



# **Pexip Infinity and Cisco UCM**

## **Deployment Guide**

**Software Version 32**

**Document Version 32.a**

**June 2023**

**] pexip [**

# Contents

|                                    |   |
|------------------------------------|---|
| Introduction .....                 | 2 |
| Pexip Infinity configuration ..... | 3 |
| CUCM configuration .....           | 3 |
| Testing the deployment .....       | 6 |

## Introduction

The Cisco Unified Communications Manager (CUCM) is a SIP registrar and call control device. This guide describes how to integrate a single Pexip Infinity location with a single CUCM by setting up a SIP trunk between the two systems, so that calls can be routed between endpoints registered to the CUCM, and the Pexip Infinity platform.

In larger deployments where you may have multiple CUCM nodes, and where you have a distributed Pexip Infinity architecture with many Conferencing Nodes deployed across various locations in your network, you should ensure that calls from CUCM-registered devices are routed to their nearest Pexip Infinity Conferencing Nodes when they dial a Virtual Meeting Room alias.

Please contact your Pexip authorized support representative if you want help in designing a distributed setup with Pexip Infinity and CUCM.

## Prerequisites

This guide assumes that you are familiar with CUCM.

It assumes that Pexip Infinity and CUCM have been deployed successfully, configured with basic settings (such as an IP address, DNS and NTP servers) and are able to route calls. It also assumes that Pexip Infinity has been configured with Virtual Meeting Rooms and associated aliases appropriate to your dial plan. For complete information on how to configure your Pexip Infinity solution, see the Pexip Infinity technical documentation website at [docs.pexip.com](https://docs.pexip.com).

## Example deployment scenario

The examples used in this guide assume a dial plan where all Virtual Meeting Room aliases are in one of the following two formats:

- `meet.<name>@example.com`
- `555<extension>@example.com`

It assumes that a Virtual Meeting Room, named `meet.alice`, has been configured with two aliases: `meet.alice@example.com` and `555123@example.com`.

Note that Pexip Infinity supports aliases that include a domain (e.g. `555123@example.com`), as well as aliases without a domain (e.g. just `555123`). To match a received destination alias that includes a domain, the aliases configured within Pexip Infinity must also include the same domain. If an alias configured on Pexip Infinity does not include a domain:

- calls to `<alias>` without any domain portion (e.g. `555123`) will be matched
- calls to `<alias>@<IPaddress>` (e.g. `555123@192.0.2.0`) will be matched
- calls to `<alias>@<domain>` (e.g. `555123@example.com`) will not be matched.

Depending on your dial plan, you may need to configure CUCM's Call Routing to ensure the Virtual Meeting Room aliases are in the expected format when received by Pexip Infinity.

## Pexip Infinity configuration

In these steps, you configure Pexip Infinity to use CUCM as the SIP proxy it will use for outbound calls from the desired Pexip Infinity location. It involves:

- [Adding a SIP proxy](#)
- [Assigning the SIP proxy to a location](#)

### Adding a SIP proxy

To add CUCM as a SIP proxy:

1. Go to **Call Control > SIP Proxies**.
2. Select **Add SIP proxy**.
3. Complete the following fields:

| Option           | Input   |
|------------------|---|
| Name             | Enter the name you want to use to refer to this SIP proxy. This example uses <b>CUCM</b> .  |
| Description      | Enter a description of the SIP proxy. This example uses <b>SIP proxy to CUCM</b> .  |
| Address          | Enter the IP address or FQDN of the CUCM.   |
| Port / Transport | Depending on your security policy, select either: <ul style="list-style-type: none"><li>◦ Port of <b>5060</b> and Transport of <b>TCP</b></li><li>◦ Port of <b>5061</b> and Transport of <b>TLS</b></li></ul> |

4. Select **Save**.

### Assigning the SIP proxy to a location

This is only required if the CUCM is the only route for outgoing calls from Pexip Infinity for the location.

To nominate CUCM as the SIP proxy to be used for outbound calls from a Pexip Infinity location:

1. Go to **Platform > Locations**.
2. Select the location.
3. From the **SIP proxy** drop-down menu, select the name of the SIP proxy added earlier (**CUCM** in this example).
4. Select **Save**.

