

为CUCM 11.5配置SIP注册以按用户身份验证和授权(MRA)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍Cisco Unified Communications Manager(CUCM)中的增强行为，该行为在会话初始协议(SIP)REGISTER消息中提供了额外的用户ID身份验证层，而目前仅在Expressway上提供身份验证方法。

先决条件

要求

Cisco 建议您了解以下主题：

- CUCM管理和配置
- SIP协议
- 视频通信服务器(VCS)Expressway

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科统一通信管理器11.5及更高版本
- 视频通信服务器(VCS)Expressway

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

过去，当设备通过超文本传输协议(HTTP)发送用户名和密码时，通过Video Communication

Server(VCS)Expressway进行设备注册会起作用。然后，Expressway对用户名进行身份验证，允许设备继续向CUCM注册，而无需进一步验证。

新行为是，现在CUCM检查SIP REGISTER消息并确保用户ID与设备有正确的关联。通过此功能，UserID在注册到CUCM之前应进行授权；因此，为来自外部/未知网络的设备提供下一级保护。这确保SIP REGISTER已授权，即仅与有效用户关联的有效设备应进行注册。如果没有与设备的用户ID关联，则注册会拒绝401响应代码。

背景历史记录

- [CSCuu97283](#)
- [CVE ID CVE-2015-6410](#)

