Konfigurieren von SIP-Registrierungen zur Authentifizierung und Autorisierung pro Benutzer (MRA) für CUCM 11.5

Inhalt

Einführung

Dieses Dokument beschreibt ein verbessertes Verhalten in Cisco Unified Communications Manager (CUCM), das eine zusätzliche Ebene der UserID-Authentifizierung in den SIP-REGISTERN-Nachrichten (Session Initiation Protocol) gegenüber der aktuellen Authentifizierungsmethode nur auf dem Expressway bietet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CUCM-Administration und -Konfiguration
- SIP-Protokoll
- Video Communication Server (VCS) Expressway

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Unified Communications Manager 11.5 und höher
- Video Communication Server (VCS) Expressway

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

In der Vergangenheit funktioniert die Geräteregistrierung über Video Communication Server (VCS) Expressway, wenn das Gerät Benutzernamen und Kennwort über das Hypertext Transfer Protocol (HTTP) sendet. Expressway authentifiziert dann den Benutzernamen und ermöglicht es dem Gerät, die Registrierung zum CUCM ohne weitere Überprüfung fortzusetzen.

Das neue Verhalten ist, dass CUCM jetzt die SIP-REGISTER-Nachricht überprüft und sicherstellt, dass die Benutzer-ID dem Gerät ordnungsgemäß zugeordnet ist. Mithilfe dieser Funktion sollte die Benutzer-ID autorisiert werden, bevor sie sich beim CUCM anmeldet. bietet daher den nächsten Schutz vor dem Gerät vor externen/unbekannten Netzwerken. Dadurch wird sichergestellt, dass der SIP-REGISTER autorisiert ist, d. h. nur ein gültiges Gerät, das dem gültigen Benutzer zugeordnet ist, sollte registriert werden. Wenn keine UserID-Zuordnung zum Gerät besteht, lehnt die Registrierung den Antwortcode 401 ab.

Hintergrundgeschichte

- CSCuu97283
- CVE-ID CVE-2015-6410

Einschränkungen

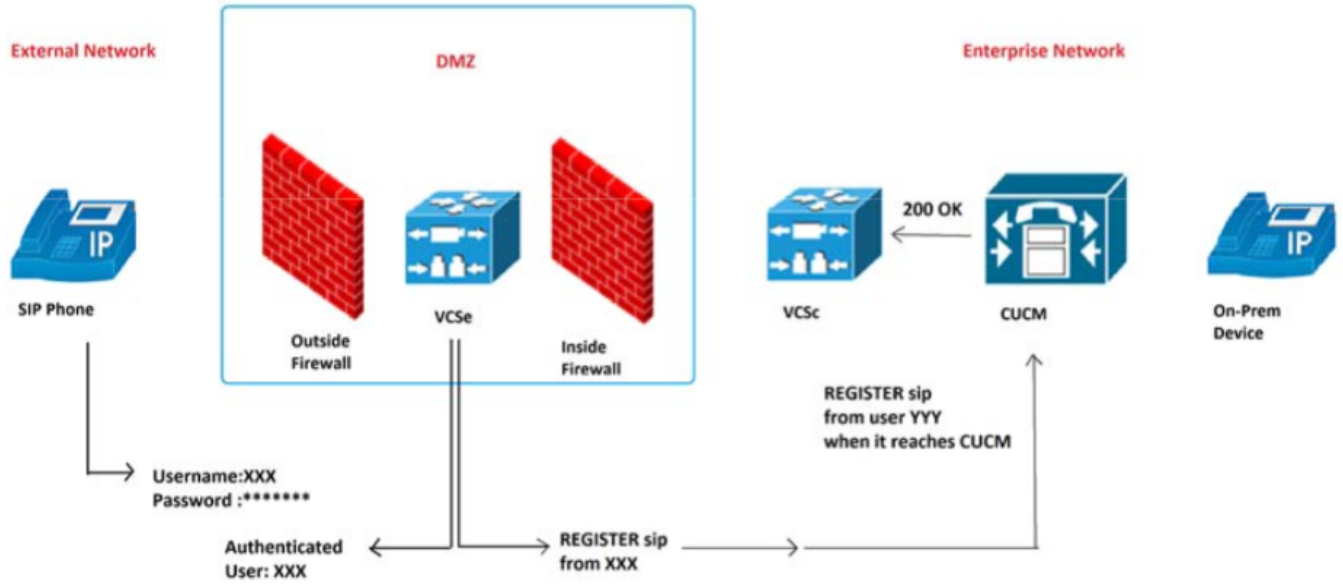
- Betrifft nur SIP-Telefone
- Standortbasierte Registrierungen sind nicht betroffen.

