

Configure and Troubleshoot SNMPv3 for CER

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[CER Configuration](#)

[Communications Manager Configuration](#)

[Switch Configuration](#)

[Verify](#)

[Troubleshoot](#)

[SNMP Walk Version 3](#)

[Packet Capture](#)

[Enable the Logs in CER](#)

[Related Information](#)

Introduction

This document describes how to configure and troubleshoot the Simple Network Management Protocol (SNMP) version 3 for Cisco Emergency Responder (CER).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communications Manager (CUCM)
- Cisco Emergency responder
- SNMP protocol

Components Used

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

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

The information in this document was created from the devices in a specific lab environment. All the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Emergency Responder uses SNMP to obtain information about the ports on a switch. Once the information is obtained, CER admin user can assign the ports to Emergency Response Locations (ERL), and so that Emergency Responder can identify phones that are attached to the ports and update their ERL assignments.

SNMP V3 provides additional security features that cover message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree.

Emergency Responder only reads SNMP information, it does not write changes to the switch configuration, so you only have to configure the SNMP read community strings.

There are some conditions to track by switch ports in CER:

- CER fetches switch interfaces, ports and VLANs (just for CAM), Cisco Discovery Protocol (CDP) information.
- CER fetches registered phones from CUCM.
- CER looks at device name sent from CUCM and searches if MAC belongs to a switch port. If the MAC is found, CER updates its database with port location of a phone.

Configure

When you configure the SNMP strings for your switches, you must also configure the SNMP strings for your Unified Communications Manager servers. Emergency Responder must be able to make SNMP queries of all Unified CM servers where the phones are registered to in order to get the phone information.

CER offers the possibility to use patterns, for example 10.0.*.* or 10.1.*.* for those devices with IPs that begin with 10.0 or 10.1. If you want to include all the possible addresses, you can use the subnet *.*.*.*

CER Configuration

In order to configure SNMPv3 for phone tracking in Cisco Emergency Responder follow these steps:

Step 1. As shown in the image, ensure that the SNMP Master Agent, the CER, and the Cisco Phone Tracking Engine services are started.

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

Step 2. In order to configure the SNMP settings used for switches and CUCM nodes, navigate to **CER Admin > Phone tracking > SNMPv2/v3**. You can configure the SNMP username, authentication, and privacy information as shown in the 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 *

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	

In this example, 10.1.61.10 is the IP of the switch and 10.1.61.158 is the IP of the Call Manager. The SNMPv3 configuration in CER is as shown in the image.

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	

Note: You can specify *.*.* or other wildcards/ranges in the **IP Address/Hostname** in order to include more than one server, otherwise, you can configure specific IP Addresses.

Step 3. In order to configure the switch IP on LAN switches, navigate to **CER Admin > Phone tracking > LAN switch detail > Add LAN Switch** as shown in the 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		

Communications Manager Configuration

In CUCM, there are two levels of SNMP connectivity, the SNMP Master Agent and Cisco CallManager SNMP Service. You must enable both services in all those nodes with CallManager service activated. In order to configure your Cisco Unified Communications Manager server follow these steps.

Step 1. In order to check the status of the Cisco CallManager SNMP Service, navigate to **Cisco Unified Serviceability > Tools > Feature services**. Select the server and ensure that the status of the **Cisco CallManager SNMP Service** is activated as shown in the 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 V3 Service	Started	Activated	Mon Jul 1 18:11:35 2019	11 days 12:12:41	

Step 2. In order to check the status of the SNMP Master Agent, navigate to **Cisco Unified Serviceability > Tools > Network services**. Select the server and verify that the SNMP Master Agent service runs as shown in the 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"/> V3 Master Agent	Running	Mon Jul 1 10:30:23 2019	11 days 12:19:43	

Step 3. In order to configure the SNMPv3 in CUCM, navigate to **Cisco Unified Serviceability > SNMP > V3 > User**. Select the server and configure the User Name, Authentication Information and Privacy Information as shown in the image.

