McAfee WebGateway Version7
設定バックアップ・リストア手順書

平成 30 年 11 月 21 日
株式会社ディアイティ
ネットワークセキュリティ事業部

目次

1 はじめに

1.1 本書の目的

本書では、McAfee Web Gateway(MWG) Version7 の設定バックアップ及びリストア手順を記載します。
なお、設定のリストアは基本的に WebUI より実施します。WebUI 接続に必要な IP アドレスやルーティング等基本的な設定項目については、紙の資料など設定バックアップファイル以外の方法による記録を実施下さい。

本書作成時の MWG 最新バージョンは 7.8.2.4.0 となります。

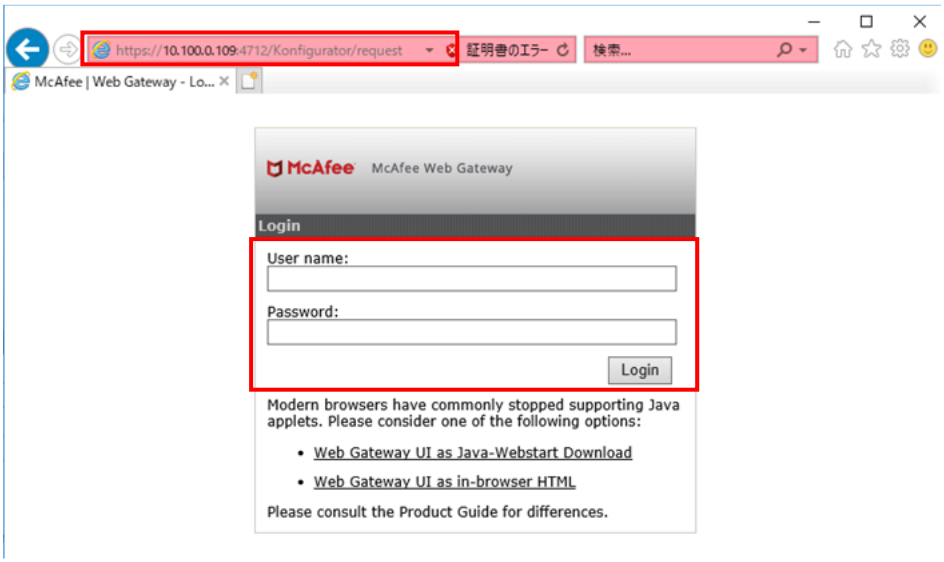
2 設定バックアップ

2.1 WebUI へのログイン

MWG Version7 にブラウザよりログインします。以下 URL を参照します。(ポート 4712 はデフォルト値)

