

Multi-Service Business Routers (MSBR)

Session Border Controllers (SBC)

VoIP Analog & Digital Media Gateways

Recommended Security Guidelines

Version 6.8



Table of Contents

1	Introduction.....	7
1.1	Security Threats	7
1.2	AudioCodes Security Solution.....	9
2	Separate Network Traffic	11
2.1	Identify Trusted and Un-trusted Networks.....	11
2.2	Use VLANs to Separate LAN Traffic	11
2.3	Implement Physical Network Separation using Ethernet Port Groups	12
2.4	Implement Physical Network Separation (Mediant 3000)	13
2.5	Data-Router Specific Security Guidelines	14
2.5.1	Use VLANs and VRFs to Separate WAN Traffic	14
2.5.2	Use Port VLANs (PVID) to Physically Separate LAN Traffic.....	14
3	Implement Layer 3/4 (Network) Firewall	15
3.1	Block Unused Network Ports.....	15
3.2	Define VoIP Traffic Firewall Rules.....	15
3.3	Define Data-Routing Firewall Rules for WAN.....	17
3.3.1	Avoid Creation of DMZ Host	17
3.3.2	Define Explicit Access List Rules.....	17
4	Secure Management Access	19
4.1	Change Default Management User Login Passwords.....	19
4.2	Implement LDAP-based User Authentication and Authorization	20
4.3	Implement RADIUS-based User Authentication.....	20
4.4	Implement Two-Way Authentication with X.509 Certificates	21
4.5	Secure HTTP Access using HTTPS.....	22
4.6	Secure Telnet Sessions	22
4.7	Secure SSH Sessions	23
4.8	Define Web, Telnet, and SSH Authorized Access List.....	24
4.9	Secure SNMP Interface Access	25
4.9.1	Prefer SNMPv3 over SNMPv2.....	25
4.9.2	Secure SMNPv2 Access.....	25
4.9.3	Secure LDAP Communication	27
5	Secure SIP using TLS (SIPS).....	29
5.1	Use Strong Authentication Passwords	29
5.2	Use TLS Version 1.0 Only	29
5.3	Use TLS for SIP Interfaces and Block TCP/UDP Ports.....	30
5.4	Use TLS for Routing Rules.....	30
5.5	Implement X.509 Certificates for SIPS (TLS) Sessions	31
5.6	Use an NTP Server	32

6	Define Maximum Call Duration.....	33
7	Define SIP Message Blacklist/Whitelist	35
8	Monitor and Log Events.....	37
8.1	Implement Dynamic Blacklisting of Malicious Activity (IDS)	37
8.2	Enable Syslog	38
8.3	Enable Logging of Management-Related Events	39
8.4	Enable Call Detail Records	40
9	SBC-Specific Security Guidelines.....	41
9.1	General Guidelines.....	41
9.2	Secure Media (RTP) Traffic using SRTP	42
9.3	Implement SIP Authentication and Encryption	43
9.3.1	Authenticating Users as an Authentication Server	43
9.3.2	Authenticating Users by RADIUS Server.....	44
9.3.3	Authenticating SIP Servers as an Authentication Server	45
9.3.4	Enforce SIP Client Authentication by SIP Proxy.....	45
9.3.5	Enforce SIP Digest Authentication by IP PBX	45
9.4	Secure Routing Rules	46
9.4.1	Classify by Classification Rules versus Proxy Set.....	46
9.4.2	Define Strict Classification Rules	47
9.4.3	Allow Calls only with Specific SIP User-Agent Header Value	49
9.4.4	Block Unclassified Calls.....	50
9.4.5	Define Strict Routing Rules.....	50
9.5	Define Call Admission Control Rules	50
9.6	Secure SIP User Agent Registration	52
9.6.1	Configure Identical Registration Intervals	52
9.6.2	Limit SBC Registered Users per IP Group / SRD.....	53
9.6.3	Block Calls from Unregistered Users	54
9.6.4	Block Registration from Un-Authenticated Users	55
9.7	Authenticate BYE Messages.....	55
9.8	Use SIP Message Manipulation for Topology Hiding	56
10	Gateway-Specific Security Guidelines	57
10.1	Block Calls from Unknown IP Addresses	57
10.2	Enable Secure SIP (SIPS)	57
10.3	Define Strict Routing Rules	58
10.4	Define Call Admission Control.....	58

Notice

This document describes the recommended security guidelines for AudioCodes Mediant Series devices.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents as well as software files can be viewed by registered customers at <http://www.audiocodes.com/downloads>.

© Copyright 2015 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: December-02-2015

Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNOM and CloudBond 365 are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Throughout this manual, unless otherwise specified, the term *device* refers to AudioCodes products.

Document Revision Record

LTRT	Description
30204	Initial document release.
30207	Recommended classification method for incoming SIP dialogs updated.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at <http://www.audiocodes.com/downloads>.

1 Introduction

This document provides recommended security guidelines for safeguarding your network and your AudioCodes device against malicious attacks.



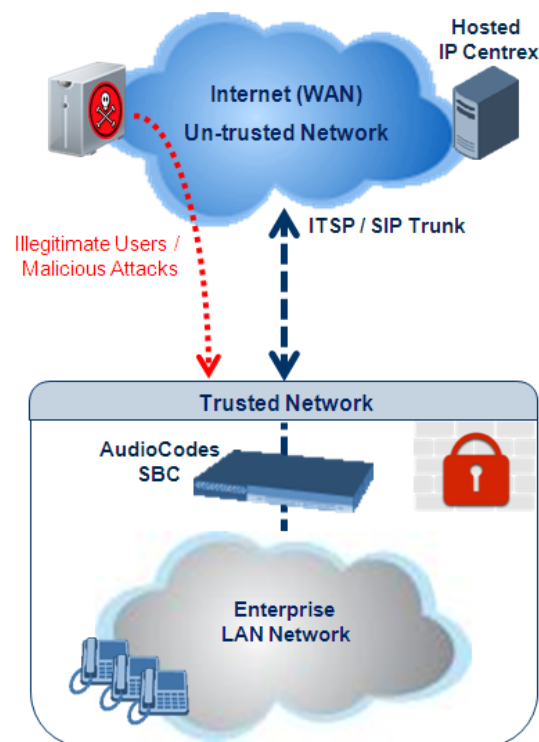
Notes:

- The security guidelines described in this document are applicable to **Version 6.8** and earlier.
- This document provides only recommended security guidelines; your network architecture may require additional and/or different security measures.
- This document includes partial configuration; for detailed configuration, refer to the device's *User's Manual*.

1.1 Security Threats

AudioCodes devices are commonly located at the demarcation point between safe (*trusted*) and unsafe (*un-trusted*) networks. A typical example of an un-trusted network would be a SIP trunk connected to an Internet Telephony Service Provider (ITSP) network while the internal LAN would be the trusted network. The figure below illustrates the basic concept of trusted and un-trusted networks.

Figure 1: Trusted and Un-trusted Networks



Attacks on your network from the un-trusted network may include the following:

- **Denial of Service (DoS) attacks:** Malicious attacks designed to cripple your VoIP network by overloading it with calls or service requests.
- **Overload events:** In addition to purposeful DoS attacks, non-malicious periods of intense activity can also cause an increase in call signaling rates that exceed what

your infrastructure can support, resulting in network conditions that are similar in effect to DoS attacks. Successful attacks resulting in contact center downtime can result in lost revenue and diminished customer satisfaction.

- **Network abuse and fraud:** Malicious intrusion or service theft may take the form of an unauthorized user gaining access to your VoIP network by mimicking an authorized user or seizing control of a SIP proxy and initiating outbound calls to the PSTN for free. Another possibility is using a compromised endpoint to redirect or forward calls for eavesdropping.
- **Viruses and malware:** Computer viruses, worms, Trojan horses, and other malware can infect user agent phones and SIP-based ACD infrastructure - just as they can computers and servers - and degrade performance or completely disrupt service. As devices become more sophisticated with distinct operating systems, malware also serves as a way to subjugate devices and launch DoS attacks that piggyback encrypted links.
- **Identity theft:** Phishing and "man-in-the-middle" can be used to acquire caller identification information to gain unauthorized access to services and information. Theft by phone (or service theft), whereby access to your corporate phone system is attempted by users posing as legitimate ones can sky-rocket your corporation's phone bill.
- **Eavesdropping:** The ability to listen to or record calls is easier on VoIP networks than on PSTN. This is a concern not only because of personal privacy violations, but also because sensitive information can be compromised and exploited.
- **Spam over Internet Telephony (SPIT):** The delivery of unsolicited calls or voicemails can inundate networks, annoy subscribers, and diminish the usefulness of VoIP networks.

These threats exist, for example, at the following main IP network border points:

- **Interconnect:** SIP trunks to ITSPs, using SIP signaling for inbound and outbound calls.
- **Trusted access:** Private, managed IP networks that connect service providers' residential, enterprise, or mobile subscribers (as part of an emerging federation of trusted networks).
- **Un-trusted access:** Unmanaged Internet for connections to work-at-home agents or inbound callers.

1.2 AudioCodes Security Solution

The AudioCodes device provides a comprehensive package of security features that handles the following two main security areas:

- **Securing the Service:** Secures the call services it provides by implementing separation and defense of different network entities (e.g., SIP Trunk, softswitch, and users). This is accomplished by the following:
 - Physical separation of networks
 - SRDs for each entity
 - IP Groups per entity
- **Securing the Device Itself:** This concerns two areas:
 - Management – ensuring that only authorized users can access the device's management interface
 - Defense against attacks on the device regarding SIP signaling and media (RTP)

Due to the vast number and types of potential attacks (some described in the previous section), security of your trusted VoIP network should be your paramount concern. The AudioCodes device provides a rich set of features to support perimeter defense for protecting your trusted network from the un-trusted ones. However, the device's security features and capabilities are only effective if implemented correctly. Improper use of the device for perimeter defense may render the overall security solution ineffective, thereby exposing your network to multiple threats.

The benefits of an IP-based telephony network are quite clear, but so are the threats and security implications that need to be addressed. The IP borders of the IP telephony network are the attack points and it is the AudioCodes security solutions that are designed to help safeguard your trusted network from such threats.

This page is intentionally left blank.

2 Separate Network Traffic

This section provides recommendations for separating network traffic.

2.1 Identify Trusted and Un-trusted Networks

It is crucial that you identify the trusted network (i.e., your local LAN) and un-trusted network (i.e., public Internet – WAN) in the environment in which the device is deployed (for an example illustration of such an architecture, see [Figure 1](#) on page 7). There may be multiples of each. For example, far-end users and a SIP trunk with an ITSP may represent two un-trusted networks.

Once identified, you need to handle the un-trusted networks with extreme caution to safeguard your trusted network from malicious attacks from it. One of the main precautions is to separate your trusted network from the un-trusted network using different logical configuration entities such as SRDs etc. The precautions and security guidelines are described in detail in subsequent sections.

2.2 Use VLANs to Separate LAN Traffic



Note: This section is applicable only to MP-11x, Mediant MSBR Series, Mediant 2000, and Mediant 3000.

It is recommended to implement virtual LANs (VLAN) to separate OAMP, media, and SIP signaling traffic on the LAN. VLANs may increase security in your network. VLANs are configured for the device's network interfaces in the Interface table (**Configuration** tab > **VoIP** > **Network** > **IP Interfaces Table**), as shown below:

- MP-1xx; Mediant 2000; Mediant 3000:

Figure 2-1: VLANs in Interface Table

Interface Table									
Add +									
Inde	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	VLAN ID	Interface Name	Primary DNS	Secondary DNS
0	OAMP	IPv4 Manual	10.8.6.55	16	10.8.0.1	100	Mng	10.1.1.11	10.1.1.10
1	Media	IPv4 Manual	10.8.6.56	16	10.8.0.1	200	Voice-Media	10.1.1.11	10.1.1.10
2	Control	IPv4 Manual	10.8.6.51	16	10.8.0.1	300	Voice-Sig	10.1.1.11	10.1.1.10

- Mediant MSBR Series:

Figure 2-2: Configuring VLAN IDs in Ethernet Device Table

Ethernet Device Table		
Index	VLAN ID	Name
0	100	vlan 100
1	200	vlan 200
2	300	vlan 300

Figure 2-3: Assigning VLANs (Underlying Devices) to Interfaces in Interface Table

Interface Table									
Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP	IPv4 Manual	10.8.6.55	16	10.8.0.1	Mng	10.1.1.11	10.1.1.10	vlan 100
1	Media	IPv4 Manual	10.8.6.56	16	10.8.0.1	Voice-Media	10.1.1.11	10.1.1.10	vlan 200
2	Control	IPv4 Manual	10.8.6.51	16	10.8.0.1	Voice-Sig	10.1.1.11	10.1.1.10	vlan 300

2.3 Implement Physical Network Separation using Ethernet Port Groups



Note: This section is applicable only to Mediant 500 Gateway & SBC, Mediant 800 Gateway & SBC, Mediant 1000B Gateway & SBC, Mediant 2600 E-SBC, Mediant 4000 SBC, Mediant 9000 SBC, and Mediant Software SBC.

