

Cisco CallManager Express Security

What Is Cisco CallManager Express?

The Cisco® CallManager Express is an optional software feature in Cisco IOS® Software that enables Cisco routers to deliver Key System or Hybrid PBX functionality for Enterprise Branch Offices or Small Businesses. Cisco CallManager Express is ideal for customers for data connectivity requirements that also have a need for a telephony solution. Whether offered through a service provider's managed Services offering, or purchased directly by a corporation, Cisco CallManager Express offers many of the core telephony features required in the small office as well as many advanced features not available on traditional telephony solutions. Being able to deliver IP Telephony and data routing on a single converged solutions allows customers to optimize their operations and maintenance costs, resulting in a very cost-effective solution to meet their office needs.

Cisco CallManager Express delivers integrated IP Communications and call processing solutions in Cisco IOS Software on the Cisco Voice Gateway Routers. As a result, the same security best practices that are recommended for the Cisco IOS Software gateways are applicable to Cisco CallManager Express. In addition, the following Cisco CallManager Express specific security practices can be implemented to provide additional security protections.

Cisco CallManager Express on Cisco IOS Software Router or Voice Gateway

Cisco CallManager Express, a software feature added to Cisco IOS Software, delivers integrated IP Communications and call processing solutions in Cisco IOS Software on the Cisco Voice Gateway Routers.

Cisco CallManager Express is vulnerable to attacks to the Cisco IOS Software Router and Voice Gateways. As a result, the same security best practices that are recommended for the Cisco IOS Software routers and gateways are applicable to Cisco CallManager Express. In addition, the following Cisco CallManager Express-specific security practices can be implemented to provide additional levels of security control and security protection.

It's not the scope of this document to cover Cisco IOS Software gateway VPN/IP Sec/3DES/AES feature set because it's generic to the voice gateways and is not specific to Cisco CallManager Express.

System Access Locally and Remotely

When in EXEC mode, **config t**, the **telephony-service** command takes a user into the Cisco CallManager Express configuration mode. The **show running-configure** and **show telephony-service** commands show all registered phones/users, extension numbers, and username/passwords for Cisco CallManager Express GUI access. The first step of security control is at the system access level. Password encryption, user authentication, and command auditing are very critical to prevent security breaches and holes.



Enable Secret and Encrypt Passwords

Enable password is cleartexted to provide access control to EXEC mode of the router. Use Enable Secret to encrypt the enable password:

```
enable secret <removed>
no enable password
```

The **enable secret** command takes precedence over the **enable password** command if both are configured; they cannot be used simultaneously.

To increase security access, passwords can be encrypted to prevent any unauthorized users from viewing the passwords when packets are examined by protocol analyzers:

```
Service password-encryption
```

Create Multiple Privilege Levels

By default, Cisco IOS Software has two levels of access to commands: EXEC mode (level 1) and privileged EXEC mode (level 15). Configuring up to 16 privilege levels (from 0, the most restricted level, to 15, the least restricted level) to protect the system from unauthorized access.

```
Privilege mode level level
Enable secret level level {0|5} password string
```

Restrict Access to vty

Allow only certain users/locations to Telnet to the router via vty by defining and applying an access list for permitting or denying remote Telnet sessions.

```
line vty 0 4
 access-class 10 in
 access-list 10 permit 10.1.1.0 0.0.0.255
```

Using AAA to Secure Access

An authentication server can be used to validate user access to the system. The following commands allow an AAA server, TACACS+ server, to be used for authentication services.

```
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication enable default tacacs+ enable
ip tacacs source-interface Loopback0
tacacs-server host 215.17.1.2
tacacs-server host 215.17.34.10
tacacs-server key xyz (defines the shared encryption key to be xyz)
```



Command Accounting/Auditing on AAA

The following commands use a TACACS+ server for command accounting and auditing purposes.

```
aaa new-model
aaa authentication login default tacacs+ enable
(login uses TACACS+, if not available, use enable password)

aaa authentication enable default tacacs+ enable
aaa accounting command 1 start-stop tacacs+
(runs accounting for commands at the specified privilege level 1)

aaa accounting exec start-stop tacacs+
ip tacacs source-interface Loopback0
tacacs-server host 215.17.1.2
tacacs-server host 215.17.34.10
tacacs-server key xyz (defines the shared encryption key to be xyz)
```

