

# EW50 クイックスタート

フエニックス・コンタクト株式会社  
IMA統括本部プロダクトマーケティング部



2021. 9..29 改版

- 1.0 初版
- 2.1 データロギング追記 (2019.11.8)
- 3.0 初期化、ファームウェア更新他 (2021.9.14)
- 3.1 設定ファイル読み書き (2021.9.29)

はじめに

本書は、EW50の機能についての限定的な説明書です。詳細な機能仕様説明は、下記のEtherWANウェブサイトにある英文マニュアルを参照してください。

[https://www.etherwan.com/sites/default/files/ew50\\_manual.pdf](https://www.etherwan.com/sites/default/files/ew50_manual.pdf)

## 目次

1. 基本的な接続.....	3
1.1. SIM カードのセットとアンテナ、電源接続.....	3
1.2. 初期状態の EW50 にログイン.....	4
1.3. SIM カード情報の設定 .....	4
1.4. 3G/4G の接続確認.....	5
1.5. DHCP クライアントの EW50 経由のインターネットアクセス.....	6
1.6. 静的 IP アドレスをつけた LAN 側機器の EW50 経由のインターネットアクセス.....	6
2. VPN .....	6
2.1. IPSec VPN.....	6
2.1.1. IPSec VPN 設定の作成 .....	6

A) サーバー側VPN設定の作成.....	6
B) クライアント側IPSec VPN設定の作成.....	9
3. データロギング.....	12
3.1. MODBUS ゲートウェイの設定 .....	12
3.1.1. シリアル接続.....	12
3.1.2. シリアルポートの設定 .....	12
3.1.3. MODBUS の設定 .....	13
3.2. データロギングの設定.....	14
3.2.1. Modbus Proxy Rule List Configuration の設定(データ収集方法の設定).....	14
3.2.2. Scheme の設定 (データロギング方法の設定).....	15
3.2.3. Log File Management の設定 (データロギングファイル管理の設定).....	16
3.2.4. データロギングの有効化と保存場所の設定 .....	16
3.2.5. ロギング結果のダウンロード.....	17
4. 初期化.....	17
4.1. 初期化の方法 .....	17
4.2. ユーザ設定の初期状態.....	18
5. 設定ファイルの読み書き .....	18
5.1. 設定ファイルへの保存.....	18
5.2. 設定ファイルからの読み込み .....	18
6. ファームウェアの更新.....	19
6.1. ファームウェアの入手 .....	19
6.2. ファームウェアファイルの取り出し.....	20
6.3. 現在インストールされているファームウェアバージョンの確認 .....	20
6.4. ファームウェアのインストール .....	20

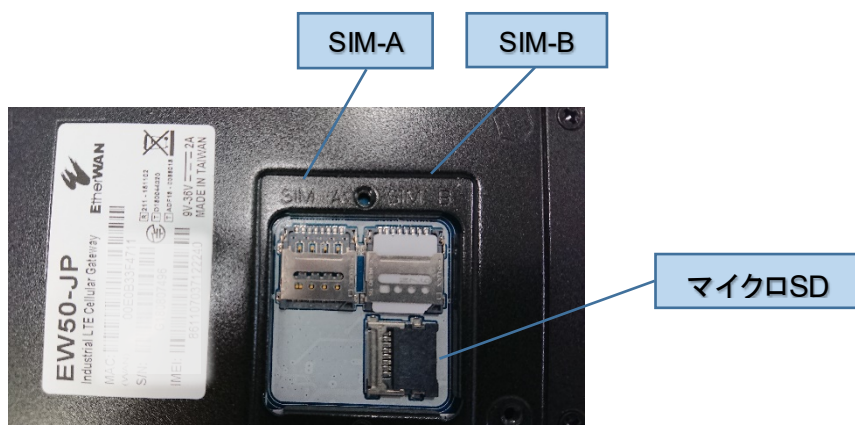
## 1. 基本的な接続

下記の手順で内部デバイスからインターネットへの基本的な接続ができるようになります。

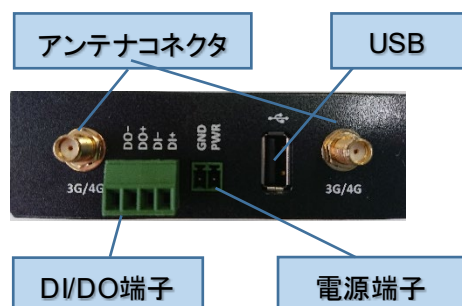
### 1.1. SIM カードのセットとアンテナ、電源接続

本体の下面にあるフタを開け、マイクロSIMカードを挿入し (例:スロットSIM-A)、左側面のアンテナコネクタにアンテナを、電源端子に電源を接続します。

[下面]



[左側面]



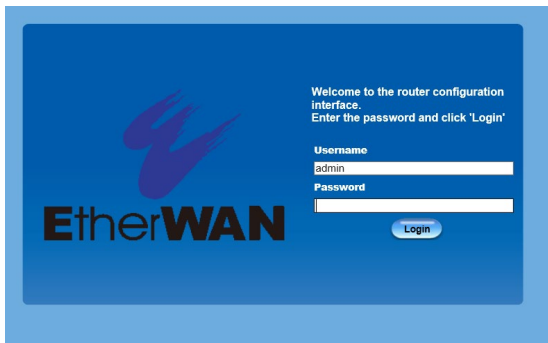
[前面]



## 1.2. 初期状態の EW50 にログイン

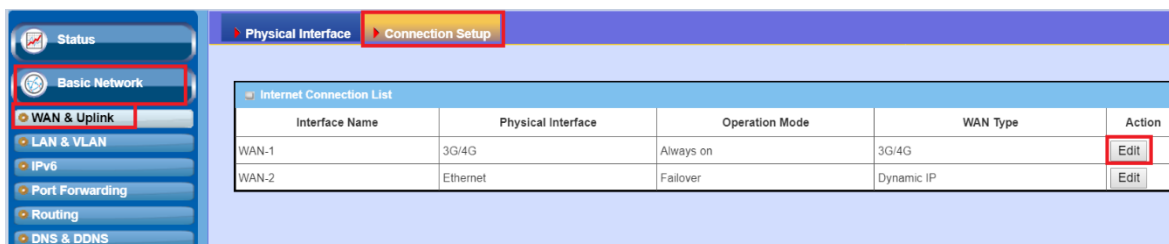
EW50 Web設定画面にログインします。

(デフォルトのIP: 192.168.123.254 /ユーザー名:admin /パスワード:admin)



## 1.3. SIM カード情報の設定

Basic network > WAN & Uplink > Connection Setup > Edit (for WAN-1 3G/4G) を開いて、接続業者が提供するSIMカードの情報に記載されているAPN、Account(ユーザー名)、Passwordなどの設定値を入力してください。



SIMカードを2枚使用する場合は、3G/4G WAN Type ConfigurationのPreferred SIM Cardで優先するのがスロットAのSIMか(SIM-A First)、スロットBのSIMか(SIM-B First)を設定します。優先SIMでの接続がなんらかの事情で切断すると、非優先SIMで接続されます。FailbackのEnableにチェックをすると、優先SIMでの接続が復旧したらそちらでの接続に戻ります。

スロットAの設定は、Configuration with SIM A Card、スロットBの設定は、Configuration with SIM B Cardに設定します。

詳細は、「はじめに」に記載したEtherWANウェブサイトにある英文マニュアル 2.1.2 Internet SetupのConfigure 3G/4G WAN Settingを参照してください。



