SNMPv3 für CER konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration und Fehlerbehebung des Simple Network Management Protocol (SNMP) Version 3 für Cisco Emergency Responder (CER).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Unified Communications Manager (CUCM)
- Cisco Notfallschutz
- SNMP-Protokoll

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Der Emergency Responder verwendet SNMP, um Informationen über die Ports eines Switches abzurufen. Sobald die Informationen abgerufen wurden, kann der CER-Administrator die Ports den Emergency Response Locations (ERL) zuweisen, sodass der Emergency Responder die an die Ports angeschlossenen Telefone identifizieren und ihre ERL-Zuweisungen aktualisieren kann.

SNMP V3 bietet zusätzliche Sicherheitsfunktionen, die Nachrichtenintegrität, Authentifizierung und Verschlüsselung abdecken. Darüber hinaus steuert SNMP V3 den Benutzerzugriff auf bestimmte Bereiche der MIB-Struktur.

Der Emergency Responder liest nur SNMP-Informationen, schreibt keine Änderungen an der Switch-Konfiguration, sodass Sie nur die SNMP-Community-Strings für Lesezugriffe konfigurieren müssen.

Es gibt einige Bedingungen, unter denen die Switchports in CER nachverfolgt werden können:

- CER ruft Switch-Schnittstellen, -Ports und -VLANs (nur für CAM) ab und enthält Informationen zum Cisco Discovery Protocol (CDP).
- CER ruft registrierte Telefone vom CUCM ab.
- CER prüft den vom CUCM gesendeten Gerätenamen und sucht, ob die MAC zu einem Switch-Port gehört. Wenn die MAC-Adresse gefunden wird, aktualisiert CER die Datenbank mit dem Port-Standort eines Telefons.

Konfiguration

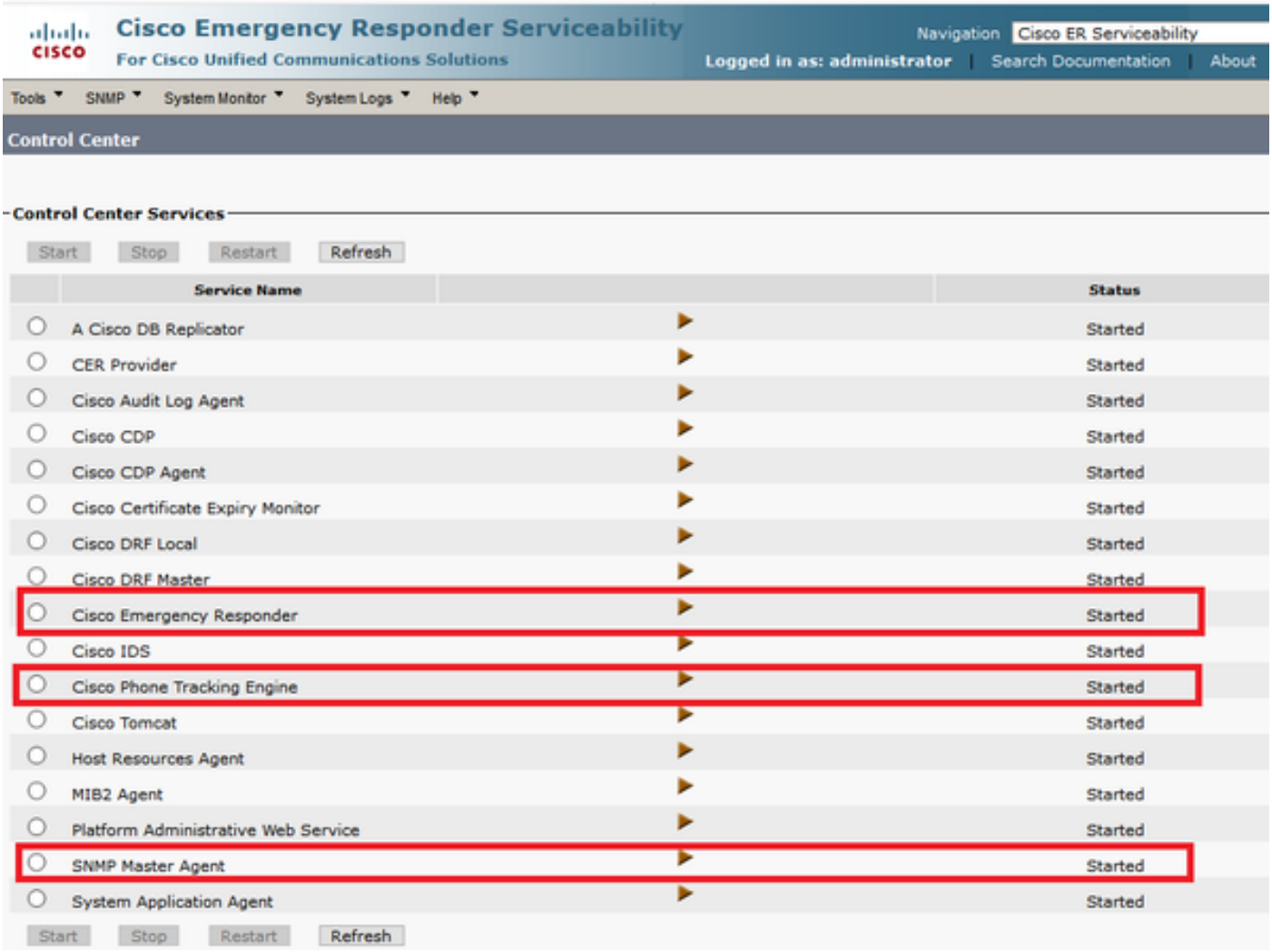
Wenn Sie die SNMP-Zeichenfolgen für die Switches konfigurieren, müssen Sie auch die SNMP-Zeichenfolgen für die Unified Communications Manager-Server konfigurieren. Der Emergency Responder muss in der Lage sein, SNMP-Abfragen von allen Unified CM-Servern durchzuführen, auf denen die Telefone registriert sind, um die Telefoninformationen abzurufen.