https://MWG の IPaddress:4712/

ログイン画面が表示されます。Username、Password を入力してログインして下さい。

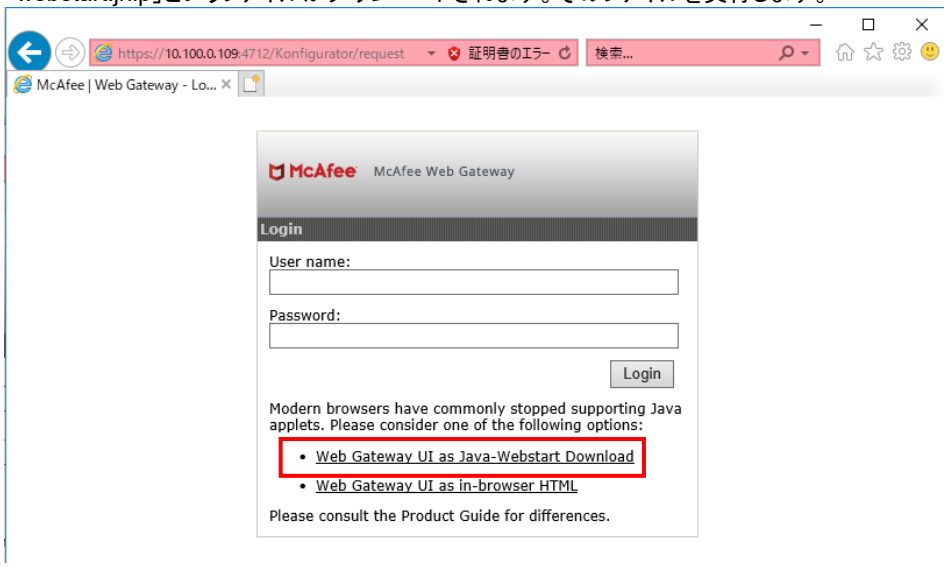


2.1.1 ブラウザがユーザーインターフェースに対応していない場合

Google Chrome、Mozilla Firefox などの一部のブラウザは、プラグイン アーキテクチャの関係で MWG のユーザーインターフェースに対応していません。今後、サポートを終了となるブラウザもあります。
これらのブラウザを使用している場合には、ログイン画面より Web Start アプリケーションをダウンロードすると、ブラウザなしでユーザーインターフェースを実行できます。(MWG v7.6.1 以降より利用可能)
また、ブラウザより HTML 形式でユーザーインターフェースを実行可能です。(MWGv7.8.0 以降より利用可能)

2.1.1.1 Web Start アプリケーションによるログイン

[Web Gateway UI as Java-Webstart Download](MWGv7.8 以前のバージョンの場合は[Download MWG-UI Webstart])をクリックします。
「webstart.jnlp」というファイルがダウンロードされます。そのファイルを実行します。



Web Start アプリケーションがダウンロードされます。ダウンロード完了後、アプリケーションを起動すると別のログイン画面が開きます。Username、Password を入力してログイン下さい。

[詳細] オプションを使用すると、MWG の IP アドレスとポートを設定して、SSL セキュア通信を使用できます。SSL のデフォルトポート番号は 4712 です。それ以外の場合は 4711 です。

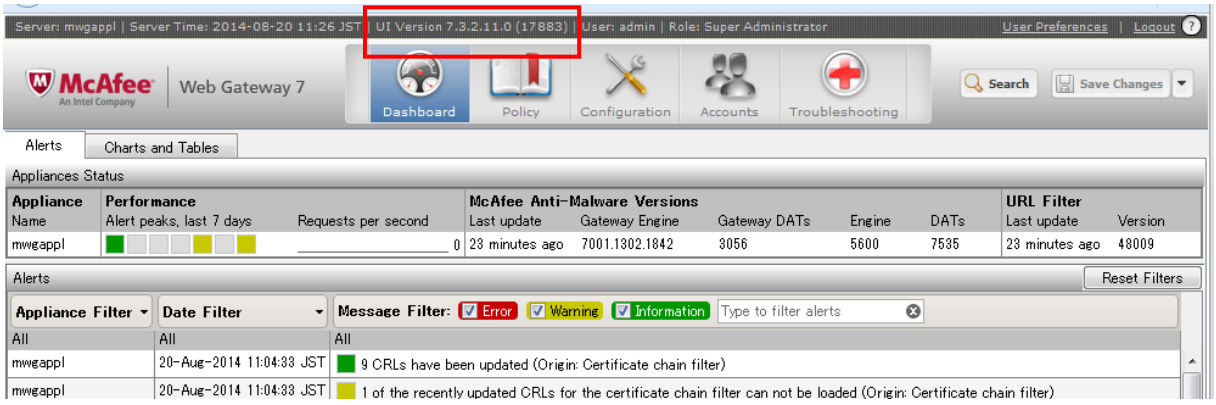
- Central Management 機能有効時の注意事項

Central Management 機能で複数台の MWG で設定を同期している場合には、仕様により 1 号機にログイン中は、2 号機にログインできません。逆に 2 号機にログイン中は 1 号機にログインできません。