Konfigurieren

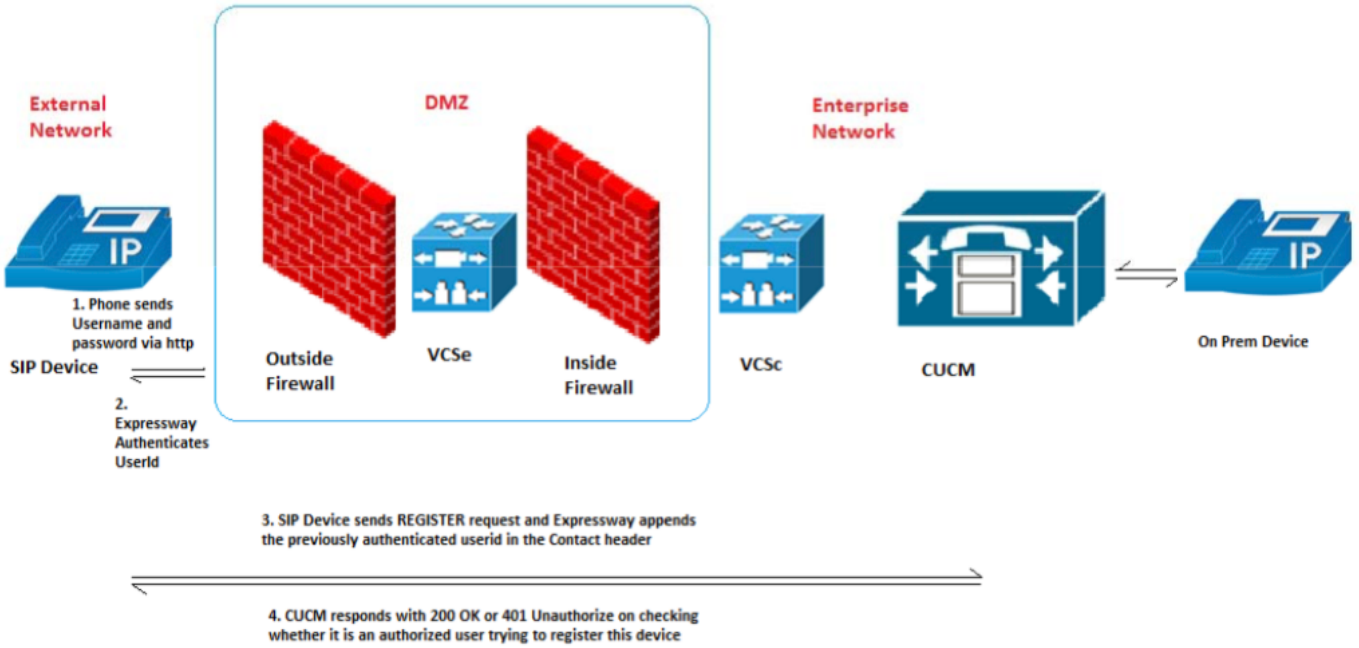
Netzwerkdiagramm

Verwendete Komponenten (alte und neue Architektur)

Altes Verhaltensbild:



Neues Verhaltensbild:



Konfigurationen

Neuer Dienstparameter zum Ein-/Ausschalten dieser Funktion **System > Dienstparameter > *Server* > Cisco CallManager > SIP-Registrierungs-Autorisierung aktiviert**

Werte:

- True - (Standard)
- Falsch

Die richtige UserID-Zuordnung zum richtigen Gerät bestimmt, ob die SIP-Registrierung autorisiert oder abgelehnt wird.