CER bietet die Möglichkeit, Muster zu verwenden, z. B. 10.0.*.* oder 10.1.*.* für Geräte mit IP-Adressen, die mit 10.0 oder 10.1 beginnen. Wenn Sie alle möglichen Adressen einbinden möchten, können Sie das Subnetz *.*.*.* verwenden.

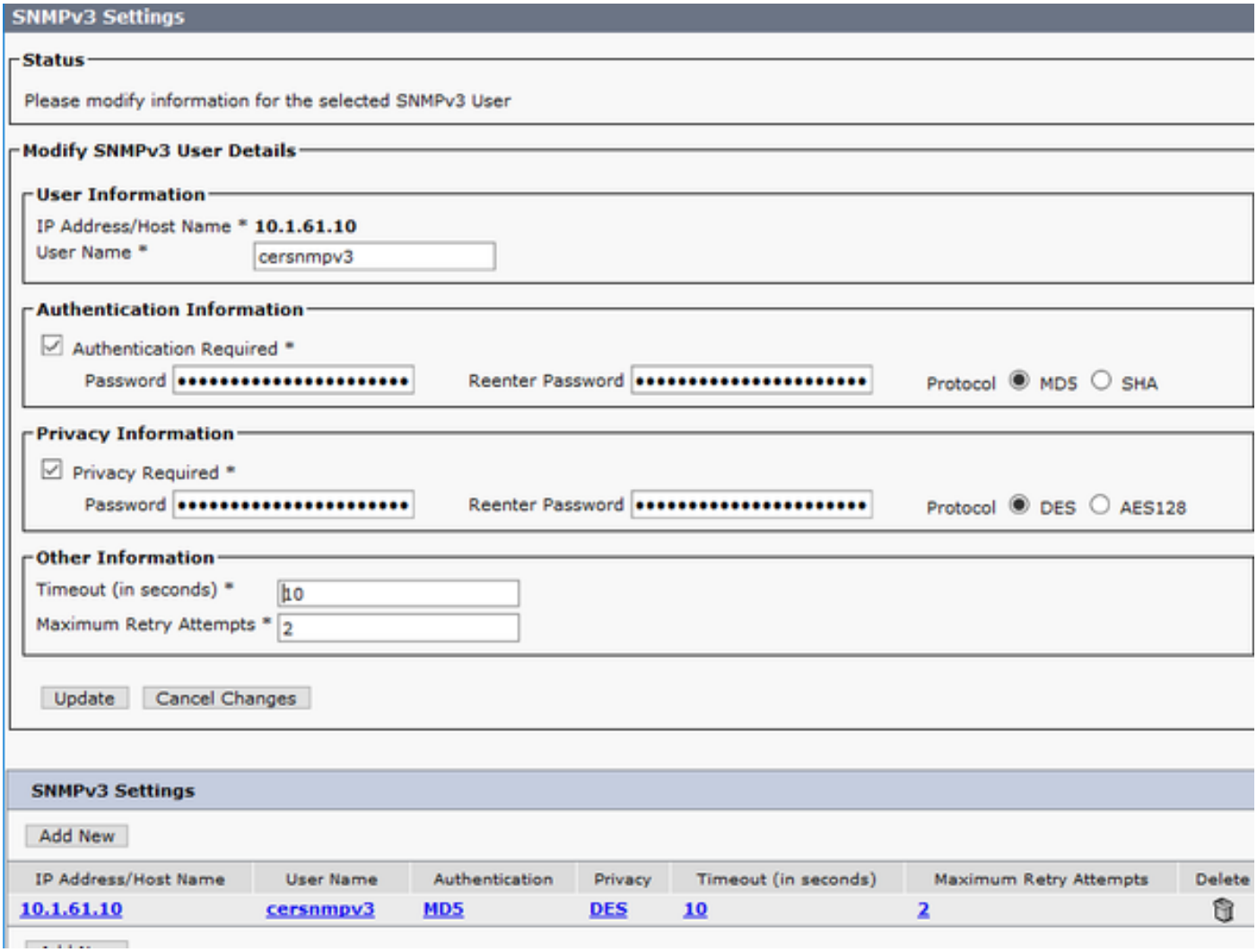
CER-Konfiguration

Um SNMPv3 für die Telefonverfolgung in Cisco Emergency Responder zu konfigurieren, gehen Sie wie folgt vor:

