# Configuración CGR 1000 con CGOS para el despliegue cero del tacto

## Contenido



## Introducción

Este documento describe los pasos para la configuración requeridos para registrar con éxito al router conectado Cisco 1000 (CGR 1000) de la rejilla con el sistema operativo conectado de la rejilla (CGOS) para colocar al director de la red (FND) como dispositivo del campo. Antes de que registren a un router al FND, debe resolver varios requisitos previos que incluyan la inscripción en el Public Key Infrastructure (PKI) y configuración personalizada. Además de esto, una configuración de muestra esterilizada será incluida.

Contribuido por el arquero de Ryan, ingeniero de Cisco TAC.

## Prerrequisitos

### Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servidor de aplicaciones 1.0 o haber instalado posterior y el ejecutarse CG-NMS/FND con el acceso de la red UI disponible.
- Servidor proxy del servidor de aprovisionamiento del túnel (TP) instalado y el ejecutarse.
- Servidor de base de datos Oracle instalado y configurado correctamente.
- setupCgms.sh se ejecuta con éxito por lo menos una vez con un db_migrate por primera vez acertado.
- Servidores DHCPv4 y DHCPv6 configurados ya y disponibles con las configuraciones de representación guardadas en **Admin > página Configuración del aprovisionamiento de la** interfaz del Web User FND (UI).
- El archivo del .csv del dispositivo se debe haber importado ya al FND y el dispositivo debe estar en el estatus “inaudito”.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FND 3.0.1-36
- SS basado en software (también 3.0.1-36)
- las cgms-herramientas empaquetan instalado en el servidor de aplicaciones (3.0.1-36)
- Todos los servidores Linux que ejecutan RHEL 6.5
- Todos los Servidores Windows que dirigen la empresa 2008 del r2 del Servidor Windows
- CSR 1000v que se ejecuta en un VM como router de centro distribuidor
- CGR-1120/K9 usados como router de área de Fied (LEJANO) con CG-OS 4(3)

Un ambiente de laboratorio controlado FND fue utilizado durante la creación de este documento. Mientras que diferenciarán otras implementaciones, usted debe adherirse a todos los requerimientos mínimos de las guías de instalación.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Configuración e inscripción graduales

1. Configure el nombre del host del dispositivo.

2. Configure el Domain Name.

3. Configure los servidores DNS.

4. Configure y verifique time/NTP.

5. Saque a colación los indicadores luminosos LED amarillo de la placa muestra gravedad menor y/o las interfaces de Ethernet celulares. Asegúrese de que todas las interfaces necesarias tengan sus IP y de que el router tiene un gateway de último recurso.
Para que el FND provision con éxito la interfaz del loopback0, debe ser creado ya con los direccionamientos. Cree la interfaz del loopback0 y verifiquela que tiene direccionamientos del IPv4 y del IPv6. Usted puede utilizar los” IP desechables porque serán substituidos después del aprovisionamiento del túnel.

6. Habilite estas características: NTP, ike crypto, DHCP, túnel, virtual-túnel crypto del IPSec.

7. Cree su perfil de la inscripción del trustpoint (éste es el URL directo para la página web de la inscripción del protocolo simple certificate enrollment (SCEP) en su Certificate Authority (CA) RSA. Si usted utiliza una autoridad de registro, el URL será diferente):

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

8. Cree su trustpoint y ate el perfil de la inscripción a él.

```
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. Autentique su trustpoint con el servidor SCEP.

```
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. Aliste su trustpoint en el 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. Verifique su encadenamiento del ceritifcate.

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

12. Configure los parámetros SNMP requeridos para que Callhome trabaje correctamente.

```
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 estas configuraciones personales del módulo de la red de área de los elementos básicos de red inalámbrica (WPAN).

```
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. Como el FND confía en Netconf sobre el HTTPS para manejar FARs, permiso y para configurar apropiadamente al servidor HTTPS para escuchar en el puerto 8443 y para autenticar las conexiones con el PKI.

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

15. Configure su perfil del callhome.

```
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. Guarde la configuración.

17. En este momento, todo lo que usted tiene que hacer es recargar al router pero si usted quiere comenzar manualmente el registro sin una recarga usted puede configurar el cgdm:

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

# Configuración de muestra:

Aquí está una configuración esterilizada tomada de un CGR1120 momentos antes de ZTD acertado (en este ambiente de laboratorio la interfaz Ethernet2/2 fue utilizada como la fuente primaria del túnel IPsec):

```
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
```

# Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

# Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.