

# Configurazione delle registrazioni SIP per l'autenticazione e l'autorizzazione per utente (MRA) per CUCM 11.5

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

## Introduzione

In questo documento viene descritto il comportamento migliorato di Cisco Unified Communications Manager (CUCM), che fornisce un livello aggiuntivo di autenticazione UserID nei messaggi REGISTER del protocollo SIP (Session Initiation Protocol), rispetto al metodo di autenticazione corrente solo in Expressway.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione e configurazione CUCM
- Protocollo SIP
- Video Communication Server (VCS) Expressway

### Componenti usati

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

- Cisco Unified Communications Manager versione 11.5 e successive
- Video Communication Server (VCS) Expressway

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

In passato, la registrazione del dispositivo tramite Video Communication Server (VCS) Expressway funziona quando il dispositivo invia nome utente e password tramite il protocollo HTTP (Hypertext Transfer Protocol). Expressway autentica quindi il nome utente e consente al dispositivo di procedere con la registrazione verso CUCM senza ulteriori verifiche.

Il nuovo comportamento è che ora CUCM controlla il messaggio SIP REGISTER e garantisce che l'UserID abbia un'associazione corretta al dispositivo. Tramite questa funzione, l'ID utente deve essere autorizzato prima della registrazione nel CUCM; fornisce pertanto il livello successivo di protezione dal dispositivo proveniente da una rete esterna/sconosciuta. Ciò garantisce che il registro SIP sia autorizzato, ovvero che solo un dispositivo valido associato all'utente valido debba registrarsi. Se al dispositivo non è associato alcun ID utente, la registrazione viene rifiutata con il codice di risposta 401.

Cronologia sfondo

- [CSCu97283](#)
- [ID CVE CVE-2015-6410](#)

Limitazioni

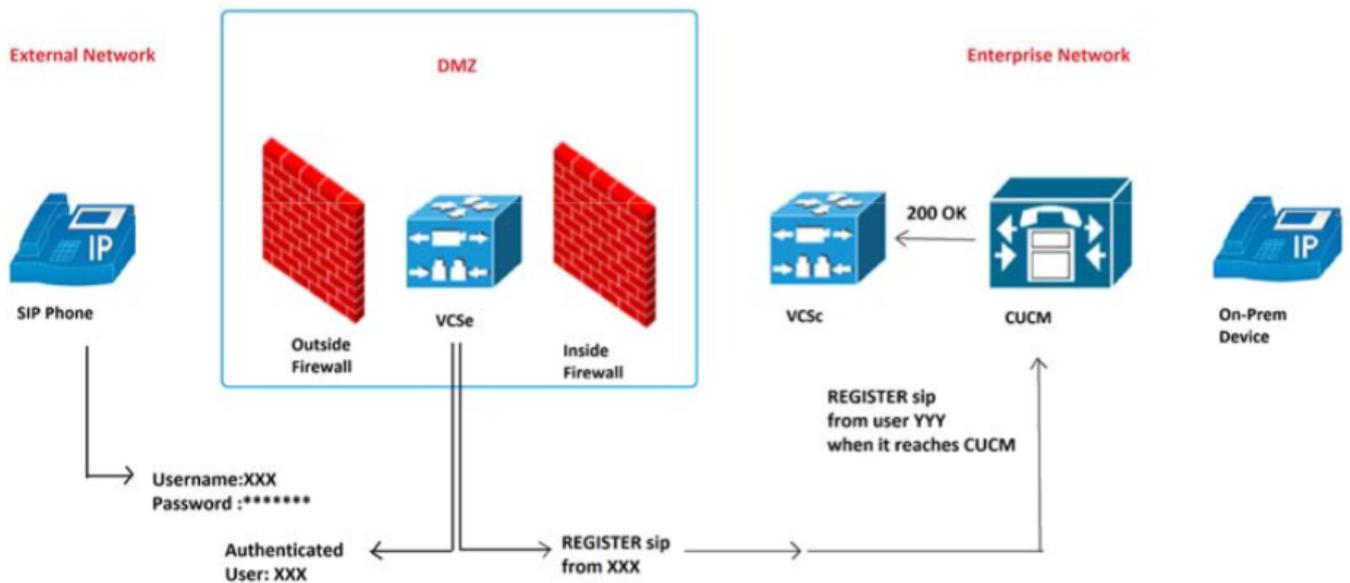
- Influisce solo sui telefoni SIP
- Le registrazioni locali non sono interessate