また、1 号機をログアウトしたあと、続けて 2 号機にログインするためには、60 秒以上経過の後、ログインします。

2.2 バージョン・ビルドの確認

ログイン後、バージョン・ビルド情報を確認します。
以下画面の場合、UI Version 7.3.2.11(17883)…の部分がバージョン・ビルド情報です。



2.3 バックアップ手順

Troubleshooting＞Backup/Restore に移動し、「Backup to file...」をクリックします。

ブラウザの保存ダイアログが表示されます。ファイルをローカル PC 上に保存します。

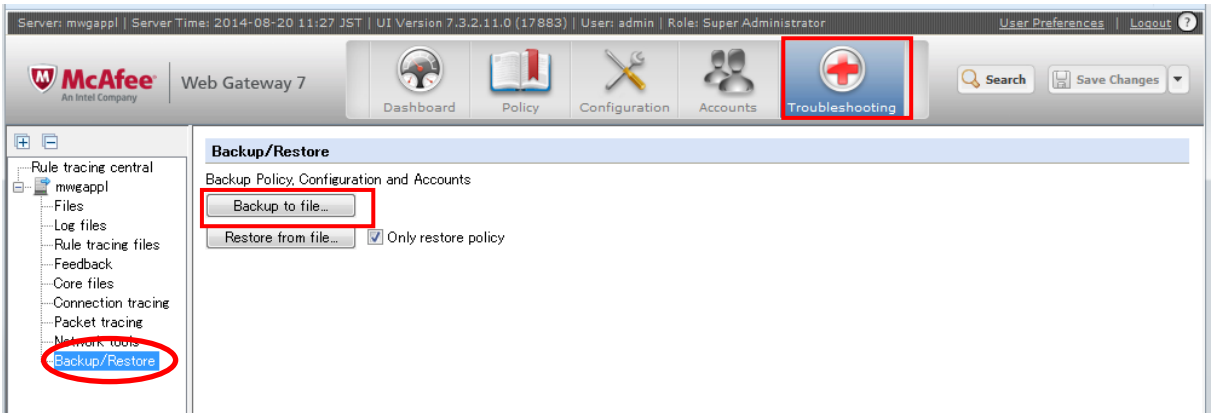
デフォルトのファイル名は、日付.backup という名前になるため、対象機器やバージョン情報がわかりません。
バックアップを取得した際の対象機器、バージョン情報、日付が分かるように、ファイル名にホスト名、バージョン情報を加えて下さい。

（例）ditwg.7.4.2.2.0_17923_2014-08-20.backup
[ホスト名.バージョン情報_ビルド情報_日付.backup]

バックアップの対象は WebUI より実施の設定のみです。
CLI より実施の設定、編集した設定についてはバックアップ対象ではございません。別途バックアップをお願い致します。

以上で設定バックアップは完了です。

- v7.3 までの WebUI



- v7.4 以降の WebUI

- Central Management 機能有効時の注意事項

Central Management 機能を有効にして、複数台の MWG で設定を同期している場合には、1 台にログインすると、その他の MWG の設定も表示されますが、Backup/Restore メニューは、ログイン中の MWG のみ表示されます。
1 号機、2 号機で設定を同期している場合は、1 号機にログインして 1 号機の設定バックを取得したあと、一旦ログアウトし、60 秒以上経過したあと、2 号機にログインして 2 号機の設定バックアップを取得します。

