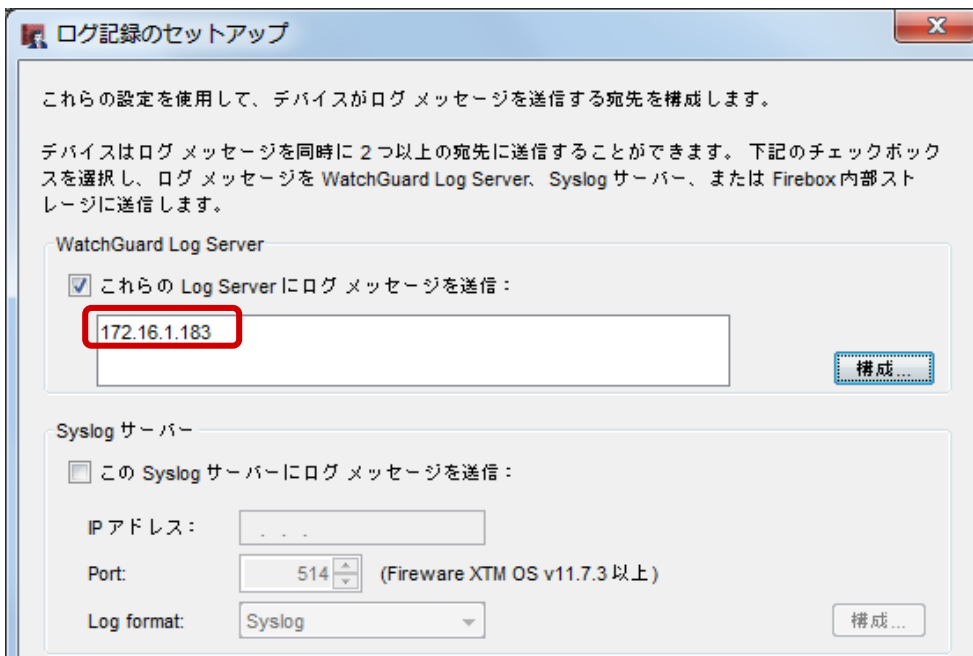


入力したら、OK をクリックして、前の画面に戻ります。

Log Server の構成の画面に戻ると、Log Server が追加されていることが確認できます。

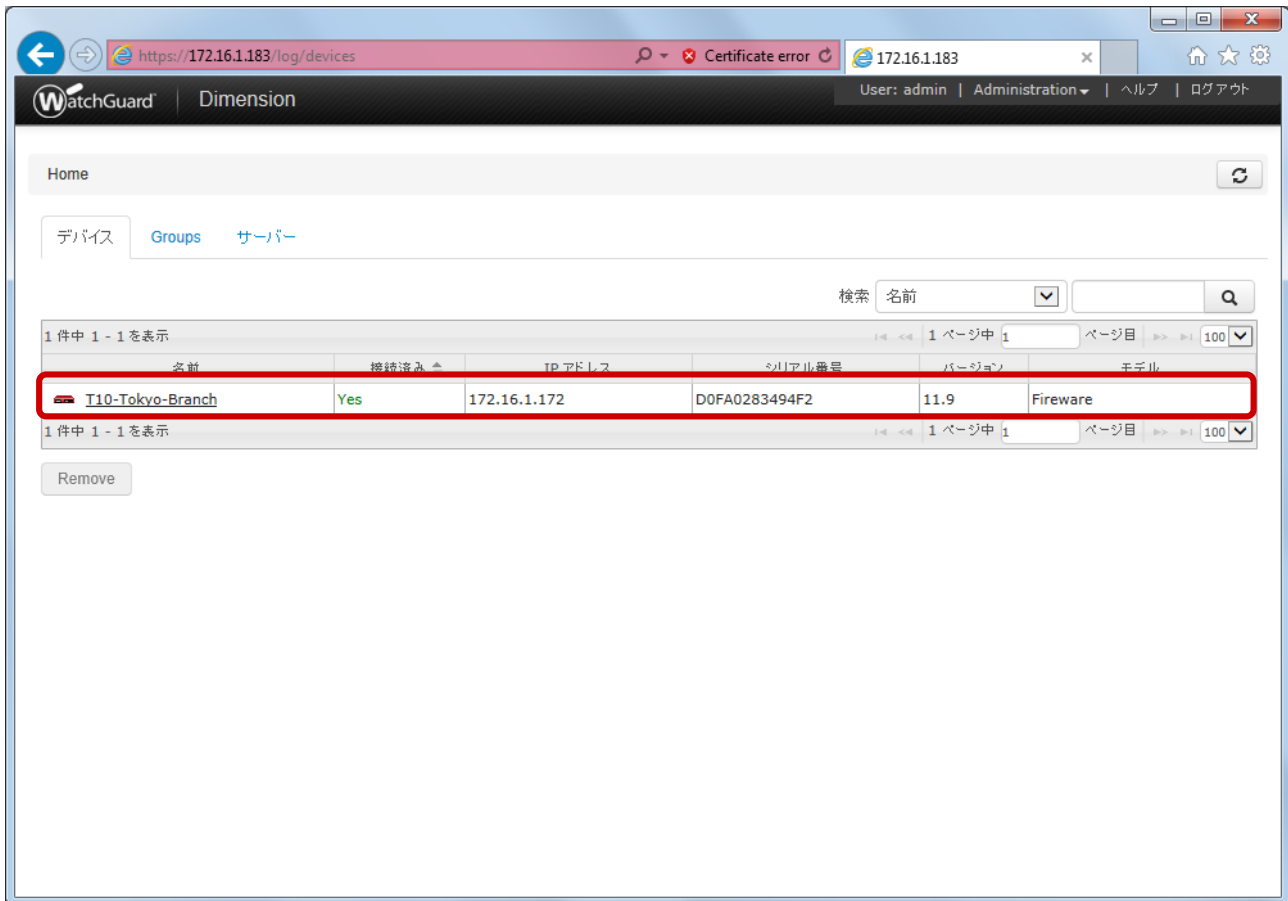


OK をクリックし、ログ記録のセットアップの画面に Log Server の IP アドレスが登録されていることが確認できます。



ログサーバーにログを送信する設定をしたら、設定を本体に保存してください。

しばらくして Dimension にログインすると、Home のデバイス一覧に設定したデバイスが見えてきます。



デバイスが表示されない場合。

IP アドレスの指定を間違えるとデバイスは Dimension と通信ができません。また、暗号化キーを間違えると接続が拒否され、デバイスが表示されません。

もう一度確認の上、再度設定してください。

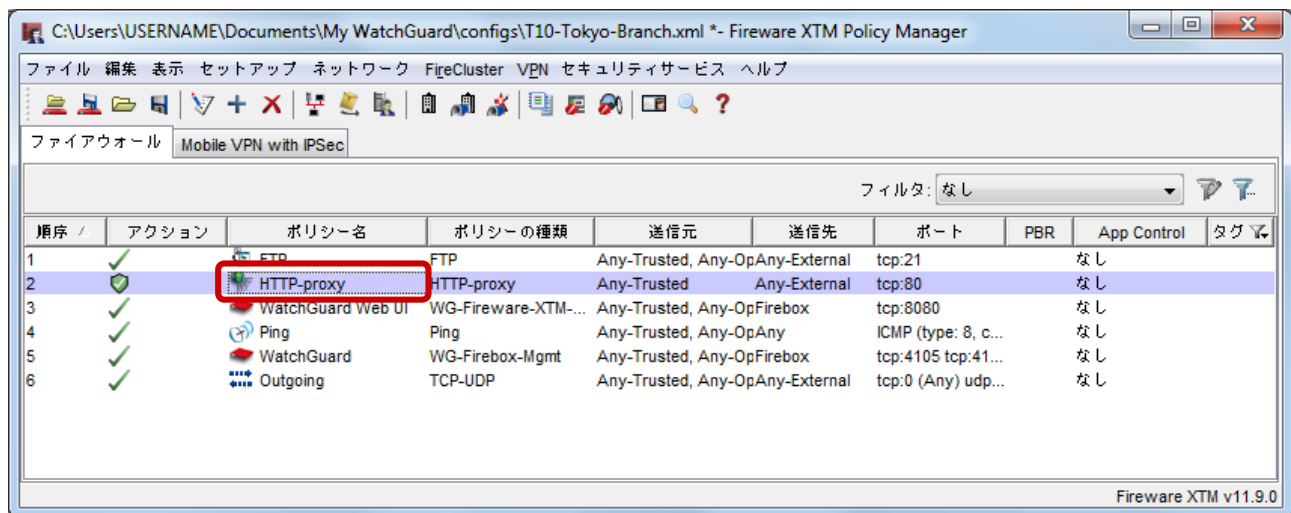
ポリシー単位でログを出力する設定

デバイスに設定されているポリシーは、標準のままだとログを送信しません。

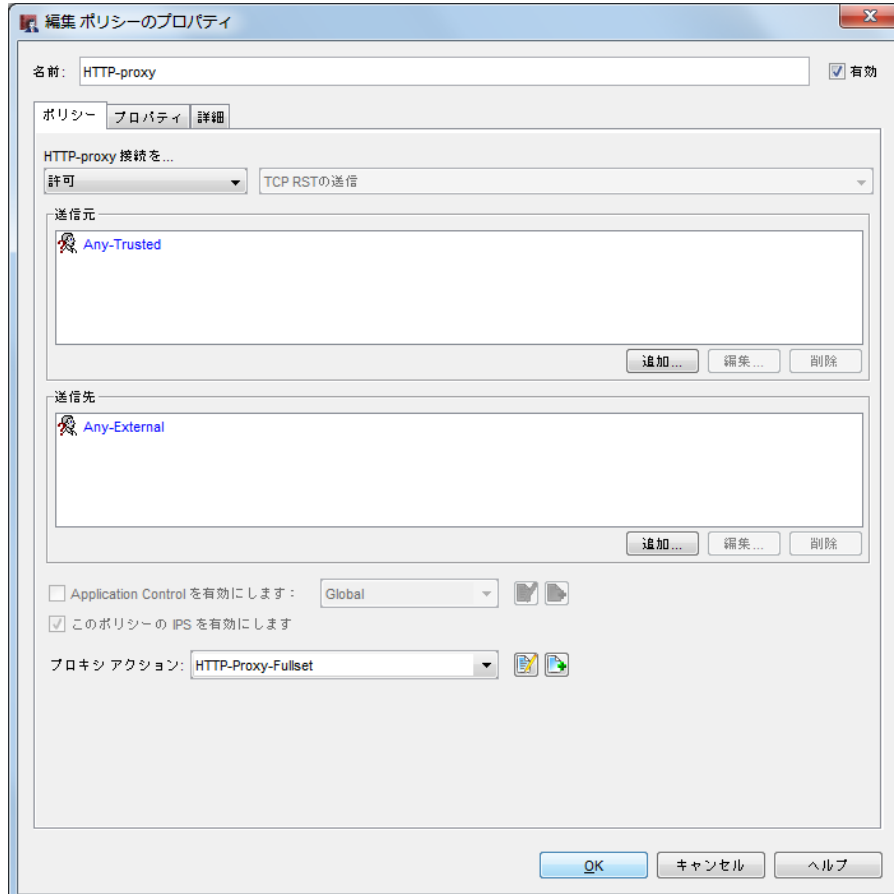
ログを取ってレポート化したいポリシーに、ログを送信する設定をする必要があります。

たとえば Web 経由でどんな脅威があり、どのように XTM が動作したかのログを取りたいければ、デバイス側で以下のように設定します。

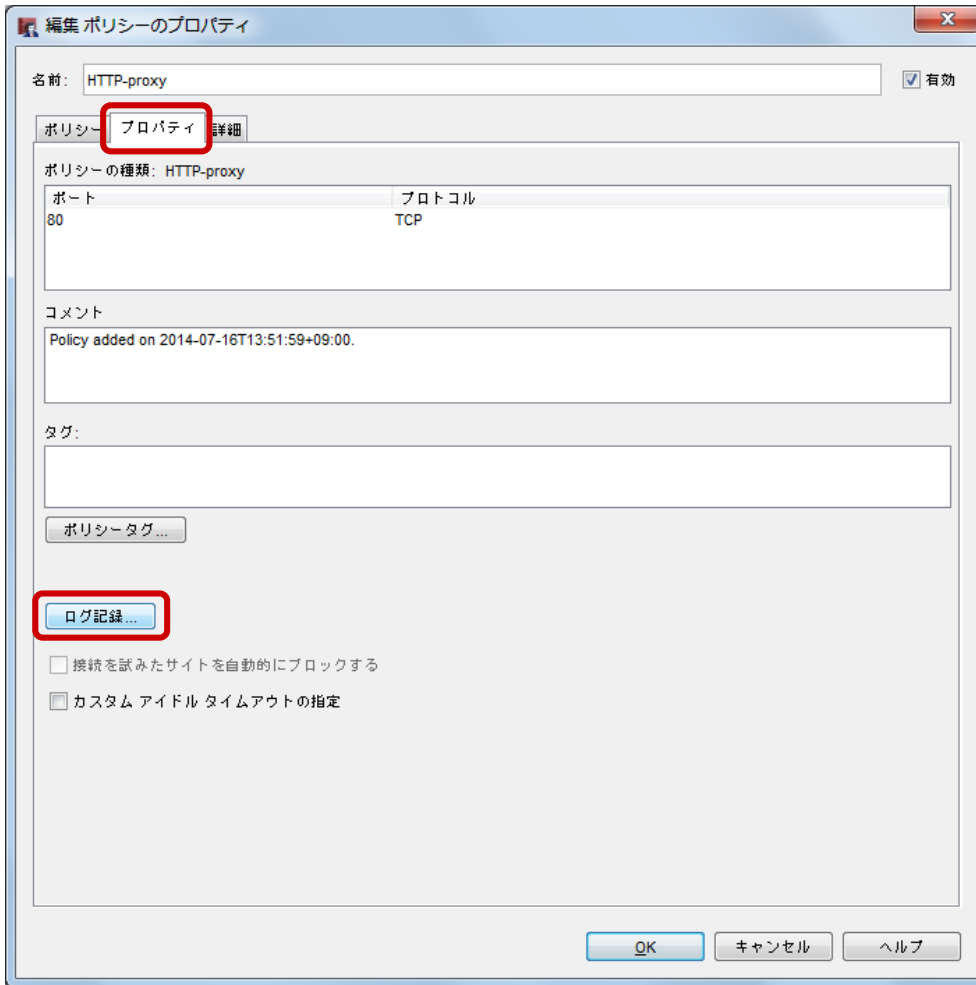
HTTP-proxy をダブルクリックし、ポリシーのプロパティ画面を開きます。



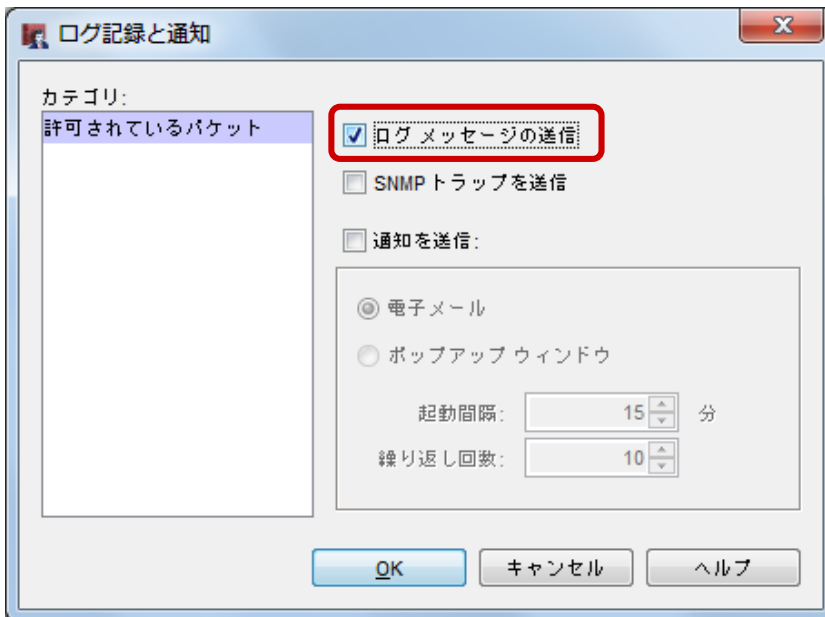
プロパティ画面。



プロパティ タブを選択し、ログ記録ボタンをクリックします。

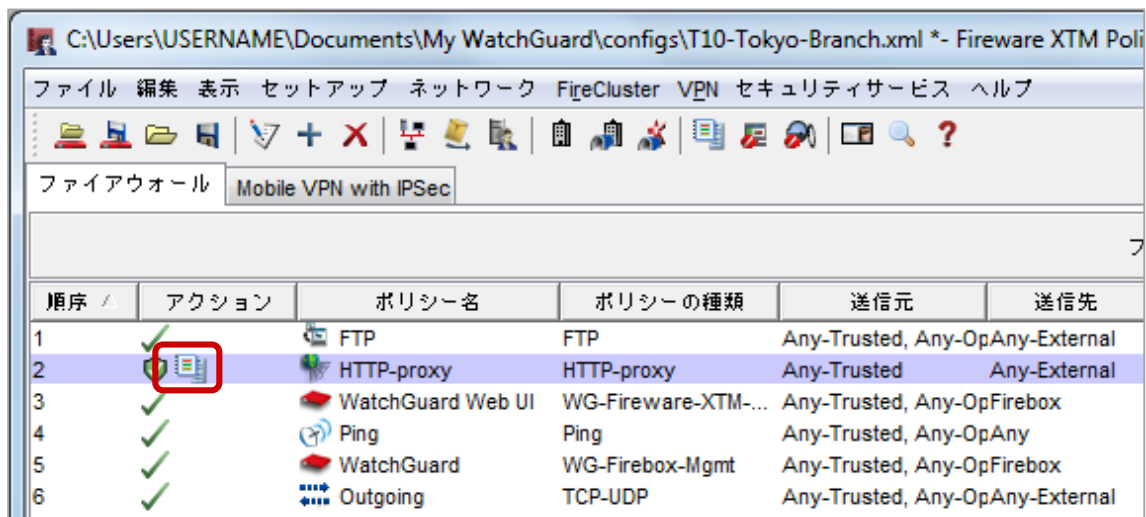


ログメッセージの送信にチェックを入れます。



OK で抜けてポリシーマネージャに戻ります。

一覧にはログ記録が有効になったことを示すアイコンが表示されます。



順序	アクション	ポリシー名	ポリシーの種類	送信元	送信先
1	✓	FTP	FTP	Any-Trusted, Any-Op	Any-External
2	📄	HTTP-proxy	HTTP-proxy	Any-Trusted	Any-External
3	✓	WatchGuard Web UI	WG-Fireware-XTM-...	Any-Trusted, Any-Op	Firebox
4	✓	Ping	Ping	Any-Trusted, Any-Op	Any
5	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Op	Firebox
6	✓	Outgoing	TCP-UDP	Any-Trusted, Any-Op	Any-External