The sample command log shows the information contained in a TACACS+ command accounting record for privilege level 1.

```
Wed Jun 25 03:46:47 1997 172.16.25.15 fgeorge tty3 5622329430/4327528 stop
task_id=3 service=shell priv-lvl=1 cmd=show version <cr>
Wed Jun 25 03:46:58 1997 172.16.25.15 fgeorge tty3 5622329430/4327528 stop
task_id=4 service=shell priv-lvl=1 cmd=show interfaces Ethernet 0 <cr>
Wed Jun 25 03:47:03 1997 172.16.25.15 fgeorge tty3 5622329430/4327528 stop
task_id=5 service=shell priv-lvl=1 cmd=show ip route <cr>
```

Configure Local User Authentication When AAA Is Not Available

Always require login—even though the external AAA server is unreachable.

```
username joe password 7 045802150C2E
username jim password 7 0317B21895FE
!
line vty 0 4
login local
```

Configure SSH Access

Use the following command to generate RSA key pairs for the router.

```
router(config)#crypto key generate rsa
```

By default the vty's transport is Telnet. The following command disabled Telnet and supports only SSH to the vty lines.

```
line vty 0 4
transport input ssh
```



ACLs for SNMP Access

The community access string can be set up to permit access to the Simple Network Management Protocol (SNMP). The following example assigns the “changeme-rw” string to SNMP, allowing read-write access and specifies that IP access list 10 can use the community string:

```
access-list 10 remark SNMP filter
access-list 10 permit 10.1.1.0 0.0.0.255
snmp-server community changeme-rw RW 10
snmp-server community changeme-ro RO 10
```

Because “read” and “write” are two common community strings for read and write access, respectively, change the community strings to different ones.

Disable CDP Unless Needed

Because CDP automatically discovers the neighboring network devices supporting CDP, disable CDP in an untrusted domain so that Cisco CallManager Express routers won’t show in the CDP table of other devices.

```
no cdp run
```

If CDP is needed, then consider disabling CDP on a per-interface basis.

```
Interface FastEthernet0/0
no cdp enable
```

Cisco CallManager Express Security for IP Telephony

IP Phone Registration Control

Cisco CallManager Express should be configured to allow IP phones in the trusted domain for registration. Assuming that the local segment is a trusted domain, use the **strict-match** option in the **ip source-address** command, so that only locally attached IP phones will be able to register to the Cisco CallManager Express router and get telephony services.

```
Cisco CallManager Express-3.0(config-telephony)#ip source-address 1.1.1.1 port 2000
strict-match
```

You’d want to block port 2000 access from the WAN side to prevent external SCCP phones from registering with Cisco CallManager Express. Use the following **access-list** to block port 2000 access from WAN interfaces

```
access-list 101 deny tcp any any eq 2000
```

Note: Unknown phones or phones that are not configured in Cisco CallManager Express are allowed to register with Cisco CallManager Express by default for ease of management, but they don’t get dial tones until you configure them by associating the buttons with ephone-dns or configuring auto assign dns under telephony service.

Cisco IP Phone Registration Monitory

Cisco CallManager Express 3.0 has added the following syslog messages to generate and display all registration/deregistration events:

```
%IPPHONE-6-REG_ALARM
%IPPHONE-6-REGISTER
%IPPHONE-6-REGISTER_NEW
%IPPHONE-6-UNREGISTER_ABNORMAL
%IPPHONE-6-REGISTER_NORMAL
```



The following message indicates that a phone has registered and is not part of the explicit router configuration—ephone configuration has not been created:

```
%IPPHONE-6-REGISTER_NEW: ephone-3:SEP003094C38724 IP:1.4.170.6 Socket:1 DeviceType:Phone has registered.
```

Cisco CallManager Express allows unconfigured phones to register in order to make provisioning of the Cisco CallManager Express system more convenient. By default, phones designated as “new” are not assigned phone lines and cannot make calls.