## Configurazione

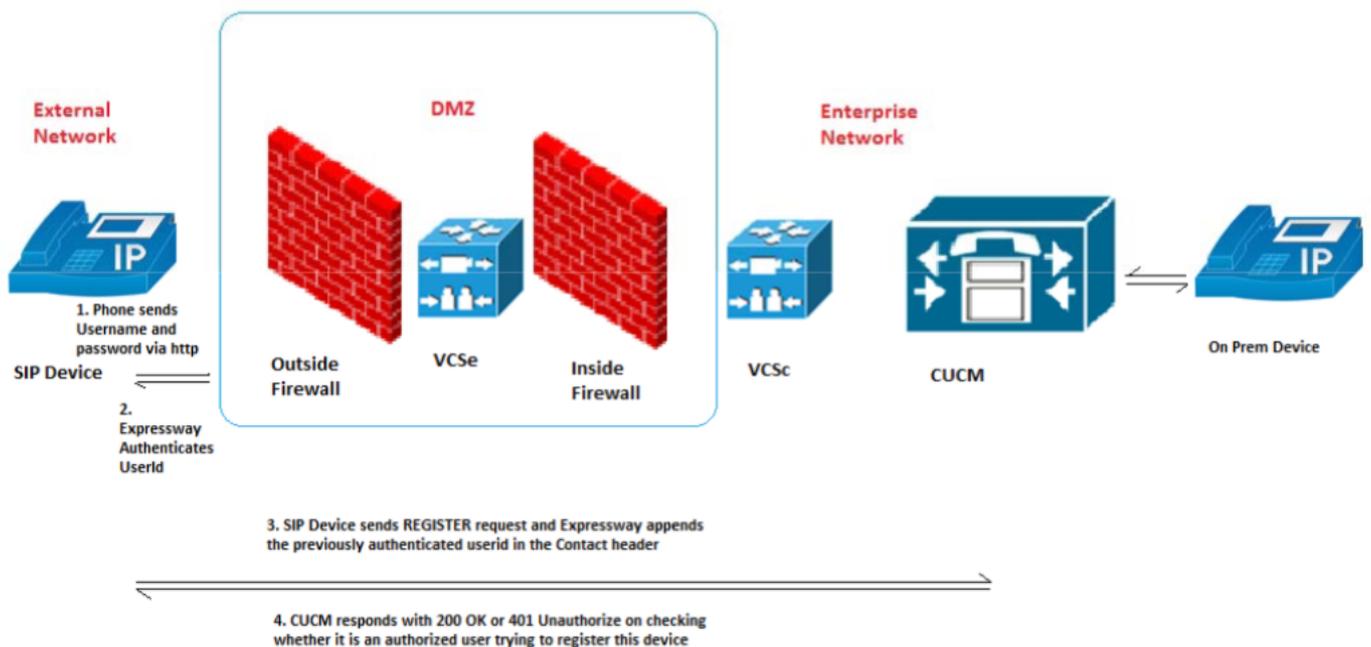
### Esempio di rete

Componenti usati (vecchia o nuova architettura)

Immagine comportamento precedente:



Nuova immagine comportamento:



## Configurazioni

Nuovo parametro del servizio per attivare/disattivare questa funzionalità: **Sistema > Parametri servizio > server > Cisco CallManager > Autorizzazione registrazione SIP abilitata**

Valori:

- True - (predefinito)
- Falso

La corretta associazione dell'ID utente al dispositivo corretto determina se la registrazione SIP è autorizzata o rifiutata.

La richiesta di registrazione del processo di autorizzazione prevede gli scenari seguenti:

Scenario 1. Se l'ID utente non è presente nel messaggio REGISTER, deve essere autorizzato e viene inviato 200 OK.

Nota: Ciò garantisce l'interoperabilità in locale e la compatibilità con le versioni precedenti di Expressway.

Scenario 2. Se nel messaggio REGISTER è presente l'ID utente...

- SE l'ID utente corrisponde al campo dell'ID proprietario nella pagina Configurazione telefono CUCM, THEN Autorizza e invia 200 OK
- SE l'ID utente corrisponde all'associazione dell'ID utente al dispositivo nella pagina Configurazione utente finale CUCM, QUINDI Autorizza e invia 200 OK
- SE il campo dell'ID del proprietario è vuoto e l'associazione del dispositivo all'utente finale non esiste, THEN Autorizza e invia 200 OK
- ELSE IF no match, THEN FAIL e send 401 Unauthorized

Scenario 3. Se il messaggio REGISTER contiene più ID utente di valori diversi, THEN FAIL e send 401 Unauthorized.

