# Configurar registros SIP para autenticar e autorizar por usuário (MRA) para CUCM 11.5

## Contents



## Introduction

Este documento descreve o comportamento aprimorado no Cisco Unified Communications Manager (CUCM) que fornece uma camada adicional de autenticação UserID nas mensagens de REGISTER do Session Initiation Protocol (SIP) versus o método atual de autenticação somente no Expressway.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração e configuração do CUCM
- Protocolo SIP
- VCS (Video Communication Server, servidor de comunicação por vídeo) Expressway

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Unified Communications Manager 11.5 e posterior
- VCS (Video Communication Server, servidor de comunicação por vídeo) Expressway

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

### Informações de Apoio

Antigamente, o registro de dispositivos através do Video Communication Server (VCS) Expressway funciona quando o dispositivo envia nome de usuário e senha via HTTP. O Expressway autentica o nome de usuário e permite que o dispositivo continue com o registro em direção ao CUCM sem mais verificação.

O novo comportamento é que agora o CUCM verifica a mensagem SIP REGISTER e garante que o ID de usuário tenha a associação adequada ao dispositivo. Por meio desse recurso, a ID de usuário deve autorizar antes de se registrar no CUCM; portanto, fornece o próximo nível de proteção contra o dispositivo de rede externa/desconhecida. Isso garante que o SIP REGISTER seja autorizado, ou seja, apenas um dispositivo válido associado ao usuário válido deve se registrar. Se não houver associação de ID de usuário ao dispositivo, o registro será rejeitado com o código de resposta 401.

Histórico do plano de fundo

- CSCuu97283
- CVE ID CVE-2015-6410

Limitações

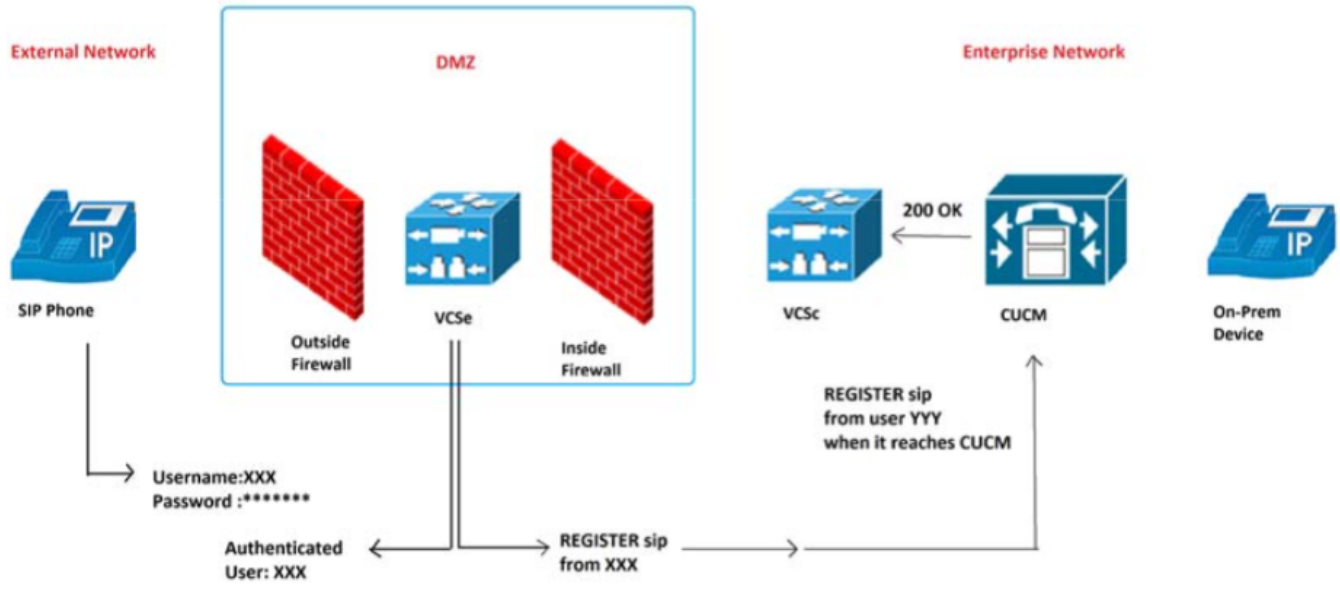
- Apenas afeta telefones SIP
- Os registros no local não são afetados

