A MITEL
PRODUCT
GUIDE

AG4100 Series Analog Gateway Administration Guide

Document Version 7.1

August 2026

Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks Corporation (MITEL®).** The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC), its affiliates, parents, or subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website:http://www.mitel.com/trademarks.

Contents

What Is New in This Document 1

Summarizes the significant content changes made to each published version of this document, with links to the affected topics.

This section summarizes the changes made to this document to reflect new and changed AG4124/AG4172 Analog Gateway functionality. For details on the underlying feature updates, see the *Bug Fixes and Improvements* section of the *AG41xx yy.yy.yy.yy Release Notes*.

The changes are summarized in the following tables.

Table 1: Document Version 7.1

Feature/enhancement	Update	Location	Publish date
AG Standalone Behavior When MiVB Is Unavailable	Newly added.	Analog Gateway Behavior When the SIP Server Is Unavailable on page 149	August 2026

Table 2: Document Version 7.0

Feature/enhancement	Update	Location	Publish date
AG4124 Analog Gateway Support for MiVoice Business	Updated document content.	Configuring Analog Gateway With MiVoice Business on page 129	June 2026
Configuring Hotline Feature	Updated document content.	Configure the Hotline Feature From MiVoice Business on page 36	June 2026
Port	Updated document content.	Port on page 67	June 2026
Local Network	Updated the description of the WAN Dual Mode parameter.	Local Network on page 48	June 2026
SIP Server	Updated document content.	SIP Server on page 56	June 2026

Feature/enhancement	Update	Location	Publish date
Tel Profile	Updated document content.	Tel Profile on page 64	June 2026
Line Parameters	Updated document content.	Line Parameters on page 70	June 2026
FXS Parameters	Updated document content.	FXS Parameters on page 73	June 2026
Service Parameters	Updated the description of the Domain Query Type parameter.	Service Parameters on page 77	June 2026
NAT Parameter	Updated document content.	NAT Parameter on page 86	June 2026
Feature Codes	Updated document content.	Feature Codes on page 89	June 2026
Call and Routing	Updated document content.	Call and Routing on page 94	June 2026
Manipulation	Updated document content.	Manipulation on page 100	June 2026
SNMP	Updated document content.	SNMP on page 103	June 2026
Syslog	Updated document content.	Syslog on page 105	June 2026
ACL Configuration for Analog Gateway	Updated document content.	ACL Configuration for Analog Gateway on page 111	June 2026
Certificate Management	Updated document content.	Certificate Management on page 113	June 2026

Feature/enhancement	Update	Location	Publish date
Firmware Upload	Updated document content.	Firmware Upload on page 117	June 2026
Network Capture	Updated document content.	Perform a Network Capture on page 125	June 2026
MiVoice Business - Resiliency Configuration	Newly added.	MiVoice Business Resiliency Configuration on page 146	June 2026
Configuring AG Connectivity to MiVB through MBG (Teleworker Mode)	Newly added.	Configuring AG Connectivity to MiVB Through MBG (Teleworker Mode) on page 139	June 2026
Sample Network Capture Procedures	Newly added.	Perform a Network Capture on page 125	June 2026
Sample Digitmap Configuration	Newly added.	Sample Digitmap Configuration on page 93	June 2026
Sample NAT Parameter Configuration	Newly added.	Sample NAT Parameter Configuration on page 88	June 2026

Table 3: Document Version 6.0

Feature/enhancement	Update	Location	Publish date
ACL Configuration	Updated the ACL configuration to prevent login failures.	ACL Configuration for Analog Gateway on page 111	November 2025
Feature list for AG4124/ AG4172 Analog Gateway in OpenScape Business	Added Appendix C.	Configuring OpenScape Business for Use With the Mitel AG4124/ AG4172 Analog Gateway on page 158	September 2025

Table 4: Document Version 5.0

Feature/enhancement	Update	Location	Publish date
AG4124 Analog Gateway Support for MiVoice MX-ONE	Updated document content.	Configuring Analog Gateway With MiVoice MX-ONE on page 152	May 2025
Australian Compliance	Added the procedure for Australian compliance.	Configure the AG for Australian Regulatory Compliance on page 164	
AG4124/AG4172 Analog Gateway Support for OpenScape Business	Added Appendix C.	Configuring OpenScape Business for Use With the Mitel AG4124/ AG4172 Analog Gateway on page 158	March 2025

Table 5: Document Version 4.0

Feature/enhancement	Update	Location	Publish date
AG4124/AG4172 Analog Gateway Support for MiVoice Business	Updated to include AG4172 support for the MiVoice Business 10.2 release.	Configuring Analog Gateway With MiVoice Business on page 129	November 2024
	On the **Certificate Manage** page, the **Only Accept Trusted** parameter has been removed. This change does not affect the upgrade process.	For information on certificate upload, see Certificate Management on page 113.	
	Added support for uploading Certificate Authority (CA) certificates through the Web Management System.		
	Added support for the *No Operation Logout Time* parameter.	To configure this parameter, see Table 46: Description of System Parameters on page 91.	

Feature/enhancement	Update	Location	Publish date
	The same firmware package can be used on both the AG4172 and AG4124.	For information on firmware upload, see Firmware Upload on page 117.	
	Vendor Class Identifier (Option 60) is added to identify the firmware on the Dynamic Host Configuration Protocol (DHCP) server.	For more information, see DHCP Option on page 53.	
	Added information about role-based access for the new user role.	Table 57: Role-Based Access on page 107	
	Updated the FXS Parameters.	FXS Parameters on page 73	
	Updated the SIP compatibility parameters.	SIP Compatibility Parameters on page 80	
	Updated the number dialing plan.	Methods of Number Dialing on page 29	
	Added the Positive Disconnect feature configuration.	Configure Positive Disconnect on page 34	
	Added the Secondary dial tone feature configuration.	Configure Second Dial Tone on page 35	
	Added the procedure to resolve the Hypertext Transfer Protocol Secure (HTTPS) certificate expiry scenario.	Handle HTTPS Certificate Expiry on page 37	
	For the AG4172, added the procedure to update the Us erCard Firmware.	Update the UserCard Firmware (AG4172 Only) on page 38	

Table 6: Document Version 3.0

Feature/enhancement	Update	Location	Publish date
AG4124 Analog Gateway Support for MiVoice MX-ONE	Updated to include MiVoice MX-ONE support from release 7.6 onward.	Configuring Analog Gateway With MiVoice MX-ONE on page 152	December 2023

Preface 2

This chapter contains the following section(s):

- About This Manual
- About the AG4124/AG4172 Documentation Set
- Intended Audience
- Disclaimer
- About Security

Front matter for the AG4124/AG4172 Analog Gateway Administration Guide, including the manual's scope, the documentation set, intended audience, disclaimer, and security information.

2.1 About This Manual

Describes the purpose of this manual and the AG4124/AG4172 firmware versions it applies to.

This manual describes the AG4124/AG4172 Analog Gateway, including how to install, configure, and use it. Read this document carefully before you begin installing the Analog Gateway.

This guide applies to the AG4124 and AG4172 with the following firmware versions:

Note: Starting from firmware version **33.83.12.08 and later**, the firmware versions for both **AG4124** and **AG4172** are aligned and use the same version numbering.

- **AG4124:**
  - *33.83.11.29*
  - *33.83.12.08*
  - *33.83.12.15*
- **AG4172:**
  - *33.83.12.08*
  - *33.83.12.15*

2.2 About the AG4124/AG4172 Documentation Set

Lists the related Mitel product documents that complement this guide.

This guide is complemented by the following documents for the AG4124/AG4172 Analog Gateway and other Mitel products:

- AG4100 Analog Gateway
- MiVoice Business
- General IP Phone Documentation
- MiVoice Border Gateway

- MiVoice 5000
- MiVoice MX-ONE

Note: Always use the latest version of these documents.

2.3 Intended Audience

Identifies who this manual is written for.

This manual is written primarily for:

- Administrators
- Engineers who install, configure, and maintain the Analog Gateway

2.4 Disclaimer

Notes that images and sample data shown in this guide are for demonstration purposes only.

The images, screenshots, server names, file names, and database names used in this document are for demonstration purposes only. Actual names, screens, or images may vary from those shown here, particularly after updates to the Web Management System user interface.

2.5 About Security

Points administrators and installers to the documents that describe AG4124/AG4172 security controls.

Before you install or administer the AG4124/AG4172 Analog Gateway, become familiar with its security controls.

The following documents provide details about the AG4100 security controls in their *Security* section:

- *Personal Data Protection and Privacy Controls*
  Helps you identify the information you need to comply with applicable security regulations.
- *Analog Gateway Security Guidelines*
  Provides an overview of the security mechanisms available to protect the AG4124/AG4172 Analog Gateway from network threats and to maintain user data privacy.

For the latest version of these documents, see AG4100 Analog Gateway.

2.5.1 Additional Security Documentation

Lists further MiVoice Business and MiVoice MX-ONE security documents available on the Mitel Document Center.

Additional security information is available on the Mitel Document Center:

- See MiVoice Business for the latest version of the following documents:
  - *MiVoice Business Security Guidelines*

- *MiVoice Business Secure Voice Communications*
- *MiVoice Business Security FAQ*

- See MiVoice MX-ONE for the latest version of the following documents:
  - *MiVoice MX-ONE Personal Data Protection and Privacy Controls*
  - *MiVoice MX-ONE Security Guidelines*

Product Introduction 3

This chapter contains the following section(s):

Introduces the AG4124/AG4172 Analog Gateway: what it is, where it fits in the network, and its physical and feature specifications.

3.1 Overview

Introduces the AG4124/AG4172 as multi-functional Analog Gateways and lists their part numbers and Field Replacement Units.

The AG4124/AG4172 are multi-functional Analog Gateways that offer seamless connectivity between Internet Protocol (IP)-based telephony networks and legacy analog telephones, fax machines, and other analog devices. The AG4124 gateway provides both RJ-11 and RJ-21 Foreign Exchange Station (FXS) interfaces. The AG4172 provides RJ-21 FXS interfaces. Both provide a comprehensive feature set, ideally suited for all types of businesses that need cost-efficient analog to VoIP services.

Note: The AG4172 Analog Gateway device only provides RJ-21 interfaces, unlike the AG4124, which provides RJ-11 and RJ-21 interfaces.

The Mitel AG4124 Analog Gateway part number is *50008403 AG4124 Universal (w/o AC cord)*.

The Mitel AG4172 Analog Gateway part number is *50008407 AG4172 Universal (w/o AC cord)*.

The Mitel AG4124/AG4172 Analog Gateway Field Replacement Units (FRUs) are listed below:

- 51311137 AG4124/AG4172 Installation Kit
- 50006271 PWR CRD C13 10A 125V - North America Plug
- 50005611 PWR CRD C13 10A 250V - European Plug
- 50005612 PWR CRD C13 5A 250V - United Kingdom Plug (5A FUSE)
- 50006270 PWR CRD C13 10A 250V - Australian Plug

3.2 Application Scenario

Shows how the AG4124/AG4172 Analog Gateway fits into the network and warns against direct Internet connection.

The following figure illustrates a typical application scenario for the AG4124/AG4172 Analog Gateway.

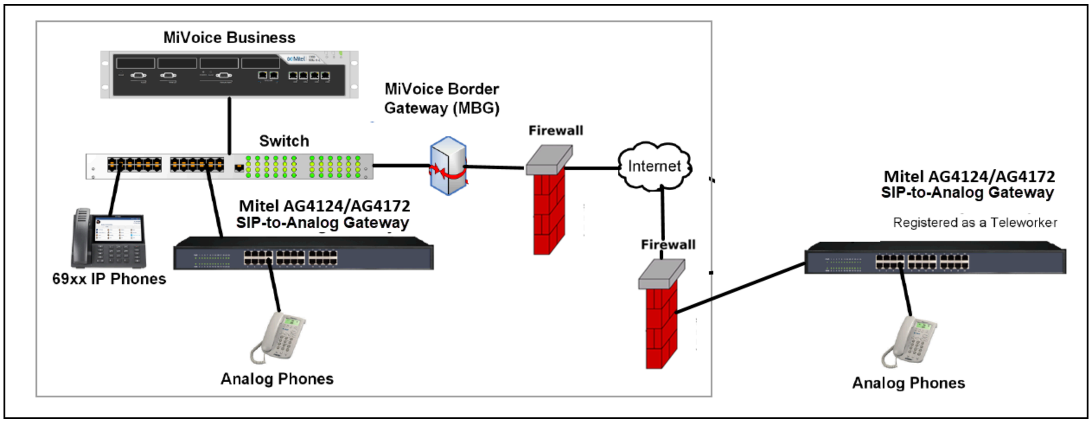

Figure 1: Application Scenario of AG4100

CAUTION: The AG4124/AG4172 Analog Gateway must never be connected directly to the Internet. If it must be reachable from the Internet, connect it through a correctly configured firewall.

3.3 Product Description

Covers the physical description of the AG4124/AG4172 Analog Gateway: front/rear panels and physical interfaces.

3.3.1 Front and Rear Panels

Describes the connectors and indicators on the front and rear panels of the AG4124 and AG4172 Analog Gateways.

Front and Rear Panels AG4124

The following image shows the front panel of the AG4124 Analog Gateway.

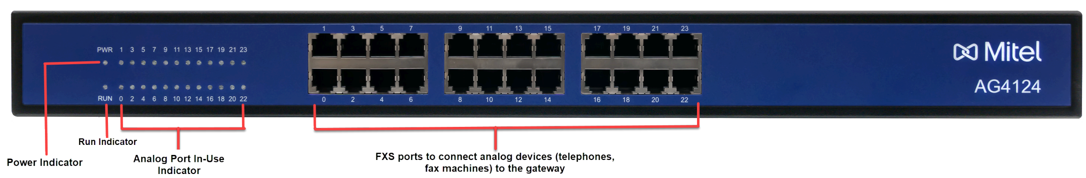

Figure 2: Front Panel AG4124

The following image shows the rear panel of the AG4124 Analog Gateway.

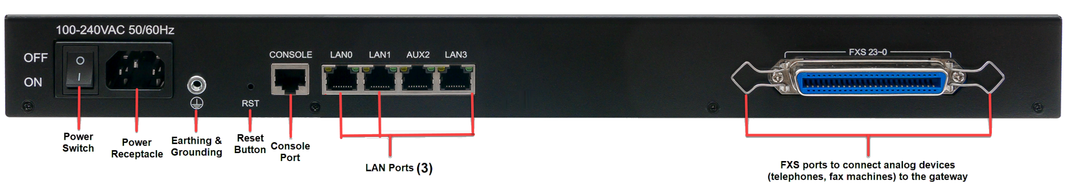

Figure 3: Rear Panel AG4124

Following is a description of the interfaces on the AG4124 Analog Gateway.

Table 7: Connectors

Port name	Connector	Description
Power Receptacle	IEC-950	To connect 100-240 VAC, 50-60 Hz power supply.
LAN Port Qty 3	RJ-45	To connect to the Internet Protocol (IP) network.
FXS Ports 0-23	RJ-11	Foreign Exchange Station (FXS) ports to connect a standard analog phone, a fax machine, or a Private Branch Exchange (PBX).
Console Port	RJ-48	Console port is used to carry out maintenance-related configurations.
AUX2 Port	RJ-45	AUX2 port is for factory use only.

Following is a description of the indicators on the AG4124 Analog Gateway.

Table 8: Indicators

Indicator	Definition	Status	Description
PWR	Shows whether the AG4124 Analog Gateway is on or off	On	The AG4124 Analog Gateway is on.
		Off	The AG4124 Analog Gateway is off, or the power supply is defective.
RUN	Shows whether the AG4124 Analog Gateway is working well	Slow flicker	The AG4124 Analog Gateway works properly.
		Fast flicker	The Session Initiation Protocol (SIP) account is registered.

Indicator	Definition	Status	Description
		Off	The AG4124 Analog Gateway is working improperly.
FXS	Shows whether the port is in use	On	The FXS port is in use.
		Off	The FXS port is inactive or defective.
LAN	Shows whether the AG4124 Analog Gateway is connected to the network	Flicker	The AG4124 Analog Gateway is connected to the network.
		Off	The AG4124 Analog Gateway is disconnected from the network, or the network is defective.
	Network speed	Slow flicker	100 Mbps
		Fast flicker	10 Mbps

Front and Rear Panels AG4172

The following image shows the front panel of the AG4172 Analog Gateway.

Figure 4: Front Panel AG4172

The following image shows the rear panel of the AG4172 Analog Gateway.

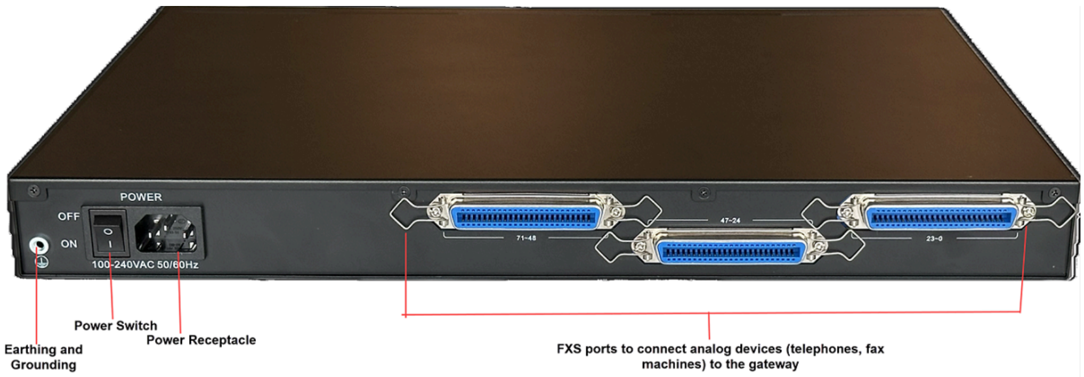

Figure 5: Rear Panel AG4172

Following is a description of the interfaces on the AG4172 Analog Gateway.

