CHAPTER 21

SIP Trunk Security Profile Configuration

Cisco Unified CallManager Administration groups security-related settings in the SIP trunk security profile, which works like a template; that is, you configure the settings in the profile and then apply the profile to the SIP trunk. After you apply the profile to the trunk, it uses the settings that you configured in the SIP Trunk Security Profile window. If you want to do so, you can use the same profile for many SIP trunks, which eliminates having to configure the same fields multiple times.

The SIP Trunk Security Profile window includes security-related settings such as Incoming Transport Type, Outgoing Transport Type, Device Security Mode, Enable Digest Authentication, Nonce Validity Time, X.509 Subject Name, Incoming Port, Enable Application Level Authorization, Accept Presence Subscription, Accept Out-of-Dialog REFER, Accept Unsolicited Notification, and Accept Header Replacement.

Tip All SIP trunks require that you apply a security profile.

For information on configuring and applying a SIP trunk security profile, refer to the *Cisco Unified CallManager Security Guide*.