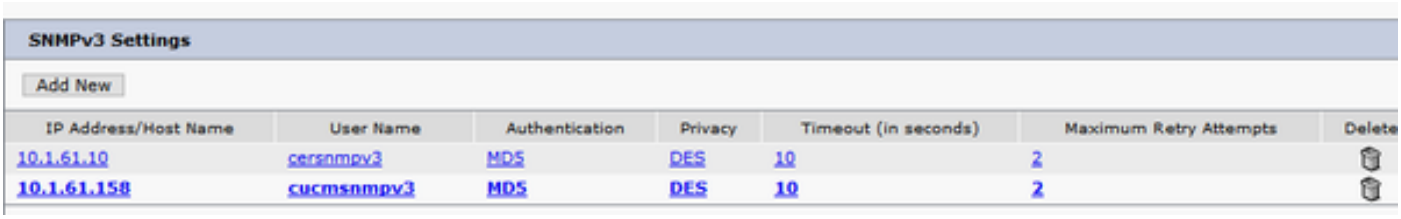
Schritt 1: Stellen Sie, wie im Bild gezeigt, sicher, dass der SNMP Master Agent, der CER und die Dienste der Cisco Phone Tracking Engine gestartet werden.



Schritt 2: Um die für Switches und CUCM-Knoten verwendeten SNMP-Einstellungen zu konfigurieren, navigieren Sie zu **CER Admin > Phone Tracking > SNMPv2/v3**. Sie können den SNMP-Benutzernamen, die Authentifizierungs- und Datenschutzinformationen wie im Bild gezeigt konfigurieren.

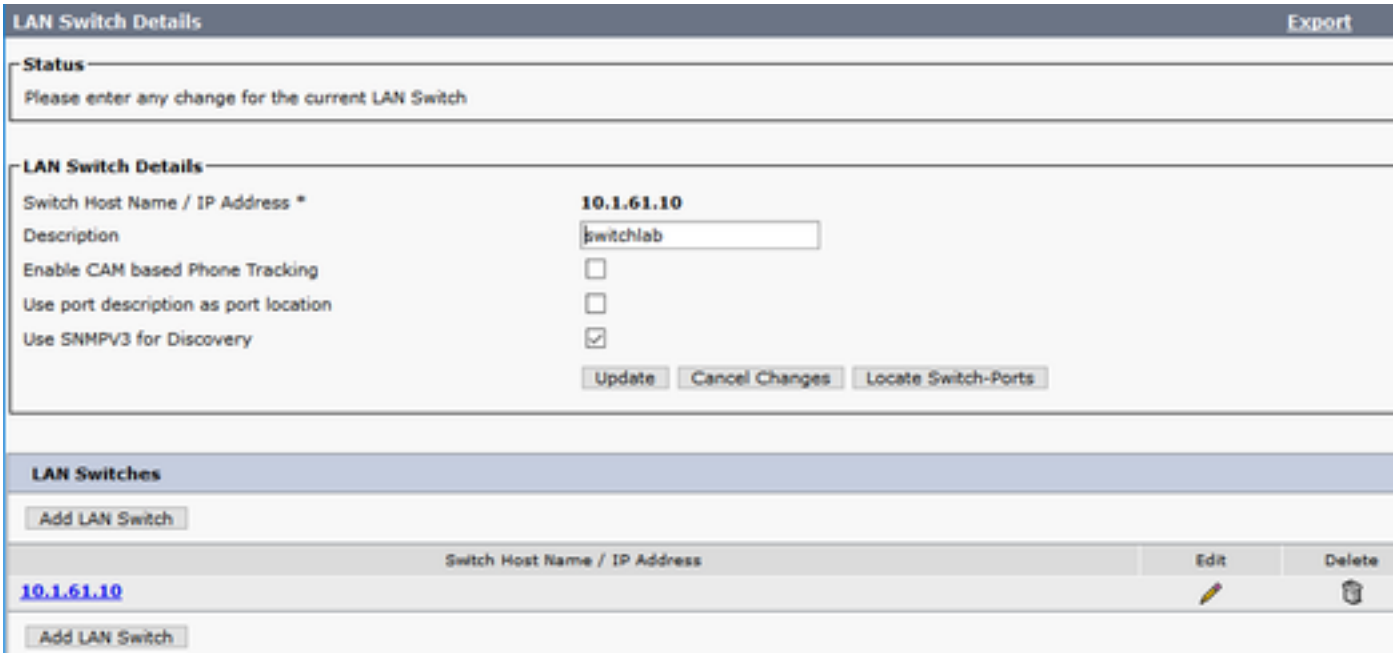


In diesem Beispiel ist 10.1.61.10 die IP-Adresse des Switches und 10.1.61.158 die IP-Adresse des Call Managers. Die SNMPv3-Konfiguration in CER ist im Bild dargestellt.