Table 9: Connectors

Port name	Connector	Description
Power Receptacle	IEC-950	To connect 100-240 VAC, 50-60 Hz power supply.
LAN Port Qty 2	RJ-45	To connect to the IP network.
FXS Ports 0-72	RJ-21	FXS ports to connect a standard analog phone, a fax machine, or a PBX.
MGMT Qty 1	RJ-45	Management: this is a dedicated Ethernet port used for local access to the Web Management System. **Note**: Do not use this port to connect the AG4100 to the customer's LAN. For more information, see Configure the AG4172 Management Port on page 26.
Console Port	RJ-48	Console port is used to carry out maintenance-related configurations.
AUX Port	RJ-45	AUX port is for factory use only.

Following is a description of the indicators on the AG4172 Analog Gateway.

Table 10: Indicators

Indicator	Definition	Status	Description
PWR	Power indicator	On	The AG4172 Analog Gateway is on.
		Off	The AG4172 Analog Gateway is off, or there is no power supply
RUN	Running indicator	Slow flashing	The AG4172 Analog Gateway is running properly. Slow flashing means the running indicator flashes for 2 seconds.
		Fast flicker	The SIP account is registered successfully. Fast flashing means the running indicator flashes for 0.5 seconds.
		Off	The AG4172 Analog Gateway is running improperly.
FXS	Telephone In-use Indicator	On	FXS port is currently occupied by a call
		Off	FXS port is idle or faulty
MGMT	Network Link Indicator	Green Flashing	The gateway is properly connected to the network.
		Off	The gateway is not connected to the network, or the network connection is faulty.

Indicator	Definition	Status	Description
	Network Speed Indicator	On	100 Mbps
		Off	10 Mbps
LAN0/LAN1	Network Link Indicator	Green Flashing	The AG4172 Analog Gateway is connected to the network.
		Off	The AG4172 Analog Gateway is not connected to the network, or the network connection is faulty.
	Network Speed Indicator	On	1000 Mbps
		Off	10/100 Mbps

3.3.2 Physical Interfaces

Lists the telephone, Ethernet, AUX, and console interfaces on the AG4124/AG4172 Analog Gateway.

- Telephone Ports
  - 24 FXS ports (RJ-11 and RJ-21) for AG4124
  - 72 FXS ports (RJ-21) for AG4172
- Ethernet Interfaces
  - AG4124: 3 x Local Area Network (LAN) ports, 10/100 Mbps, RJ-45 (use CAT-5 or better Unshielded Twisted Pair (UTP) cable)
  - AG4172: 2 x LAN ports, 10/100/1000 Mbps, RJ-45 (use CAT-5e, CAT-6, or better UTP cable)

    Note: Multiple LAN connections are not supported. Connect only one LAN port to the LAN.

  - Qty 1 Management Port 10/100 Mbps, RJ-45
- AUX2 (AG4124) and AUX (AG4172) Interface
  - 1 x LAN port, 10/100 Mbps, RJ-45 (for factory use only)
- Console
  - 1 x RS232, 115200 bps (Cable should be EIA/TIA-561 compliant)

3.4 Supported Browsers

Identifies the web browsers supported for the AG4124/AG4172 Web Management System.

The AG4124/AG4172 Analog Gateway supports only the following browser:

- Google Chrome

Note:

- This is the recommended browser for the AG4124/AG4172 Analog Gateway.
- The AG4124/AG4172 Analog Gateway might work with browsers such as Firefox and Microsoft Edge. However, Mitel does not fully support these browsers if issues occur.

3.5 Unsupported Features

Lists Management menu features that are not supported and will be deprecated.

The Mitel AG4124/AG4172 Analog Gateway does not support the following features listed in the **Management** menu:

- Cloud Server
- NMS Configuration
- Remote Server

These features will be deprecated in future releases. Therefore, do not use these features.

Features and Specifications 4

This chapter contains the following section(s):

Covers the AG4124/AG4172 feature set, telephony and Foreign Exchange Station (FXS) port capabilities, supported protocols, security features, maintenance and test tools, environmental specifications, and compliances.

4.1 AG4124/AG4172 Features Overview

Summarizes the AG4124/AG4172 Analog Gateway's positioning as a cost-effective, fully managed FXS to SIP Gateway.

The AG4124/AG4172 Analog Gateway is a cost-effective, fully managed Foreign Exchange Station (FXS) to Session Initiation Protocol (SIP) gateway. The AG4124 supports 24 FXS ports and the AG4172 supports 72 FXS ports, giving customers a way to connect analog phones, fax machines, and other analog devices to a SIP call server over their Local Area Network (LAN).

The AG4124/AG4172 Analog Gateway is available in most global markets and addresses the diverse networking and management needs of small and medium-sized businesses:

- A high-availability solution with support for resilient SIP call servers.
- Support for a wide range of networking protocols.
- Fully managed through a web-based graphical user interface (GUI).
- Selectable call progress tone plans for multiple geographic regions and countries.
- Selectable FXS port analog characteristics that accommodate the network and telephone-set requirements of different geographic regions and countries.
- A rich, integrated telephony feature set.
- Support for traditional fax, fax over Internet Protocol (IP), and POS terminals.
- Security controls that protect customer data and privacy.
- Robust user access and authentication controls.

4.2 Local Call Control Features

Lists the local call control features supported by the AG4124/AG4172 Analog Gateway.

- Call Waiting
- Call Holding

> **Note**: The AG supports only device-level (soft) hold. System-level Call Hold (hard hold) is not supported. As a result, calls placed on hold are not registered in the Call Control hold queue and cannot be retrieved by other devices. For more information, refer to the *Feature Access Code* section of the *MiVoice Business System Administration Online Help*.

- Call Forwarding (Unconditional/Busy/No Reply)
- Call Transfer (Blind and Attended)
- Immediate Hotline
- Do-not-Disturb
- Three-Way Conference
- Message Waiting Indicator
- Supports Hook Flash
- Digitmap
- Call Detail Record (CDR)

4.3 Telephony Features and Specifications

Lists CODEC support, voice quality features, and fax/modem capabilities of the AG4124/AG4172 Analog Gateway.

- CODEC support: G.711A/µ law, G.729A/B
- Silence Suppression for reduced Local Area Network (LAN) bandwidth consumption
- Comfort Noise Generator (CNG)
- Voice Activity Detection (VAD)
- Echo Cancellation: G.168 with up to 128 ms delay.
- Adaptive (Dynamic) Jitter Buffers
- Hook Flash
- Programmable Gain Controls for Foreign Exchange Station (FXS) ports
- T.38 fax over Internet Protocol (IP) supported
- T.38 fax over IP G.711 Pass-through supported
- High-speed fax up to 14.4 kbps
- Modem support
- Point of Sale (POS) Terminal Support

> **Note**: MiVoice Business supports G.711A/µ, G.729A. MiVoice 5000 supports G.711A/µ law, G.729A/B. MX-ONE supports G.711 A/µ and G.729A/B.

4.4 FXS Port Features

Lists FXS connector types, dial modes, caller ID, and polarity reversal support.

- Foreign Exchange Station (FXS) connectors:
  - AG4124 supports RJ-11 and RJ-21 connectors
  - AG4172 supports RJ-21 connectors
- Dial mode: Dual-Tone Multi-Frequency (DTMF) and pulse dialing are supported
- Pulse dial mode: support for 10 PPS and 20 PPS
- Caller ID: DTMF or Frequency-Shift Keying (FSK) Calling Line Identification (CLI) presentation
- Polarity reversal, for use when connected to a Foreign Exchange Office (FXO) port

4.5 Management and Administration

Lists the management and administration capabilities of the AG4124/AG4172 Analog Gateway.

- Web Management System, a browser-based Graphical User Interface (GUI) for management and administration
- Local syslog support (emergency, alert, critical, and error warnings)
- Telnet support for diagnostics
- Auto-provisioning of the AG4124 through Hypertext Transfer Protocol (HTTP), FTP, or Trivial File Transfer Protocol (TFTP)

> **Note**: This feature is applicable only for MiVoice Voice 5000.

- Configuration backup and restore
- Firmware upgrade through the web interface
- IVR/phone-based management interface for local maintenance
- Remote management support through Technical Report 069 (TR-069)

4.6 Protocols Supported

Covers the SIP and networking protocols supported by the AG4124/AG4172 Analog Gateway.

4.6.1 SIP Protocols

Lists the SIP-related RFCs and protocol features supported by the AG4124/AG4172 Analog Gateway.

- Session Initiation Protocol (SIP) v2.0 (User Datagram Protocol (UDP)/Transmission Control Protocol (TCP)), RFC3261, Session Description Protocol (SDP), Real-time Transport Protocol (RTP) (RFC2833), RFC3262, RFC3263, RFC3264, RFC3265, RFC3515, RFC2976, and RFC3311
- RTP/RTCP, RFC2198, and RFC1889
- SIP over Transport Layer Security (TLS)
- RFC4028 session timer
- RFC3266 SDP URI
- Domain Name System (DNS) SRV/A query/NATPR query

- Early Media/Early Answer (SIP)
- RFC 3581 Network Address Translation (NAT).rport

4.6.2 Networking Protocols

Lists the networking protocols and standards supported by the AG4124/AG4172 Analog Gateway.

- IPv4/IPv6 network protocols
- Network Time Protocol (NTP) with support for daylight saving time
- Simple Network Management Protocol (SNMP) V1/V2/V3
- Dual-Tone Multi-Frequency (DTMF): Session Initiation Protocol (SIP) Info/RFC2833/Inband
- Virtual Local Area Network (VLAN): 802.1P/802.1Q (voice/data/management VLANs)
- Layer 2 Quality of Service (QoS), Layer 3 QoS, and DiffServ
- Hypertext Transfer Protocol (HTTP)
- Hypertext Transfer Protocol Secure (HTTPS)
- Secure Real-time Transport Protocol (SRTP) (128-bit and 256-bit)
- Transport Layer Security (TLS)

4.7 Security Features

Lists the access control, authentication, and encryption features of the AG4124/AG4172 Analog Gateway.

- Web interface Access Control List (ACL)
- Telnet interface ACL
- Web Management System supports role-based access controls
- Robust user access and authentication controls
- Brute-force login protection
- Syslog
- All data communications are encrypted
- Web Management System uses self-signed certificates

4.8 Maintenance and Test

Lists the maintenance and diagnostic utilities available on the AG4124/AG4172 Analog Gateway.

- System configuration data backup and restore
- Ping utility for network latency tests
- Tracert diagnostic utility for network route tracing
- Outward Test, based on the Generic Requirement 909 (GR-909) standard: standards-based tests for detecting physical problems with the FXS phone line.

4.9 Environmental Specifications

Lists power, temperature, humidity, dimension, and weight specifications for the AG4124/AG4172 Analog Gateway.

The AG4124/AG4172 Analog Gateway has the following environmental and physical specifications:

- Power supply: 100-240 VAC, 50-60 Hz
- Power consumption: AG4124 40 W, AG4172 95 W (typical)
- Operating temperature: 0 °C to 45 °C (32 °F to 110 °F)
- Storage temperature: -20 °C to 80 °C (-4 °F to 170 °F)
- Humidity: 10%-90%, non-condensing
- Dimensions (W/D/H):
  - AG4124: 440mm (17 5/16") x 250mm (9 13/16") x 44mm (1 ¾")
  - AG4172: 440mm (17 5/16") x 328mm (12 15/16") x 44mm (1 ¾")
- Unit weight:
  - AG4124: 3.2 kg/7 lbs
  - AG4172: 4.25 kg/9.4 lbs

Quick Installation 5

This chapter contains the following section(s):

Covers site preparation, hardware installation, network requirements and connections, and logging in to the AG4124/AG4172 Web Management System for the first time.

5.1 Location Requirements

Points to the Location Guidelines section of the Quick Installation Guide.

Before you install the AG4124/AG4172 Analog Gateway, review the *Location Guidelines* section of the *Mitel AG4100 Analog Gateways - Quick Installation Guide* for guidance on choosing a suitable installation site.

5.2 Installation Steps

Points to the hardware installation guide and the PBX-specific configuration appendices.

Use the following resources to complete the hardware installation and any Private Branch Exchange (PBX)-specific configuration for the AG4124/AG4172 Analog Gateway.

- For hardware installation instructions for the AG4124/AG4172 Analog Gateway, see the *Mitel AG4100 Analog Gateways - Quick Installation Guide*.
- To configure the AG4124/AG4172 Analog Gateway for use with MiVoice Business, see Configuring Analog Gateway With MiVoice Business on page 129.
- To configure the AG4124 Analog Gateway for use with MiVoice MX-ONE, see Configuring Analog Gateway With MiVoice MX-ONE on page 152.
- To configure the AG4124/AG4172 Analog Gateway for use with OpenScape Business, see Configuring OpenScape Business for Use With the Mitel AG4124/AG4172 Analog Gateway on page 158.

Note: When the SIP server is unavailable and ports are unregistered, only inter-port calling within the same Analog Gateway unit is supported. All other call control features not supported, including Call Transfer, Call Forwarding, Conference, and Message Waiting Indicator, since they require an active SIP server connection. For details, see Analog Gateway Behavior When the SIP Server Is Unavailable on page 149.

5.3 Network Requirements

Lists the bandwidth and voice-quality network requirements for the AG4124/AG4172 Analog Gateway, including the minimum network thresholds for voice calls and for fax over G.711 pass-through.

The network must meet the following requirements.

The network must provide adequate bandwidth for voice traffic carried over Internet Protocol (IP). As a general guideline, the Ethernet bandwidth required is approximately 85 Kb/s per G.711 voice session and 29 Kb/s per G.729 voice session (assuming 20 ms packetization). For example, 20 simultaneous Session Initiation Protocol (SIP) sessions consume approximately 1.7 Mb/s of Ethernet bandwidth for G.711 or 0.6 Mb/s for G.729 voice sessions. Almost all enterprise LAN networks can support this level of traffic without special engineering. For more information, see the *MiVoice Business Engineering Guidelines* and *Network Engineering for IP Telephony* documents on the MiVB documentation center page (MiVoice Business).

For high-quality voice, the network must also support a voice-quality grade of service. The following tables list the minimum network requirements for voice calls and for fax calls using G.711 pass-through. The **Status** column indicates whether each threshold is acceptable (Go), marginal (Caution), or unacceptable (Stop) for voice or fax quality.

Table 11: Minimum Network Requirements: Voice Network Limits

Packet loss	Jitter	End-to-end delay	Status
< 0.5%	< 20 ms	< 50 ms	Go
< 2%	< 60 ms	< 80 ms	Caution
> 2%	> 60 ms	> 80 ms	Stop

Table 12: Minimum Network Requirements: Fax Over G.711 Pass-Through

Packet loss	Jitter	End-to-end delay	Status
< 0.1%	< 20 ms	< 300 ms	Go
< 0.2%	< 40 ms	< 500 ms	Caution
> 0.2%	> 40 ms	> 500 ms	Stop

5.4 Network Connections

Covers the LAN connectors, management PC connection, and VLAN options for the AG4124/AG4172 Analog Gateway.

5.4.1 LAN Connectors

Describes the four RJ-45 LAN connectors on the AG4124/AG4172 rear panel and which ones you can use for LAN or management PC connections.

The AG4124/AG4172 has four RJ-45 connectors on its rear panel.

Warning:

- The AG4124/AG4172 supports only one LAN connection. Do not connect more than one LAN port to the Ethernet LAN; doing so can cause network broadcast storms and network degradation.
- Connect the AG4124/AG4172 to the Ethernet LAN using Category-5 Unshielded Twisted Pair (UTP) cabling or better.

Table 13: LAN Connectors for AG4124/AG4172

<table>
<tr><th>Supported device type</th><th>Connector type</th><th>Description</th></tr>
<tr><td rowspan="3">AG4124/AG4172</td><td>AUX2</td><td>AUX2 is reserved for factory use. Do not use it.</td></tr>
<tr><td>LAN0</td><td rowspan="3">AG4124: LAN0, LAN1, and LAN3 are connected internally to the AG4124's integrated Layer 2 (L2) Ethernet switch and can be used to connect to the LAN or the management PC.

AG4172: LAN 0 and LAN1 are connected internally to the AG4172's integrated L2 Ethernet switch and can be used to connect to the LAN or the management PC.</td></tr>
<tr><td>LAN1</td></tr>
<tr><td>AG4124</td><td>LAN3</td></tr>
<tr><td>AG4172</td><td>MGMT</td><td>MGMT is a dedicated management port. It can only be accessed by a Personal Computer (PC) that resides on the same subnet as the AG4172.</td></tr>
</table>

5.4.2 Connecting a Management PC

Identifies which LAN port or management port to use when connecting a management PC to the AG4124/AG4172 Analog Gateway.

A management PC is a Personal Computer (PC) that you use to reach the AG4100 Web Management System. You can connect a management PC to a LAN port on the AG4100.

Table 14: Connecting a Management PC

Device type	Description
AG4124	**Using the AG4124 LAN port:** • The management PC can reach the AG4124 Web Management System through LAN0, LAN1, or LAN3. • Enabling or disabling Virtual Local Area Networks (VLANs) does not change this behavior. • Connect the AG4124 to the management PC with Category-5 Unshielded Twisted Pair (UTP) cabling. • For information about configuring the management PC, see Prepare for Login on page 28.