## 1.5. DHCP クライアントの EW50 経由のインターネットアクセス

EW50のDHCPサーバー(\*1)とNAT機能(IPマスカレード)(\*2)はデフォルトで有効になっています。  
EW50のRJ45ポートに接続するLAN側機器がDHCPクライアントとして設定されていれば、デフォルトゲートウェイやDNSは自動的に割り当てられるので、そのままインターネットに接続できます。

\*1 Basic Network > LAN & VLAN > DHCP Server

\*2 Basic Network > WAN & Uplink > Connection Setup > 3G/4G Connection Common Configuration > NAT

## 1.6. 静的 IP アドレスをつけた LAN 側機器の EW50 経由のインターネットアクセス

Basic Network > LAN & VLAN > Ethernet LANのConfigurationで、LAN側機器のIPアドレスに合わせてEW50のLAN側IPアドレスを変更できます。

LAN側機器のIPアドレスがEW50と同じサブネットの場合は、ゲートウェイ及びDNSサーバーとしてEW50のLAN側IPアドレスを指定することで、LAN側機器からインターネット上のサイトにアクセスできるようになります。

Item	Setting
IP Mode	Static IP
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0 (/24)

ID	Name	Interface	IP Address	Subnet Mask	Enable	Action
----	------	-----------	------------	-------------	--------	--------

## 2. VPN

遠隔から安全に接続するためのいくつかのVPNの設定方法を説明します。

### 2.1. IPSec VPN

IPSec VPNを使用して、1つのネットワーク(サーバー側ネットワーク)に複数のネットワーク(クライアントネットワーク)から接続する方法を説明します。

#### 2.1.1. IPSec VPN 設定の作成

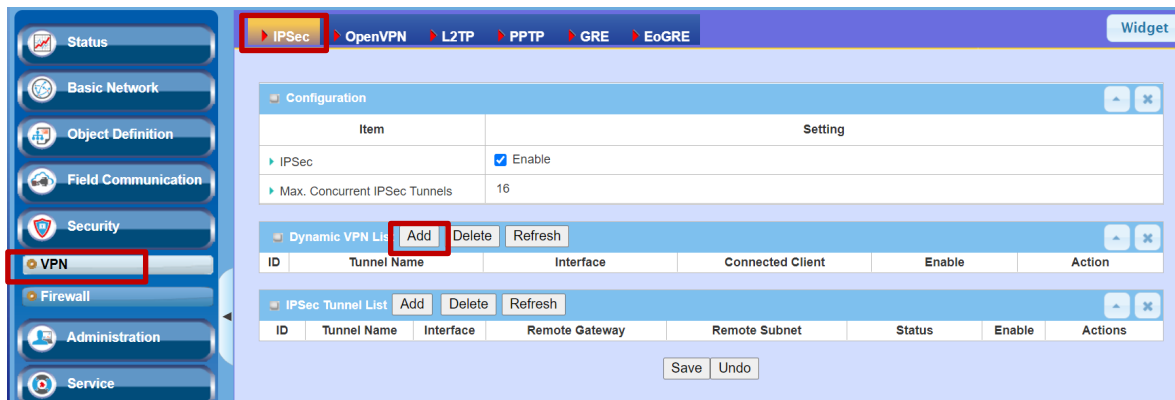
EW50をサーバー側ネットワーク、クライアントネットワークそれぞれからインターネットに接続するために配置し、さらにEW50相互にVPN接続するための設定をします。

##### A) サーバー側VPN設定の作成

サーバー側ネットワークの EW50 の設定をします。

##### ① Dynamic IPSec VPN設定の追加

Security > VPN > IPSec で、Dynamic VPN List テーブルの[Add]ボタンをクリックします。



## ② Tunnel Configuration の設定

[Tunnel]を Enable にします。

Tunnel Configuration	
Item	Setting
Tunnel	<input checked="" type="checkbox"/> Enable
Tunnel Name	Dynamic IPSec1
Interface	WAN-1 ▼
Tunnel Scenario	Tunnel Mode ▼
Encapsulation Protocol	ESP ▼
IKE Version	v1 ▼

## ③ Local & Remote Configuration の設定

サーバー側のローカルネットワークのネットワークアドレス[Local Subnet]とネットマスク[Local Netmask]を指定します。

Local & Remote Configuration	
Item	Setting
Local Subnet	10.11.123.0
Local Netmask	255.255.255.0

## ④ Authentication の設定

ここでは、VPN接続のための[Key Management]として、Pre-Shared-Key(事前認証鍵)を設定します。クライアント側と合わせる必要があります。より強固な認証方式として、X.509証明書を使用した認証方式も[Key Management]として選択できます。

Authentication	
Item	Setting
Key Management	IKE+Pre-shared Key ▼ EtherWAN (Min. 2 charact
Local ID	Type: User Name ▼ ID: (Optional)

## ⑤ IKE Phrase の設定

デフォルトのままとします。

IKE Phase	
Item	Setting
▶ Negotiation Mode	Main Mode ▼
▶ X-Auth	None ▼ X-Auth Account (Optional)
▶ Dead Peer Detection (DPD)	<input checked="" type="checkbox"/> Enable Timeout : 180 (seconds) Delay : 30 (seconds)
▶ Phase1 Key Life Time	14400 (seconds) (Max. 86400)

## ⑥ IKE Phrase Definition の設定

デフォルトのままとします。

IKE Proposal Definition				
ID	Encryption	Authentication	DH Group	Definition
1	AES-128 ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
2	AES-128 ▼	MD5 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
3	DES ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
4	AES-128 ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable

## ⑦ IPSec Phase の設定

デフォルトのままとします。

IPSec Phase	
Item	Setting
▶ Phase2 Key Life Time	28800 (seconds) (Max. 86400)

## ⑧ IPSec Proposal Definition の設定

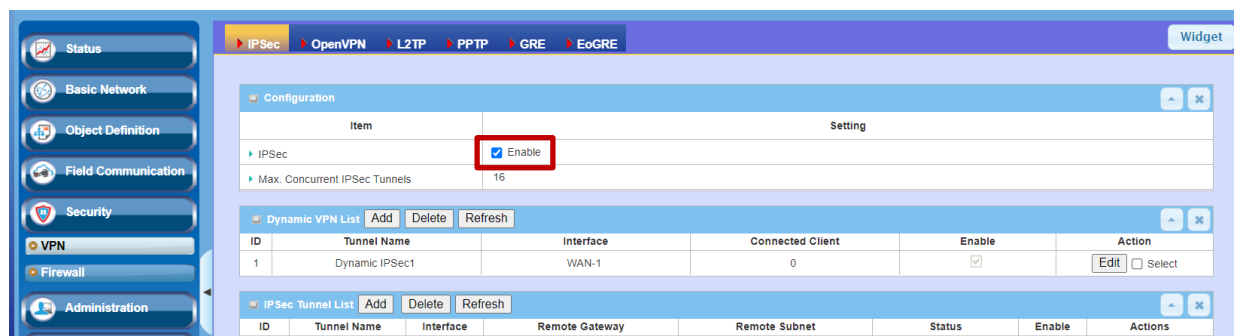
デフォルトのままとします

IPSec Proposal Definition				
ID	Encryption	Authentication	PFS Group	Definition
1	AES-128 ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
2	AES-128 ▼	MD5 ▼		<input checked="" type="checkbox"/> Enable
3	DES ▼	SHA1 ▼		<input checked="" type="checkbox"/> Enable
4	3DES ▼	SHA1 ▼		<input checked="" type="checkbox"/> Enable



