

INTRODUCTION

Security of IP networks has been evolving over a long period of time, resulting in multiple tried and true measures.



However, VoIP has created new challenges. With its continued growth worldwide, VoIP has only recently generated a concern for security, but that concern has been reaching a crescendo! An IT manager tasked with security of a data network, which typically includes well-known devices such as servers, routers, PCs, etc., must now also secure a voice network, which include gateways, IP PBXs, IP Phones, Session Border Controllers, and any number of access points to IP-based voice applications. Many of these devices are foreign to the IT world, and the telecom world didn't have the problem!

Now, securing VoIP systems is taking on paramount importance. To address this need, security measures have been evolving. The most common security mechanisms today include authorization and authentication.

Tenor Gateways, one of the early innovative VoIP devices, incorporated several measures to assure that VoIP calls are secure, both from a programming perspective and a common sense perspective.

Security is a simple and effective process, especially when you deploy Tenors. If you adhere to a few built-in prompts, and follow a few common sense suggestions, your VoIP network should be safe from hackers.

We have simplified the process of securing your Tenor. Below are the steps that you can follow after you've connected the Tenor on your network.

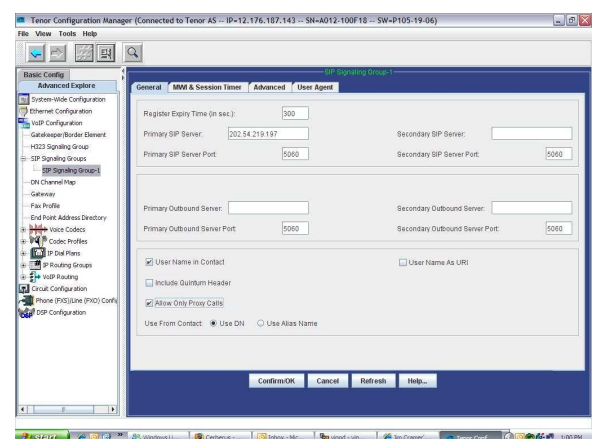
SIP Method - Allow Only Proxy Calls

Tenors can support both H.323 and SIP protocols. Deciding which protocol you want to use will be your first decision. Let's do SIP first.

SIP (Session Initiation Protocol) is a signaling protocol that establishes a session on an IP network. SIP is a request-response protocol that closely resembles Hypertext Transfer Protocol (HTTP), which, of course, forms the basis of the World Wide Web. It re-uses many of the constructs and concepts of Internet protocols such as HTTP and Simple Mail Transfer Protocol (SMTP).

The purpose of SIP is only to establish, change or terminate sessions. SIP is not concerned with the content or details of the session. It was designed to solve only a few problems and to work with many existing and future IP protocols.

SIP is Transport layer-independent, which means it can be used with any transport protocol: UDP, TCP, ATM, etc. It is text-based, requiring no encoding/decoding like H.323. And SIP supports user mobility, using proxies and redirecting requests to your current location.



Registrar and Proxy Servers

While the SIP Registrar and SIP Proxy may be two different entities, it is possible that the Proxy you are using may provide both Registrar and Proxy services at the same IP address. If you want to make an IP call using a SIP Proxy, or if you want REGISTER messages to be sent out, you must configure your Proxy IP address (or DNS name) at [PrimarySIPServer](#).

The IP address or DNS name of the Primary Server used to make outgoing SIP calls. This Server may be used for both Proxy and Registrar services. The default is null. If you choose to enter a SIP configuration, you must enter the IP address or domain name of the primary server used to make outgoing SIP calls.

The [AllowOnlyProxyCalls](#) flag indicates whether or not the Tenor should only accept incoming calls that are routed through the configured SIP Server. Be sure that this is set to "1" (enabled - default) to impose greater security through the Proxy. P104 or later code has the latest SIP features.

You may create SIP Signaling Groups (up to 4 for a Tenor Gateway, and up to 8 for a CMS).

The required steps to reach the **allowonlyproxycalls** in the Tenor Configuration Manager are as follows:

VoIP configuration > SIP Signaling Groups > SIP Signaling Group-n > Advanced tab > Allow Only Proxy Calls. (*This feature is enabled by default. Click the checkbox to disable this feature.)