You can use the following configuration to enable syslogging to a router’s buffer/console or a syslog server:

```
logging console | buffer
logging 172.19.153.129 !!! 172.19.153.129 is the syslog server
```

Call Activity Monitoring—Call History Logging

The Cisco CallManager Express GUI provides call history table information so that a network administrator can monitor the call history information for unknown callers and use this information to disallow calling activities based on select calling patterns. The call history log should be configured to perform forensics and accounting and allow the administrator to track down fraudulent calling patterns.

```
!
dial-control-mib retain-timer 10080
dial-control-mib max-size 500
!
gw-accounting syslog
```

HTTPS for Cisco CallManager Express GUI Management

HTTP over SSL (HTTPS) provides Secure Socket Layer (SSL) version 3.0 support for the HTTP 1.1 server and HTTP 1.1 client within Cisco IOS Software. SSL provides server authentication, encryption, and message integrity to allow secure HTTP communications. SSL also provides HTTP client authentication. This feature is supported in only Cisco IOS software images that support SSL. Specifically, SSL is supported in IPsec 56 and IPsec 3DES images (contains “k8” or “k9” in the image name) in Cisco IOS Software Release 12.2(15)T.

Currently IP phones do not serve as HTTPS clients. If HTTPS is enabled on the Cisco CallManager Express router, IP phones will still attempt to connect to port 80. Because the SSL default port is 443, the phones will not be able to display local directory and system speed-dials.

Workaround for this is to enable both HTTP and HTTPS, as shown in the following example:

```
ip http server
ip http secure-server
ip http secure-port port_number (if https port is changed from default 443)

ip http authentication AAA | TACACS | local
```

Use the following command to generate an RSA usage key pair with a length of 1024 bits or greater:

```
crypto key generate rsa usage 1024
```

If you do not generate an RSA usage key pair manually, an RSA usage key pair with a length of 768 bits will be generated automatically when you connect to the HTTPS server for the first time. These automatically generated RSA keys are not saved to the startup configuration; therefore they will be lost when the device is rebooted unless you save the configuration manually.



You should obtain an X.509 digital certificate with digital signature capabilities for the device from a certification authority (CA). If you do not obtain a digital certificate in advance, the device creates a self-signed digital certificate to authenticate itself.

If you change the device hostname after obtaining a device digital certificate, HTTPS connections to the device fail because the hostname does not match the hostname specified in the digital certificate. Obtain a new device digital certificate using the new hostname to fix this problem.

The **ip http secure-server** command will prevent cleartext passwords across the wires when a Cisco CallManager Express administrator/customer administrator logs into the Cisco CallManager Express GUI. However, communication between the phone and the router will still stay unsecured. A signed digital signature is required in the phoneload and Cisco IOS Software for secure connection.

The following are the suggested best practices for using HTTP's interactive access to the Cisco CallManager Express router:

1. Use **ip http access-class** command to restrict IP packets connecting to Cisco CallManager Express.
2. Use **ip http authentication** with a central TACACS+ or RADIUS server for authentication purposes. Configuring authentication for the HTTP and HTTPS servers adds additional security to communication between clients and the HTTP and HTTPS servers on the device.
3. Do not use the same enable password as an HTTP/Cisco CallManager Express login password. (To prevent a regular user from gaining administrator's right.)

COR for Incoming/Outgoing Calls—To Prevent Toll Fraud

The configuration example below illustrates Class of Restriction (COR). There are two classes of service in the configuration: user and super-user along with various permissions allowed such as local calling, long distance calling, 911 access, and 411 access. In this example, "superuser" has access to everything and "user" has access to all resources with the exception of toll "1900", directory assistance "411", and international calling.

```
dial-peer cor custom
  name 911
  name 1800
  name local-call
  name ld-call
  name 411
  name int-call
  name 1900

dial-peer cor list call911
  member 911
!
dial-peer cor list call1800
  member 1800
!
dial-peer cor list calllocal
  member local-call
!
dial-peer cor list callint
  member int-call
!
```



```
dial-peer cor list callld
  member ld-call
!
dial-peer cor list call411
  member 411
!
dial-peer cor list call1900
  member 1900

dial-peer cor list user
  member 911
  member 1800
  member local-call
  member ld-call
!
dial-peer cor list superuser
  member 911
  member 1800
  member local-call
  member ld-call
  member 411
  member int-call
  member 1900

dial-peer voice 9 pots
  corlist outgoing callld
  destination-pattern 91.....
  port 1/0
  prefix 1
!
dial-peer voice 911 pots
  corlist outgoing call911
  destination-pattern 9911
  port 1/0
  prefix 911
!
dial-peer voice 11 pots
  corlist outgoing callint
  destination-pattern 9011T
  port 2/0
  prefix 011
!
dial-peer voice 732 pots
  corlist outgoing calllocal
  destination-pattern 9732.....
  port 1/0
  prefix 732
!
dial-peer voice 800 pots
  corlist outgoing call1800
  destination-pattern 91800.....
  port 1/0
  prefix 1800
!
dial-peer voice 802 pots
  corlist outgoing call1800
```



```
destination-pattern 91877.....
port 1/0
prefix 1877
!
dial-peer voice 805 pots
corlist outgoing call1800
destination-pattern 91888.....
port 1/0
prefix 1888
!
dial-peer voice 411 pots
corlist outgoing call411
destination-pattern 9411
port 1/0
prefix 411
!
dial-peer voice 806 pots
corlist outgoing call1800
destination-pattern 91866.....
port 1/0
prefix 1866

ephone-dn 1
number 2000
cor incoming user

Ephone-dn 2
number 2001
cor incoming superuser
```