For some devices (see note above), the network traffic can be physically separated by Ethernet ports, using Ethernet Port Groups. Each Ethernet Port Group can include up to two physical Ethernet ports. The Ethernet Device defines the VLAN per Ethernet Port Group. The Ethernet Device is then assigned to the network interface as an Underlying Device. The below show examples of such a configuration.

Figure 2-4: Assigning Ports to Ethernet Groups in Ethernet Group Settings Table

Ethernet Group Settings				
Index	Group	Mode	Member 1	Member 2
0	GROUP_1	Single	GE_0_1	None
1	GROUP_2	Single	GE_0_2	None
2	GROUP_3	Single	GE_0_3	None

Figure 2-5: Assigning VLANs to Ethernet Groups in Ethernet Device Table

Ethernet Device Table			
Index	VLAN ID	Underlying Interface	Name
0	1	GROUP_1	vlan 1
1	2	GROUP_2	vlan 2
2	3	GROUP_3	vlan 3

Figure 2-6: Assigning VLANs (Underlying Devices) to Interfaces in Interface Table

Interface Table									
Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP	IPv4 Manual	10.8.6.55	16	10.8.0.1	Mng	10.1.1.11	10.1.1.10	vlan 1
1	Media	IPv4 Manual	10.8.6.56	16	10.8.0.1	Voice-Media	10.1.1.11	10.1.1.10	vlan 2
2	Control	IPv4 Manual	10.8.6.51	16	10.8.0.1	Voice-Sig	10.1.1.11	10.1.1.10	vlan 3

2.4 Implement Physical Network Separation (Mediant 3000)



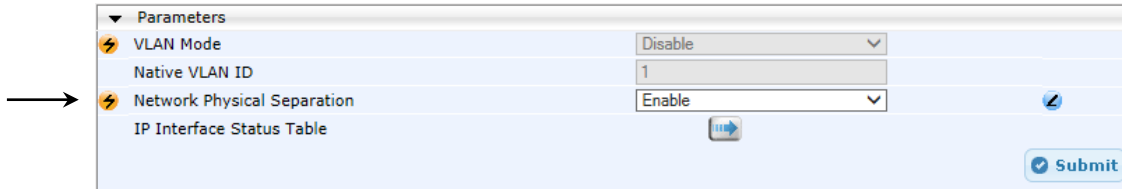
Note: This section is applicable only to Mediant 3000 with the TP-8410 blade.


It is highly recommended to separate traffic (i.e., OAMP, call control / SIP messages, and RTP media) so that each has its own dedicated physical Ethernet port. This Physical Network Separation feature eliminates the need for a VLAN-aware switch using VLAN tags to separate the different traffic of each network.

The physical interface provided for each network application type is as follows:

- **Media:** provided by the Gigabit Ethernet port on the RTM-8410
- **Control (SIP):** provide by 10/100BaseT Ethernet ports labeled **1A** (lower PEM module) and **1B** (upper PEM module) – two PEMs are used for redundancy
- **OAMP:** provided by 10/100BaseT Ethernet ports labeled **2A** (lower PEM module) and **2B** (upper PEM module) - two PEMs are used for redundancy

To enable this feature, the 'Network Physical Separation' parameter in the Interface table must be set to **Enable**.

Figure 2-7: Enabling Network Physical Separation in Interface Table


Parameters	
VLAN Mode	Disable
Native VLAN ID	1
Network Physical Separation	Enable
IP Interface Status Table	

2.5 Data-Router Specific Security Guidelines



Note: This section is applicable only to the MSBR series.

2.5.1 Use VLANs and VRFs to Separate WAN Traffic

It is recommended to implement the device's Virtual Routing and Forwarding (VRF) feature to segregate VoIP (SIP and media) / OAMP traffic from data-routing traffic into routing domains on the WAN interface. This is achieved by using the following CLI commands:

- `ip vrf, ip vrf forwarding`
- `ip route vrf`

Below shows a basic example for creating two VRFs, one for VoIP / OAMP ("VOIP") and one for data ("DATA"):

```
(config-data)# ip vrf VOIP
(conf-if-VLAN 200)# ip vrf forwarding VOIP
(config-data)# ip route vrf VOIP 10.1.1.1 255.255.0.0 10.8.0.1
vlan 200

(config-data)# ip vrf DATA
(conf-if-VLAN 300)# ip vrf forwarding DATA
(config-data)# ip route vrf VOIP 10.1.1.1 255.255.0.0 10.8.0.1
vlan 300
```

2.5.2 Use Port VLANs (PVID) to Physically Separate LAN Traffic

You can also separate the LAN traffic you configured in the Interface table between physical LAN ports, using port VLANs (PVID).

3 Implement Layer 3/4 (Network) Firewall

This section discusses Layer 3/4 (Network) firewall recommendations. By default, there are no firewall rules and this exposes the device to security risks. Therefore, configuring firewall rules is highly recommended to protect the device from external attacks.

3.1 Block Unused Network Ports

It is highly recommended that you disable network ports that are not used in your deployment. For example, if you are not using Trivial File Transfer Protocol (TFTP) in your network, then you should disable this network port application.

3.2 Define VoIP Traffic Firewall Rules

For packets whose source IP addresses are known, it is recommended to define VoIP firewall rules that allow receipt of calls or packets from this network and block all calls from elsewhere. These rules can be defined per source IP address, port, protocol, and network IP interface. If an incoming packet is received from an invalid source (as defined in the firewall), the call or packet is discarded.



Note: For devices with LAN and WAN interface ports (i.e., MSBR series), it is more important that a firewall be configured for the WAN interface, which is exposed to the public network (i.e., Internet). For more information, see Section 3.3.

Below is a list of recommended guidelines when configuring the VoIP firewall:

- **Add firewall rules per network interface:** It is recommended to define firewall rules for packets from source IP addresses received on the OAMP interface and each SIP Control (SIP) interface (defined in the Multiple Interface table). A less recommended alternative is to define a single rule that applies to all interfaces (by setting the 'Use Specific Interface' parameter to 'Disable').
- **Define bandwidth limitation per rule:** For each IP network interface, it is advised to define a rate-limiting value (byte rate, burst bytes and maximum packet size). Bandwidth limitation prevents overloading (flooding) of your network and thereby, helps in preventing attacks such as DoS on your device (on each network).
- **Define rules as specific as possible:** Define the rules as detailed as possible so that they block only the intended traffic.
- **Add an ICMP firewall rule:** ICMP is typically used for pinging. However, malicious attackers can send over-sized (floods) ICMP packets to a specific network address. Therefore, it is recommended to define a rule for limiting these packets.
- **Add a rule to block all traffic:** You must define a firewall rule that blocks **all** incoming traffic (i.e., block all protocol traffic from all source IP addresses and ports for all interfaces). This rule must be the **last** rule listed in the table, so that rules above it that allow specific traffic are valid (otherwise, all traffic is blocked).



Warning: If the 'Prefix Length' field on the Firewall Settings page is set to "0", the rule will apply to **all** IP addresses, regardless of whether an IP address is specified in the 'Source IP' field. Thus, if you need to apply a rule to a specific IP address, ensure that you also set the 'Prefix Length' field to a value other than "0".

The Layer 3-4 VoIP traffic firewall rules are configured on the Firewall Settings page (**Configuration** tab > **VoIP** menu > **Security** > **Firewall Settings**). The figure below shows an example of the following firewall rules:

- **Rules 1 and 2:** Typical firewall rules that allow packets ONLY from specified IP addresses (e.g., proxy servers). Note that the prefix length is configured.
- **Rule 3:** A more "advanced" firewall rule - bandwidth rule for ICMP, which allows a maximum bandwidth of 40,000 bytes/sec with an additional allowance of 50,000 bytes. If, for example, the actual traffic rate is 45,000 bytes/sec, then this allowance would be consumed within 10 seconds, after which all traffic exceeding the allocated 40,000 bytes/sec is dropped. If the actual traffic rate then slowed to 30,000 bytes/sec, the allowance would be replenished within 5 seconds.
- **Rule 4:** Allows traffic from the LAN voice interface and limits bandwidth.
- **Rule 5:** Blocks all other traffic.

Figure 3-1: Layer 3-4 VoIP Traffic Firewall Rules in Firewall Settings Page

Firewall Settings						
Add +						
Index	Source IP	Prefix Length	Start Port	End Port	Protocol	Action Upon Match
1	12.194.231.76	16	0	65535	Any	Allow
2	12.194.230.7	16	0	65535	Any	Allow
3	0.0.0.0	0	0	65535	icmp	Allow
4	192.0.0.0	8	0	65535	Any	Allow
5	0.0.0.0	0	0	65535	Any	Block

Firewall Rule Settings

Parameter	Value per Rule				
	1	2	3	4	5
Source IP	12.194.231.76	12.194.230.7	0.0.0.0	192.0.0.0	0.0.0.0
Prefix Length	16	16	0	8	0
Start Port and End Port	0-65535	0-65535	0-65535	0-65535	0-65535
Protocol	Any	Any	icmp	Any	Any
Use Specific Interface	Enable	Enable	Disable	Enable	Disable
Interface Name	WAN	WAN	None	Voice	None
Byte Rate	0	0	40000	40000	0
Burst Bytes	0	0	50000	50000	0
Action Upon Match	Allow	Allow	Allow	Allow	Block

3.3 Define Data-Routing Firewall Rules for WAN



Note: This section is applicable only to the MSBR series and if you are using the WAN interface.

The device provides two main network interfaces. The LAN which is the internal, private network of your enterprise, and the WAN which is the public network (Internet). Since the WAN interface is your LAN's "door" to the public network, you must define data-routing firewall rules for the WAN interface to prevent unwanted access from this unsafe, public network. The data-routing firewall rules are relevant for application protocols that are used by VoIP networks such as DHCP and TFTP. For example, firewall rules can be applied to configuration file downloads from a TFTP server that is located in the un-trusted network, by SIP user agents (e.g., IP phones) located in the trusted network.

This section discusses the guidelines for securing the device's WAN interface using the data-routing firewall capabilities.

3.3.1 Avoid Creation of DMZ Host

It is recommended not to configure a demilitarized zone (DMZ) host. The DMZ host allows a single local computer to be exposed to all services on the Internet, without any restrictions. A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other equipment in the network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.

3.3.2 Define Explicit Access List Rules

If your enterprise wishes to use the device's data-routing functionality, for example, a DHCP server (for distributing IP addresses to the enterprise's IP phones connected through the LAN switch), it is recommended that you define Access List rules (ACL) for blocking (*deny*) and allowing (*permit*) specified ingress (inbound) traffic from the public IP network on the WAN interface. If not defined, the device accepts all traffic.



Note: If your device is deployed solely as an SBC (VoIP functionality) without using the data-router functionality, ACL rules are unnecessary. This is due to the device's automatic NAT / port forwarding feature, which ensures that only desired traffic is allowed into the network.

You must define ACL rules as explicitly as possible:

- Include as much information as possible for each rule. For example, if you want to allow RTP traffic from only a specific IP address (e.g., 1.1.1.3), in addition to the IP address, you should also specify the allowed destination port (e.g., 6000-8000).
- Define adjacent rules (or overlapping rules) to block unwanted incoming traffic that may "slip" through an already defined allowed rule. For example, if the rule mentioned above is defined, unwanted RTP packets from IP address 1.1.1.3 destined to port 6600-6700 will also be allowed. Therefore, to block this traffic, define another rule explicitly denying traffic to port 6600-6700.

- Define rules to suite your environment so that only the required, minimum traffic is allowed (while all others are blocked).



Note: Incoming traffic that does not match any ACL rule is discarded even if a rule has not been defined to deny it (and no matching with an allowed rule exists where it can "slip" through).

Below shows an example of configured ACL rules called "WAN Firewall":

- Allow HTTPS traffic from IP address 1.1.1.1 and destined to port 443:

```
(config-data)# access-list wan-firewall permit tcp host
1.1.1.1 any eq 443
```

- Allow SSH traffic from IP address 1.1.1.1 and destined to port 22:

```
(config-data)# access-list wan-firewall permit tcp host
1.1.1.1 any eq 22
```

- Block all UDP traffic from IP address 1.1.1.3 destined to port 6600-6700. This is an "adjacent" rule for the rule below to prevent undesired traffic from "slipping" through:

```
(config-data)# access-list wan-firewall deny udp host 1.1.1.1
any range 6600 6700
```

- Allow UDP (RTP) traffic from IP address 1.1.1.3 and destined to port 6000-8000:

```
(config-data)# access-list wan-firewall permit udp host
1.1.1.1 any range 6000 8000
```

To associate the ACL with an interface (e.g., Gigabit WAN Ethernet):

```
(config-data)# interface GigabitEthernet 0/0
(conf-if-GE 0/0)# ip access-group wan-firewall in
(conf-if-GE 0/0)# exit
```

4 Secure Management Access

This section provides guidelines to secure access to the device's management interface.

