

# Opengear Bulk Provisioning Guide

**Document version:** 1.0 – 17 Dec 2013

**Contact:** support@opengear.com

## Contents

1. Introduction
2. Golden master: *make-template*
3. Target appliance: *setup-wizard*
4. Target appliance: *callhome-wizard*
5. Lighthouse: *enrollment-wizard*

## 1. Introduction

This feature is supported by firmware version 3.9.1 or later, and Lighthouse version 4.4.0 and later (optional).

Opengear appliances include wizard scripts to facilitate configuration and deployment en masse. These wizards operate at the command line level, so knowledge of the Linux command line and shell scripting is useful, but not necessary – they aim to be user-friendly enough for remote hands to manage.

Both the bulk provisioning of Opengear appliances and bulk enrollment of these appliances into Lighthouse central management system(s) is supported. These features may be used separately or in conjunction.

Using this method, an Opengear appliance can be fully configured and enrolled into Lighthouse with minimal interaction, in under 5 minutes.

The basic steps are:

1. Configure an individual “golden master” appliance with the baseline configuration shared by all Opengear appliances. This may be a minimal configuration if the installs are quite diverse, or a complete configuration when dealing with replicated installs.
2. Use *make-template* to turn the golden master’s active configuration into a template configuration that may be applied to other appliances.
3. Create an OPG backup of the templated golden master appliance.

4. Restore this configuration to each target devices via the CLI, web UI or using a USB thumb drive.
5. Login via the CLI to complete configuration using *setup-wizard*.
6. (Optional) On Lighthouse, use *enrollment-wizard* to automatically place appliances under management. This may be local/routable appliances, or remote appliances that have automatically Call Home using *callhome-wizard*.

Note that steps 5 and 6 may be reversed for remote setup via Lighthouse.

## 2. Golden master: *make-template*

Once the golden master appliance has been configured, its configuration may be templated. This step is one run once per bulk-provisioning. The templated configuration may be applied to other appliances of different model, however care must be taken.

If your configuration requires the appliances to Call Home to Lighthouse system(s), set up the Call Home connections before running *make-template*.

Login to the Opengear CLI via SSH or local serial console (recommended, in case IP settings change midway through) and run:

```
/etc/scripts/wizard/make-template
```

One or more of following prompts are displayed:

```
*** Template Lighthouse management settings [y/n]?
```

If you are using Lighthouse management, say yes here. This removes any generated Call Home SSH client keys and and Call Home ports which are unique to each device.

```
*** Configure automatic Call Home wizard [y/n]?
```

If you have templatable Call Home connections, you can automatically set these up with a unique Call Home to your Lighthouse system(s) on first boot by supplying the Call Home password.

This password is stored in cleartext in the template OPG but does not grant any privileges on the Lighthouse, so can be considered secure.

\*\*\* Pre-authorize Lighthouse management [y/n]?

Include one or more Lighthouse SSH public SSH management client key in the `authorized_keys` file. This enables hands off enrollment of the target appliance from the Lighthouse, without having to enter any passwords.

See the enrollment-wizard section for more information.

\*\*\* Template per-console server settings [y/n]?

Recommended. Removes any auto-detected, per-model settings and auto-generated SSH server keys so they are regenerated by each target appliance.

This step also templates any and all instances of the current golden master appliance hostname that occur in configuration. This makes the hostname special in this process.

When the target device's hostname is set via `setup-wizard`, it proliferates to each of these templated settings. Therefore the hostname should be used to uniquely identify the target device in any other settings that may require it, e.g. the SMTP sender email address may be *hostname@yourdomain.com* or IPsec VPN tunnel Left ID may be *@hostname*.

\*\*\* Set Network Interface to default DHCP/192.168.0.1 (static config preserved) [y/n]?

Sets factory default dual DHCP and static/192.168.0.1 mode on the first network port. This is to assist discoverability when deploying the target appliance into a remote network, e.g. by remote hands who may be following the factory quick setup guide.

Static settings including DNS are not removed, so will be available when static network configuration mode is re-enabled.

Alternative you may choose your own default network settings by enabling a static network configuration on the golden master, and skipping this step.

\*\*\* Disable failover/enable always-up OOB [y/n]?

If e.g. a cellular modem is being used a failover connection for remote management, you may choose to set this to always-up.

Used in conjunction with the previous step, this is useful for testing the cellular reachability of target appliances as they are provisioned before being shipped to

site, particularly useful for creating a configuration to “parachute” into sites where WAN connectivity is yet to be setup or must be restored via cellular.

\*\*\* Template security settings [y/n]?

This scrubs any IPsec pre-shared keys and AAA server passwords. This settings are re-entered during the target appliance’s setup-wizard phase.

\*\*\* Default root password [y/n]?

Say yes to set the root password back to *default*. This is to aid remote hands who might be following the factory quick setup guide.

\*\*\* Queue setup wizard for next login [y/n]?

Automatically run setup-wizard at next login, i.e. first login on the target appliance.