After-hours Blocking to Restrict Outgoing Calling Pattern—Toll Fraud

After-hours blocking can be added to restrict incoming calls after certain hours. After-hours blocking can also be used to restrict calls to numbers/area codes known as fraudulent calling patterns. The configuration example below is used to restrict calls to certain area codes:

```
telephony-service
after-hours block pattern 1 .1242
after-hours block pattern 2 .1264
after-hours block pattern 3 .1268
after-hours block pattern 4 .1246
after-hours block pattern 5 .1441
after-hours block pattern 6 .1284
after-hours block pattern 7 .1345
after-hours block pattern 8 .1767
after-hours block pattern 9 .1809
after-hours block pattern 10 .1473
after-hours block pattern 11 .1876
after-hours block pattern 12 .1664
after-hours block pattern 13 .1787
after-hours block pattern 14 .1869
after-hours block pattern 15 .1758
after-hours block pattern 16 .1900
after-hours block pattern 17 .1976
after-hours block pattern 18 .1868
after-hours block pattern 19 .1649
```



```
after-hours block pattern 20 .1340
after-hours block pattern 21 .1784
after-hours block pattern 22 .1684
after-hours block pattern 23 .1590
after-hours block pattern 24 .1456
after-hours day Sun 00:00 23:59
after-hours day Mon 00:00 23:59
after-hours day Tue 00:00 23:59
after-hours day Wed 00:00 23:59
after-hours day Thu 00:00 23:59
after-hours day Fri 00:00 23:59
after-hours day Sat 00:00 23:59
```

Cisco CallManager Express with Firewall

Cisco CallManager Express with NAT

The Cisco CallManager Express router's LAN interface (Ethernet interface) is used as the source IP address that IP phones and the Cisco CallManager Express router communicate with. The IP addresses of the IP phones are internal addresses to the Cisco CallManager Express router and are in a different segment that is not visible by the external devices or callers. Other devices including Cisco gateways or gatekeeper use the Cisco CallManager Express router's IP address to communicate instead of directly communicating with the IP phones. The Cisco CallManager Express router translates IP addresses back and forth for the traffic to route to the IP phones or outside of the network area. Therefore, no NAT configuration is needed when talking to the IP phones locally attached to the Cisco CallManager Express router. However, in the case when IP phones need to talk to other devices outside the firewall of the Cisco CallManager Express network, NAT needs to be configured on the Cisco CallManager Express router.

Cisco CallManager Express with Cisco IOS Firewall

Overview of Cisco IOS Firewall with Cisco CallManager Express

The Cisco IOS Firewall, running on Cisco IOS Software routers, provides a network-based firewall solution with the functionality of CBAC (Context-based Access Control) or Protocol Inspection, IDS (Intrusion Detection System), Authentication Proxy, and URL Filtering. A firewall provides access control between internal and external networks. It identifies networks as "inside" (private) or "outside" (public) in which packets can get from the inside to the outside, be blocked by default from outside to inside, and packets associated with an inside-originated connection are allowed to pass in. Many firewalls work only if all outside traffic originates from well-known sockets and don't handle asymmetric traffic (i.e., UDP media). Cisco IOS Firewalls allow the packets/traffic to pass through based on their source and destination IP addresses and the configured firewall policy.

