Configure SIP Registrations to Authenticate and Authorize on a Per-user Basis (MRA) for CUCM 11.5

Contents

Introduction

This document describes enhanced behavior in Cisco Unified Communications Manager (CUCM) that provides an additional layer of UserID authentication in the Session Initiation Protocol (SIP) REGISTER messages versus the current method of authentication only at the Expressway.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CUCM Administration and Configuration
- SIP Portocol
- Video Communication Server (VCS) Expressway

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Unified Communications Manager 11.5 and later
- Video Communication Server (VCS) 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. If your network is live, Ensure that you understand the potential impact of any command.

Background Information

In the past, device registration through Video Communication Server (VCS) Expressway works when the device sends username and password via Hypertext Transfer Protocol (HTTP). Expressway then authenticates the username and allows the device to proceed with the registration towards CUCM without further verification.

The new behavior is that now CUCM checks the SIP REGISTER message and ensures the UserID has proper association to the device. Through this feature the UserID should authorize before it registers into the CUCM; therefore, provides the next level of protection against the device from external/unknown network. This ensures that the SIP REGISTER is authorized, i.e only a valid device associated with the valid user should register. If there is no UserID association to the device then registration rejects with 401 response code.

Background History

- CSCuu97283
- CVE ID CVE-2015-6410

Limitations

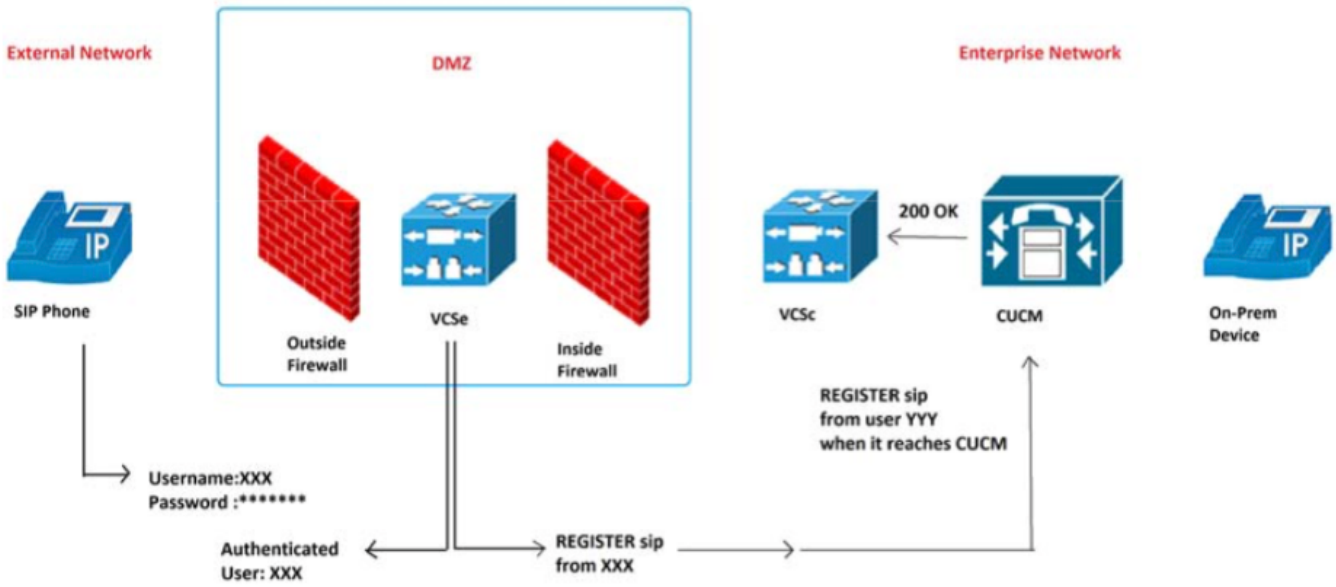
- Only affects SIP Phones
- On-Premise registrations are unaffected