設定を本体に保存してください。

ユーザーの追加

これまでの設定では、常時、管理者権限を持つ admin ユーザーでログインしており、すべての設定変更が可能な状態になってしまっています。

関係者が誤って設定変更しないよう、ログやレポートを閲覧する専用のユーザーを追加します。

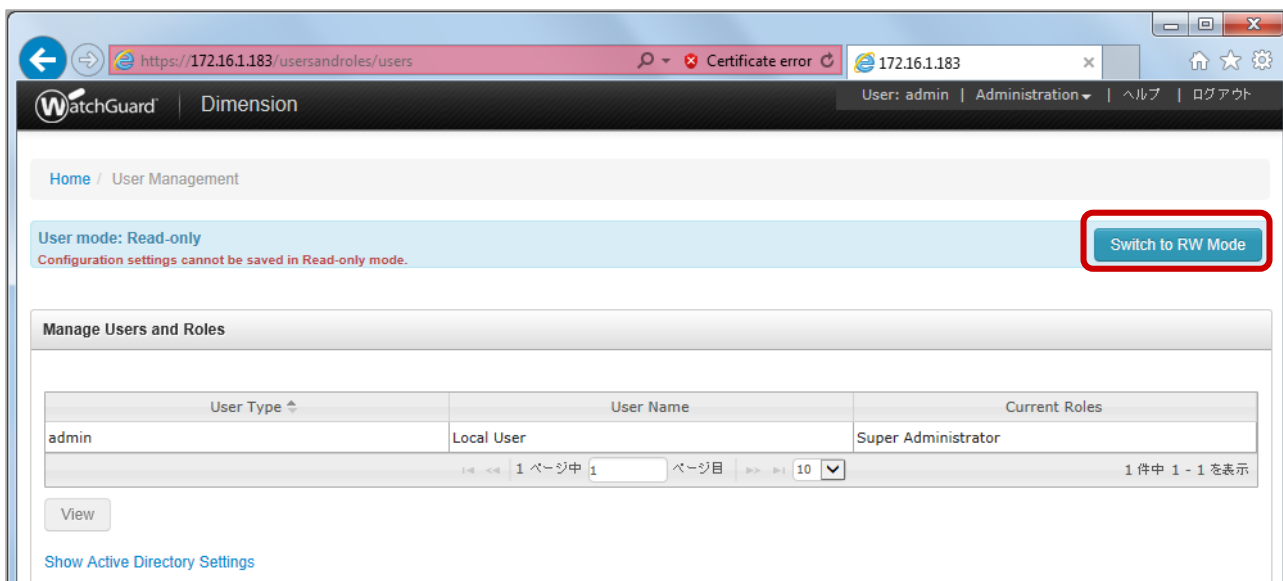
読み取り専用ユーザーの作成

Administration メニューから、User Management をクリックします。



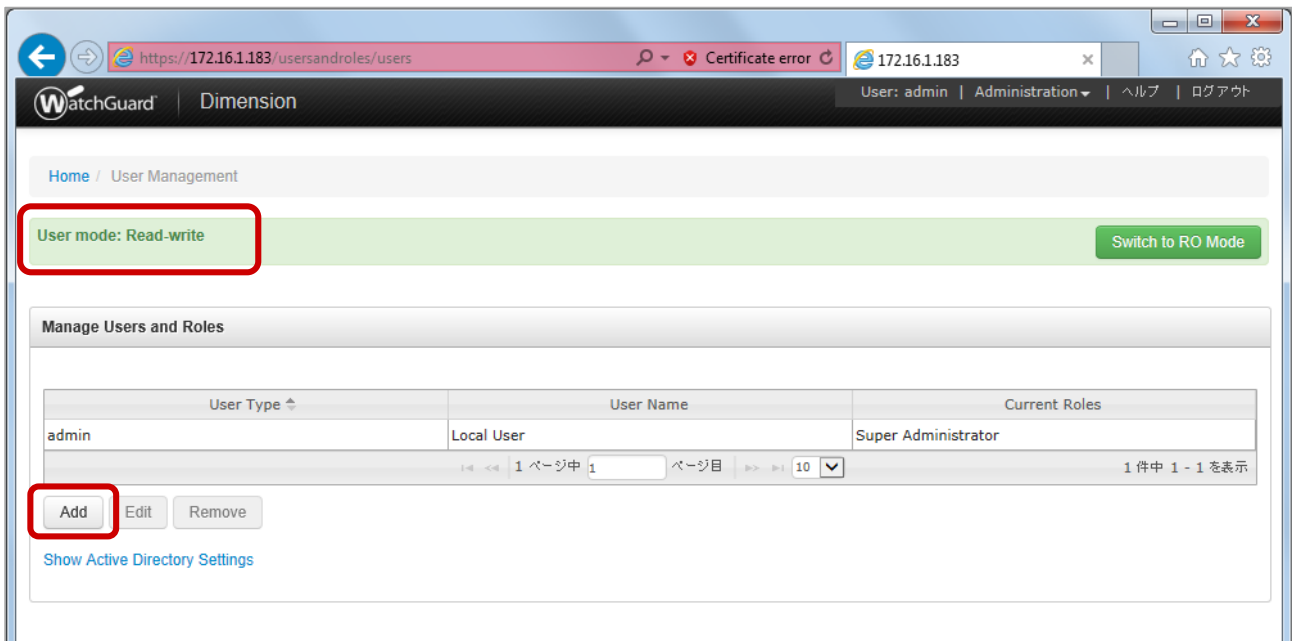
ユーザー一覧が表示されます。デフォルトでは読み取り専用モードになっています。

ここにユーザーを追加するには、Switch to RW Mode ボタンをクリックします。

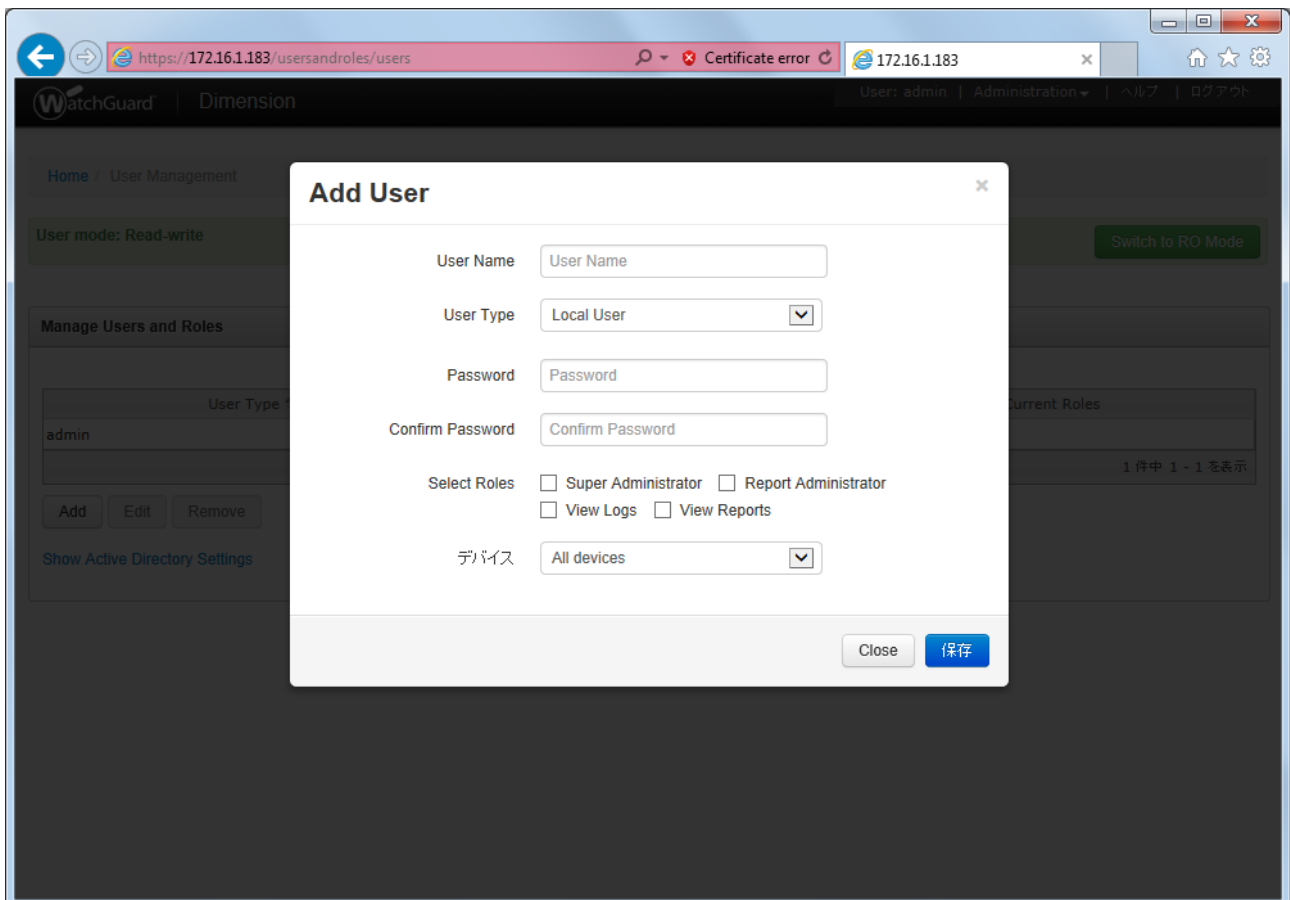


User mode : Read write という表示になり、ユーザーの追加・編集・削除ができる状態になります。

Add ボタンをクリックし、ユーザーを追加してみましょう。

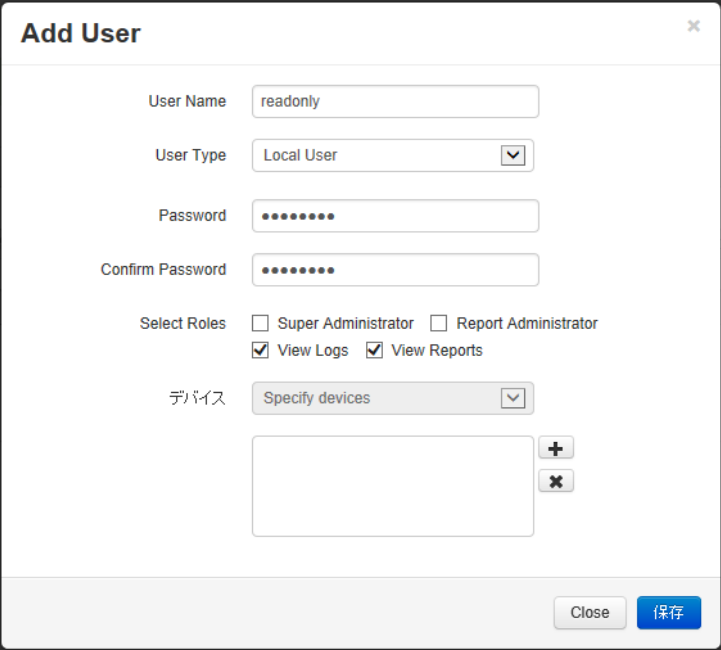


ユーザー追加画面になります。



User Name, Password, Confirm Password, に新規ユーザーの名前とパスワードを入力します。

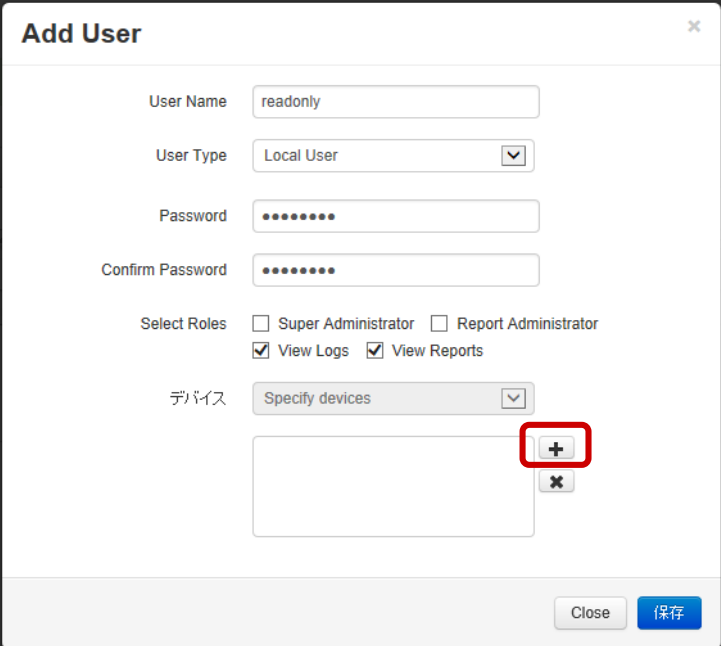
Select Roles は、付与する権限と役割を設定します。ログとレポートの閲覧だけなら View Logs と View Reports にチェックを入れます。ログは見せないでレポートだけ見せたい場合は、View Reports のみをチェックします。



The screenshot shows the 'Add User' dialog box with the following details:


- User Name: readonly
- User Type: Local User
- Password: [Redacted]
- Confirm Password: [Redacted]
- Select Roles: Super Administrator, Report Administrator, View Logs, View Reports
- デバイス: Specify devices
- Buttons: Close, 保存

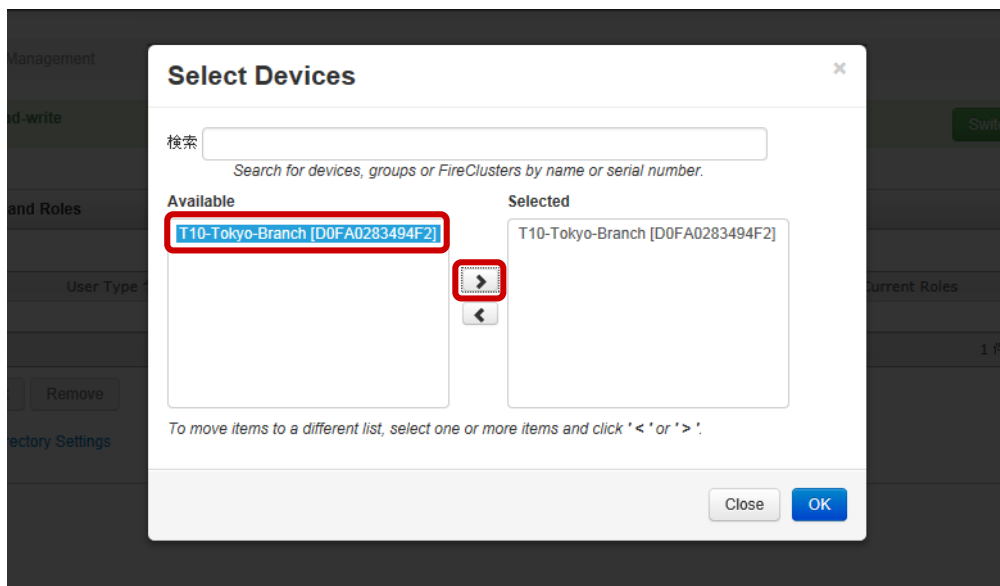
次に、どのデバイスのレポートの閲覧を許可するのか、設定します。デバイスのセクションにある **+** ボタンをクリックします。



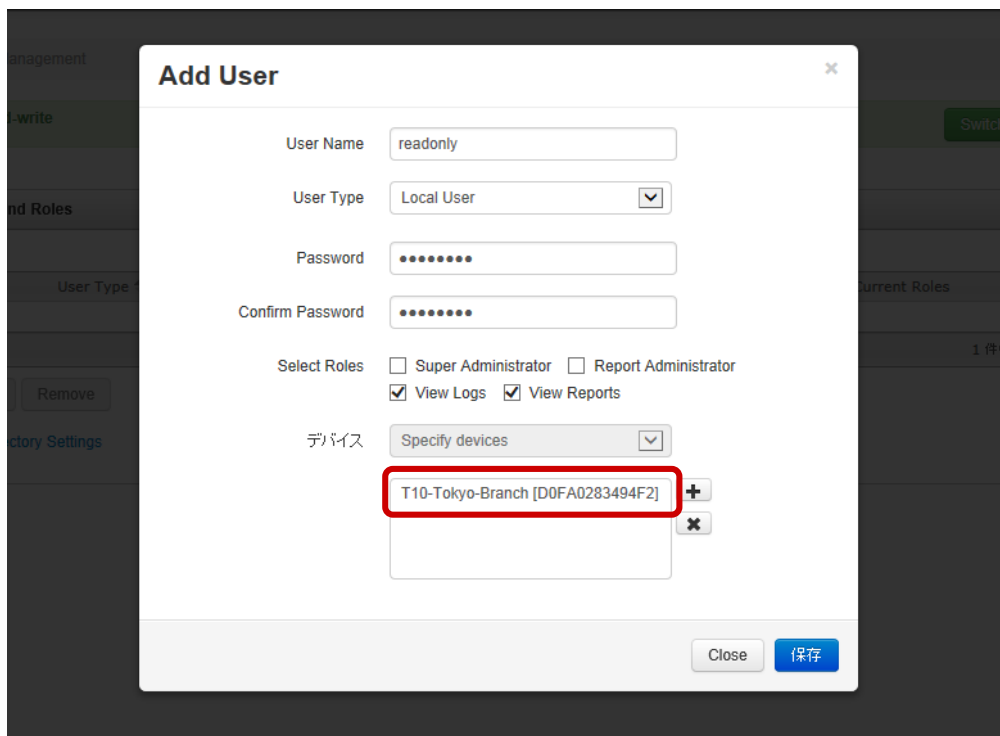
This screenshot is identical to the previous one, but the '+' button in the 'Devices' section is highlighted with a red square, indicating the next step in the process.

