Configure CGR 1000 with CGOS for Zero Touch Deployment

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Step-by-Step Configuration and Enrollment](#)
[Sample Configuration](#)
[Verify](#)
[Troubleshoot](#)

Introduction

This document describes configuration steps required to successfully register Cisco Connected Grid Router 1000 (CGR 1000) with Connected Grid Operating System (CGOS) to Field Network Director (FND) as a Field Device. Before a router is registered to the FND, it must meet several pre-requisites that include enrollment in Public Key Infrastructure (PKI) and custom configuration. In addition to this, a sanitized sample configuration will be included.

Contributed by Ryan Bowman, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CG-NMS/FND application server 1.0 or later installed and running with web UI access available.
- Tunnel Provisioning Server (TPS) proxy server installed and running.
- Oracle database server installed and correctly configured.
- setupCgms.sh successfully run at least once with a successful first-time db_migrate.
- DHCPv4 and DHCPv6 server(s) already configured and available with proxy settings saved on the **Admin > Provisioning Settings** page of the FND web User Interface (UI).
- The device .csv file should have already been imported to the FND and the device should be in 'unheard' status.

Components Used

The information in this document is based on these software and hardware versions:

- FND 3.0.1-36
- Software-based SSM (also 3.0.1-36)
- cgms-tools package installed in application server (3.0.1-36)
- All Linux servers running RHEL 6.5
- All Windows servers running Windows Server 2008 R2 Enterprise
- CSR 1000v running on a VM as head-end router
- CGR-1120/K9 used as Fied Area Router (FAR) with CG-OS 4(3)

A controlled FND lab environment was used during the creation of this document. While other deployments will differ, you should adhere to all minimum requirements from the installation guides.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Step-by-Step Configuration and Enrollment

1. Configure the device hostname.

2. Configure the domain-name.

3. Configure the DNS server(s).

4. Configure and verify time/NTP.

5. Bring up the cellular cards and/or Ethernet interfaces. Ensure that all necessary interfaces have their IPs and that the router has a gateway of last resort.
In order for the FND to successfully provision the Loopback 0 interface, it must already be created with addresses. Create the Loopback 0 interface and verify that it has IPv4 and IPv6 addresses. You can use throwaway" IPs because they will be replaced after tunnel provisioning.

6. Enable these features: ntp, crypto ike, dhcp, tunnel, crypto ipsec virtual-tunnel.

7. Create your trustpoint enrollment profile (This is the direct URL for the Simple Certificate Enrollment Protocol (SCEP) enrollment webpage on your RSA Certificate Authority (CA). If you use a Registration Authority, the URL will be different):

```
Router(config)#crypto ca profile enrollment LDevID_Profile
Router(config-enroll-profile)#enrollment url
http://networkdeviceenrollmentserver.your.domain.com/CertSrv/mscep/mscep.dll
```

8. Create your trustpoint and bind the enrollment profile to it.

```
Router(config)#crypto ca trustpoint LDevID
Router(config-trustpoint)#enrollment profile LDevID_Profile
Router(config-trustpoint)#rsakeypair LDevID_Keypair 2048
Router(config-trustpoint)#revocation-check none
Router(config-trustpoint)#serial-number
Router(config-trustpoint)#fingerprint
xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
```

9. Authenticate your trustpoint with the SCEP server.

```
Router(config)#crypto ca authenticate LDevID
  Trustpoint CA authentication in progress. Please wait for a response...
```

```
  2017 Mar  8 19:02:00 %$ VDC-1 %$ %CERT_ENROLL-2-CERT_EN_SCEP_CA_AUTHENTICATE_OK: Trustpoint
LDevID: CA certificates(s) authenticated.
```

10. Enroll your trustpoint in Public Key Infrastructure (PKI).

```
Router(config)#crypto ca enroll LDevID
Create the certificate request ..
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Challenge password:
Re-enter challenge password:
The serial number in the certificate will be: PID:CGR1120/K9 SN:JAF############
Certificate enrollment in progress. Please wait for a response...
2017 Mar  8 19:02:24 %$ VDC-1 %$ %CERT_ENROLL-2-CERT_EN_SCEP_ENROLL_OK: Trustpoint LDevID:
Device identity certificate successfully enrolled to CA.
```

11. Verify your ceritifcate chain.

```
Router#show crypto ca certificates
```

12. Configure SNMP parameters required for Callhome to work correctly.

```
Router(config)#snmp-server contact NAME
Router(config)#snmp-server user admin network-admin
Router(config)#snmp-server community PUBLIC group network-operator
```