# Configurar

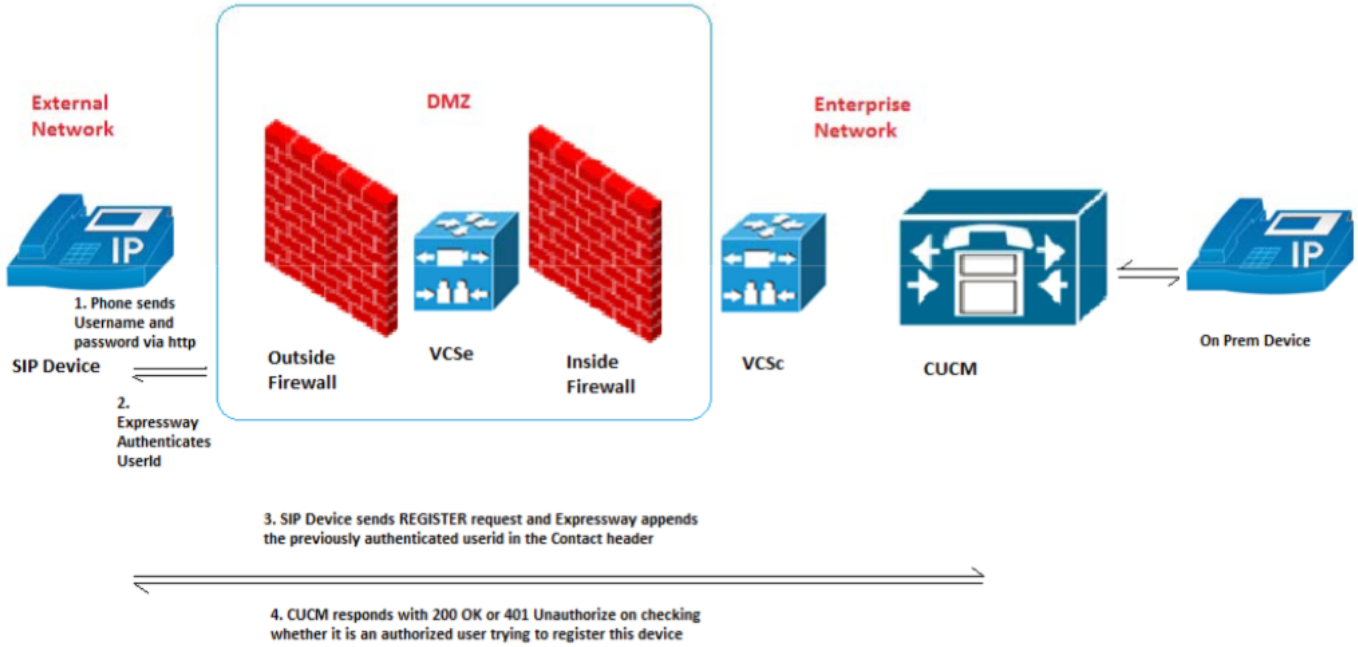
## Diagrama de Rede

Componentes usados (antiga versus nova arquitetura)

Imagem de comportamento antiga:



Nova imagem de comportamento:




## Configurações

Novo parâmetro de serviço para ativar/desativar esta funcionalidade: **System > Service Parameters > *server* > Cisco CallManager > SIP Registration Authorization Enabled**

Valores:

- Verdadeiro - (padrão)
- Falso

A associação correta de ID de usuário ao dispositivo correto determina se o registro SIP autoriza ou rejeita.

A solicitação do processo de autorização de registro segue estes cenários:

Cenário 1. Se UserID não estiver presente na mensagem REGISTER, ela deverá autorizar e 200 OK será enviado.

Note: Isso garante interoperabilidade no local e compatibilidade com versões anteriores do Expressway mais antigas.

Cenário 2. Se UserID estiver presente na mensagem REGISTER, então...

- SE ID de usuário corresponder ao campo ID de proprietário na página Configuração do telefone CUCM, EM SEGUIDA, Autorize e envie 200 OK
- SE ID de usuário corresponder à associação ID de usuário com o dispositivo na página Configuração do usuário final do CUCM, EM SEGUIDA, autorize e envie 200 OK
- SE ambos os campos owner-id estiverem em branco e a associação do dispositivo ao usuário final não existir, ENTÃO autorize e envie 200 OK
- ELSE se não houver correspondência, ENTÃO FALHA e envie 401 Não autorizado

Cenário 3. Se a mensagem REGISTER contiver mais de um ID de usuário de valores diferentes,

ENTÃO FALHA e envie 401 Não autorizado.

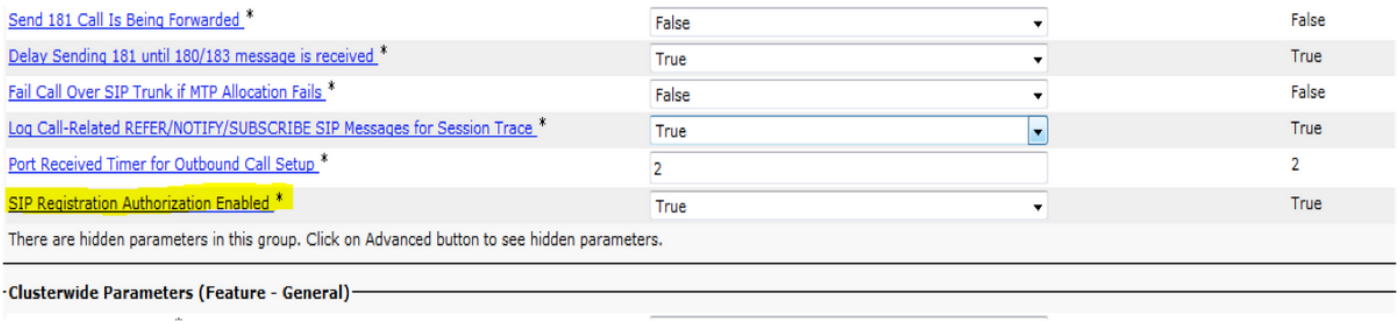
Note: Somente o Expressway preenche esses cabeçalhos UserID

