

Configuration et dépannage de SNMPv3 pour CER

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Configuration CER](#)

[Configuration de Communications Manager](#)

[Configuration du commutateur](#)

[Vérification](#)

[Dépannage](#)

[SNMP Walk Version 3](#)

[Capture de paquets](#)

[Activer les journaux dans CER](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer et dépanner le protocole SNMP (Simple Network Management Protocol) version 3 pour Cisco Emergency Responder (CER).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de communications unifiées de Cisco (version CUCM)
- Intervenant d'urgence Cisco
- protocole SNMP

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CUCM: 11.5.1.14900-8
- CER : 11.5.4.50000-6
- Commutateur : WS-C3560CX-12PC-S

The information in this document was created from the devices in a specific lab environment. Tous les dispositifs utilisés dans ce document ont démarré par une configuration effacée (par défaut). If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Emergency Responder utilise SNMP pour obtenir des informations sur les ports d'un commutateur. Une fois les informations obtenues, l'utilisateur de l'administrateur d'URCE peut affecter les ports aux Emplacements d'intervention d'urgence (ERL), de sorte que Emergency Responder puisse identifier les téléphones qui sont connectés aux ports et mettre à jour leurs affectations d'ERL.

SNMP V3 fournit des fonctions de sécurité supplémentaires qui couvrent l'intégrité, l'authentification et le chiffrement des messages. En outre, SNMP V3 contrôle l'accès utilisateur à des zones spécifiques de l'arborescence MIB.

Emergency Responder lit uniquement les informations SNMP, il n'écrit pas les modifications apportées à la configuration du commutateur, donc vous n'avez qu'à configurer les chaînes de communauté de lecture SNMP.

Certaines conditions doivent être suivies par les ports de commutation dans CER :

- CER récupère les interfaces de commutation, les ports et les VLAN (uniquement pour CAM), ainsi que les informations du protocole CDP (Cisco Discovery Protocol).
- CER récupère les téléphones enregistrés à partir de CUCM.
- CER examine le nom de périphérique envoyé à partir de CUCM et recherche si MAC appartient à un port de commutateur. Si l'adresse MAC est trouvée, CER met à jour sa base de données avec l'emplacement du port d'un téléphone.

Configuration

Lorsque vous configurez les chaînes SNMP pour vos commutateurs, vous devez également configurer les chaînes SNMP pour vos serveurs Unified Communications Manager. Emergency Responder doit être en mesure d'effectuer des requêtes SNMP de tous les serveurs Unified CM sur lesquels les téléphones sont enregistrés afin d'obtenir les informations du téléphone.

CER offre la possibilité d'utiliser des modèles, par exemple 10.0.*.* ou 10.1.*.* pour les périphériques dont les adresses IP commencent par 10.0 ou 10.1. Si vous voulez inclure toutes les adresses possibles, vous pouvez utiliser le sous-réseau *.*.*.*.

Configuration CER

Afin de configurer SNMPv3 pour le suivi téléphonique dans Cisco Emergency Responder, procédez comme suit :

Étape 1. Comme l'illustre l'image, assurez-vous que les services SNMP Master Agent, CER et Cisco Phone Tracking Engine sont démarrés.

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

Étape 2. Afin de configurer les paramètres SNMP utilisés pour les commutateurs et les noeuds CUCM, accédez à **CER Admin > Phone Tracking > SNMPv2/v3**. Vous pouvez configurer le nom d'utilisateur SNMP, l'authentification et les informations de confidentialité comme indiqué dans l'image.

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 * cersnmpv3

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) * 10
Maximum Retry Attempts * 2

Update Cancel Changes

SNMPv3 Settings

Add New

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

Dans cet exemple, 10.1.61.10 est l'adresse IP du commutateur et 10.1.61.158 l'adresse IP du Call Manager. La configuration SNMPv3 dans CER est celle illustrée dans l'image.

SNMPv3 Settings

Add New

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	

Note: Vous pouvez spécifier *.*.* ou d'autres caractères génériques/plages dans l'adresse IP/nom d'hôte afin d'inclure plusieurs serveurs, sinon, vous pouvez configurer des adresses IP spécifiques.

Étape 3. Afin de configurer l'adresse IP du commutateur sur les commutateurs LAN, accédez à CER Admin > Phone tracking > LAN switch detail > Add LAN Switch comme indiqué dans l'image.

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		

Configuration de Communications Manager

Dans CUCM, il existe deux niveaux de connectivité SNMP : SNMP Master Agent et Cisco CallManager SNMP Service. Vous devez activer les deux services dans tous ces noeuds avec le service CallManager activé. Pour configurer votre serveur Cisco Unified Communications Manager, procédez comme suit.

