

Configurazione e risoluzione dei problemi di SNMPv3 per CER

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazione CER](#)

[Configurazione di Communications Manager](#)

[Configurazione degli switch](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[SNMP Walk versione 3](#)

[Acquisizione pacchetti](#)

[Abilita Logs in CER](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare e risolvere i problemi relativi al protocollo Simple Network Management Protocol (SNMP) versione 3 per Cisco Emergency Responder (CER).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Communications Manager (CUCM)
- Cisco Emergency Responder
- protocollo SNMP

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CUCM 11.5.1.14900-8
- CER: 11.5.4.50000-6
- Interruttore: WS-C350CX-12PC-S

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Emergency Responder utilizza il protocollo SNMP per ottenere informazioni sulle porte di uno switch. Una volta ottenute le informazioni, l'utente amministratore CER può assegnare le porte alle posizioni di risposta di emergenza (ERL, Emergency Response Locations) e consentire a Emergency Responder di identificare i telefoni collegati alle porte e aggiornare le loro assegnazioni ERL.

SNMP V3 fornisce funzioni di sicurezza aggiuntive che coprono l'integrità, l'autenticazione e la crittografia dei messaggi. Inoltre, SNMP V3 controlla l'accesso degli utenti ad aree specifiche della struttura MIB.

Emergency Responder legge solo le informazioni SNMP, non scrive le modifiche alla configurazione dello switch, quindi è necessario configurare solo le stringhe della community di lettura SNMP.

In CER è possibile tenere traccia delle singole porte dello switch in presenza di alcune condizioni:

- CER acquisisce interfacce di switch, porte e VLAN (solo per CAM), informazioni Cisco Discovery Protocol (CDP).
- CER recupera i telefoni registrati da CUCM.
- La tecnologia CER analizza il nome del dispositivo inviato da CUCM e cerca se l'indirizzo MAC appartiene a una porta dello switch. Se il MAC viene trovato, il CER aggiorna il proprio database con la posizione della porta di un telefono.

Configurazione

Quando si configurano le stringhe SNMP per gli switch, è necessario configurare anche le stringhe SNMP per i server Unified Communications Manager. Emergency Responder deve essere in grado di eseguire query SNMP su tutti i server Unified CM in cui sono registrati i telefoni per ottenere le informazioni telefoniche.

CER offre la possibilità di utilizzare modelli, ad esempio 10.0.*.* o 10.1.*.* per i dispositivi con IP che iniziano con 10.0 o 10.1. Se si desidera includere tutti i possibili indirizzi, è possibile utilizzare la subnet *.*.*.*

Configurazione CER

Per configurare SNMPv3 per la traccia telefonica in Cisco Emergency Responder, attenersi alla seguente procedura:

Passaggio 1. Come mostrato nell'immagine, verificare che l'agente principale SNMP, il CER e i servizi Cisco Phone Tracking Engine siano stati avviati.

Cisco Emergency Responder Serviceability
For Cisco Unified Communications Solutions

Navigation **Cisco ER Serviceability**
Logged in as: administrator | Search Documentation | About

Tools ▾ SNMP ▾ System Monitor ▾ System Logs ▾ Help ▾

Control Center

Control Center Services

Start Stop Restart Refresh

	Service Name	Status
<input type="radio"/>	A Cisco DB Replicator	Started
<input type="radio"/>	CER Provider	Started
<input type="radio"/>	Cisco Audit Log Agent	Started
<input type="radio"/>	Cisco CDP	Started
<input type="radio"/>	Cisco CDP Agent	Started
<input type="radio"/>	Cisco Certificate Expiry Monitor	Started
<input type="radio"/>	Cisco DRF Local	Started
<input type="radio"/>	Cisco DRF Master	Started
<input type="radio"/>	Cisco Emergency Responder	Started
<input type="radio"/>	Cisco IDS	Started
<input type="radio"/>	Cisco Phone Tracking Engine	Started
<input type="radio"/>	Cisco Tomcat	Started
<input type="radio"/>	Host Resources Agent	Started
<input type="radio"/>	MIB2 Agent	Started
<input type="radio"/>	Platform Administrative Web Service	Started
<input type="radio"/>	SNMP Master Agent	Started
<input type="radio"/>	System Application Agent	Started

Start Stop Restart Refresh

Passaggio 2. Per configurare le impostazioni SNMP utilizzate per gli switch e i nodi CUCM, selezionare **CER Admin > Phone tracking > SNMPv2/v3**. È possibile configurare il nome utente SNMP, l'autenticazione e le informazioni sulla privacy come mostrato nell'immagine.