2.4 バックアップに含まれない設定

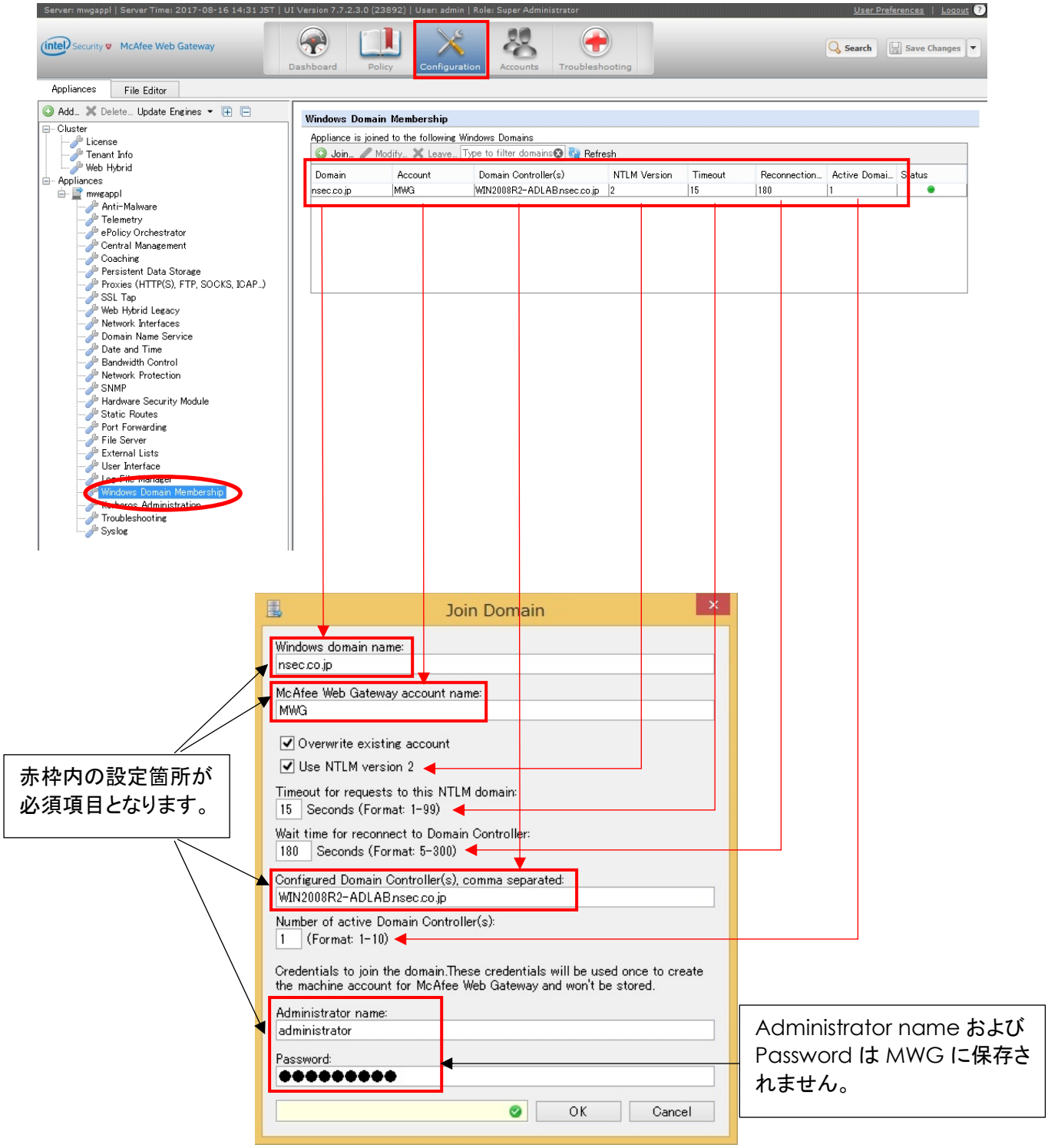
現在確認されている内容として、下記項目はバックアップファイルに含まれないため、リストア後に手動で設定実施の必要があります。
そのため、設定内容を事前に紙面等で控えリストアに備えご準備下さい。

2.4.1 CLI 用 root パスワード

CLI 用に準備されている root パスワードはインストール時に設定されています。
バックアップファイル中には root パスワードは含まれないため、構築時等に別途記録を残して下さい。

2.4.2 Windows Domain Membership(NTLM 認証)

NTLM 認証利用時、MWG は GUI の
[Configuration] > [Appliances] > ホスト名 > [Windows Domain Membership]
よりドメイン参加の設定を実施されています。



2.4.3　シリアルポート転送レート設定確認

一部の環境でシリアルポートの設定値を変更されるケースがあります。
（ほぼ UPS 利用のための設定変更です）
設定変更手順については「3.4.3 シリアルポートの転送レート設定変更」を参照下さい。