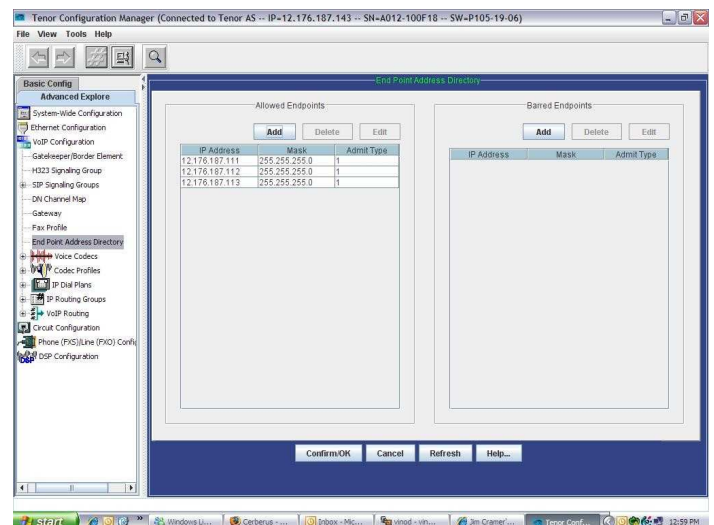
Each SIP Signaling Group may contain up to 24 User Agents.

Valid settings are: 0 – Allow calls from everyone; 1 – Only allow calls from SIP proxy server (default)

H.323 Method - Endpoint Address Directory (EPAD)

Use the [Endpoint Address Directory](#) to configure specific IP and/or subnet masks that are allowed or are not allowed (barred) to make calls to this Tenor.

The **EndPointAddressDirectory** Prompt is located under the Gateway Prompt. The parameter settings listed here are used to configure specific IP and/or subnet masks that are allowed or are not allowed (barred) to make calls to this Tenor.



Guidelines

If no IP addresses/subnet masks are specified to be either allowed or barred, then all IP addresses will be allowed to send VoIP calls to this unit, without restrictions.

If you choose to use the "Allow" feature, you must include the IP address of this Tenor as one of the allowed IP addresses.

Keep in mind that there is a limit on the number of entries that can be added in the Allowed and Barred lists:

- Tenor CMS/Tenor Call Relay SP - 128 in each list
- Tenor AS/AX/AF/BX/DX - 24 in each list

Disable Administrative Access, ie. Lock Down/Disable SIP and H.323

If you set the **webserverport** parameter to "0" (off) and submit the change, you will be able to continue to establish a Telnet/FTP session, but you (or anyone else) will not be able to initiate a new Configuration Manager session with this Tenor until someone re-enables this setting through the CLI.

If you set the **ManagementAccess** parameter to "0" (off) and submit the change, you will be able to continue your current Telnet/FTP session, but you (or anyone else) will not be able to initiate a new Telnet/FTP session with this Tenor until someone re-enables this setting using the Console/Serial Port or Configuration Manager.

ONE LAST PIECE TO THE SECURITY PUZZLE:

THE PASSWORD!



Of course, once you've configured your Tenors with its high tech software barriers, you have to create a few barriers of your own! The key here is to USE STRONG AND CREATIVE PASSWORDS at every level of entry to the Gateway!

When programming the Tenor, you have multiple layers in which you can use passwords to thwart hackers. These include:

- ◆ Admin password which enables you to change the Tenor's password;
- ◆ GateKeeper password, which, for authentication reasons and to prevent fraud, offers the opportunity to create an optional, encrypted password that can be included in the messages that flow between a Gatekeeper and Border Element. (In order for the Gatekeeper and Border Element to communicate normally, the password must be the same in all Gatekeepers and Border Elements in the network.)
- ◆ CDR password that is configured on the Tenor which allows the CDR server to connect. This password is separate from the system password, and is optional.
- ◆ RADIUS passwords allow you to configure both Primary and Secondary RADIUS authentication ports. As a security measure, the **sharedsecret** enables the Tenor to share encrypted data with the RADIUS server. This value must be identical to the value configured on the RADIUS server

- ◆ SNMP public community string, which ensures security, when the SNMP agent in the Tenor validates each request received from an SNMP manager before responding to the request. It does this by verifying that the manager belongs to an SNMP *community* with access privileges to the agent. All SNMP message exchanges consist of a community name and a data field, which contains instructions for the device.

Need more help?

The following sites will generate several suggestions for fairly strong and easy-to-remember passwords. You are likely to see one on the list that you will find easy to remember, or it may trigger an idea for something similar.

- ◆ <http://paulding.net/password.html>
- ◆ <http://www.adel.nursat.kz/apg/online/index.php>

And if you're not feeling particularly creative, here is a website to help inspire you.

- ◆ <http://wiki.ehow.com/Remember-Your-Password>

And, now, for the bad news: Once you've created your list of passwords, you should redo the entire process at least once every three months or so.