Cisco Unified Serviceability
For Cisco Unified Communications Solutions

Navigation Cisco Unified Serviceability
administrator | About

Alarm Trace Tools Snmp CallHome Help

SNMP User Configuration

Save Clear All Cancel

Status
Status : Ready

Server* 10.1.61.158--CUCM Voice/Video

User Information
User Name* cucmsnmpv3

Authentication Information
 Authentication Required
 Password [masked] Reenter Password [masked] Protocol MDS SHA

Privacy Information
 Privacy Required
 Password [masked] Reenter Password [masked] Protocol DES AES128

Host IP Addresses Information
 Accept SNMP Packets from any host
 Accept SNMP Packets only from these hosts
 Host IP Address [input] Insert
 Host IP Addresses [list] Remove

Access Privileges
 Access Privileges* ReadOnly
 Notify access privilege is required in order to configure Notification Destinations.

Switch Configuration

In order to track phones by switchport, the SNMP configuration in the switch must match with the configuration in CER server. Use these commands to configure the switch.

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 included

Example:

```
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
```

In order to verify your configuration, use the **show run | s snmp** as shown in the example.

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

Verify

Each CUCM that runs Cisco CallManager service must also run SNMP services. If all is configured correctly, you must see all the CallManager nodes when you click on the **Cisco Unified Communications Manager List** hyperlink and the phones must be tracked by switchport.

Step 1. In order to verify the CUCM nodes list, navigate to **CER Admin > Phone tracking > Cisco Unified Communications Manager**. Click on the hyperlink as shown in the image.

The screenshot shows the Cisco Emergency Responder Administration interface. The main configuration area is titled "Cisco Unified Communications Manager Clusters". It contains several sections:

- Status:** Please enter any change for the current Cisco Unified Communications Manager.
- Modify Cisco Unified Communications Manager Cluster:** This section is highlighted with a red box and contains the following fields:
 - Cisco Unified Communications Manager *: 10.1.61.158
 - 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: [Empty]
 - Telephony Port Begin Address: 500
 - Number of Telephony Ports: 2
- Secure Connection Parameters:** Includes fields for TFTP Server IP Address, TFTP Server Port (69), Backup TFTP Server IP Address, CAPF Server IP Address, CAPF Server Port (3804), Instance ID for Publisher, Secure Authentication String for Publisher, Instance ID for Subscriber, and Secure Authentication String for Subscriber.
- AXL Settings:** This section is also highlighted with a red box and contains:
 - AXL Username: administrator
 - AXL Password: [Redacted]
 - AXL Port Number: 8443
- SNMP Settings:** Use SNMPV3 for discovery:

On the right side, a browser window titled "Cisco Emergency Responder Administration" is open, showing the "List of Cisco Unified Communications Managers" page. This page lists two CUCM nodes with IP addresses 10.1.61.158 and 10.1.61.159, both of which are highlighted with a red box.

Step 2. In order to confirm that phones are tracked by switchport, navigate to **CER Admin > ERL Membership > Switchport > Filter >** and click on **Find**. The switch IP address and phones tracked must be listed as shown in the image.

The screenshot shows the "Assign ERL to Selected Switch Ports" table. The table has the following columns: Switch IP Address, ERL Name, Switch IP Address, IFName, Location, Phone Extension, Phone IP Address, and Phone Typ. The table is filtered to show switch IP address 10.1.61.10. The data rows are as follows:

Switch IP Address	ERL Name	Switch IP Address	IFName	Location	Phone Extension	Phone IP Address	Phone Typ
<input type="checkbox"/> 10.1.61.10		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"/>	ERL_MEX	10.1.61.10	Gi0/10	View			
<input type="checkbox"/>		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			

Troubleshoot

SNMP Walk Version 3

In order to confirm that both CUCM and the switch respond to CER you can use the **SNMP walk v3** command. The recommended Object Identifier (OID) is 1.3.6.1.2.1.1.2.0 as shown in the example.