Die Anforderung des Registrierungs-Autorisierungsprozesses folgt folgenden Szenarien:

Szenario 1. Wenn die Benutzer-ID in der REGISTER-Nachricht nicht vorhanden ist, sollte sie autorisiert werden, und 200 OK werden gesendet.

Hinweis: Dadurch wird eine Interoperabilität vor Ort und Abwärtskompatibilität mit älteren Expressway-Versionen gewährleistet.

Szenario 2. Wenn die Benutzer-ID in der REGISTER-Nachricht vorhanden ist,..

- WENN die Benutzer-ID mit dem Feld Owner-ID auf der Seite "CUCM Phone Configuration" (CUCM-Telefonkonfiguration) übereinstimmt, dann 200 OK autorisieren und senden
- WENN die Benutzer-ID mit der Benutzer-ID-Zuordnung des Geräts auf der Seite "CUCM-Endbenutzerkonfiguration" übereinstimmt, autorisieren und senden Sie dann 200 OK.
- Wenn beide Felder für die Eigentümer-ID leer sind und die Gerätezuordnung zum Endbenutzer nicht vorhanden ist, dann autorisieren und senden Sie 200 OK.
- ELSE WENN keine Übereinstimmung, DANN FEHLEN und senden 401 nicht autorisiert

Szenario 3. Wenn die REGISTER-Nachricht mehr als eine UserID mit unterschiedlichen Werten enthält, VERSAGEN SIE THEN FAIL und senden Sie 401 Unauthorized.

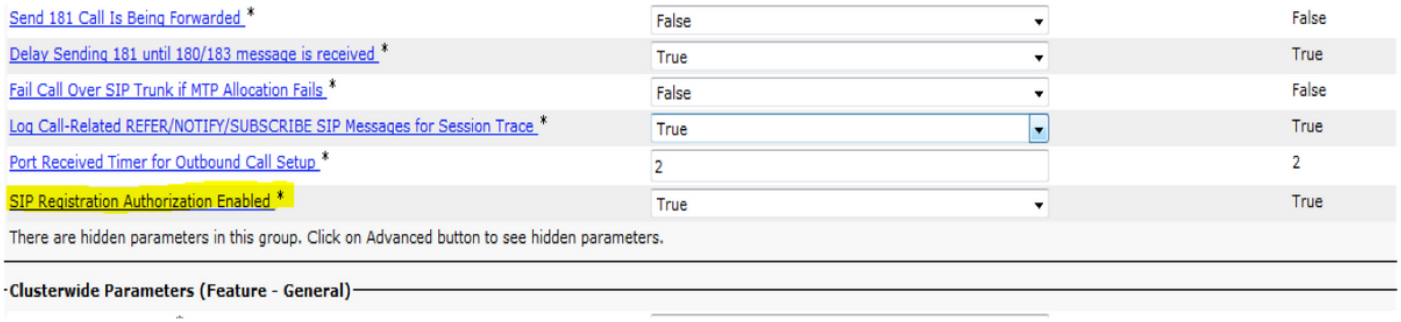
Hinweis: Nur Expressway füllt diese UserID-Header auf.

Use Cases Results Table

Nummer	Testfälle	Autorisierung zur SIP-Registrierung aktiviert	Erwartetes Ergebnis
1	Der UserId-Parameter im Contact-Header ist nicht vorhanden.	Richtig	Autorisieren (200 OK)
2	Der UserId-Parameter im Kontakt-Header stimmt mit der OwnerId auf der Konfigurationsseite des Telefons überein.	Richtig	Autorisieren (200 OK)
1	Der UserId-Parameter im Kontakt-Header stimmt mit der BenutzerID überein, die einem Gerät auf der Seite Endbenutzer zugeordnet ist.	Richtig	Autorisieren (200 OK)
4	Die BenutzerID im Kontakt-Header stimmt mit der OwnerId auf der Seite "Phone Config" (Telefonkonfig.) überein und stimmt nicht mit der auf der Endbenutzer-Seite konfigurierten Benutzer-ID überein.	Richtig	Autorisieren (200 OK)
5	Die BenutzerID im Kontakt-Header stimmt mit der Benutzer-ID auf der Endbenutzer-Seite überein und stimmt nicht mit der OwnerId auf der Seite für die Telefonkonfiguration überein.	Richtig	Autorisieren (200 OK)
6	Die OwnerId auf der Seite "Phone Config" (Telefonkonfiguration) ist leer, und dem Gerät ist auf der Seite "Endbenutzer" kein Benutzer zugeordnet.	Richtig	Autorisieren (200 OK)
7	OwnerId auf der Seite "Phone Config" (Telefonkonfig.) und userId für ein Gerät auf der Seite "End User" (Endbenutzer) konfiguriert, aber keine Übereinstimmung gefunden	Richtig	401 Unautorisiert