SNMPv3 Settings

Status
Please modify information for the selected SNMPv3 User

Modify SNMPv3 User Details

User Information
IP Address/Host Name * **10.1.61.10**
User Name *

Authentication Information
 Authentication Required *
Password Reenter Password Protocol MD5 SHA

Privacy Information
 Privacy Required *
Password Reenter Password Protocol DES AES128

Other Information
Timeout (in seconds) *
Maximum Retry Attempts *

SNMPv3 Settings

IP Address/Host Name	User Name	Authentication	Privacy	Timeout (in seconds)	Maximum Retry Attempts	Delete
10.1.61.10	cersnmpv3	MD5	DES	10	2	

Nell'esempio, 10.1.61.10 è l'indirizzo IP dello switch e 10.1.61.158 è l'indirizzo IP del Call Manager. La configurazione di SNMPv3 in CER è come mostrato nell'immagine.

SNMPv3 Settings

IP Address/Host Name	User Name	Authentication	Privacy	Timeout (in seconds)	Maximum Retry Attempts	Delete
10.1.61.10	cersnmpv3	MD5	DES	10	2	
10.1.61.158	cucmsnmpv3	MD5	DES	10	2	

Nota: È possibile specificare *.*.* o altri caratteri jolly/intervalli nell'indirizzo IP/nome host per includere più server. In caso contrario, è possibile configurare indirizzi IP specifici.

Passaggio 3. Per configurare lo switch IP sugli switch LAN, selezionare **CER Admin > Phone tracking > LAN switch detail > Add LAN Switch** come mostrato nell'immagine.

LAN Switch Details
Export

Status

Please enter any change for the current LAN Switch

LAN Switch Details

Switch Host Name / IP Address * **10.1.61.10**

Description

Enable CAM based Phone Tracking

Use port description as port location

Use SNMPV3 for Discovery

LAN Switches

Switch Host Name / IP Address	Edit	Delete
10.1.61.10		

Configurazione di Communications Manager

In CUCM, esistono due livelli di connettività SNMP: l'agente principale SNMP e il servizio SNMP di Cisco CallManager. È necessario abilitare entrambi i servizi in tutti i nodi con il servizio CallManager attivato. Per configurare il server Cisco Unified Communications Manager, attenersi alla seguente procedura.

Passaggio 1. Per controllare lo stato del servizio SNMP di Cisco CallManager, selezionare **Cisco Unified Serviceability > Tools > Feature Services**. Selezionare il server e verificare che lo stato del servizio SNMP Cisco CallManager sia attivato, come mostrato nell'immagine.

Performance and Monitoring Services					
Service Name	Status	Activation Status	Start Time	Up Time	
<input type="checkbox"/> Cisco Serviceability Reporter	Started	Activated	Mon Jul 1 18:11:34 2019	11 days 12:12:43	
<input type="checkbox"/> Cisco CallManager V3 Service	Started	Activated	Mon Jul 1 18:11:36 2019	11 days 12:12:41	

Passaggio 2. Per controllare lo stato dell'agente principale SNMP, selezionare **Cisco Unified Serviceability > Tools > Network services** (Servizi di rete unificati Cisco > Strumenti > Servizi di rete). Selezionare il server e verificare che il servizio Agente principale SNMP venga eseguito come mostrato nell'immagine.

Platform Services				
Service Name	Status	Start Time	Up Time	
<input type="checkbox"/> Platform Administrative Web Service	Running	Mon Jul 1 10:18:49 2019	11 days 12:11:17	
<input type="checkbox"/> A Cisco DB	Running	Mon Jul 1 10:19:17 2019	11 days 12:19:49	
<input type="checkbox"/> A Cisco DB Replicator	Running	Mon Jul 1 10:19:18 2019	11 days 12:19:48	
<input type="checkbox"/> V3 Master Agent	Running	Mon Jul 1 10:19:23 2019	11 days 12:19:43	

Passaggio 3. Per configurare il protocollo SNMPv3 in CUCM, selezionare **Cisco Unified Serviceability > SNMP > V3 > User**. Selezionare il server e configurare Nome utente, Informazioni di autenticazione e Informazioni sulla privacy come illustrato nell'immagine.