Example of SNMP walk version 3 from CER to 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
```

Example of SNMP walk version 3 from CER to the 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
```

Example of SNMP walk v3 with root access in CER:

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

Where:

- u : is the snmp v3 user.
- l : is the authentication mode [noAuthNoPriv|authNoPriv|authPriv].
- A : is the Authentication password.
- a : is the authentication protocol [MD5|SHA].
- x : is the privacy protocol [DES|AES128].
- X : is the privacy protocol password.

Example of the output is as show in the image.



If you receive the following error "*Error generating a key (Ku) from the supplied privacy pass phrase*" try with the following syntax:

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

Verify that the OID returned is one of the supported devices in the CER release notes of your version.

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cer/11_5_1/english/release_notes/guide/ER_BK_C838747F_00_cisco-emergency-responder-version-1151.html#CER0_CN_SE55891C_00

Some of the OIDs that CER sends to the switch are:

- 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

Some of the OIDs that CER sends to the CUCM are:

- 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

Packet Capture

It is very useful to get a packet capture in order to isolate issues with phone tracking, these are the steps to get a packet capture in CER.

Step 1. Start a packet capture via CLI with the command **utils network capture eth0 file ExampleName size all count 10000**, where ExampleName is the name for your packet capture.

Step 2. Replicate the issue (place the 911 call, SNMP walk, phone tracking update, etc).

Step 3. Stop the packet capture with **Ctrl+C**

Step 4. Confirm that the packet capture was saved in CER with the command **file list activelog platform/cli/***

Step 5. Retrieve the packet capture with the command **file get activelog platform/cli/ExampleName.cap** (an SFTP server is required to export the file).

Enable the Logs in CER

In order to enable the logs in Emergency Responder Server, navigate to **CER Admin > System > Server Settings**. Activate all the checkboxes, it does not generate any service impact on the server.

Server Settings For CERServerGroup

Status

Ready

Select Server



[Publisher \(primary\)](#)



[Subscriber\(standby\)](#)

Modify Server Settings

Server Name *

Publisher

Host Name

mycerpubvictogut

Debug Package List

Select All

Clear All

- | | |
|---|--|
| <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

Select All

Clear All

- | | |
|---|--|
| <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 |

In order to troubleshoot a switch that is not shown in the switchports (**CER > Admin > ERL membership > Switch Ports**), these steps must be taken:

1. Verify the configuration in **Admin > Phone tracking > LAN Switch details**.
2. Verify the configuration in **Admin > Phone tracking > SNMP v2 / v3**.
3. Verify the **Enable CAM based Phone Tracking** checkbox. If it is a non-Cisco switch, or CDP is disabled, check the Enable CAM based Phone Tracking checkbox.
4. Verify the SNMP configuration on the switch.

5. Collect phone tracking logs.

If switch ports show up but phones do not, these steps must be taken:

1. SNMP configuration on CER and Communications Managers.
2. Confirm the IP/Hostname under Cisco Unified Communications Manager.
3. Confirm if phones not showed belong to an specific Communications Manager.
4. Confirm both SNMP Services (SNMP Master Agent / CallManager SNMP Service) are started on all CallManager nodes in the cluster.
5. Confirm CUCM reachability via SNMP walk.
6. Collect phone tracking logs.

Example 1 of CER phone tracking logs:

```
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
```

Possible reason: Wrong configuration on SNMPv3 Privacy Information.

Example 2 of CER phone tracking logs:

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

Possible reason: Cisco CallManager SNMP Service is deactivated in one of the CUCM nodes.

Related Information

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cer/11_5_1/english/administration/guide/CER_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/CER0_BK_CA66317A_00_cisco-emergency-responder-administration-10_0/CER0_BK_CA66317A_00_cisco-emergency-responder-administration-10_0_chapter_01100.pdf