

4.3 UNENCRYPTED SIP Trunks

Click on the **New Sip Trunk** to go to the Edit Sip Trunk page.

Create SIP Trunk

Name	Unencrypted SIP Trunk
Failover Group	None
IP / Hostname	unencryptedserver.com
Port	5060
Transport Protocol	UDP
Outbound Proxy	
Register	<input checked="" type="checkbox"/>
Username	test_user
Password	*****
Virtual Phone Number	001123456789
SIP OPTIONS flag	<input checked="" type="checkbox"/>
Enable SIP URI	<input type="checkbox"/>
SIP Proxy flag	<input checked="" type="checkbox"/>
SIP Crypt. Suite	DEFAULT
Secure RTP	
Incoming Call Treatment	
New Connected Calls	NO
SAI	NO
Direct Media	<input checked="" type="checkbox"/>
Send Response to Peer ID	<input checked="" type="checkbox"/>
Codec	gsmulaw,alaw,g722
Announcement	Yes
SIP Signaling Method	RFC6020
Trusted	<input checked="" type="checkbox"/>

Create

figure 1. "Edit Sip Trunk" form

In figure 1. "Edit Sip Trunk" form you can read an example configuration for an unencrypted SIP trunk. Mandatory fields for the unencrypted configuration are:

- **NAME:** a meaningful name for this trunk
- **IP / HOSTNAME:** IP address/hostname of the SIP server provided by ITSP
- **PORT:** this is **5060** by RFC
- **TRANSPORT PROTOCOL:** UDP
- **SRTP ENCRYPTION:** disabled (unchecked)

We do also suggest the following values to be set:

- **ANNOUNCEMENT: ON EARLY MEDIA** works fine with the Cisco Unified Communications Manager.

- **DTMF SIGNALING METHOD:** choose your values considering the PBX on the other end of the Trunk. Usually we suggest to choose the value **RF C2833**
- **DIRECT MEDIA:** enabled (checked)
- **SEND REMOTE-PARTY-ID:** enabled (checked)

Other fields in the form depend by your network topology and by the features on the other end PBX.

When you are done with your changes, commit them by clicking on the **Update** icon.

[4.2 ENCRYPTED SIP Trunks ZRTP](#)

[4.4 Authentication in SIP Trunks](#)