# Configuratie van SIP-registraties om per-gebruiker een verificatie en autorisatie voor CUCM 11.5 uit te voeren

## Inhoud



## Inleiding

Dit document beschrijft verbeterd gedrag in Cisco Unified Communications Manager (CUCM) dat een extra laag van User ID-verificatie biedt in de Session Initiation Protocol (SIP) REGISTER-berichten tegen de huidige methode van verificatie alleen op de expressway.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CUCM-beheer en -configuratie
- SIP-protocol
- VCS-snelweg (Video Communication Server)

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Unified Communications Manager 11.5 en hoger
- VCS-snelweg (Video Communication Server)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg ervoor dat u de potentiële impact van om het even welke opdracht begrijpt.

## Achtergrondinformatie

In het verleden werkt apparaatregistratie via VCS-snelweg (Video Communication Server) wanneer het apparaat een gebruikersnaam en wachtwoord via Hypertext Transfer Protocol (HTTP) verstuurt. Expressway authenticeert de gebruikersnaam en stelt het apparaat in staat om de registratie naar CUCM te starten zonder verdere verificatie.

Het nieuwe gedrag is dat CUCM nu het SIP REGISTER-bericht controleert en garandeert dat de User-ID een juiste associatie met het apparaat heeft. Met behulp van deze functie dient de gebruiker-ID toestemming te geven voordat hij zich in het UCM registreert. biedt derhalve het volgende beschermingsniveau tegen het apparaat van het externe/onbekende netwerk. Dit waarborgt dat het SIP REGISTER is toegestaan, d.w.z. dat alleen een geldig apparaat dat aan de geldige gebruiker is gekoppeld, zich moet registreren. Als er geen User ID Association aan het apparaat is gekoppeld, wijst de registratie af met de 401-responscode.

Achtergrondhistorie

- CSCu97283
- CVE-ID CVE-2015-6410

Beperkingen

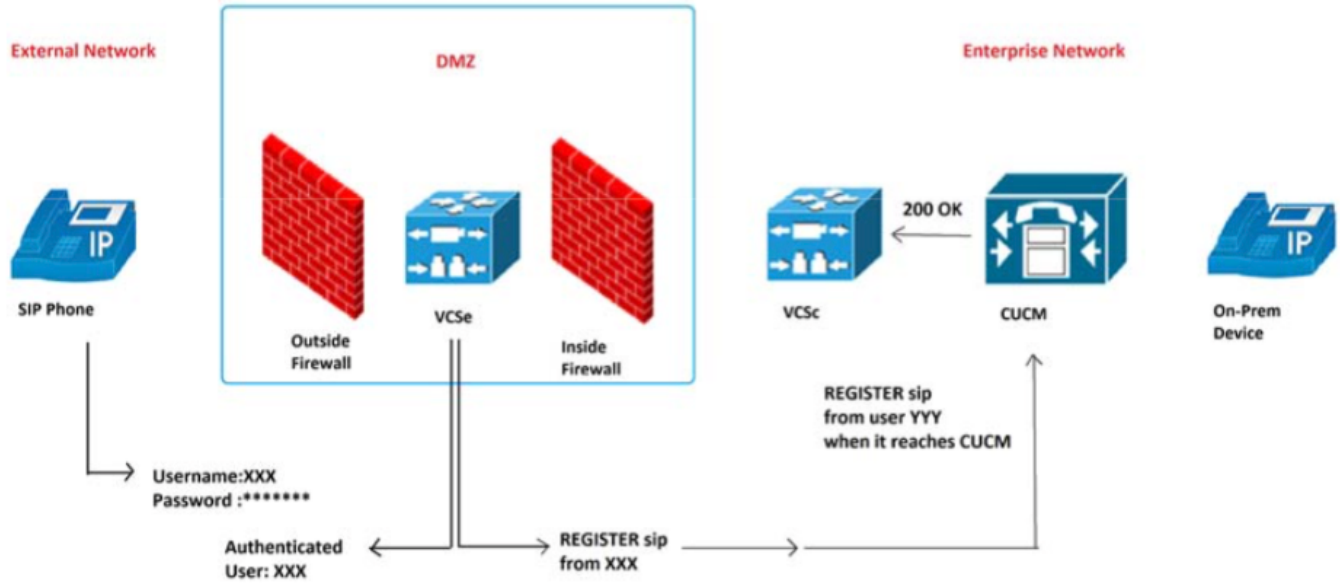
- Alleen gevolgen voor SIP-telefoons
- Aanbevolen registraties worden niet beïnvloed