左側に閲覧可能なデバイスの一覧が表示されています。

その中から閲覧させてよいデバイスを選択し、 ボタンで右側の閲覧させるデバイスをコピーします。

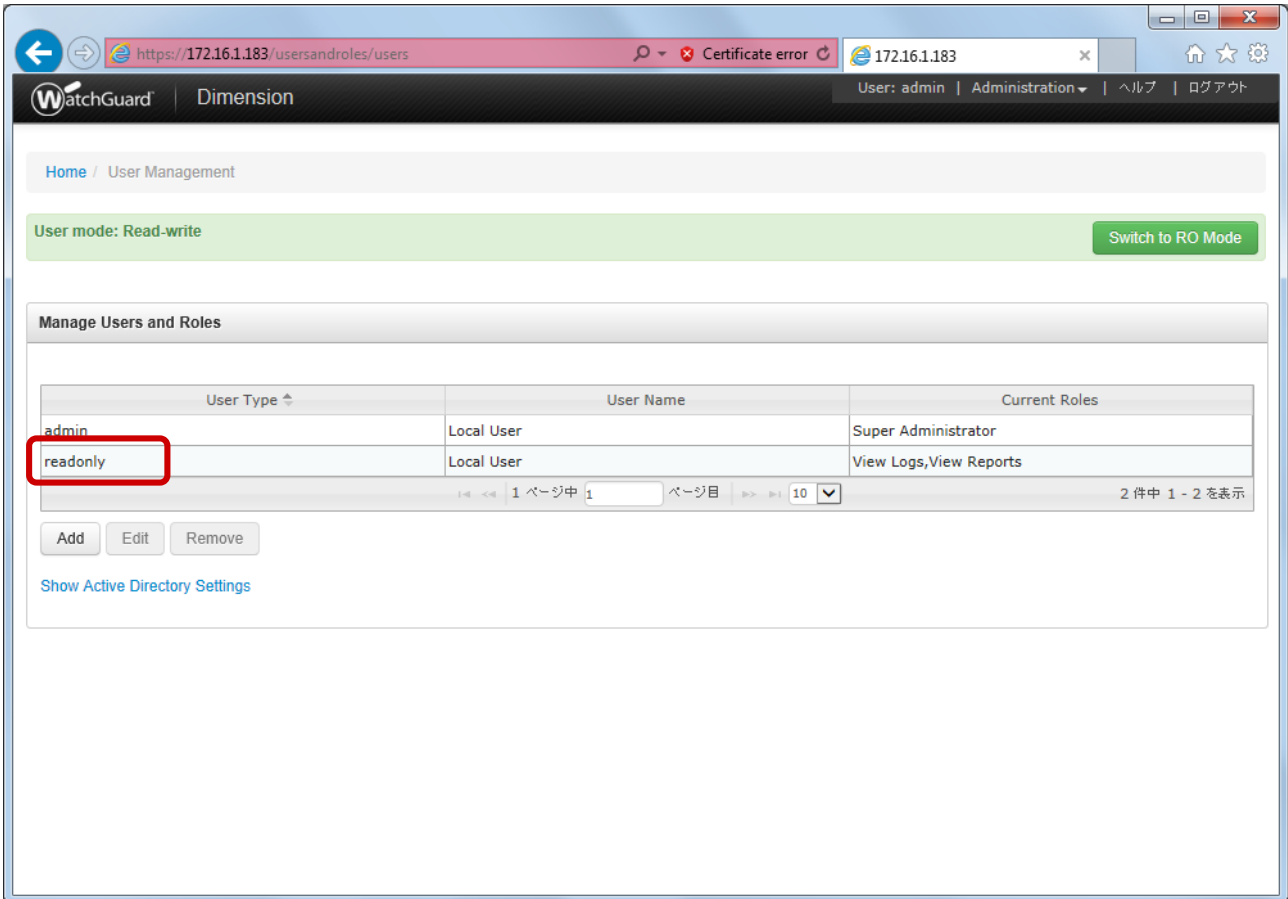


OK で Add User の画面に戻ると、追加するユーザーが閲覧できるデバイスが追加されているのを確認できます。

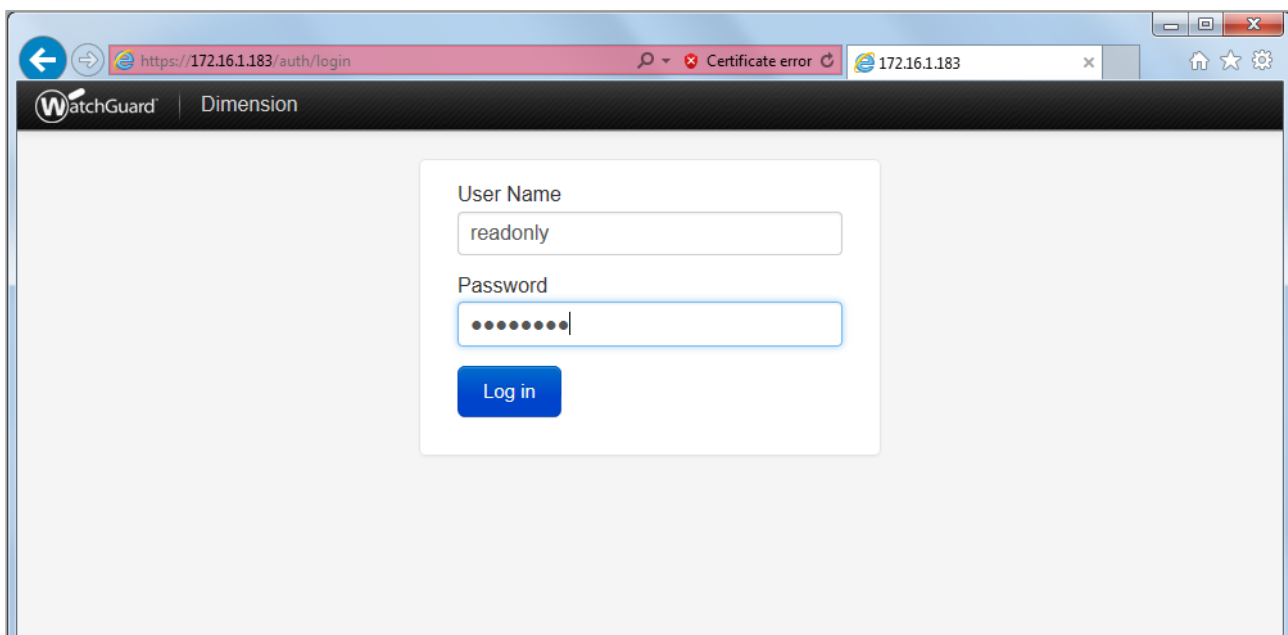


保存ボタンをクリックして、設定を反映させましょう。

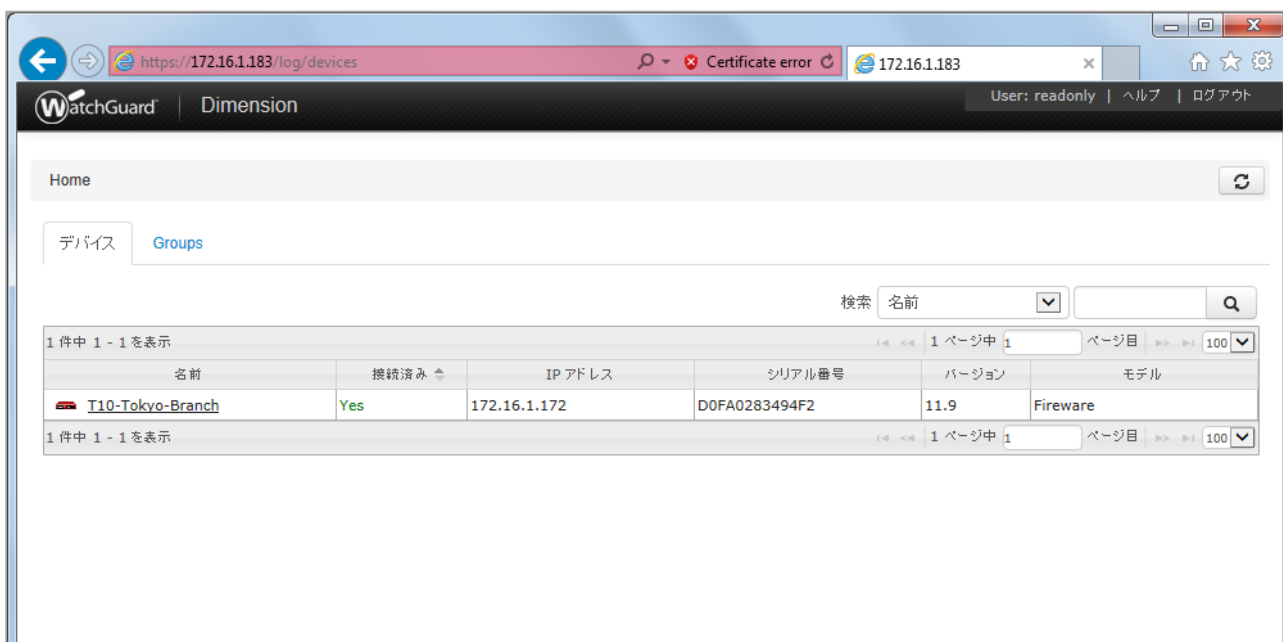
User management の画面に戻ると、readonly ユーザーが追加されているのを確認できます。



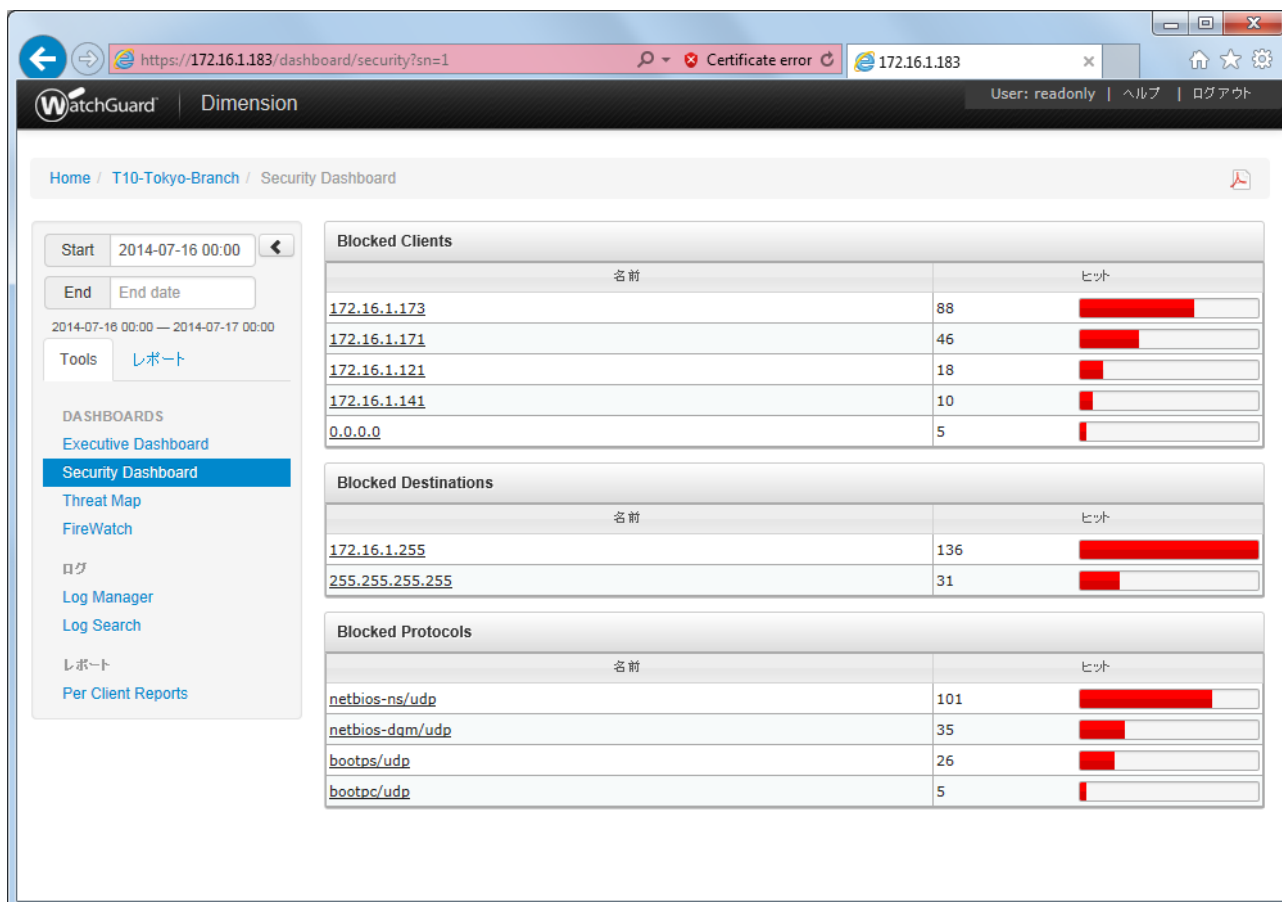
追加したユーザーでログインしてみます。



ログインし、閲覧可能にしたデバイスも表示されますが、Admin ユーザーと違い、右上部の Administration メニューが表示されません。



レポートを閲覧することができます。



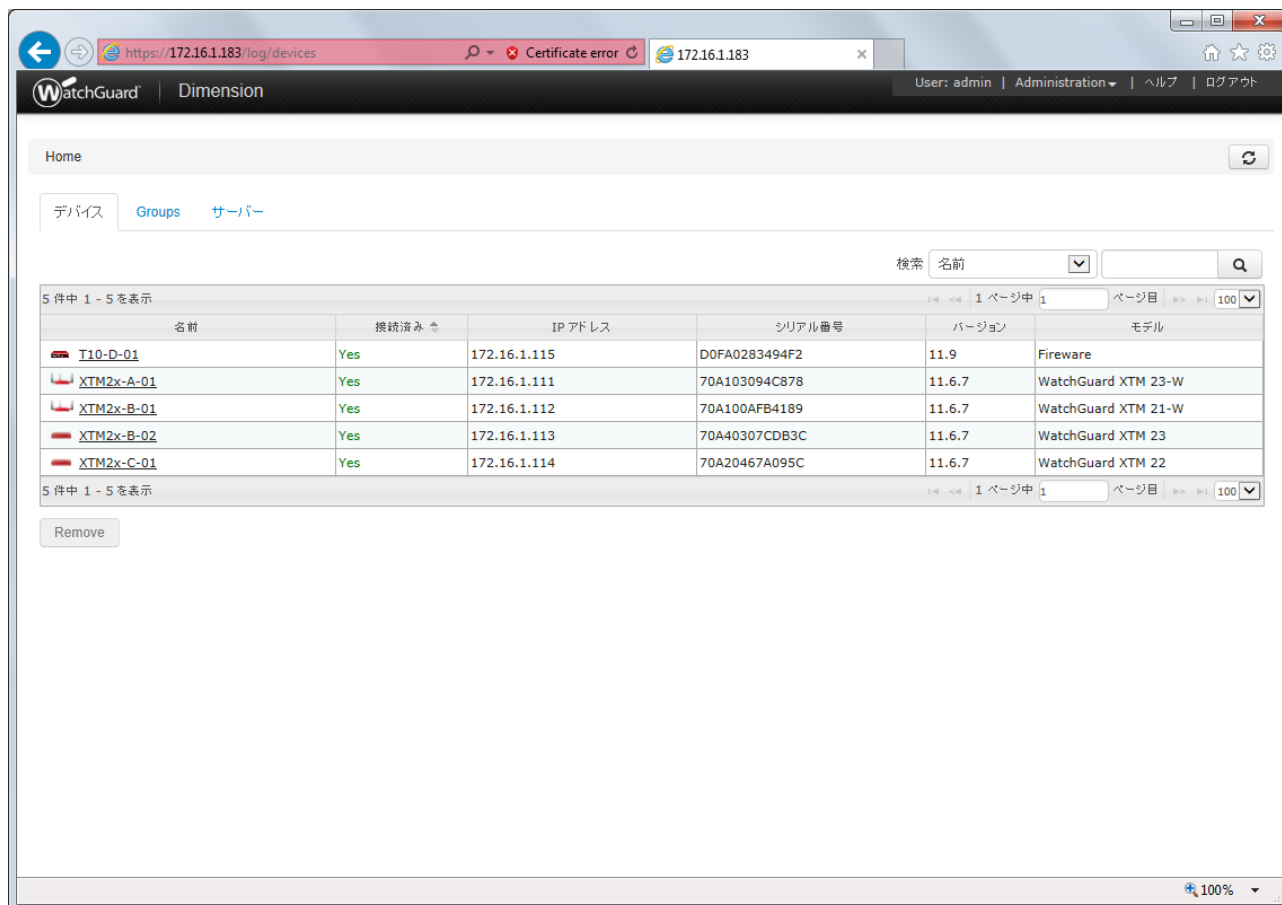
MSSP における運用

MSSP において、お客様にレポート公開する場合でも、これまでの要領で簡単に設定し、サービスを提供することが可能です。

仮に以下のようなお客様と機器があると想定します。それぞれの機器に会社のイニシャルを入れてわかりやすくしてあります。

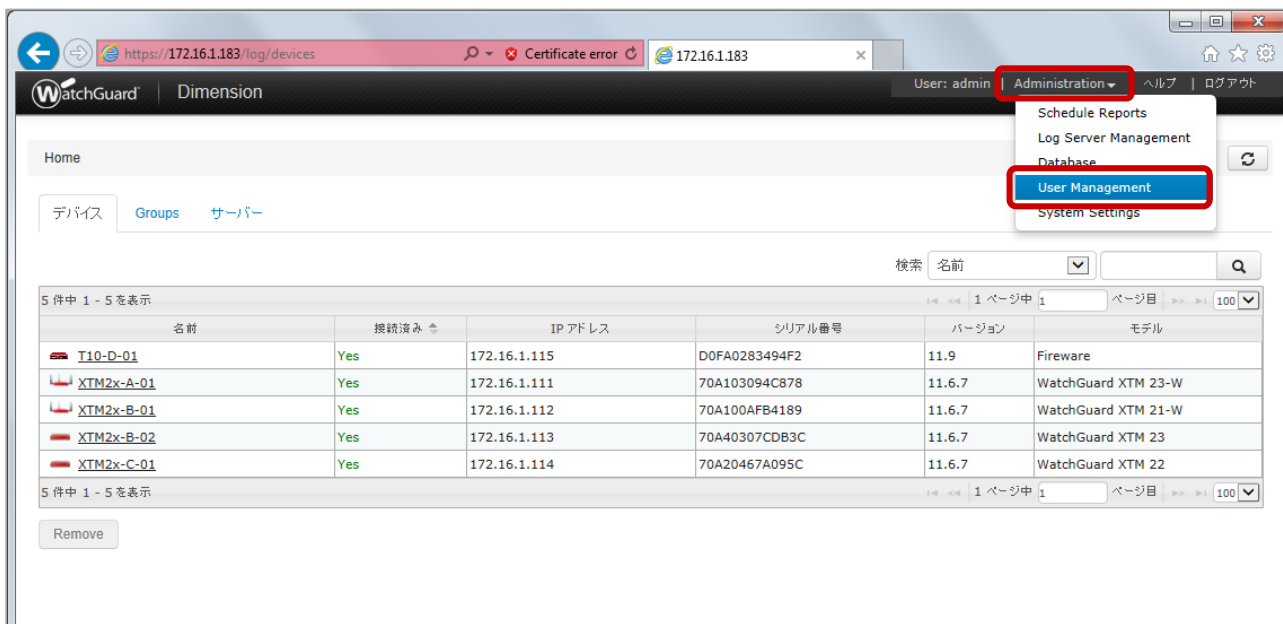
会社名	機器名	ユーザー名
A 社	XTM2x-A-01	AcompanyReportUser
B 社	XTM2x-B-01	BcompanyReportUser
	XTM2x-B-02	
C 社	XTM2x-C-01	CcompanyReportUser
D 社	T10-D-01	DcompanyReportUser