8	Mehrere Benutzer-IDs im Kontakt-Header.	Richtig	401 Unautorisiert
9	Auf der Endbenutzerseite für ein Gerät konfigurierte Benutzer-ID	Richtig	Autorisierung (200 OK)
10	Benutzer-ID entschlüsseln	Richtig	Autorisierung (200 OK)
11	Aktualisierungsregister	Richtig	Wie bei der ersten REGISTER-Nachricht
12	UserId im Contact-Header ist eine leere Zeichenfolge, OwnerId und UserId sind für das Gerät nicht konfiguriert.	Richtig	Autorisierung (200 OK)
13	UserId im Contact-Header ist eine leere Zeichenfolge. Die OwnerId/UserId ist für das Gerät konfiguriert.	Richtig	401 Unautorisiert
14	UserID ist im Kontakt-Header vorhanden, OwnerId/UserId ist für das Gerät konfiguriert, aber keine Übereinstimmung gefunden	Falsch	200 OK
15	Mehr als eine Benutzer-ID im Kontakt-Header vorhanden	Falsch	200 OK
16	UserId im Contact-Header ist eine leere Zeichenfolge, ownerId /UserId ist für das Gerät konfiguriert.	Falsch	200 OK

Aktivieren Sie die Funktion über den Communications Manager-Serviceparameter (CCM). Standardmäßig ist sie aktiviert, und es ist keine weitere Konfiguration erforderlich.



Überprüfen

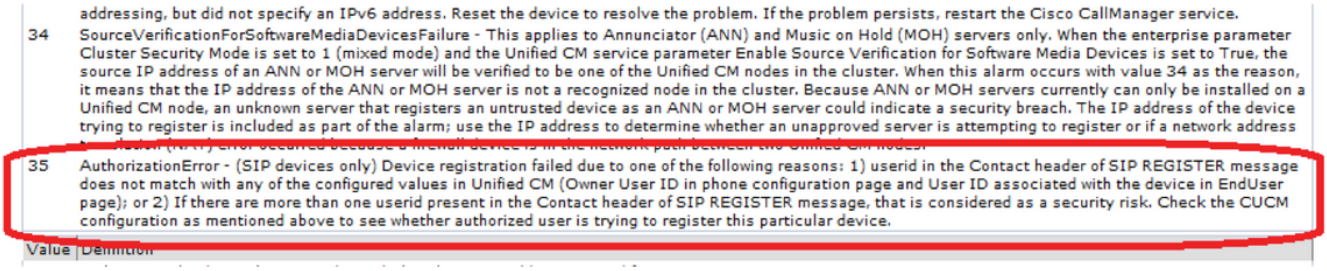
Kopfzeile des Kontakts

CUCM überprüft den Contact-Header der REGISTER-Nachricht auf Änderungen durch 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"
```

Neuer Alarm (AuthorizationErrorWarningLevel)

Ein neuer Alarm (AuthorizationErrorWarningLevel) ist jetzt verfügbar, wenn ein Fehler bei der SIP-Registrierung auftritt.



Fehlerbehebung

Suchen nach Autorisierungsversuchen in der Debugausgabe von CCM Traces

Erfolgreiche Autorisierungsbeispiele:

Szenario 1:

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

Szenario 2:

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

Autorisierung fehlgeschlagen und Alarm:

```
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=
```