# Configureren

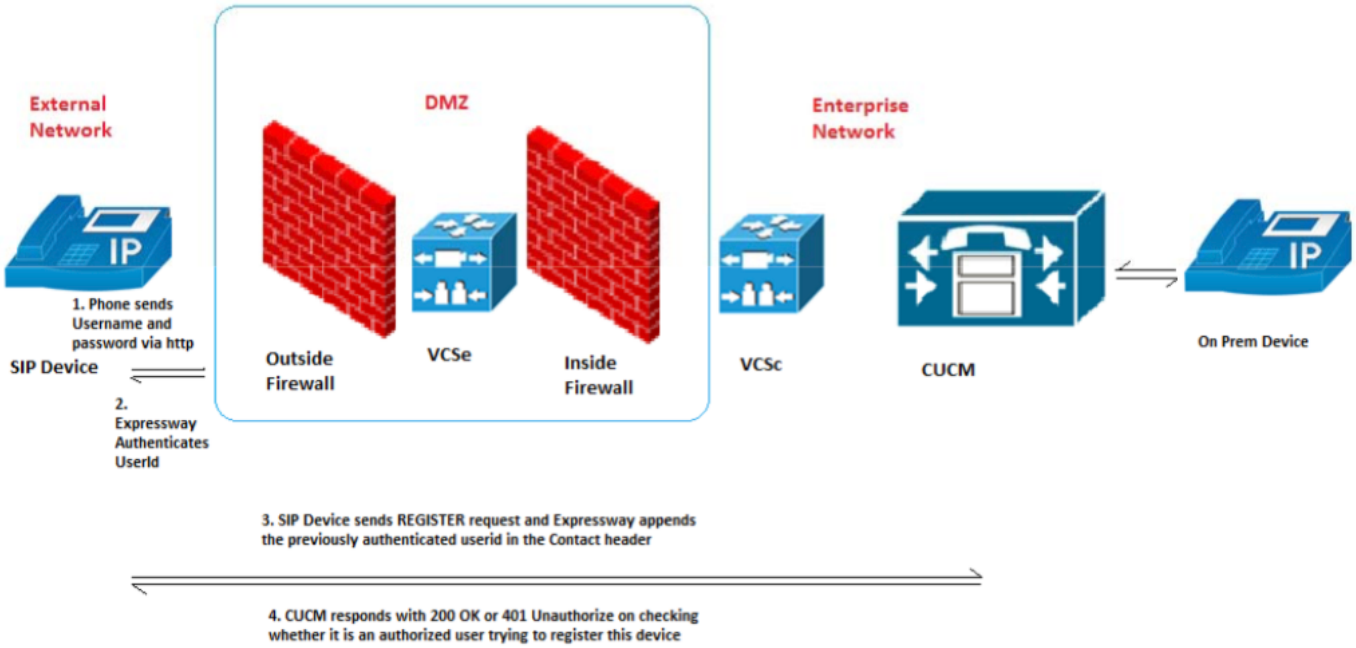
## Netwerkdiagram

Gebruikte componenten (oude vs. nieuwe architectuur)

Afbeelding ouder gedrag:




Nieuw gedragsbeeld:




## Configuraties

Nieuwe service parameter om deze functie in/uit te schakelen: **Systeem > Serviceparameters > *server* > Cisco CallManager > SIP-registratieservice**

Waarden:

- Waar - (standaard)
- Onjuist

De juiste User-ID associatie met het juiste apparaat bepaalt of de SIP-registratie toestemming geeft of afwijst.

In het verzoek om een registratievergunning worden deze scenario's gevolgd:

Scenario 1. Als de gebruiker-ID niet in het REGISTER-bericht staat, moet hij toestemming geven en wordt 200 OK verzonden.

Opmerking: Dit waarborgt interoperabiliteit vooraf en compatibiliteit met oudere expressway versies.

scenario 2. Als de gebruiker-ID in het REGISTER-bericht staat, dan...

- ALS User-ID overeenkomt met het veld Eigennaam-id in de configuratiescherm van CUCM-telefoon, autoriseer dan en stuur 200 OK
- ALS User-ID overeenkomt met de associatie van de gebruikerID met het apparaat in de pagina van de CUCM-eindgebruiker Configuration, autoriseert u vervolgens 200 OK
- ALS zowel het veld Eigenaar-id leeg is als er geen apparaatassociatie naar de eindgebruiker bestaat, autoriseer dan 200 OK
- ELSE ALS GEEN match, VERVOLGENS FAIL en 401 ongeautoriseerd verzenden

Scenario 3. Als REGISTER-bericht meer dan één gebruiker-ID van verschillende waarden bevat, moet u het bestand onjuist laten en 401 niet-geautoriseerd verzenden.