Admin ユーザーでログインすると、すべての機器が表示されています。

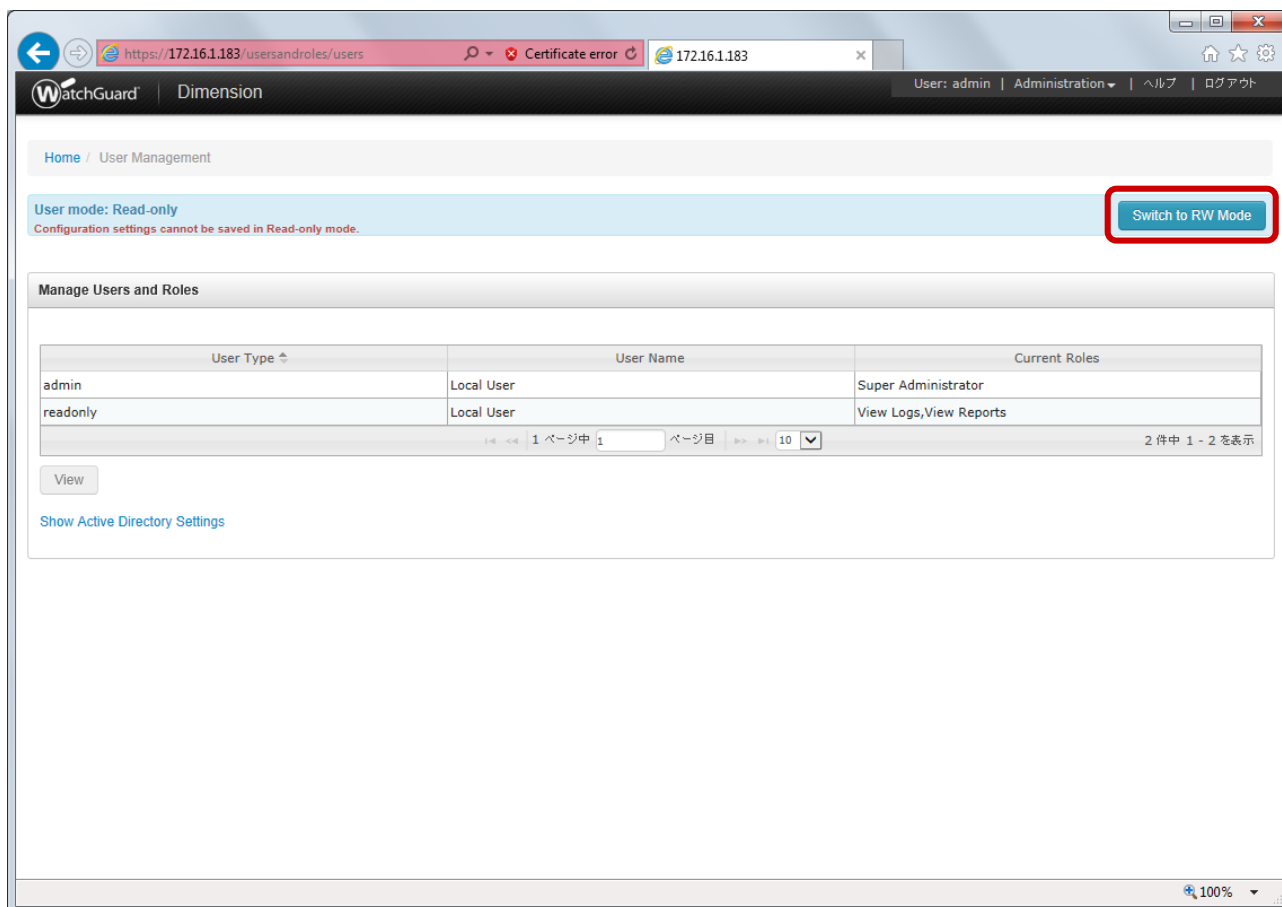


前章の手順でお客様ごとに Dimension ユーザーを作成し、該当の機器のみが閲覧できるようにします。

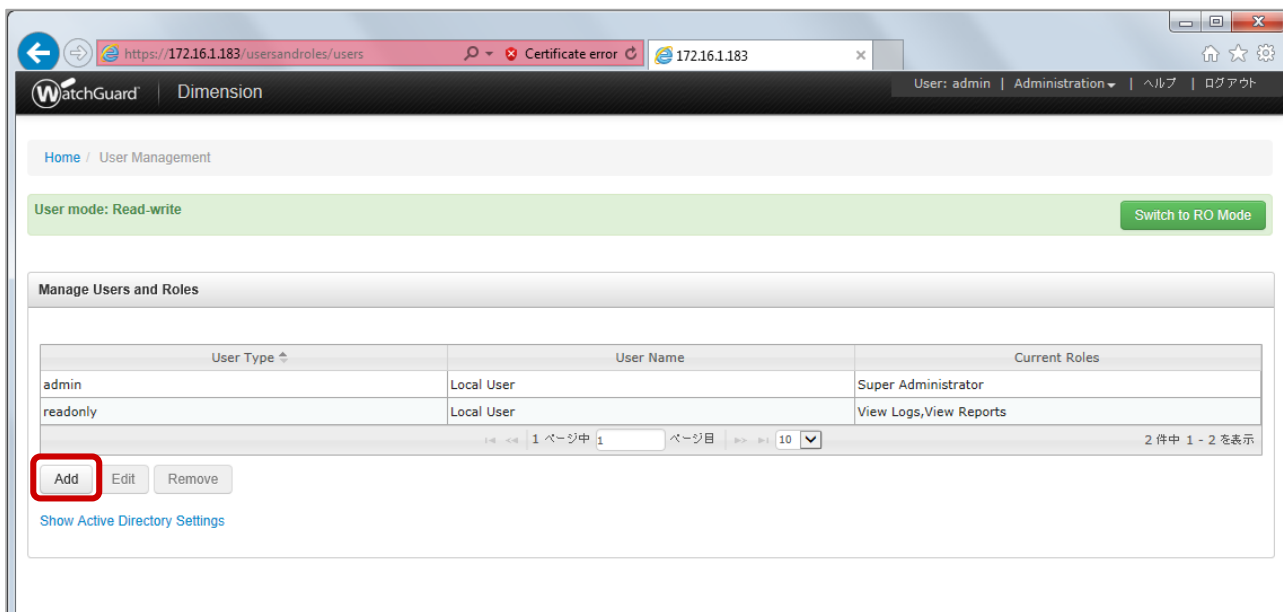
User Management の画面に移ります。



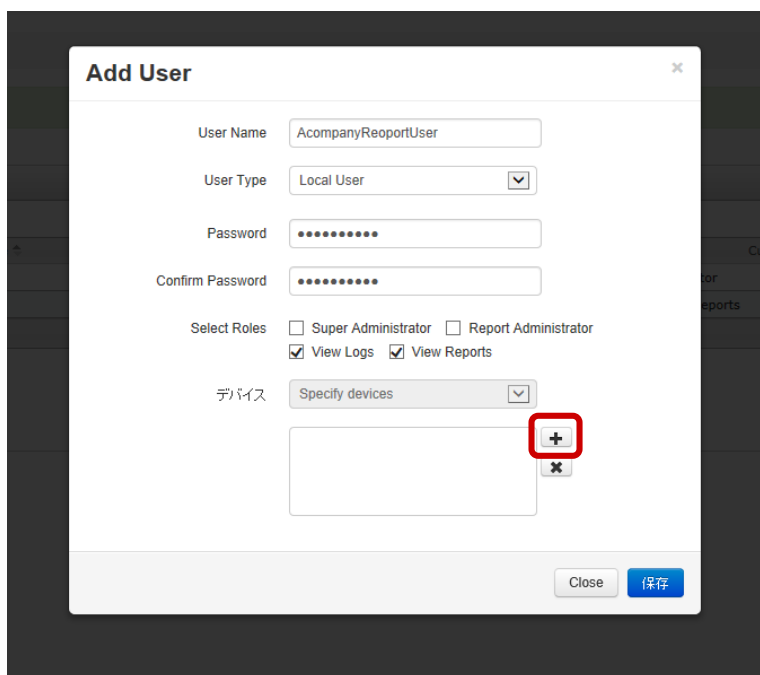
RW Mode にします。



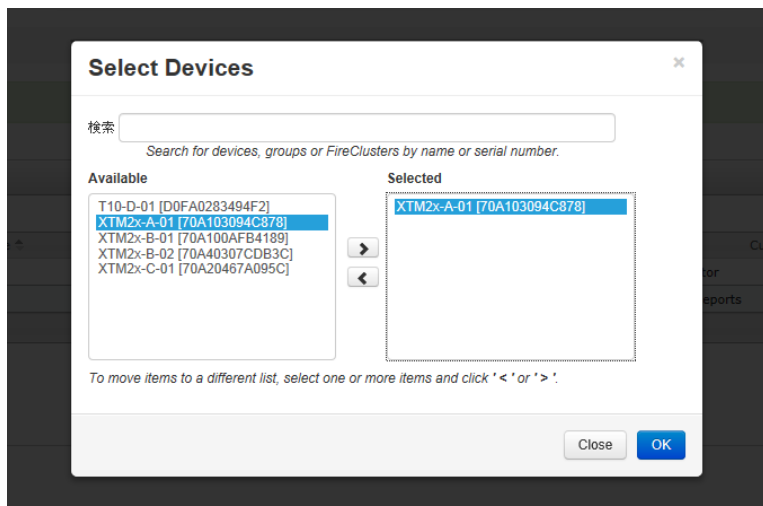
Add ボタンをクリックしてユーザーを追加します。



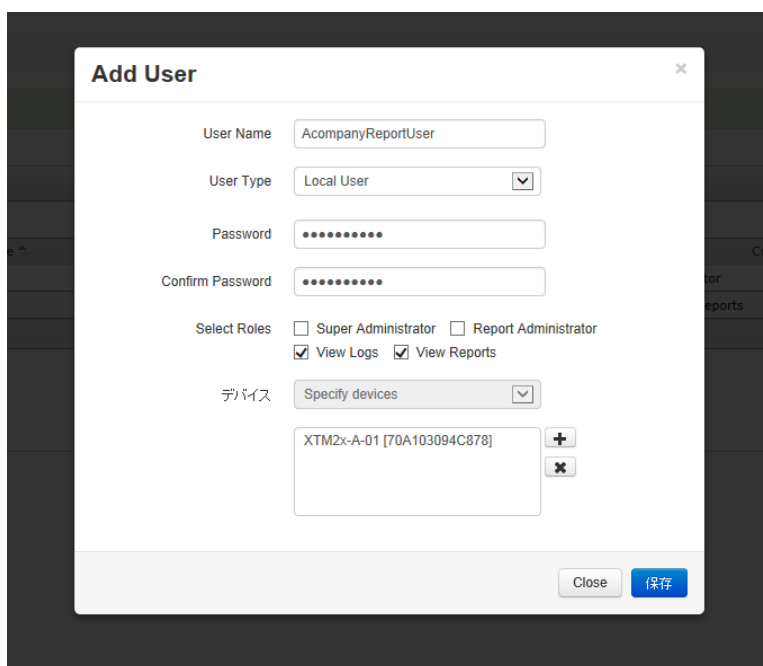
A 社のユーザー情報を入力し、バイスを選択します。



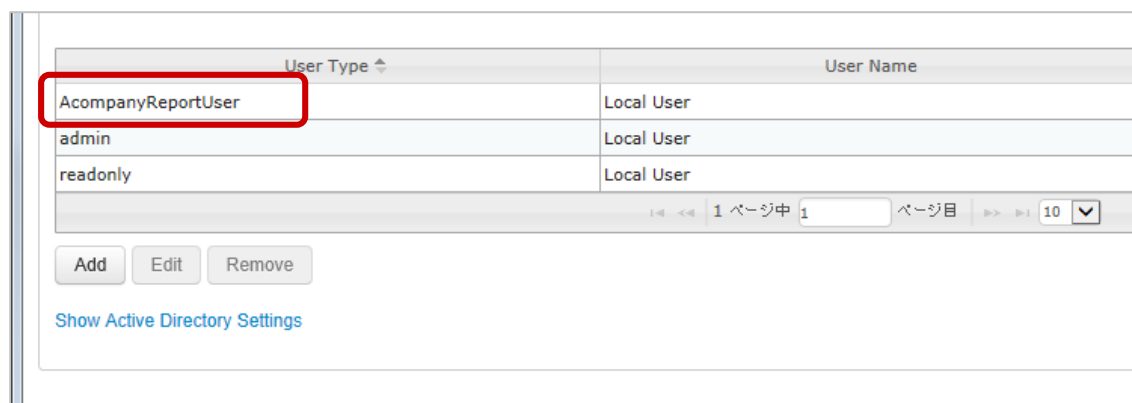
A社のデバイスのみを閲覧可能なデバイスとして選択します。



この状態で保存します。



A社ユーザーが追加されました。



同様に B 社ユーザーを追加し、B 社のデバイスのみを閲覧可能な設定にします。

Add User

User Name: BcompanyReportUser

User Type: Local User

Password:

Confirm Password:

Select Roles: Super Administrator Report Administrator
 View Logs View Reports

デバイス: Specify devices

- XTM2x-B-01 [70A100AFB4189]
- XTM2x-B-02 [70A40307CDB3C]

Close 保存

同じく C 社を設定。

Add User

User Name: CcompanyReportUser

User Type: Local User

Password:

Confirm Password:

Select Roles: Super Administrator Report Administrator
 View Logs View Reports

デバイス: Specify devices

- XTM2x-C-01 [70A20467A095C]

Close 保存

同じく D 社を設定。

Add User

User Name: DcompanyReportUser

User Type: Local User

Password:

Confirm Password:

Select Roles: Super Administrator Report Administrator
 View Logs View Reports

デバイス: Specify devices

T10-D-01 [D0FA0283494F2]

Close 保存

保存してユーザーの一覧に戻ると、A から D 社のユーザーが設定されていることが確認できます。

User Type	User Name
AcompanyReportUser	Local User
admin	Local User
BcompanyReportUser	Local User
CcompanyReportUser	Local User
DcompanyReportUser	Local User
readonly	Local User

1 ページ中 1 ページ目 10

では A 社のユーザーでログインしてみましょう。

WatchGuard Dimension

User Name: AcompanyReportUser

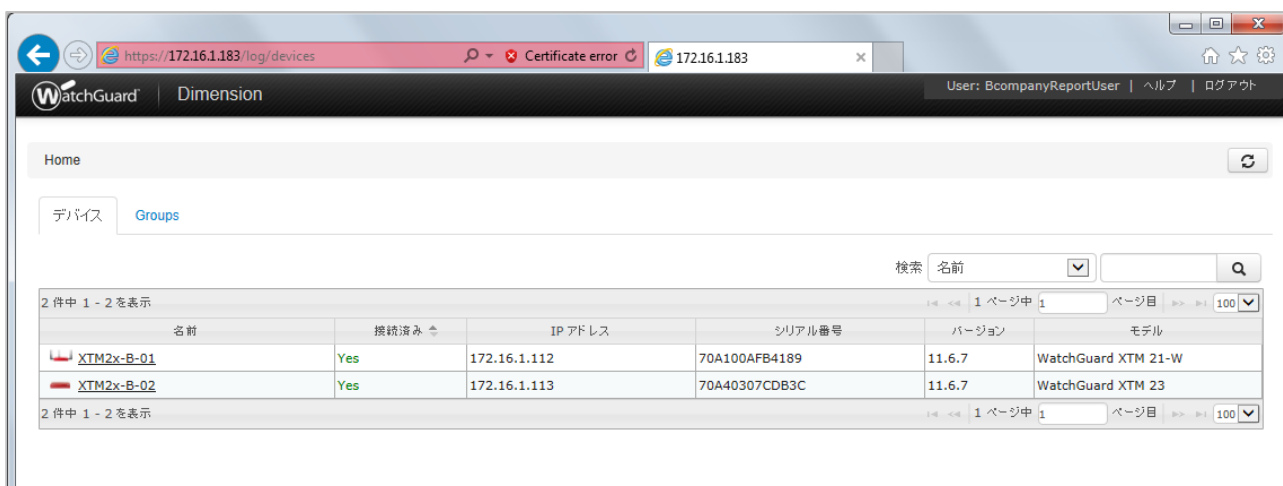
Password:

Log in

すると A 社ユーザーに紐付けられたデバイスだけが閲覧できます。



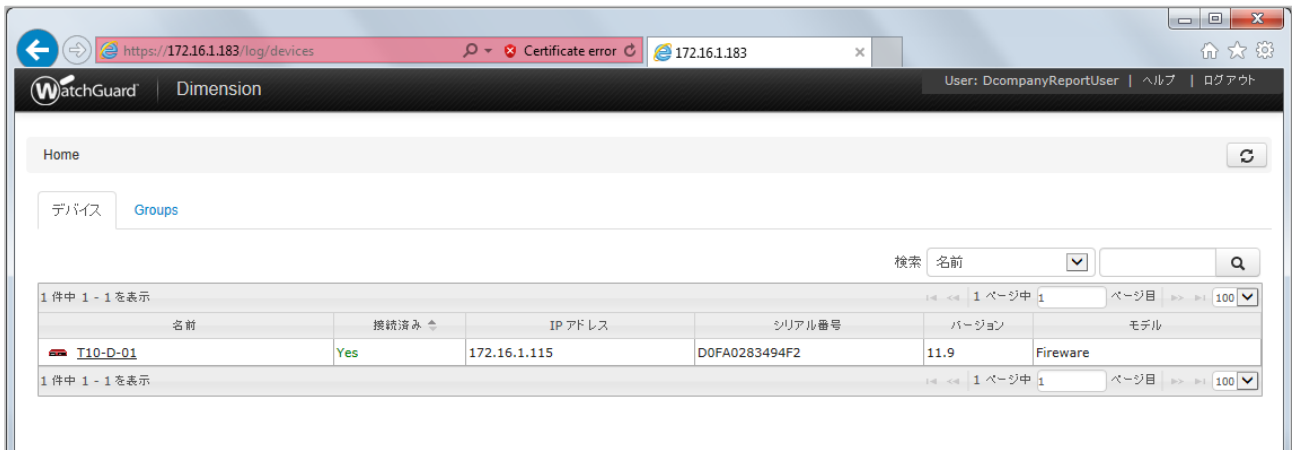
B 社ユーザーでログインすると、B 社に属する別な 2 台のデバイスが表示されます。



C 社でログイン。



D 社も他のお客様では見えてこなかった自社の Firebox T-10 が表示されています。



このようにお客さまごとのログインアカウントを作成し、そのアカウントにお客様のデバイスを紐付けることによってレポートサービスを提供できるようになります。

管理者メニュー リファレンス

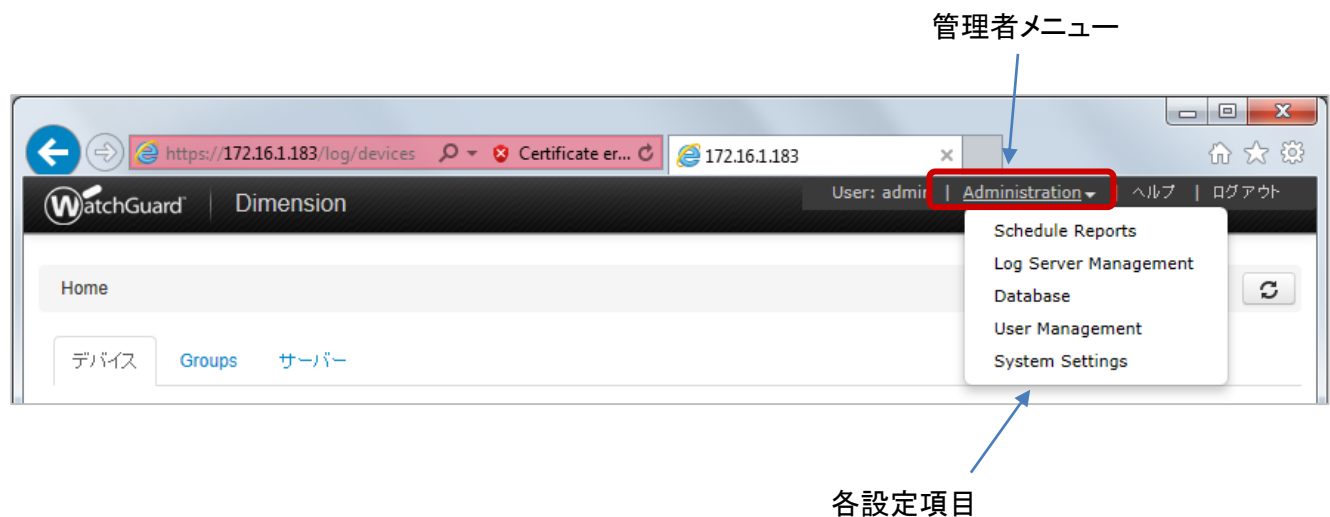
前章までは Dimension の導入から実運用までの手順を最短コースで解説しましたが、この章では管理者メニューの設定項目を網羅的に解説します。

管理者メニューについて

管理者メニューとは

admin ユーザーで Dimension にログインした際に、画面右上部に「Administration」と表示されるメニューです。クリックすると、以下の各設定項目を選択することができます。

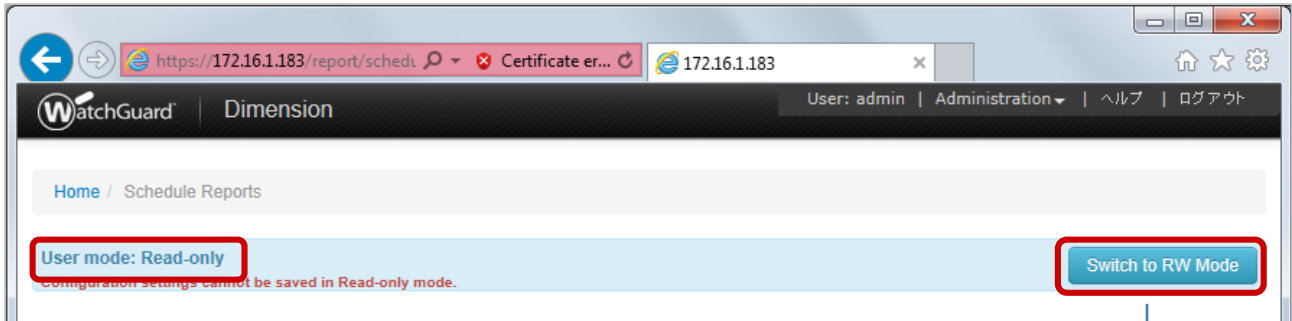
- Schedule Reports
- Log Server Management
- Database, User Management
- System Settings



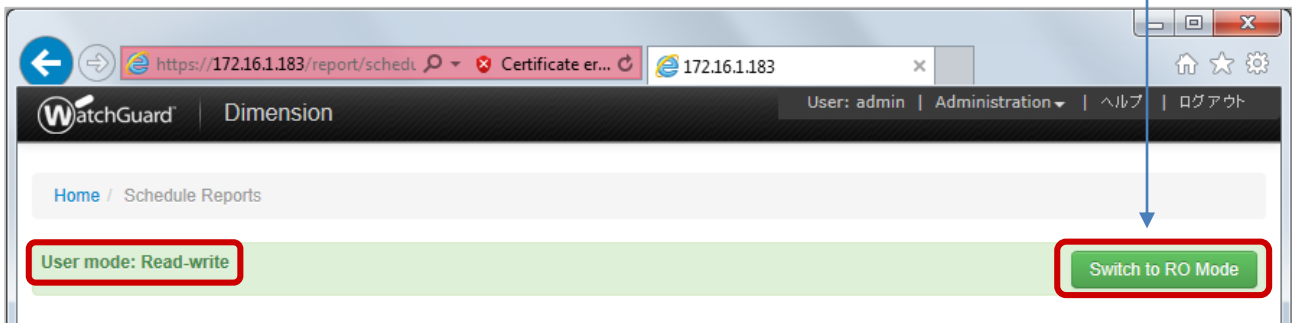
モードの切り替え

各設定項目の画面に移った際に User mode が Read only でと表示されている場合、読み取り専用モードであることを意味しており、このままでは設定変更はできません。

設定を変更する場合は Switch to RW Mode のボタンをクリックし、読み書き許可モードに切り替えます。



User mode: Read write と表示され、ボタンが緑色になったら設定変更が可能です。



Schedule Reports

Schedule Reports では、Dimension が生成したレポートを PDF 形式にし、それを E メールで定期的送信するスケジュールを設定することができます。

メールを送信するためには、あらかじめ Log Server Management — Configuration — Notification でメール送信を可能にするための設定を済ませておく必要があります。

また、レポートは FTP に保存することもでき、その場合はあらかじめ Log Server Management — Configuration — Reporting で FTP サーバーの設定を済ませてください。

レポートスケジュールの追加

RW Mode にしたら、Add ボタンをクリックします。



The screenshot shows the WatchGuard Dimension web interface. At the top, there is a navigation bar with the WatchGuard logo, the text 'Dimension', and user information 'User: admin | Administration | ヘルプ | ログアウト'. Below the navigation bar, there is a breadcrumb trail 'Home / Schedule Reports'. A green banner indicates 'User mode: Read-write' with a 'Switch to RO Mode' button. The main content area is titled 'Report Schedules' and contains a table with columns '名前', 'Description', and 'Report Runs'. The table is currently empty, and a message at the bottom right says '表示するレコードがありません'. Below the table, there are three buttons: 'Add', 'Edit', and 'Remove'. The 'Add' button is highlighted with a red box.