The screenshot displays the 'SNMP User Configuration' page in the Cisco Unified Serviceability interface. At the top, there is a navigation bar with 'Cisco Unified Serviceability' and 'For Cisco Unified Communications Solutions'. Below this is a menu bar with options like 'Alarm', 'Trace', 'Tools', 'Snmp', 'CallHome', and 'Help'. The main content area is titled 'SNMP User Configuration' and includes a toolbar with 'Save', 'Clear All', and 'Cancel' buttons. The configuration is organized into several sections:

- Status:** A field showing 'Status : Ready'.
- Server:** A dropdown menu currently set to '10.1.61.158--CUCM Voice/Video'.
- User Information:** A text field for 'User Name*' containing 'cucmsnmpv3'.
- Authentication Information:** Includes a checked 'Authentication Required' checkbox, password fields for 'Password' and 'Reenter Password', and a 'Protocol' selection with 'MDS' selected and 'SHA' unselected.
- Privacy Information:** Includes a checked 'Privacy Required' checkbox, password fields for 'Password' and 'Reenter Password', and a 'Protocol' selection with 'DES' selected and 'AES128' unselected.
- Host IP Addresses Information:** Features two radio buttons: 'Accept SNMP Packets from any host' (selected) and 'Accept SNMP Packets only from these hosts'. The latter has a 'Host IP Address' input field with an 'Insert' button and a 'Host IP Addresses' list box with a 'Remove' button.
- Access Privileges:** A dropdown menu for 'Access Privileges*' set to 'ReadOnly'. A note below states: 'Notify access privilege is required in order to configure Notification Destinations.'

Configurazione degli switch

Per tenere traccia dei telefoni tramite switchport, la configurazione SNMP nello switch deve corrispondere alla configurazione nel server CER. Utilizzare questi comandi per configurare lo switch.

gruppo snmp-server <NomeGruppo> autenticazione v3 lettura <Nome_visualizzazione>

snmp-server user <Utente> <NomeGruppo> v3 auth [sha/md5] <password_autenticazione> priv [DES/AES128] <password_privacy>

visualizzazione snmp-server <Name_of_View> iso inclusa

Esempio:

```
Switch(config)#snmp-server group Grouptest v3 auth read Viewtest
Switch(config)#snmp-server user cersnmpv3 Grouptest v3 auth md5 cisco123 priv des cisco123
Switch(config)#snmp-server view Viewtest iso included
```

Per verificare la configurazione, usare il comando **show run | s snmp** come mostrato nell'esempio.

```
Switch#show run | s snmp
snmp-server group Grouptest v3 auth read Viewtest
```

snmp-server view Viewtest iso included

Verifica

Ogni CUCM che esegue il servizio Cisco CallManager deve eseguire anche i servizi SNMP. Se la configurazione di tutti i nodi è corretta, è necessario visualizzare tutti i nodi di CallManager quando si fa clic sul collegamento ipertestuale **Cisco Unified Communications Manager List** e i telefoni devono essere registrati da switchport.

Passaggio 1. Per verificare l'elenco dei nodi CUCM, selezionare **CER Admin > Phone tracking > Cisco Unified Communications Manager**. Fare clic sul collegamento ipertestuale come illustrato nell'immagine.

The screenshot displays the Cisco Emergency Responder Administration web interface. The main configuration page is titled "Cisco Unified Communications Manager Clusters" and includes sections for "Modify Cisco Unified Communications Manager Cluster", "Secure Connection Parameters", "AXL Settings", and "SNMP Settings".