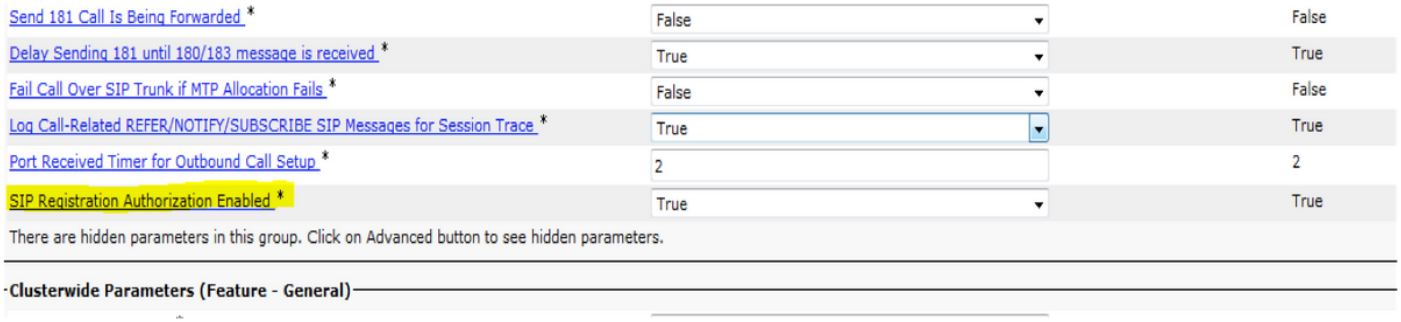
Opmerking: Alleen expresse-opdruk van deze User-ID-headers

Resultaten cases gebruiken

| Nummer | Testgevallen | Invoervergunning voor SIP-registratie | Verwacht resultaat |
|---|---|---|---|
| 1 | GebruikerID-parameter in de contactkop is niet aanwezig | Waar | autoriseren (200 OK) |
| 2 | UserID-parameter in de contactheader-overeenkomsten met OwnerID in de configuratie-pagina van de telefoon | Waar | autoriseren (200 OK) |
| 3 | GebruikerID-parameter in de contactheader-overeenkomsten met gebruikerID gekoppeld aan een apparaat in de Eindgebruikerspagina. | Waar | autoriseren (200 OK) |
| 4 | GebruikerID in contactkopbalwedstrijden met eigenaarID in pagina Telefonische configuratie, komt niet overeen met gebruikerID ingesteld in Eindgebruikerspagina | Waar | autoriseren (200 OK) |
| 5 | GebruikerID in contactkopbalwedstrijden met gebruikerID op de pagina Eindgebruiker komt niet overeen met EigenaarID in pagina Telefonische configuratie | Waar | autoriseren (200 OK) |
| 6 | Gebruiker ID in pagina Config voor telefoon is leeg en er is geen gebruiker gekoppeld aan de eindpagina | Waar | autoriseren (200 OK) |
| 7 | EigenaarID in pagina Config voor telefoon en gebruikerID voor een apparaat in pagina van de eindgebruiker, maar geen overeenkomst gevonden | Waar | 401 niet-geautoriseerd |
| 8 | Meer dan één gebruiker aanwezig in de contactkop. | Waar | 401 niet-geautoriseerd |
| 9 | Meervoudige gebruikerID ingesteld voor een | Waar | autoriseren (200 |

| | | | |
|---|---|---|---|
| | apparaat in de eindgebruikerspagina | | OK) |
| 10 | GebruikerID ontsnapen | Waar | autoriseren (200 OK) |
| 11 | Registreren verversen | Waar | Dit is hetzelfde als het oorspronkelijke REGISTER-bericht |
| 12 | GebruikerID in contactkop is lege string, OwnerID en UserID niet ingesteld voor het apparaat | Waar | autoriseren (200 OK) |
| 13 | GebruikerID in contactkop is lege string, OwnerID/UserID ingesteld voor het apparaat | Waar | 401 niet-geautoriseerd |
| 14 | UserID is aanwezig in de contactkop, OwnerID/UserID ingesteld voor het apparaat, maar er is geen overeenkomst gevonden | Onjuist | 200 OK |
| 15 | Meer dan één gebruikerID aanwezig in de contactheader | Onjuist | 200 OK |
| 16 | GebruikerID in contactkop is lege string, eigenaarID /UserID ingesteld voor het apparaat | Onjuist | 200 OK |

Schakel deze optie in via Communications Manager (CCM) Service Parameter. Het is standaard ingeschakeld en er is geen verdere configuratie vereist.