## ⑨ IPsec VPN 起動の確認

[IPsec]をEnableにしてIPsecサーバー機能を有効にします。



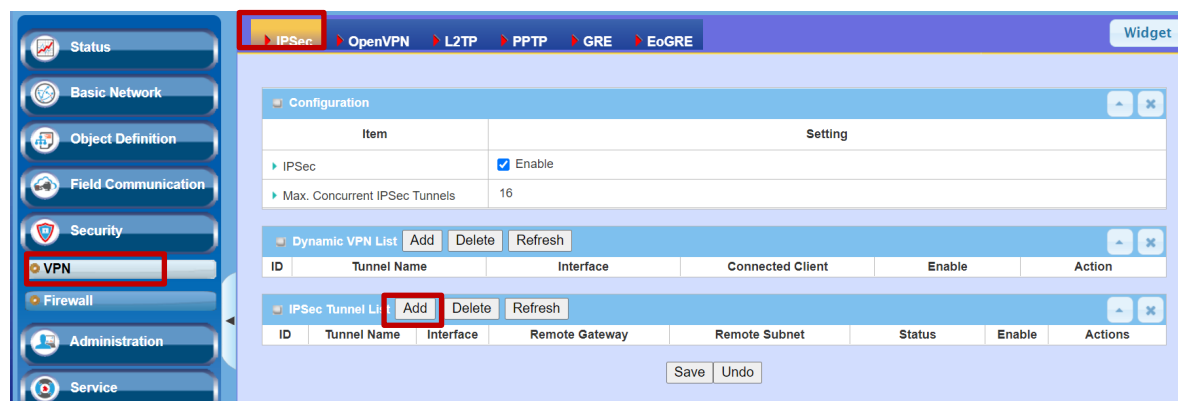
備考) FWバージョン0EW0Y80.IA2\_uA7.0EW0\_03201500まではNAT Traversalの設定はそれ以降のFWでは、自動的に適用されるようになったので廃止された。

## B) クライアント側IPsec VPN設定の作成

クライアント側ネットワークの EW50 の設定をします。

### ① IPsec VPN 設定の追加

Security > VPN > IPsecで、IPsec Tunnel Listテーブルの[Add]ボタンをクリックします。



## ② Tunnel Configuration の設定

[Tunnel]をEnableにします。

Tunnel Configuration	
Item	Setting
Tunnel	<input checked="" type="checkbox"/> Enable
Tunnel Name	IPSec #1
Interface	WAN-1
Tunnel Scenario	Site-to-Site(Tunnel mode)
Tunnel TCP MSS	Auto 0 (64~1500 Bytes)
ICMP Keep alive	<input type="checkbox"/> Enable Max. fail times 3 Interval 30 (secs.) Source Addr. Destination Addr.
Encapsulation Protocol	ESP
IKE Version	v1

## ③ Local & Remote Configuration の設定

クライアント側のローカルネットワークのネットワークアドレスを[Local Subnet List]の[Subnet IP Address]とネットマスク[Local Netmask]に指定します。

サーバー側のローカルネットワークのネットワークアドレスを[Remote Subnet List]の[Subnet IP Address]とネットマスク[Local Netmask]に指定します。(サーバー側ネットワークのEW50の[Local Subnet]、[Local Netmask]に設定したのと同じ値)

サーバー側EW50のグローバルIPアドレスを[Remote Gateway]に指定します。

Local & Remote Configuration				
Item	Setting			
Local Subnet List	ID	Subnet IP Address	Subnet Mask	Actions
	1	192.168.123.0	255.255.255.0(/24)	Delete
	Add			
Remote Subnet List	ID	Subnet IP Address	Subnet Mask	Actions
	1	192.168.1.0	255.255.255.0(/24)	Delete
	Add			
Remote Gateway	116.115.114.113 (IP Address/FQDN)			

## ④ Authentication の設定

IPSec VPN サーバー側の Key Management と同じ設定にします。

Authentication	
Item	Setting
Key Management	IKE+Pre-shared Key EtherWAN (Min. 8 characters)
Local ID	Type: User Name ID: (Optional)
Remote ID	Type: User Name ID:

## ⑤ IKE Phrase の設定

デフォルトのままとします。

IKE Phase	
Item	Setting
▶ Negotiation Mode	Main Mode ▼
▶ X-Auth	None ▼ X-Auth Account (Optional) User Name : <input type="text"/> Password : <input type="password"/>
▶ Dead Peer Detection (DPD)	<input checked="" type="checkbox"/> Enable Timeout : <input type="text" value="180"/> (seconds) Delay : <input type="text" value="30"/> (seconds)
▶ Phase1 Key Life Time	<input type="text" value="14400"/> (seconds) (Max. 86400)

## ⑥ IKE Phrase Definition の設定

デフォルトのままとします。

IKE Proposal Definition				
ID	Encryption	Authentication	DH Group	Definition
1	AES-128 ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
2	AES-128 ▼	MD5 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
3	DES ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
4	3DES ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable

## ⑦ IPSec Phase の設定

デフォルトのままとします。

IPSec Phase	
Item	Setting
▶ Phase2 Key Life Time	<input type="text" value="28800"/> (seconds) (Max. 86400)

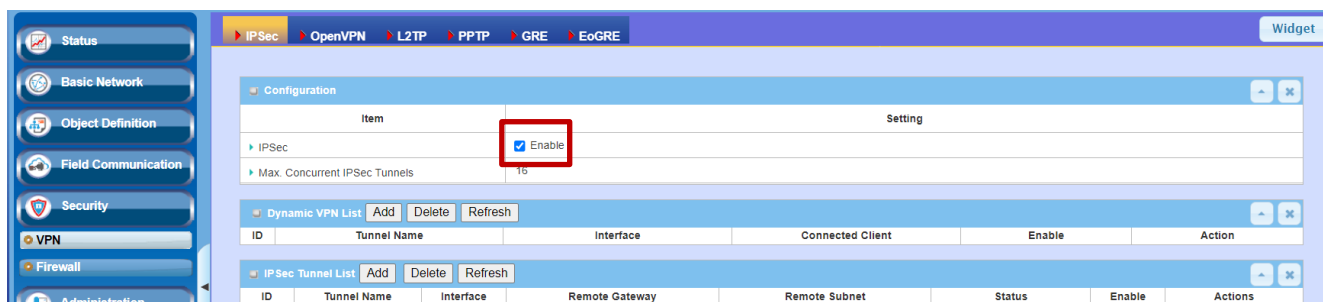
## ⑧ IPSec Proposal Definition の設定

デフォルトのままとします。

IPSec Proposal Definition				
ID	Encryption	Authentication	PFS Group	Definition
1	AES-128 ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
2	AES-128 ▼	MD5 ▼		<input checked="" type="checkbox"/> Enable
3	DES ▼	SHA1 ▼		<input checked="" type="checkbox"/> Enable
4	3DES ▼	SHA1 ▼		<input checked="" type="checkbox"/> Enable