2.4.3.1　MWGv7.7.x 以前の場合

1. MWG の CLI にログインし、/etc/init に移動します。
2. ttyS0.conf を開き、ファイル中の以下の記載を確認します。
   （デフォルトでは 19200 となっております）

   exec /sbin/agetty /dev/ttyS0 9600 vt100

2.4.3.2　MWGv7.8.x 以降の場合

1. MWG の CLI にログインし、/etc/default に移動します。
2. Grub を開き、ファイル中の以下の 2 か所の記載を確認します。
   （デフォルトでは 19200 となっております）

一箇所目：
GRUB_CMDLINE_LINUX="$GRUB_CMDLINE_LINUX console=ttyS0,9600n8 console=tty0"

二箇所目：
GRUB_SERIAL_COMMAND="serial --speed=9600 --word=8 --parity=no --stop=1"

2.4.4　HA 機能を利用する際の MFEND-LBID 設定

/etc/sysconfig/mfend において、最下行の MFEND-LBID=数値
の設定を実施している場合に、対象行を手動で記録しておいて下さい。

なお、本設定は同一ネットワーク内に複数の MWG にて HA システムを構築する際に利用するため、通常設定されていないケースがほとんどです。

3 設定リストア

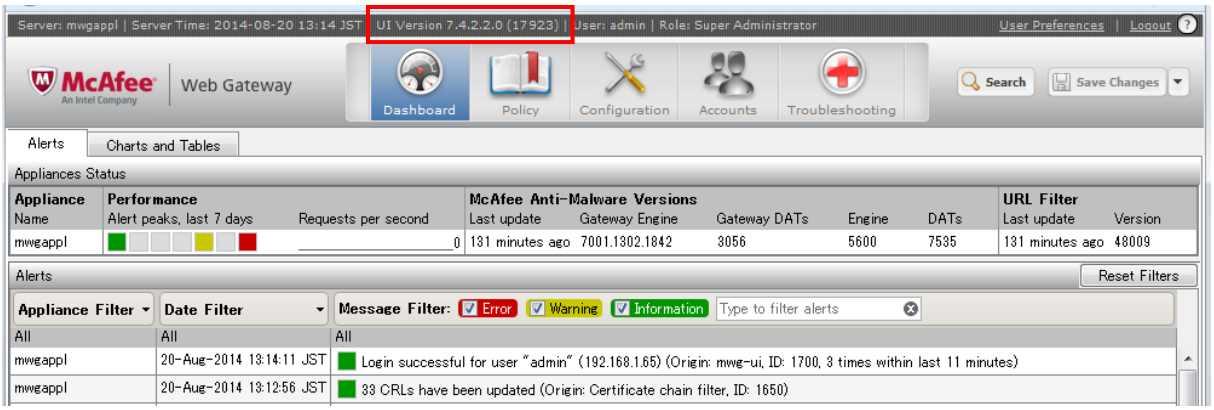
3.1 WebUI へのログイン

設定バックアップの際と同様、「2.1WebUI へのログイン」の手順にてログインを実施します。

3.2 バージョン適合確認

リストアを実行する前に、バックアップ取得した際の MWG のバージョンと、これよりリストア対象機器のバージョンをご確認下さい。バックアップファイルのバージョン情報については、バックアップファイル名をご確認下さい。

以下画面の場合、UI Version 7.4.2.2.0 (17923)…の 7.4.2.2.0 の部分が同一であることをご確認下さい。
build に差異がある場合でも、問題なくリストアすることが可能です。下記の例では、17923 が build 番号です。



3.2.1 バージョン情報が同一の場合

「3.3 リストア実施」の手順に従ってリストアを実施下さい。

3.2.2 バックアップ取得した際のバージョンと、MWG のバージョンに差異がある場合

過去のバージョンでバックアップ取得したファイルを、それよりも新しいバージョンにリストアすることは可能ですが、新しいバージョンでバックアップ取得したファイルをそれより過去のバージョンにリストアすることはできません。

例:

v7.3.2.3 でバックアップ取得したファイルを v7.4.2.2 にリストアすることができます。
v7.4.2.2 でバックアップ取得したファイルを v7.3.2.3 にリストアすることができません。

特定バージョンの MWG を構築するためには、下記の Content & Cloud Security Portal サイト(旧称:Extranet)より、構築したいバージョンのインストール用 ISO イメージファイルをダウンロードして、新規インストールを行う必要があります。

https://contentsecurity.mcafee.com/software_mwg7_download
ログインに必要な ID とパスワードは保守契約サポート証書をご確認下さい。