限制

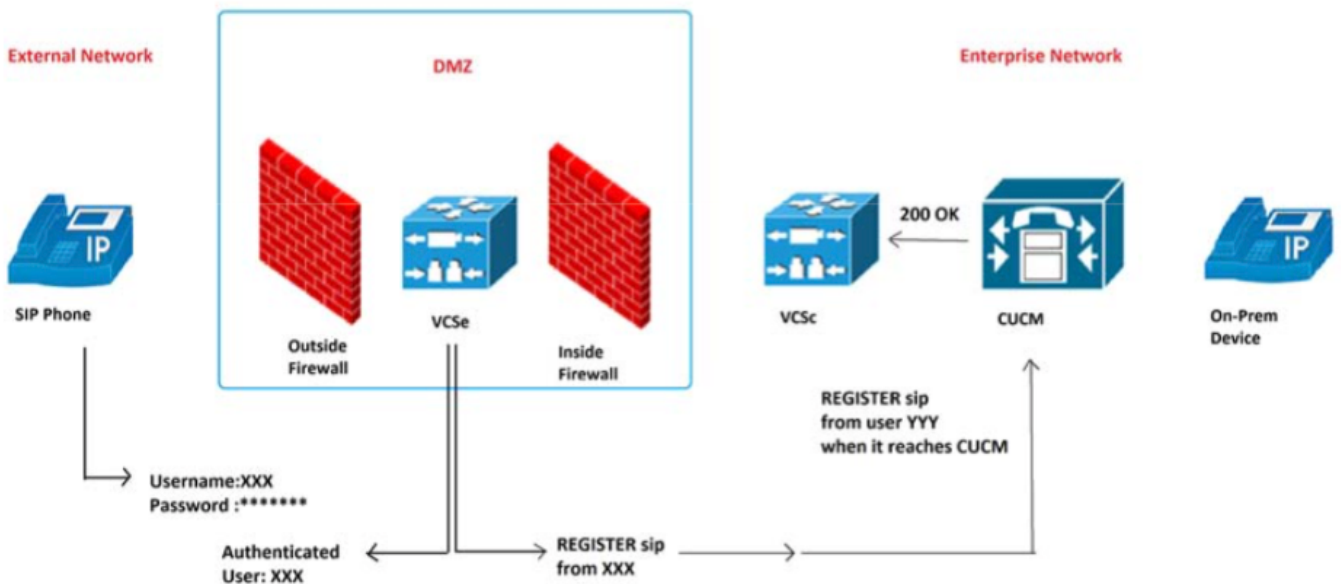
- 仅影响SIP电话
- 本地注册不受影响

配置

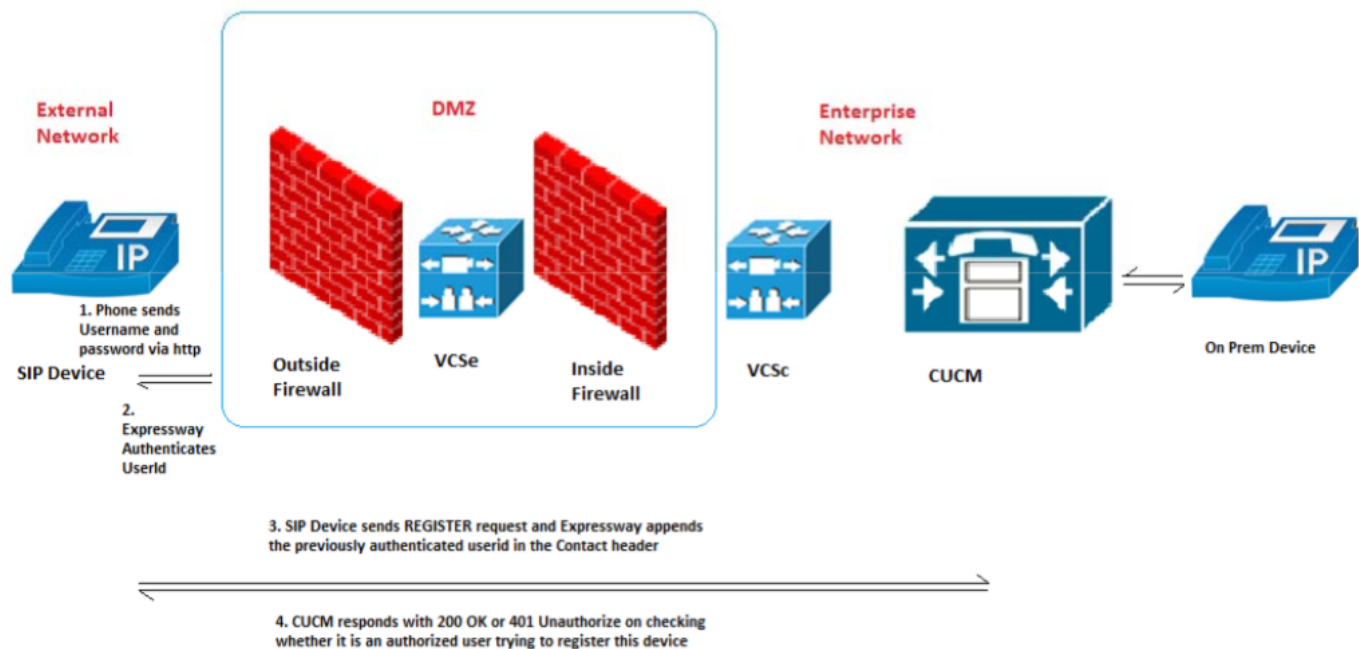
网络图

使用的组件 (旧架构与新架构)

旧行为图像：



新行为图像：



配置

新服务参数，用于打开/关闭此功能：**系统>服务参数>服务器> Cisco CallManager > SIP注册授权已启用**

价值:

- True — (默认)
- 错误

正确的用户ID与正确设备的关联决定了SIP注册是授权还是拒绝。

注册授权流程请求遵循以下场景：

场景1.如果REGISTER消息中不存在UserID，则应授权并发送200 OK。

注意：这可确保内部互操作性和向后兼容较旧的Expressway版本。

场景2.如果REGISTER消息中存在UserID，则.....

- 如果用户ID与CUCM电话配置页面的owner-id字段匹配，则授权并发送200 OK
- 如果用户ID与CUCM最终用户配置页面中的设备的用户ID关联匹配，则授权并发送200 OK
- 如果所有者ID字段为空且设备与最终用户的关联不存在，则授权并发送200 OK
- 否则，如果不匹配，则失败并发送401未授权

场景3.如果REGISTER消息包含多个不同值的用户ID，则失败并发送401未授权。

注意：只有Expressway填充这些用户ID报头

使用案例结果表

编号	测试用例	已启用SIP注册授权	预期结果
1	联系人信头中的UserId参数不存在	真	授权 (200 OK)

2	联系人信头中的UserId参数与电话配置页中的OwnerId匹配	真	授权 (200 OK)
3	联系人标题中的UserId参数与“最终用户”页中与设备关联的用户ID匹配。	真	授权 (200 OK)
4	联系人标题中的UserId与“电话配置”页中的ownerId匹配，与“最终用户”页中配置的用户Id不匹配	真	授权 (200 OK)
5	联系人标题中的UserId与“最终用户”页中的userId匹配，与“电话配置”页中的OwnerId不匹配	真	授权 (200 OK)
6	“电话配置”页中的OwnerId为空，并且设备在“最终用户”页中没有关联用户	真	授权 (200 OK)
7	在“电话配置”页中为设备配置的OwnerId和在“最终用户”页中为设备配置的用户ID，但未找到匹配项	真	401未授权
8	联系人信头中存在多个用户ID。	真	401未授权
9	在“最终用户”(EndUser)页面中为设备配置多个用户ID	真	授权 (200确定)
10	取消转义userId	真	授权 (200确定)
11	刷新注册	真	与初始注册消息相同
12	联系人信头中的UserId为空字符串，未为设备配置OwnerId和UserId	真	授权 (200确定)
13 个	联系人信头中的UserId为空字符串，为设备配置了OwnerId/UserId	真	401未授权
14	UserId存在于为设备配置的联系人标题OwnerId/UserId中，但未找到匹配项	错误	200 OK
15	联系人信头中存在多个用户ID	错误	200 OK
16	联系人信头中的UserId为空字符串，为设备配置了ownerId /UserId	错误	200 OK

通过Communications Manager(CCM)Service Parameter启用该功能。默认情况下，它处于打开状态，无需进一步配置。

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

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

Clusterwide Parameters (Feature - General)

验证

联系人信头

CUCM检查REGISTER消息的联系人报头，以便Expressway进行修改

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"
```

新警报(AuthorizationErrorwithWarningLevel)

当SIP注册授权失败时，现在可以使用新警报(AuthorizationErrorwithWarningLevel)

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 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.

故障排除

在CCM跟踪调试输出中查找授权尝试

成功授权示例：

情形 1：

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

方案 2：

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

授权和警报失败示例：

```
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=
```