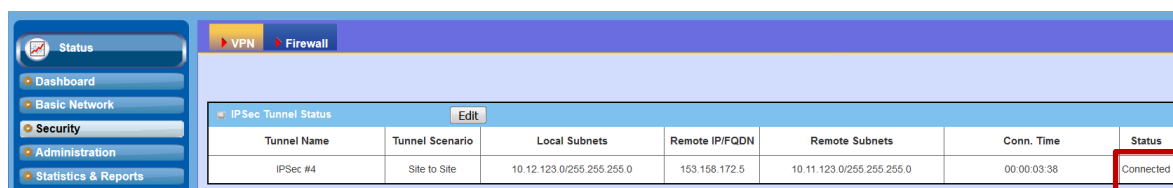
## ⑨ IPsec VPN 起動の確認

[IPsec]をEnableにしてIPsecクライアント機能を有効にします。



## ⑩ 接続の確認

[Status] > [Security] > [VPN] > [IPsec Tunnel Status]の[Status]でVPNの動作状態を確認できます。接続できていればConnectedと表示されます。



## 3. データロギング

EW50のシリアル通信端子に接続されているMODBUSスレーブ機器の状態をロギングする方法を説明します。

MODBUSスレーブ機器がシリアル通信機器の場合、3.1 MODBUSゲートウェイの設定に従って、シリアルポート及び、MODBUSに関する設定をしてください。

### 3.1. MODBUS ゲートウェイの設定

#### 3.1.1. シリアル接続

EW50前面に取り付けられているシリアル通信端子に、下記のピン番号と信号の対照表を参照して、RS232またはRS485で接続可能なMODBUSスレーブ機器を接続します。



ピン番号 1 2 3 4 5 6

ピン番号	1	2	3	4	5	6
ポート	SPort-0			SPort-1		
RS-232	RxD (RD)	TxD (SD)	GND(SG)	GND(SG)	RxD(RD)	TxD(SD)
RS-485	DATA-	DATA+	GND	GND	DATA-	DATA+

#### 3.1.2. シリアルポートの設定

Field Communication > Bus & Protocol > Port Configurationで、Serial Port Configurationテーブルを表示させ、

SPort0またSPort1のいずれか使用するポートで[Edit]をクリックします。

[Operation Mode] : 「Modbus」を設定します。

[Interface] : 実際に接続されているシリアルインタフェースに従って、「RS-232」または「RS-485」を設定します。

[Baud Rate] : MODBUS機器に合わせて設定します。

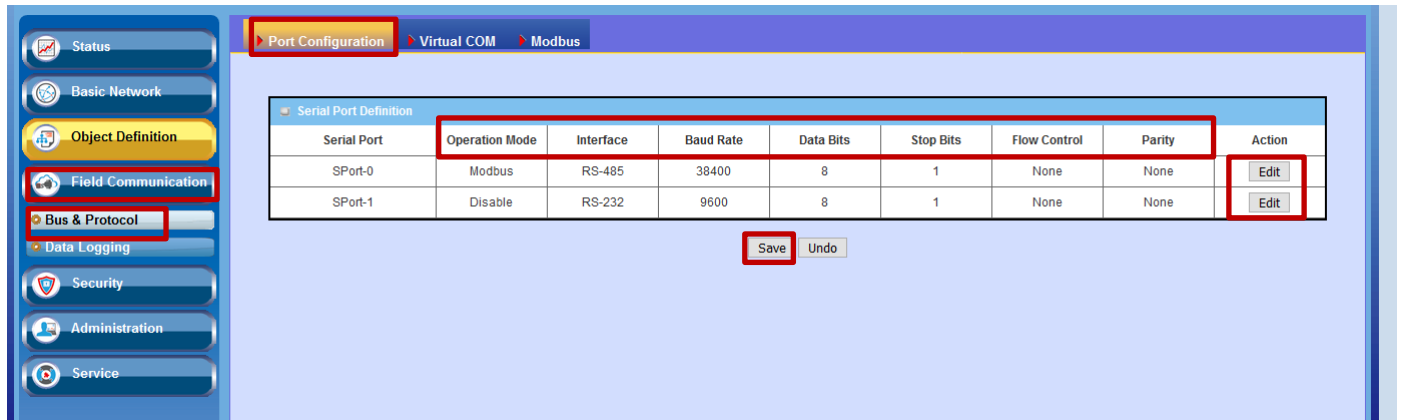
[Data Bits] : MODBUS機器に合わせて設定します。

[Stop Bits] : MODBUS機器に合わせて設定します。

[Flow Control] : MODBUS機器に合わせて設定します。

[Parity] : MODBUS機器に合わせて設定します。

[Save]で編集結果を保存します。

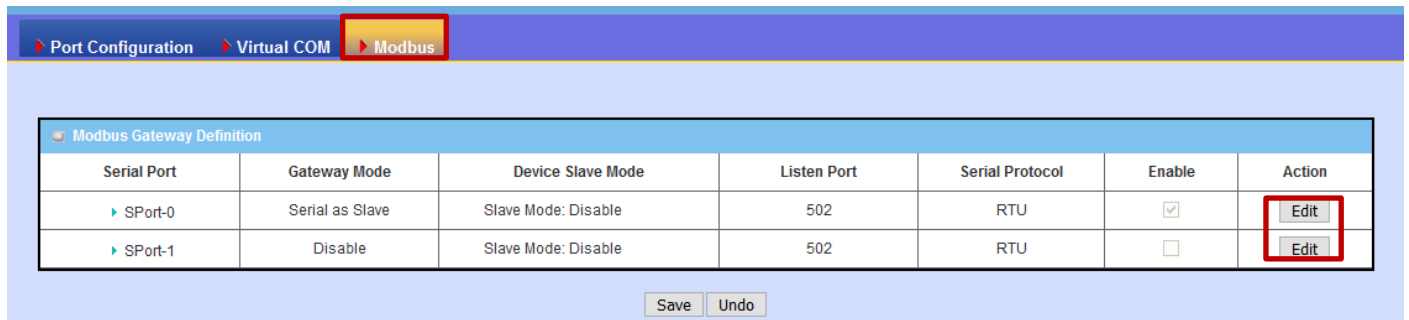


### 3.1.3. MODBUS の設定

MODBUS機器が接続されているEW50のシリアルポートのMODBUSに関する設定をします。

[Modbus]タブをクリックします。

MODBUS機器が接続されているポートのSPort-0またはSport-1で[Edit]をクリックします。



[Gateway Mode] : Serial as Slaveに設定します。

[Device Slave Mode] : Enableにします。

[Listen Port] : 特に指定がない場合、502のままとします。(外部MODBUS/TCPクライアントに応答するポート)

[Serial Protocol] : RTUかASCIIか、MODBUS機器に合わせてます。

[Enable] : Enableにします。

Response Timeout : デフォルトのままとします(あるいは、MODBUS機器の応答が間に合うように設定します)。

Timeout Retries : デフォルトのままとします。(MODBUS機器無応答時のコマンド再送回数)

0Bh Exception : デフォルトのままとします。(MODBUS機器無応答時のEW50からの応答)

Tx Delay：デフォルトのままとします。MODBUS機器が早い応答周期に耐えられない場合、チェックしてください。  
 TCP Connection Idle Time：デフォルトのままとします。(MODBUS/TCPクライアントとの接続を切断するまでの無通信時間)

Maximum TCP Connections：デフォルトのままとします。(接続可能な最大TCP接続数)

TCP Keep-alive：デフォルトのままとします。

Modbus Master IP Access：デフォルトのままとします。(あるいは、MODBUS機器にアクセス可能なMODBUS/TCPクライアントのIPアドレスを指定します。)

Message Buffering：デフォルトのままとします。

[Save]をクリックして編集結果を保存します。

The screenshot shows the 'Modbus Gateway Definition' and 'Gateway Mode Configuration for SPort-0' windows. The 'Modbus Gateway Definition' table has columns: Serial Port, Gateway Mode, Device Slave Mode, Listen Port, Serial Protocol, Enable, and Action. The 'Gateway Mode Configuration for SPort-0' table has columns: Item and Setting.