インストールは CD より起動することで自動的に行われます。
詳細は、以下のメーカーナレッジセンターをご確認下さい。
McAfee Web Gateway v7.x 新規インストール手順
https://kc.mcafee.com/corporate/index?page=content&id=KB80726&actp=null&viewlocale=ja_JP&showDraft=false&platinum_status=false&locale=ja_JP

不明点は弊社保守サポート窓口までお問い合わせ下さい。

3.3 リストア実施

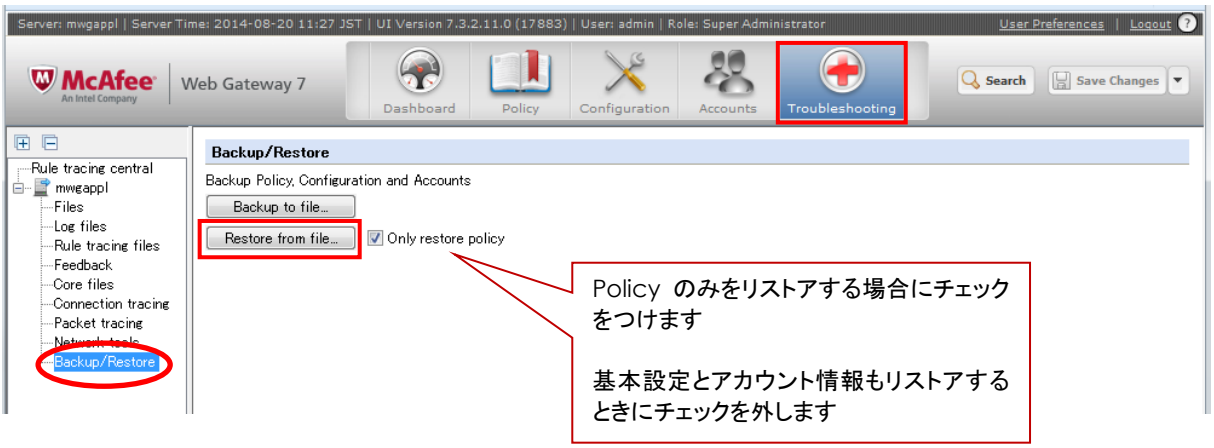
3.3.1 同一筐体の場合

ここでの「筐体」とは WG4000 等の機種ではなく個体を意味します。
IP アドレスやルーティング等 Policy メニュー以外の設定項目のリストアは、WebUI よりはバックアップ取得を行った筐体と同一の筐体に対してのみ可能です。異なる筐体に対して Policy メニュー以外の設定をリストアする場合には、次項「3.3.2 異なる筐体の場合（RMA 等で交換や、機器リプレースの場合）」を参照下さい。

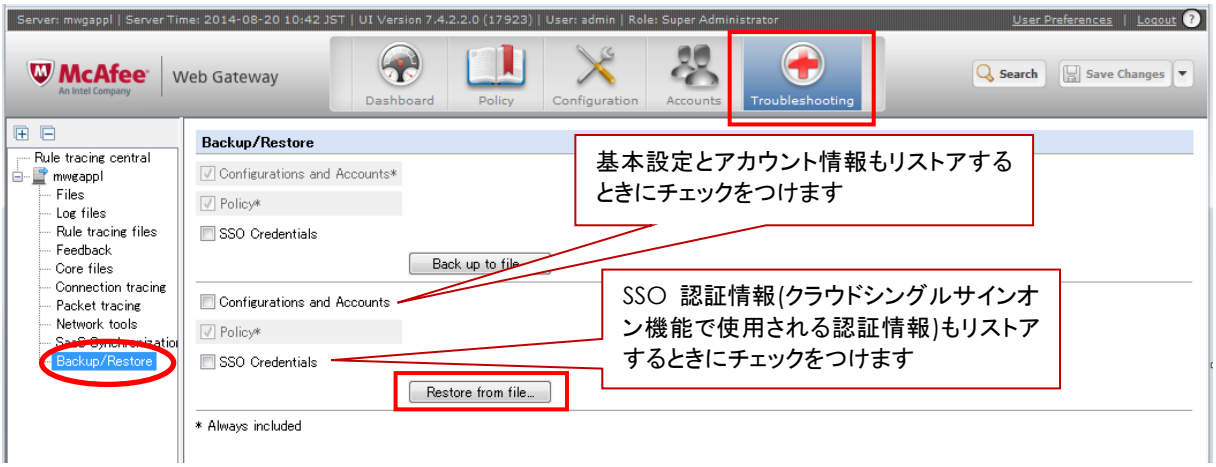
Troubleshooting＞ Backup/Restore に移動し、Restore from file をクリックしてリストアしたいファイルを選択して下さい。
また、この際に Policy のみをリストアしたい場合には、Only restore policy にチェックします。