> **Hinweis:** Sie können *.*.*.* oder andere Platzhalter/-bereiche in der **IP-Adresse/** dem **Hostnamen** angeben, um mehr als einen Server einzubinden. Andernfalls können Sie bestimmte IP-Adressen konfigurieren.

Schritt 3: Um die Switch-IP auf LAN-Switches zu konfigurieren, navigieren Sie zu **CER Admin > Phone Tracking > LAN Switch detail > Add LAN Switch** wie im Image gezeigt.

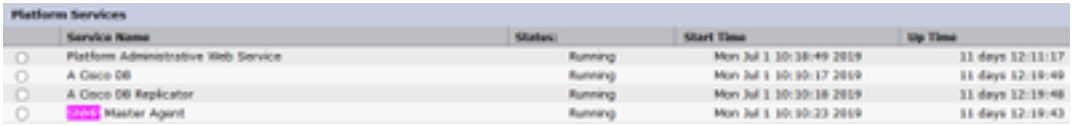


Communications Manager-Konfiguration

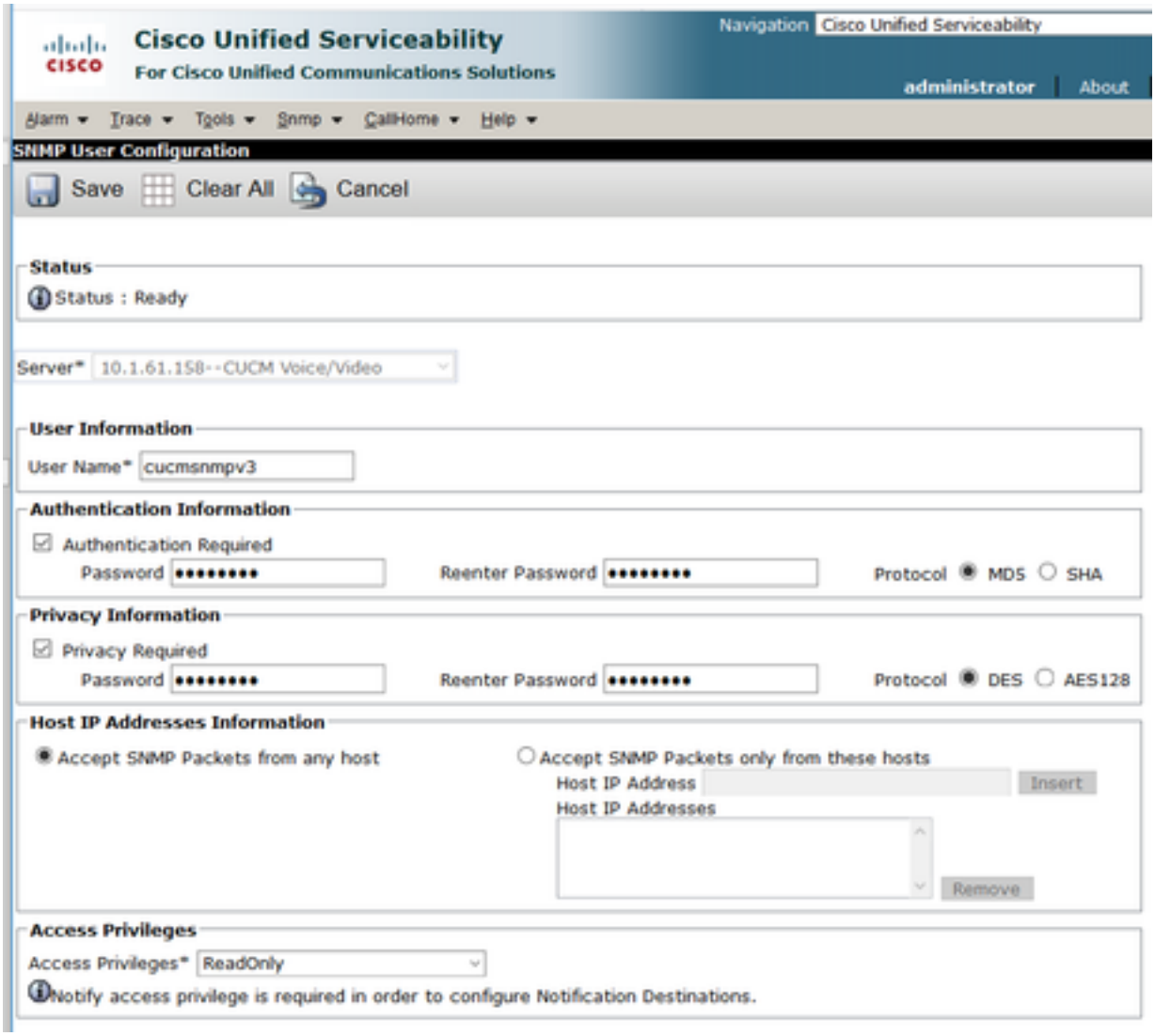
In CUCM gibt es zwei Stufen der SNMP-Konnektivität: den SNMP Master Agent und den Cisco CallManager SNMP Service. Sie müssen beide Dienste in allen diesen Knoten aktivieren, wenn der CallManager-Dienst aktiviert ist. Führen Sie die folgenden Schritte aus, um Ihren Cisco Unified Communications Manager-Server zu konfigurieren.