See the setup-wizard section for more information.

Once make-template has successfully completed, back up the OPG configuration as instructed (i.e. in the usual way).

### 3. Target appliance: *setup-wizard*

This step is applied once per target appliance, so aims to be a minimal as possible. First, restore the template OPG to each target appliance using one of these methods:

#### Web UI

1. Browse to the target appliance, click:

```
Backup -> Backup File -> Browse for template.opg ->
Restore
```

#### CLI

1. Copy *template.opg* into the appliance’s /tmp directory using WinScp or similar
2. Login to the CLI via Web Terminal, SSH or local serial console and run:

```
config -i /tmp/template.opg
```

## USB drive

Combined with callhome-wizard, you can complete remote provisioning with only physical interaction with USB-enabled Opendgear models.

Note that the USB storage device must be formatted with a Windows FAT32/VFAT file system on the first partition or the entire disk, most USB thumb drives are already formatted this way.

### Prepare the USB key:

1. Insert the USB drive into your workstation
2. Copy template.opg to the top level directory of the drive and rename the file to:

```
default.opg
```

3. Rename the volume label (drive name) to:

```
OPG_DEFAULT
```

### Apply the template via USB:

4. Insert the USB drive into any of the Opendgear appliance's USB ports, then perform a factory reset (e.g. press the Reset/Erase button twice within 2 seconds)
5. When you have confirmed the device has booted, or after 5 minutes, you can safely remove the USB key

The target appliance reboots, and auto-generates SSH keys (similar to first boot after a factory erase). After a short time, it is ready to run setup-wizard to complete per-appliance personality settings and re-enter any scrubbed settings from the make-template phase.

This either runs automatically after authenticating to the CLI, or you may run it manually:

```
/etc/scripts/wizard/make-template
```

One or more of following prompts are displayed:

```
*** Hostname:
```

This is the system name for this device, but also may be used in other parts of the configuration where unique identification is useful. See the note under “Template per-console server settings” in the make-template section for more information.

```
*** Enable DHCP [y/n]?
```

This is the start of network setup. Select yes to enable DHCP, or no to enter static IP, netmask and gateway settings. Note that when using static settings, DNS servers are not requested, this must be part of the templated configuration or set manually.

```
*** Pre-shared key/Password:
```

Any scrubbed security settings are re-entered now, see “Template security settings” in the make-template section for more information.

```
*** Set root password [y/n]?
```

Select yes to set a root password now.

## 4. Target appliance: *callhome-wizard*

If you chose to enable the automatic Call Home wizard, this script runs automatically on first boot of the target appliance. Once SSH client keys have been generated, as Lighthouse system(s) become available it uses the pre-supplied Call Home password to establish Call Home connection(s).

You may also run this script manually, and enter a Call Home password manually if it has not been pre-supplied:

```
/etc/scripts/wizard/callhome-wizard
```

Once the script is complete, the target appliance’s unique Call Home port is logged to its syslog.

```
*** Lighthouse (lighthouse-address:lighthouse-port) Call  
Home redirected port is: 54321
```

This feature is particularly useful deploying Opendgear appliances onto remote networks where access is problematic, and/or where skilled remote hands may not be available.

## 5. Lighthouse: enrollment-wizard

This script automatically enrolls candidates for management (either routable or Call Home). It has several modes of operation to suit your workflow and security policy.

The target appliance is interrogated to determine the hostname and number of serial ports. This information makes up its basic configuration in Lighthouse. Note that due to performance and bandwidth, full managed device monitoring is disabled and must be manually enabled if required.

Fully automatic operation requires the Lighthouse's public key to be pre-authorized in the template OPG. See the "Pre-authorize Lighthouse key" in the make-template section. The public key may be installed by other means, so this feature can operate independently of the make-template and target appliance wizard scripts.

Running this script with no configuration enrolls any and all unmanaged remote console servers with a Call Home connection.

```
/etc/scripts/wizard/enrollment-wizard
```

You can view these connections by running:

```
/etc/scripts/wizard/list-callhome
```

The following configuration files on the Lighthouse are used to further control automatic enrollment.

```
/etc/config/wizard/autoenroll.txt
```

Only the console servers listed will be enrolled. Whitelist restrictions also apply (see below). List one per line, with the format address:sshport. These may be any combination of local or remote loopback connections (aka Call Home), e.g.:

```
localhost:54321  
opengear.fqdn.com:2222  
192.168.0.2:22
```

On successful enrollment the corresponding line is removed.

```
/etc/config/wizard/whitelist.txt
```

Restricts enrollment to pre-defined console servers by hardware address. Appliances are identified by the MAC address of their first network port

(eth0/Network 1). This MAC address is physically printed on the outside of the appliance and its packaging, or can be found under `Status -> Support Report`. List one MAC address per line with the format (case insensitive):

```
00:13:C6:00:FF:FF
```

If this file exists and is not empty, non-matching console servers are ignored. On successful enrollment, the file remains unchanged.