4.1 Change Default Management User Login Passwords

To secure access to the device's Web management interface, please adhere to the following recommended guidelines:

- The device is shipped with a default **Security Administrator** access-level user account, "Admin" username. This user has full access and write privileges to the device. The default login password is "Admin". Change this to a hard-to-hack string. The login username and password are configured on the Web User Accounts page (**Configuration** tab > **System** > **Web User Accounts**) using the 'Current Password', 'New Password', and 'Confirm New Password' fields, as shown below:

Figure 2: Changing Password of Default Security Administrator User

Account Data for User: Admin		
User Name	Admin	<input type="button" value="Change User Name"/>
Access Level	Security Administrator	
Fill in the following 3 fields to change the password		
Current Password	<input type="button" value="Change Password"/>
New Password	<input type="button" value="Change Password"/>
Confirm New Password	<input type="button" value="Change Password"/>

- The device is shipped with a default **Monitor** access-level user account, "User" username. This user only has read access privileges to the device. The read access privilege is also limited to certain Web pages. However, this user can view certain SIP settings such as proxy server addresses. Therefore, in order to prevent an attacker from obtaining sensitive SIP settings that could result in possible call theft etc., change the access level of this user to **No Access** (see figure below). In addition (or alternatively), change its default login password ("User") to a hard-to-hack string.

Figure 3: Changing Access Level to No Access of Default Monitor User

Account Data for User: User		
User Name	User	<input type="button" value="Change User Name"/>
Access Level	<div style="border: 1px solid black; padding: 2px;"> No Access User Monitor Administrator Security Administrator </div>	<input type="button" value="Change Access Level"/>
Fill in the following 3 fields to change the password		

- If you have deployed multiple devices, use a unique password for each device.
- Change the login password periodically (for example, once a month).

4.2 Implement LDAP-based User Authentication and Authorization

It is highly recommended that you implement a third-party, LDAP server in your network for authenticating and authorizing the device's management users (Web and CLI). This can be done by using an LDAP-compliant server such as Microsoft Active Directory (AD). When a user attempts to log in to one of the management platforms, the device verifies the login username and password with AD. The device can also determine the user's management access level (privileges) based on the user's profile in the AD. This is configured in the LDAP Configuration table (**Configuration** tab > **VoIP** menu > **Services** > **LDAP** > **LDAP Configuration Table**).

Figure 4: LDAP Configuration Table for LDAP-Based User Authentication

Index	LDAP Server IP	LDAP Server Port	LDAP Server Domain Name	LDAP Bind DN	Type	Use TLS
0	202.145.5.6	389		\$/sales.local	Management	Yes
1	0.0.0.0	389			Control	No

An alternative is to use a RADIUS server, as discussed in the next section.

4.3 Implement RADIUS-based User Authentication

It is highly recommended that you implement a third-party, RADIUS server in your network for authenticating Web / Telnet users and thereby, preventing unauthorized access. RADIUS allows you to define different passwords for different interface users, with centralized management of the password database. When RADIUS is used, logging into the Web / Telnet interfaces is performed through the RADIUS server. The device verifies the authenticity of the user name and password with the RADIUS server.

An alternative is to use an LDAP server, as discussed in the previous section.

RADIUS is configured on the RADIUS Settings page (**Configuration** tab > **System** > **Management** > **Authentication Settings**), using the following parameters:

- 'Enable RADIUS Access Control': select **Enable**.
- 'Use RADIUS for Web/Telnet Login': select **Enable**.
- 'RADIUS Authentication Server IP Address' and 'RADIUS Authentication Server Port': enter the RADIUS authentication server's IP address and port respectively.
- 'RADIUS Shared Secret': enter the 'secret' password used to authenticate the device with the RADIUS server.

Figure 5: Enabling RADIUS for Web User Authentication

RADIUS Settings	
Enable RADIUS Access Control	Enable
Use RADIUS for Web/Telnet Login	Enable
RADIUS Authentication Server IP Address	100.125.10.5
RADIUS Authentication Server Port	1645
RADIUS Shared Secret	*****
RADIUS VSA Vendor ID	5003
RADIUS VSA Access Level Attribute	35

4.4 Implement Two-Way Authentication with X.509 Certificates

It is recommended to use two-way authentication (in addition to HTTPS) between the device's Web server and the management station (i.e., computer) accessing it. Authentication is performed and connection to the Web interface is subsequently allowed only if the following conditions are met:

- The management station possesses a client certificate from a Certification Authority (CA).
- The CA certificate is listed in the device's Trusted Root CA Store.

Otherwise, the connection is rejected. Therefore, this prevents unauthorized access to the Web management tool.



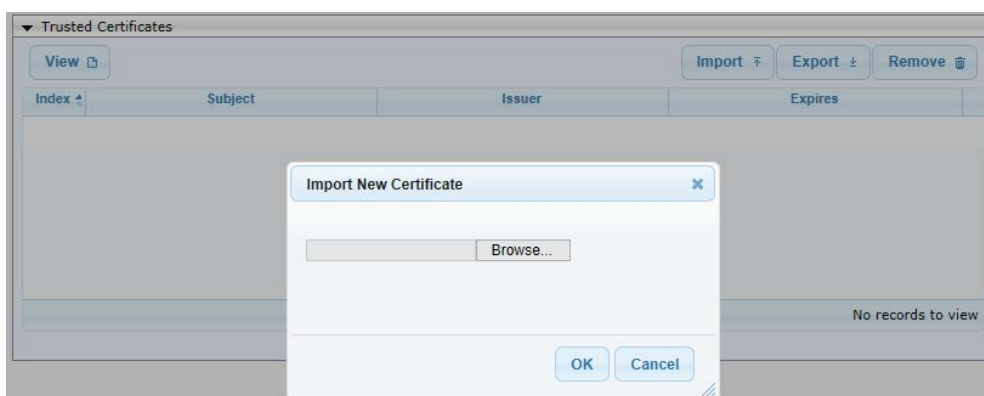
Notes:

- Implementation of two-way authentication requires a third-party security equipment vendor, CA server, and security administrator personnel. These should create certificates and deploy them to all the computers in the organization.
- The device is supplied with a working TLS configuration consisting of a unique self-signed server certificate. Replace this certificate with one provided by your security administrator. For more information, refer to the *User's Manual*.

➤ To configure client-server, two-way authentication using X.509 certificates:

1. Install a client certificate on the management station (your network administrator should provide you with a certificate).
2. Install your organization's CA certificate on the management station.
3. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
4. In the TLS Contexts table, select the required TLS Context index row, and then click the **TLS Context Trusted Root Certificates** button, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
5. Click the **Import** button, browse to and select the Root CA certificate file (in base64-encoded PEM format), and then import the file.

Figure 6: Importing CA Certificate to CA Store



6. Since X.509 certificates have an expiration date and time, the device must be configured to use Network Time Protocol (NTP) to obtain the current date and time. Without the correct date and time, client certificates cannot operate.
7. Ensure that client certificates for HTTPS connections are required, by setting the 'Requires Client Certificates for HTTPS connection' to **Enable** on the Web Security Settings page (**Configuration** > **System** > **Management** > **Web Security Settings**).

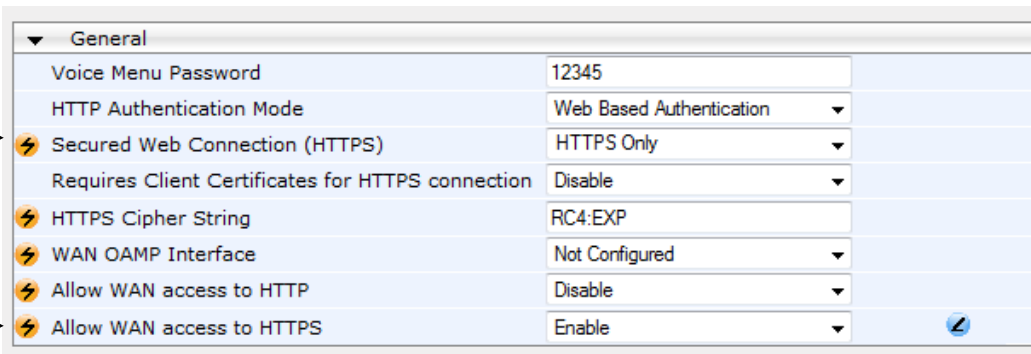
4.5 Secure HTTP Access using HTTPS

It is recommended to allow access to the Web interface using HTTPS only. In addition, it is recommended to block port 80.

This is configured on the WEB Security Settings page (**Configuration** tab > **System** > **Management** > **Web Security Settings**), by setting the following parameters:

- 'Secured Web Connection (HTTPS)': select **HTTPS Only**.
- **(MSBR Series)** If you are accessing the Web management through the WAN port, set the 'Allow WAN access to HTTPS' parameter to **Enable**.

Figure 7: Securing Access to Web Interface using HTTPS



The screenshot shows the 'General' tab of the Web Security Settings page. The following parameters are visible:

Parameter	Value
Voice Menu Password	12345
HTTP Authentication Mode	Web Based Authentication
Secured Web Connection (HTTPS)	HTTPS Only
Requires Client Certificates for HTTPS connection	Disable
HTTPS Cipher String	RC4:EXP
WAN OAMP Interface	Not Configured
Allow WAN access to HTTP	Disable
Allow WAN access to HTTPS	Enable

Arrows point to the 'Secured Web Connection (HTTPS)' and 'Allow WAN access to HTTPS' rows.



Note: MSBR Series: For security, it is recommended to disable access from the WAN port. However, if HTTP management access from the WAN is necessary, then it is recommended that you disable the WAN port for all other management access types (i.e., Telnet, SSH / CLI, and SNMP). In addition, if you enable WAN management access, ensure that you define Layer 5 (see Section 4.8) and Layer 3-4 (see Section 2) firewall rules to prevent access by undesirable elements from the public network.

4.6 Secure Telnet Sessions

If you require the use of Telnet and your management PC software provides a secure Telnet application, use a secured Telnet connection (i.e., Transport Layer Security / TLS). TLS protects Telnet traffic from network sniffing.

This is configured on the Telnet/SSH Settings page (**Configuration** tab > **System** > **Management** > **Telnet/SSH Settings**), by setting the following parameters:

- 'Embedded Telnet Server': select **Enable Secured**.
- 'Telnet Server TCP Port': Change the default TCP port (if required). This setting is applicable for access from the LAN.
- **(MSBR Series)** If management is through the WAN port, then set the 'Allow WAN access to Telnet' parameter to **Enable**.

Figure 8: Securing Telnet with TLS

Telnet Settings	
Embedded Telnet Server	Enable Secured
Telnet Server TCP Port	25
Telnet Server Idle Timeout	5
Allow WAN access to Telnet	Enable



Note: MSBR Series: It is recommended to disable access from the WAN port. However, if Telnet management access from the WAN is necessary, then it is recommended that you disable the WAN port for all other management access types (i.e., HTTPS, SSH / CLI, and SNMP). In addition, if you enable WAN management access, ensure that you define Layer 5 (see Section 4.8) and Layer 3-4 (see Section 2) firewall rules to prevent access by undesirable elements from the public network.

4.7 Secure SSH Sessions

Secure SHell (SSH) is the de-facto standard for secure CLI. SSH 2.0 is a protocol built above TCP, providing methods for key exchange, authentication, encryption, and authorization. By default, SSH uses the same user name and password as the Telnet and Web server. In addition, SSH supports 1024- and 2048-bit RSA public keys, providing carrier-grade security.

This is configured on the Telnet/SSH Settings page (**Configuration** tab > **System** > **Management** > **Telnet/SSH Settings**), by setting the following parameters:

- 'Enable SSH Server': select **Enable**.
- 'Server Port': If desired, you may change the default TCP port used for SSH, although this is not recommended. Note that this is applicable for access from the LAN.
- **(MSBR Series)** If management is through the WAN port, set the 'Allow WAN access to SSH' parameter to **Enable**.