## CUCM configuration

This section lists the tasks required to configure CUCM so that it can be integrated with one Pexip Infinity location. Each task is described in full in the sections that follow:

- [Uploading TLS certificates \(TLS only\)](#)
- [Creating a SIP trunk security profile \(TLS only\)](#)
- [Creating a SIP profile for Pexip Infinity \(optional\)](#)
- [Creating a SIP trunk](#)
- [Configuring the dial plan for calls from CUCM to Pexip Infinity](#)
- [Adding a SIP route pattern](#)

**i** This guide is based on CUCM 9.x. If you are using other versions of CUCM, you will need to perform the same set of tasks, but the CUCM menus and options may differ slightly from those described here.

## Uploading TLS certificates (TLS only)

If you are using TLS, you need to ensure that CUCM trusts the certificates installed on the Pexip Infinity Conferencing Nodes.

To configure CUCM to trust the Conferencing Node's certificates:

1. From the CUCM web interface, from the top right **Navigation** box select *Cisco Unified OS Administration* and log in to the OS Administration interface.
2. Go to **Security > Certificate Management**, and select **Upload Certificate/Certificate chain**.
3. In the **Certificate Name** field, select *CallManager-trust*.
4. Upload the certificate of the CA that signed the Conferencing Node's TLS certificate.

Repeat this process, if necessary, to ensure that every Conferencing Node certificate is trusted.

## Creating a SIP trunk security profile (TLS only)

If you are using TLS, you must set up a SIP Trunk Security Profile. This is used to configure the TLS parameters for the SIP trunk to Pexip Infinity. For TCP-only (i.e. non-secure) trunks you can use the existing *Non-Secure SIP Trunk Profile*.

To set up a SIP Trunk Security Profile:

1. From the CUCM web interface, from the top right **Navigation** box select *Cisco Unified CM Administration* and log in.
2. Go to **System > Security > SIP Trunk Security Profile** and select **Add New**.
3. Complete the following fields:

|                         |   |
|-------------------------|---|
| Name                    | Enter a name for the profile. This example uses <i>Pexip Infinity Encrypted TLS SIP trunk</i> .   |
| Device Security Mode    | Select <i>Encrypted</i> .   |
| Incoming Transport Type | Select <i>TLS</i> .   |
| Outgoing Transport Type | Select <i>TLS</i> .   |
| X.509 Subject Name      | Enter the X509 subject name of the certificate installed on the Pexip Infinity Conferencing Node (usually the FQDN of the Conferencing Node). |
| Incoming Port           | Enter <i>5061</i> .   |

4. Select **Save**.

## Creating a SIP profile for Pexip Infinity (optional)

CUCM version 9.x includes a preconfigured SIP profile — **Standard SIP Profile For Cisco VCS** — which you can use for Pexip Infinity integration.

If you want a distinct profile for Pexip Infinity you can copy the **Standard SIP Profile For Cisco VCS** and set the name, for example, to **SIP profile for Pexip Infinity**.

## Creating a SIP trunk

This configures the connection towards the Pexip Infinity Conferencing Nodes to allow CUCM to make outgoing calls towards Pexip services.

1. From the CUCM web interface, from the top right **Navigation** box select *Cisco Unified CM Administration* and log in.
2. Go to **Device > Trunk** and select **Add New**.

- Complete the following fields:

|                    |                                |
|--------------------|--------------------------------|
| Trunk Type         | Select <i>SIP Trunk</i> .      |
| Device Protocol    | Select <i>SIP</i> .            |
| Trunk Service Type | Select <i>None (Default)</i> . |

- Select **Next**.
- Complete the following fields (leave all other settings as default):

|   |   |
|---|---|
| <b>Device information</b>                           |   |
| Device Name   | Enter a name for the SIP Trunk. This example uses <b>Pexip_Infinity</b> (no spaces are allowed).  |
| Device Pool   | Select the pool you want the Conferencing Node to belong to (in CUCM, these are configured in <b>System &gt; Device Pool</b> ).   |
| Location  | Select the location you want the Conferencing Node to belong to (in CUCM these are configured in <b>System &gt; Location</b> ).   |
| SRTP Allowed  | Select this option if you are using TLS.  |
| Run On All Active Unified CM Nodes                  | Select this option.   |
| <b>Call Routing Information &gt; Outbound Calls</b> |   |
| Calling Party Transformation CSS                    | Select <b>&lt;None&gt;</b> .  |
| <b>SIP Information</b>                              |   |
| Destination Address is an SRV                       | Select this option if the address you will enter in the field below is an SRV.  |
| Destination Address                                 | Enter the addresses of all of the Conferencing Nodes in the Pexip Infinity location. These can be an IPv4 address, FQDN or (if the field above is selected) an SRV e.g. <b>example.com</b> .  |
| Destination Port                                    | Enter <b>5060</b> for TCP or <b>5061</b> for TLS.   |
| SIP Trunk Security Profile                          | If you are using TCP, select the existing <b>Non-Secure SIP Trunk Profile</b> .<br><br>If you are using TLS, select the name of the security profile you have just created. This example uses <b>Pexip Infinity Encrypted TLS SIP trunk</b> . |
| SIP Profile   | Select either <b>Standard SIP Profile For Cisco VCS</b> , or if you have created a new profile — for example <b>SIP profile for Pexip Infinity</b> — select that one instead.   |
| Normalization Script                                | Select <b>vcs-interop</b> , if available. (This is only necessary if SRTP will be used.)  |