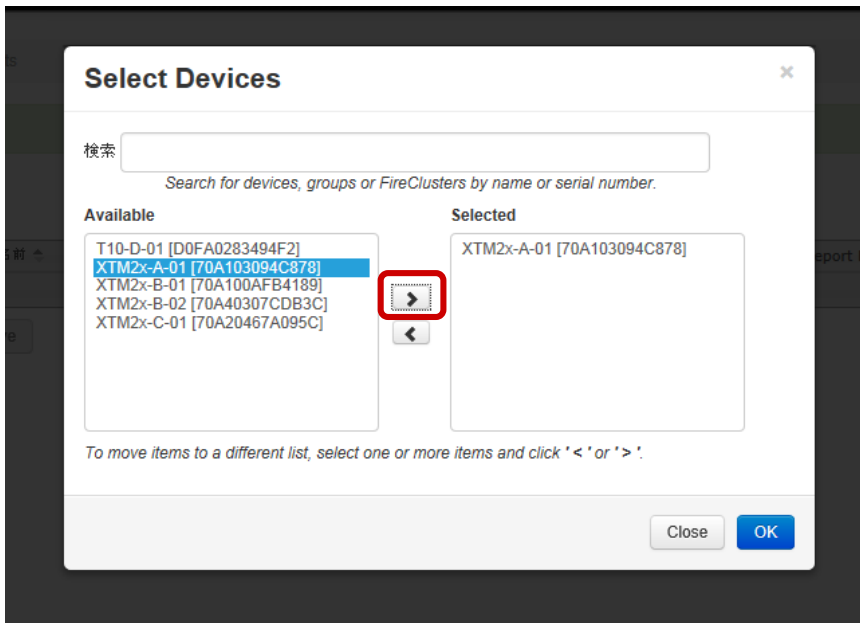
Create Schedule 画面になります。最初にスケジュール名と説明を入力し、Next。

The screenshot shows the 'Create Schedule' dialog box with the 'Name & Description' step selected. The 'Schedule Name' field contains 'Acorp-1day'. The 'Description' field is empty and marked as '(Optional)'. There are 'Back' and 'Next' buttons at the bottom right.

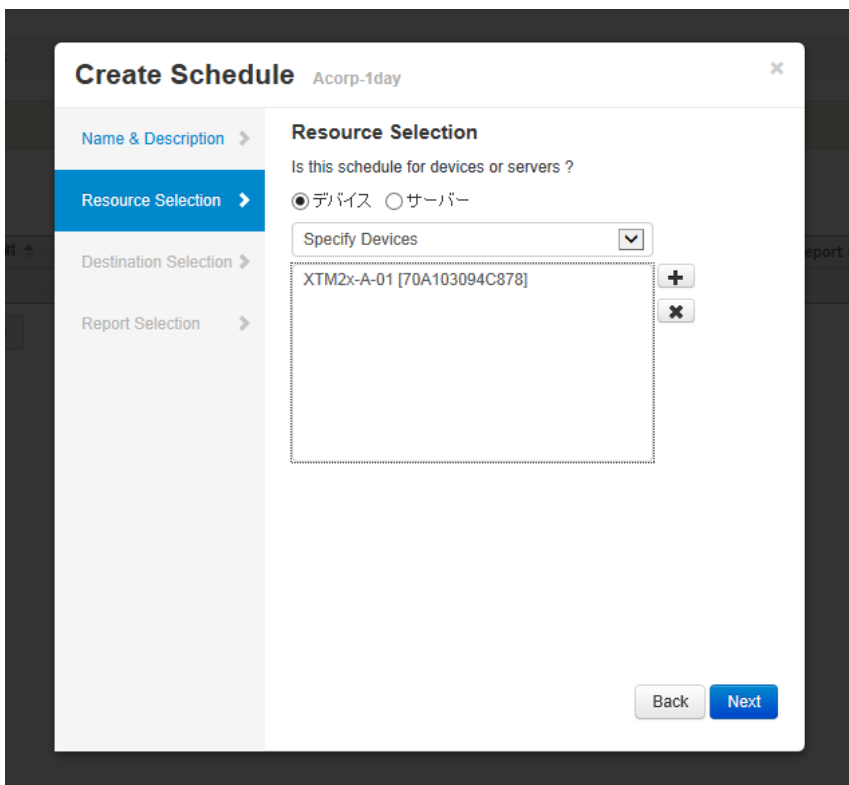
どのデバイスのレポートを対象にするか指定します。デバイスにチェックを入れ、ドロップダウンリストでは Specify Devices を選択し、**+** をクリックします。

The screenshot shows the 'Create Schedule' dialog box with the 'Resource Selection' step selected. The 'Specify Devices' dropdown menu is open, and the '+' button is highlighted with a red box. There are 'Back' and 'Next' buttons at the bottom right.

左側の Available エリアであるデバイスを選択し、**>** をクリックして右側 Selected エリアにコピーします。
選択したら OK ボタンをクリックします。



レポートするデバイスが指定された状態になります。Next。



送信先のメールアドレスを指定します。

Send Reports in email. にチェックを入れると、宛先のメールアドレスを追加する欄が表示されます。

そこに必要なだけ送り先を入力し、**+** をクリックし、追加してゆきます。

Create Schedule Acorp-1day

Name & Description > **Destination Selection**

Resource Selection >

Destination Selection >

Report Selection >

Send reports to:

Send reports in email

admin@acorp.mail.domain [X] **+**

itcML@acorp.mail.domain [X]

[Show email subject and body settings](#)

Send reports to the specified directory

Send reports to ConnectWise ?

Back Next

追加できました。Next。

Create Schedule Acorp-1day

Name & Description > **Destination Selection**

Resource Selection >

Destination Selection >

Report Selection >

Send reports to:

Send reports in email

Send email to [X] **+**

itcML@acorp.mail.domain [X]

admin@acorp.mail.domain

[Show email subject and body settings](#)

Send reports to the specified directory

Send reports to ConnectWise ?

Back Next

レポートの種類、タイムゾーン、頻度などを指定し、Finish をクリックします。

Create Schedule Acorp-1day

Name & Description > **Report Selection**

Resource Selection >

Destination Selection >

Report Selection >

Report Types
Executive Summary Reports

Time Zone
Asia/Tokyo (UTC +09:00)

Report Template
WatchGuard

Report Aggregation
Single

Run Reports
毎日

Report time: Each morning, 12:00 AM, Asia/Tokyo (UTC +09:00)
Date range: Start from the previous day

Back Finish

スケジュールが一覧に追加されれば設定完了です。

WatchGuard Dimension User: admin | Administration | ヘルプ | ログアウト

Home / Schedule Reports

User mode: Read-write Switch to RO Mode

Report Schedules

名前	Description	Report Runs
Acorp-1day		毎日

1 ページ中 1 ページ目 10 1 件中 1 - 1 を表示

Add Edit Remove

Log Server Management

Status

ログサーバーの稼働状態、負荷、ログ量を表示しています。

WatchGuard | Dimension | User: admin | Administration | ヘルプ | ログアウト

Home / Log Server Management | Status | Configuration | IP Address Mapping | Diagnostics

Log Server Status

Log Server	Available
Log Database	Available
Uptime	12 days, 22 hours, 43 minutes, 57 seconds

Start Stop Restart

Log Server Information

CPU Usage	0.2%
Memory Usage	40.27MB
Database Disk Usage	0.05GB of 32GB used (39GB free on disk)

Log Rate

Log Server Activity (last 24 hours)

Log Server Status

Dimension 組み込みのログサーバーの開始/停止/再起動ができます。

Log Server Status

Log Server	Available
Log Database	Available
Uptime	12 days, 22 hours, 43 minutes, 57 seconds

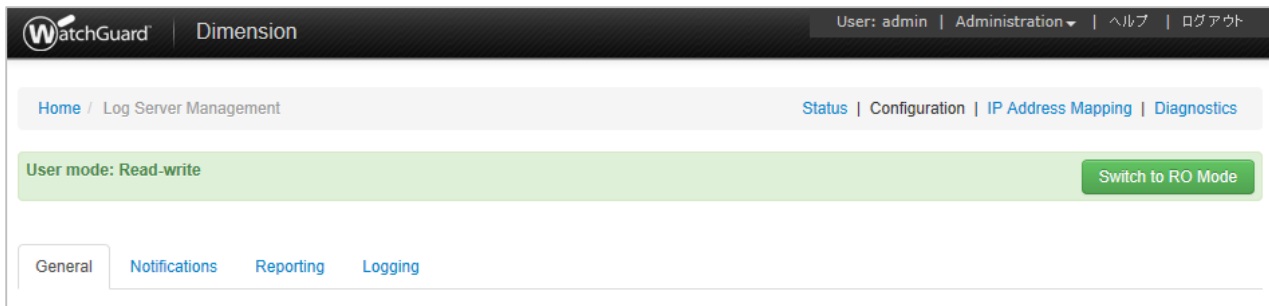
Start Stop Restart

参考： 以下は Stop ボタンをクリックしたところです。

Start Stop Restart

Configuration

Log Server Management の Configuration セクションでは、ログサーバーの設定変更を行なうことができます。設定カテゴリーには General, Notifications, Reporting, Logging があります。



General

Encryption Key

ログ送信する際の暗号化キーを再設定できます。

Encryption Key

Change the Log Server Encryption Key

New Encryption Key

Confirm Encryption Key

注意: 変更するとそれまで通信していた機器も、再設定するまでログが送信できなくなります。

Database Size

Automatically delete log messages older than days のチェックを有効にすると、指定した日数を超えたログは自動的に削除されます。

Database Size

Maximum Database Size 32 GB

Current Database Size 0.05 GB

Available Space 31.95 GB (99.85% free)

Automatically delete log messages older than days

例として、このように 120 日に設定すると、閲覧者からは少なくとも直近 3 ヶ月のログ/レポートの閲覧を保証する形で運用できます。

Database Backup

ログを格納したデータベースのバックアップを行ないます。

Automatically back up log messages にチェックを入れて有効にします。

Database Backup

Automatically back up log messages (a remote backup server must be configured)

Back Up Every day(s)

Back Up At

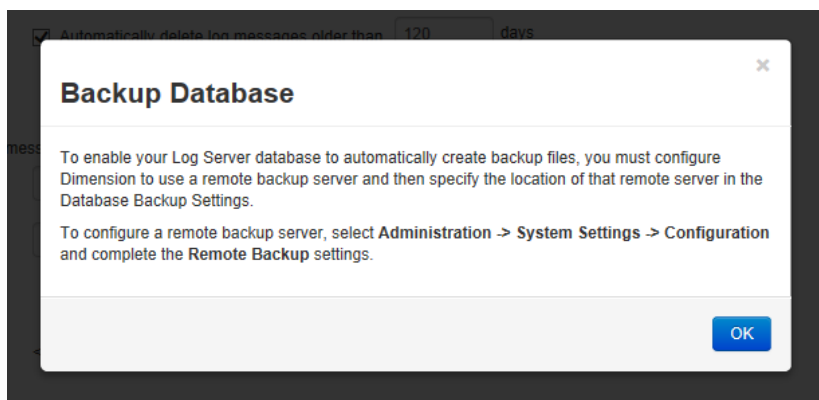
Directory for Backup Files

Date of Last Backup <None>

Next Scheduled Backup <None>

[Create Backup Now](#) | [Restore a Backup Log File](#)

有効にすると、Administration — System Settings — Configuration and complete the Remote Backup であらかじめバックアップ先を設定する必要がある旨が表示されます。OK をクリックします。



データベースをバックアップする頻度と時間を設定します。

Database Backup

Automatically back up log messages

Back Up Every day(s)

Back Up At

Directory for Backup Files

Date of Last Backup <None>

Next Scheduled Backup <None>

[Create Backup Now](#) [Restore a Backup Log File](#)

また、スケジュールを設定しなくても、Create Backup Now リンクをクリックすれば、いつでも手動でバックアップを実行できます。

Database Location Settings (requires restart)

データベースを Dimension 標準のものにするか、外部に構築した PostgreSQL にするか、指定できます。

Database Location Settings (requires restart)

Built-in database External PostgreSQL database

Log data is stored and managed at this location: /var/opt/watchguard/dimension/data/db

External PostgreSQL database を選択すると、接続に必要なサーバーとデータベースの情報を入力できるようになります。入力したら、Test Connection ボタンをクリックし、問題ないことを確認してください。

Database Location Settings (requires restart)

Built-in database External PostgreSQL database

Database Name

IP アドレス

ポート

Database User

Password

Log Server Management の設定が完了したら、保存ボタンをクリックし、設定を反映させてください。

Notifications

Notifications は、ログサーバーに何かしらのイベントが発生した場合に、メールで通知する機能です。

Events

When a failure event occurs on this Log Server

- ログサーバーに深刻な問題が発生した場合に通知します。
(DB のエラー、ディスクフル、バックアップエラー、接続エラーなど)

When an event notification is received from any device or server

- 接続している機器から何らかのイベント通知があったばあいに通知します。

When log messages are purged from the database

- データベースからログが削除処理された場合に通知します。

Events

- Send an Email Notification
- When a failure event occurs on this Log Server
 - When an event notification is received from any device or server
 - When log messages are purged from the database

SMTP Server Settings

通知機能のために使用するメールサーバーの情報を設定します。

SMTP Server Settings

Outgoing Email Server (SMTP)
Example: smtp.mydomain.com or smtp.mydomain.com:<port number>

Send credentials to the email server

User Name

Password

Enable STARTTLS

The SMTP Server certificate must be signed by a CA trusted by Dimension for STARTTLS to succeed. For a list of CA certificates trusted by Dimension, [click here](#). To use a certificate signed by a CA that is not in the list, you must import the certificate.

Notification Setup

メール通知する際の宛先、Sender、件名を設定します。

Test Email ボタンで正常に送信できるかテストできます。

Notification Setup

Send Email To
Example: administrator@mycompany.com

Send Email From
Example: logServer@mycompany.com

Subject

Notification の設定が済んだら、保存ボタンをクリックして設定を反映させてください。

Reporting

Reporting では、レポートのテンプレート、FTP の転送先などを設定できます。



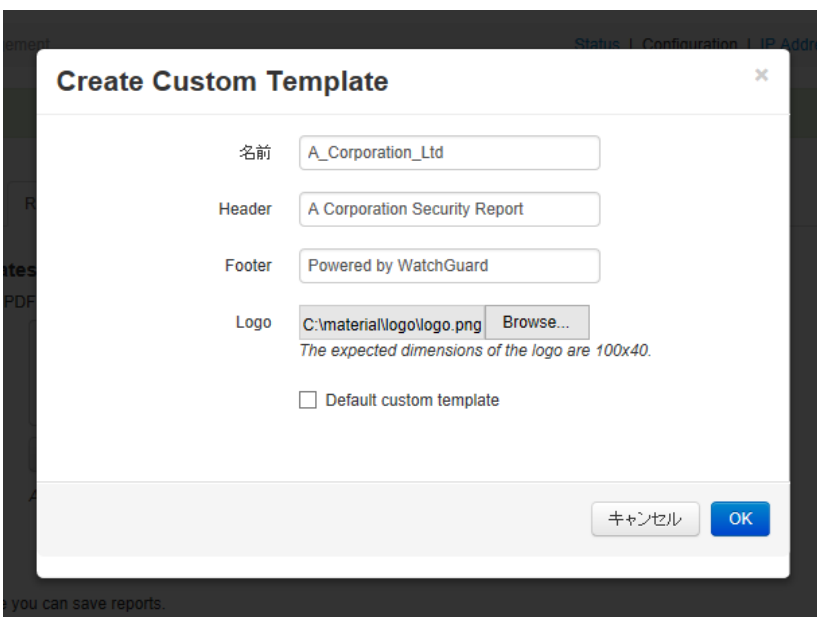
Custom Report Templates

ウォッチガードのテンプレートを使用しないで、カスタマイズされたテンプレートを作成する場合、Add ボタンをクリックします。

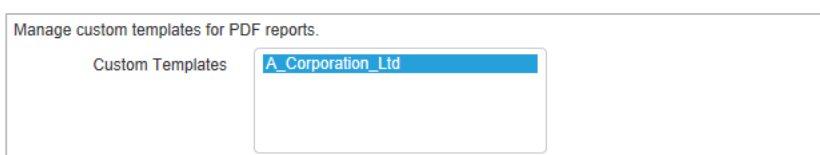


カスタムテンプレートを作成する画面になります。

名前(社名など)を指定し、ロゴもオリジナルのものを使用することができます。サイズは 100×40 より大きくならないようにします。ヘッダーとフッターは各ページの上下に固定のテキストとして表示されます。

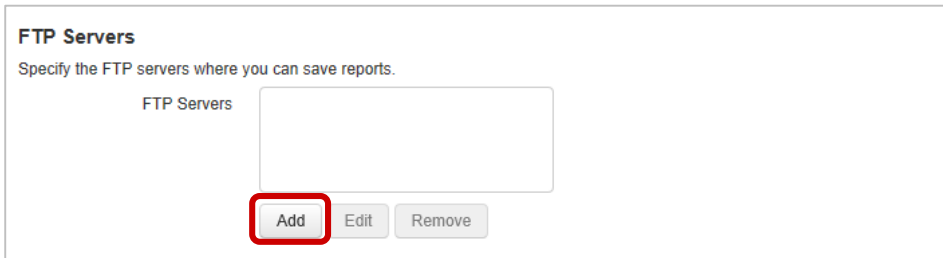


OK をクリックしてテンプレートの追加となります。



FTP Servers

レポートを FTP に格納したい場合に指定します。Add ボタンをクリックします。

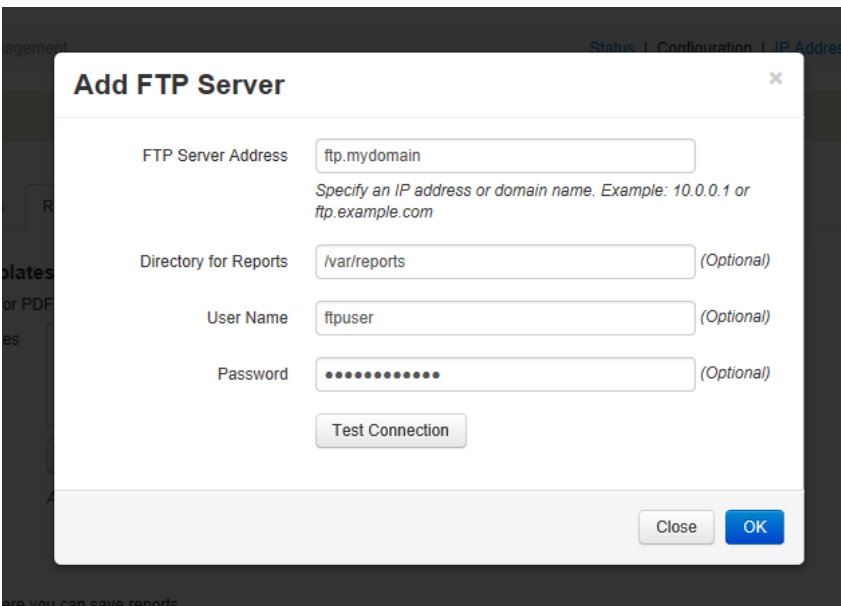


FTP Servers
Specify the FTP servers where you can save reports.

FTP Servers

Add Edit Remove

FTP サーバーの接続情報を設定します。設定後は正常に動作するか、Test Connection ボタンで確認してください。



Add FTP Server

FTP Server Address: ftp.mydomain
Specify an IP address or domain name. Example: 10.0.0.1 or ftp.example.com

Directory for Reports: /var/reports (Optional)

User Name: ftpuser (Optional)

Password: (Optional)

Test Connection

Close OK

OK をクリックすれば FTP サーバーの追加となります。

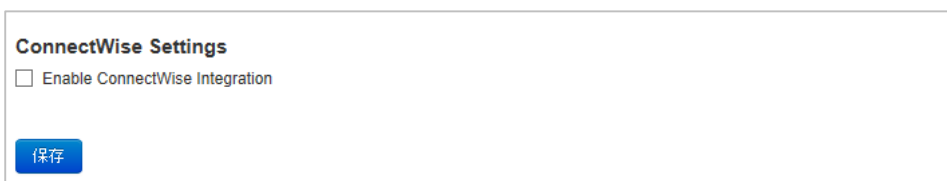


Specify the FTP servers where you can save reports.