Figure 9: Securing SSH (CLI) Sessions

SSH Settings	
Enable SSH Server	Enable
Server Port	22
Admin Key	
Require Public Key	Disable
Max Payload Size	32768
Max Binary Packet Size	35000
Enable Last Login Message	Enable
Max Login Attempts	3
Allow WAN access to SSH	Enable
Maximum SSH Sessions	5



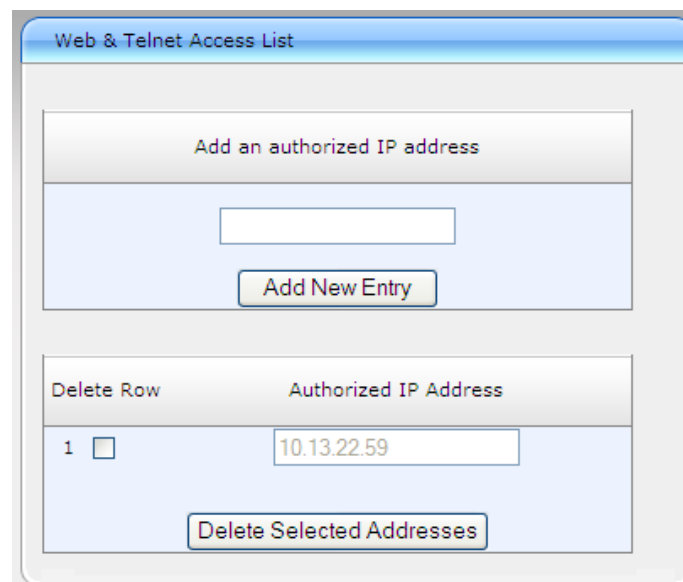
Note: MSBR Series: It is recommended to disable access through the WAN port. However, if CLI management access from the WAN is necessary, then it is recommended that you disable the WAN port for all other management access types (i.e., HTTPS, Telnet, and SNMP). In addition, if you enable WAN management access, ensure that you define Layer 5 (see Section 4.8) and Layer 3-4 (see Section 2) firewall rules to prevent access by undesirable elements from the public network.

4.8 Define Web, Telnet, and SSH Authorized Access List

Allow only user-defined LAN IP addresses to access the Web, Telnet, and SSH based management interfaces. The device denies access from undefined IP addresses.

This is configured on the Web & Telnet Access List page (**Configuration** tab > **System** > **Management** > **Web & Telnet Access List**).

Figure 10: Authorized IP Addresses for Accessing Web / Telnet / SSH Interfaces



Delete Row	Authorized IP Address
1 <input type="checkbox"/>	10.13.22.59



Notes:

- The first authorized IP address in the list must be your PC's (terminal) IP address; otherwise, access from your PC will be denied.
- **MSBR Series:** This authorized access list concerns access only from the LAN (not WAN).
- The Web / Telnet / SSH authorized access list concerns OSI Layer 5 (Session). However, you can also add firewall rules for Layer 3 (Network) and Layer 4 (Transport) with bandwidth limitation to limit access to management interfaces (see Section 3.1).

4.9 Secure SNMP Interface Access

This section discusses recommended security guidelines relating to Simple Network Management Protocol (SNMP).

4.9.1 Prefer SNMPv3 over SNMPv2

It is highly recommended to use SNMP Version 3 (SNMPv3) over SNMPv1 and SNMPv2c, if possible. SNMPv3 provides secure access to the device using a combination of authentication (MD5 or SHA-1) and encryption (DES, 3DES, AES-128, AES-192, or AES-256) of packets over the network. It is also recommended that you periodically change the SNMPv3 authentication and privacy keys.

The SNMPv3 users are configured on the SNMP v3 Users page (**Maintenance** tab > **System** > **Management** > **SNMP** > **SNMP V3 Users**), as shown in the figure below:

Figure 11: Defining SNMPv3 Users

The screenshot shows the 'SNMPv3 Users' configuration page. At the top, there are buttons for 'Add +', 'Edit', and 'Delete'. A 'Show/Hide' button is on the right. Below is a table with the following data:

Index	User Name	Authentication Protocol	Privacy Protocol	Authentication Key	Privacy Key	Group
0	John	MD5	DES	*	*	Read-Write

At the bottom of the table, there is a pagination control: 'Page 1 of 1' and 'Show 10 records per page'. The status 'View 1 - 1 of 1' is shown at the bottom right.

4.9.2 Secure SMNPv2 Access

If you are using SNMPv2, change the community strings from their default values ('public') as they can easily be guessed by hackers. In addition, by default, the SNMPv2 agent accepts SNMP Get and Set requests from any IP address as long as the correct community string is used in the request. Therefore, to enhance security with SNMPv2, implement Trusted Managers. A Trusted Manager is an IP address (management station) from which the SNMP agent accepts and processes Get and Set requests. It is also recommended that you periodically change these SNMP community string values.

- SNMPv2 community strings are configured on the SNMP Community String page (**Maintenance** tab > **System** > **Management** > **SNMP** > **SNMP Community Settings**) by setting the following parameters:
 - 'Community String': enter a read-write community string (up to 19 characters; default string is "private").
 - **(MSBR Series)** If the SNMP management is through the WAN port, then set the 'Allow WAN access to SNMP' parameter to **Enable**.

Figure 12: SNMPv2 Community Strings

Community String	Access Level
	Read Only
	Read Only
	Read Only
	Read Only
	Read Only
snmpv2user_john	Read / Write
	Read / Write
	Read / Write
	Read / Write
	Read / Write

<input type="checkbox"/> Disable SNMP	No
Trap Community String	trapuser
Trap Manager Host Name	
<input checked="" type="checkbox"/> Allow WAN access to SNMP	Enable



Note: MSBR Series: It is recommended to disable access from the WAN port. However, if SNMP management access from the WAN is necessary, then it is recommended that you disable the WAN port for all other management access types (i.e., HTTPS, Telnet, and CLI / SSH). In addition, if you enable WAN management access, ensure that you define Layer 3-4 (see Section 2) firewall rules to prevent access by undesirable elements from the public network.

- SNMPv2 management stations are configured on the SNMP Trusted Managers page (Maintenance tab > System > Management > SNMP > SNMP Trusted Managers).

Figure 13: SNMPv2 Trusted Managers

Delete	Trusted Managers IP Address	
<input type="checkbox"/>	SNMP Trusted Manager 1	10.13.22.25
<input type="checkbox"/>	SNMP Trusted Manager 2	0.0.0.0
<input type="checkbox"/>	SNMP Trusted Manager 3	0.0.0.0
<input type="checkbox"/>	SNMP Trusted Manager 4	0.0.0.0
<input type="checkbox"/>	SNMP Trusted Manager 5	0.0.0.0

4.9.3 Secure LDAP Communication

If you are using LDAP-based login management (username-password) and/or LDAP-based SIP routing in your deployment, it is recommended to employ TLS for secure device communication with the LDAP server. This ensures that the device encrypts the username and password sent to the LDAP server.

TLS for LDAP communication is configured in the LDAP Configuration table (Configuration tab > VoIP menu > Services > LDAP > LDAP Configuration Table). The parameter 'Use SSL' must be set to **Yes**.

This page is intentionally left blank.

5 Secure SIP using TLS (SIPS)

It is crucial that you implement the TLS-over-TCP protocol to best secure the device's SIP signaling connections. TLS provides encryption and authentication of SIP signaling for your VoIP traffic, preventing tampering of calls. Use it whenever possible for far-end users and ITSPs.

The device's TLS feature supports the following:

- **Transports:** SSL 2.0, SSL 3.0, TLS 1.0
- **Ciphers:** 3DES, RC4 compatible, Advanced Encryption Standard (AES)
- **Authentication:** X.509 certificates
- **Revocation checking:** OCSP (CRLs are currently not supported)
- Receipt of wildcards (*) in X.509 Certificates when establishing TLS connections. These wildcards can be part of the CN attribute of the Subject field or the DNSName attribute of the SubjectAltName field.

Recommended security guidelines for ensuring TLS for SIP signaling are described in the subsequent subsections.

5.1 Use Strong Authentication Passwords

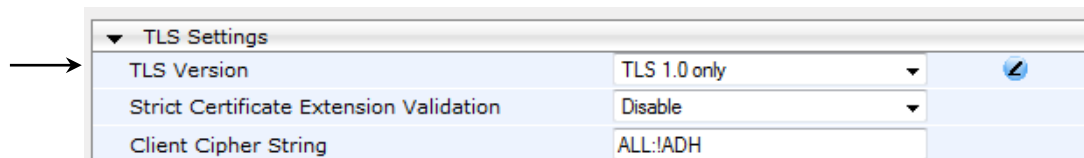
Always use strong authentication passwords, which are more difficult to detect than weak ones. A strong password typically includes at least six characters with a combination of upper and lower case letters, numbers and symbols.

5.2 Use TLS Version 1.0 Only

It is highly recommended to use TLS version 1.0 only. This ensures that only TLS 1.0-based connections are accepted while offers of previous versions (i.e., SSL 2.0 and SSL 3.0) are rejected.

This is configured on the General Security Settings page (**Configuration** tab > **VoIP** > **Security** > **General Security Settings**) by setting the 'TLS Version' parameter to **TLS 1.0 only**, as shown below:

Figure 14: Enabling TLS Version 1.0



Note: TLS 1.0 should be implemented only if it is compatible with the rest of your network. If other network entities use SSL 2.0 / SSL 3.0 handshakes, then this recommendation should be ignored and SSL 2.0 / SSL 3.0 should be allowed.

5.3 Use TLS for SIP Interfaces and Block TCP/UDP Ports

Each port can be vulnerable to attacks. Therefore, it is highly recommended that your SIP interfaces use **only** TLS. When configuring your SIP Interfaces, define the TLS port number, but set the UDP and TCP ports to zero (0). This configuration blocks (disables) the UDP and TCP ports. In other words, to disable UDP and TCP ports, you must define SIP Interfaces. In addition, to increase security, define only SIP Interfaces that are absolutely necessary.

SIP Interfaces are configured on the SIP Interface Table page (**Configuration** tab > **VoIP** > **VoIP Network** > **SIP Interface Table**). The figure below shows an example of a SIP Interface configured for the Voice network interface (LAN) with UDP and TCP ports set to 0:

Figure 15: SIP Interface using only TLS Port

The screenshot shows a configuration window titled "Add Record" for a SIP interface. The fields are as follows:

Index	0
SIP Interface Name	LanVoice
Network Interface	Voice
Application Type	SBC
UDP Port	0
TCP Port	0
TLS Port	5061
SRD	1
Message Policy	None
TLS Context Name	TLSContexts_2
TLS Mutual Authentication	
Enable TCP Keepalive	Disable
Classification Failure Response Type	500
Pre-classification Manipulation Set ID	-1

Arrows on the left point to the UDP Port, TCP Port, and TLS Port fields.

5.4 Use TLS for Routing Rules

It is recommended that your routing rules use TLS only as the transport type. This is configured in the IP-to-IP Routing table (**Configuration** tab > **VoIP** > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**) by setting the 'Destination Transport Type' parameter to **TLS**:

Figure 16: IP-to-IP Routing Rule using SIP over TLS

The screenshot shows a configuration window for an IP-to-IP Routing Rule. The fields are as follows:

Index	0
Destination Type	IP Group
Destination IP Group ID	-1
Destination SRD ID	None
Destination Address	
Destination Port	0
Destination Transport Type	TLS
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None

An arrow on the left points to the Destination Transport Type field.

5.5 Implement X.509 Certificates for SIPS (TLS) Sessions

It is highly recommended to implement the X.509 certificate authentication mechanism for enhancing and strengthening TLS. X.509 is an ITU-T standard for Public Key Infrastructure (PKI).

The device supports the configuration of multiple TLS certificates, referred to as TLS Contexts. TLS Contexts are assigned to Proxy Sets and/or SIP Interfaces, thereby enabling specific calls to use specific TLS certificates.

The device is shipped with a working TLS configuration (TLS Context ID 0), consisting of a unique Self-Signed Server Certificate. Self-Signed Certificate is the simplest form of an X.509 Certificate that is issued by the device itself without the use of any certificate signer (CA). The Self-Signed Certificate consists of the Public Key of the device that is signed by the Private Key of the device itself. However, use of this certificate is **strongly discouraged**. The Self-Signed Certificate is typically used in testing environments or for a low-scale deployment where solution security may be sacrificed in favor of simplified configuration procedures. The Self-Signed Certificate does not utilize CA trust relationships and its authenticity cannot be reliably verified. Instead, you should establish a PKI for your organization (provided by your security administrator) and use certificates signed by genuine CAs.

In a typical PKI scheme, Certificates are issued by a CA and provide an attestation by the CA that the identity information and the public key belong together. Each party has a list of Trusted Root Certificates – certificates of the CAs (or their roots) that are well-known and trusted by the party. When the certificate from the other party is received, its signing entity (CA) is compared with the Trusted Root Certificates list and if a match is found, the certificate is accepted.

The device uses the following files to implement X.509 PKI:

- **Private Key File:** This file contains a private key that is used to perform decryption. It is the most sensitive part of security data and should never be disclosed to other entities.
- **Certificate File:** This file contains a digital signature that binds together the Public Key with identity information. The Certificate may be issued by a CA or self-signed (issued by the device itself, which is not recommended – see above).
- **Trusted Root Certificate File:** This file is the certificate of the Trusted Root CA used to authorize certificates received from remote parties, based on the identity of the CA that issued it. If the root certificate of this CA matches one of the Trusted Root Certificates, the remote party is authorized.

5.6 Use an NTP Server

It is recommended to implement a third-party, NTP server so that the device receives the correct current date and time. This is necessary for validating certificates of remote parties.