AG4172	Use either of the following options to connect a management PC:
	• **Using the AG4172 LAN port:**
	  ◦ Connect the AG4172 to the customer's LAN and/or the management PC using LAN0 or LAN1.
	  ◦ Enabling or disabling VLANs does not change this behavior.
	  ◦ Connect the AG4172 to the management PC with Category-5 UTP cabling.
	  ◦ For information about configuring the management PC, see Prepare for Login on page 28.
	• **Using the AG4172 management port:** see Configure the AG4172 Management Port on page 26.

5.4.2.1 Configure the AG4172 Management Port

Configure the AG4172 management port so a PC on the same subnet can reach the Web Management System, including when the network DHCP server is unavailable.

The AG4172 management port is a dedicated Ethernet port for accessing the Web Management System. It can only be reached from a Personal Computer (PC) residing on the same subnet as the AG4172.

The management port is especially useful if the customer's network has problems with the network Dynamic Host Configuration Protocol (DHCP) server and the AG4172 relies on DHCP to obtain an Internet Protocol (IP) address.

If you have already configured the management port with a static IP address, you can still reach the Web Management System through the management port even if the DHCP server fails.

To let a PC access the Web Management System through the management port, configure the AG4172 as follows.

1. Log in to the Web Management System.
2. Click **Quick Setup Wizard**.
3. In the **Setup Wizard - Local Network** page that opens, set the fields described in the following table, then click **Save and Next**.

Table 15: Setup Wizard: Local Network Fields

Section	Field	Value to set
Network Configuration	WAN Dual Mode	Select **Separation** from the drop-down list.
Manage Address	IP Address	Enter **192.168.11.1**.
Manage Address	Subnet Mask	Enter **255.255.255.0**.

4. Connect the management PC to the MGMT port with a Category-5 or better Unshielded Twisted Pair (UTP) cable.
5. From the PC's browser, go to IP address 192.168.11.1.

5.4.3 VLAN Configuration

Identifies which LAN port to use when VLANs are enabled on the AG4124/AG4172 Analog Gateway.

Table 16: VLAN Configuration

Device type	Description
AG4124	If Virtual Local Area Networks (VLANs) are enabled, then **LAN3** must be used to connect the AG4124 to the Ethernet LAN. All VLAN traffic is transmitted and received through LAN3.
AG4172	If VLANs are enabled, either **LAN0 or LAN1** can be used to connect to the Ethernet LAN.

Mitel recommends enabling VLANs to help ensure voice quality and to strengthen network security.

- For information about configuring VLANs and Layer 2 (L2) QoS on the AG4124/AG4172, see Virtual Local Area Networks on page 52.
- For information about configuring Layer 3 (L3) QoS, see QoS on page 54.

5.5 Prepare for Login

Prepare the AG4124/AG4172 Analog Gateway and your PC so you can reach the Web Management System for the first login.

1. Connect the Analog Gateway to the network, and connect a telephone to the Foreign Exchange Station (FXS) port.
2. Dial *158# to query the Internet Protocol (IP) address of the LAN port (the default IP address is 192.168.11.1).
3. Change the IP address of the Personal Computer (PC) so that it is on the same network segment as the LAN port of the Analog Gateway.
4. Verify connectivity between the PC and the Analog Gateway.
5. At a command prompt on the PC, run `ping 192.168.11.1` to verify the IP address and connection information.

After the AG4124/AG4172 Analog Gateway is fully commissioned and administrative accounts are established, Mitel recommends that the administrator set up access controls on the FXS port's management capabilities.

5.5.1 Log in to the Web Management System

Log in to the AG4124/AG4172 Web Management System using the default administrator credentials.

Note: When you access the AG4124/AG4172 Web User Interface (UI) by entering the unit's name or Internet Protocol (IP) address, Hypertext Transfer Protocol Secure (HTTPS) is used for enhanced security. However, if you instead enter a specific page name directly into your browser's address bar, the system might revert to Hypertext Transfer Protocol (HTTP), which is not secure. To avoid this, log in by entering only the name or IP address of the unit into your browser, so that HTTPS is used, and then navigate to the login page from there.

To log in to the Web Management System:

1. Open a web browser and enter the IP address of the LAN port (the default IP address is 192.168.11.1).

   The login Graphical User Interface (GUI) is displayed.
2. Enter the default admin user name and password, and click **Login** to access the Web Management System.

   Both the default user name and default password are **admin**.

For security, Mitel recommends changing the user name and password at first login. For more information about passwords, see Passwords on page 112.

Basic Operation 6

This chapter contains the following section(s):

Covers day-to-day operation of the AG4124/AG4172 Analog Gateway: dialing, fax, resets, port data import, emergency services, and other basic features.

6.1 Methods of Number Dialing

Describes the two supported methods for dialing a telephone or extension number.

There are two supported methods for dialing a telephone number or an extension number:

- Dial the called number. The AG4124/AG4172 determines that the digit sequence is complete based on how the **Time Out for dialing** parameter is configured. The default dialing timeout is 4 seconds; do not set it below 3 seconds, so that users have sufficient time to enter each digit when dialing a number or extension. If Digitmap is configured, the AG4124/AG4172 instead determines that the digit sequence is complete based on the Digitmap programming.
- Dial the called number and press **#**, if Dial Key ending is programmed.

For more information, see Service Parameters on page 77.

6.2 Sending and Receiving Fax

Covers the fax modes supported by the AG4124/AG4172 Analog Gateway and guidelines for reliable fax transport.

6.2.1 Supported Fax Modes

Lists the fax modes supported by the AG4124/AG4172 Analog Gateway and where the Fax Mode field is configured.

The AG4124/AG4172 Analog Gateway supports the following fax modes:

- T.38 (IP-based)
- T.30 (G.711 pass-through)
- Adaptive fax mode (automatically matched to the peer fax mode)
- G.711 fax

The **Fax Mode** field, along with the other Fax Parameter settings, is located in the Fax Parameter section of the **Advanced > Line Parameter** page of the Web Management System. For details on all Line Parameter fields, see Line Parameters on page 70.

6.2.2 Explanation of T.38 and Pass-Through

Explains the T.38 fax-over-IP protocol and G.711 fax pass-through operating mode.

T.38 is the protocol recommended by the ITU for transmitting real-time Group 3 fax over Internet Protocol (IP) networks. In T.38 mode, the Analog Gateway converts the analog fax signal to a digital signal and regenerates the fax signal tone based on the signal from the peer Analog Gateway. In this mode, the gateway carries fax traffic in T.38 packets.

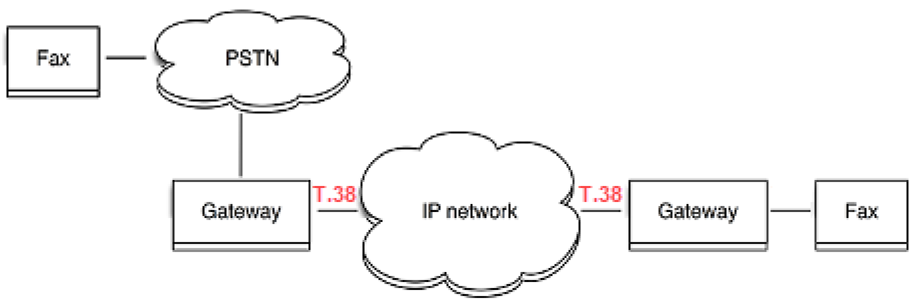

Figure 6: T.38 and Pass-Through

G.711 fax pass-through is an operating mode in which the AG4124/AG4172 transmits fax information as G.711 packets over an IP network to another AG4124/AG4172. In effect, the data-modulated fax signals are carried as voice traffic across the IP network.

6.2.3 Fax Guidelines

Provides G.711 fax pass-through performance guidelines and explains why T.38 is recommended for fax over IP.

G.711 fax pass-through performance guidelines

Fax machines are sensitive to time delays and error rates. Typically, these devices are designed to run over Time-Division Multiplexing (TDM) links. A single lost Internet Protocol (IP) packet can contain a significant quantity of data, and although the fax application can recover from some losses, it may not be able to handle large losses such as a burst loss of IP packets.

Because many variables are involved in sending fax data over G.711 pass-through on IP networks, reliable transport cannot be guaranteed. However, practical experience shows that with careful network planning, a TDM-equivalent link can be made to work. These considerations include:

- The IP link must use G.711 only.
- The rate of packet loss on the link must be less than 0.1%.
- The link delay must be below 200 ms.
- Jitter must be less than 30 ms (ideally less than 20 ms).

Under these network conditions, G3 fax at V.17 speeds has been found to work with reliability comparable to standard TDM connections. However, without error correction mechanisms, such connections should be considered best-effort only. Using T.38 to transport faxes over IP networks is strongly recommended.

T.38 – reliable fax over IP transport

Do not attempt to transmit fax over IP without interfaces that provide signal redundancy and error correction. The most widely used real-time protocol for this purpose is T.38, which allows a standard T.30 fax session to be carried over an IP network. The T.38 protocol includes mechanisms to handle network latency, jitter, and packet loss.

Note:

T.38 fax transmissions are not encrypted.

6.3 Factory Reset Using the RST Button

Describes how to perform a hardware factory reset using the RST button on the AG4124/AG4172 rear panel.

Pressing the **RST** button (on the rear panel of the AG4124/AG4172 Analog Gateway) for about 10 seconds triggers a factory reset. During the reset, the RUN indicator changes from *slow flashing* to *no flashing*, and then back to *slow flashing*.

Note:

- To confirm that the reset completed successfully, watch for the RUN indicator to go from slow flashing to no flashing, and then back to slow flashing. This sequence confirms that the Analog Gateway has been restored to factory defaults.
- Pressing the **RST** button resets all Analog Gateway settings to factory defaults except the IP address. To reset the IP address to its default value as well, reboot the Analog Gateway a second time.
- A factory reset also resets the Shell password back to the Mitel default username and password, **admin/admin**. For security, change the Shell password to a unique value afterward. For more information, see *AG4100 Analog Gateway Security Guidelines*.

CAUTION: Only use the RST button after all other attempts to restore functionality have failed.

You can also restore the Analog Gateway to default settings from the Web Management System instead of using the RST button. For more information, see Restore the Analog Gateway to Default Settings on page 32.

6.4 Import Port Data Into the AG4124/AG4172 Analog Gateway

Import port data into the AG4124/AG4172 Analog Gateway using a CSV template through the Web Management System.

1. Log in to the Web Management System.

2. Go to **Port**.
3. In the page that opens, click **FileImport**.
4. In the page that opens, in the **Template File** field, click **Download** to download the template.
5. Save the file to your local computer.
6. In the **Account File (CSV)** field, click **Choose file** and select the template you downloaded.
7. Click **Upload** to import the port data into the AG4124/AG4172 Analog Gateway.

Note:

- The MiVoice Business system cannot import port data into the AG4124 Analog Gateway device. When you use the import option with existing data in the port programming, the "Parameters error, setting failed" error appears. To resolve this issue, delete the header information in the template you are importing.
- If you import the port information using a template, the existing port information is deleted.

6.5 Query IP Address and Restore Default Setting

Covers querying the gateway's IP address, resetting the password, and restoring the Analog Gateway to default settings.

6.5.1 Query IP Address

Describes how to query the LAN port IP address from a connected telephone.

After connecting a telephone to a Foreign Exchange Station (FXS) port, you can dial *158# to query the Internet Protocol (IP) address of the Local Area Network (LAN) port.

6.5.2 Reset Password

Points to where the admin username and password are reset on the Web Management System.

You reset the username and password on the **Security** > **Passwords** page of the Web Management System.

Both the default username and default password are *admin*.

For security, Mitel recommends changing the username and password at first login. If you forget the password, you can log in through the Telnet interface to create a new one. For more information on passwords, see Passwords on page 112.

Note: For more information, see *AG4124/AG4172 Analog Gateway Personal Data Protection and Privacy Control*.

6.5.3 Restore the Analog Gateway to Default Settings

Restore the AG4124/AG4172 Analog Gateway configuration to factory default settings from the Web Management System.

1. Go to the **Tools** > **Factory Reset** page of the Web Management System.
2. Click **Apply** to restore the Analog Gateway configuration to factory defaults.

Note: Only an administrator should perform a factory reset. Because a factory reset deletes all AG4124/AG4172 configuration information, perform it only when absolutely necessary.

CAUTION: An administrator must restore the default settings only when all other attempts to restore functionality have failed.

6.6 Emergency Services

Describes emergency call handling for MiVoice 5000, MiVoice Business, and MiVoice MX-ONE.

Emergency call handling for devices connected to the Analog Gateway is configured on the call control system, not on the Analog Gateway itself. This topic describes emergency services considerations for each supported call control system:

- MiVoice 5000
- MiVoice Business
- MiVoice MX-ONE

Emergency Services With MiVoice 5000

Emergency call routing is handled by the MiVoice 5000 Call Control application. When deploying the AG4124 Analog Gateway, verify that MiVoice 5000 is correctly configured to route emergency calls for the devices connected to the AG4124 Analog Gateway.

If the AG4124 Foreign Exchange Station (FXS) wiring plan (cross-connections) changes, notify the administrator so that MiVoice 5000 can be reconfigured accordingly.

Emergency Services With MiVoice Business

When deploying the AG4124/AG4172 Analog Gateway, verify that MiVoice Business is correctly configured to route emergency calls for the devices connected to the AG4124/AG4172 Analog Gateway. For the MiVoice Business configuration required to support emergency services on these devices, see *System Applications > General Business Solutions > Emergency Services* in the *MiVoice Business System Administration* online help.

Emergency Services With MiVoice MX-ONE

Emergency call routing is handled by the MiVoice MX-ONE Call Control application. When deploying the AG4124 Analog Gateway, verify that MiVoice MX-ONE is correctly configured to route emergency calls for the devices connected to the AG4124 Analog Gateway.

If the AG4124 FXS wiring plan (cross-connections) changes, notify the administrator so that MiVoice MX-ONE can be reconfigured accordingly.

6.7 Configure Positive Disconnect

Configure Positive Disconnect (Loop Current Support) so that ending a call also disconnects the far end without automatic redial.

Before configuring Positive Disconnect, ensure the following:

- Access to the Analog Gateway Web Management System is available.
- Telephone Profiles are created or planned for configuration.
- Loop Current timing requirements are known, if specific device behavior is required.

When User A calls User B and User A ends the call, User B's line is also disconnected, without automatically redialing User A. This feature is typically used for situations such as emergency calls made from an elevator phone, where the call must disconnect immediately with no callback.

> **Note**: Positive Disconnect is supported from AG version *33.83.12.15* or later.

Positive Disconnect (Loop Current Support) is configured across three areas: Foreign Exchange Station (FXS) Parameters, Tel Profile, and Port.

- **FXS Parameters**
  - Defines the default values.
  - Controls what new Tel Profiles inherit.
- **Tel Profile**
  - Enables or disables the feature per profile.
- **Port**
  - Determines which profile is assigned to the port.

1. Log in to the Analog Gateway Web Management System.
2. **FXS Parameter** configuration:
   a. Navigate to **Advanced > FXS Parameter**. For port configuration parameters, see FXS Parameters on page 73.
   b. Enable **Loop Current Support**.
   c. Configure the Loop Current timing parameters (**Loop Current Time** and **Busytone Duration**) as required.
   d. Click **Save**.
3. **Tel Profile** configuration:
   a. Navigate to **Tel Profile**. For port configuration parameters, see Tel Profile on page 64.
   b. Select an existing profile or create a new profile.
   c. Click **Modify** (or **Add** for a new profile).
   d. Under **FXS Param**, enable **Loop Current Support**.
   e. Click **Save**.
4. **Port** configuration:
   a. Navigate to **Port**. For port configuration parameters, see Port on page 67.
   b. Select the required port.
   c. Click **Modify**.
   d. Under **FXS Param**, enable **Loop Current Support**.

e. Click **Save**.

Loop Current Support is enabled only on ports assigned to the Telephone Profile you configured.

- Enabling Loop Current in FXS Parameters alone does not activate the feature.
- The Telephone Profile assigned to a port determines whether Loop Current Support is applied.
- After an upgrade, existing profiles may have Loop Current Support disabled by default.

6.8 Configure Second Dial Tone

Configure a second dial tone so users hear a prompt to dial an external number after entering an access prefix, on both MiVoice Business and the Analog Gateway.

Ensure that the second dial tone prefix is configured on MiVoice Business (MiVB).

To configure second dial tone on MiVB:

1. Log in to the MiVB System Administration Tool.
2. Navigate to the **Call Routing > Automatic Route Selection (ARS) > ARS Digits Dialed**.
3. Configure the **ARS Digits Dialed** as follows:

Table 17: ARS Digits Dialed

Digits dialed	Number of digits to follow	Termination type	Termination number
6	Unknown	Route	12

4. Configure the **ARS Leading Digits** as follows:

Table 18: ARS Leading Digits

Leading digits	Second dial tone
6	Yes

As a result, MiVB enables the second dial tone for the digit **6**. For more information on the configuration, see the MiVoice Business *System Administration Tool Help*.

The user accesses the public network by dialing a specific prefix number. After the user enters the prefix number, the system plays a second dial tone, prompting the user to dial the desired phone number to place the call.

1. Log in to the Web Management System.
2. Navigate to **Advanced > SIP Compatibility**.

3. Configure the **Second Dial Prefix** parameter as described in the following table. For more information on the SIP compatibility parameters, see Table 43: Description of SIP Compatibility Parameters on page 80.