Schritt 1: Um den Status des Cisco CallManager SNMP Service zu überprüfen, navigieren Sie zu **Cisco Unified Serviceability > Tools > Feature Services**. Wählen Sie den Server aus, und stellen Sie sicher, dass der Status des **Cisco CallManager SNMP Service** wie im Bild gezeigt aktiviert ist.

Schritt 2: Um den Status des SNMP Master Agent zu überprüfen, navigieren Sie zu **Cisco Unified Services > Tools > Network Services**. Wählen Sie den Server aus, und überprüfen Sie, ob der SNMP Master Agent-Dienst wie im Bild gezeigt ausgeführt wird.



Schritt 3: Um SNMPv3 in CUCM zu konfigurieren, navigieren Sie zu **Cisco Unified Serviceability > SNMP > V3 > User**. Wählen Sie den Server aus, und konfigurieren Sie den Benutzernamen, die Authentifizierungsinformationen und die Datenschutzinformationen wie im Bild gezeigt.



Switch-Konfiguration

Um Telefone nach Switch-Port zu verfolgen, muss die SNMP-Konfiguration im Switch mit der Konfiguration im CER-Server übereinstimmen. Verwenden Sie diese Befehle, um den Switch zu konfigurieren.

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 enthalten

Beispiel:

```
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
```

Um Ihre Konfiguration zu überprüfen, verwenden Sie den **Befehl show run. | s snmp**, wie im Beispiel gezeigt.