FTP Servers: ftp.mydomain

ConnectWise Settings

ConnectWise にレポートを統合する場合はこのオプションを有効にします。



ConnectWise Settings

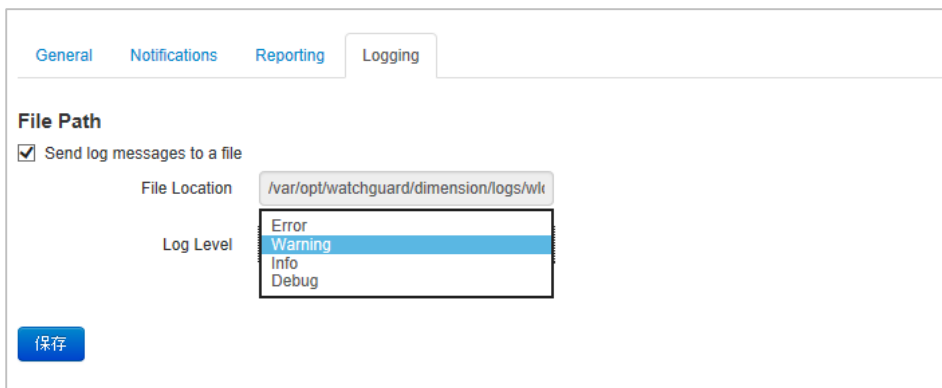
Enable ConnectWise Integration

保存

Reporting について設定できたら、保存ボタンをクリックして設定を反映させてください。

Logging

Dimension サーバー内のログ出力先を指定します。またログレベルを指定できます。



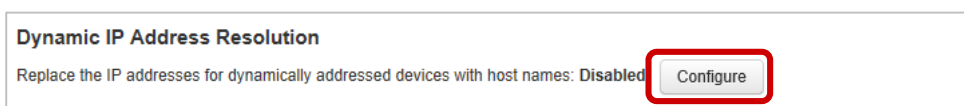
IP Address Mapping

IP Address Mapping セクションでは、レポート内の IP アドレスを名前で表現するための、IP アドレスと名前の対応を設定します。

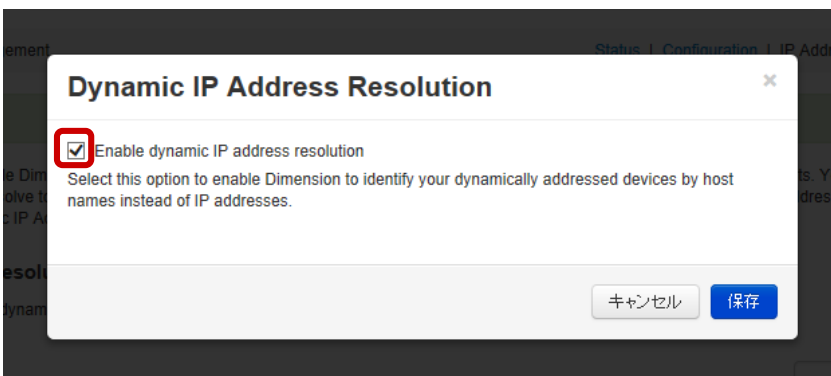
Dynamic IP Address Resolution

Dynamic IP Address Resolution は、動的に IP アドレスを割り当てられるデバイスの名前解決を有効にします。プライベートアドレスの範囲であれば、Dimension は DNS サーバーに IP アドレスを逆引きし、ホスト名とマッピングします。

この機能を有効にするには、Configure ボタンをクリックします。



Enable dynamic IP address resolution にチェックを入れ、保存します。



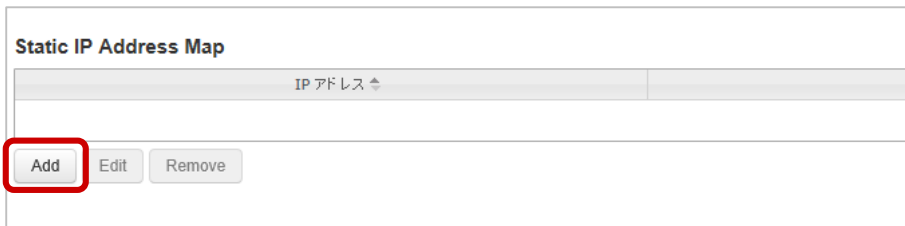
Static IP Address Map

静的 IP アドレスを持つデバイスについては、IP アドレスとホスト名のペアを設定できます。この場合 DNS サーバーに問い合わせることはありません。

このマッピングは、CSV ファイルでインポートすることもできます。

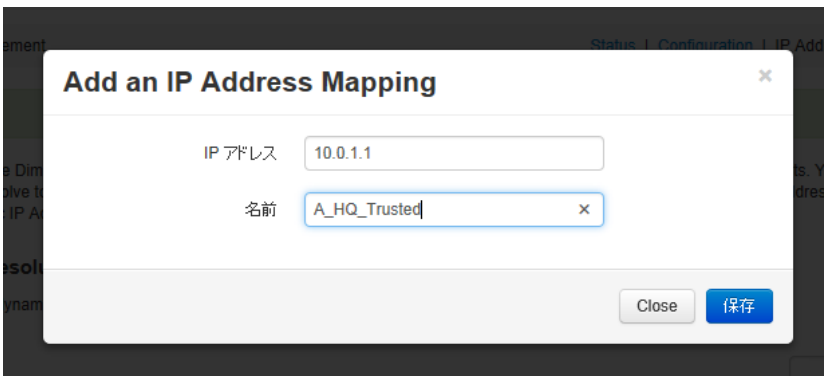
個別の追加

Add ボタンをクリックします。



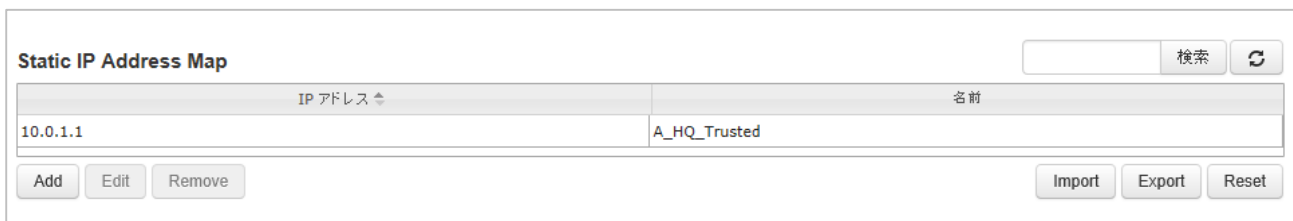
The screenshot shows the 'Static IP Address Map' interface. It features a table with a header row containing 'IP アドレス' and an empty second column. Below the table are three buttons: 'Add', 'Edit', and 'Remove'. The 'Add' button is highlighted with a red rectangle.

IP アドレスと名前を入力し、保存します。



The screenshot shows a dialog box titled 'Add an IP Address Mapping'. It has two input fields: 'IP アドレス' with the value '10.0.1.1' and '名前' with the value 'A_HQ_Trusted'. At the bottom right, there are 'Close' and '保存' (Save) buttons.

一覧に追加されます。



The screenshot shows the 'Static IP Address Map' interface after the entry has been added. The table now contains one row with '10.0.1.1' in the 'IP アドレス' column and 'A_HQ_Trusted' in the '名前' column. Below the table are buttons for 'Add', 'Edit', 'Remove', 'Import', 'Export', and 'Reset'. There is also a search bar with a '検索' (Search) button and a refresh icon.

インポート/エクスポート

CSV ファイルで、一行につき IP アドレス, 名前のフォーマットで記述し、インポートすることができます。

また、以前に割り当てられた IP アドレスを持つエントリーを再度インポートすると、既存のマッピングは、新しくインポートされたマッピングに置き換えられます。

インポートを実行するには、Import ボタンをクリックします。

The screenshot shows the 'Static IP Address Map' configuration window. It features a search bar at the top right with '検索' and a refresh icon. Below is a table with two columns: 'IP アドレス' and '名前'. The table contains one entry: IP address '10.0.1.1' and name 'A_HQ_Trusted'. At the bottom, there are buttons for 'Add', 'Edit', 'Remove', 'Import', 'Export', and 'Reset'. The 'Import' button is highlighted with a red rectangular box.

CSV ファイルを指定し、OK をクリックします。

The screenshot shows a dialog box titled 'Import Map File'. The text inside reads: 'Select a CSV map file with the IP address/name pairs to import into the Static IP Address Map.' Below the text is a text input field containing the file path 'C:\Users\user\Desktop\mapping.csv' and a 'Browse...' button. At the bottom of the dialog, there are two buttons: 'キャンセル' (Cancel) and 'OK'.

次のようにインポートされます。

The screenshot shows the 'Static IP Address Map' configuration window after the import operation. The table now contains six entries:

IP アドレス	名前
10.0.1.1	A_HQ_Trusted_01
10.0.2.1	A_HQ_Trusted_02
10.0.3.1	A_HQ_Trusted_03
10.0.4.1	A_HQ_Trusted_04
10.0.5.1	A_HQ_Trusted_05
10.0.6.1	A_HQ_Trusted_06

The 'Import' button is now disabled, and the 'Export' button is active.

エクスポートボタンをクリックすると、現時点のマッピングがすべて CSV 形式で保存できます。

The screenshot shows the 'Static IP Address Map' configuration window with the 'Export' button highlighted by a red rectangular box. Below the window, a file save dialog box is open, asking: 'Do you want to open or save ip_domain_map_2014_08_01.csv from 172.16.1.183?'. The dialog has buttons for 'Open', 'Save', and 'Cancel', and a close button (X). The zoom level is set to 100%.

Diagnostics

Diagnostics では、診断ログの閲覧や削除を実行することができます。

また、Dimension サーバー上のアクティブなプロセスを確認することができます。

Purge Diagnostic Log Messages

診断ログメッセージの削除機能です。デバッグレベル以上のすべての診断ログメッセージを削除し、データベースのスペースを節約することができます。

Purge Diagnostic Log Messages ボタンをクリックします。

Purge Diagnostic Log Messages

Use this option to delete all Diagnostic log messages (debug level or higher) generated by your devices from the Log Server database.

Purge Diagnostic Log Messages

即座に診断メッセージがデータベースから削除されます。

Process List

Dimension サーバー上のアクティブなプロセスを確認ことができ、その詳細(CPU 使用率やメモリの使用量など)も確認できます。

Process List



PID	名前	CPU	Memory	Create Time	Command Line
1273	httpd	1.0%	35.87MB	2014-07-31 13:28	/opt/watchguard/dimension/bin httpd -d /opt/watchguard/dimension -d /opt/watchguard/dimension/share/wlogserver -f /etc/opt/watchguard/dimension/wlogserver/conf/httpd.conf
1271	httpd	0.0%	3.47MB	2014-07-31 13:28	/opt/watchguard/dimension/bin httpd -d /opt/watchguard/dimension -d /opt/watchguard/dimension/share/wlogserver -f /etc/opt/watchguard/dimension/wlogserver/conf/httpd.conf
1267	wlcollector	0.2%	15.28MB	2014-07-31 13:28	/opt/watchguard/dimension/bin/wlcollector
1262	wlcollector	0.0%	4.53MB	2014-07-31 13:28	/opt/watchguard/dimension/bin/wlcollector

Log Messages

ログサーバーとログコレクターによって生成されたログを表示できます。表示の行数も指定できます。

Log Server タブを選択してログサーバーの表示

Log Messages

Select a tab to review the log messages generated by the Log Server or the Log Collector.

Log Server Log Collector

Lines in the Log File to Show

```
<SrvProcess d="2014-07-31T13:26:34Z" orig="report03" pri="2" app="ap_logging" proc_id="30342-1097119936" mc="8196" msg="Error (8196), DB_Cursor: exception in ex
<SrvProcess d="2014-07-31T13:26:34Z" orig="report03" pri="2" app="ap_logging" proc_id="30342-1097119936" mc="8196" msg="Error (8196), DB_Connection: exception i
<SrvProcess d="2014-07-31T13:26:34Z" orig="report03" pri="2" app="ap_logging" proc_id="30342-1097119936" mc="8196" msg="Error (8196), DB_Connection: exception i
<SrvProcess d="2014-07-31T13:26:34Z" orig="report03" pri="2" app="ap_logging" proc_id="30342-1097119936" mc="8196" msg="Error (8196), DB_Connection: exception i
<SrvProcess d="2014-07-31T13:26:34Z" orig="report03" pri="2" app="ap_logging" proc_id="30342-1097119936" mc="8196" msg="Error (8196), DB_Cursor: exception in op
<SrvProcess d="2014-07-31T13:26:34Z" orig="report03" pri="2" app="ap_logging" proc_id="30342-1097119936" mc="8196" msg="Error (8196), DB_Cursor: exception in ex
<SrvProcess d="2014-07-31T13:26:34Z" orig="report03" pri="2" app="ap_logging" proc_id="30342-1097119936" mc="8196" msg="Error (8196), DB_Connection: exception i
<SrvProcess d="2014-07-31T13:26:34Z" orig="report03" pri="2" app="ap_logging" proc_id="30342-1097119936" mc="8196" msg="Error (8196), DB_Connection: exception i
<SrvProcess d="2014-07-31T13:26:34Z" orig="report03" pri="2" app="ap_logging" proc_id="30342-1097119936" mc="8196" msg="Error (8196), DB_Cursor: exception in op
<SrvProcess d="2014-07-31T13:26:34Z" orig="report03" pri="2" app="ap_logging" proc_id="30342-1097119936" mc="8196" msg="Error (8196), *****CLEAN Exception: The
<SrvProcess d="2014-07-31T13:46:58Z" orig="report03" pri="2" app="ap_logging" proc_id="1273:1420343040" mc="8196" msg="Error (8196), Unable to access the remote t
<SrvProcess d="2014-07-31T13:53:04Z" orig="report03" pri="2" app="ap_logging" proc_id="1273:905819904" mc="8196" msg="Error (8196), Get archive list: unable to acce
<SrvProcess d="2014-07-31T14:38:11Z" orig="report03" pri="2" app="ap_logging" proc_id="1273:1006532352" mc="8196" msg="Error (8196), ==== NOTIFY_SEND_EMAIL
<SrvProcess d="2014-07-31T14:40:55Z" orig="report03" pri="2" app="ap_logging" proc_id="1273:964568832" mc="8196" msg="Error (8196), ==== NOTIFY_SEND_EMAIL E
```

Log Collector タブを選択してログコレクターのログを表示

Log Server Log Collector

Lines in the Log File to Show

```
<SrvProcess d="2014-08-01T10:11:09Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:649918208" mc="9233" rc="0" msg="Information (9233), resolver task run
<SrvProcess d="2014-08-01T10:11:09Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:649918208" mc="9234" rc="0" msg="Information (9234), resolver task pro
<SrvProcess d="2014-08-01T10:12:01Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:671086336" mc="9244" msg="Information (9244), **rate [RECEIVE 0/s WF
<SrvProcess d="2014-08-01T10:12:02Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:649918208" mc="9233" rc="0" msg="Information (9233), resolver task run
<SrvProcess d="2014-08-01T10:12:08Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:771733248" mc="9244" msg="Information (9244), -----segment 20140801
<SrvProcess d="2014-08-01T10:13:01Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:671086336" mc="9244" msg="Information (9244), **rate [RECEIVE 0/s WF
<SrvProcess d="2014-08-01T10:13:08Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:771733248" mc="9244" msg="Information (9244), -----segment 20140801
<SrvProcess d="2014-08-01T10:13:10Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:649918208" mc="9244" msg="Information (9244), 172.16.1.121: Domain n
<SrvProcess d="2014-08-01T10:13:10Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:649918208" mc="9234" rc="0" msg="Information (9234), resolver task pro
<SrvProcess d="2014-08-01T10:14:01Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:671086336" mc="9244" msg="Information (9244), **rate [RECEIVE 0/s WF
<SrvProcess d="2014-08-01T10:14:08Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:771733248" mc="9244" msg="Information (9244), -----segment 20140801
<SrvProcess d="2014-08-01T10:14:23Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:649918208" mc="9233" rc="0" msg="Information (9233), resolver task run
<SrvProcess d="2014-08-01T10:15:01Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:671086336" mc="9244" msg="Information (9244), **rate [RECEIVE 0/s WF
<SrvProcess d="2014-08-01T10:15:08Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:771733248" mc="9244" msg="Information (9244), -----segment 20140801
<SrvProcess d="2014-08-01T10:15:25Z" orig="report03" pri="6" app="ap_collector" proc_id="1267:649918208" mc="9244" msg="Information (9244), 172.16.1.171: Domain n
```

Database

Database メニューでは、データベースのモニタリングができます。

Database Status

現在のデータベースの稼働状況を確認することができます。

また、Start, Stop, Restart ボタンで、データベースの起動、停止、再起動を行なうことができます。

Database Status

Availability	接続済み (built-in database)
場所	/var/opt/watchguard/dimension/data/db
Uptime	0 days, 21 hours, 1 minute, 3 seconds
CPU Usage	0.4%
Memory Usage	242.27MB
Disk Usage	0.05GB of 32GB used (39GB free on disk)

Process List

Dimension データベースである PostgreSQL のプロセスが確認できます。

Process List					
Database process list 🔄					
PID	名前 ↕	CPU	Memory	Create Time	Command Line
974	postgres	0.0%	13.42MB	2014-07-31 13:28	/opt/watchguard/dimension/bin/postgres -D /var/opt/watchguard/dimension/data/db
1234	postgres: autovacuum launcher process	0.0%	2.89MB	2014-07-31 13:28	postgres: autovacuum launcher process
1231	postgres: checkpointer process	0.0%	9.39MB	2014-07-31 13:28	postgres: checkpointer process
1197	postgres: logger process	0.0%	1.04MB	2014-07-31 13:28	postgres: logger process
1235	postgres: stats collector process	0.0%	1.45MB	2014-07-31 13:28	postgres: stats collector process
1233	postgres: wal writer process	0.0%	5.32MB	2014-07-31 13:28	postgres: wal writer process
1269	postgres: wuser wlog 127.0.0.1(60425) idle in transaction	0.0%	9.98MB	2014-07-31 13:28	postgres: wuser wlog 127.0.0.1(60425) idle in transaction
1351	postgres: wuser wlog 127.0.0.1(60426) idle in transaction	0.0%	12.44MB	2014-07-31 13:28	postgres: wuser wlog 127.0.0.1(60426) idle in transaction
1352	postgres: wuser wlog 127.0.0.1(60427) idle in transaction	0.0%	5.41MB	2014-07-31 13:28	postgres: wuser wlog 127.0.0.1(60427) idle in transaction
1353	postgres: wuser wlog 127.0.0.1(60428) idle in transaction	0.0%	4.34MB	2014-07-31 13:28	postgres: wuser wlog 127.0.0.1(60428) idle in transaction

Log Messages

Log Messages

Review the log messages generated by the Dimension database.

Select Log File

Lines in the Log File to show

```
2014-07-18 10:24:36 UTC LOG: received fast shutdown request
2014-07-18 10:24:36 UTC LOG: aborting any active transactions
2014-07-18 10:24:36 UTC FATAL: terminating connection due to administrator command
2014-07-18 10:24:36 UTC FATAL: terminating connection due to administrator command
2014-07-18 10:24:36 UTC FATAL: terminating connection due to administrator command
2014-07-18 10:24:36 UTC FATAL: terminating connection due to administrator command
2014-07-18 10:24:36 UTC FATAL: terminating connection due to administrator command
2014-07-18 10:24:36 UTC FATAL: terminating connection due to administrator command
2014-07-18 10:24:36 UTC FATAL: terminating connection due to administrator command
2014-07-18 10:24:36 UTC FATAL: terminating connection due to administrator command
2014-07-18 10:24:36 UTC FATAL: terminating connection due to administrator command
2014-07-18 10:24:36 UTC FATAL: terminating connection due to administrator command
2014-07-18 10:24:36 UTC FATAL: terminating connection due to administrator command
```

Status Report

Status Report では、Dimension に接続されているデバイス、およびログサーバーやデータベースの統計情報が含まれます。ログメッセージ数やデータベースのレコード数、テーブルのサイズ情報が含まれていますので、Dimension サーバーのストレージ要件を決定するのに役立ちます。

Status Report

The Status Report includes contains information related to the database used by WatchGuard Dimension.