It is also recommended to enable the device to authenticate and validate messages received from the NTP server. Authentication is done using an authentication key with the MD5 cryptographic hash algorithm. NTP messages that are received without authentication are ignored.

The NTP server is configured on the Application Settings page (**Configuration** tab > **System** > **Application Settings**):

Figure 5-17: NTP Server Configuration

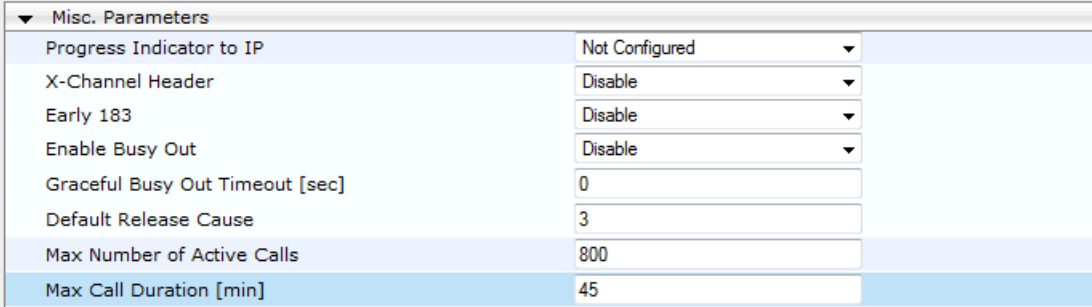
▼ NTP Settings	
NTP Server Address (IP or FQDN)	<input type="text" value="timenetservices.com"/>
NTP UTC Offset	Hours: <input type="text" value="0"/> Minutes: <input type="text" value="0"/>
NTP Updated Interval	Hours: <input type="text" value="24"/> Minutes: <input type="text" value="0"/>
NTP Secondary Server Address (IP or FQDN)	<input type="text"/>
NTP Authentication Key Identifier	<input type="text" value="6788"/>
NTP Authentication Secret Key	<input type="password" value="••••"/>

6 Define Maximum Call Duration

It is recommended to define maximum call duration (in minutes) to prevent calls from utilizing valuable device resources that could otherwise be used for additional new calls. If a call exceeds this duration, the device terminates the call.

This is configured on the Advanced Parameters page (**Configuration** tab > **VoIP** > **SIP Definitions** > **Advanced Parameters**) using the 'Max Call Duration' field:

Figure 18: Configured Maximum Call Duration



The screenshot shows a configuration window titled 'Misc. Parameters'. It contains a list of parameters with their respective values. The 'Max Call Duration [min]' parameter is highlighted in blue, and an arrow points to it from the left.

Misc. Parameters	
Progress Indicator to IP	Not Configured
X-Channel Header	Disable
Early 183	Disable
Enable Busy Out	Disable
Graceful Busy Out Timeout [sec]	0
Default Release Cause	3
Max Number of Active Calls	800
Max Call Duration [min]	45

This page is intentionally left blank.

7 Define SIP Message Blacklist/Whitelist

It is recommended to configure SIP message policy rules for blocking (blacklist) unwanted incoming SIP messages or allowing (whitelist) receipt of desired messages. This allows you to define legal and illegal characteristics of a SIP message.

SIP message policy is helpful against VoIP fuzzing (also known as robustness testing), which sends different types of packets to its "victims" for finding bugs and vulnerabilities. For example, the attacker might try sending a SIP message containing an oversized parameter or too many occurrences of a parameter.

Each SIP message policy rule can be configured with, for example, maximum message length, header length, body length, number of headers, and number of bodies. Each rule is then set as a blacklist or whitelist.

The SIP message policy rules are configured on the Message Policy Table page (**Configuration** tab > **VoIP** > **SBC** > **Message Policy Table**). Below shows a configured policy that defines maximum SIP messages to 32,768 characters, headers to 256 characters, bodies to 512 characters, number of headers to 16, and only permits two bodies. Invalid requests are rejected. Only INVITE and BYE requests are permitted and there are no restrictions on bodies

Figure 7-1: Configured Message Policy Rule

Message Policy Table				
Index	Max Message Length	Max Header Length	Max Body Length	Max Num Headers
0	1400	300	300	20

Page 1 of 1 Show 10 records per page View 1 - 1 of 1

Message Policy #0

Max Message Length: 1400	Max Header Length: 300
Max Body Length: 300	Max Num Headers: 20
Max Num Bodies: 5	Send Rejection: Policy Reject
Method List: invite\refer	Method List Type: Policy Blacklist
Body List:	Body List Type: Policy Blacklist

This page is intentionally left blank.

8 Monitor and Log Events

It is highly recommended that you log and monitor device events (including device operations and calls). The importance of monitoring device events is that you can quickly detect unauthorized access and subsequently take counter measures to effectively terminate the attacker before any potential damage is done to your network.

8.1 Implement Dynamic Blacklisting of Malicious Activity (IDS)

It is important to configure the Intrusion Detection System feature (IDS) to enable the device to detect malicious attacks targeted on the device (e.g., DoS, SPAM, and Theft of Service). It is crucial to be aware of any attacks to ensure the legitimate call service is maintained at all times. If any user-defined attacks are identified, the device can do the following:

- Block (blacklist) remote hosts (IP addresses / ports) considered as malicious. The device automatically blacklists the malicious source for a user-defined period after which it is removed from the blacklist.
- Send SNMP traps to notify of the malicious activity and/or whether an attacker has been added to or removed from the blacklist.

The IDS configuration is based on IDS Policies, where each policy can be configured with a set of IDS rules. Each rule defines a type of malicious attack to detect and the number of attacks (alarm threshold) during an interval (threshold window) before an SNMP trap is sent. Each policy is then applied to a target under attack (SIP Interface) and/or source of attack (Proxy Set and/or subnet address).

For configuring IDS, use the tables under the **Intrusion Detection and Prevention** menu (**Configuration** tab > **VoIP** menu > **Security** > **Intrusion Detection and Prevention**):

- **Global Parameters** – enables IDS
- **Policy Table** – defines IDS Policies and rules
- **Match Table** – assigns the IDS Policies to targets under attack (SIP Interface) and/or source of attacks (Proxy Set and/or subnet address)

Below is an example of an IDS rule for identifying DoS attacks from ITSP:

- IDS Policy "ITSP DOS" configured with three rules:

Table 8-1: IDS Policy Example

IDS Policy	Rule	Attack Type	Threshold Window (sec)	Alarm Threshold		
				Minor	Major	Critical
ITSP DOS	1	Malformed messages	30	10	15	30
	2	Connection abuse	20	-	70	-
	3	Authentication failure	1	-	5	-

- IDS Policy above assigned to a specific SIP interface and subnet:

Table 8-2: IDS Policy Example

ID	SIP Interface	Proxy Set	Subnet	IDS Policy
1	1	-	-	ITSP DOS
2	-	-	10.33.0.0/16	

For more information, refer to the *User's Manual*.

8.2 Enable Syslog

The device supports the generation and reporting of Syslog messages and SNMP traps to external logging servers. It is crucial that you enable one or both of these features (preferably Syslog) so that you can monitor events on your device. In addition, as the device does not retain logged reports (SNMP is limited), it is recommended that you ensure that your Syslog server saves all logged events for future analysis and reference.

This is configured on the Syslog Settings page (**Configuration** tab > **System** > **Syslog Settings**), as shown below:

Figure 2: Enabling Syslog Server

▼ Syslog Settings	
Enable Syslog	Enable ▼
Syslog Server IP Address	10.33.2.1
Syslog Server Port	514
Debug Level	7 ▼



Note: Debug level 5 may be traffic affecting.

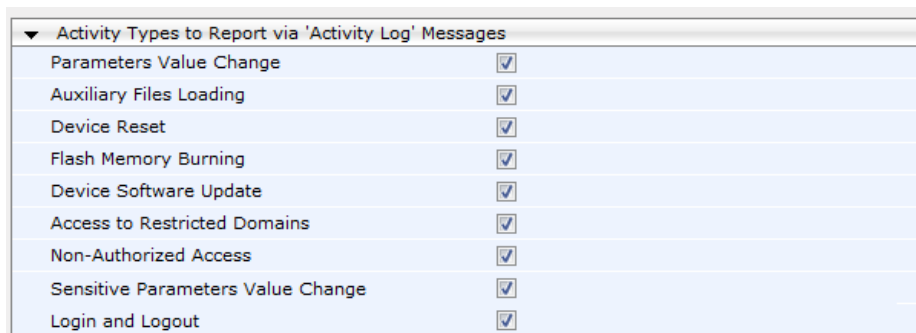
8.3 Enable Logging of Management-Related Events

Through Syslog, you can log and monitor management-related events to help you detect and identify unauthorized management-related activities such as:

- Unauthorized Web login attempts (attempts to access the Web interface with a false or empty user name or password)
- Access to restricted Web pages such as the page on which firewall rules are defined
- Modifications to parameter values (for example, deletion of firewall rules, allowing future unauthorized access)
- Modifications to "sensitive" parameters - changes made to important parameters such as IP addresses
- Unauthorized SIP messages (logged SIP messages)

This is configured in the Activity Types to Report section on the Syslog Settings page (**Configuration** tab > **System** > **Syslog Settings**), as shown below:

Figure 3: Enabling Logging of Management Events to a Syslog Server



▼ Activity Types to Report via 'Activity Log' Messages	
Parameters Value Change	<input checked="" type="checkbox"/>
Auxiliary Files Loading	<input checked="" type="checkbox"/>
Device Reset	<input checked="" type="checkbox"/>
Flash Memory Burning	<input checked="" type="checkbox"/>
Device Software Update	<input checked="" type="checkbox"/>
Access to Restricted Domains	<input checked="" type="checkbox"/>
Non-Authorized Access	<input checked="" type="checkbox"/>
Sensitive Parameters Value Change	<input checked="" type="checkbox"/>
Login and Logout	<input checked="" type="checkbox"/>

8.4 Enable Call Detail Records

Call Detail Records (CDR) provide vital information on SIP calls made through the device. This information includes numerous attributes related to the SIP call such as port number, physical channel number, source IP address, call duration, and termination reason (provided by the CDR field *TrmReason*). The device can be configured to generate and report CDRs for various stages of the call (beginning, initial connection, and end of the call). Once generated, the CDR logs are sent to a user-defined logging server.

This is configured on the Advanced Parameters page (**Configuration** tab > **VoIP** > **SIP Definitions** > **Advanced Parameters**), as shown below:

Figure 4: Enabling CDR Generation

▼ CDR and Debug	
CDR Server IP Address	<input type="text" value="10.13.5.22"/>
CDR Report Level	<input type="text" value="Start & End & Connect Call"/> ▼
Media CDR Report Level	<input type="text" value="Start & End Media"/> ▼



Note: Syslog must be enabled for this CDR feature.

9 SBC-Specific Security Guidelines

This section provides basic SBC security guidelines that should be implemented in your network deployment.



Note: This section is applicable only to AudioCodes Session Border Controllers (SBC).

9.1 General Guidelines

It is crucial that you separate trusted from un-trusted networks:

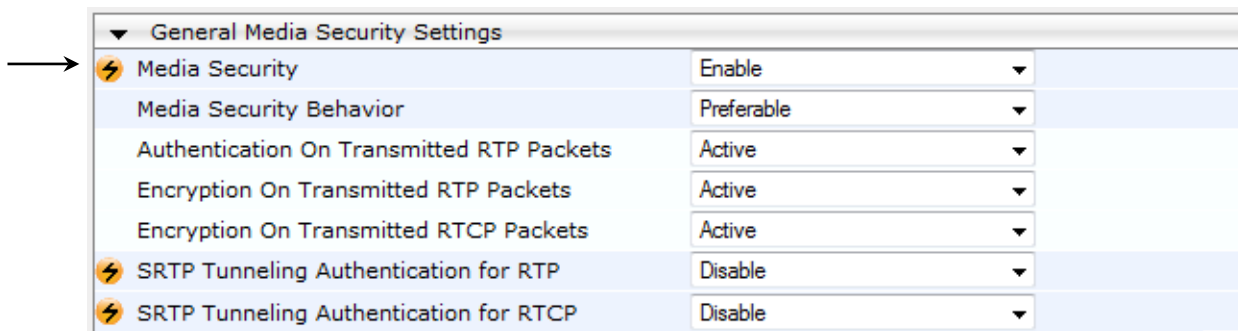
- Separate un-trusted networks from trusted networks, by using different SRDs, IP Groups, SIP Interfaces, and SIP Media Realms (with limited port range).
- Similarly, separate un-trusted networks from one another. In particular, far-end users must be separated from the ITSP SIP trunk, using a different SRD, IP Group, SIP interface, and SIP Media Realms. This separation helps in preventing attacks targeted on far-end user ports from affecting other users.
- For un-trusted networks, use strict classification rules over vague rules. For example, if the ITSP's proxy IP address, port and host name are known, then use them in the classification rules. This ensures that all other potentially malicious SIP traffic is rejected.
- Unclassified packets must be discarded (rejected).