Table 19: Second Dial Tone Configuration

Parameter	Description
Second Dial Prefix	If this parameter is enabled, the AG4124/AG4172 Analog Gateway plays a dial tone to indicate readiness for the second dial prefix number, which is required for external calls. For example, when making an outside call from a hotel, the user enters the prefix number, and the system plays a dial tone, indicating that the user can now dial an external number. **Note**: The **Second Dial Prefix** must match the digit configured in #unique_35/unique_35_Connect_42_section-3199 on page 35. For example, if the **Second Dial Prefix** is configured as **6** and the user dials 12345678 after the second dial tone, the system sends 612345678 to MiVB.

6.9 Configure the Hotline Feature From MiVoice Business

Configure the Hotline feature so the Analog Gateway automatically dials a preconfigured number when the analog device goes off-hook.

Some deployments require a two-stage dialing process: when the phone goes off-hook, the Analog Gateway automatically dials a preconfigured number, and once that call connects, the user hears a second dial tone and can dial the destination number.

The Hotline feature automatically dials a specified answer point when the analog device goes off-hook. It works together with the Positive Disconnect feature; to configure Positive Disconnect, see Configure Positive Disconnect on page 34.

Important:

- When the Analog Gateway is integrated with MiVoice Business (MiVB), configure the **Offhook Auto-Dial** value in MiVB. Do not configure this parameter directly on the Analog Gateway.
- MiVB automatically synchronizes the configured **Offhook Auto-Dial value** to the Analog Gateway. Any changes made directly on the Analog Gateway may be overwritten the next time the Analog Gateway configuration is synchronized from MiVB.

1. Log in to the MiVB System Administration Tool.
2. Navigate to the Analog Gateway port configuration.
3. Select the required Analog Gateway port.
4. Configure the **Hotline** (Offhook Auto-Dial) number.
5. Save the configuration.

6. Verify that the Offhook Auto-Dial value has been synchronized to the Analog Gateway.
   a. Log in to the Analog Gateway Web Management System.
   b. Navigate to **Port**.
   c. Select the port for which the Hotline feature was configured and click **Modify**.
   d. Verify that the **Offhook Auto-Dial** field displays the same value configured in MiVB.
   e. Lift the handset connected to the configured analog port and verify that the Analog Gateway automatically dials the configured Hotline number.

6.10 Handle HTTPS Certificate Expiry

Restore the default Dinstar certificate using the CLI when an expired user certificate blocks login to the Web Management System.

When a user certificate expires, the system does not allow the user to log in. Perform the following procedure to restore the default Dinstar certificate, which is valid until September 7, 2028.

To restore the default certificate:

1. Log in to the Analog Gateway as an administrator.

   > **Note**:
   > - The connection type must be **Serial**.
   > - If Access Control List (ACL) is enabled, you must add 127.0.0.1 for Telnet.

   The *Welcome to Command Shell* message appears.
2. Enter the username and password. The default username and password are **admin/admin@123#**.
3. After you log in successfully, enter the following command.

```
enable
```

4. Enter the following command.

```
aos
```

5. Enter the web user login credentials.
6. After you log in successfully, enter the following command.

```
en
```

7. Enter the following command to configure the certificate settings.

```
^config
```

8. Enter the following command to restore the default web certificate.

```
cert delete web
```

9. Reboot the Analog Gateway.
10. Log in to the Web Management System.
11. Navigate to **Security > Certificate Manage**.

The WEB Https Certificate field shows the default Dinstar certificate.

12. Upload the valid certificate as described in Add a Web HTTPS Certificate on page 115.

6.11 Update the UserCard Firmware (AG4172 Only)

Update the UserCard (DTU) firmware on the AG4172 Analog Gateway.

The Mitel AG4172 Analog Gateway requires an update of the UserCard, also called the Data Terminal Unit (DTU), for each global update.

To update UserCard firmware:

1. Log in to the Web Management System.
2. Navigate to **Tools > Firmware Upload**.
3. Select **UserCard Firmware** in the **File Type** drop-down list.
4. Click the button on the **UserCard Firmware** line to open the file manager.
5. Select the firmware file to install.

> **Note**: The UserCard firmware files are provided in the `DTUFirmware_vX.X.tar.gz` format. For the latest DTU firmware version, see the latest **Release Notes**.

6. Click the **Upload** button to install the firmware.

   The installation lasts a few minutes. Leave the page open during the installation.
7. Reboot the Analog Gateway after the firmware installation finishes.
   a. Navigate to **Tools > Device Restart**.
   b. Click the **Restart** button to launch the reboot.

      The Analog Gateway reboots. During the reboot, the RUN indicator turns off and all the FXS port indicators stay on.

The Analog Gateway is accessible again:

- When the RUN indicator flickers.
- When the unused FXS port indicators turn off.

Web Management System Configuration Forms

7

This chapter contains the following section(s):

- Navigation Tree
- Status Statistics
- Quick Setup Wizard
- Network
- SIP Server
- IP Profile
- Tel Profile
- Port
- Sample Port Configuration
- Advanced
- Call and Routing
- Manipulation
- Management
- Security
- Tools

Introduces the navigation tree and configuration forms of the Web Management System.

The Web Management System of the AG4124/AG4172 Analog Gateway provides a navigation tree and a set of configuration forms for viewing device status and configuring the gateway.

7.1 Navigation Tree

Describes the navigation tree of the Web Management System and lists the configuration forms it provides access to.

The Web Management System of the AG4124/AG4172 Analog Gateway consists of the navigation tree and a set of detailed configuration forms. Select a node in the navigation tree to open its corresponding configuration form.

7.2 Status Statistics

Introduces the Status & Statistics menu of the Web Management System.

The **Status & Statistics** menu displays read-only status and statistical information for the AG4124/AG4172 Analog Gateway, including system information, port status, active calls, Real-time Transport Protocol (RTP) sessions, call detail records, and, on the AG4124, Virtual Private Network (VPN) connection state.

7.2.1 System Information

Describes the read-only system information fields displayed on the Status & Statistics > System Information page.

Displays key device details such as Internet Protocol (IP) address, firmware version, system uptime, and resource usage. It helps you verify basic configuration and monitor the overall status of the gateway.

The following table describes the system information.

Table 20: System Information

System interface	Description
Device ID	The unique ID of each Analog Gateway. This ID is used for warranty and cloud server authentication.
MAC address	Hardware address of the Wide Area Network (WAN) port.

IP Address	• **DHCP: Obtain IP address automatically.** The AG4124/AG4172 Analog Gateway acts as a Dynamic Host Configuration Protocol (DHCP) client: it broadcasts a request and waits for a DHCP server on the Local Area Network (LAN) to respond. The first DHCP server to respond assigns an IP address to the AG4124/AG4172 Analog Gateway from its defined address range.
	• **Static IP Address:** A static IP address is a semi-permanent address that remains associated with a single device over an extended period, unlike a dynamic IP address, which is assigned ad hoc at the start of each session and typically changes from one session to the next.
	If you choose a static IP address, you must supply the following information:
	  • **IP Address**: the IP address of the AG4124/AG4172 Analog Gateway.
	  • **Subnet Mask**: the subnet mask of the router on the AG4124/AG4172 Analog Gateway's subnet.
	  • **Default Gateway**: the IP address of the router on the AG4124/AG4172 Analog Gateway's subnet.

DNS Servers	Displays the IP addresses of the primary and standby Domain Name System (DNS) servers.
SIP TLS Link Status	Displays the current status of the Session Initiation Protocol (SIP) over Transport Layer Security (TLS) connection between the gateway and the configured SIP server.
System Uptime	The running time of the AG4124/AG4172 Analog Gateway after it was powered on.

System interface	Description
System Time	Specifies the current system date and time of the gateway, used for time-dependent operations such as logging, Call Detail Record (CDR) generation, and other protocol functions.
Traffic Statistics	Total number of bytes sent and received over Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) on the LAN port since the last reboot of the AG4124/AG4172.
Usage of Flash	Detailed usage of Flash memory.
Usage of Backup Flash	Detailed usage of backup Flash memory.
Usage of RAM in Linux	Detailed Random Access Memory (RAM) usage of the Linux core.
Usage of RAM in AOS	Detailed RAM usage of the AOS.
Current Software Version	The software version that runs on the AG4124/AG4172 Analog Gateway. The device displays the model name, version number, and software development date.
Backup Software Version	The backup software provides redundancy for the current software. If the current software fails, the backup software version takes over.
DSP Version	The version of the Digital Signal Processor (DSP) software running on the gateway.
U-boot Version	The version of the U-boot bootloader installed on the device.
Kernel Version	Linux kernel version.
RootFS Version	Version information for the RootFS image on the device.
FS Version	File system version.
Hint Language	The current language of the AG4124/AG4172 Analog Gateway.

7.2.2 Port Status

Describes the real-time per-port status fields displayed on the Status & Statistics > Port Status page.

Displays real-time status information for each Foreign Exchange Station (FXS) port, including Session Initiation Protocol (SIP) registration, line state, and call activity. It helps you monitor port availability, verify connectivity with the SIP server, and identify issues such as unregistered ports or abnormal line conditions.

The following table describes the port status information.

Table 21: Port Status

Parameter	Description
Port No	Identifies the physical or logical FXS port number on the gateway. Each port represents a single analog line interface, used to map configuration and status to a specific port.
Type	Indicates the port type supported by the gateway. For this device, it is typically FXS, which connects to analog endpoints such as phones or fax machines.
SIP User ID	Displays the SIP extension or user identifier assigned to the port. This ID is used for SIP registration and call routing between the gateway and the SIP server.
User Status	Shows the SIP registration status of the port with the configured SIP server. Typical values include Registered or Unregistered. If unregistered, the port cannot make or receive SIP calls.
Server	Displays the Internet Protocol (IP) address or domain name of the SIP server to which the port is registered. This helps verify which server is handling signaling for the port.
Port Status	Indicates the physical line state of the FXS port. Common values include OnHook (idle) and OffHook (in use). Reflects whether the connected device is actively engaged.
Voltage	Shows the current line voltage supplied by the FXS port. This is used to power analog devices and can help identify line conditions or faults.
Current	Displays the electrical current drawn by the connected device on the FXS port. Useful for monitoring line usage and detecting abnormal conditions.

Parameter	Description
Call Status	Indicates the current call state of the port. Typical values include Idle or Active. Provides a quick view of whether the port is currently handling a call.

7.2.3 Current Call

Describes the active-call fields displayed on the Status & Statistics > Current Call page.

This page displays information about calls that are active on the Analog Gateway. Click **Refresh** to update the displayed status of active calls.

The following table describes the current call information.

Table 22: Current Call

Parameter	Description
Port	Displays the port number currently handling the call, identifying which Foreign Exchange Station (FXS) port is in use for the active session.
Type	Indicates the port type involved in the call, typically FXS, representing the interface through which the call is established.
Source	Shows the calling party number or identifier. Used to identify the origin of the call.
Destination	Displays the called party number or identifier. Indicates the target end-point of the call.
Connected Time	Indicates the time at which the call was successfully connected. Useful for tracking call start time.
Duration(s)	Shows the elapsed time of the active call in seconds. Helps monitor call duration in real time.

7.2.4 RTP Session

Describes the real-time RTP media session fields displayed on the Status & Statistics > RTP Session page.

Displays real-time information about active Real-time Transport Protocol (RTP) sessions, including media flow details such as source, destination, packet statistics, and jitter. It helps you monitor voice stream performance and troubleshoot audio-related issues.

The following table describes the RTP session information.

Table 23: RTP Session

Parameter	Description
Port	Displays the port associated with the RTP session, identifying which Foreign Exchange Station (FXS) port is handling the media stream.
Source	Indicates the source address or identifier of the RTP stream. Represents where the media traffic originates.
Destination	Displays the destination address or identifier of the RTP stream. Represents where the media traffic is sent.
Payload Type	Specifies the RTP payload type used for the session. Indicates the codec or media format used for voice transmission.
Packet Period	Shows the interval between RTP packets in milliseconds. Determines how frequently audio packets are transmitted.
Local Port	Displays the local User Datagram Protocol (UDP) port used by the gateway for the RTP session, for sending and receiving media packets.
Peer IP	Indicates the Internet Protocol (IP) address of the remote endpoint involved in the RTP session, helping identify the media peer.
Peer Port	Shows the UDP port number on the remote endpoint used for RTP communication.
Sent Packets	Displays the number of RTP packets transmitted by the gateway during the session.

Parameter	Description
Recv Packets	Displays the number of RTP packets received by the gateway from the remote endpoint.
Lost Packets Rate(%)	Indicates the percentage of RTP packets lost during transmission. High values may result in degraded audio quality.
Jitter	Shows the variation in packet arrival time. High jitter can cause audio distortion or gaps in voice communication.
Duration(s)	Displays the duration of the RTP session in seconds. Helps track how long the media stream has been active.

7.2.5 CDR

Describes the Call Detail Record (CDR) control fields and the record fields captured for each call through the Analog Gateway.

A Call Detail Record (CDR) is a data record produced by a telephone exchange or telecommunication device. It contains the details of a telephone call that passes through the Analog Gateway.

You can enable the CDR function to view the details of all calls through the Foreign Exchange Station (FXS) ports of the AG4124/AG4172 Analog Gateway. You can also export, filter, or clear the CDRs. A maximum of 5000 CDR files can be saved.

Note: Mitel recommends disabling CDRs for security and privacy reasons.

Table 24: CDR Configuration Fields

Field	Description
Enable CDR	Yes/No toggle that turns CDR recording on or off. Click **Save** to apply.
Port	Filters the displayed CDR list by FXS port. Default is All.
Call State	Filters the displayed CDR list by call state. Default is All.
Source	Filters the displayed CDR list by the calling party number.

Field	Description
Destination	Filters the displayed CDR list by the called party number.
CDR Oper	Provides **Export**, **Filter**, and **Clear** buttons to export the CDR list, apply the Port/Call State/Source/Destination filters, or clear all stored CDRs.
Enable Advanced Option	Yes/No toggle that shows additional CDR filter/display options when enabled.

Table 25: CDR Record Fields

Column	Description
Port	The FXS port that handled the call.
Start Time	The time the call attempt started.
Answer Time	The time the call was answered.
Direction	Indicates whether the call was inbound or outbound.
Source	The calling party number.
Destination	The called party number.
PeerIP	The Internet Protocol (IP) address of the remote Session Initiation Protocol (SIP) endpoint involved in the call.
Codec	The voice codec used for the call.
Reason	The call termination reason.
Duration (s)	The call duration, in seconds.

7.2.6 VPN State (AG4124 Only)

Describes the VPN connection status fields displayed on the Status & Statistics > VPN State page (AG4124 only).

Displays the current status of the Virtual Private Network (VPN) connection, including connectivity, assigned Internet Protocol (IP) address, and data transmission details. It helps you verify whether the VPN is active and diagnose connectivity issues.

The following table describes the VPN state information.

Table 26: VPN State

Parameter	Description
Protocol	Indicates the VPN protocol used for the connection. Defines the method used to establish secure communication between the gateway and the VPN server.
State	Shows whether the VPN feature is enabled or disabled on the device. Does not indicate actual connection status.
IP Address	Displays the IP address assigned to the gateway by the VPN server. This address is used for communication within the VPN network.
Gateway	Indicates the gateway address provided by the VPN server. Used for routing traffic within the VPN connection.
Server Address	Displays the IP address or domain name of the VPN server to which the gateway connects.
RX / TX Bytes	Shows the amount of data received (RX) and transmitted (TX) over the VPN connection. Useful for monitoring traffic usage.
Connection Status	Indicates the current state of the VPN connection, such as online or offline. Reflects whether the VPN tunnel is actively established.
Login Time	Displays the duration since the VPN connection was established. Helps track how long the session has been active.

7.3 Quick Setup Wizard

Introduces the Quick Setup Wizard, which guides you through the minimum configuration needed to place voice calls on the AG4124/AG4172 Analog Gateway.

The Quick Setup Wizard walks you step by step through the minimum settings required to configure the Analog Gateway. From the wizard interface, you configure the network settings, the Session Initiation Protocol (SIP) server, and the SIP port. Once these three basic steps are complete, the AG4124/AG4172 Analog Gateway is ready to make voice calls.

For details about the network, SIP server, and SIP port settings, see Network on page 48, SIP Server on page 56, and Port on page 67.

7.4 Network

Describes a cabling requirement for the AG4124/AG4172 Local Area Network (LAN) ports before you configure network settings.

Warning: The integrated Layer 2 (L2) Ethernet switch on the AG4124/AG4172 does not support multiple connections to the same LAN. Connect only one AG4124/AG4172 LAN port to the LAN; connecting more than one port creates a network loop.

7.4.1 Local Network

Describes the Local Network configuration parameters on the Network > Local Network page, including IP addressing, PPPoE, management address, internal IP prefix, and DNS server settings.

The AG4124/AG4172 Local Area Network (LAN) interfaces connect to an integrated Layer 2 (L2) Ethernet switch. You must configure the IP address of the integrated L2 Ethernet switch, the Subnet Mask, and the Default Gateway. You can obtain these IP addresses from a Dynamic Host Configuration Protocol (DHCP) server or program them statically.

You must ensure that the IP addresses of the Primary and Secondary Domain Name System (DNS) servers are programmed. The DNS IP addresses can be statically programmed or obtained from a DHCP server.

The following table lists the sample Local Network configuration.

Table 27: Local Network Configuration

Parameter	Description
>IP Protocol	Specifies the IP version used by the gateway for network communication (IPv4 or IPv6). When IPv6 is selected, ensure that the **IP Protocol for SIP Stack** is configured to use the same IP version.