Key configuration fields are highlighted with red boxes:

- Modify Cisco Unified Communications Manager Cluster:**
 - Cisco Unified Communications Manager * (CTI Manager *): 10.1.61.158
 - CTI Manager User Name *: CER
 - CTI Manager Password *: [Redacted]
 - BackUp CTI Manager 1: 10.1.61.159
 - BackUp CTI Manager 2: [Redacted]
 - Telephony Port Begin Address: 500
 - Number of Telephony Ports: 2
- AXL Settings:**
 - AXL Username: administrator
 - AXL Password: [Redacted]
 - AXL Port Number: 8443

On the right side, a browser window titled "Cisco Emergency Responder Administration - Mozilla Firefox" is open, displaying the "List of Cisco Unified Communications Managers" page. This page shows a table with two entries, both of which are highlighted with red boxes:

Cisco Unified Communications Manager	
[Icon]	10.1.61.158
[Icon]	10.1.61.159

Passaggio 2. Per verificare che i telefoni siano tracciati da switchport, selezionare **CER Admin > ERL Membership > Switchport > Filter >** e fare clic su **Find**. L'indirizzo IP dello switch e i telefoni tracciati devono essere elencati come mostrato nell'immagine.

Switch IP Address	<input type="checkbox"/>	ERL Name	Switch IP Address	IFname	Location	Phone Extension	Phone IP Address	Phone Typ
<input type="checkbox"/> 10.1.61.10	<input type="checkbox"/>		10.1.61.10	Gi0/1	View			
	<input type="checkbox"/>		10.1.61.10	Gi0/2	View			
	<input type="checkbox"/>		10.1.61.10	Gi0/3	View			
	<input type="checkbox"/>		10.1.61.10	Gi0/4	View			
	<input type="checkbox"/>		10.1.61.10	Gi0/5	View	100	10.1.61.24	Cisco 9971
	<input type="checkbox"/>		10.1.61.10	Gi0/6	View			
	<input type="checkbox"/>		10.1.61.10	Gi0/7	View			
	<input type="checkbox"/>		10.1.61.10	Gi0/8	View			
	<input type="checkbox"/>	ERL_MEX	10.1.61.10	Gi0/9	View	103	10.1.61.12	Cisco 8945
	<input type="checkbox"/>		10.1.61.10	Gi0/10	View			
	<input type="checkbox"/>	ERL_MEX	10.1.61.10	Gi0/11	View	107	10.1.61.16	Cisco 8945
	<input type="checkbox"/>		10.1.61.10	Gi0/12	View			
	<input type="checkbox"/>		10.1.61.10	Gi0/13	View			
	<input type="checkbox"/>		10.1.61.10	Gi0/14	View			

Risoluzione dei problemi

SNMP Walk versione 3

Per verificare che sia CUCM che lo switch rispondano a CER, usare il comando **SNMP walk v3**. L'identificatore di oggetto (Object Identifier, OID) consigliato è 1.3.6.1.2.1.1.2.0, come mostrato nell'esempio.

Esempio di percorso SNMP versione 3 da CER a CUCM:

```
admin:utils snmp walk 3
Enter the user name:: cucmsnmpv3
Enter the authentication protocol [SHA]::
Enter the authentication protocol [SHA]:: MD5
Enter the authentication protocol pass phrase:: *****
Enter the privacy protocol [AES128]:: DES
Enter the privacy protocol pass phrase:: *****
Enter the ip address of the Server, use 127.0.0.1 for localhost.Note that you need to provide
the IP address, not the hostname.:: 10.1.61.158
The Object ID (OID):: 1.3.6.1.2.1.1.2.0
Enter parameter as "file" to log the output to a file. [nofile]::
This command may temporarily impact CPU performance.
Continue (y/n)?y
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.1348
```

Esempio di percorso SNMP versione 3 da CER allo switch:

```
admin:utils snmp walk 3
Enter the user name:: cersnmpv3
Enter the authentication protocol [SHA]:: MD5
Enter the authentication protocol pass phrase:: *****
Enter the privacy protocol [AES128]:: DES
Enter the privacy protocol pass phrase:: *****
Enter the ip address of the Server, use 127.0.0.1 for localhost.Note that you need to provide
the IP address, not the hostname.:: 10.1.61.10
The Object ID (OID):: 1.3.6.1.2.1.1.2.0
Enter parameter as "file" to log the output to a file. [nofile]::
This command may temporarily impact CPU performance.
Continue (y/n)?y
```


SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.2134

Esempio di percorso SNMP v3 con accesso root in CER:

```
snmpwalk -v3 -u <User> -l authPriv -A <auth_password> -a [MD5/SHA] -x [DES/AES128] -X  
<Priv_password> IP_Device <OID>
```

Dove:

-u: è l'utente snmp v3.