9.2 Secure Media (RTP) Traffic using SRTP

It is recommended to use Secured RTP (SRTP) for encrypting the media (RTP and RTCP) path and thereby, protecting the VoIP traffic. The device supports SRTP according to RFC 3711. SRTP performs a Key Exchange mechanism (according to RFC 4568). This is done by adding a 'crypto' attribute to the SDP. This attribute is used (by both sides) to declare the supported cipher suites and to attach the encryption key. If negotiation of the encryption data is successful, the call is established. The device's SRTP feature supports various suites such as AES_CM_128_HMAC_SHA1_32.

- SRTP is enabled on the Media Security page (**Configuration** tab > **VoIP** > **Media** > **Media Security**) by setting the 'Media Security' parameter to **Enable**.

Figure 5: Enabling SRTP



- SRTP is enforced on the SBC legs, using IP Profiles (**Configuration** tab > **VoIP** > **Coder and Profiles** > **IP Profiles**). For each IP Profile associated with a leg, set the 'SBC Media Security Behavior' parameter to **SRTP**. This enforces the SBC legs to negotiate only SRTP media lines; RTP media lines are removed from the incoming SDP offer \ answer.

Figure 6: Enforcing SRTP per SBC Leg



9.3 Implement SIP Authentication and Encryption

It is paramount that your network implements authentication and encryption to secure the network and ensure integrity and confidentiality of sensitive communications over untrusted networks. Some of the main authentication and encryption guidelines are discussed in the subsequent sections.

9.3.1 Authenticating Users as an Authentication Server

Instead of relying on external, third-party authentication servers, the device can be configured to act as an Authentication server, performing authentication and validation challenges with SIP user agents. The SIP method (INVITE or REGISTER) on which it challenges can be defined. If the message is received without an Authorization header, the device challenges the client by sending a 401 or 407 SIP response. The client then resends the request with an Authorization header containing its user name and password. The device validates the SIP message and if it fails, the message is rejected and the device sends a 403 "Forbidden" response. If the SIP message is validated, the device verifies identification of the UA by checking whether the user name and password received from the user is correct. The user names and passwords are obtained from the User Information table. If after three attempts the UA is not successfully authenticated, the device sends a 403 "Forbidden" response. The device can also perform authentication on behalf of its UAs with an external third-party server.

To setup the E-SBC as an Authentication server, you need to do the following:

- Set the following parameters in the User-type IP Group of the UAs (**Configuration** tab > **VoIP** > **VoIP Network** > **IP Group Table**):
 - 'Authentication Mode': select **SBC as Server**.
 - 'Authentication Method List': enter "INVITE\REGISTER".

Figure 7: Setting E-SBC as Authentication Server in IP Group

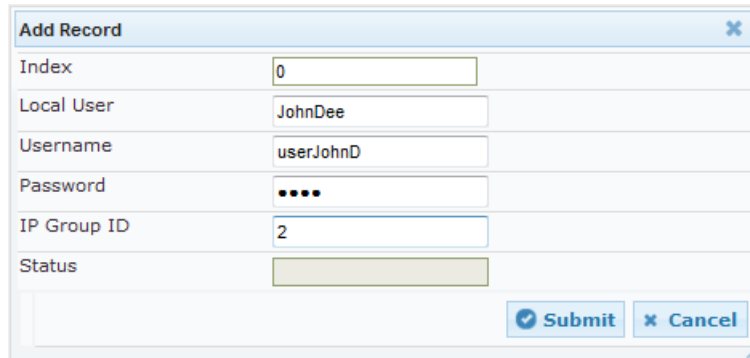
The screenshot displays the configuration interface for an SBC, with the 'SBC' tab selected. The 'Authentication Mode' is set to 'SBC as Server' and the 'Authentication Method List' is set to 'INVITE\REGISTER'. Two arrows point to these two settings.

Index	0
Classify By Proxy Set	Enable
Max Number Of Registered Users	100
Source URI Input	Not Configured
Destination URI Input	Not Configured
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	-1
Registration Mode	User initiates registrations
Authentication Mode	SBC as Server
Authentication Method List	INVITE\REGISTER
SBC Client Forking Mode	Sequential

Submit Cancel

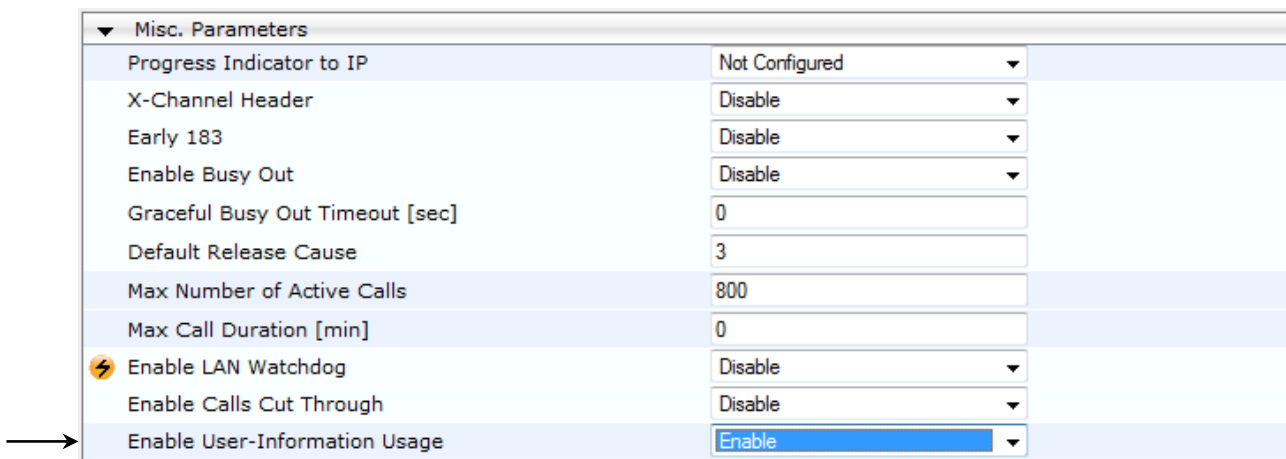
- Create a User Info table:
 - Add users with authentication usernames and passwords in the SBC User Info table (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **User Information** > **SBC User Info Table**)

Figure 8: Adding Users to User Info Table



- Enable the use of the User Info file by setting the 'Enable User-Information Usage' parameter to **Enable** on the Advanced Parameters page (**Configuration** > **VoIP** > **SIP Definitions** > **Advanced Parameters**).

Figure 9: Enabling User Info File Usage



Misc. Parameters	
Progress Indicator to IP	Not Configured
X-Channel Header	Disable
Early 183	Disable
Enable Busy Out	Disable
Graceful Busy Out Timeout [sec]	0
Default Release Cause	3
Max Number of Active Calls	800
Max Call Duration [min]	0
⚡ Enable LAN Watchdog	Disable
Enable Calls Cut Through	Disable
→ Enable User-Information Usage	Enable

9.3.2 Authenticating Users by RADIUS Server

Instead of authorizing calls locally, digest authentication of SIP users can be done by a RADIUS server (according to RFC 5090). In this way, the device offloads the MD5 calculation (validation) to the RADIUS server, where the device is classed as a RADIUS client. To implement this, the following configuration is required:

- 'RADIUS Authentication Server IP Address' – defines the RADIUS server's address
- 'RADIUS Authentication Server Port' - defines the RADIUS server's port
- 'RADIUS Shared Secret' - defines the shared secret
- 'SBC Server Auth Mode' – set to 1 to enable authentication by a RADIUS server

9.3.3 Authenticating SIP Servers as an Authentication Server

It is advised to enable the device to authenticate remote SIP servers (for example, Proxy servers). This provides protection from rogue SIP servers, preventing unauthorized usage of the device's resources and functionality. The device authenticates remote servers by challenging them with a user-defined username and password that is shared with the remote server. From such a challenge, the device can confirm the server's identity as being genuine.

SIP server authentication is configured per IP Group, thereby enabling unique authentication handling per specific calls. The configuration in the IP Group is as follows:

- 'Authentication Mode' - set to **SBC as Server**.
- 'Authentication Method List' - specifies SIP requests (for example, INVITE) that must be challenged
- 'Username' / 'Password' - shared authentication username and password :

9.3.4 Enforce SIP Client Authentication by SIP Proxy

When the device is located between a SIP client and a third-party SIP proxy server, and SIP Digest Authentication is used, the device relays authentication messages between these entities. Although the device gathers and maintains some information in its registration database (Address of Record / AOR) it does not actively participate in the authentication process. Instead, it is the SIP proxy that handles and enforces SIP client authentication. Therefore, it is imperative that your SIP proxy server be configured to enforce SIP client authentication.

9.3.5 Enforce SIP Digest Authentication by IP PBX

If TLS cannot be configured (for whatever reason) and if you are using an on-premise IP PBX, it is crucial that your IP PBX implements SIP Digest Authentication for remote users. In addition, authentication should be applied to as many SIP methods as possible (i.e., not only on REGISTER messages, but also INVITEs, re-INVITEs, etc.).

9.4 Secure Routing Rules

This section provides recommended security guidelines regarding routing rules.

9.4.1 Classify by Classification Rules versus Proxy Set

An important security functionality of the SBC is to make sure that it does not mistakenly identify incoming SIP dialog-initiating requests (e.g., INVITE messages) from malicious attackers as belonging to a configured server-type IP Group entity. The SBC provides two optional mechanisms that can be employed to identify incoming dialogs as coming from a specific server-type IP Group:

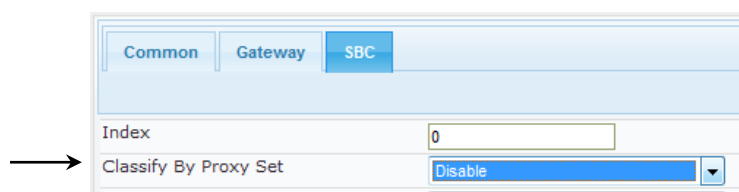
- **Classification rules in the Classification table:** Identifies incoming dialogs based on the characteristics of the SIP message such as host name in the INVITE message (Layer 4-7), and/or based on the source IP address (Layer-3).
- **Proxy Set:** Identifies incoming dialogs based on source IP address (Layer-3) only. The Proxy Set defines the address of the IP Group.

Regarding which classification method to employ, please adhere to the following guidelines:

- If the IP address of the IP Group entity is known, it is recommended to employ SIP dialog classification based on a Classification rule, where the rule is configured with not only the IP address, but also with SIP message characteristics to increase the strictness of the classification process. For more information on configuring Classification rules, see Section 9.4.2.
- If the IP address is unknown, in other words, the Proxy Set associated with the IP Group is configured with an FQDN, it is recommended to employ SIP dialog classification based on Proxy Set. This allows the SBC to classify the incoming dialog based on the DNS-resolved IP address. The reason for classifying by Proxy Set is that IP address forgery (commonly known as IP spoofing) is more difficult than malicious SIP message tampering and therefore, using a Classification rule without an IP address offers a weaker form of security. When classification is based on Proxy Set, the Classification table is ignored.

Classification by Proxy Set is enabled in the IP Group table, using the 'Classify By Proxy Set' parameter:

Figure 10: Enabling Classification based on Proxy Set in the IP Group Table



9.4.2 Define Strict Classification Rules

Classification rules are used to identify incoming SIP dialog-initiating requests (e.g., INVITE messages) and bond them to IP Groups. In other words, these rules identify the source of the call. Once the source IP Group is identified, the traffic can then be routed to its destination according to IP-to-IP routing rules.

When defining Classification rules, adhere to the following recommendations:

- For Server-type IP Groups, use Classification rules **only** if the IP address of the IP Group is known. If known, include the IP address in the Classification rule ('Source IP Address' parameter). In addition, to increase classification strictness, configure SIP message characteristics in the rule as well.



Note: If the IP address is unknown (i.e., the Proxy Set associated with the IP Group is configured with an FQDN), it is recommended to employ SIP dialog classification based on Proxy Set (see Section 9.4.1). In such a scenario, the Classification table is ignored and must not be configured for the specific IP Group.