Parameter	Description
	Default Value: IPv4
>WAN Dual Mode	Enables the WAN interface to operate in a dual-mode configuration, allowing the gateway to support multiple IP protocol modes on the network interface. For information about LAN connectors, see LAN Connectors on page 25. The three modes are: • **Separation Mode** (default) In Separation Mode, the two Ethernet interfaces operate independently. Each interface can connect to a different network or VLAN. This mode does not provide network redundancy or automatic failover between interfaces. • **Bonding Mode** (recommended for redundancy) In Bonding Mode, both Ethernet interfaces provide network redundancy for the Analog Gateway. If one network link or switch fails, the Analog Gateway continues operating using the remaining active interface. **Important**: In Bonding Mode, both Ethernet interfaces must: • Connect to different network switches. • Use the same VLAN and subnet configuration. • **Bridge Mode** (not recommended) In Bridge Mode, the two Ethernet interfaces are bridged together and operate as a single Layer 2 network connection. Network traffic received on one interface can be forwarded to the other interface. **Note**: This parameter is visible only for AG4172.
>Network Configuration	
>>Obtain an IP address automatically	Enables the gateway to function as a DHCP client, allowing it to automatically obtain an IP address and related network parameters (such as subnet mask and default gateway) from a DHCP server in the network.
>>Use the following IP address	
>>>IP Address	Specifies the IP address assigned to the network port of the gateway when static IP configuration is selected.

Parameter	Description
>>>Subnet Mask	Specifies the subnet mask associated with the configured IP address, used to define the network and host portions of the IP address for the gateway.
>>>Default Gateway	Specifies the IP address of the router connected to the gateway, used to forward traffic to networks outside the local subnet.
>>PPPoE	PPPoE (Point-to-Point Protocol over Ethernet) refers to the IP address assigned through PPPoE mode. If you choose PPPoE, you must provide the following information: • Username: the account name for the PPPoE connection. • Password: the password for the PPPoE connection. • Server Name: the name of the server that hosts the PPPoE connection. • DNS Server: displays the IP addresses of the primary and standby DNS servers. **Note**: This parameter is visible only for AG4124.
>>Account	Specifies the username used for PPPoE authentication, required for establishing a connection to the ISP over Ethernet. **Note**: This parameter is visible only for AG4124.
>>Password	Specifies the password used for PPPoE authentication, paired with the Account (username) to establish a PPPoE session with the service provider. **Note**: This parameter is visible only for AG4124.
>>Service Name	Specifies the PPPoE service identifier used to select a particular PPPoE service on the server during connection establishment. **Note**: This parameter is visible only for AG4124.
>>WAN MTU	Specifies the Maximum Transmission Unit (MTU) for the WAN (network) interface, which defines the maximum size (in bytes) of IP packets that can be transmitted without fragmentation.
>Manage Address	

Parameter	Description
>>IP Address	Specifies the management IP address used to access the Web Management System and other management services, for example, Telnet and Simple Network Management Protocol (SNMP).
>>Subnet Mask	Specifies the subnet mask associated with the management IP address, used to define the network range for accessing the gateway's management interface.
>Internal IP Prefix	
>> Internal IP Prefix	Defines a full internal IP range. Configure only the first two octets. **Example:** • Sample Input: `10.251` • Internal range: `10.251.x.x` • Used internally by the device of user board • Not intended for external routing **Default Value:** • `10.251` **Notes:** Do not configure a prefix that overlaps with your production network. If you do: • Devices in that range may become unreachable. • Routing conflicts occur. **Note**: This parameter is visible only for AG4172.
>DNS Server	
>>Obtain DNS server address automatically	Enables the gateway to automatically obtain DNS server addresses from a DHCP server instead of using manually configured DNS values.
>>Use the following DNS server address	Enables manual configuration of DNS server addresses, allowing the gateway to use administrator-defined DNS servers instead of obtaining them automatically via DHCP.

Parameter	Description
>>Primary DNS Server	Specifies the primary DNS server IP address used by the gateway to resolve domain names, for example, the SIP server's Fully Qualified Domain Name (FQDN).
>>Secondary DNS Server	Specifies the secondary (backup) DNS server IP address used by the gateway when the primary DNS server is unavailable for domain name resolution.

7.4.2 Virtual Local Area Networks

Describes the Data, Voice, and Management VLANs supported on the Network > VLAN page, and the recommended Layer 2 (L2) QoS priority settings.

On the **Network** > **VLAN** page, you can assign AG4124/AG4172 Local Area Network (LAN) traffic to three different Virtual Local Area Networks (VLANs). The AG4124/AG4172 supports a Data VLAN, a Voice VLAN, and a Management VLAN.

The **Data VLAN** carries low-priority, non-time-sensitive traffic.

The **Voice VLAN** carries high-priority VoIP traffic, both telephony signaling and voice media.

The **Management VLAN** carries management-related traffic to support management protocols such as Simple Network Management Protocol (SNMP), Technical Report 069 (CPE WAN Management Protocol) (TR-069), and the Telnet interface.

Note: The traffic for the AG4124/AG4172 Web Management System is not included in the Management VLAN.

The Voice VLAN transmits VoIP signaling and voice media, while the Data VLAN transmits data packets.

Table 28: Description of VLAN Parameters

VLAN parameters	Description
VLAN NO	The Analog Gateway supports a maximum of three VLANs. Enable VLANs according to actual needs.
Data/Voice/Management	Select what kind of messages are allowed to go through this VLAN. For example, if the check box to the left of Data is selected, data messages are subject to the network settings of this VLAN.
802.1Q VLAN ID (0-4095)	Set an ID to identify a VLAN based on 802.1Q protocol. Range is from 0 to 4095.

VLAN parameters	Description
802.1p L2 Priority (0-7)	Set the L2 priority of a VLAN based on 802.1p protocol.

L2 QoS settings that Mitel recommends:

- Telephony (Voice Media) 6
- Telephony Signaling 3
- Multimedia Conferencing 4
- Standard 0

  For information about configuring **L3 QoS**, see the section QoS on page 54.

Note: After you complete the configuration changes, restart the Analog Gateway to apply them.

7.4.2.1 Using VLANs to Assist With Security

Explains how segregating LAN traffic into VLANs makes the network more resistant to eavesdropping, denial of service, and virus-based attacks.

You should group Local Area Network (LAN) traffic by traffic type and trust level so that eavesdropping and denial-of-service attacks are more difficult to carry out, or less effective if attempted. Virtual Local Area Networks (VLANs) provide this grouping, letting you segregate management traffic from VoIP traffic.

Isolating traffic types with VLANs also makes the network more resistant to virus-based attacks and network flooding attacks. For example, if VoIP traffic is confined to a single VLAN and the nodes on that VLAN are strongly protected, a worm-based attack that overloads the network from a node on a different VLAN affects the VoIP VLAN only marginally.

Once traffic types are segregated by VLAN, hosts or devices on different VLANs can communicate only through a Layer 3 switch or router that connects the two VLANs. Broadcast traffic is blocked across VLAN boundaries, which prevents broadcast storms from propagating across the network.

For more information about IDPS, see the following documents in Technical Papers:

- *Intrusion Detection and Prevention Systems-Technical Paper*
- *Securing Mitel Cloud based Unified Communications Networks*

7.4.3 DHCP Option

Describes the DHCP option fields on the Network > DHCP Option page that the AG4124/AG4172 Analog Gateway can request from a DHCP server.

When the AG4124/AG4172 Analog Gateway acts as a Dynamic Host Configuration Protocol (DHCP) client and requests an IP address, the DHCP server returns packets containing the IP address and the configuration information for any enabled option fields.

The following table describes each option field supported by the AG4124/AG4172 Analog Gateway. When an option field is enabled, the DHCP server returns the corresponding information for that option.

Table 29: DHCP Option Fields

Option	Description
Option 15 (Domain Name)	Sets a Domain Name System (DNS) suffix.
Option 42 (NTP Servers)	Specifies the Network Time Protocol (NTP) server.
Option 60 (Class Identifier)	Identifies the Analog Gateway's device type to the DHCP server using a Vendor Class Identifier (VCI) string. The DHCP server can use this VCI value to apply device-specific policies, such as firmware assignment, configuration parameters, or provisioning rules. Configure the VCI value in the Analog Gateway Web Management System, under DHCP options, if DHCP server-side device identification is required. Example: • AG4124: Mitel AG4124 • AG4172: Mitel AG4172
Option 66 (TFTP Server)	Specifies the Trivial File Transfer Protocol (TFTP) server that assigns the software version to the AG4124/AG4172 Analog Gateway.
Option 120 (SIP Server)	Retrieves the Session Initiation Protocol (SIP) server address.
Option 121 (Classless Static Route)	Obtains classless static routes; the AG4124/AG4172 Analog Gateway adds these routes to its static route table after retrieving them from the DHCP server.

7.4.4 QoS

Describes the Layer 3 (L3) Differentiated Services Code Point (DSCP) configuration fields for QoS on the Network > QoS page, and lists Mitel's recommended L3 QoS settings.

The AG4124/AG4172 Analog Gateway can label QoS priority on the Internet Protocol (IP) messages it sends out, to resolve network delay or network congestion. The Analog Gateway can give different QoS tags for management-related packets of Web/Telnet, voice packets and signal packets.

The DSCP code point is used for the diffserv setting. It uses the first 6 bits of the IP ToS field. The default values are EF(184), AF1(1), AF2(2), AF3(3), AF4(4), and BE(0). You can use different DSCPs for voice or data based on the network provider.

Table 30: QoS Configuration Fields

Field	Description
Set DSCP Code/IP ToS	Enables DSCP/IP ToS tagging of outgoing IP messages.
Manage (WEB/Telnet)	Sets the DSCP code point applied to management traffic (Web/Telnet).
Voice Packet	Sets the DSCP code point applied to voice media packets.
Signal Packet	Sets the DSCP code point applied to telephony signaling packets.

L3 QoS settings that Mitel recommends:

- Telephony (Voice Media) 46 (EF)
- Telephony Signaling 24 (CS3)
- Multimedia Conferencing 34 (AF41)
- Standard 0 (DF) (BE)

Note: For information about configuring L2 QoS, see the **Mitel recommended L2 QoS settings** section under the **Virtual Local Area Network (VLAN)** topic.

7.4.5 ARP

Explains the Address Resolution Protocol (ARP) and describes the fields on the Network > ARP page used to view or add ARP entries.

Address Resolution Protocol (ARP) is the protocol the Analog Gateway uses to resolve a device's Internet Protocol (IP) address to its Media Access Control (MAC) address. On a Transmission Control Protocol (TCP)/IP network, every host is assigned a 32-bit IP address, but the physical network requires the MAC address to deliver messages. ARP performs this conversion from IP address to MAC address.

Table 31: ARP Parameter Fields

Field	Description
Type	Indicates whether an ARP entry is Static (added manually) or Dynamic (learned automatically by the gateway).
IP Address	The IP address associated with the ARP entry.
MAC Address	The MAC (hardware) address resolved for the IP address in the entry.

7.5 SIP Server

Describes the SIP server registration and proxy parameters configured on the SIP Server page.

The SIP server is the main component of the VoIP network and is responsible for establishing all SIP calls. The SIP server is also called the SIP proxy server or the registrar server. Both an IP Private Branch Exchange (PBX) and a softswitch can act as the SIP server.

For more information about the SIP server configuration for the AG4124 Analog Gateway and MiVoice 5000, see MiVoice 5000. For information about SIP Server configuration for the AG4124/AG4172 Analog Gateway and MiVoice Business, see Configure Settings Using the Web Management System on page 137.

The following table describes the sample SIP server configuration.

Note: After you upgrade the device, existing configuration values are retained and are not updated to new default values. To apply or verify updated default settings introduced in the release, you must perform a factory reset. This applies only to default configuration behavior and does not affect existing user-defined settings.

Important: For security reasons, Mitel recommends using Transport Layer Security (TLS) with port 5061 instead of non-secure SIP communication over port 5060. TLS encrypts SIP signaling traffic and reduces the risk of unauthorized monitoring, interception, or modification of call signaling data.

Table 32: Description of SIP Server Parameters

SIP Server Parameter	Description
IP Protocol for SIP Stack	Specifies whether the SIP stack uses IPv4 or IPv6. This parameter depends on the network setting of the AG.
SIP Server	
SIP Server	Specifies the SIP server IP address: the MiVoice Business IP address or Fully Qualified Domain Name (FQDN).
SIP Server port	Specifies the service port of the SIP server. Default: 5061. The supported SIP server port range is from 1 to 65534.

SIP Server Parameter	Description
Registration Expires (Default: 300)	Avoids excessively frequent re-registrations. When the timer expires, the AG4124/AG4172 Analog Gateway sends a register request to the SIP server. Default: 300 seconds.
Heartbeat	Checks that the connection between the AG4124/AG4172 Analog Gateway and the SIP call server is operating properly.
Primary Outbound Proxy	
Primary Outbound Proxy Address	Specifies the IP address or domain name of the primary outbound proxy server.
Primary Outbound Proxy Port	Specifies the service port of the primary outbound proxy server. Default: 5061. The port range is from 1 to 65534.
Secondary Outbound Proxy	
Secondary Outbound Proxy Address	Specifies the IP address or domain name of the secondary outbound proxy server.
Secondary Outbound Proxy Port	Specifies the service port of the secondary outbound proxy server. Default: 5061. The port range is from 1 to 65534.
Registration	
Re-registration Percent(Expires)(0: means random, range: 25%-75%)	Specifies the retry interval after a SIP call server registration fails. Default: 30 seconds. The registration interval is set as a percentage.

SIP Server Parameter	Description
	For example, if the session interval is 60 seconds and the percentage is set to 75%, the AG tries to send a re-registration message to the server when the timer reaches 60 x 75% = 45 seconds.
Retry Interval when Registration failed	Specifies the retry interval to use when a SIP registration fails.
Registration Limit (counts/ time, time: 0 means unlimited)	Defines the maximum number of registration attempts allowed within a time window. • Counts = number of registrations. • Time = duration in seconds. **Recommended values:** • AG4172 (72 ports): **72 / 30** • AG4124 (24 ports): **24 / 30** **Example:** • `24 / 30` means the system allows 24 registrations every 30 seconds. **Scaling considerations:** When you deploy multiple Analog Gateways: • Increase the **Time** value. • Spread registration attempts over a longer period. **Warning:** Setting Registration **Time** to **0** (unlimited) can have the following effects: • It can break resiliency behavior. • It can delay failover significantly.
Send SIP Unregistration Request when the Device Restart	When you restart the device through the Web Management System, the AG sends an unregistration message to the server before applying the restart.
MOH	

SIP Server Parameter	Description
MOH Dial Number	On some servers, if Music on Hold (MOH) plays, the server requests that the AG carry the dial number to it. **Important**: Do not enable this option for MiVB and MBG.
SIP Transport Type	Specifies the transport protocol for SIP-based traffic. Options: UDP, TCP, TLS, or Automatic. Default: UDP. **Note**: The default value UDP does not work if the MiVB security system option is set to **High UDP**. In this case, set **SIP Transport Type** to **TLS** and configure **SIP Server port** as **5061**.
SIPS URL	When the AG sends a SIP message to the server, it uses SIPS in place of SIP in the URI. For example: Request-URI: sips:123456@call.mitel.com:5061
Contact Uses the Local Connection Port	When the AG is behind a router and using TCP/TLS SIP, this parameter carries the real local connection port in the Contact header. For example: CONTACT sip:dead85a3f0c8@10.46.32.110:16002; Default: disabled. When disabled, the Contact header carries the local SIP port: CONTACT sip:dead85a3f0c8@10.46.32.110:5061
Local SIP Port	
Use Random Port	If you select this parameter, the local port that the AG4124/AG4172 Analog Gateway uses for SIP services is chosen randomly from the range 12000-14000.
SIP TLS Local Port	Specifies the TLS port that the AG4124/AG4172 Analog Gateway uses for SIP services.

SIP Server Parameter	Description
	Default: 5061. **Note**: This parameter appears when the **SIP Transport Type** is set to **TLS**.
SIP UDP/TCP Local Port	Specifies the UDP/TCP port that the AG4124/AG4172 Analog Gateway uses for SIP services. Default: 5061. **Note**: This parameter appears when the **SIP Transport Type** is set to **UDP**.
SIP Protocol Stack Startup Protection	
Reboot After Stack Consecutive Startup Failures(0: means no reboot)	Configure this parameter to restart the AG if the SIP stack startup fails the specified number of times. Default: 0.

7.6 IP Profile

Describes the IP Profile parameters that define SIP server, proxy, and codec settings assigned to a port.

An IP Profile is a named group of Internet Protocol (IP)-related settings — Session Initiation Protocol (SIP) server, outbound proxy, Dual-Tone Multi-Frequency (DTMF), codec, and related parameters — that you assign to one or more FXS ports.

The following table describes the IP Profile parameters.

Parameter	Description
Index	Specifies the profile index used to identify this IP Profile. This index is referenced when assigning the profile to ports.
Description	Provides a user-defined description for the IP Profile, to help identify its purpose or configuration.
IP Protocol for SIP Stack	Defines the IP protocol used for SIP signaling, such as IPv4 or IPv6. Must match the SIP server configuration.