Nota: Solo Expressway popola queste intestazioni UserID

#### Tabella Risultati Use Case

Numero	Test case	Autorizzazione registrazione SIP abilitata	Risultato previsto
1	Il parametro UserID nell'intestazione del contatto non è presente	Vero	Authorize (200 OK)
2	Il parametro UserID nell'intestazione del contatto corrisponde a OwnerId nella pagina di configurazione del telefono	Vero	Authorize (200 OK)
3	Il parametro UserID nell'intestazione del contatto corrisponde all'ID utente associato a un dispositivo nella pagina EndUser.	Vero	Authorize (200 OK)
4	L'ID utente nell'intestazione del contatto corrisponde all'ID proprietario nella pagina di configurazione del telefono, non corrisponde all'ID utente configurato nella pagina Utente finale	Vero	Authorize (200 OK)
5	L'ID utente nell'intestazione del contatto corrisponde all'ID utente nella pagina Utente finale, non corrisponde all'ID proprietario nella pagina Configurazione telefono	Vero	Authorize (200 OK)
6	OwnerId nella pagina Phone Config è vuoto e nessun utente associato al dispositivo nella pagina EndUser	Vero	Authorize (200 OK)
7	OwnerId nella pagina Phone Config e userID configurati per un dispositivo nella pagina EndUser, ma nessuna corrispondenza trovata	Vero	401 Non autorizzato
8	Nell'intestazione del contatto sono presenti più ID utente.	Vero	401 Non autorizzato

9	Più ID utente configurati per un dispositivo nella pagina Utente finale	Vero	Autorizza (200 Ok)
10	ID utente senza escape	Vero	Autorizza (200 Ok)
11	Aggiorna registro	Vero	Uguale al messaggio di registro iniziale
12	L'ID utente nell'intestazione del contatto è una stringa vuota, l'ID proprietario e l'ID utente non sono configurati per il dispositivo	Vero	Autorizza (200 Ok)
13	L'ID utente nell'intestazione del contatto è una stringa vuota. ID proprietario/ID utente configurato per il dispositivo	Vero	401 Non autorizzato
14	L'ID utente è presente nell'intestazione del contatto, ma non è stata trovata alcuna corrispondenza	Falso	200 OK
15	Nell'intestazione del contatto sono presenti più ID utente	Falso	200 OK
16	L'ID utente nell'intestazione del contatto è una stringa vuota. ID proprietario /ID utente configurato per il dispositivo	Falso	200 OK

Abilitare la funzionalità tramite il parametro del servizio di Communications Manager (CCM). È attivata per impostazione predefinita e non sono necessarie ulteriori configurazioni.

<a href="#">Send 181 Call Is Being Forwarded *</a>	False	False
<a href="#">Delay Sending 181 until 180/183 message is received *</a>	True	True
<a href="#">Fail Call Over SIP Trunk if MTP Allocation Fails *</a>	False	False
<a href="#">Log Call-Related REFER/NOTIFY/SUBSCRIBE SIP Messages for Session Trace *</a>	True	True
<a href="#">Port Received Timer for Outbound Call Setup *</a>	2	2
<b>SIP Registration Authorization Enabled *</b>	True	True

There are hidden parameters in this group. Click on Advanced button to see hidden parameters.

Clusterwide Parameters (Feature - General)

## Verifica

### Intestazione contatto

CUCM verifica l'intestazione del contatto del messaggio REGISTER per la modifica tramite Expressway

```
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="mjavier";+u.sip!serialno.ccm.cisco.com=A1AZ20D00153;audio=TRUE;video=TRUE;mobility="fixed";duplex="full";description="TANDBERG-SIP"
```

### Nuovo allarme (AuthorizationErrorwithWarningLevel)

È ora disponibile un nuovo allarme (AuthorizationErrorwithWarningLevel) in caso di errore di autorizzazione registrazione SIP

34	SourceVerificationForSoftwareMediaDevicesFailure - This applies to Annunciator (ANN) and Music on Hold (MOH) servers only. When the enterprise parameter Cluster Security Mode is set to 1 (mixed mode) and the Unified CM service parameter Enable Source Verification for Software Media Devices is set to True, the source IP address of an ANN or MOH server will be verified to be one of the Unified CM nodes in the cluster. When this alarm occurs with value 34 as the reason, it means that the IP address of the ANN or MOH server is not a recognized node in the cluster. Because ANN or MOH servers currently can only be installed on a Unified CM node, an unknown server that registers an untrusted device as an ANN or MOH server could indicate a security breach. The IP address of the device trying to register is included as part of the alarm; use the IP address to determine whether an unapproved server is attempting to register or if a network address translation (NAT) error occurred because a firewall device is in the network path between the Unified CM nodes.
35	AuthorizationError - (SIP devices only) Device registration failed due to one of the following reasons: 1) userid in the Contact header of SIP REGISTER message does not match with any of the configured values in Unified CM (Owner User ID in phone configuration page and User ID associated with the device in EndUser page); or 2) If there are more than one userid present in the Contact header of SIP REGISTER message, that is considered as a security risk. Check the CUCM configuration as mentioned above to see whether authorized user is trying to register this particular device.

## Risoluzione dei problemi

Cerca tentativi di autorizzazione nell'output di debug di Tracce CCM

Esempi di autorizzazioni riuscite:

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
```

Esempio di autorizzazione e allarme non riusciti:

```
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=
```