# Verifiëren

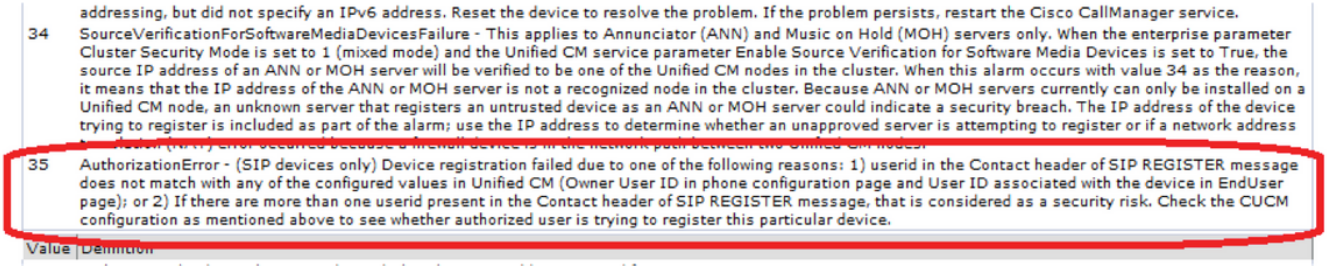
### Contactheader

CUCM controleert de contactkop van het REGISTER-bericht voor wijziging door middel van expresse

```
Contact: <sip:ffeffb75-880e-f58f-a8ec-f5025d0f9136@10.50.179.6:5060;transport=tcp;orig-
hostport=192.168.0.121:55854>;+sip.instance="<urn:uuid:00000000-0000-0000-0000-
00506005457e>";+u.sip!model.ccm.cisco.com="604";+u.sip!userid.ccm.cisco.com="mjavie
r";+u.sip!serialno.ccm.cisco.com=A1AZ20D00153;audio=TRUE;video=TRUE;mobility="fixed";
duplex="full";description="TANDBERG-SIP"
```

### Nieuwe alarmfase (autorisatie, fout met waarschuwingsniveau)

Er is nu een nieuw alarm (AuthorizationErrorwithWarningLevel) beschikbaar wanneer er een fout in de SIP-registratievergunning is opgetreden




# Problemen oplossen

Bekijk autorisatie pogingen in CCM Traces debug uitvoer

Succesvolle vergunningsvoorbeelden:

Scenario 1:

```
00013222.041 |15:46:20.792 |AppInfo |SIPStationD(7) - User Authorized - Phone Config page
```

Scenario 2:

```
00015642.041 |16:01:39.112 |AppInfo |SIPStationD(9) - User Authorized - EndUser page
```

Vergunning mislukt en voorbeeld:

```
00186341.041 |13:17:37.187 |AppInfo |SIPStationD(133) - User: shree is unauthorized to register
a device
00186341.042 |13:17:37.187 |AppInfo |SIPStationD(133) - sendRegisterResp: non-200 response code
401, ccbId 2303, expires 4294967295, warning Authorization failure -
Unauthorized user for this device 00186341.043 |13:17:37.188 |AppInfo
|EndPointTransientConnection - An endpoint attempted to register but did not complete
registration Connecting Port:5060 Device name:
SEPCD1111000015 Device type:647 Reason Code:35 Protocol:SIP Device MAC address:CD1111000015
LastSignalReceived:SIPRegisterInd StationState:wait_register App ID:Cisco
CallManager Cluster ID:10.77.29.71 Node ID:CuCM-71 00186341.044 |13:17:37.188
|AlarmWarn|AlarmClass: CallManager, AlarmName: EndPointTransientConnection, AlarmSeverity:
Warning, AlarmMessage: , AlarmDescription: An endpoint
attempted to register but did not complete registration, AlarmParameters: ConnectingPort:5060,
DeviceName:SEPCD1111000015, DeviceType:647, Reason:35, Protocol:SIP,
MACAddress:CD1111000015, LastSignalReceived:SIPRegisterInd, StationState:wait_register,
AppID:Cisco CallManager, ClusterID:10.77.29.71, NodeID:CuCM-71, 00186346.000 |13:17:37.189
|SdlSig |SIPRegisterResp |wait |SIPHandler(1,100,80,1) |SIPStationD(1,100,74,133)
|1,100,14,772.2^10.77.29.189^SEPCD1111000015 |[T:N-H:0,N:0,L:0,
V:0,Z:0,D:0] ccbID= 2303 --TransType=1 --TransSecurity=0 PeerAddr= 10.77.29.189:5060 respCode=
401 action= 2 device=
```