13. Configure these basic Wireless Personal Area Network (WPAN) module settings.

```
Router(config)#interface wpan 4/1
Router(config-if)#no shutdown
Router(config-if)#panid 5
Router(config-if)#ssid meshssid
Router(config-if)#ipv6 add 2001:db8::1/32
```

14. As the FND relies on Netconf over HTTPS to manage FARs, enable and appropriately configure the HTTPS server to listen on port 8443 and to authenticate connections with PKI.

```
Router(config)#ip http secure-server
Router(config)#ip http secure-server trustpoint LDevID
Router(config)#ip http secure-port 8443
```

15. Configure your callhome profile.

```
Router(config)#callhome
Router(config-callhome)#email-contact email@domain.com
Router(config-callhome)#phone-contact +1-555-555-5555
Router(config-callhome)#streedaddress TEXT
Router(config-callhome)#destination-profile nms
Router(config-callhome)#destination-profile nms format netconf
Router(config-callhome)#destination-profile nms transport-method http
Router(config-callhome)#destination-profile nms http https://tpsproxy.your.domain.com:9120
Router(config-callhome)#enable
```

16. Save the configuration.

17. At this point, all you have to do is reload the router but if you want to manually start registration without a reload you can configure cgdm:

```
Router(config)#cgdm
Router(config-cgdm)#registration start trustpoint LDevID
```

Sample Configuration

Here is a sanitized configuration taken from a CGR1120 just before successful ZTD (in this lab environment the Ethernet2/2 interface was used as the primary IPSec tunnel source):

```
version 5.2(1)CG4(3)
logging level feature-mgr 0
hostname YOUR-HOSTNAME
vdc YOUR-HOSTNAME id 1
   limit-resource vlan minimum 16 maximum 4094
   limit-resource vrf minimum 2 maximum 4096
   limit-resource u4route-mem minimum 9 maximum 9
   limit-resource u6route-mem minimum 24 maximum 24
   limit-resource m4route-mem minimum 58 maximum 58
   limit-resource m6route-mem minimum 8 maximum 8
feature ntp
feature crypto ike
feature dhcp
feature tunnel
feature crypto ipsec virtual-tunnel
username admin password YOURPASSWORD role network-admin
username Administrator password YOURPASSWORD role network-admin
ip domain-lookup
ip domain-name your.domain.com
ip name-server x.x.x.x
crypto key param rsa label LDevID_keypair modulus 2048
crypto key param rsa label YOUR-HOSTNAME.your.domain.com modulus 2048
crypto ca trustpoint LDevID
   enrollment profile LDevID_Profile
   rsakeypair LDevID_keypair 2048
   revocation-check none
   serial-number
   fingerprint xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
crypto ca profile enrollment LDevID_Profile
   enrollment url http://x.x.x.x/CertSrv/mscep/mscep.dll
snmp-server contact NAME
snmp-server user Administrator network-admin
snmp-server community public group network-operator
callhome
   email-contact ciscotac@cisco.tac.com
   phone-contact +1-555-555-5555
   streetaddress Here
   destination-profile nms
   destination-profile nms format netconf
   destination-profile nms transport-method http
   destination-profile nms http https://tpsproxy.your.domain.com:9120 trustpoint LDevID
   destination-profile nms alert-group all
   enable
ntp server x.x.x.x
ntp server x.x.x.x
crypto ike domain ipsec
vrf context management
vlan 1
service dhcp
ip dhcp relay
line tty 1
line tty 2

interface Dialer1
interface Ethernet2/1
interface Ethernet2/2
   ip address x.x.x.x/30
   no shutdown
interface Ethernet2/3
interface Ethernet2/4
```

```
interface Ethernet2/5
interface Ethernet2/6
interface Ethernet2/7
interface Ethernet2/8
interface loopback0
   ip address 1.1.1.1/32
   ipv6 address 2001:x:x::80/128
interface Serial1/1
interface Serial1/2
interface Wpan4/1
   no shutdown
   panid 20
   ssid austiniot
   ipv6 address 2001:db8::1/32
interface Wifi2/1
clock timezone CST -6 0
clock summer-time CST 2 Sun Mar 02:00 1 Sun Nov 02:00 60
line console
line vty
boot kickstart bootflash:/cgr1000-uk9-kickstart.5.2.1.CG4.3.SPA.bin
boot system bootflash:/cgr1000-uk9.5.2.1.CG4.3.SPA.bin
ip route 0.0.0.0/0 x.x.x.x
feature scada-gw
scada-gw protocol t101
scada-gw protocol t104
ip http secure-port 8443
ip http secure-server trustpoint LDevID
ip http secure-server
cgdm
   registration start trustpoint LDevID
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.