Étape 1. Afin de vérifier l'état du service SNMP de Cisco CallManager, accédez à **Cisco Unified Serviceability > Tools > Feature services**. Sélectionnez le serveur et assurez-vous que l'état du service SNMP de Cisco CallManager est activé comme indiqué dans l'image.

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 SNMP Service	Started	Activated	Mon Jul 1 18:11:35 2019	11 days 12:12:41	

Étape 2. Afin de vérifier l'état de SNMP Master Agent, accédez à **Cisco Unified Serviceability > Tools > Network services**. Sélectionnez le serveur et vérifiez que le service SNMP Master Agent s'exécute comme indiqué dans l'image.

Platform Services				
Service Name	Status	Start Time	Up Time	
<input type="checkbox"/> Platform Administrative Web Service	Running	Mon Jul 1 10:38:49 2019	11 days 12:11:17	
<input type="checkbox"/> A Cisco DB	Running	Mon Jul 1 10:30:17 2019	11 days 12:19:49	
<input type="checkbox"/> A Cisco DB Replicator	Running	Mon Jul 1 10:30:18 2019	11 days 12:19:48	
<input type="checkbox"/> SNMP Master Agent	Running	Mon Jul 1 10:30:23 2019	11 days 12:19:43	

Étape 3. Afin de configurer SNMPv3 dans CUCM, accédez à **Cisco Unified Serviceability > SNMP > V3 > User**. Sélectionnez le serveur et configurez le nom d'utilisateur, les informations d'authentification et les informations de confidentialité comme indiqué dans l'image.

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, a menu bar includes 'Alarm', 'Trace', 'Tools', 'Snmp', 'CallHome', and 'Help'. The main content area is titled 'SNMP User Configuration' and contains 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.'

Configuration du commutateur

Afin de suivre les téléphones par port de commutation, la configuration SNMP dans le commutateur doit correspondre à la configuration dans le serveur CER. Utilisez ces commandes pour configurer le commutateur.

```
snmp-server group <GroupName> v3 auth read <Name_of_View>
```

```
snmp-server user <User> <GroupName> v3 auth [sha/md5] <authentication_password> priv [DES/AES128] <privacy_password>
```

```
snmp-server view <Name_of_View> iso inclus
```

Exemple :

```
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
```

Afin de vérifier votre configuration, utilisez la commande **show run | s snmp** comme indiqué dans l'exemple.

```
Switch#show run | s snmp
```

```
snmp-server group Groupptest v3 auth read Viewtest
snmp-server view Viewtest iso included
```

Vérification

Chaque CUCM qui exécute le service Cisco CallManager doit également exécuter des services SNMP. Si tout est configuré correctement, vous devez voir tous les noeuds CallManager lorsque vous cliquez sur le lien hypertexte **Cisco Unified Communications Manager List** et que les téléphones doivent être suivis par port de commutation.

Étape 1. Afin de vérifier la liste des noeuds CUCM, accédez à **CER Admin > Phone tracking > Cisco Unified Communications Manager**. Cliquez sur le lien hypertexte tel qu'illustré dans l'image.

The screenshot displays the 'Cisco Unified Communications Manager Clusters' configuration page. The 'Modify Cisco Unified Communications Manager Cluster' section is highlighted with a red box, showing the following configuration:

Cisco Unified Communications Manager *	10.1.61.158	Cisco Unified Communications Managers List
CTI Manager *	10.1.61.158	
CTI Manager User Name *	CER	
CTI Manager Password *	*****	
Backup CTI Manager 1	10.1.61.159	
Backup CTI Manager 2		
Telephony Port Begin Address	500	
Number of Telephony Ports	2	

The 'AXL Settings' section is also highlighted with a red box, showing:

AXL Username	administrator
AXL Password	*****
AXL Port Number	8443

On the right, a browser window titled 'Cisco Emergency Responder Administration - Mozilla Firefox' shows the 'List of Cisco Unified Communications Managers' page. This page lists two managers, both highlighted with a red box:

Cisco Unified Communications Manager	
	10.1.61.159
	10.1.61.158

Étape 2. Afin de confirmer que les téléphones sont suivis par switchport, accédez à **CER Admin > ERL Membership > Switchport > Filter >** et cliquez sur **Find**. L'adresse IP du commutateur et les téléphones suivis doivent être répertoriés comme indiqué dans l'image.