-l : è la modalità di autenticazione [noAuthNoPriv|authNoPriv|authPriv].

-A : è la password di autenticazione.

-a : è il protocollo di autenticazione [MD5|SHA].

-x : è il protocollo di privacy [DES/AES128].

-X : è la password del protocollo di privacy.

L'esempio dell'output è come mostrato nell'immagine.



Se viene visualizzato il seguente messaggio di errore "*Errore durante la generazione di una chiave (Ku) dalla passphrase per la privacy fornita*", provare con la sintassi seguente:

```
snmpwalk -v3 -l authPriv -u <User> -a [MD5/SHA] -A <auth_password> -x [DES/AES128] -X  
<Priv_password> IP_Device <OID>
```

Verificare che l'OID restituito sia uno dei dispositivi supportati nelle note di rilascio CER della versione in uso.

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cer/11_5_1/english/release_notes/guide/CE_R_BK_C838747F_00_cisco-emergency-responder-version-1151.html#CER0_CN_SE55891C_00

Alcuni degli OID inviati da CER allo switch sono:

- 1.3.6.1.2.1.1.1.0 - sysDescr
- 1.3.6.1.2.1.1.2.0 - sysObjectID
- 1.3.6.1.2.1.1.5.0 - sysName
- 1.3.6.1.2.1.1.3.0 - sysUpTime

Alcuni degli OID inviati da CER al CUCM sono:

- 1.3.6.1.4.1.9.9.156.1.1.2.1.7 - ccmEntry/ccmInetAddress
- 1.3.6.1.2.1.1.2.0 - sysObjectID
- 1.3.6.1.4.1.9.9.156.1.1.2.1.2 - ccmName

Acquisizione pacchetti

È molto utile acquisire un pacchetto per isolare i problemi con il tracciamento del telefono. Questi sono i passaggi per ottenere un'acquisizione del pacchetto in CER.

Passaggio 1. Avviare l'acquisizione di un pacchetto tramite CLI con il comando **utils network capture eth0 file ExampleName size all count 10000**, dove ExampleName è il nome dell'acquisizione del pacchetto.

Passaggio 2. Replicare il problema (effettuare la chiamata 911, l'accesso SNMP, l'aggiornamento

della traccia telefonica, ecc.).

Passaggio 3. Arrestare l'acquisizione del pacchetto con **Ctrl+C**

Passaggio 4. Confermare che l'acquisizione del pacchetto è stata salvata in CER con il comando **file list activelog platform/cli/***

Passaggio 5. Recuperare l'acquisizione del pacchetto con il comando **file get activelog platform/cli/ExampleName.cap** (per esportare il file è necessario un server SFTP).

Abilita Logs in CER

Per abilitare i log in Emergency Responder Server, selezionare **CER Admin > System > Server Settings** (Amministratore CER > Sistema > Impostazioni server). Se si attivano tutte le caselle di controllo, non verrà generato alcun impatto sul servizio del server.

Server Settings For CERServerGroup

Status

Ready

Select Server



[Publisher \(primary\)](#)



[Subscriber\(standby\)](#)

Modify Server Settings

Server Name *

Host Name

mycerpubvictogut

Debug Package List

- | | |
|---|--|
| <input checked="" type="checkbox"/> CER_DATABASE | <input checked="" type="checkbox"/> CER_SYSADMIN |
| <input checked="" type="checkbox"/> CER_REMOTEUPDATE | <input checked="" type="checkbox"/> CER_TELEPHONY |
| <input checked="" type="checkbox"/> CER_PHONETRACKINGENGINE | <input checked="" type="checkbox"/> CER_AGGREGATOR |
| <input checked="" type="checkbox"/> CER_ONSITEALERT | <input checked="" type="checkbox"/> CER_GROUP |
| <input checked="" type="checkbox"/> CER_CALLENGINE | <input checked="" type="checkbox"/> CER_CLUSTER |
| <input checked="" type="checkbox"/> CER_PROVIDER | <input checked="" type="checkbox"/> CER_ACCESSPOINT |
| <input checked="" type="checkbox"/> CER_AUDIT | <input checked="" type="checkbox"/> CER_CREDENTIALPOLICY |