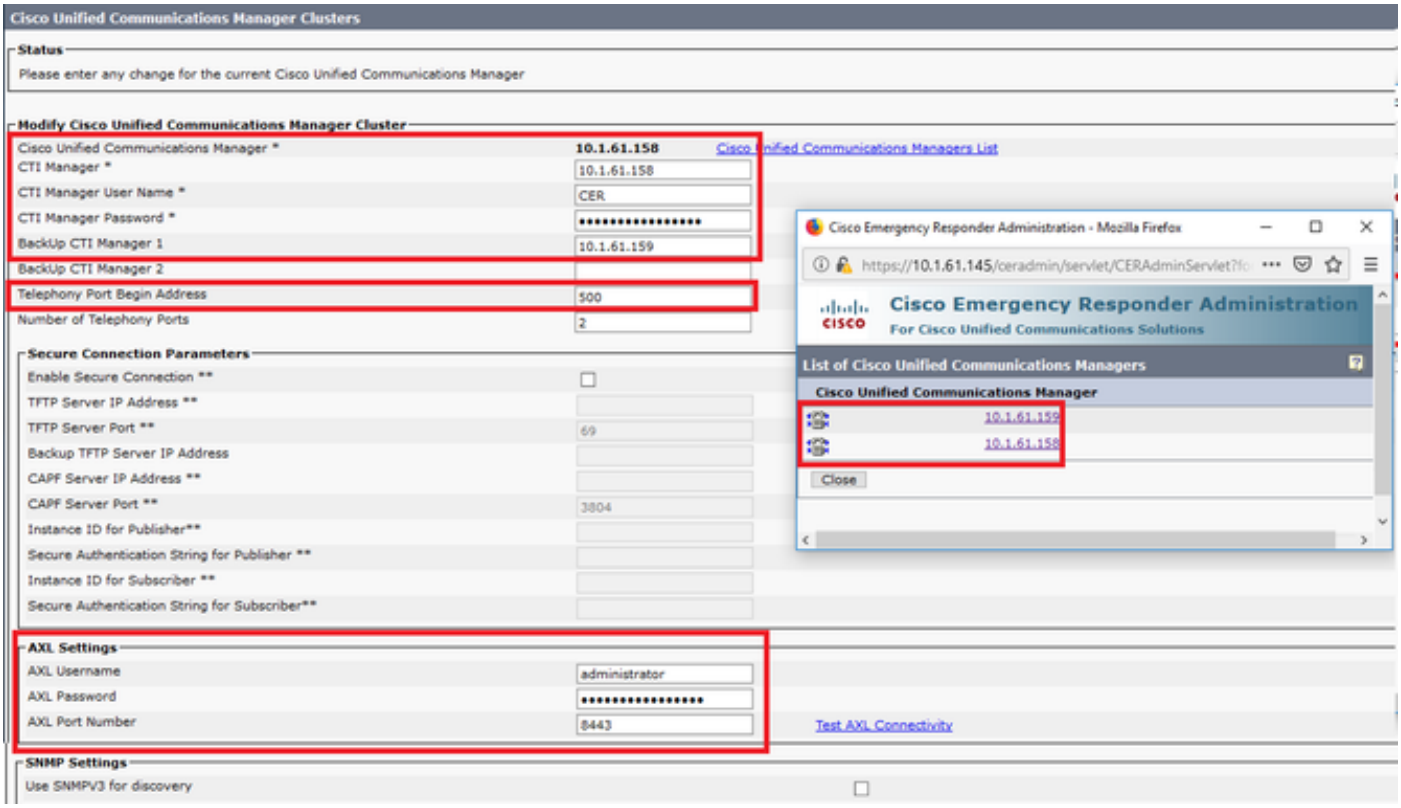
```
Switch#show run | s snmp
```

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

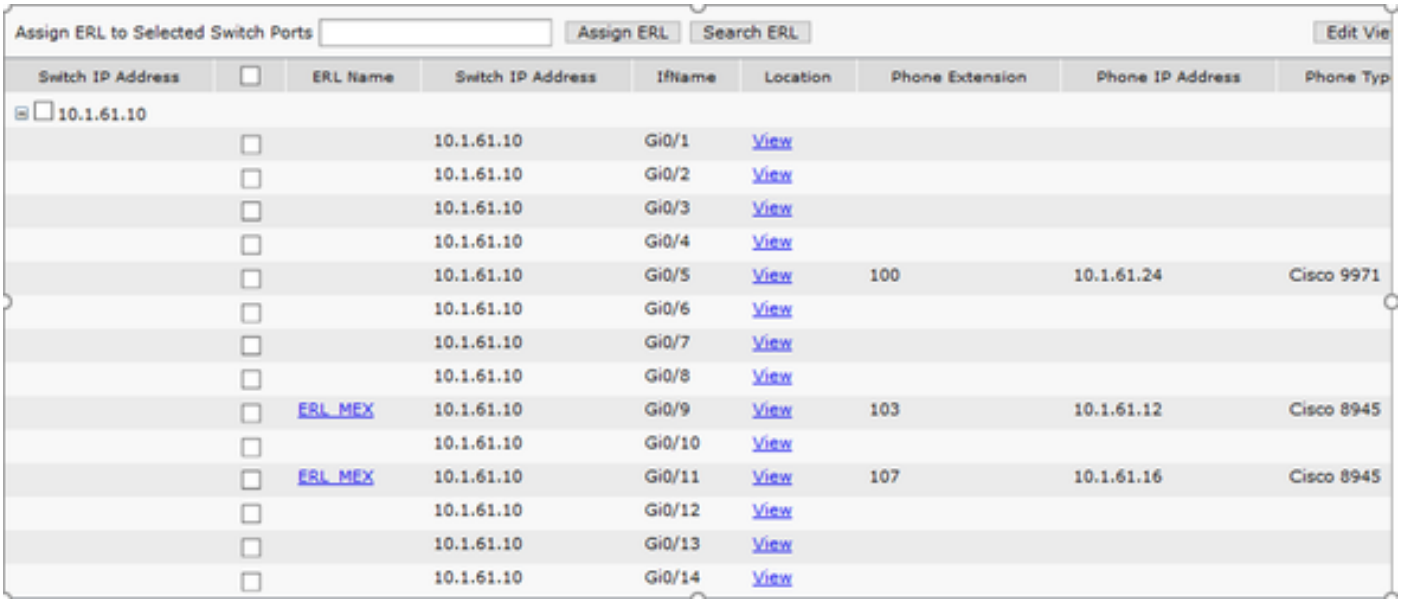
Überprüfung

Jeder CUCM, der den Cisco CallManager-Dienst ausführt, muss auch SNMP-Dienste ausführen. Wenn alle korrekt konfiguriert sind, müssen alle CallManager-Knoten angezeigt werden, wenn Sie auf den Hyperlink **Cisco Unified Communications Manager List** klicken, und die Telefone müssen über den Switch-Port nachverfolgt werden.

Schritt 1: Um die Liste der CUCM-Knoten zu überprüfen, navigieren Sie zu **CER Admin > Phone tracking > Cisco Unified Communications Manager**. Klicken Sie auf den Hyperlink, wie im Bild gezeigt.