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			

Dépannage

SNMP Walk Version 3

Afin de confirmer que CUCM et le commutateur répondent à CER, vous pouvez utiliser la commande **SNMP walk v3**. L'identificateur d'objet recommandé (OID) est 1.3.6.1.2.1.1.2.0 comme indiqué dans l'exemple.

Exemple de marche SNMP version 3 de CER à 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
```

Exemple de la version 3 de marche SNMP de CER au commutateur :

```
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

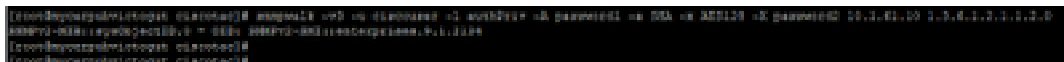
Exemple de marche SNMP v3 avec accès racine dans CER :

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

Where:

- u : est l'utilisateur snmp v3.
- l : est le mode d'authentification [noAuthNoPriv|authNoPriv|authPriv].
- A : est le mot de passe d'authentification.
- a : est le protocole d'authentification [MD5|SHA].
- x : est le protocole de confidentialité [DES/AES128].
- X : est le mot de passe du protocole de confidentialité.

L'exemple de la sortie est comme illustré dans l'image.



Si vous recevez l'erreur suivante "*Erreur lors de la génération d'une clé (Ku) à partir de la phrase de passe de confidentialité fournie*", essayez avec la syntaxe suivante :

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

Vérifiez que l'OID retourné est l'un des périphériques pris en charge dans les notes de version du CER de votre version.

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

Voici quelques-uns des OID que CER envoie au commutateur :

- 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

Voici quelques-uns des OID que le CER envoie au CUCM :

- 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

Capture de paquets

Il est très utile d'obtenir une capture de paquets afin d'isoler les problèmes avec le suivi téléphonique, voici les étapes pour obtenir une capture de paquets dans CER.

Étape 1. Démarrez une capture de paquets via l'interface de ligne de commande à l'aide de la commande **utils network capture eth0 file ExampleName size all count 10000**, où ExampleName est le nom de votre capture de paquets.

Étape 2. Répliquer le problème (passer l'appel 911, marche SNMP, mise à jour du suivi

téléphonique, etc.)

Étape 3. Arrêter la capture de paquets avec **Ctrl+C**

Étape 4. Confirmer que la capture de paquets a été enregistrée dans CER avec la **liste de fichiers de commandes `activelog platform/cli/*`**

Étape 5. Récupérez la capture de paquets avec le **fichier de commande `get activelog platform/cli/ExampleName.cap`** (un serveur SFTP est nécessaire pour exporter le fichier).

Activer les journaux dans CER

Afin d'activer les journaux dans Emergency Responder Server, accédez à **CER Admin > System > Server Settings**. Activez toutes les cases à cocher, cela ne génère aucun impact sur le service sur le serveur.

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 |

Afin de dépanner un commutateur qui n'apparaît pas dans les ports de commutation (**CER > Admin > ERL Membership > Switch Ports**), ces étapes doivent être effectuées :

1. Vérifiez la configuration dans **Admin > Phone tracking > LAN Switch details**.
2. Vérifiez la configuration dans **Admin > Phone tracking > SNMP v2 / v3**.
3. Cochez la case **Activer le suivi téléphonique basé sur CAM**. S'il s'agit d'un commutateur non Cisco ou si le protocole CDP est désactivé, cochez la case **Activer le suivi téléphonique basé sur CAM**.

4. Vérifiez la configuration SNMP sur le commutateur.
5. Collecter les journaux de suivi téléphonique.

Si les ports de commutateur s'affichent mais que les téléphones ne s'affichent pas, ces étapes doivent être effectuées :

1. Configuration SNMP sur CER et Communications Manager.
2. Confirmez le nom IP/hôte sous Cisco Unified Communications Manager.
3. Confirmez si les téléphones non affichés appartiennent à un gestionnaire de communications spécifique.
4. Vérifiez que les deux services SNMP (SNMP Master Agent / CallManager SNMP Service) sont démarrés sur tous les noeuds CallManager du cluster.
5. Confirmez l'accessibilité CUCM via SNMP walk.
6. Collecter les journaux de suivi téléphonique.

Exemple 1 des journaux de suivi des téléphones 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
```

Raison possible : Configuration incorrecte sur les informations de confidentialité SNMPv3.

Exemple 2 des journaux de suivi des téléphones CER :

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

Raison possible : Le service SNMP de Cisco CallManager est désactivé dans l'un des noeuds CUCM.

Informations connexes

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