- For Server-type IP Groups whose IP addresses are known, it is recommended to also configure VoIP firewall rules (see Section 3.1).
- Use strict Classification rules over vague ones so that all other potentially malicious SIP traffic is rejected. In other words, configure the rule with as much information as possible that accurately characterizes the incoming SIP dialog (e.g. source and destination host name).
- Define a range for the source and destination prefix numbers.
- Define a combination of Classification rules to guarantee correct and accurate identity of sender of call.
- Use Message Condition rules to increase the strictness of the Classification process. Message Condition rules enhance the process of classifying incoming SIP dialogs to an IP Group. When a Classification rule is associated with a Message Condition rule, the Classification rule is used only if its' associated Message Condition rule are matched. Message Condition rules are SIP message conditions based on the same syntax used in the Message Manipulations table. You can define complex rules using the "AND" or "OR" Boolean operands. You can also use regular expressions (regex) as Message Condition rules, for example:
 - "body.sdp regex pcmu" can be used to enable routing based on the offered codec (G.711 Mu) in the incoming SDP message
 - "body.sdp regex (AVP[0-9]|\s]*\s8[\s|\n])" can be used to enable routing based on payload type 8 in the incoming SDP message

Message Condition rules are configured in the Message Condition table (**Configuration** tab > **VoIP** > **SBC** > **Routing SBC** > **Message Condition Table**) and then later associated with Classification rules in the Classification table. The figure below shows a Message Condition rule for P-Asserted-Identity headers that contain "abc":

Figure 11: Configured Message Condition Rule in Message Condition Table

Index	Condition	Description
1	header.p-asserted-identity.url.user contains 'abc'	P-Asserted-Identity has "abc"

- The last Classification rule in the Classification table should be one that denies all calls.

Classification rules are configured in the Classification table (**Configuration** tab > **VoIP** > **SBC** > **Routing SBC** > **Classification Table**). The figure below shows an example of Classification rules:

- **Index 0 "ITSP"**: Classifies received calls to Server-type IP Group "ITSP" if they have the following incoming matching characteristics:
 - 'Source SIP Interface': 10.15.7.96
 - 'Source Username Prefix': 2 through 4
 - 'Source Host': domain.com
 - 'Destination Username Prefix': 1 through 7
 - 'Message Condition': SIP message with P-Asserted-Identity header containing "abc" (Message Condition rule described previously in this section)
- **Index 2 "Deny"**: Denies calls that cannot be classified (unknown calls).

Figure 12: Configured Classification Rules in Classification Table

Index	Source SRD ID	Source IP Address	Source Port	Source Transport Type	Source Username Prefix	Destination Username Prefix	Source IP Group ID	Action Type
0	1		0	ANY	[2-4]	[1-7]	1	Allow
1	2		0	ANY	*	*	2	Allow
2	None		0	ANY	*	*	None	Deny

Classification Table #0

Source SRD ID: 1	Source IP Address:
Source Port: 0	Source Transport Type: ANY
Source Username Prefix: [2-4]	Source Host: domain.com
Destination Username Prefix: [1-7]	Destination Host: *
Message Condition: 1	Source IP Group ID: 1
Action Type: Allow	

9.4.3 Allow Calls only with Specific SIP User-Agent Header Value

The SIP User-Agent header contains information about the User Agent Client (UAC) originating the request. This information is unique to the Enterprise and therefore, it is recommended to configure your device so that it allows calls only with a specified User-Agent header value.

This is configured by adding a Message Condition rule for this SIP header type and then assigning the rule to a Classification rule.

The figure below shows a Message Condition rule in the Message Condition table (**Configuration** tab > **VoIP** > **SBC** > **Routing SBC** > **Message Condition Table**) whose condition is for the SIP User-Agent header to have the value "abc.com":

Figure 13: Condition Rule

Index	Condition	Description
0	header.user-agent='abc.com'	Accept only abc.com calls

The above configured Message Condition rule is assigned to the Classification rule in the Classification table (**Configuration** tab > **VoIP** > **SBC** > **Routing SBC** > **Classification Table**).

Figure 14: Condition Rule Assigned to Classification Rule

Index	Source SRD ID	Source IP Address	Source Port	Source Transport Type	Source Username Prefix	Destination Username Prefix	Source IP Group ID	Action Type
1	None		0	ANY	[2-4]	[1-7]	1	Allow

Classification Table #1

Source SRD ID: None	Source IP Address:
Source Port: 0	Source Transport Type: ANY
Source Username Prefix: [2-4]	Source Host: domain.com
Destination Username Prefix: [1-7]	Destination Host: itsp.com
Message Condition: 1	Source IP Group ID: 1
Action Type: Allow	

9.4.4 Block Unclassified Calls

It is recommended that you block incoming calls that cannot be classified to an IP Group, based on the rules in the Classification table (discussed in the previous section). If unclassified calls are not blocked, they are sent to the default SRD / IP Group and therefore, illegitimate calls can be established.

This is configured on the General Settings page (**Configuration** tab > **VoIP** > **SBC** > **SBC General Settings**), by setting the Unclassified Calls' parameter to **Reject**:

Figure 15: Blocking Unclassified Incoming Calls



SBC Survivability Registration Time [sec]	0
Forking Handling Mode	Latch On First
Unclassified Calls	Reject
Session-Expires [sec]	180
Direct Media	Disable

9.4.5 Define Strict Routing Rules

It is crucial that you adhere to the following guidelines when configuring your IP-to-IP routing rules:

- Ensure that your routing rules are accurate and correctly defined. Inaccurate or weak routing rules can easily result in Service Theft.
- Ensure that your routing rules from **source IP Group** to **destination IP Group** are accurately defined to be eligible for the desired call routing outcome.
- Avoid (if possible) using the asterisk (*) symbol to indicate "any" for a specific parameter in your routing rules. This constitutes weak routing rules that can be vulnerable to attackers. For strong routing rules, enter specific alphanumeric values instead of the asterisk.

9.5 Define Call Admission Control Rules

It is recommended to define call admission control (CAC) rules for regulating VoIP traffic volume. CAC rules can help in limiting the rate of call requests, preventing excessive signaling requests (originating from malicious and legitimate sources) from overwhelming your network resources.

CAC rules limit the number of concurrent calls (SIP dialogs) per IP Group / SRD (or for all IP Groups / SRDs). The call limitation can be defined per SIP-dialog initiating request type (e.g., INVITE or REGISTER messages), direction (inbound, outbound, or both), and user. Requests that exceed the user-defined limits are rejected (with SIP 486 "Busy Here" responses). You can also limit the incoming packet rate based on the "token bucket" mechanism.

Adhere to the following CAC recommendations:

- It is crucial that your CAC rules include call limitations per user. This ensures that a user does not make unlimited, simultaneous calls.
- Define rules as specific as possible. For example, instead of defining one rule for all SIP request types, create rules for each SIP request type.

Note that if the call routing to a specific IP Group is blocked due to a CAC rule, the device searches for an alternative route (if defined) in the SBC IP-to-IP Routing table. If this

alternative route does not exceed the CAC rule limitation, the device uses it to route the call.

The CAC rules are configured In the Admission Control table (**Configuration** tab > **VoIP** > **SBC** > **Admission Control**). The figure below displays a CAC rule that defines a maximum of 100 concurrent SIP dialog-initiating requests for IP Group #2. SIP requests received above this threshold are rejected:

Figure 16: Configured CAC Rule

▼ Admission Control

Show/Hide

Index	Admission Name	Limit Type	IP Group ID	SRD ID	Request Type	Request Direction	Limit	Limit per User	Rate
0	MaxIPG2	IP Group	-1	-1	All	Both	100	-1	0

View 1 - 1 of 1

Selected Row #0

Admission Name:	MaxIPG2	Limit:	100
Limit Type:	IP Group	Limit per User:	-1
IP Group ID:	-1	Rate:	0
SRD ID:	-1	Maximum Burst:	0
Request Type:	All	Reserved Capacity:	0
Request Direction:	Both		

9.6 Secure SIP User Agent Registration

Service theft can result from a lack of security in the SIP user registration process. This section provides recommended guidelines regarding user registration.

9.6.1 Configure Identical Registration Intervals

In scenarios where the device does not send registrations to a server (e.g., a PBX), if the device receives a new REGISTER request from the same number (i.e., same AOR) but without an Authentication header, the device still sends a SIP 200 OK response to the user. This is because the AOR exists in the device's SBC registration database. Therefore, if an illegitimate user attempts to connect with a legitimate IP address and phone number (without authentication), the malicious user is able to connect and steal calls. To overcome this and prevent stealing of calls, ensure that you set the user and proxy registration times with identical values, as shown below:

- Define the duration of the periodic registrations between the user and the device in the 'SBC User Registration Time' field on the General Settings page (**Configuration** tab > **VoIP** > **SBC** > **SBC General Settings**):
- Define the time interval (in seconds) for registering to the server (e.g., PBX) in the 'SBC Proxy Registration Time' field on the General Settings page (**Configuration** tab > **VoIP** > **SBC** > **SBC General Settings**):

Figure 17: Configured User Registration Time

BroadWorks Survivability Feature	Disable
BYE Authentication	Disable
SBC User Registration Time [sec]	100
SBC Proxy Registration Time [sec]	100
SBC Survivability Registration Time [sec]	0
Forking Handling Mode	Latch On First



9.6.2 Limit SBC Registered Users per IP Group / SRD

It is recommended that you define a maximum number of allowed registered users per IP Group (User-type IP Group). This ensures that illegitimate users are blocked from registering with this IP Group.

This is configured in the IP Group table or SRD table (**Configuration** tab > **VoIP** > **VoIP Network** > **IP Group Table**) in the 'Max. Number of Registered Users' field:

Figure 18: Configured Maximum Registered Users in IP Group

The screenshot shows the 'IP Group Table' configuration interface. At the top, there are buttons for 'Add +', 'Edit', and 'Delete -', along with a 'Show/Hide' button. Below this is a table with the following columns: Index, Type, Description, Proxy Set ID, SIP Group Name, Contact User, Local Host Name, SRD, Media Realm Name, and IP Profile ID. The table contains one row with the following values: Index: 1, Type: User, Description: (empty), Proxy Set ID: -1, SIP Group Name: (empty), Contact User: (empty), Local Host Name: (empty), SRD: 0, Media Realm Name: (empty), IP Profile ID: 0. Below the table, there is a pagination control showing 'Page 1 of 1' and 'Show 10 records per page'. The main configuration area is titled 'IP Group Table #1' and contains two columns of settings. The left column includes: Type: User, Proxy Set ID: -1, Contact User: (empty), SRD: 0, IP Profile ID: 0, Routing Mode: Not Configured, Enable Survivability: Disable, Classify By Proxy Set: Enable, Source URI Input: Not Configured, Inbound Message Manipulation Set: -1, and Registration Mode: User initiates registrations. The right column includes: Description: (empty), SIP Group Name: (empty), Local Host Name: (empty), Media Realm Name: (empty), Always Use Route Table: No, SIP Re-Routing Mode: Not Configured, Serving IP Group ID: -1, Max Number Of Registered Users: 100 (indicated by a black arrow), Destination URI Input: Not Configured, Outbound Message Manipulation Set: -1, and Authentication Mode: User Authenticates. At the bottom of the right column, it says 'SBC Client Forking Mode: Sequential'.

Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User	Local Host Name	SRD	Media Realm Name	IP Profile ID
1	User		-1				0		0

IP Group Table #1

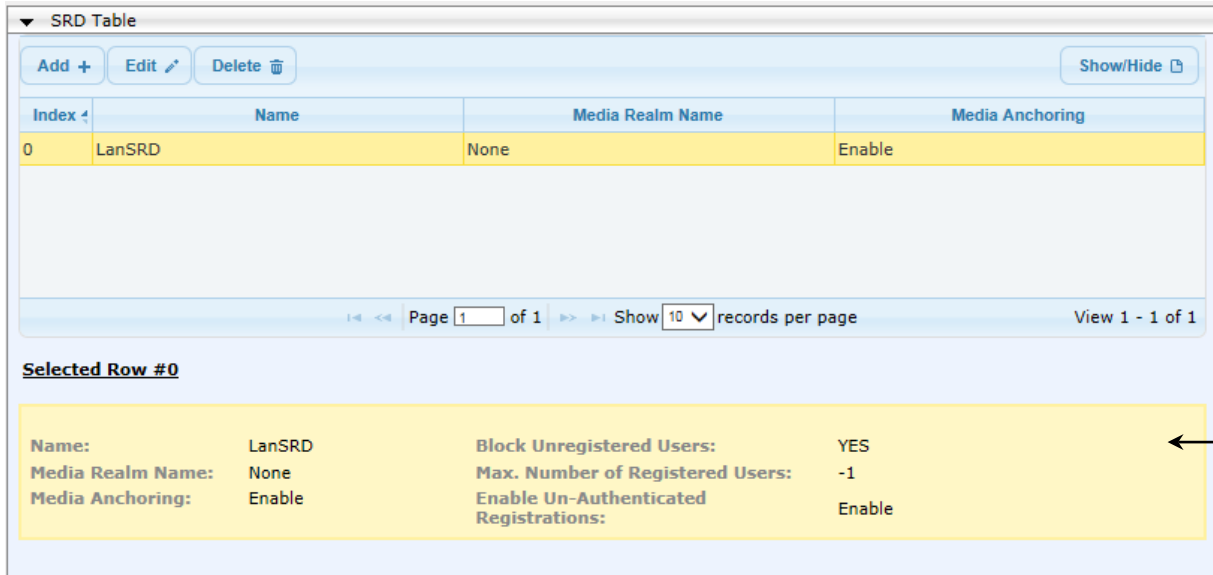
Type: User	Description:
Proxy Set ID: -1	SIP Group Name:
Contact User:	Local Host Name:
SRD: 0	Media Realm Name:
IP Profile ID: 0	Always Use Route Table: No
Routing Mode: Not Configured	SIP Re-Routing Mode: Not Configured
Enable Survivability: Disable	Serving IP Group ID: -1
Classify By Proxy Set: Enable	Max Number Of Registered Users: 100
Source URI Input: Not Configured	Destination URI Input: Not Configured
Inbound Message Manipulation Set: -1	Outbound Message Manipulation Set: -1
Registration Mode: User initiates registrations	Authentication Mode: User Authenticates
Authentication Method List:	SBC Client Forking Mode: Sequential

9.6.3 Block Calls from Unregistered Users

Ensure that calls from unregistered users are blocked (rejected) and that calls from only registered users are allowed.