Serial Port	Gateway Mode	Device Slave Mode	Listen Port	Serial Protocol	Enable	Action
SPort-0	Serial as Slave	Slave Mode: <input type="checkbox"/> Enable	502 (1~65535)	RTU	<input checked="" type="checkbox"/>	Edit
SPort-1	Disable	Slave Mode: Disable	502	RTU	<input type="checkbox"/>	Edit

Item	Setting
Response Timeout	1000 ms (1~65535)
Timeout Retries	0 times (0~5)
0Bh Exception	<input type="checkbox"/> Enable
Tx Delay	<input type="checkbox"/> Enable
TCP Connection Idle Time	300 sec (1~65535)
Maximum TCP Connections	1 connections (1~4)
TCP Keep-alive	<input type="checkbox"/> Enable
Modbus Master IP Access	Allow All
Message Buffering	<input type="checkbox"/> Enable

At the bottom, there are 'Save' and 'Undo' buttons.

## 3.2. データロギングの設定

Field Communication > Data Logging > Configurationを選択します。

Modbus Proxy Rule Listテーブルで、[Add]をクリックして新しいModbus Proxy Rule List Configuration設定を作成します。

The screenshot shows the 'Configuration' window with 'Data Logging' settings and the 'Modbus Proxy Rule List' table. The 'Data Logging' settings are: Data Logging (checked), Storage Device (External). The 'Modbus Proxy Rule List' table has columns: ID, Name, Modbus Slave Type, Slave ID, Function Code, Start Address, Number of Coils/Registers, Polling Rate (ms), and Actions.

Item	Setting
Data Logging	<input checked="" type="checkbox"/> Enable
Storage Device	External

ID	Name	Modbus Slave Type	Slave ID	Function Code	Start Address	Number of Coils/Registers	Polling Rate (ms)	Actions
Add Delete								

### 3.2.1. Modbus Proxy Rule List Configuration の設定(データ収集方法の設定)

Modbus Proxy Rule List Configurationに、MODBUSを使っでのデータ収集方法を設定します。

Modbus Proxy Rule Listテーブルで、[Add]をクリックし新たな設定を新規作成します。

[Name] : 適当な名称を設定してください。

[Type] : デフォルトままとしてください。

[Modbus Slave Type] : MODBUSスレーブ機器が、Ethernet経由でMODBUS/TCP接続の場合、MODBUSスレーブ機器のIPアドレスとポート番号(デフォルト: 502)を指定します。シリアル通信接続の場合、Local Serial Portと選択し、2ポートあるシリアル接続のいずれかを指定します(SPort1またはSPort2)。

[Slave ID] : このデータ収集方法でアクセスするMODBUSスレーブ機器のスレーブアドレスの範囲を指定します。  
[Function Code] : MODBUSファンクションコードを指定します。使用できるファンクションコードはMODBUSスレーブ機器の取扱説明書を参照してください。

[Start Address] : MODBUSスレーブ機器内のデータ収集対象となる先頭データアドレスを指定します。

[Number of Coils/Registers] : 先頭データアドレスから数えていくつのデータを収集するかを指定します。

[Polling Rate] : データ収集周期をms単位で指定します。

[Save]をクリックして、設定を保存します。

ID	Name	Type	Modbus Slave Type	Slave ID	Function Code	Start Address	Number of Coils/Registers	Polling Rate (ms)	Actions
1	Radiolog	Proxy	SPort-0	1 - 1	Read Input Registers (0x04)	5000	1	1000	Edit <input type="checkbox"/> Select

Item	Setting
Name	Radiolog
Type	Proxy
Modbus Slave Type	Local Serial Port SPort-0
Slave ID	1 (1~247) - 1 (1~247)
Function Code	Read Input Registers (0x04)
Start Address	5000 (0~65535)
Number of Coils/Registers	1 (1~125)
Polling Rate (ms)	1000 (500~99999)

### 3.2.2. Scheme の設定 (データロギング方法の設定)

Schemeで、データロギングの方法を設定します。

[Scheme Setup]タブを選択します。

Schema Listテーブルで、[Add]をクリックし新たな設定を新規作成します。

[Name] : 適当な名称を設定します。

[Mode] : データロギングの方法を次の選択肢から選択します。

Sniffer : 他のMODBUSマスタ、スレーブ間のMODBUSランザクションをすべてロギングします。

Off-Line Proxy : MODBUSマスタからのEW50への接続が途切れたのを確認してEW50が代わりにMODBUSコマンドを発行し、データ収集、ロギングします。

Full-Time Proxy : EW50から常時MODBUSコマンドを発行しデータ収集、ロギングします。

Sniffer & Off-Line Proxy : SnifferとOff-Line Proxyを共に実行します。

Sniffer & Full-Time Proxy : SnifferとFull-Time Proxyを共に実行します。

[Save]をクリックして設定を確定します。

Scheme List							
<div>Add Delete</div>							
ID	Name	Mode	Master Type	Master Query Timeout (sec)	Proxy Rules	Enable	Actions
1	ExecRadioLogVLRa	Sniffer & Full-Time Proxy	192.168.123.30	N/A	<div>Detail</div>	<input checked="" type="checkbox"/>	<div>Edit Select</div>

Scheme Configuration

Save Undo

Item	Setting
Name	ExecRadioLogVLRa
Mode	Sniffer & Full-Time Proxy
Master Type	IP Address 192.168.123.30
Proxy Rules	<input checked="" type="checkbox"/> Radiolog
Enable	<input checked="" type="checkbox"/>

### 3.2.3. Log File Management の設定 (データロギングファイル管理の設定)

収集したデータロギングをどのように管理するかを設定します。

[Log File Management]タブをクリックします。

管理方法を設定したいデータロギングのSchemeを名前で選択し、[Edit]ボタンをクリックします。

[File Content Format] : Raw Data(生のフォーマット)またはMODBUS Type(値のバイト列がそれ以外のフィールドと切り離されている) から選択します。

[Split File by] : ファイルをどのサイズで分割するかを指定します。

[Auto Upload] : そのままとします。Enableを設定すると外部FTPサーバーに自動転送します。

[Delete File After Upload] : Auto Uploadを有効にした場合、これをEnableにすると転送後にログファイルを削除できます。

[When Storage Full] 保存メディアが一杯になった場合の処理を記載します。Remove the Oldestは、最も古いファイルを削除します。Stop Recordingは、ロギングを中止します。

[Save]で設定を保存します。

Log File List								
ID	Name	File Content Format	Split File by	Auto Upload	Log File Compression	Delete File After Upload	When Storage Full	Actions
1	ExecRadioLogVLRa	Raw Data	200 KB	Disabled	N/A	N/A	Remove the Oldest	<div>Edit Download Log</div>

Log File List Configuration

Save Undo

Item	Setting
File Content Format	Raw Data
Split File by	Size 200 KB
Auto Upload	<input type="checkbox"/> Enable
When Storage Full	Remove the Oldest

### 3.2.4. データロギングの有効化と保存場所の設定

設定を有効にして、ロギングを開始します。



[Configuration]タブの画面を表示し、

[Data Logging] : Enableにします。

[Storage Device] : ロギングデータの保存場所をUSBポートに接続したUSBメモリにする場合は、Exernalに、内部SDカードスロットに挿したマイクロSDカードの場合はInternalに設定します。