Tabela de resultados de casos de uso

| Número | Casos de teste | Autorização de registro SIP habilitada | Resultado esperado |
|---|---|---|---|
| 1 | O parâmetro UserId no cabeçalho do contato não está presente | Verdadeiro | Autorizar (200 OK) |
| 2 | O parâmetro UserId no cabeçalho do contato corresponde ao OwnerId na página de configuração do telefone | Verdadeiro | Autorizar (200 OK) |
| 3 | O parâmetro UserId no cabeçalho do contato corresponde a userId associado a um dispositivo na página EndUser. | Verdadeiro | Autorizar (200 OK) |
| 4 | O ID de usuário no cabeçalho do contato corresponde ao ownerId na página Phone Config, não corresponde ao ID de usuário configurado na página EndUser | Verdadeiro | Autorizar (200 OK) |
| 5 | O ID de usuário no cabeçalho do contato corresponde a userId na página EndUser, não corresponde ao OwnerId na página Phone Config | Verdadeiro | Autorizar (200 OK) |
| 6 | OwnerId na página Phone Config está em branco e o dispositivo não tem nenhum usuário associado na página EndUser | Verdadeiro | Autorizar (200 OK) |
| 7 | OwnerId na página Phone Config e userId configurados para um dispositivo na página EndUser, mas não foi encontrada nenhuma correspondência | Verdadeiro | 401 Não Autorizado |
| 8 | Mais de um ID de usuário presente no cabeçalho do contato. | Verdadeiro | 401 Não Autorizado |
| 9 | ID de usuário múltipla configurada para um dispositivo na página Usuário final | Verdadeiro | Autorizar (200 Ok) |
| 10 | Sem escapamento de userId | Verdadeiro | Autorizar (200 Ok) |
| 11 | Atualizar registro | Verdadeiro | Igual à mensagem de REGISTRO inicial |
| 12 | UserId no cabeçalho do contato é uma string vazia, OwnerId e UserId não configurados para o dispositivo | Verdadeiro | Autorizar (200 Ok) |
| 13 | UserId no cabeçalho do contato é uma string vazia, OwnerId/UserId configurada para o dispositivo | Verdadeiro | 401 Não Autorizado |
| 14 | UserId está presente no cabeçalho do contato, OwnerId/UserId configurado para o dispositivo, mas não foi encontrada nenhuma correspondência | Falso | 200 OK |
| 15 | Mais de um ID de usuário presente no | Falso | 200 OK |

| | | | |
|---|---|---|---|
| 16 | cabeçalho do contato<br>UserId no cabeçalho do contato é uma string vazia, ownerId /UserId configurada para o dispositivo | Falso | 200 OK |

Ative o recurso por meio do parâmetro de serviço do Communications Manager (CCM). Ele está ativado por padrão e nenhuma outra configuração é necessária.




# Verificar

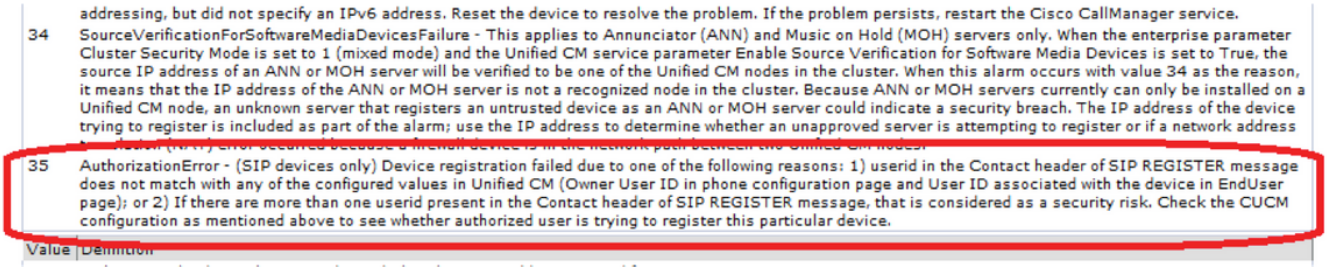
### Cabeçalho do contato

O CUCM verifica o cabeçalho de contato da mensagem REGISTER para modificação pelo 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="mjavie
r";+u.sip!serialno.ccm.cisco.com=A1AZ20D00153;audio=TRUE;video=TRUE;mobility="fixed";
duplex="full";description="TANDBERG-SIP"
```

### Novo Alarme (AuthorizationErrorwithWarningLevel)

Um novo Alarme (AuthorizationErrorwithWarningLevel) está agora disponível quando há falha na autorização de registro SIP




# Troubleshoot

Procurar tentativas de autorização na saída de depuração do CCM Traces

Exemplos de autorização bem-sucedidos:

Cenário 1:

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

Cenário 2:

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

Exemplo de autorização e alarme com falha:

```
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=
```