This is configured in the SRD table (**Configuration** tab > **VoIP** > **VoIP Network** > **SRD Table**), by setting the 'Block Unregistered Users' parameter to **YES**.

Figure 19: Blocking Unregistered Users



The screenshot shows the 'SRD Table' configuration interface. At the top, there are buttons for 'Add +', 'Edit', and 'Delete', along with a 'Show/Hide' button. Below this is a table with the following data:

Index	Name	Media Realm Name	Media Anchoring
0	LanSRD	None	Enable

Below the table, there is a pagination control showing 'Page 1 of 1' and 'Show 10 records per page'. Underneath, the 'Selected Row #0' configuration is displayed in a yellow box:

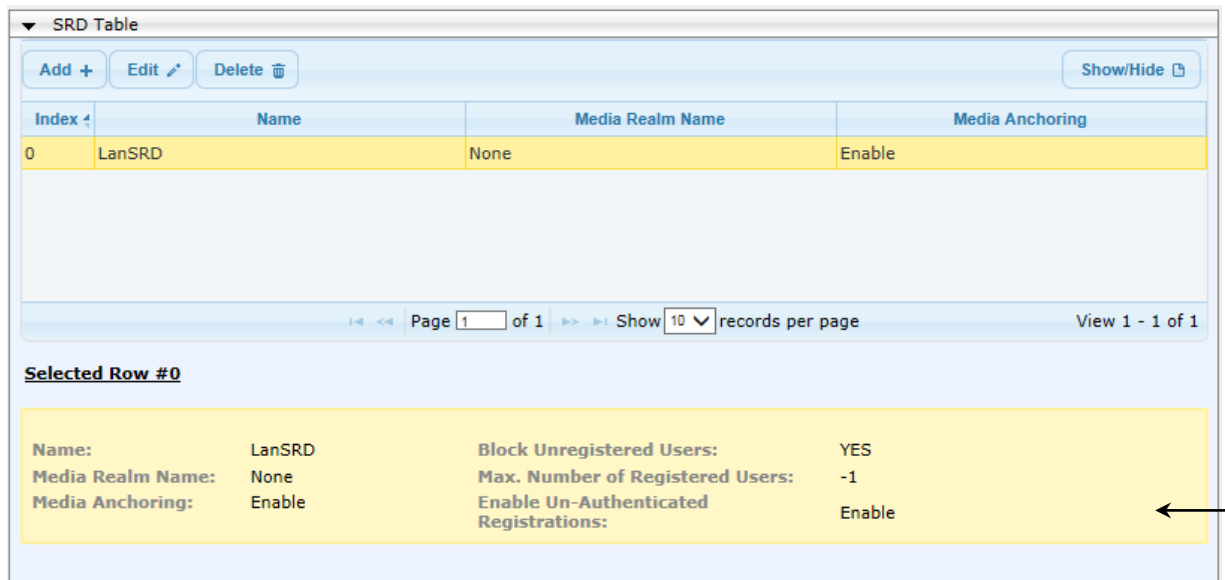
Name:	LanSRD	Block Unregistered Users:	YES
Media Realm Name:	None	Max. Number of Registered Users:	-1
Media Anchoring:	Enable	Enable Un-Authenticated Registrations:	Enable

An arrow points to the 'Block Unregistered Users: YES' parameter in the configuration details.

9.6.4 Block Registration from Un-Authenticated Users

Ensure that un-authenticated users cannot register to the SBC's registration database. In this case, the SBC registers only users who have been authenticated by a SIP proxy server. This is configured on the SRD Settings page (**Configuration** tab > **VoIP** > **VoIP Network** > **SRD Table**), by setting the 'Enable Un-Authenticated Registrations' parameter to **Yes**.

Figure 20: Preventing Registration of Un-Authenticated Users



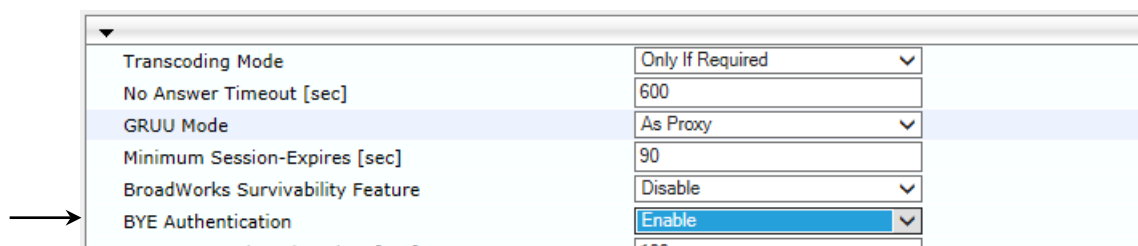
9.7 Authenticate BYE Messages

It is recommended to enable the device to authenticate all received SIP BYE requests before disconnecting the call. This feature prevents, for example, a scenario in which the SBC SIP client receives a BYE request from a third-party imposer assuming the identity of a participant in the call and as a consequence, the call between the first and second parties is inappropriately disconnected.

When enabled, the device sends a SIP authentication response to the sender of the BYE request and waits for the user to authenticate it. The call is disconnected only if the authenticating server responds with a 200 OK.

This is configured on the SBC General Settings page (**Configuration** tab > **VoIP** > **SBC** > **SBC General Settings**) by setting the 'BYE Authentication' to **Enable**.

Figure 9-21: Enabling BYE Authentication



9.8 Use SIP Message Manipulation for Topology Hiding

The device intrinsically employs topology hiding, limiting the amount of topology information displayed to external parties (i.e., un-trusted networks). This anonymous information minimizes the chances of directed attacks on your network.

The device employs topology hiding by implementing back-to-back user agent (B2BUA) leg routing:

- Strips all incoming SIP Via header fields and creates a new Via value for the outgoing message
- Each leg has its own Route/Record Route set
- Generates a new SIP Call-ID header value (different between legs)
- Changes the SIP Contact header to the device's address
- Performs Layer-3 topology hiding by modifying the source IP address in the SIP IP header (for example, IP addresses of ITSPs equipment such as proxies, gateways, and application servers can be hidden from outside parties)

In addition, to enhance topology hiding, you can modify the SIP To header, From header, and/or Request-URI host name. This can be done using the Message Manipulation table or the IP Group (for SIP URI host part manipulations). The Message Manipulation table also supports Regular Expressions (Regex).

10 Gateway-Specific Security Guidelines

This section describes recommended security guidelines for the device's supporting the Gateway application. These guidelines are important for preventing malicious attacks such as DoS.

10.1 Block Calls from Unknown IP Addresses

Ensure that the device accepts incoming calls only from source IP addresses that are defined in the Proxy Set table or Outbound IP Routing table. In addition, if an FQDN is defined in these tables, the call is accepted only if the resolved DNS IP address of the call is defined in any one of these tables. All other calls whose source IP address is not defined in these tables are rejected. This is useful in preventing unwanted SIP calls, SIP messages, and VoIP spam.

This is configured on the Advanced Parameters page (**Configuration** tab > **VoIP** > **SIP Definitions** > **Advanced Parameters**), by setting the 'IP Security' parameter to **Secure All calls**:

Figure 22: Allowing Calls only from Defined IP Addresses

▼ General	
IP Security	Secure Incoming calls ▼
Filter Calls to IP	Don't Filter ▼

10.2 Enable Secure SIP (SIPS)

Ensure that you enable Secure SIP (SIPS) so that the device initiates TLS all the way to the destination, i.e., over multiple hops. SIPS runs SIP over TLS on a hop-by-hop basis. This is important as using TLS as a transport by itself guarantees only encryption over a single hop. Since it is very common for a SIP call to traverse multiple proxy servers from one end to the other, there is a need to guarantee end-to-end security for SIP traffic. A call to a SIPS URI is guaranteed to be encrypted from end to end. All SIP traffic within this call is secured using TLS from the sender to the domain of the final recipient.

This is configured on the SIP General Parameters page (**Configuration** tab > **VoIP** > **SIP Definitions** > **General Parameters**), by setting the following parameters:

- 'SIP TLS Local Port': enter the TLS port for SIP traffic.
- 'Enable SIPS': select **Enable**.

Figure 23: Defining SIP over TLS (For Gateway Application)

Session Expires Method	Re-INVITE ▼
Asserted Identity Mode	Disabled ▼
Fax Signaling Method	T.38 Relay ▼
Detect Fax on Answer Tone	Initiate T.38 on Preamble ▼
SIP Transport Type	UDP ▼
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5061
Enable SIPS	Enable ▼



Note: It is highly recommended to use the 'Enable SIPS' parameter and not the 'SIP Transport Type' parameter to define TLS. The 'SIP Transport Type' parameter provides only a TLS connection to the next network hop, whereas the 'Enable SIPS' parameter provides TLS to the final destination (over multiple hops).

10.3 Define Strict Routing Rules

When defining IP-to-Tel (Inbound IP Routing table) and Tel-to-IP (Outbound IP Routing table) routing rules, it is crucial that you adhere to the following security guidelines:

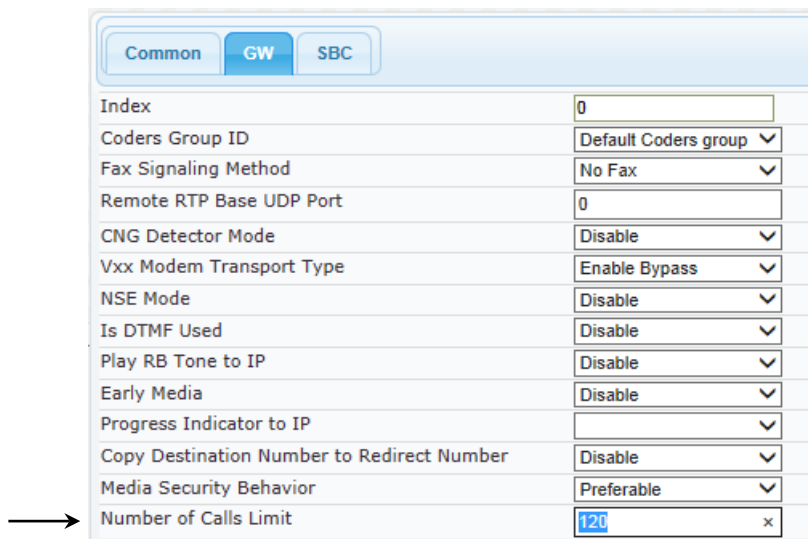
- Ensure that your routing rules are accurate and correctly defined for the desired routing outcome. Inaccurate or “loose” routing rules can easily result in Service Theft.
- Avoid, if possible, using the asterisk "*" symbol to indicate "any" for a specific parameter in your routing rules. This constitutes weak routing rules that can be vulnerable to attackers. For strong routing rules, enter specific alphanumeric values instead of the asterisk.

10.4 Define Call Admission Control

Ensure that you set the maximum, allowed concurrent calls per routing rule or IP Group. This is done by defining a call limit for an IP Profile and then assigning the IP Profile to IP-to-Tel and/or Tel-to-IP routing rules, or IP Groups. Note that this maximum number of calls takes into account incoming and outgoing calls (i.e., summation of all calls to which the IP Profile is assigned).

This is configured in the 'Number of Calls Limit' field on the IP Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**):

Figure 24: Configured Maximum Concurrent Calls for IP Profile



The screenshot shows the 'IP Profile Settings' page with the 'GW' tab selected. The 'Number of Calls Limit' field is highlighted with a blue arrow pointing to it from the left. The value '120' is entered in the field, and a small 'x' icon is visible to the right of the input box. Other fields include Index (0), Coders Group ID (Default Coders group), Fax Signaling Method (No Fax), Remote RTP Base UDP Port (0), CNG Detector Mode (Disable), Vxx Modem Transport Type (Enable Bypass), NSE Mode (Disable), Is DTMF Used (Disable), Play RB Tone to IP (Disable), Early Media (Disable), Progress Indicator to IP (empty), Copy Destination Number to Redirect Number (Disable), and Media Security Behavior (Preferable).

This page is intentionally left blank.



Security Guidelines



www.audiocodes.com