Configuration や Account の項目も全てリストアしたい場合には、Only restore policy のチェックを外して下さい。
（v7.4 以降では、Configurations and Accounts にチェックします）

- v7.3 までの WebUI



- v7.4 以降の WebUI



リストア実施後、自動的にログアウトされます。再度ログインしてアプライアンスを再起動下さい。
再起動後、設定反映をご確認下さい。

以上で設定リストアは完了です。

3.3.2　異なる筐体の場合（RMA 等で交換や、機器リプレースの場合）

バックアップを取得した筐体とリストア先筐体が別個体である場合、リストアはコマンドラインより実施します。
詳細は、以下のメーカーナレッジセンターをご確認下さい。

コマンドラインより backup ファイルをフルリストアする方法
https://kc.mcafee.com/corporate/index?page=content&id=KB80762&actp=null&viewlocale=ja_JP&showDraft=false&platinum_status=false&locale=ja_JP

3.4 リストア対象外の再設定方法

現在確認されている一部の設定についてはバックアップに含まれないため、
リストア後に手動で再設定を行います。

3.4.1 CLI 用 root パスワード

リストア対象の機器は WebGateway インストール時に設定された root パスワードを保持しています。
パスワードを変更する場合は、passwd コマンドを利用し、下記の通り変更します。
（CAPS Lock 等により、想定外パスワードとなることを回避するため、複数 root にて CLI を接続しておき、
パスワード変更後、想定パスワードでログイン可能なことを確認する手順を推奨します。）

```
# passwd
Changing password for user root.
New password:                    <-- 1 回目の新しいパスワードを入力
Retype new password:             <-- 2 回目の新しいパスワードを入力（1 回目と同内容を確認）
passwd: all authentication tokens updated successfully.
[root@mwg ~]#
```

以上でパスワードの変更完了です。

3.4.2 Windows Domain Membership(NTLM 認証)

NTLM 認証を行っている場合、リストア後に再度 MWG をドメインに参加する必要があります。
詳細は、以下のメーカーナレッジセンターの手順 1、2 をご確認下さい。

NTLM 認証を使用したアクセス制限について
https://kc.mcafee.com/corporate/index?page=content&id=KB80715&actp=null&viewlocale=ja_JP&showDraft=false&platinum_status=false&locale=ja_JP

3.4.3 シリアルポートの転送レート設定変更

一部の環境でシリアルポートの設定値を変更されるケースがあります。
（ほぼ UPS 利用のための設定変更です）

ファイルの編集は vi コマンド等をご利用下さい。
設定変更を行う前に変更対象のファイルをコピーするなどしてバックアップ後、実施下さい。

3.4.3.1 MWGv7.7.x 以前の場合

1. MWG の CLI にログインし、/etc/init に移動します。
2. ttyS0.conf を開き、ファイル中の 19200 を 9600 に変更します。
   （デフォルトでは 19200 となっております）

   ```
   exec /sbin/agetty /dev/ttyS0 19200 vt100
   ↓
   exec /sbin/agetty /dev/ttyS0 9600 vt100
   ```