Trace Package List

- | | |
|---|--|
| <input checked="" type="checkbox"/> CER_DATABASE | <input checked="" type="checkbox"/> CER_SYSADMIN |
| <input checked="" type="checkbox"/> CER_REMOTEUPDATE | <input checked="" type="checkbox"/> CER_TELEPHONY |
| <input checked="" type="checkbox"/> CER_PHONETRACKINGENGINE | <input checked="" type="checkbox"/> CER_AGGREGATOR |
| <input checked="" type="checkbox"/> CER_ONSITEALERT | <input checked="" type="checkbox"/> CER_GROUP |
| <input checked="" type="checkbox"/> CER_CALLENGINE | <input checked="" type="checkbox"/> CER_CLUSTER |
| <input checked="" type="checkbox"/> CER_PROVIDER | <input checked="" type="checkbox"/> CER_ACCESSPOINT |
| <input checked="" type="checkbox"/> CER_AUDIT | <input checked="" type="checkbox"/> CER_CREDENTIALPOLICY |

Per risolvere i problemi relativi a uno switch non presente nelle porte dello switch (**CER > Admin > ERL membership > Switch Ports**), effettuare le seguenti operazioni:

1. Verificare la configurazione in **Admin > Phone tracking > LAN Switch details** (Amministrazione > Phone tracking > Dettagli switch LAN).
2. Verificare la configurazione in **Admin > Phone tracking > SNMP v2 / v3**.
3. Verificare la casella di controllo **Abilita registrazione telefono basata su CAM**. Se si tratta di uno switch non Cisco o il CDP è disabilitato, selezionare la casella di controllo Enable CAM

based Phone Tracking (Abilita registrazione telefono basata su CAM).

4. Verificare la configurazione SNMP sullo switch.
5. Raccogliere i registri di verifica telefonica.

Se vengono visualizzate le porte dello switch ma i telefoni no, è necessario procedere come segue:

1. Configurazione SNMP su CER e Communications Manager.
2. Confermare il nome IP/host in Cisco Unified Communications Manager.
3. Verificare che i telefoni non mostrati appartengano a uno specifico responsabile delle comunicazioni.
4. Verificare che entrambi i servizi SNMP (Agente principale SNMP / Servizio SNMP CallManager) siano avviati su tutti i nodi CallManager nel cluster.
5. Confermare la raggiungibilità di CUCM tramite l'itinerario SNMP.
6. Raccogliere i registri di verifica telefonica.

Esempio 1 di registri di tracciabilità telefonica CER:

```
305: Jun 30 12:05:17.385 EDT %CER-CER_PHONETRACKINGENGINE-7-DEBUG:SnmpSocketReader-47637:SnmpPrivacyParam encryptDESPrivParam Exception thrown while encrypting DES parameters :Cannot find any provider supporting DES/CBC/NoPadding
```

Possibile motivo: Configurazione errata delle informazioni sulla privacy di SNMPv3.

Esempio 2 di registri di tracciabilità telefonica CER:

```
Snmp exception while reading ccmVersion on <IP address CCM Node>
```

Possibile motivo: Il servizio SNMP di Cisco CallManager è disattivato in uno dei nodi CUCM.

Informazioni correlate

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cer/11_5_1/english/administration/guide/CE_R_BK_R00ED2C0_00_cisco-emergency-responder-administration-guide-1151/CER_BK_R00ED2C0_00_cisco-emergency-responder-administration-guide-1151_appendix_01101.html#CER0_RF_S51098E7_00

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cer/10_0_1/english/administration/guide/CE_R0_BK_CA66317A_00_cisco-emergency-responder-administration-10_0/CER0_BK_CA66317A_00_cisco-emergency-responder-administration-10_0_chapter_01100.pdf