[Save]をクリックして、ロギングを開始します。

※上記を設定する前に保存するためのメディアは接続しておく必要があります。

Configuration    Scheme Setup    Log File Management

Item	Setting
Data Logging	<input checked="" type="checkbox"/> Enable
Storage Device	External ▼

Modbus Proxy Rule List    Add    Delete

ID	Name	Modbus Slave Type	Slave ID	Function Code	Start Address	Number of Coils/Registers	Polling Rate (ms)	Actions
1	Radiolog	SPort-0	1 - 1	Read Input Registers (0x04)	5000	1	1000	Edit <input type="checkbox"/> Select

Save    Undo

### 3.2.5. ロギング結果のダウンロード

収集したロギングデータをまとめてダウンロードします。

[Log File Management]タブをクリックして、Log File Listテーブルを表示します。

[Download Log]をクリックしてデータロギングファイルのアーカイブをtgzフォーマットでダウンロードします。

Configuration    Scheme Setup    Log File Management

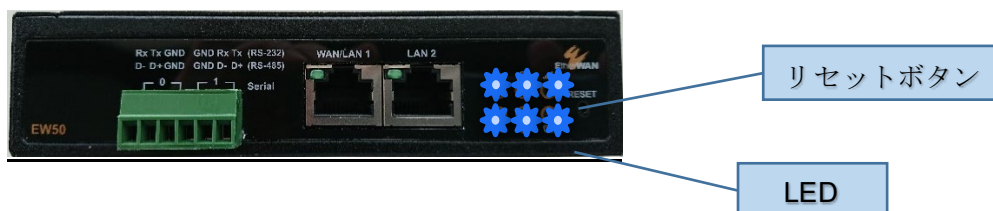
Log File List

ID	Name	File Content Format	Split File by	Auto Upload	Log File Compression	Delete File After Upload	When Storage Full	Actions
1	ExecRadiologVLRaw	Raw Data	200 KB	Disabled	N/A	N/A	Remove the Oldest	Edit    Download Log

## 4. 初期化

EW50に設定したIPアドレスやパスワードを忘れてアクセスできなくなってしまった場合、EW50を初期化して復旧することができます。

### 4.1. 初期化の方法



リセットボタン6秒押し続け離すと、少し間が空いてから上記のように一旦LEDが全点灯して初期化、再起動される。

## 4.2. ユーザ設定の初期状態

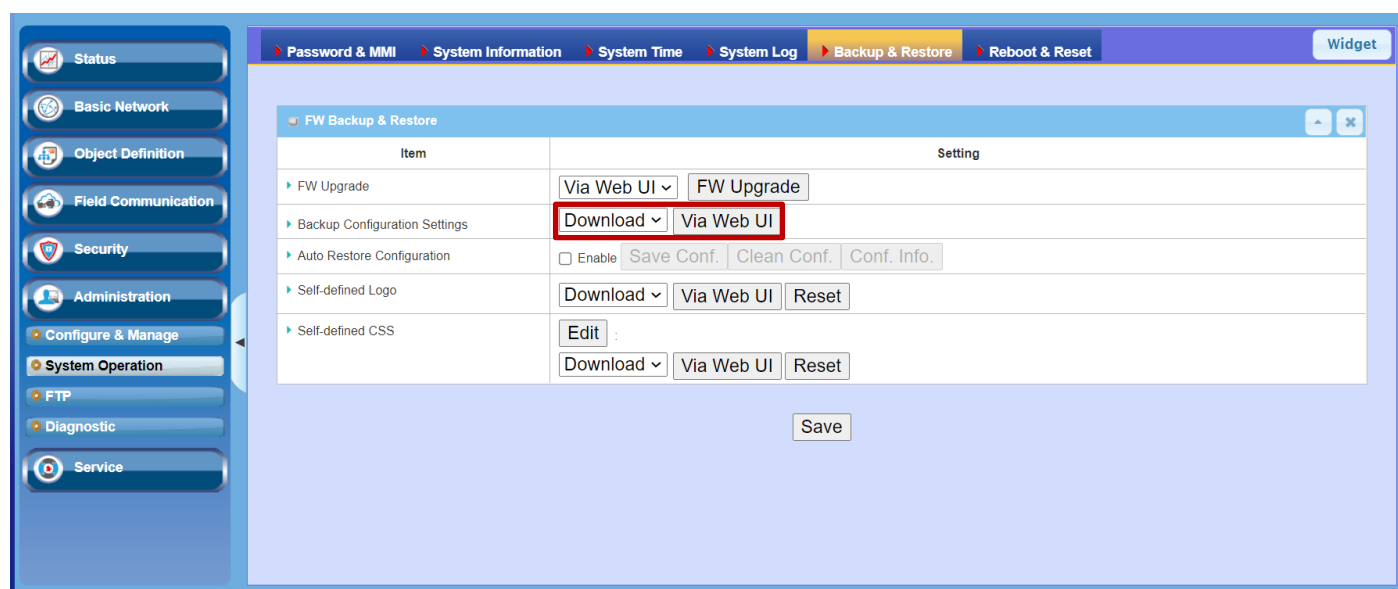
IPアドレス：192.168.123.254、ユーザー名：admin、パスワード：adminで再度アクセスできるようになります。

## 5. 設定ファイルの読み書き

### 5.1. 設定ファイルへの保存

EW50の設定をWindows上のファイルに保存することができます。

Administration > System Operation > Backup & Restoreで、FW Backup & Restoreテーブルを表示させ、[Backup Configuration Settings] で、[Download]を選択し、[Via Web Ui]ボタンをクリックしてください。

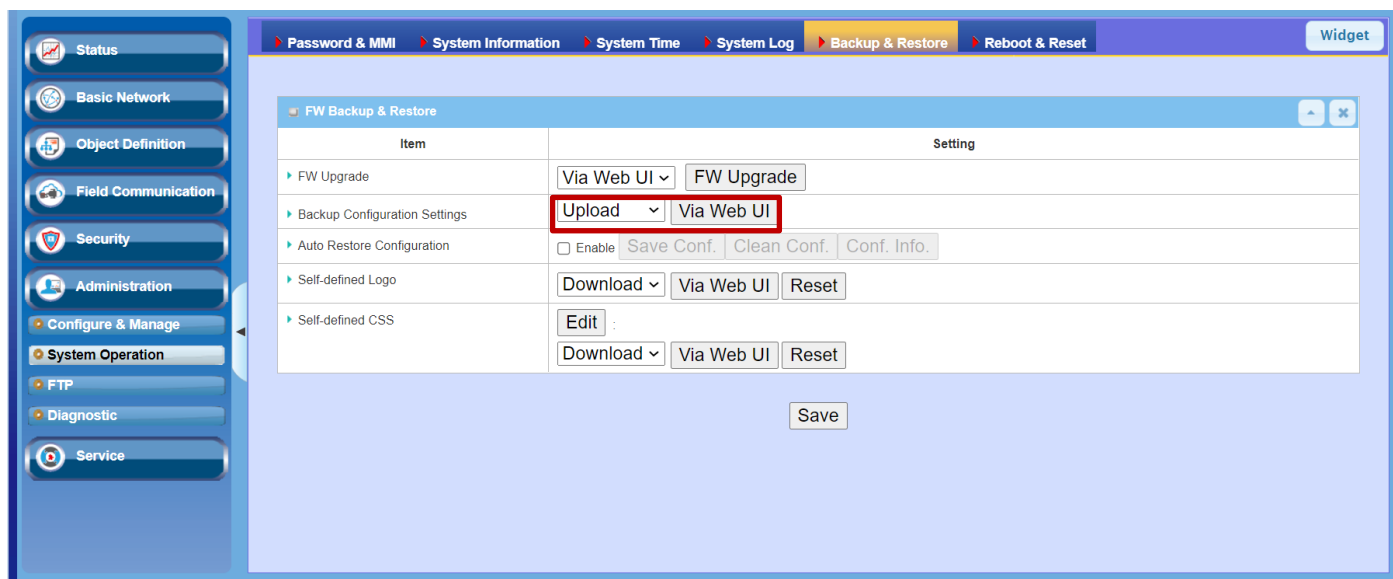


Windowsの[ダウンロード]フォルダにconfig.binないしconfig(数字).binというネーミングのファイルが保存されます。(数字)がついた名前は既に保存された設定がある場合です。