Schritt 2: Um zu überprüfen, ob die Telefone nach Switch-Port verfolgt werden, navigieren Sie zu **CER Admin > ERL Membership > Switchport > Filter >** und klicken Sie auf **Find**. Die IP-Adresse des Switches und die verfolgten Telefone müssen wie im Bild gezeigt aufgeführt sein.



Assign ERL to Selected Switch Ports | Assign ERL | Search ERL | Edit Vie

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

Fehlerbehebung

SNMP Walk Version 3

Um zu bestätigen, dass CUCM und Switch auf CER reagieren, können Sie den Befehl **SNMP walk v3** verwenden. Der empfohlene Objekt-ID (OID) ist 1.3.6.1.2.1.1.2.0, wie im Beispiel gezeigt.

Beispiel für den SNMP-Laufsteg Version 3 von CER zu 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
```

Beispiel für den SNMP-Laufsteg Version 3 von CER zum 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
```

Beispiel für SNMP-Walk v3 mit Root-Zugriff in CER:

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

Wo:
-u: ist der Benutzer snmp v3.
-l: ist der Authentifizierungsmodus [noAuthNoPriv|authNoPriv|authPriv].
A: ist das Authentifizierungskennwort.
-a: ist das Authentifizierungsprotokoll [MD5|SHA].
-x: ist das Datenschutzprotokoll [DES/AES128].
-X: ist das Datenschutzprotokoll-Passwort.

Ein Beispiel für die Ausgabe ist wie im Bild dargestellt.

Wenn Sie den folgenden Fehler "*Fehler beim Generieren eines Schlüssels (Ku) aus der bereitgestellten Kennzeichenfolge für den Datenschutzhinweis*" erhalten, versuchen Sie mit der folgenden Syntax:

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

Überprüfen Sie, ob die zurückgegebene OID eines der unterstützten Geräte in den CER-Versionshinweisen Ihrer Version ist.

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cer/11_5_1/english/release_notes/guide/CER_BK_C838747F_00_cisco-emergency-responder-version-1151.html#CER0_CN_SE55891C_00

Einige der OIDs, die CER an den Switch sendet, sind:

- 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

Einige der OIDs, die CER an den CUCM sendet, sind:

- 1.3.6.1.4.1.9.9.156.1.1.2.1.7 - ccmEntry/ccmInternetAddress
- 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

Paketerfassung

Es ist sehr nützlich, eine Paketerfassung zu erhalten, um Probleme mit der Telefonverfolgung zu isolieren. Dies sind die Schritte, um eine Paketerfassung in CER zu erhalten.

Schritt 1: Starten Sie eine Paketerfassung über die CLI mit dem Befehl **utils network capture eth0 file ExampleName size all count 10000**, wobei ExampleName der Name für die Paketerfassung ist.

Schritt 2: Replizieren Sie das Problem (tätigen Sie den Anruf 911, SNMP-Spaziergang,

Aktualisierung der Telefonverfolgung usw.).