3. 機器を再起動し変更を反映させます。

3.4.3.2　MWGv7.8.x 以降の場合

1. MWG の CLI にログインし、/etc/default に移動します。

   # cd /etc/default

2. ファイル編集前に、ディレクトリ内にある grub を cp コマンド等でコピーし、バックアップを作成します。

   # cp grub grub.backup20181121

3. 下記コマンドにて生成したバックアップファイルが表示されることを確認します。

   # ls -la

4. grub を開き、ファイル中 2 か所ある 19200 を 9600 に変更します。

一箇所目：
GRUB_CMDLINE_LINUX="$GRUB_CMDLINE_LINUX console=ttyS0,19200n8 console=tty0"
↓
GRUB_CMDLINE_LINUX="$GRUB_CMDLINE_LINUX console=ttyS0,9600n8 console=tty0"

二箇所目：
GRUB_SERIAL_COMMAND="serial --speed=19200 --word=8 --parity=no --stop=1"
↓
GRUB_SERIAL_COMMAND="serial --speed=9600 --word=8 --parity=no --stop=1"

5. CLI 上で以下のコマンドを実行し、変更を適用します。

   # /usr/sbin/grub2-mkconfig -o /boot/grub2/grub.cfg

6. 下記コマンドを実行し、grub.cfg に設定が適用されていることを確認します。
   (適用出来ていない場合は、実行結果が戻りません)

   # cd /boot/grub2
   # grep 9600 grub.cfg
   実行例）
   serial --speed=9600 --word=8 --parity=no --stop=1
   linux16 /boot/vmlinuz-3.18.118-2.mlos2.mwg.x86_64 root=UUID=e2445e0b-ea01-49ce-b62b-6882230d6de0 ro acpi=on rootfstype=ext4 net.ifnames=0 biosdevname=0 quiet selinux=0 crashkernel=128M elevator=deadline console=ttyS0,9600n8 console=tty0
   linux16 /boot/vmlinuz-3.18.118-2.mlos2.mwg.x86_64 root=UUID=e2445e0b-ea01-49ce-b62b-6882230d6de0 ro acpi=on rootfstype=ext4 net.ifnames=0 biosdevname=0 quiet selinux=0 crashkernel=128M elevator=deadline console=ttyS0,9600n8 console=tty0
   linux16 /boot/vmlinuz-3.18.118-1.mlos2.mwg.x86_64 root=UUID=e2445e0b-ea01-49ce-b62b-6882230d6de0 ro acpi=on rootfstype=ext4 net.ifnames=0 biosdevname=0 quiet selinux=0 crashkernel=128M elevator=deadline console=ttyS0,9600n8 console=tty0

7. 機器を再起動し変更を反映させます。

8. 再起動後、CLI にて下記コマンドを実行し、9600 への変更を確認します。
   (変更出来ていない場合は、実行結果が戻りません)

   # dmesg | grep 9600
   実行例）
   [0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-3.18.118-2.mlos2.mwg.x86_64 root=UUID=e2445e0b-ea01-49ce-b62b-6882230d6de0 ro acpi=on rootfstype=ext4 net.ifnames=0 biosdevname=0 quiet selinux=0 crashkernel=128M elevator=deadline console=ttyS0,9600n8 console=tty0
   [0.000000] [ffffea0000000000-ffffea00061fffff] PMD -> [ffff8801b9600000-ffff8801be9fffff] on node 0
   [0.000000] Kernel command line: BOOT_IMAGE=/boot/vmlinuz-3.18.118-2.mlos2.mwg.x86_64 root=UUID=e2445e0b-ea01-49ce-b62b-6882230d6de0 ro acpi=on rootfstype=ext4 net.ifnames=0 biosdevname=0 quiet selinux=0 crashkernel=128M elevator=deadline console=ttyS0,9600n8 console=tty0

3.4.4　HA 機能を利用する際の MFEND-LBID 設定

/etc/sysconfig/mfend に手動でタイプし、MWG をリブートします。
なお、HA 対向装置（リストア対象でない）にて MFEND-LBID=の記述がない場合は、不要です。

HA の 2 台に対して、同時に復旧する場合は、同一ネットワーク内に MWG（HA 構成）がなければ不要。あれば、重複しない ID を指定しリストア下さい。

以上