Log Server Database Statistics Report

```
=====
Start date:          2014-08-01 UTC
Days to report:     1
Collect detailed statistics: Disabled
Collect statistics for: The 10 appliances with the most traffic logs
=====

Date: 2014-08-01
=====

Appliances with logs: 1
Appliances in report:
  T10-D-01 (D0FA0283494F2):

Statistics for appliance T10-D-01 (D0FA0283494F2):
-----
Log Counts:
Traffic:    242
Event:      0
Alarm:      0
Performance: 0
Status/Debug: 0

Average Log Rates:
Traffic: 0.01/s
Status/Debug: 0.00/s
Alarm: 0.00/min
```


User Management

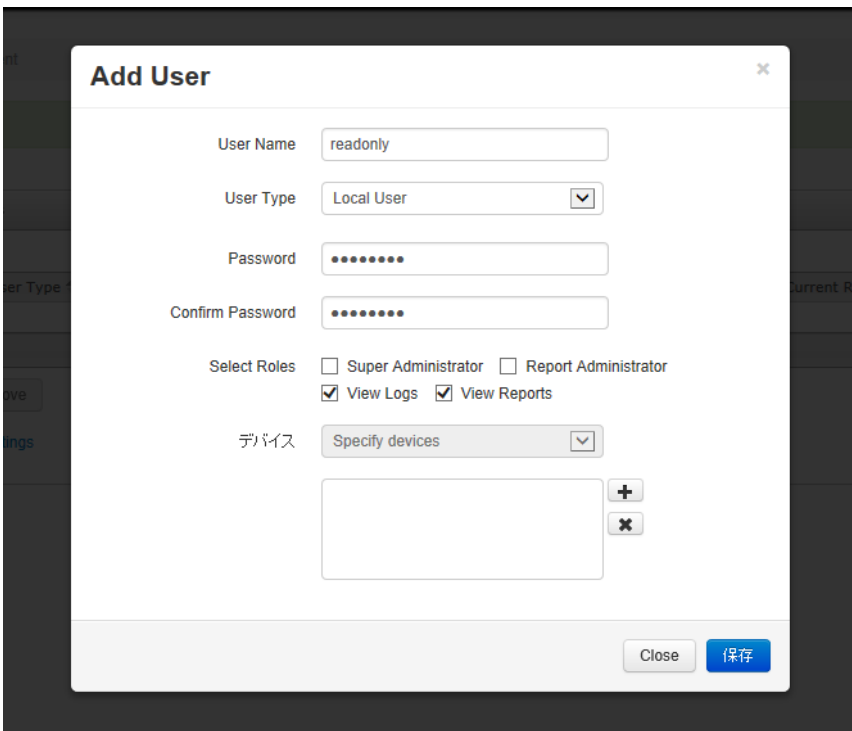
User Management では、Dimension に接続するユーザーの新規追加、編集、削除ができます。また割り当てる Role(役割)もユーザーごとに細かく指定できます。

ユーザーの追加

Add ボタンをクリックします。

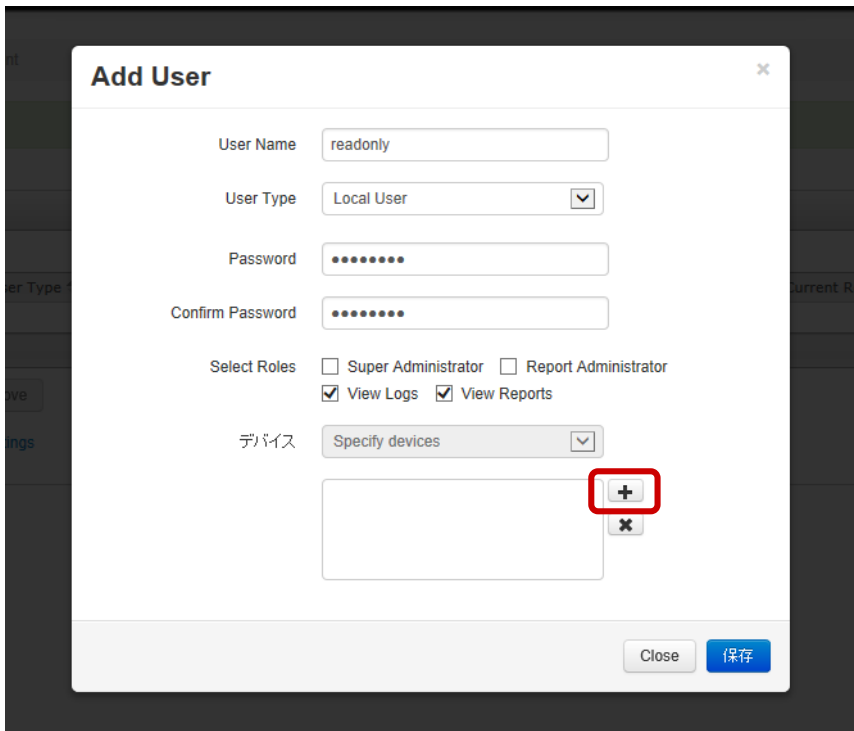


ユーザー追加画面になります。User Name, Password, Confirm Password, に新規ユーザーの名前とパスワードを入力します。



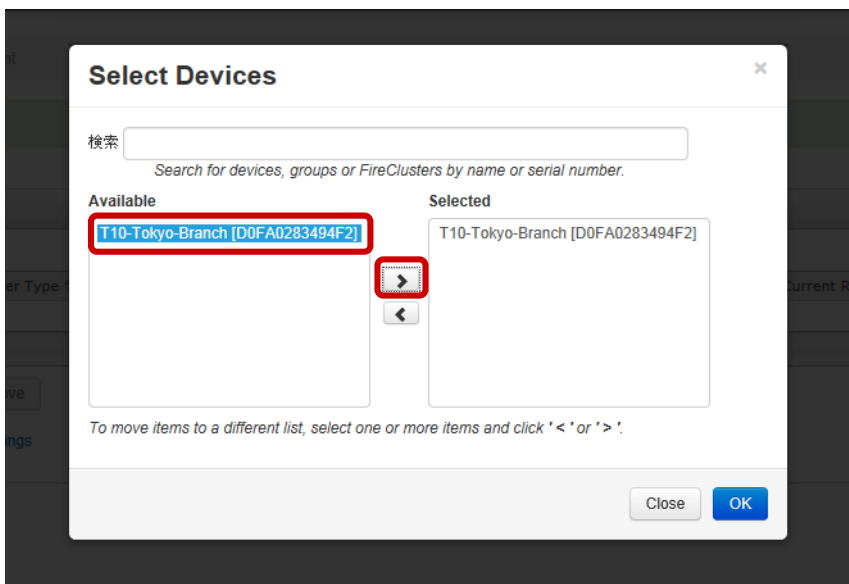
Select Roles は、付与する権限と役割を設定します。ログとレポートの閲覧だけなら View Logs と View Reports にチェックを入れます。ログは見せないでレポートだけ見せたい場合は、View Reports のみをチェックします。

次に、どのデバイスのレポートの閲覧を許可するのか、設定します。デバイスのセクションにある **+** ボタンをクリックします。



左側に閲覧可能なデバイスの一覧が表示されています。

その中から閲覧させてよいデバイスを選択し、**>** ボタンで右側の閲覧させるデバイスをコピーします。



OK で Add User の画面に戻ると、追加するユーザーが閲覧できるデバイスが追加されているのを確認できます。

保存ボタンをクリックして、設定を反映させます。

User management の画面に戻ると、readonly ユーザーが追加されているのを確認できます。

Manage Users and Roles		
User Type	User Name	Current Roles
admin	Local User	Super Administrator
readonly	Local User	View Logs,View Reports

1 ページ中 1 ページ目 10 2 件中 1 - 2 を表示

Add Edit Remove

[Show Active Directory Settings](#)

ユーザーの編集

編集したいユーザーを選択し、Edit ボタンをクリックします。

User Type	User Name	Current Roles
AcompanyReportUser	Local User	View Logs,View Reports
admin	Local User	Super Administrator
BcompanyReportUser	Local User	View Logs,View Reports
CcompanyReportUser	Local User	View Logs,View Reports
DcompanyReportUser	Local User	View Logs,View Reports
readonly	Local User	View Logs,View Reports

1 ページ中 1 ページ目 10 6 件中 1 - 6 を表示

Add Edit Remove

[Show Active Directory Settings](#)

変更したい項目を修正します。

Edit User

User Name: readonly

User Type: Local User

Change Password

Select Roles: Super Administrator Report Administrator
 View Logs View Reports

デバイス: Specify devices

T10-D-01 [D0FA0283494F2]

Close 保存

User Name は変更できません。

ユーザーの削除

削除対象のユーザーを選択し、Remove ボタンをクリックします。

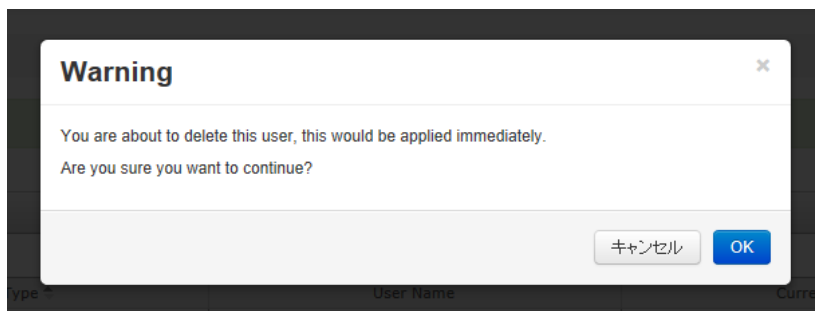
CcompanyReportUser	Local User	View Logs,View Reports
DcompanyReportUser	Local User	View Logs,View Reports
deleteuser	Local User	View Logs,View Reports
readonly	Local User	View Logs,View Reports

1 ページ中 1 ページ目 10 7 件中 1 - 7 を表示

Add Edit **Remove**

[Show Active Directory Settings](#)

警告がでますので、OK をクリックします。



以上で削除が完了します。

Active Directory を利用する

Active Directory 認証を有効にするには、AD との有効な接続がひとつ以上あり、AD サーバーの SSL 証明書をインポートしておく必要があります。

設定をするには、Show Active Directory Settings を開きます。

Active Directory Settings

Note: Before you can use Active Directory authentication, you must enable LDAP over SSL in the Active Directory domain settings.

Enable Active Directory Authentication

Active Directory domain: AD Domain +

x

Test

Validate the SSL certificate from the domain controller

SSL certificates that are signed by most well-known, public Certificate Authorities (CAs) are automatically trusted. For a list of supported CAs, [click here](#). To use a certificate signed by a CA that is not in the list, you must import the certificate.

Import Certificate

以下、手順のみ掲載します。

1. Enable Active Directory Authentication にチェックを入れます。
2. Active Directory Domain で Active Directory サーバーのドメインを入力し をクリックします。ドメイン名が一覧に表示されます。
3. Test ボタンをクリックします。ディメンションでは、Active Directory サーバーに接続を確立できることを確認します。
4. ドメイン コントローラー上の SSL 証明書が有効であることを確認するには、Validate the SSL certificate from the domain controller のチェック ボックスを選択します。
5. 保存をクリックします。

System Settings

System Settings メニューからは、Dimension のステータス確認、システム保守のためのタスクを実行できません。Status, Configuration, Diagnostics のセクションに分かれています。

[Home](#) / [System Settings](#)

[Status](#) | [Configuration](#) | [Diagnostics](#)

Status

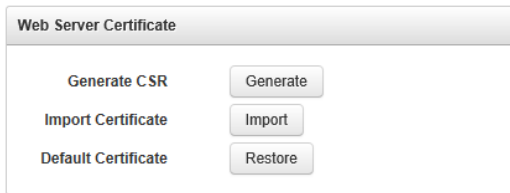
Dimension System Information

Dimension のシステムの状態を確認できます。ここで利用できる情報は、Dimension をインストールした仮想マシンプラットフォームに依存します。

Dimension System Information	
System Name	report03
Operating System	Linux 3.2.0-23-virtual (x86_64)
バージョン	1.1 U1 (442674)
CPU Usage	0.6%
Memory Usage	258MB of 2100MB used (12.3%)
Current Time	Mon Aug 4 14:27:35 UTC 2014
IP アドレス	● 172.16.1.183/24 (eth0)

Web Server Certificate

このセクションでは、CSR ファイルの生成、証明書のインポート、CA 証明書の管理できます。

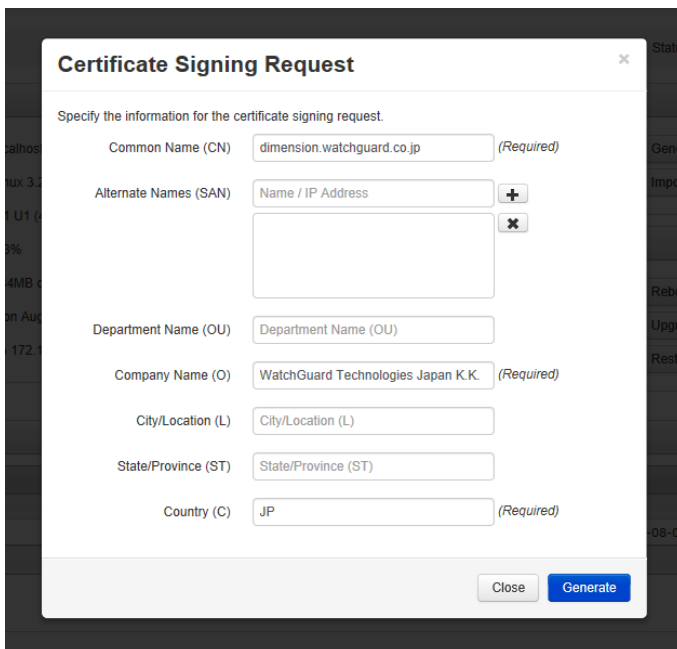


The image shows a panel titled "Web Server Certificate" with three rows of controls:

Generate CSR	Generate
Import Certificate	Import
Default Certificate	Restore

Generate CSR

CSR ファイルを生成します。Generate ボタンをクリックすると、Certificate Signing Request ダイアログが表示されます。Common name, Company Name, Country を入力します。それ以外の項目はオプションです。



The image shows a "Certificate Signing Request" dialog box with the following fields and controls:

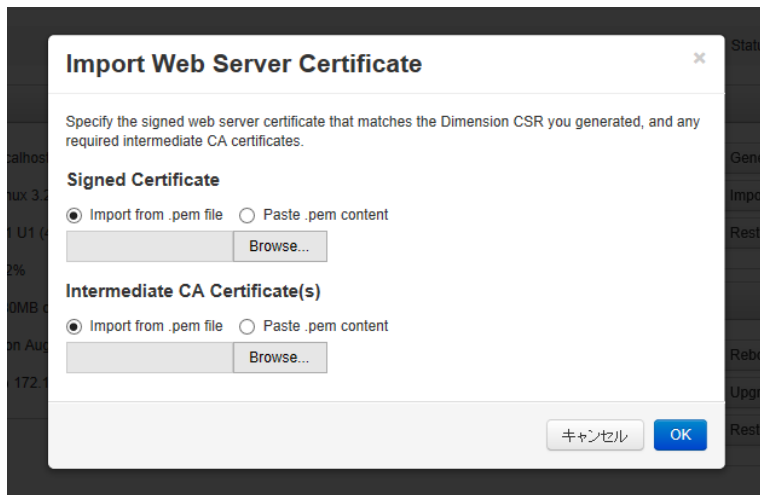
- Common Name (CN): dimension.watchguard.co.jp (Required)
- Alternate Names (SAN): Name / IP Address (with + and x buttons)
- Department Name (OU): Department Name (OU)
- Company Name (O): WatchGuard Technologies Japan K.K. (Required)
- City/Location (L): City/Location (L)
- State/Province (ST): State/Province (ST)
- Country (C): JP (Required)

Buttons: Close, Generate

Import Certificate

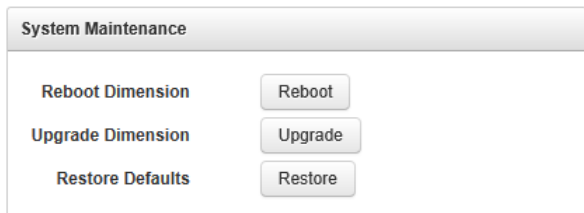
Web サーバー証明書をインポートするには Import Certificate ボタンをクリックします。

Import Web Server Certificate の画面になるので Import from .pem file で証明書ファイルを読み込むか、Paste .pem content を選択して証明書の内容を貼り付けてインポートすることができます。



System Maintenance

このセクションでは、Dimension の再起動、Dimension のアップグレード、Dimension のリストアができます。



Reboot Dimension

Dimension を安全に再起動します。

Upgrade Dimension

後述の Dimension のアップグレード手順を参照してください。

Restore Defaults

Dimension をデフォルトの状態に戻すことができます。これを実行すると、Dimension を仮想マシンプラットフォームにデプロイした直後の状態になります。

デフォルト状態の Dimension を利用するには、再度初期セットアップウィザードの手順を実施してください。

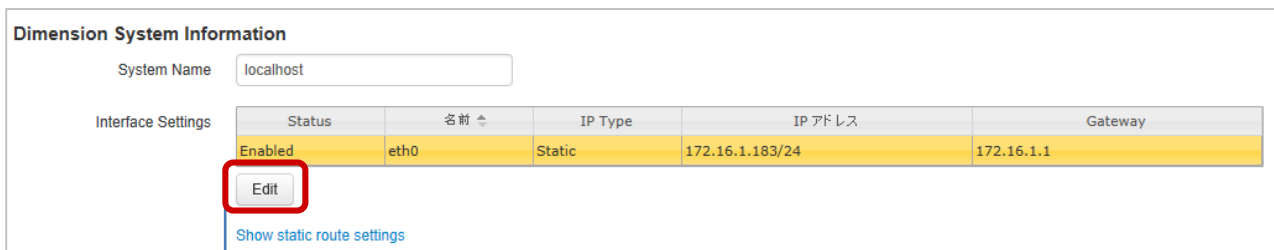
Configuration

このセクションでは、Dimension のセットアップウィザードで設定した、ネットワークインターフェースや他の項目の設定変更ができます。また、DNS や NTP サーバーの設定も変更できます。

Dimension System Information

Dimension サーバーのホスト名とネットワーク インターフェースの情報を参照できます。

Edit ボタンをクリックすると、設定変更が可能です。



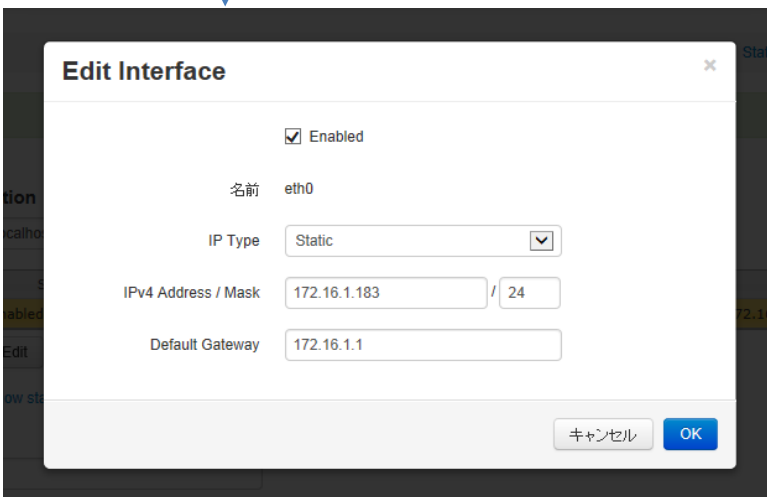
Dimension System Information

System Name: localhost

Status	名前 ↑	IP Type	IP アドレス	Gateway
Enabled	eth0	Static	172.16.1.183/24	172.16.1.1

Edit

Show static route settings



Edit Interface

Enabled

名前: eth0

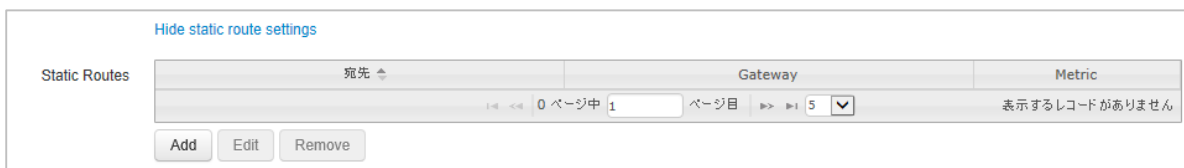
IP Type: Static

IPv4 Address / Mask: 172.16.1.183 / 24

Default Gateway: 172.16.1.1

キャンセル OK

Show static route settings のリンクをクリックすると、静的ルートの追加・編集・削除が行なえます。



Hide static route settings

宛先 ↑	Gateway	Metric
------	---------	--------

0 ページ中 1 ページ目 5

表示するレコードがありません

Add Edit Remove

Domain Settings

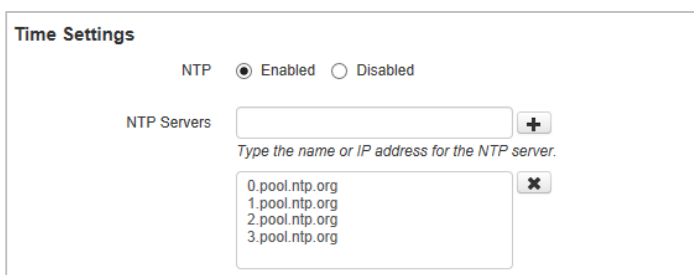
DNS サーバーの追加と削除が行なえます。



The screenshot shows the 'Domain Settings' form. It has a 'Domain Name' text input field. Below it is the 'DNS Servers' section, which includes a text input field containing '10.0.110.100', a small 'x' icon to its right, and a '+' icon to its left. Below this is a list box containing '10.0.100.100' and a small 'x' icon to its right.

