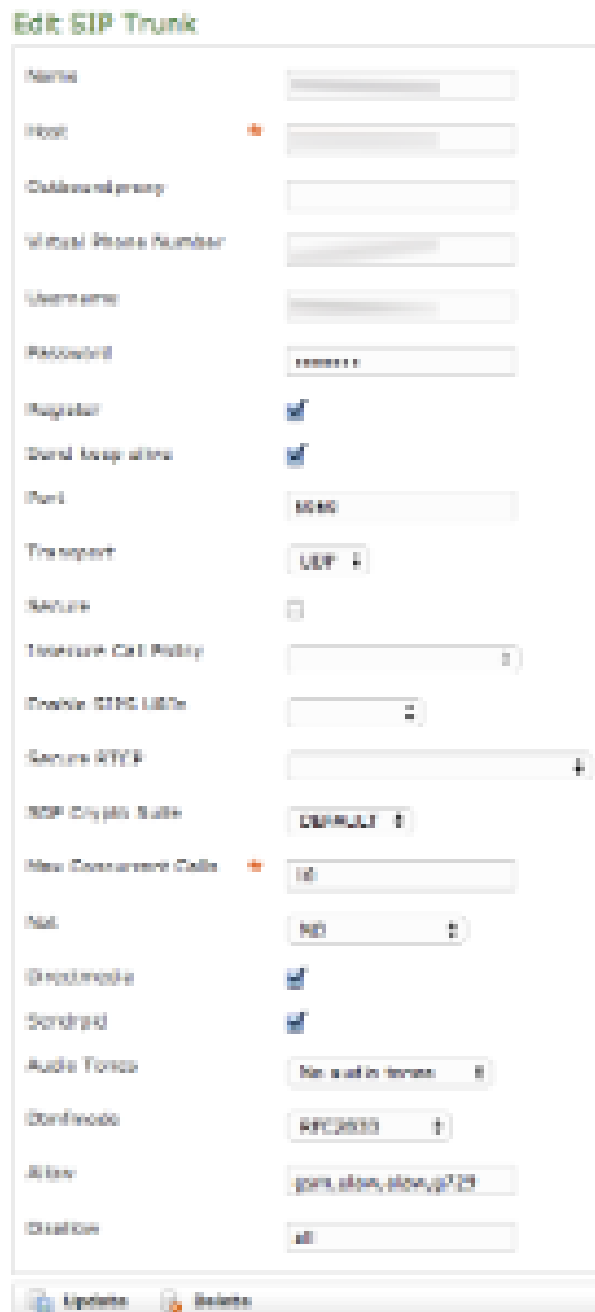


4.2 UNENCRYPTED SIP Trunks

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



The screenshot shows the 'Edit SIP Trunk' form with the following fields and values:

Field	Value
Name	
Host	
Child record group	
Initial Phone Number	
Username	
Password	secret
Register	<input checked="" type="checkbox"/>
Send keep alive	<input checked="" type="checkbox"/>
Port	5060
Transport	UDP
Secure	<input type="checkbox"/>
Trunk Call Policy	
Enable SIP MGCP	
Secure RTP	
RTP Crypt Suite	DEFAULT
New Connected Calls	10
Rel	NO
DTMF mode	<input checked="" type="checkbox"/>
Sendrpt	<input checked="" type="checkbox"/>
Audio Tones	No audio tones
DTMF mode	RFC2833
Allow	gsm, gsm, gsm, g729
Disallow	all

At the bottom of the form are buttons for 'Update' and 'Delete'.

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
- **HOST:** IP address/hostname of the SIP server provided by ITSP
- **PORT:** this is **5060** by RFC
- **TRANSPORT:** UDP
- **ENCRYPTION:** disabled (unchecked)

We do also suggest the following values to be set:

- **AUDIO TONES: ON EARLY MEDIA** works fine with the Cisco Unified Communications Manager.
- **DTMFMODE:** choose your values considering the PBX on the other end of the Trunk. Usually we suggest to choose the value **RFC2833**

- **DIRECTMEDIA**: enabled (checked)
- **SENDRPID**: 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.

[4.1 ENCRYPTED SIP Trunks](#)

[4.3 Authentication in SIP Trunks](#)