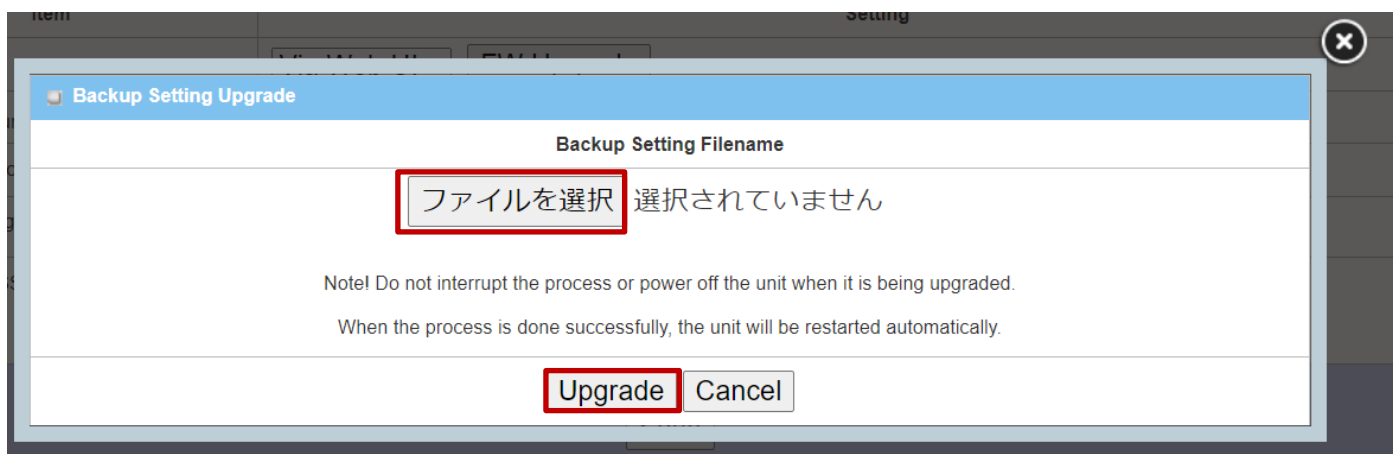
### 5.2. 設定ファイルからの読み込み

保存した設定ファイルを読み込むことによってEW50の設定を一括ですることができます。

Administration > System Operation > Backup & Restoreで、FW Backup & Restoreテーブルを表示させ、[Backup Configuration Settings] で、[Upload]を選択し、[Via Web Ui]ボタンをクリックしてください。



下記のダイアログが表示されるので、[ファイルを選択]で設定ファイルを選択し、[Upgrade]ボタンをクリックしてください。数分以内に設定の読み込みと再起動を行います。



## 6. ファームウェアの更新

EW50に設定したIPアドレスやパスワードを忘れてアクセスできなくなってしまった場合、EW50を初期化して復旧することができます。

### 6.1. ファームウェアの入手

下記URLからEtherWAN社のEW50の製品ページにアクセスし、  
<https://www.etherwan.com/jp/products/ew50-series>

[Downloads]セクションの[Firmware]をクリックします。

#### Downloads

Datasheet

Manuals

**Firmware**

Visio Stencil

Utility

最新のファームウェアが表示されますが、ファームウェアはモデル別になっています。ご使用のモデルに合わせてダウンロードお願いします。

ew50\_firmware.zip : EW50-EUS、EW50-TA用  
ew50\_firmware\_jp.zip : EW50-JP用

ew50_release_note
Edition: updated: 20210121
Download: ew50_release_note.pdf

ew50_firmware.zip
Edition: updated: 20210121
Detail and Release Note: EUS, TA Models
Download: ew50_firmware.zip

ew50_firmware_jp
Edition: updated: 20210121
Detail and Release Note: JP Model
Download: ew50_firmware_jp.zip

## 6.2. ファームウェアファイルの取り出し

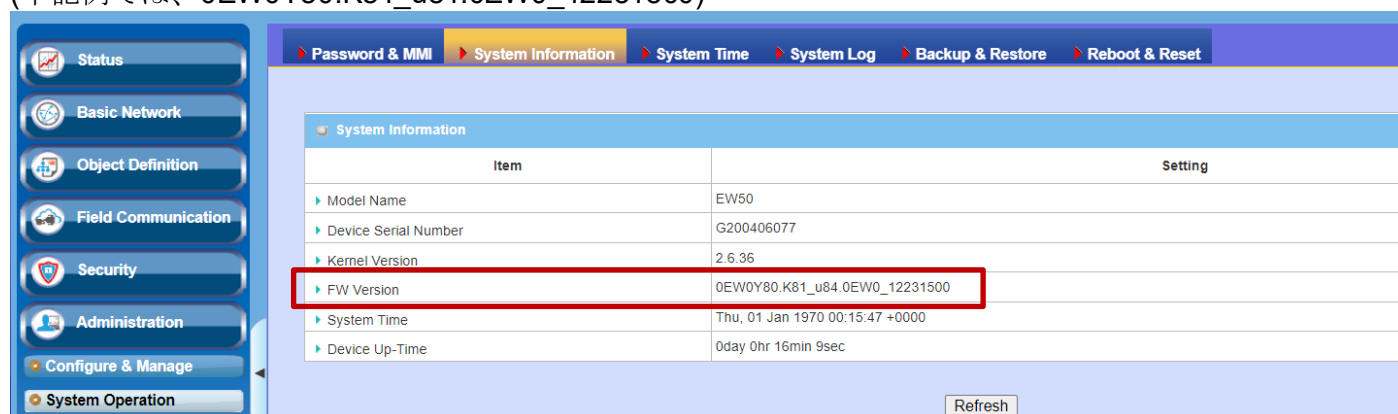
ダウンロードしたファイルを解凍し、拡張子が.binのファームウェアファイルを取り出します。

## 6.3. 現在インストールされているファームウェアバージョンの確認

Administration > System Operation > System Information

で、[System Information]画面を表示させ、Item名 FW VersionのSettingを確認します。

(下記例では、0EW0Y80.K81\_u84.0EW0\_12231500)