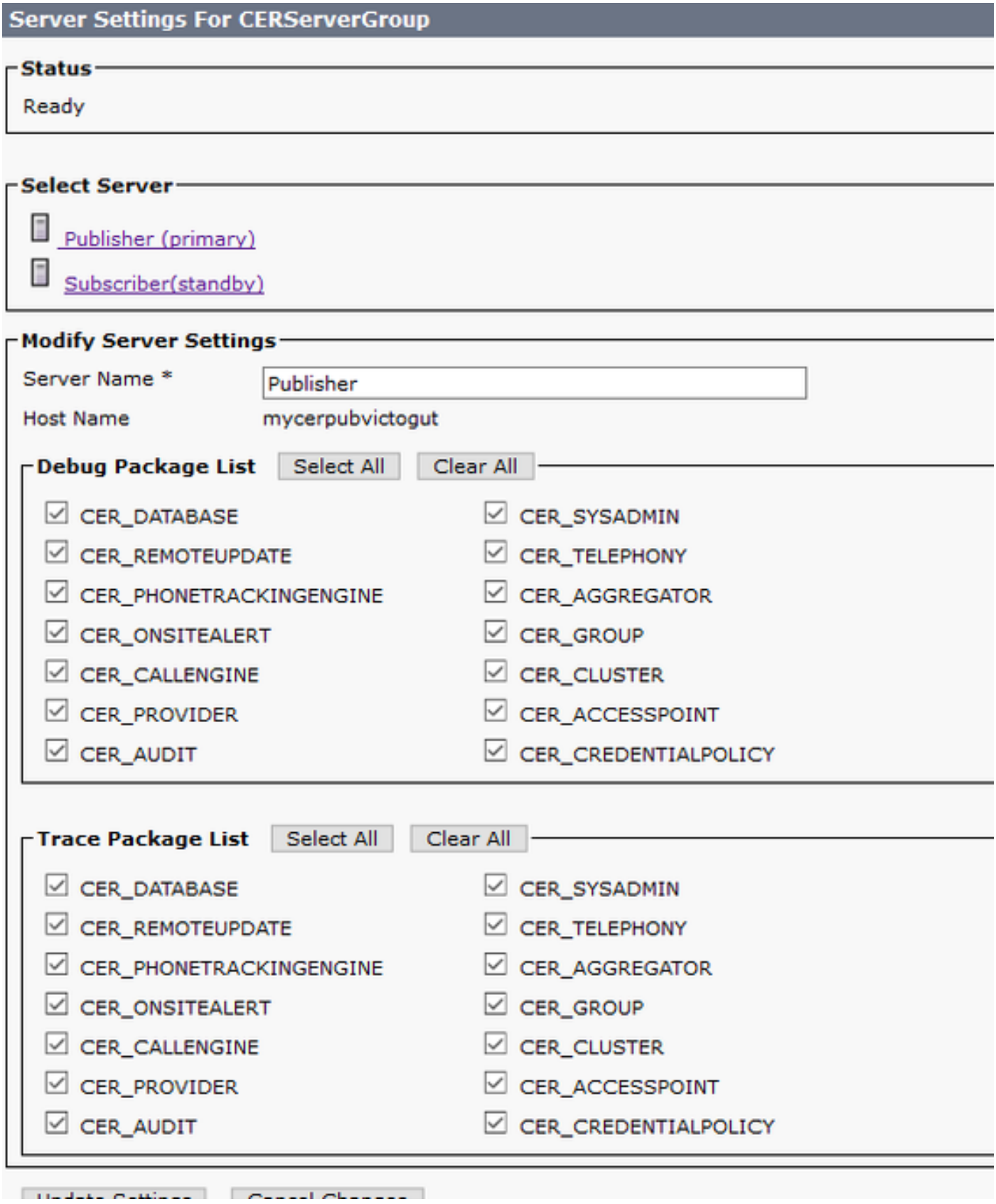
Schritt 3: Stoppen Sie die Paketerfassung mit **Strg+C.**

Schritt 4: Bestätigen Sie, dass die Paketerfassung mit der **Active-Plattform/CLI/*** in CER gespeichert wurde.

Schritt 5: Rufen Sie die Paketerfassung mit dem Befehl **file get activelog platform/cli/ExampleName.cap** (für den Export der Datei ist ein SFTP-Server erforderlich) ab.

Aktivieren Sie die Protokolle in CER.

Um die Protokolle im Emergency Responder Server zu aktivieren, wählen Sie **CER Admin > System > Server Settings aus**. Aktivieren Sie alle Kontrollkästchen, es werden keine Servicebeeinträchtigungen für den Server generiert.



Zur Fehlerbehebung bei Switches, die nicht in den Switch-Ports angezeigt werden (**CER > Admin > ERL mitgliedschaft > Switch Ports**), müssen folgende Schritte ausgeführt werden:

1. Überprüfen Sie die Konfiguration unter **Admin > Phone Tracking > LAN Switch details**.
2. Überprüfen Sie die Konfiguration unter **Admin > Phone Tracking > SNMP v2/v3**.
3. Überprüfen Sie das Kontrollkästchen **CAM-basierte Telefonverfolgung aktivieren**. Wenn es sich um einen Nicht-Cisco-Switch handelt oder CDP deaktiviert ist, aktivieren Sie das Kontrollkästchen Enable CAM based Phone Tracking (CAM-basierte Telefonverfolgung

aktivieren).
4. Überprüfen Sie die SNMP-Konfiguration auf dem Switch.
5. Sammeln Sie die Telefonverfolgungsprotokolle.

Wenn Switch-Ports angezeigt werden, Telefone jedoch nicht, müssen folgende Schritte ausgeführt werden:

1. SNMP-Konfiguration auf CER- und Communications Manager.
2. Bestätigen Sie den IP/Hostnamen unter Cisco Unified Communications Manager.
3. Bestätigen Sie, ob die Telefone nicht zu einem bestimmten Communications Manager gehören.
4. Bestätigen Sie, dass beide SNMP-Dienste (SNMP Master Agent/CallManager SNMP Service) auf allen CallManager-Knoten im Cluster gestartet werden.
5. Bestätigen Sie die CUCM-Erreichbarkeit über SNMP-Walk.
6. Sammeln Sie die Telefonverfolgungsprotokolle.

Beispiel 1 für CER-Telefon-Nachverfolgungsprotokolle:

```
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
```

Mögliche Gründe: Falsche Konfiguration der SNMPv3-Datenschutzinformationen.

Beispiel 2 der CER-Telefon-Nachverfolgungsprotokolle:

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

Mögliche Gründe: Der Cisco CallManager SNMP Service wird in einem der CUCM-Knoten deaktiviert.

Zugehörige Informationen

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