- Select **Save**

## Configuring the dial plan for calls from CUCM to Pexip Infinity

CUCM can be configured to route calls to a SIP trunk based on a specific prefix.

In our example deployment, all our Virtual Meeting Rooms have an alias with a prefix of 555 followed by 3 digits. To ensure that all calls from CUCM-registered devices to Pexip Infinity Virtual Meeting Rooms are routed correctly we must configure CUCM to route calls starting with 555 to Pexip Infinity without changing the number that was dialed.

To route calls based on a specific prefix:

- From the CUCM web interface, from the top right **Navigation** box select **Cisco Unified CM Administration** and log in.
- Go to **Call Routing > Route/Hunt > Route Pattern** and select **Add New**.

3. Complete the following fields:

| Pattern Definition        |  |
|---------------------------|--|
| Route Pattern             | Enter 555XXX   |
| Description               | Enter a description of the pattern. This example uses <i>Route 555XXX to Pexip Infinity SIP trunk.</i> |
| Gateway/Route List        | Select the SIP trunk you created earlier. This example uses <i>Pexip_Infinity</i> .                    |
| Call Classification       | Select <i>OnNet</i> .  |
| Provide Outside Dial Tone | Do not select this option.   |

4. Select **Save**.

## Adding a SIP route pattern

SIP route patterns are used to route calls based on a SIP destination FQDN rather than a numeric route pattern.

1. From the CUCM web interface, from the top right **Navigation** box select *Cisco Unified CM Administration* and log in.
2. Go to **Call Routing > SIP Route Pattern** and select **Add New**.
3. Complete the following fields (leave all other settings as default):

|               |   |
|---------------|---|
| Pattern Usage | Select <i>Domain Routing</i> .  |
| IPv4 Pattern  | Enter the domain to route. This example uses <i>example.com</i> .                   |
| SIP Trunk     | Select the SIP trunk you created earlier. This example uses <i>Pexip_Infinity</i> . |

4. Select **Save**.

## Testing the deployment

To confirm that you have successfully integrated Pexip Infinity and CUCM, you need to test that endpoints registered to CUCM can make calls to, and receive calls from, the Pexip Infinity platform.

### Calls to Pexip Infinity

- From a SIP endpoint registered to CUCM, place a call to one of your Pexip Infinity Virtual Meeting Room aliases. Use at least one other endpoint to place a call to the same Virtual Meeting Room. In this example, you would call *meet.alice@example.com*.
- Each endpoint should connect to the Virtual Meeting Room and be able to send and receive audio and video from all of the other participants.

### Calls from Pexip Infinity

There are a number of ways that Pexip Infinity Conferencing Nodes can be prompted to make outbound calls. For a full list, see [Automatically dialing out to a participant from a conference](#) and [Manually dialing out to a participant from a conference](#). For the purposes of this test, we will place the call manually using the Administrator interface, as follows:

1. From the Pexip Infinity Administrator interface, go to **Services > Virtual Meeting Rooms** and select the name of the Virtual Meeting Room from which you want to place the call. In this example we select *meet.alice*.
2. At the bottom left of the screen, select **Dial out to participant**.

3. Complete the following fields:

| Field             | Description  |
|-------------------|--|
| System location   | Select the system location to which the Conferencing Node that you added as a SIP trunk belongs.   |
| Service alias     | This lists all of the aliases that have been configured for the selected Virtual Meeting Room or Virtual Auditorium. The participant will see the incoming call as coming from the selected alias. |
| Destination alias | The alias of the endpoint that you want to dial.   |
| Protocol          | Select SIP.  |

4. Select **Dial out to participant**.

The call should be received by the destination endpoint, with the call showing as coming from the selected alias. On answer, the endpoint should connect to the selected Virtual Meeting Room and be able to send and receive audio and video from all of the other participants.