Parameter	Description
SIP Server	
SIP Server Address	Specifies the IP address or domain name of the SIP server. Used for registration and call control signaling.
SIP Server Port	Defines the port used for SIP signaling on the server. Default is 5060 for UDP/TCP.
Registration Expires	Specifies the SIP registration interval, in seconds. The gateway refreshes its registration before this timer expires.
Heartbeat	Enables periodic keepalive messages to maintain connectivity with the SIP server and detect connection failures.
Primary Outbound Proxy	
Primary Outbound Proxy Address	Specifies the primary outbound proxy server used for routing SIP requests. Required in certain network deployments.
Primary Outbound Proxy Port	Defines the port used by the primary outbound proxy server for SIP signaling.
Secondary Outbound Proxy	
Secondary Outbound Proxy Address	Specifies a backup outbound proxy server used if the primary proxy is unavailable.
Secondary Outbound Proxy Port	Defines the port used by the secondary outbound proxy server.
MOH	Enables the Music on Hold (MOH) feature. When enabled, a predefined number is dialed to provide music during hold.

Parameter	Description
MOH Dial Number	Specifies the number used to retrieve music on hold. Must be configured on the SIP server side.
Digit Map	
Match Failed (When the registration is successful)	Defines the action taken when dialed digits do not match any pattern in the digit map while the device is successfully registered to the SIP server. Typically forwards the unmatched digits to the SIP server for further processing.
Digit Map	Specifies dialing patterns and rules used to interpret user input. Controls how digits are collected, validated, and when a call is initiated or sent to the SIP server. Incorrect configuration may result in failed or delayed call routing.
Service Parameter	
SUBSCRIBE for MWI	Enables SIP SUBSCRIBE messages for the Message Waiting Indicator (MWI). Required for voicemail indication support.
MWI Subscription Expires	Defines the interval for MWI subscription refresh, in seconds.
Voicemail User ID	Specifies the user ID used for voicemail subscription and message waiting indication.
Echo Cancel Tail	Defines the echo cancellation duration, in milliseconds. Higher values improve echo handling but increase processing load.
SIP Compatibility	
PRACK (RFC3262)	Enables support for the Provisional Response Acknowledgement (PRACK) method, used for reliable provisional responses. Required by some SIP servers for early media handling.

Parameter	Description
PRACK only for 18x with SDP	Restricts PRACK usage to provisional responses that contain Session Description Protocol (SDP) content. Helps maintain compatibility with certain SIP implementations.
Early Media	Allows media transmission before the call is fully established. Used for announcements or ringback tones.
Early Answer	Enables answering calls at an early stage, before the final SIP response. Behavior depends on SIP server support.
DTMF Parameter	
DTMF Method	Specifies how DTMF tones are transmitted, such as RFC2833, SIP INFO, or in-band.
RFC2833 Payload Type Preferred	Determines whether the local or remote payload type is preferred for incoming DTMF.
RFC2833 Payload Type	Defines the payload type number used for RFC2833 DTMF transmission.
DTMF Gain	Adjusts the amplitude of DTMF signals. Used to improve detection reliability.
Send Flash Event	Enables sending hook flash events to the SIP server. Required for features such as call transfer.
Send DTMF Tone to Analog When Call in Active	Allows DTMF tones to be sent to the analog side during active calls.
Codec Parameter	
Codecs Preferred	Determines whether codec selection follows local configuration or remote negotiation.

Parameter	Description
Coder Name	Specifies the audio codec used for voice communication. Multiple codecs can be prioritized.
Payload Type	Defines the Real-time Transport Protocol (RTP) payload type associated with the selected codec.
Packetization Time(ms)	Specifies the duration of audio data per RTP packet, in milliseconds. Affects latency and bandwidth.
Rate(kbps)	Defines the bit rate of the selected codec. Lower rates reduce bandwidth usage but may affect voice quality.
Silence Suppression	Enables suppression of silent audio periods to reduce bandwidth consumption.
Encryption Configuration	
SIP Encrypt	Enables encryption for SIP signaling. Used to secure communication between the gateway and the SIP server.
RTP Encrypt	Enables encryption for RTP media streams. Protects voice data during transmission.
Encrypt Mode	Specifies the encryption algorithm used for SIP/RTP traffic. Must be supported by both endpoints.

7.7 Tel Profile

Describes the Tel Profile parameters that control analog line behavior, gain, and fax-related settings assigned to a port.

The Tel Profile mainly consists of a series of line-related parameters including those for fax, gain value, and so on, which are used to configure different parameters for each FXS port.

Note:

- If a customer has multiple Tel Profiles configured, add a custom Tel Profile for each different Message Waiting Indicator (MWI) type to ensure that MWI works for analog sets. However, not all analog sets require different Tel Profiles. In such cases, the ports are assigned based on the port to which the phone is connected.
- The Tel Profile you create is available as an option in the **Tel Profile** field on the **Port** page.

The following table describes the Tel Profile parameters.

Table 33: Tel Profile

Parameter	Description
>Index	Specifies the profile index number used to identify this Tel Profile. This index is referenced when assigning the profile to ports.
>Description	Provides a user-defined description for the profile. Helps identify the purpose or configuration of the profile.
>Line Parameter	
>>Work Mode	Defines the operating mode of the port, such as voice only or voice and fax. Determines how the gateway processes analog signals.
>>Voice Output Mode	Specifies the output type for connected devices, such as telephone or headset. Affects audio characteristics and signal levels.
>>Config Mode (Gain)	Determines whether gain settings are configured using basic presets or advanced manual values. Advanced mode allows fine-tuning of audio levels.
>>>Tx Gain (IP->PSTN)	Adjusts the transmit audio gain from IP to the analog (PSTN) side. Used to control output volume toward the connected analog device.

Parameter	Description
>>>Rx Gain (PSTN->IP)	Adjusts the receive audio gain from the analog (PSTN) side to IP. Used to control input volume from the connected device.
>>Send CID before Ringing	Enables sending caller ID information before the ringing signal. Required for certain analog devices to correctly display caller ID.
>Service Parameter	
>>Visual MWI Type	Specifies the method used for visual message waiting indication, such as NEON. Determines how voicemail indication is signaled on analog devices.
>>>NEON Voltage (75-100V)	Defines the voltage level used for NEON-based message waiting indication. Must match the requirements of the connected analog device.
>FAX Parameter	
>>Fax Mode	Specifies the fax transmission method, such as T.38 or pass-through. Determines how fax signals are handled over IP.
>>>ECM	Enables Error Correction Mode for fax transmission. Improves reliability by detecting and correcting transmission errors.
>>>Rate	Defines the maximum fax transmission speed. Lower values may improve stability on poor network conditions.
>>Tone Detection by	Specifies whether fax tone detection is handled locally or by the remote side. Affects how fax calls are identified and processed.
>>Switch into Fax Mode When Detected CNG or CED	Automatically switches to fax mode when fax tones (CNG or CED) are detected. Ensures proper handling of incoming fax calls.

Parameter	Description
>FXS Param	
>>Loop Current Support	Enables loop current detection on the FXS port. Used to detect off-hook/on-hook conditions for connected analog devices. **Note**: This parameter is enabled by default if **Loop Current Time** is enabled on the **Advanced > FXS Parameters** page. You can enable or disable this parameter for each Tel Profile. For loop current configuration, see Configure Positive Disconnect on page 34.
>>Long Line Support	Optimizes the port for long cable distances. Helps maintain signal quality when analog devices are connected over extended wiring.

7.8 Port

Describes the per-port SIP account parameters configured on the Port page for each FXS port of the AG4124/AG4172 Analog Gateway.

Each FXS port of the AG4124/AG4172 Analog Gateway can be configured with a unique Session Initiation Protocol (SIP) account for registration. The SIP account parameters include the port number, whether to register, primary display name, primary SIP user ID, primary authenticate ID, primary authenticate password, off-hook auto-dial number, and caller ID.

Note: MiVoice Business cannot import port data into an AG4124 Analog Gateway. If you use the import option while port programming already contains existing data, the gateway displays a "Parameters error, setting failed" error. To resolve this error, delete the header information in the template before importing.

The following table lists the Port parameters.

Table 34: Port

Parameter	Description
Port	Specifies the FXS port number to configure. Each port represents a single analog endpoint.

Parameter	Description
Disable Port	Disables the selected port. When enabled, the port cannot make or receive calls.
Registration	Enables SIP registration for the port. Required for the port to communicate with the SIP server.
IP Profile	Selects the IP Profile that defines the SIP server, proxy, and codec settings for the port.
Tel Profile	Assigns a Tel Profile that controls analog line behavior, gain, and fax-related settings.
Display Name	Specifies the caller name sent in SIP signaling. Displayed on the called party's device, if supported.
SIP User ID	Defines the SIP extension or username used for registration and call routing.
Authenticate ID	Specifies the authentication username used for SIP registration. May differ from the SIP User ID.
Authenticate Password	Defines the password used for SIP authentication. Must match the credentials configured on the SIP server.
Offhook Auto-Dial	Automatically dials a predefined number when the handset goes off-hook. Used for hotline or emergency scenarios.
Auto-Dial Delay Time	Specifies the delay before auto-dial is triggered after going off-hook. Allows manual dialing within the delay period.
DND (Do Not Disturb)	Blocks incoming calls to the port. Outgoing calls may still be allowed, depending on configuration.

Parameter	Description
Caller-ID	Enables sending caller identification information to the connected analog device.
Number for CFU (Call Forwarding Unconditional)	Defines the destination number for unconditional call forwarding. All incoming calls are redirected to this number.
Number for CFB (Call Forwarding Busy)	Defines the destination number to use when the port is busy. Calls are forwarded to this number when the line is in use.
Number for CFNRy (Call Forwarding No Reply)	Defines the destination number to use when a call is not answered within a set time.
Call Waiting	Enables the call waiting feature, allowing the user to receive another incoming call while already on a call.
Play Call Waiting Tone	Enables an audible tone to notify the user of an in-coming call while on an active call.
Call Waiting Send CID	Sends caller ID information for the waiting call to the connected device, if supported.

For the step-by-step procedure to assign a Tel Profile to a port, see Sample Port Configuration on page 69. For the step-by-step procedure to import port configuration from a Comma-Separated Values (CSV) file, see Import Port Data Into the AG4124/AG4172 Analog Gateway on page 31.

7.9 Sample Port Configuration

Assign a Tel Profile to an FXS port on the Port page of the Web Management System.

Use this procedure to assign a Tel Profile to an FXS port.

1. Log in to the Analog Gateway (AG) Web Management System.
2. Navigate to **Port**.
3. Select the port and click **Modify**.
4. Set **Tel Profile** to the profile created in Tel Profile on page 64. For example, if you created a profile named FSK in Tel Profile, select FSK here.

Note:
- Ensure that the Tel Profile you add matches the port, since this is required for the Message Waiting Indicator (MWI) type.
- Configure the other parameters according to the site requirements.

5. Click **Save**.

7.10 Advanced

Introduces the Advanced menu, where you configure the SIP, port, and system-level parameters of the Analog Gateway.

The **Advanced** menu groups the pages used to configure Session Initiation Protocol (SIP) accounts, per-port profiles, and system-level behavior for the Analog Gateway. Use the pages under this menu to define SIP Server, IP Profile, Tel Profile, Port, Line Parameter, FXS Parameter, Media Parameter, Service Parameter, SIP Compatibility Parameter, NAT Parameter, Feature Code, and System Parameter settings.

7.10.1 Line Parameters

Describes the analog line parameters configured on the Advanced > Line Parameters page.

The Line Parameters page configures analog line behavior, including call progress tones, auto gain control, and fax settings.

The following table lists the Line Parameters.

Table 35: Description of Line Parameters

Parameter	Description
Call Progress Tone (Country and Region)	Selects predefined tone settings based on country or region. Automatically configures standard telephony tones, such as dial, busy, and ring tones.
Ring Back Tone	Defines the tone pattern played to the caller while waiting for the called party to answer. The format represents frequency and timing values.
Busy Tone	Specifies the tone pattern played when the called line is busy. Must align with regional telephony standards.
Dial Tone	Defines the tone played when the user lifts the handset, indicating readiness to dial.

Parameter	Description
Ringing Tone	Specifies the tone pattern used for incoming call alerting on the analog device.
Call Waiting Tone	Defines the tone behavior when a second call arrives during an active call. Controlled by duration, gap, and repeat-count parameters.
Call Waiting Tone Duration	Specifies how long the call waiting tone plays for each alert cycle, in milliseconds.
Call Waiting Tone Gap	Defines the interval between repeated call waiting tones, in milliseconds.
Call Waiting Tone Repeat Count	Specifies how many times the call waiting tone repeats during an incoming call alert.
Auto Gain Control	
IP->PSTN	Enables automatic adjustment of audio levels from the IP side to the analog side. Helps maintain consistent output volume.
PSTN->IP	Enables automatic adjustment of audio levels from the analog side to the IP side. Helps normalize input audio levels.
DSP Jitter Buffer (Recv) Config Mode	Defines how the jitter buffer operates for incoming RTP packets. Adaptive mode adjusts the buffer size dynamically, based on network conditions.
Buffer Size	Specifies the jitter buffer size, in milliseconds. Larger values improve stability but increase latency.
Line Parameter	

Parameter	Description
Work Mode	Defines whether the port supports voice only or voice and fax. Determines signal-handling behavior.
Voice Output Mode	Specifies the output type, such as telephone or headset. Affects audio signal characteristics.
Config Mode (Gain)	Selects basic or advanced gain configuration. Advanced mode allows manual adjustment of transmit and receive gain.
Tx Gain (IP->PSTN)	Adjusts the audio level sent from the IP network to the analog device. Used to control output volume.
Rx Gain (PSTN->IP)	Adjusts the audio level from the analog device to the IP network. Used to control input sensitivity.
FAX Parameter	
Fax Mode	Specifies how fax traffic is handled, such as T.38 or pass-through. Determines the fax transmission method over IP.
ECM	Enables Error Correction Mode (ECM) for fax transmission. Improves reliability by retransmitting corrupted data.
Rate	Defines the maximum fax transmission speed. Lower speeds may improve reliability on unstable networks.
Tone Detection by	Specifies whether fax tone detection is handled locally or remotely. Affects how fax calls are identified.
Switch into Fax Mode When Detected CNG or CED	Automatically switches to fax mode when Calling Tone (CNG) or Called Station Identification (CED) fax tones are detected. Ensures proper handling of fax calls.

7.10.2 FXS Parameters

Describes the FXS port parameters configured on the Advanced > FXS Parameters page.

On the **Advanced** > **FXS/FXO** page, you can configure FXS port parameters, including polarity reversal, hook flash detection, Caller ID (CID) type, and so on.

Table 36: Description of FXS Parameters

Parameter	Description
Send Polarity Reversal	Do not enable this parameter when an analog phone is connected to the FXS port. When an AG4124/AG4172 FXS port is connected to an FXO port on a Private Branch Exchange (PBX), enable **Send Polarity Reversal** if the PBX relies on polarity reversal to determine the start and end of a call.
Detect Hook Flash	If you enable **Detect Hook Flash**, you must also set a minimum time and a maximum time. If the phone's hook switch is held for longer than the minimum time but less than the maximum time, the gateway treats the action as a hook flash. If it is held for longer than the maximum time, the gateway treats the action as a hang-up.
Min Time	Defines the minimum duration of a hook flash. If the duration is shorter than this value, the system does not recognize it as a hook flash.
Max Time	Defines the maximum duration of a hook flash. If the duration is longer than this value, the system does not recognize it as a hook flash.
CID Type	Specifies the Caller ID (CID) type: DTMF or FSK.
Modulation Type	Specifies the modulation type used for Frequency-Shift Keying (FSK) caller ID: BFSK Bell 202 or CCITT V.23.
Message Type	Specifies the call display type: SDMF or MDMF.
Message Format	Specifies the call display format shown on the analog phone. Can be "Display Name and CID", "CID only", or "Display Name only"; the default value is "Display Name and CID".
Send CID before Ringing	If enabled, the Analog Gateway sends the caller ID to the phone before ringing; otherwise, the caller ID is displayed after ringing begins.

Parameter	Description
Delay of sending CID after Ringing	Specifies the delay before the caller ID is sent, when caller ID is set to display after ringing. Default value is 500 ms. **Note**: This parameter is visible only on the AG4172 device.
Caller Number Preferred when FXS Call Out	Configures the primary caller number that is sent to the target number for outgoing calls. You can select Adaptive, Port Account, or Port Group Account.
CFNRy Timeout	Sets the timeout for the Call Forwarding No Reply service.
SLIC Setting	Sets the Subscriber Line Interface Circuit (SLIC) impedance to match the connected analog phone.
REN	Specifies the maximum number of extensions that can be connected to a single FXS port. If you change this parameter, restart the AG4124/ AG4172 for the change to take effect.
Abnormal Off-hook Detection	Enables detection of an abnormal off-hook condition on an FXS port, where the connected analog device remains off-hook without valid call activity, or remains off-hook for an extended period after a call com- pletes.
Current Threshold(Off-Hook -> On-Hook)	Use this parameter in either of the following conditions: If an FXS port connected to a specific FXS phone detects off-hook even though the phone itself is not off-hook, set this threshold to correct the mismatch. If the issue persists, try setting both the off-hook current threshold and the on-hook current threshold to 20 mA.
Current Threshold(On-Hook -> Off-Hook)	
Port Current Protection Threshold(0: means disable)	Configures the port current anomaly protection threshold. Range is 0-11, where 0 turns the protection off.
Current of Off-Hook(Non-long Line)	Specifies how much current, in mA, is sent to the line when the port is off-hook. This parameter applies only when the device is in normal mode, with *Long Line Support* disabled.
Loop Current Support	Use this parameter in the following scenario: when a call is dropped, the AG41xx plays a busy tone to the phone, but an elevator phone connect-

Parameter	Description
	ed to the line does not support the busy tone and so cannot drop the call.
Loop Current Time	Specifies how long the loop current is maintained, in milliseconds. **Default Value:** 600 **Note**: This parameter is displayed only when *Loop Current Support* is enabled. For loop current configuration, see Configure Positive Disconnect on page 34.
Busytone Duration	Defines how long the AG41xx plays a busy tone to the phone after the remote side ends the call, in seconds. After this duration, the AG41xx sends a loop current signal to disconnect the phone. **Default Value:** 30 **Note**: This parameter is available only when *Loop Current Support* is enabled.
Long Line Support	Enable this parameter only when the cable length is between **800 meters (0.5 miles)** and **6000 meters (3.72 miles)**. **Note**: This cable length range was tested using AWG-26 gauge cable.

