Configuring SBC Edge with ITSP that Requires Digest Authentication with 401 Unauthorized Challenge

This article describes the steps necessary to configure the SBC Edge with a SIP peer or with an Internet Telephony Service Provider (ITSP) that requires digest authentication with 401 Unauthorized challenge.

On this Page

Related Articles

- Managing Remote Authorization Tables
- Creating and Modifying Entries to Remote Authorization Tables
- Creating and Modifying Entries in SIP Server Tables

Prerequisites

General

This document assumes that you have already created a Signaling Group and a SIP Server table for the ITSP.

Software Version

Verify that your SBC Edge is loaded with the correct boot image version and that your SBC Edge base software version is at least version 2.0.0, build 108.

System Licenses

The SBC Edge system must have the necessary licenses to make calls.

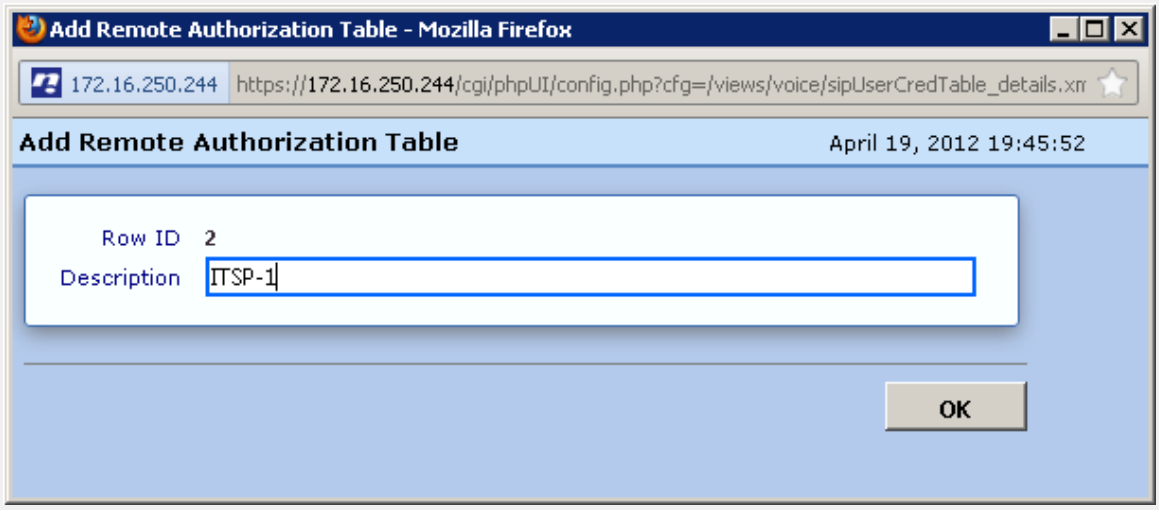
Configuration Steps

The configuration is comprised of three overall steps:

- Creating a Remote Authorization Table
- Assigning the Remote Authorization Table to the SIP Server Table
- Assigning the SIP Server Table to the Signaling Group for the ITSP