The Cisco CallManager Express is a software feature added to the Cisco IOS Software routers that provides call processing for IP phones using Skinny Client Control Protocol (SCCP) for branch/SMB, and managed SP environments. There will be cases in SMB/branch offices, where only one router will be deployed and will be required to provide Internet access, IP Telephony service, and Cisco IOS Firewall functions. Cisco CallManager Express requires that all IP phones attach to the Cisco CallManager Express router locally. Thus SCCP support on the Cisco IOS Firewall is needed for locally generated Skinny traffic.



Problems on Cisco CallManager Express with Cisco IOS Firewall

SCCP is a Cisco proprietary small version of H.323. H.323 traffic can be classified into call signaling, call control, and media communication. H.323 uses Q.931, H.225, and H.245 to set up, manage/control, and tear down calls. When running Cisco CallManager Express with H.323/SCCP protocols, we need to consider how signaling and media streams are affected by the Cisco IOS firewall.

Signaling Stream

An H.323 call requires a TCP connection for H.245 signaling that does not have a well-known port associated with it. The H.245 port is dynamically assigned. Because this port is not known ahead of time and can't be configured when defining firewall policy, the Cisco IOS Firewall will block the H.245 message and the call signaling procedure will fail. When NAT is used in the H.323 signaling path, inside IP address (behind NAT), not known to the rest of the world, will be used as "calling party" information element in the H.225 signaling stream, thus an incoming call (attempts to make an H.225 connection back to that address) will fail.

Media Streams (RTP streams)

RTP streams run on top of UDP and do not have any fixed ports associated with them. Each type of media stream has one or more channels with dynamically assigned source/destination/port numbers, which are not known ahead of time and cannot be preconfigured in the firewall policy. For the media stream to traverse the firewall, the firewall needs to open many UDP ports with source and destination pairs for each call session, thus inducing vulnerabilities to the network behind the firewall.

In short, due to the fact that Cisco IOS Firewall doesn't allow outside traffic to transverse to the inside, VoIP calls (inbound calls) will fail. Furthermore, dynamic RTP/RTCP ports used by the endpoints are not automatically opened and allowed without modification of the security policy. The problems are summarized as follows:

- The firewall only looks at Layer 3 addresses
 - VoIP signaling protocols embed IP addresses at Layer
 - RTP/RTCP works at Layer 5
 - By default, firewalls don't allow outside to inside traffic
 - Cisco IOS firewall feature set and NAT and PIX have application functionality called Application Layer GW (ALG) or fixup Protocol which helps in resolving these issues
- The VoIP application is composed of a dynamic set of protocols
 - SIP, MGCP, H.323, and SCCP for signaling
 - SDP, H.225, and H.245 for capability exchange
 - RTP/RTCP for control and audio media
 - RTP/RTCP both use a dynamic port for the audio media ranging from 16384 to 32767 for all Cisco products

DDTS CSCdx39135 was opened by MCEBU to track and resolve the problem.

Current Status

Currently, Cisco IOS Firewall does not support Skinny inspection, because outgoing packets will be converted to H323 or SIP, there is no need for Skinny inspection. However, for incoming Skinny packets inspection, ACLs can always be used to filter out unwanted packets/traffic. However, Cisco IOS Firewall will add H.323 inspection support for any locally generated traffic as a bug fix for DDTS CSCdx39135, which will be released in 12.3(4th)T/pi4 available in 2004.

Workaround

The following are four alternative solutions to provide security to the Cisco CallManager Express users:

- Running Cisco IOS Firewall on a different router
- Set up maximum number of connections in the Cisco CallManager Express. This is available with the regular H.323 implementation in Cisco IOS Software and can help control the maximum number of H.323 (H225 setup Inbound + Outbound) calls that will be processed (e.g., dial-peer voice 10 voip; max-conn 5—limits to only 5 connections)

- Set up ACLs to accept H.225 connections only from the Gatekeeper (GK) if the GK in the network is using Routed Signaling
- Use H.235 security to authenticate the callers and provide additional call security

URL References

- Cisco IOS Software Security Documentation
http://www.cisco.com/application/pdf/en/guestproducts/ps1835c106/cmigain_0918608011d1e1.pdf
- Cisco IOS Firewall Documentation
- Cisco IOS Software Configuration Guide on Cisco.com
- Cisco IOS Software Command Reference on Cisco.com



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Cisco IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R) ETMG 203246—CM 01.04