7.10.3 Media Parameters

Describes the RTP, DTMF, and preferred vocoder media parameters configured on the Advanced > Media Parameters page.

Media parameters cover the Real-time Transport Protocol (RTP) start port, Dual-Tone Multi-Frequency (DTMF) parameters, and preferred vocoder settings.

Table 37: Description of Media Parameters

Parameter	Description
Use Random Port	If enabled, the AG4124/AG4172 Analog Gateway chooses a random port as the start port for RTP.

Parameter	Description
RTP Start Port	When **Use Random Port** is not selected, configure a start port for RTP here. Default RTP start port is 8000.
UDP Checksum Validation	Enables or disables the header checksum of the User Datagram Protocol (UDP).
SRTP Mode	Sets the Secure Real-time Transport Protocol (SRTP) mode used for the media stream. Default value is AUTO.
DTMF Method	Specifies how DTMF tones are transmitted: SINGAL, INBAND, or RFC2833.
RFC2833 Payload Type Preferred (Incoming Call)	For an incoming call, selects the local or remote RFC2833 payload type as the preferred payload type.
RFC2833 Payload Type	Local payload value; default value is 101.
DTMF Gain	Default value is 0 dB.
DTMF Send Cadence	Specifies the interval for sending DTMF signals. Default value is 200 ms.
Send Flash Event	If enabled, the AG4124/AG4172 Analog Gateway sends a flash-hook event to the remote terminal, so the user does not need to handle it locally.
Send DTMF Tone to Analog When Call in Active	If enabled, DTMF tones are sent to the analog phone during an active call.
Coder Name	The Analog Gateway supports G.729, G.711U, G.711A, G.723, and G.726-16/24/32/40. Outgoing calls use G.729.
Payload Type	Each codec has a unique payload value. See RFC3551.
Packetization Time	Specifies the duration of voice data per packet.

Parameter	Description
Rate	The voice data flow rate; set by the system by default. The preferred rate is 20 ms.
Silence Suppression	Default value is disabled. When enabled, this feature reduces the band-width used for VoIP transmission, helping to avoid network congestion.
Prefer Codec	Selects the local or remote codec as the preferred codec.

7.10.4 Service Parameters

Describes the Service, MWI, IP Call, Domain Query, and Digit Map parameters configured on the Advanced > Service Parameters page.

The following tables list the service parameters.

Table 38: Service Parameters

Parameter	Description
Timeout for off-hook	Defines a timer for when the user is off-hook on an analog phone with-out dialing any digits.
Timeout for dialing	Limits the time between two digits for users typing the digits of a number through an extension. If the timeout expires, the gateway considers dial-ing finished and tries to send the call to the SIP server. Default value is 4 seconds.
Timeout for Answer (Outgo-ing Call)	Determines how long the calling party waits for an answer after making an outgoing call through a phone.
Timeout for Answer (Incom-ing call)	Determines how long the phone rings for incoming calls.
No RTP Detected	If you enable this parameter, the gateway detects when no RTP packets arrive during the set time period.
Period without RTP Packet	Specifies the time period during which no RTP packets arrive.

Table 39: MWI Parameters

Parameter	Description
SUBSCRIBE for MWI (Message Waiting Indicator)	Notifies the user of new voicemail using a SIP NOTIFY message.
MWI Subscription Expires	Specifies the expiry time of the MWI subscription. Default value is 3600 s.
Voicemail User ID	Specifies the user ID used to access voicemail. The user ID has a maximum length of 32 characters. **Note**: When a Voicemail User ID is assigned to an AG4124/ AG4172, a specific user is registered to the IP PBX. Whenever someone leaves a voicemail message on the phone, the AG4124/AG4172 uses this Voicemail User ID to send an INVITE to the IP PBX.
Visual MWI Type	Specifies the visual MWI type: NEON, FSK, or RP.

Table 40: IP Call Parameters

Parameter	Description
IP-to-IP Call	If you enable this parameter, the user can dial the IP address through a phone to call the destination gateway.
Only Accept Call from ACL (SIP server or IP Trunk)	If you enable this parameter, the Analog Gateway accepts incoming calls from the SIP server only. Default value: disabled.
Anonymous Call	If you enable this parameter, the gateway includes "anonymous" in the SIP message.
Reject Anonymous Call	If you enable this parameter, the gateway rejects all anonymous calls. Default value: enabled.
# as ending Dial Key	If you enable this parameter, the gateway uses "#" as the end mark for dialing.
# Escape	If you enable this parameter, the gateway treats "#" as a digit of the dialed number.

Parameter	Description
Send '#' when First Dial Number is '*'	If you enable this parameter, the gateway sends "#" when the first dialed digit is "*".

Table 41: Domain Query

Parameter	Description
Domain Query Type	Specifies how the gateway resolves SIP server domain names using DNS queries. Configure this parameter based on the **SIP Server** IP address type configured in SIP Server on page 56. • **A Query** resolves the domain name directly to one or more IP addresses. The gateway connects to the returned IP(s). This is the recommended method for deployments, including resiliency using multiple A records. • **SRV Query** resolves service records that provide server priority, weight, and port information. **Important**: SRV Query is not supported. Use A records with multiple IP addresses to achieve failover behavior.
Domain Re-resolution Interval	Specifies the interval for re-parsing the domain name. Range: 0 to 3600 s. Default value is 0, which means no re-parsing.
DNS cache	If you enable this parameter, the AG4124/AG4172 Analog Gateway caches the DNS query results.

The gateway uses Digit Map for number dialing of calls through FXS ports of the AG4124/AG4172 Analog Gateway. For more information on the configuration, see Configure the Digitmap Parameter on page 94.

Table 42: Digit Map

Supported Objects	Digit	0-9
	T	Timer
	DTMF	A digit, a timer, or one of the symbols of A, B, C, D, #, or *

Range	[ ]	One or more DTMF symbols enclosed in the [ ], but only one DTMF symbol can be selected.
Range	()	One or more expressions enclosed in the (), but only one can be selected.
Separator	|	Separate expressions or DTMF symbols.
Subrange	-	Two digits separated by a hyphen (-), which matches any digit between and including the two digits.
Wildcard	x	Matches any digit between 0 and 9.
Modifiers	.	Matches 0 or more times the preceding element.
Modifiers	?	Matches 0 or 1 times the preceding element.

7.10.5 SIP Compatibility Parameters

Describes the SIP interoperability compatibility parameters configured on the Advanced > SIP Compatibility Parameters page.

This section describes the Session Initiation Protocol (SIP) compatibility parameters configured on the Advanced > SIP Compatibility Parameters page, including the attended transfer trigger, early media, session timer, and heartbeat interval settings.

Table 43: Description of SIP Compatibility Parameters

Parameter	Description
RFC3407 Support	Whether to enable RFC3407 support. If this parameter is enabled, the Analog Gateway supports RFC 3407 (Request for Comments 3407), which defines the Session Description Protocol (SDP) capability for backward compatibility.
Forbid "user=phone"	When disabled, "user=phone" is not carried in the Uniform Resource Identifier (URI).

Parameter	Description
"From" SIP URI includes "user=phone"	If you enable this parameter, "user=phone" is included in the URI. When calls are routed to the Public Switched Telephone Network (PSTN), the called number comes from the user name. The default value is disabled.
Default Port Display Policy in SIP URL	It supports Hidden, Display, and Hide when the host is a domain.
INVITE with "P-Preferred-Identity" Header (RFC3325)	If you enable this parameter, the "P-Preferred-Identity" header is added to the INVITE message for anonymous calls (RFC 3325).
Implicit Subscription	Enabling implicit subscription ensures successful Message Waiting Indicator (MWI) subscription. Generally, MWI must be enabled on the device for automatic subscription. When enabled, Broadworks and certain IP-based Private Branch Exchange (IP PBX) brands support implicit subscription for MWI. Upon SIP account registration, the IP PBX sends a SIP NOTIFY message with a from-tag and to-tag to the registered endpoint. Devices without implicit subscription support ignore the NOTIFY message unless MWI subscription is active.
Only Accept Call from ACL (SIP server or IP Trunk)	If you enable this parameter, the Analog Gateway accepts incoming calls from the SIP server only. The default value is *disabled*.
Value of "Refer To" refers to "Contact"	If you enable this parameter, the contact header must be filled in in the "Refer To" field of a SIP message.
Third Party Do Not Send 18x Response	If you enable this parameter, the third party cannot send an 18x response during an attended transfer.
REFER Delay	When the call is in blind-transfer status, the call transfer initiator sends REFER only after receiving a 200 OK response from the remote side.
Send BYE when Recv REFER Re-	If you enable this parameter, the third party can send BYE to release the session after receiving REFER during a blind transfer.

Parameter	Description
sponse (Unattended)	
Send New REGISTER when Recv 423 Response	If you enable this parameter, the value of the Expires header is automatically updated and REGISTER is resent after a 423 response is received.
Verify the Contact Header in REGISTER Response	Enable this parameter to verify the contact header. If verification fails, the registration also fails.
Support Wildcard in REGISTER Response	In some cases, the IP PBX allows device registration by using a wildcard in the SIP account. When responding, the IP PBX includes the wildcard in the 200 OK message to indicate that this feature is active.
CSeq Start with 1	If you enable this parameter, the value of CSeq starts with 1.
Forbid Invalid m=line in reINVITE	If you enable this parameter, the Analog Gateway prevents an invalid m= line from being carried in the SDP of a re-INVITE.
SIP Message with ID Header	The SIP header carries two types of IDs: MAC or serial number (SN).
ID Header Separator	ID header separator for MAC or SN.
Call Waiting Response Code	You can choose 180 or 182 as the call waiting response code.
RTP Mode in SDP when Call Holding	Use "send only" or "inactive" as the RTP mode during call holding.
Accept Orphan 200 OK	If you enable this parameter, the AG4124/AG4172 Analog Gateway supports a different to-tag 200 OK in an INVITE session.

Parameter	Description
Called Number Preferred	Choose the P-Called-Party-ID header or the Request-Line.
Caller-ID Preferred	Choose the P-Asserted-Identity header or the From header.
Check SDP Strictly	Specifies whether SDP checking is strict.
Report SDP Whatever	If you enable this parameter, SDP is reported at any time.
18x Response Preferred(Without Effective P-Early-Media)	Choose "18x Response with SDP," "Last 18x Response," or "Local Ring Tone Only."
Flashhook Operation Mode	Choose Mode 1, Mode 2, or Mode 3.
Attended Transfer Trigger	Choose "On-hook" or "Flashhook +4."
Multiple Flash-Hook before Attended Transfer	If you enable this parameter, performing a flashhook initiates a second session. If flashhook is triggered again before the call transfer completes, the transfer succeeds after the call disconnects.
Multipart Payload Support	Specifies support for Multipurpose Internet Mail Extensions (MIME) types.
Local Extension is Prefered(Tel in)	If the destination number is another port on the same AG41xx unit, the call is not sent to MiVoice Business; it is sent directly to the Foreign Exchange Station (FXS) port.
Ignore ACK	When enabled, even if the FXS port is off-hook and the SIP User Agent (UA) does not receive an ACK message, the device does not resend the 200 OK response.

Parameter	Description
Report Hook State via SIP INFO	Enabling this option allows the system to send SIP INFO messages that indicate the FXS port's hook status, such as off-hook or on-hook.
Old Crypto Label	Enabling this parameter supports both new and old MiVB versions at the same time. If enabled, Secure Real-time Transport Protocol (SRTP) carries the old GES. • AES_CM_256_HMAC_SHA1_80 • AES_CM_256_HMAC_SHA1_32 • AES_CM_192_HMAC_SHA1_80 • AES_CM_192_HMAC_SHA1_32
Second Dial Prefix	If you enable this parameter, the AG4124/AG4172 Analog Gateway plays a dial tone to indicate that it is ready for the second dial-prefix number, which is required for external calls. For example, when making an outside call from a hotel room, enter the prefix number; the system plays a dial tone indicating that you can now dial an external number. **Note**: For example if the **Second Dial Prefix** is configured as **6**, and the user dials 12345678 after secondary tone, the system sends 612345678 to MiVB.
Early Media Parameters	
PRACK(RFC3262)	If you enable this parameter, the AG4124/AG4172 Analog Gateway supports reliable transmission of the provisional response (PRACK, RFC 3262).
PRACK Only for 18x with SDP	If you enable this parameter, PRACK is sent only when SDP is present in the 18x response.
Early Media	If you enable this parameter, the AG4124/AG4172 Analog Gateway supports receiving early media.
Early Answer	If you enable this parameter, the AG4124/AG4172 Analog Gateway supports early answer.
Session Timer (RFC4028)	Specifies whether to enable the session timer (RFC 4028). The default value is disabled.
Session-Expires	The interval for refreshing the session. The default value is 1800 seconds. The Session-Expires header field conveys the session interval for a SIP session.

Parameter	Description
Min-SE	The minimum interval for refreshing the session. The default value is 1800 seconds. The Min-SE header field indicates the minimum value for the session interval.
Session Refresh Method	The method used to refresh the session. The default value is INVITE.
SIP Protocol Timer Parameters	
T1	The value of the T1 timer in the SIP protocol. The default value is 500 ms.
T2	The value of the T2 timer in the SIP protocol. The default value is 4000 ms.
T4	The value of the T4 timer in the SIP protocol. The default value is 5000 ms.
Max Timeout	The maximum timeout for sending or receiving SIP messages. The default value is 32000 ms.
Heartbeat Interval	The interval for sending the heartbeat message. The default value is 10 seconds.
Heartbeat Timeout	The timeout for sending the heartbeat message. The default value is 16 seconds.
Username of OPTION(Heartbeat) for "SIP Server"	The user ID part of the OPTIONS SIP message in the heartbeat request for the SIP server.
Username of OPTION(Heartbeat) for "IP Trunk"	The user ID part of the OPTIONS SIP message in the heartbeat request for the IP trunk.
Username of REGISTER (Connectivity Check)	When sending a heartbeat message for connectivity checks to the MiVB server, the From/To fields in the message carry the username if registered. If disabled, "heartbeat" is used in the From/To fields.

Parameter	Description
Release all call when Heartbeat Timeout	When the heartbeat timeout expires, all calls are released or terminated.
User-Agent Header	Customize the User Agent (UA) header.
Response code when Fax Reinvite was Rejected	Customize the SIP response code for fax rejection.

7.10.6 NAT Parameter

Describes the NAT traversal parameters configured on the Advanced > NAT Parameter page.

The NAT Parameter settings control how the Analog Gateway handles Session Initiation Protocol (SIP) signaling and Session Description Protocol (SDP) media information when deployed behind a Network Address Translation (NAT) device such as a firewall or router. These settings determine whether the Analog Gateway uses local/private IP addresses or public/NAT-translated IP addresses for SIP and Real-time Transport Protocol (RTP) communication.

The following table describes the NAT Parameter information. For NAT parameter configuration, see Configure the NAT Parameter on page 88.

Table 44: NAT Parameter

Parameter	Description
NAT Traversal	Specifies the NAT handling mode used by the Analog Gateway for SIP communication. The following options are supported: • **Disable** - Recommended for direct MiVoice Business (MiVB) deployments where the Analog Gateway and MiVB are located within the same local network and no NAT device exists between them. • **STUN** - Use when the Analog Gateway is deployed behind a dynamic NAT router and a STUN server is available. • **Static NAT** - Use when the Analog Gateway is deployed behind a NAT device using a fixed public IP address and static port forwarding.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>Dynamic NAT - Recommended for deployments using MiVoice Border Gateway (MBG) or when the Analog Gateway is deployed behind a NAT router using dynamically assigned public IP addresses or port mappings.
Note:

When deploying the Analog Gateway through MiVoice Border Gateway (MBG), you must enable NAT Traversal for correct SIP signaling behavior. For example:
For an MBG deployment, enable the NAT.
For a direct MiVB deployment, disable the NAT.</td></tr>
<tr><td>Via of Message</td><td>Controls which IP address is used in the SIP Via header.
Local Address - Uses the local/private IP address of the Analog Gateway.
NAT Address - Uses the translated public NAT address.</td></tr>
<tr><td>Contact of Message</td><td>Controls which IP address is included in the SIP Contact header.
Local Address - Uses the local/private IP address of the Analog Gateway.
NAT Address - Uses the translated public NAT address.</td></tr>
<tr><td>SDP of Message</td><td>Controls which IP address is included in the SDP media information used for RTP audio communication.
Local Address - Uses the local/private IP address for RTP media communication.
NAT Address - Uses the translated public NAT address for RTP media communication.</td></tr>
</table>

7.10.6.1 Sample NAT Parameter Configuration

Notes and purpose for configuring Network Address Translation (NAT) behavior on the Analog Gateway for SIP connectivity scenarios.

Notes

- Network Address Translation (NAT) must be enabled when connecting to the MiVoice Border Gateway (MBG); otherwise, the Contact Uses the Local Connection Port setting does not function.
- NAT is enabled by default; no change is required for standard MBG deployments.
- In some scenarios, enabling NAT for a direct MiVB connection may cause voice-path issues; you may need to disable NAT.
- The behavior of Contact Uses the Local Connection Port depends on NAT being enabled.
- Session Traversal Utilities for NAT (STUN) is not used in this configuration.