Configure

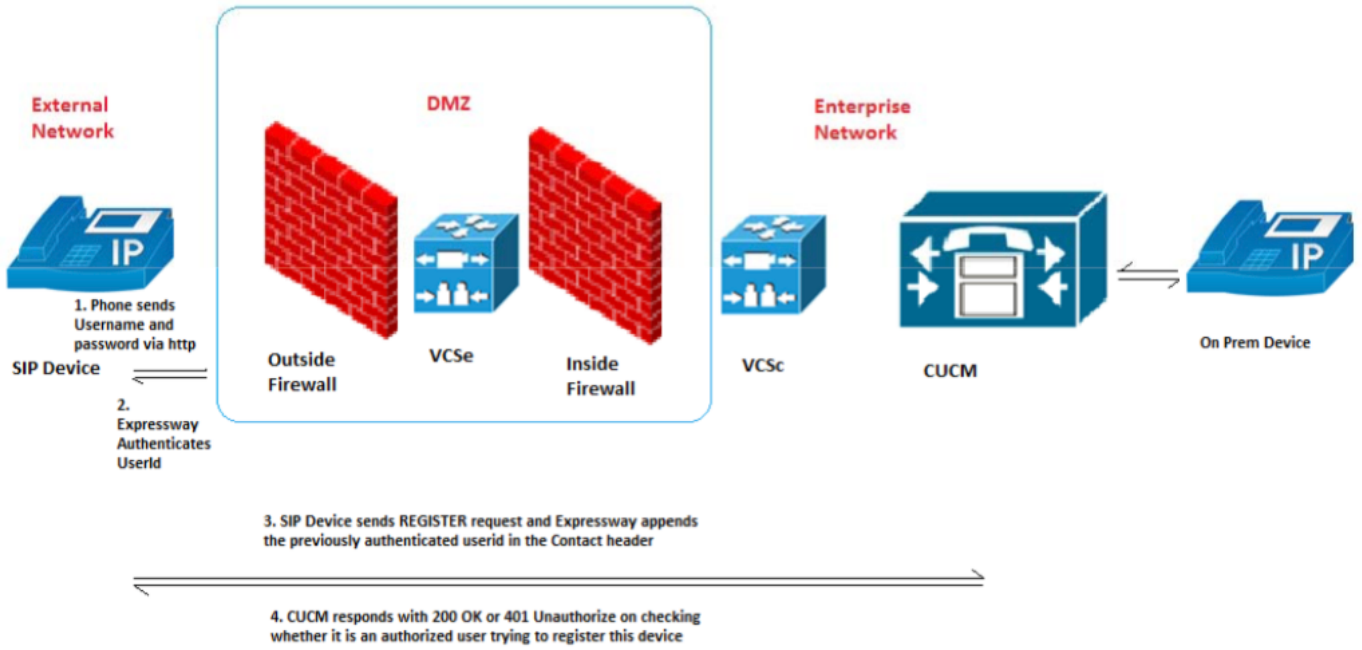
Network Diagram

Components Used (Old vs. New Architecture)

Old behavior image:



New behavior image:



Configurations

New service parameter to toggle this feature on/off: **System > Service Parameters > *server* > Cisco CallManager > SIP Registration Authorization Enabled**

Values:

- True - (default)
- False

The correct UserID association to the correct device determines if SIP registration authorizes or rejects.

The registration authorization process request follows these scenarios:

Scenario 1. If UserID is not present in the REGISTER message it should authorize and 200 OK is sent.

Note: This ensures on-prem interoperability and backward compatibility with older Expressway versions.

Scenario 2. If UserID is present in the REGISTER message then...

- IF UserID matches owner-id field in CUCM Phone Configuration page, THEN Authorize and send 200 OK
- IF UserID matches UserID association with the device in the CUCM End User Configuration page, THEN Authorize and send 200 OK
- IF both owner-id field is blank and device association to the End User does not exist, THEN Authorize and send 200 OK
- ELSE IF no match, THEN FAIL and send 401 Unauthorized