Time Settings

NTP サーバーの参照の有効化・無効化、NTP サーバーの追加と削除が行なえます。

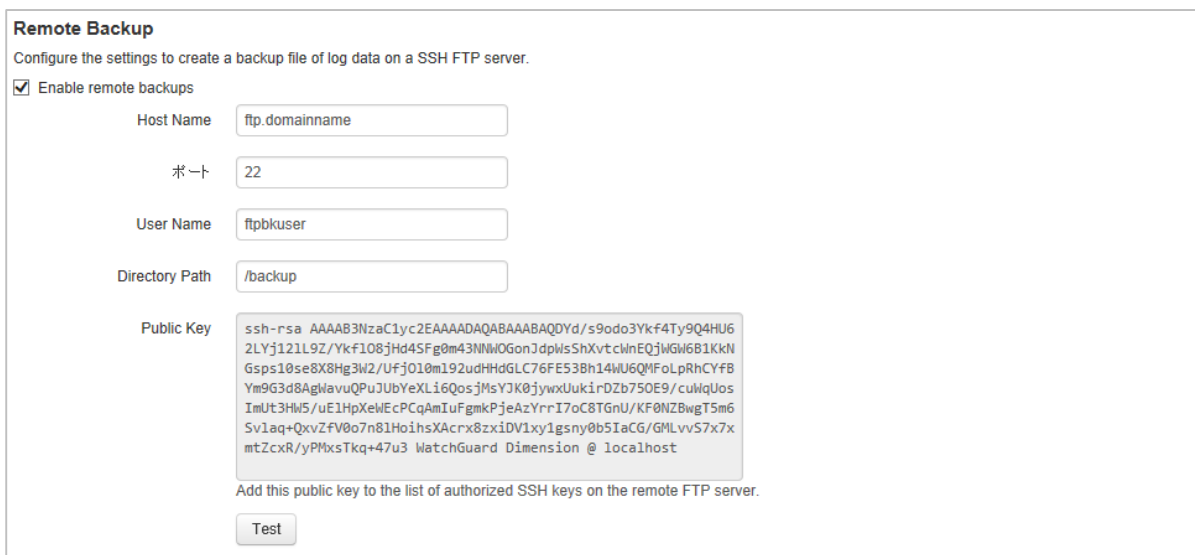


The screenshot shows the 'Time Settings' form. It has an 'NTP' section with two radio buttons: 'Enabled' (selected) and 'Disabled'. Below this is the 'NTP Servers' section, which includes a text input field, a '+' icon to its right, and the text 'Type the name or IP address for the NTP server.' Below this is a list box containing '0.pool.ntp.org', '1.pool.ntp.org', '2.pool.ntp.org', and '3.pool.ntp.org', with a small 'x' icon to its right.

Remote Backup

ログサーバーDB のログデータのバックアップをリモートホストに保存できます。SSH FTP サーバーがあり、RSA キーに基づく認証がサポートされている必要があります。

Enable remote backups にチェックを入れ、各項目にサーバー情報を入力してください。



The screenshot shows the 'Remote Backup' form. It has a title 'Remote Backup' and a subtitle 'Configure the settings to create a backup file of log data on a SSH FTP server.' Below this is a checkbox labeled 'Enable remote backups' which is checked. The form has several text input fields: 'Host Name' (ftp.domainname), 'ポート' (22), 'User Name' (ftpbkuser), and 'Directory Path' (/backup). There is also a 'Public Key' section with a text area containing a long SSH public key string. Below the text area is the text 'Add this public key to the list of authorized SSH keys on the remote FTP server.' and a 'Test' button.

設定を変更したら、保存ボタンをクリックし、設定を反映させてください。

Diagnostics

このセクションでは、オペレーティングシステムおよび Dimension サーバーの診断タスクを実行できます。

Home / System Settings Status | Configuration | Diagnostics
Operating System Dimension Server

Operating System タブ

Ping

ping コマンドを実行できます。

Ping
Ping IP address or host name

```
PING 172.16.1.137 (172.16.1.137) 56(84) bytes of data:
64 bytes from 172.16.1.137: icmp_req=1 ttl=128 time=0.549 ms
64 bytes from 172.16.1.137: icmp_req=2 ttl=128 time=0.537 ms
64 bytes from 172.16.1.137: icmp_req=3 ttl=128 time=0.561 ms

--- 172.16.1.137 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.537/0.549/0.561/0.009 ms
```

System Diagnostics

診断情報の取得ができます。ダウンロードボタンをクリックすると、wg_dimension_support.tgz という名前のファイルをダウンロードできます。

サポートを受ける際にこのファイルを求められたら、ダウンロードボタンをクリックし、取得してください。

System Diagnostics
Download a file with diagnostic information about your WatchGuard Dimension system.

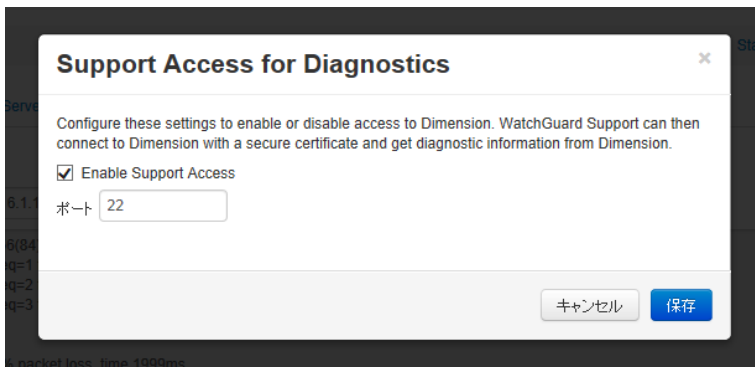
Support Access for Diagnostics

SSH でのアクセスを有効にします。これはウォッチガードのサポートを受ける際にリモートでのアクセスを許可するなどの目的で設定します。

Configure ボタンをクリックします。

Support Access for Diagnostics
Enable WatchGuard Support to connect to your Dimension system.

Support Access for Diagnostics ダイアログが表示されますので、Enable Support Access にチェックを入れます。ポートは 22 のままか、他のポートを使用するには別の番号を入力します。

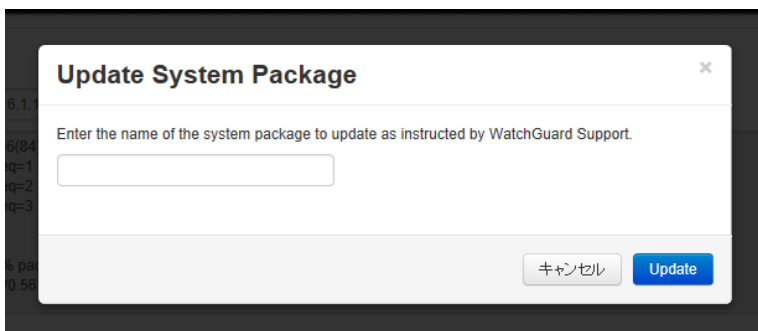


Update System Package

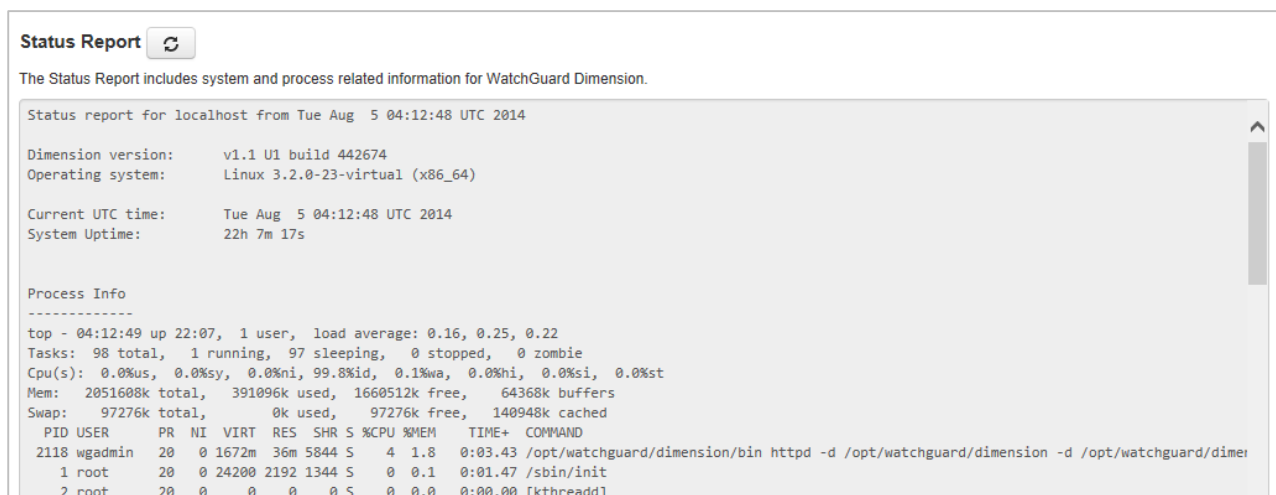
問題解決のために、ウォッチガード サポートから指定された更新パッケージを適用するためのものです。



Update System Package でアップデートファイルを指定し、Update ボタンをクリックします。



Status Report



Dimension Server タブ

Process Information

Dimension サーバーのプロセス情報を参照できます。


Process Information	
CPU	0.2%
Memory	44.10MB
Uptime	0 days, 23 hours, 1 minute, 14 seconds

Log Messages

Dimension のウェブサーバーから出力されたログを見ることができます。

Log Messages

Review the log messages generated by the Dimension web server.

Lines in the Log File to Show 

```
[04/Aug/2014:06:47:25] Time to call ws_system_scripts.get_system_stats(): 0.010 seconds
[04/Aug/2014:06:47:25] Time to call ws_system_scripts.using_built_in_webserver_cert(): 0.000 seconds
[04/Aug/2014:06:47:55] Time to call ws_system_scripts.get_system_stats(): 0.000 seconds
[04/Aug/2014:06:47:55] Time to call ws_system_scripts.using_built_in_webserver_cert(): 0.000 seconds
[04/Aug/2014:06:48:25] Time to call ws_system_scripts.get_system_stats(): 0.000 seconds
[04/Aug/2014:06:48:25] Time to call ws_system_scripts.using_built_in_webserver_cert(): 0.000 seconds
[04/Aug/2014:06:48:55] Time to call ws_system_scripts.get_system_stats(): 0.000 seconds
```

DIMENSION のアップグレード手順

Dimension は機能の向上やバグフィックスのため、時折アップデートが行なわれます。ここに記載された手順に沿って、必要に応じてアップグレード作業を実施してください。

事前準備

Dimension のアップグレードに当たっては、あらかじめウォッチガード ポータル(US)のサポートページより、アップグレード用のファイルをダウンロードしておきます。

必要なファイルは以下のとおりです ([X]と[Y]の部分はバージョンを表わす数字になります)。

WatchGuard Dimension OS X.Y Upgrade File

```
watchguard-dimension_[X]_[Y]_apt.tgz
```

バージョンによっては次のファイルも必要になります。

WatchGuard Dimension OS X.Y Upgrade Preparation File

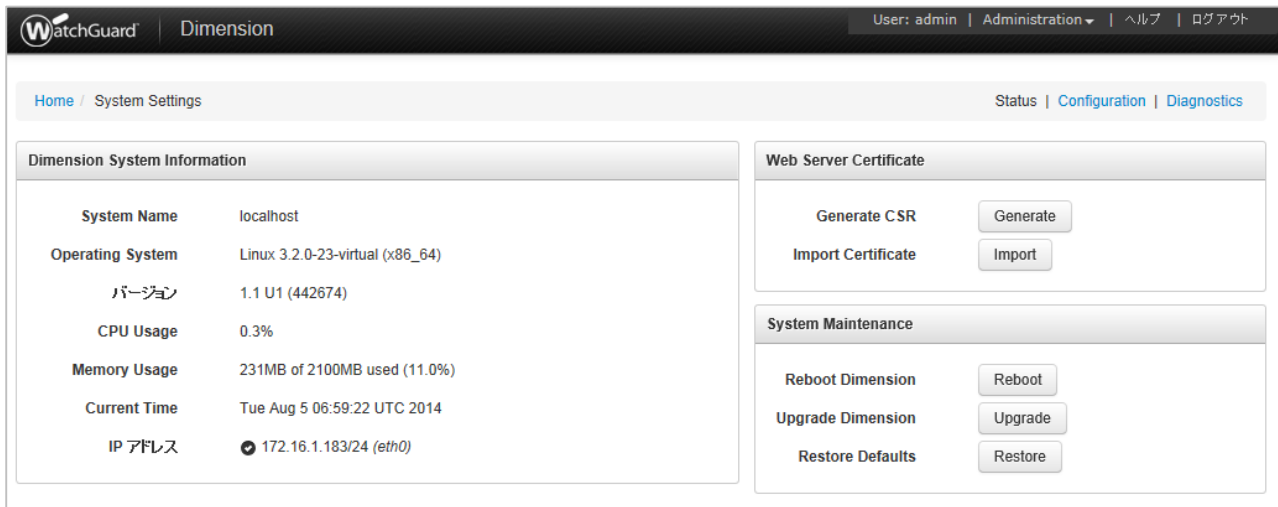
```
watchguard-dimension_[X]_[Y]_amd64.deb
```

例えば、1.0 から 1.2 にアップグレードする際には、この Preparation File でのアップグレードが必要になる、などのケースがあります。ダウンロードする際にリリースノートをご確認ください。

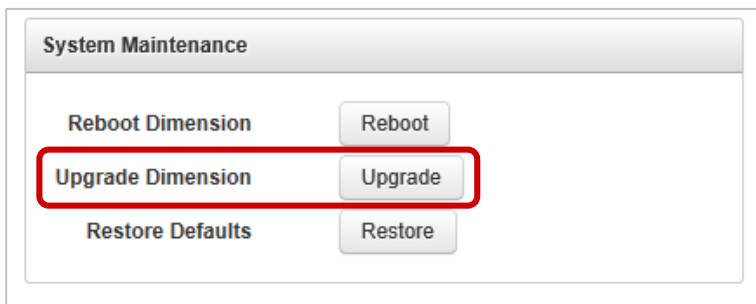
この手順書では、WatchGuard Dimension OS X.Y Upgrade File のみの手順を解説します。

アップグレード手順

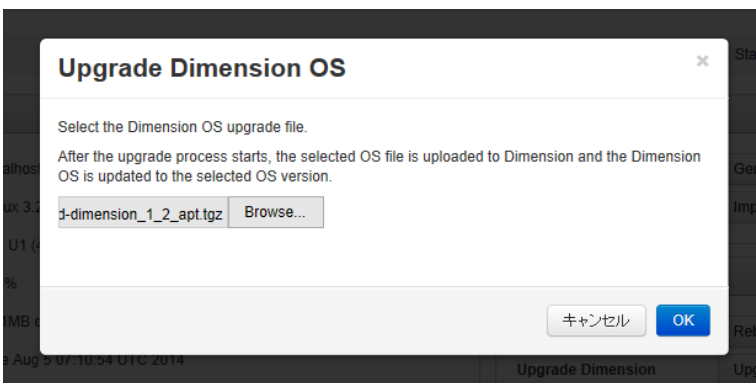
Administration メニューー System Settings を開きます。



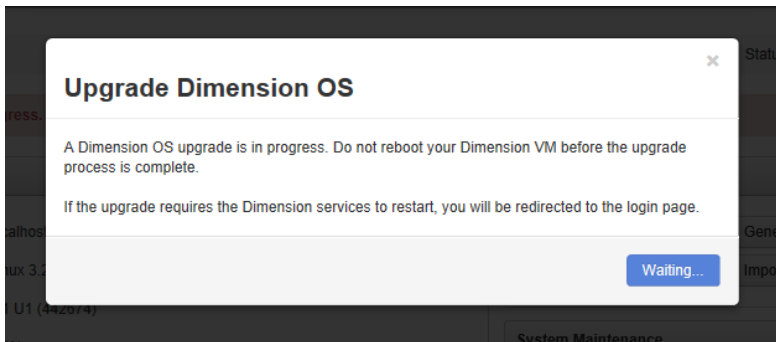
そのページの System Maintenance エリアにある Upgrade Dimension の項の Upgrade ボタンをクリックします。



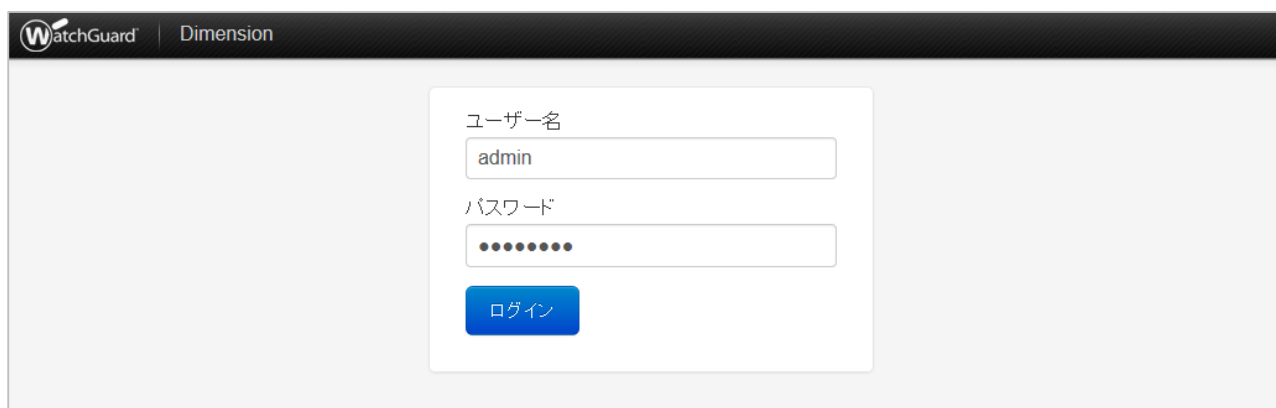
Upgrade Dimension OS のダイアログで、アップグレード用のファイルを選択し、OK をクリックします。



アップグレード中であることが表示されます。この間、一切の操作を控えてください。



アップグレードが完了すると、自動的にログイン画面にリダイレクトしますので、再度ログインしてください。



Administration メニュー - System Settings を開き、Dimension System Information のバージョンを確認し、目的のバージョンになっていたら、アップグレードは成功です。

おわりに

Dimension 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。

このガイドを通して、Dimension の導入がいかに容易か、MSSP としていかにスピーディーにセキュリティ可視化ソリューションを提供できるか、実感していただけたと思います。

WatchGuard XTM が御社のセキュリティ向上にお役に立てれば幸いです。