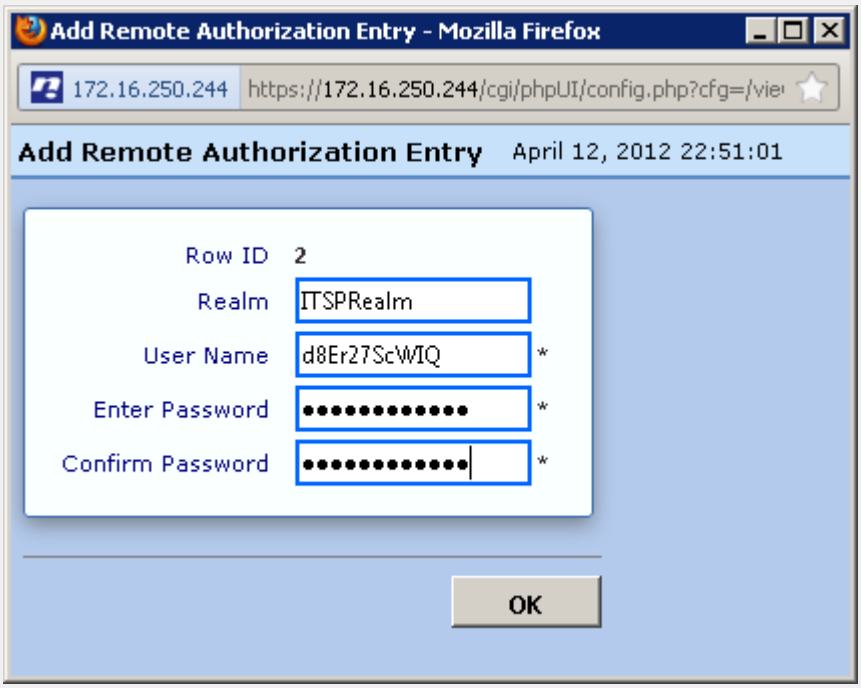
1. Add a Remote Authorization Table

Figure 1: Add Remote Authorization Table



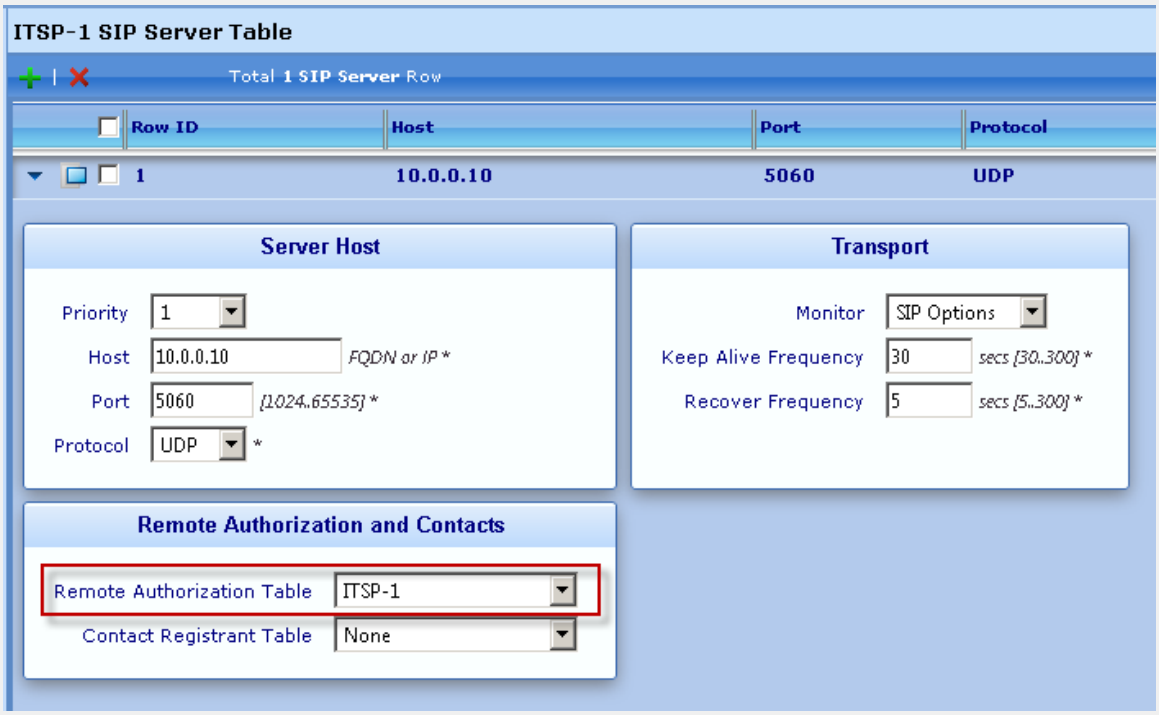
2. Add a Remote Authorization entry

Figure 2: Add Remote Authorization Entry



3. Assign the Remote Authorization Table to the SIP Server Table

Figure 3: Assign Remote Authorization Table



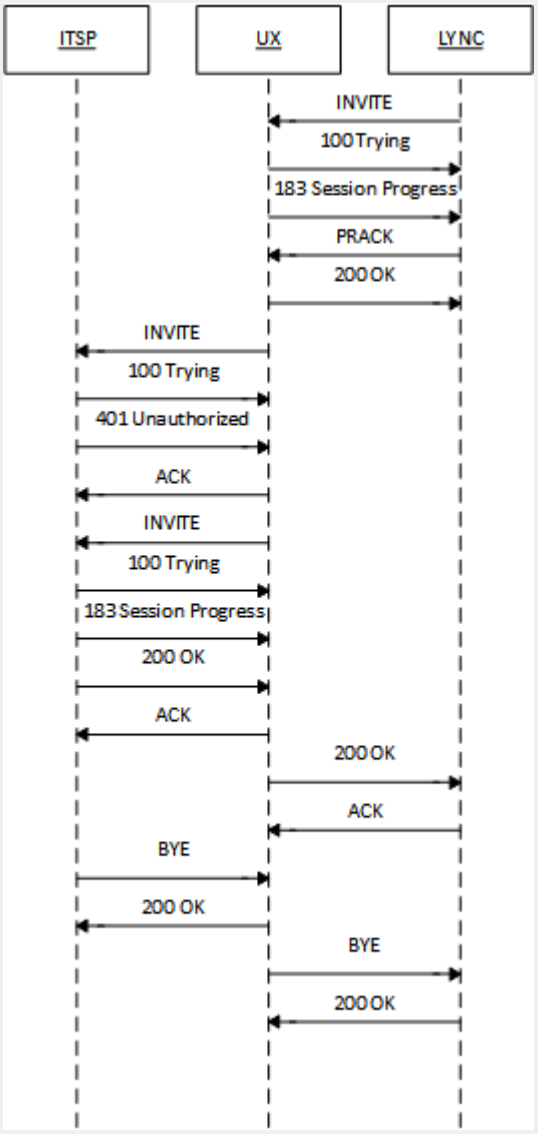
Additional Information

Call Flow

The call flow below depicts an outbound call from Lync to ITSP via Sonus SBC 1000/2000.

- After the initial INVITE from the Mediation server, SBC Edge (UA) sends an INVITE request to the ITSP proxy server (UAS).
- SBC Edge then receives 100 Trying and then 401 Unauthorized request from the ITSP proxy server.
- SBC Edge, acting as a UA, then re-sends the request and authenticates itself by including an Authorization header field with the request.
- The Authorization field value consists of credentials containing the authentication information of the UA for the realm of the resource being requested as well as parameters required in support of authentication and replay protection.
- The Realm, Username and Password information are taken from the Remote Authorization Table entry based on the username that is provided by the realm provided by the UAS.

Figure 4: Call Flow



Call Debugging Trace

The SBC Edge debug log produced at Trace level will show the information that is used to compute the MD5 string used in the Authorization header:

```
[2012-04-12 16:17:40,303] 5688 0001 com.net.ux.sip TRACE (Credentials.cpp:451) - computeResponse:
creating credentials:
   algorithm : "MD5"
   userName  : "d8Er27ScWIQ"
   passWord  : "uw83i29BeY3x"
   realm     : "ITSPRealm"
   nonce     : "ITSPRealmDe98wSj8euJdU8SHs8"
   cNonce    : "baea32a3"
   nonceCount: "00000001"
   qop       : "auth"
   method    : "INVITE"
   uri       : "sip:15105742474@10.0.0.10:5070;user=phone"
```