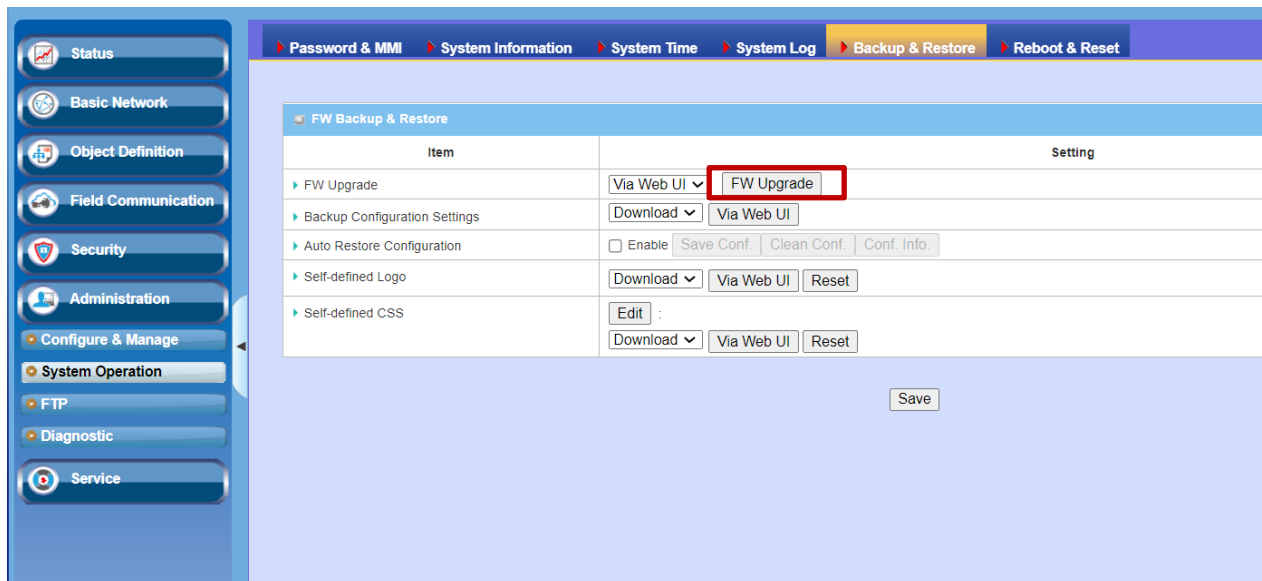


System Information	
Item	Setting
▶ Model Name	EW50
▶ Device Serial Number	G200406077
▶ Kernel Version	2.6.36
▶ FW Version	0EW0Y80.K81_u84.0EW0_12231500
▶ System Time	Thu, 01 Jan 1970 00:15:47 +0000
▶ Device Up-Time	0day 0hr 16min 9sec

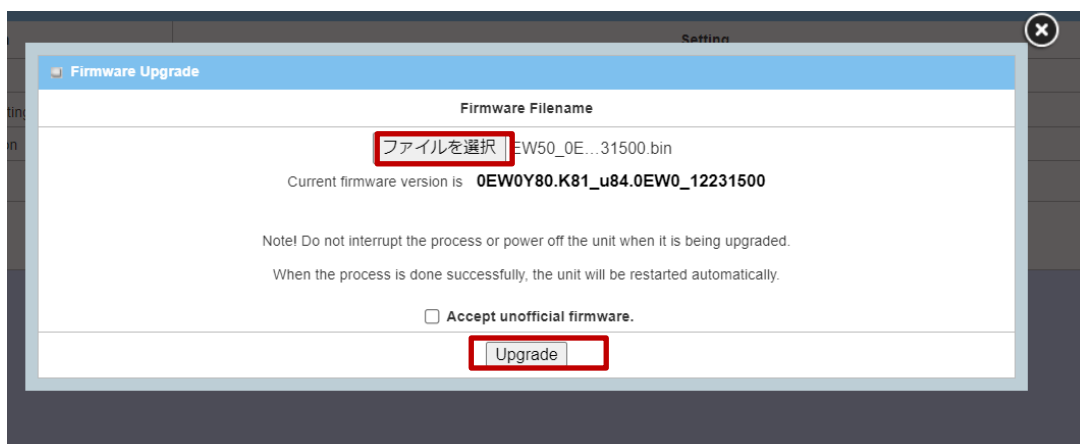
Refresh

## 6.4. ファームウェアのインストール

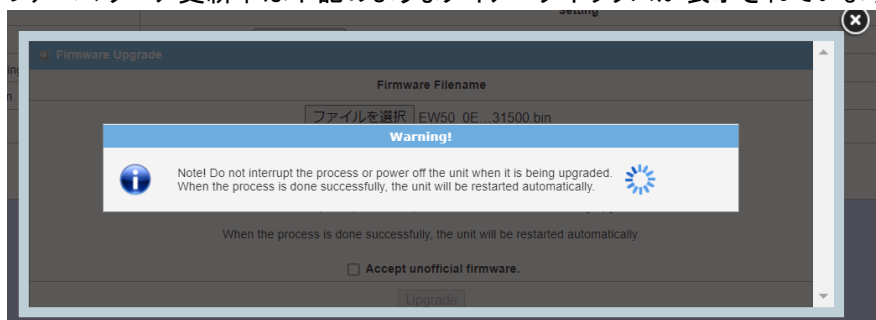
Administration > System Operation > Backup & Restoreで、[FW Backup & Restore]画面を表示させ、Item名 FW UpgradeのSettingにある[FW Upgrade]ボタンをクリックします。



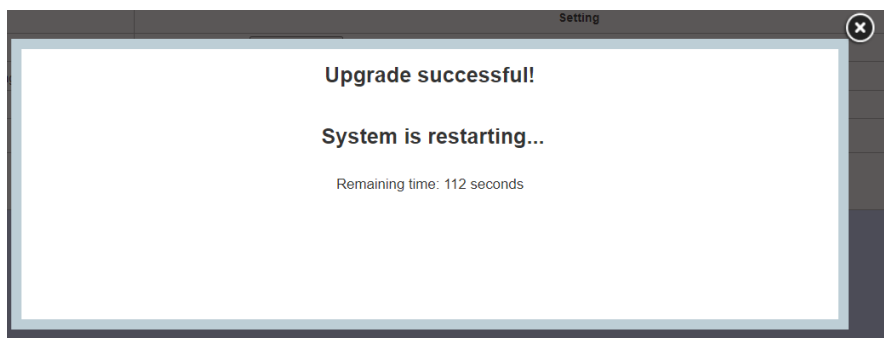
下記のようなダイアログボックスが表示されるので、[ファイルを選択]ボタンをクリックしてダウンロードした拡張子が.binのファームウェアファイルを選択し、[Upgrade]ボタンをクリックしてファームウェアの更新を開始します。



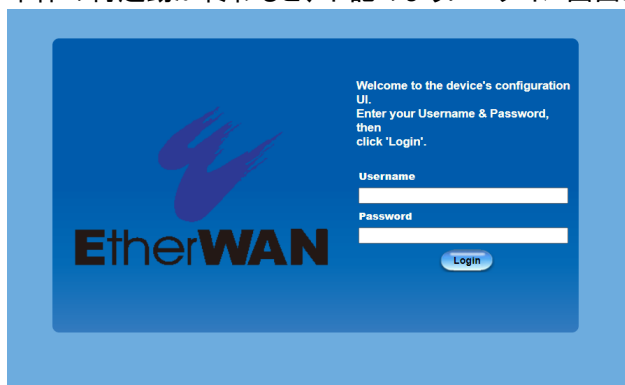
ファームウェア更新中は下記のようなダイアログボックスが表示されています。(1～2分程度かかります)



ファームウェア更新が終わると、下記のようなダイアログボックスが表示され、本体が再起動されます。



本体の再起動が終わると、下記のようにログイン画面が表示されます。



本資料に関するお問合せ先：

フエニックス・コンタクト株式会社

E-mail: [info@phoenixcontact.co.jp](mailto:info@phoenixcontact.co.jp)

Website: [www.phoenixcontact.co.jp](http://www.phoenixcontact.co.jp)