

Configure VG224 SCCP Secure Encrypted

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Verify](#)

Introduction

This document describes secure encrypted configuration Signalling Connection Control Part (SCCP) on VG224 Analog Gateway.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SCCP
- VG224
- Cisco Unified Communications Manager (CUCM)

Components Used

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

- VG224

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, ensure that you understand the potential impact of any command.

Configure

Step 1. Copy the callmanager.pem certificate to the VG224 (referenced as SECURE trustpoint in the below configuration)

Step 2. Create a self signed certificate on the VG224 with the MAC address of FastEthernet0/0 (bind interface) with only the last 10 digits as the subject-name.

Step 3. Copy the vg-cert to CUCM as a call-manager trust and restart CUCM.

The information is provided for configuration of certificates that are required for VG224.

```

Router(config)#crypto key generate rsa general-keys label vg modulus 1024
Router(config)#crypto pki trustpoint vg
Router(ca-trustpoint)#enrollment selfsigned
serial-number none
fqdn none
ip-address none
subject-name cn=1A:E2:85:7B:E2 <----- Last 10 DIGITS ONLY of the SCCP bind interface.
Formatting EXACTLY as shown with colons.
rsakeypair vg
crypto pki enroll vg
Router(config)#crypto pki export vg_cert pem terminal

```

Tip: [Command Reference Guide](#)

Note: You will not see a lock icon when calling from a secure VG224 analog phone to a secure IP phone due to caveat [CSCti08882](#)

Verify

This information is for verification for successful registration of VG224

```

Router(config)#crypto key generate rsa general-keys label vg modulus 1024
Router(config)#crypto pki trustpoint vg
Router(ca-trustpoint)#enrollment selfsigned
serial-number none
fqdn none
ip-address none
subject-name cn=1A:E2:85:7B:E2 <----- Last 10 DIGITS ONLY of the SCCP bind interface.
Formatting EXACTLY as shown with colons.
rsakeypair vg
crypto pki enroll vg
Router(config)#crypto pki export vg_cert pem terminal

```

This shows that secure VG224 using SCCP IOS configuration.

Building configuration...

```

Current configuration : 5258 bytes
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot system slot0:vg224-i6k9s-mz.151-4.M3
boot-end-marker
!
!
enable secret 5 $1$f99B$PWPC1PrUNzgsUZE08aBYG.
!
no aaa new-model
crypto pki token default removal timeout 0
!
crypto pki trustpoint SECURE
  enrollment terminal
  revocation-check crl

```

```

!
crypto pki trustpoint vg
  enrollment selfsigned
  serial-number none
  fqdn none
  ip-address none
  subject-name cn=1A:E2:85:7B:E24      ( instead of this command, we can use hiddle command
"mac-address Fast Ethernet0/0 as well )
  revocation-check crl
  rsakeypair AN1AE2857BE2400
!
!
crypto pki certificate chain SECURE
  certificate ca 588C9B7C2D4B37F03930E8C926D02A18
    <truncated>
crypto pki certificate chain vg certificate self-signed 03 <truncated> ip source-route ! ip cef
ip name-server 172.18.108.43 ip name-server 172.18.108.34 ! ! no ipv6 cef ! stcapp ccm-group 1
stcapp security trustpoint vg stcapp security mode encrypted stcapp ! stcapp feature access-code
! stcapp feature speed-dial ! ! ! stcapp supplementary-services port 2/0 fallback-dn 862224 ! !
! ! ! ! ! ! voice-card 0 ! ! ! ! ! ! ! ! interface FastEthernet0/0 ip address dhcp duplex
auto speed auto ! interface FastEthernet0/1 no ip address duplex auto speed auto ! ip forward-
protocol nd ! ip http server no ip http secure-server ip route 0.0.0.0 0.0.0.0 14.1.97.1 254 ip
route 0.0.0.0 0.0.0.0 14.1.97.1 254 ! ! ! control-plane ! ! voice-port 2/0 timeouts initial 60
timeouts interdigit 60 timeouts ringing infinity ! voice-port 2/1 ! <truncated>
! voice-port 2/23 ! ccm-manager config server 172.18.172.204 ccm-manager config ccm-manager sccp
local FastEthernet0/0 ccm-manager sccp ! ! mgcp profile default ! sccp local FastEthernet0/0
sccp ccm 172.18.172.204 identifier 1 version 7.0 sccp ccm 172.18.172.205 identifier 2 version
7.0 sccp ccm 172.18.172.206 identifier 3 version 7.0 sccp ! sccp ccm group 1 associate ccm 1
priority 1 associate ccm 2 priority 2 associate ccm 3 priority 3 ! dial-peer voice 999200 pots
service stcapp securiy mode encrypted =====> Required command
  port 2/0
!
dial-peer voice 99920 pots
! service stcapp

securiy mode encrypted =====> Required command
  port 2/1
!
!(configure all ports in same secure mode)
!
line con 0
line aux 0
line vty 0 4
  password ww
  login
  transport input all
!
ntp server 172.18.108.15
end

```