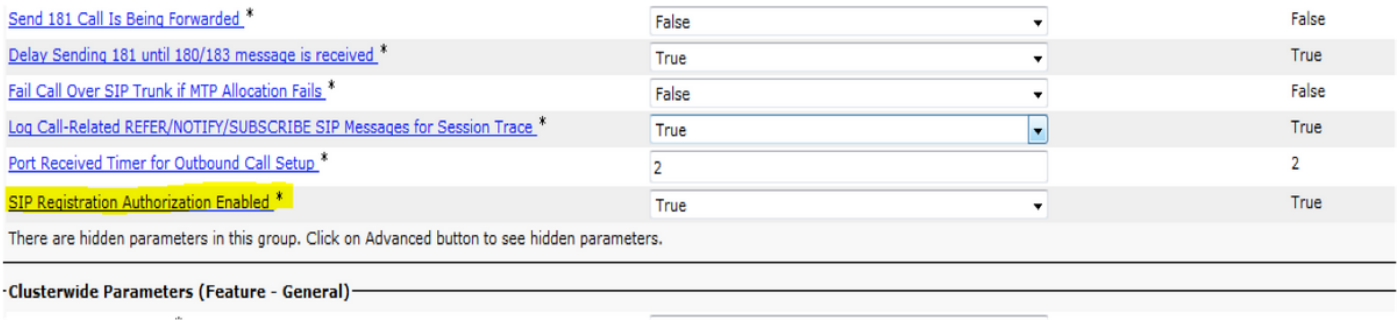
Scenario 3. If REGISTER message contains more than one UserID of different values, THEN FAIL and send 401 Unauthorized.

Note: Only Expressway populate these UserID headers

Use Cases Results Table

Number	Test Cases	SIP Registration Authorization Enabled	Expected Result
1	UserId parameter in the contact header is not present	True	Authorize (200 OK)
2	UserId parameter in the contact header matches with OwnerId in phone config page	True	Authorize (200 OK)
3	UserId parameter in the contact header matches with userId associated to a device in EndUser page.	True	Authorize (200 OK)
4	UserId in contact header matches with ownerId in Phone Config page, does not match with userId configured in EndUser page	True	Authorize (200 OK)
5	UserId in contact header matches with userId in EndUser page, does not match with OwnerId in Phone Config page	True	Authorize (200 OK)
6	OwnerId in Phone Config page is blank and device has no user associated in EndUser page	True	Authorize (200 OK)
7	OwnerId in Phone Config page and userId configured for a device in EndUser page, but no match found	True	401 Unauthorized
8	More than one userid present in the contact header.	True	401 Unauthorized
9	Multiple userId configured for a device in EndUser page	True	Authorize (200 Ok)
10	Unescaping userId	True	Authorize (200 Ok)
11	Refresh register	True	Same as Initial REGISTER message
12	UserId in contact header is empty string, OwnerId and UserId not configured for the device	True	Authorize (200 Ok)
13	UserId in contact header is empty string, OwnerId/UserId configured for the device	True	401 Unauthorized
14	UserId is present in the contact header, OwnerId/UserId configured for the device, but no match found	False	200 OK
15	More than one userId present in the contact header	False	200 OK
16	UserId in contact header is empty string, ownerId /UserId configured for the device	False	200 OK

Enable the feature via Communications Manager (CCM) Service Parameter. It is on by default and no further configuration is required.



Verify

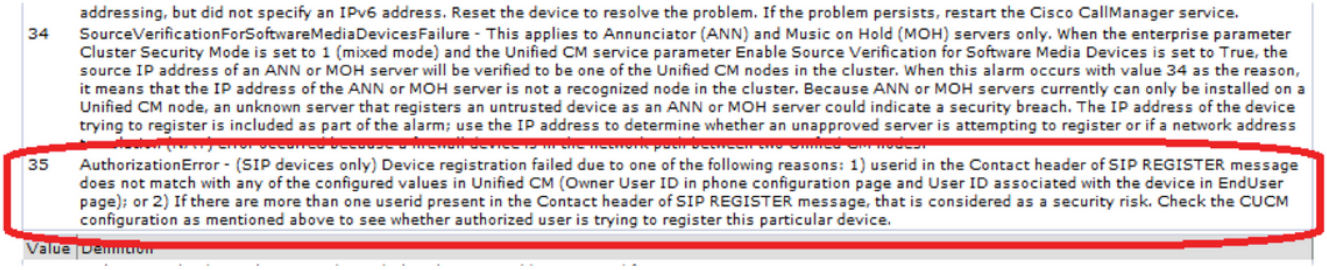
Contact Header

CUCM checks the Contact header of REGISTER message for modification by 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"
```

New Alarm (AuthorizationErrorwithWarningLevel)

A new Alarm (AuthorizationErrorwithWarningLevel) is now available when there is SIP Registration Authorization failure



Troubleshoot

Look for authorization attempts in CCM Traces debug output

Successful Authorization examples:

Scenario 1:

```
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"
```

Scenario 2:

```
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‟

Failed Authorization and Alarm example:

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‟