Purpose

Configure NAT behavior on the Analog Gateway (AG) for SIP connectivity scenarios, including MBG integration and direct MiVB connections.

7.10.6.1.1 Configure the NAT Parameter

Configure Network Address Translation (NAT) traversal settings on the Analog Gateway.

> **Note**:
>
> The default Network Address Translation (NAT) Parameter values are suitable for standard deployments and typically do not require modification. Change these settings only for specific deployment scenarios where network topology or SIP signaling behavior differs, such as MBG integration or a direct MiVB connection with NAT-related constraints. The exact conditions that require a deviation from the default configuration depend on the deployment.

1. Log in to the Analog Gateway (AG) web interface.
2. Navigate to **Advanced > NAT Parameter**.
3. Configure the NAT settings:
   - Set **NAT Traversal** to **Dynamic NAT**.

     > **Note**:
     > When you deploy the Analog Gateway through MiVoice Border Gateway (MBG), you must enable NAT Traversal for correct SIP signaling behavior. For example:
     > - For an **MBG** deployment, **enable** NAT.
     > - For a direct **MiVB** deployment, **disable** NAT.

   - For **Via of Message**, select **Local Address** or **NAT Address** based on your deployment requirements.
   - For **Contact of Message**, select **NAT Address**.
   - For **SDP of Message**, select **Local Address** or **NAT Address** based on your deployment requirements.
4. Click **Save**.

5. Restart the device for the changes to take effect.

Note:

- You must enable NAT when connecting to MBG; otherwise, expected SIP behavior may not function.
- An incorrect NAT configuration can cause registration failures, one-way audio, or failed calls.

7.10.7 Feature Codes

Describes the feature access codes configured on the Advanced > Feature Codes page.

Feature Access Codes (FACs) let connected analog devices activate specific gateway features. A user activates a feature by dialing its code from a connected device.

Note:

- Mitel recommends enabling only the feature codes required for operation and troubleshooting. Leave administrative and network-configuration feature codes disabled unless they are explicitly required.
- Enabling unnecessary feature codes may allow unauthorized users to modify device or network settings from an analog phone connected to the gateway.
- As of firmware 33.83.11.28 and later, a factory reset disables all feature access codes; this is the default setting for feature access codes. For information about factory reset, see Factory Reset Using the RST Button on page 31.

The following table lists the recommended feature codes to enable.

Important:

Ensure the following before configuring the feature codes:

- Plan feature access codes carefully to avoid conflicts with other dialing patterns, feature codes, emergency numbers, or existing PBX feature access codes.
- Mitel recommends validating all configured feature access codes against the deployment's dialing plan before enabling the feature.

Table 45: Recommended Feature Code Configuration

Feature code	Recommended state	Reason
Device function		
LAN IP Inquiry	Enabled	Allows users or administrators to query device IP information.
Inquiry Phone Number	Enabled	Allows verification of the configured phone number.

Feature code	Recommended state	Reason
Inquiry PortGroup Number	Enabled	Allows verification of the configured port group.
Inquiry Registration Status	Enabled	Allows checking SIP registration status.
Port Voice Up	Enabled	Required for port control operations.
Port Voice Down	Enabled	Required for port control operations.
Call function		
Call Park	Enabled (if used)	Required for Call Park functionality.

7.10.8 System Parameters

Describes the NTP, web, Telnet, and SSH system parameters configured on the Advanced > System Parameters page.

System parameters include Network Time Protocol (NTP), daylight saving time, daily reboot time, web parameter, telnet parameters, and remote management.

NTP is a time synchronization protocol for computers.

Warning: Enable Telnet only for diagnostic purposes, and disable Telnet after the diagnosis is complete.

Note:

- Mitel recommends enabling the Summary Log and the System Log for security reasons.
- Enable SSH only for diagnostic purposes, and disable SSH after the diagnosis is complete.
- If you enable SSH, change the Shell password to a unique password. For more information, see *AG4100 Analog Gateway Security Guidelines*.

Table 46: Description of System Parameters

Parameter	Description
NTP	Enables or disables NTP.
Primary NTP Server Address	Specifies the IP address of the primary NTP server. Default IP address: us.pool.ntp.org.
Primary NTP Server Port	Specifies the service port of the primary NTP server. Default port: 123.
Secondary NTP Server Address	Specifies the IP address of the secondary NTP server. Default IP address: 64.236.96.53.
Secondary NTP Server Port	Specifies the service port of the secondary NTP server. Default port: 123.
SYN Interval	Specifies the interval used to synchronize the time of the AG4124/AG4172 Analog Gateway. Default value is 3600 s.
Time Zone	Specifies the time zone of the Analog Gateway. Default configuration: United States Central Time, Chicago.
Daylight Saving Time	Enables or disables daylight saving time.
Log > Summary	Enables the Summary Log. It is recommended that the Summary Log be enabled for security reasons.
Log > System Log	Enables the System Log. It is recommended that the System Log be enabled for security reasons.
Network Diagnose > local network fault detection	Enables detection of local network faults. Disable this when using the local network disable ping option.
Network Diagnose > local network interruption detection	Enables detection of local network interruptions.

Parameter	Description
WEB Port	Specifies the web port of the Analog Gateway. Default port: 80.
SSL Port	Specifies the Secure Sockets Layer (SSL) port. Default port: 443.
No operation logout time	Indicates the automatic logout timer if there is no user activity on the Graphical User Interface (GUI). Default value is 10 minutes.
Maximum number of consecutive failed login attempts	Indicates the maximum number of consecutive failed login attempts allowed. When this limit is reached, the system prevents the user from logging in to the GUI for the duration configured in **Continuous login failure lock time (0: Always locked)**. Default value is 5 attempts.
Continuous login failure lock time (0: Always locked)	Indicates the lockout period after which the user can retry login. Default value is 8 minutes. **Note**: If the value is set to 0, the account is locked indefinitely after reaching the maximum number of failed login attempts. To regain access to the portal, you must restart the device.
Telnet port	Specifies the listening port of the Telnet service. Default port: 23.
Telnet Enable	Enables the Telnet service. Enable Telnet only for diagnostic purposes, and disable Telnet after the diagnosis is complete.
SSH Enable	Enables the Secure Shell (SSH) service. Enable SSH only for diagnostic purposes, and disable SSH after the diagnosis is complete. If you enable SSH, change the Shell password to a unique password.

Note:

- After Web port and Telnet port are configured, you must restart the Analog Gateway for the configurations to take effect.
- For a complete list of IP ports used by the AG4124/AG4172, see *AG4100 Analog Gateway Security Guidelines*.

7.10.9 Sample Digitmap Configuration

Overview of the Digitmap parameter, when to use it, and how the Analog Gateway applies it to dialed digits.

Overview

The Digitmap parameter defines how the Analog Gateway collects and processes dialed digits from analog devices before sending the call to the SIP server.

A digitmap controls:

- The number of digits expected
- Allowed dialing patterns
- When the gateway sends the call
- Inter-digit timeout behavior

When to Use Digitmap

Configure Digitmap when:

- The deployment requires a fixed dialing length.
- Calls must be routed based on specific dialing patterns.
- Users experience delayed call setup due to inter-digit timeout.
- The Analog Gateway is connected to systems that require predefined dialing plans.

Digitmap Behavior

The Analog Gateway collects the digits that you enter and compares them against the configured digitmap pattern.

When the dialed digits match the configured pattern:

- The gateway immediately sends the call to the SIP server.
- The inter-digit timeout is bypassed if the pattern is complete.

7.10.9.1 Example Digitmap Patterns

Sample digitmap patterns and the dialing behavior each one matches.

Table 47: Common Digitmap Examples

Digitmap	Description
[2-9]xxxxxxx	Matches eight-digit numbers starting with 2 through 9.
0xxxxxxxxx	Matches 10-digit numbers starting with 0.
*xx	Matches feature codes that begin with *.
#xx	Matches feature codes that begin with #.
x.T	Accepts variable-length dialing and waits for the t imeout before sending the call.

7.10.9.2 Configure the Digitmap Parameter

Configure the Digitmap parameter on the Analog Gateway.

1. Log in to the Analog Gateway Web Management System.
2. Navigate to **Advanced > System Parameter**.
3. Locate the **Digitmap** parameter.
4. Enter the digitmap pattern that matches your dialing requirements. See Example Digitmap Patterns on page 93.
5. Click **Save**.
6. Test the dialing behavior from an analog phone that is connected to the gateway.

Verify the following after configuration:

- Calls are routed immediately after you enter the expected digits.
- Feature codes are recognized correctly.
- No unexpected dialing delay occurs.

Note:

An incorrect digitmap configuration can prevent calls from being routed correctly or can cause delayed call setup.

Note:

If you configure variable-length dialing, the gateway may wait for the inter-digit timeout before sending the call.

7.11 Call and Routing

Introduces the Call and Routing menu, where you configure how the Analog Gateway routes calls between the IP network and its Tel (analog) interfaces, and how it manipulates caller and called numbers.

The **Call and Routing** menu groups the pages used to define how the Analog Gateway routes calls between the Internet Protocol (IP) network and its analog (Tel) ports, and how it manipulates caller and called numbers along the way. Use the pages under this menu to define Wildcard Group, Port Group, IP Trunk, and Routing Parameter settings, and to configure the IP-to-Tel and Tel-to-IP/Tel routing and number-manipulation rules for calls.

7.11.1 Wildcard Group

Describes the wildcard group parameters used to group dial patterns for call routing rules.

Defines wildcard patterns for Session Initiation Protocol (SIP) user identities, known as IP Multimedia Public Identities (IMPU), and maps them to specific identities. Use wildcard groups to group users and simplify routing or service handling based on pattern matching.

The following table lists the Wildcard Group information.

Parameter	Description
Wildcarded IMPU	Specifies a wildcarded Public User Identity pattern used to match multiple SIP user identities. Enables grouping of users based on defined patterns.
Associated IMPU	Defines the actual Public User Identity mapped to the wildcard pattern. Used for routing or service handling when a match occurs.

7.11.2 Port Group

Describes the Port Group parameters used to group FXS ports together for call routing.

When two or more Foreign Exchange Station (FXS) ports need to register with the same Session Initiation Protocol (SIP) account, you can group the ports together and then set an account for the group.

Parameters of the port group include those for registration, primary display name, primary SIP user ID, primary authentication ID and password, secondary display name, secondary SIP user ID, secondary authentication ID and password, off-hook auto dial, auto dial delay time, port select, and so on.

The following table lists the Port Group information.

Table 48: Port Group

Parameter	Description
>Index	The number of the port group; It uniquely identifies a route.
>Registration	Enables SIP registration for the port group. When enabled, ports in the group register with the SIP server using the configured account.
>IP Profile	Selects the IP Profile applied to the port group. Defines SIP server, proxy, codec, and signaling behavior for all ports in the group.
>Description	The description of the port group; it is used to identify the port group.
>Display Name	Display name of the port group that will be used in a SIP message, for example: *INVITE sip:bob@biloxi.com SIP/2.0* *Via: SIP/2.0/UDPpc33.atlanta.com;branch=z9hG4bK776asdhds*

Parameter	Description
	Max-Forwards: 70 *To: Bob <sip:bob@biloxi.com>* *From: Alice <sip:alice@atlanta.com>;tag=1928301774* *Here Bob and Alice are the display name*
>SIP User ID	Specifies the user ID for this SIP account, provided by the VoIP service provider (ITSP). It is usually in the form of digits, similar to a phone number, or it can be an actual phone number.
>Authenticate ID	Specifies the SIP service subscriber's ID for authentication. It can be identical to, or different from, the SIP user ID.
>Authenticate Password	Specifies the SIP service subscriber's password for authentication. For more information on passwords, see Passwords on page 112.
>Offhook Auto-Dial	Specifies an extension or phone number that the Analog Gateway automatically dials as soon as the user picks up the phone.
>>Auto-dial Delay time	How long auto-dialing will be delayed. Supported value: 0 to 90 seconds
>Port Select	It specifies the policy for selecting a port for ringing in the port group: • Ascending: the Analog Gateway always selects a port from the minimum number. • Cyclic ascending: selects next port sequentially; loops back after last port. • Descending: selects port from the maximum number. • Cyclic descending: selects previous port sequentially; loops back after first port. • Group ring: all ports ring at the same time.
>>Pickup UP on group	When one port rings, the user can dial '*#' to pick up the call from other ports under the same port group.
>>Call Answer Timeout	Specifies how long, in seconds, a call rings on the port group before the system considers it unanswered.

Parameter	Description
>>Select Port Count	Defines how many ports the Analog Gateway selects during call distribution. Behavior depends on the selected port selection strategy.
>Port	Select ports for this port group.

7.11.3 IP Trunk

Describes the IP Trunk parameters used to define a trunk group toward a SIP peer.

Defines a Session Initiation Protocol (SIP) trunk connection to a remote server or peer device. Use it to route calls between the gateway and external SIP systems, such as a Private Branch Exchange (PBX) or a service provider.

The following table lists the IP Trunk information.

Table 49: IP Trunk

Parameter	Description
Index	Specifies the trunk index used to identify this IP Trunk configuration.
IP Profile	Selects the IP Profile applied to this trunk. Defines SIP server settings, codecs, and signaling behavior.
Description	Provides a user-defined description for the IP trunk. Helps identify its purpose or destination.
Remote Address	Specifies the Internet Protocol (IP) address or domain name of the remote SIP server or peer endpoint.
Remote Port	Defines the port number used for SIP signaling on the remote server.
Heartbeat	Enables periodic keepalive messages to monitor connectivity with the remote SIP endpoint.

7.11.4 Routing Parameter

Describes the routing parameters that control how the Analog Gateway selects a route for a call.

Routing parameters determine whether the Analog Gateway routes a call before or after manipulation.

The following table lists the Routing Parameter information.

Table 50: Routing Parameter

Parameter	Description
Calls from IP	Specifies whether the Analog Gateway routes calls from the Internet Protocol (IP) network before manipulation or after manipulation.
Calls from Analog Line	Specifies whether the Analog Gateway routes calls from analog lines before manipulation or after manipulation.

7.11.5 IP -> Tel Routing

Describes the routing rules configured for calls arriving from IP and routed to a Tel (analog) destination.

You can route calls from the Internet Protocol (IP) network to a Foreign Exchange Station (FXS) port or port group on the AG4124/AG4172 Analog Gateway.

The following table lists the IP -> Tel Routing information.

Table 51: IP - Tel Routing

Parameter	Description
Index	Specifies the index for this IP -> Tel routing rule. The range is 0 to 127, and 0 has the highest priority.
Description	Describes this IP -> Tel routing rule so that you can identify it.
Calls from	Specifies whether calls originate from an IP trunk or a Session Initiation Protocol (SIP) server. Specify "any" to match any IP address.
Caller Prefix	Specifies a prefix for the caller number. The prefix has fewer digits than, or as many digits as, the caller number, and it helps match the routing exactly. For example, if the caller number is 2001, the caller prefix can be 200 or 2. Specify "any" to match any caller number.

Parameter	Description
Called Prefix	Specifies a prefix for the called number. The prefix has fewer digits than, or as many digits as, the called number, and it helps match the routing exactly. For example, if the called number is 008675526456659, the called prefix can be 0086755 or 00. Specify "any" to match any called number.
Calls to	Specifies the port or port group to which the Analog Gateway routes the call.

7.11.6 Tel -> IP/Tel Routing

Describes the routing rules configured for calls arriving from a Tel (analog) port and routed to IP or another Tel destination.

You can route calls from the Foreign Exchange Station (FXS) port or port group to an IP trunk, or to ports on a Session Initiation Protocol (SIP) server or another Analog Gateway.

The following table lists the Tel -> IP/Tel Routing information.

Table 52: Tel - IP/Tel Routing

Parameter	Description
Index	Specifies the index for this Tel -> IP/Tel routing rule. The range is 0 to 127, and you cannot reuse an index. An index of 0 has the highest priority.
Description	Describes this Tel -> IP/Tel routing rule so that you can identify it.
Calls From	Specifies whether calls originate from a port or a port group.
Caller Prefix	Specifies a prefix for the caller number. The prefix has fewer digits than, or as many digits as, the caller number, and it helps match the routing exactly. For example, if the caller number is 2001, the caller prefix can be 200 or 2. Specify "any" to match any caller number.
Called Prefix	Specifies a prefix for the called number. The prefix has fewer digits than, or as many digits as, the called number, and it helps match the routing exactly. For example, if the called number is 008675526456659, the called prefix can be 0086755 or 00. Specify "any" to match any called number.

Parameter	Description
Calls to	Specifies whether the Analog Gateway routes the call to a port, a port group, an IP trunk, or a SIP server.

7.12 Manipulation

Explains number manipulation, which changes a called or caller number during call processing whenever that number matches a configured rule.

Number manipulation changes a called or caller number during call processing whenever that number matches a rule you have configured. Use it to add or strip digits so a number matches the format the destination system expects.

Types of Number Manipulation

The Analog Gateway supports three types of number manipulation:

IP -> Tel Called — modifies the called number of an incoming Session Initiation Protocol (SIP) call before the gateway routes the call to the analog port. Use it, for example, to remove a country or area code so the number matches the local extension format.

Tel -> IP/Tel Caller — modifies the caller ID of a call that originates from an analog port. Use it, for example, to convert an extension number into the full number the SIP server requires.

Tel -> IP/Tel Called — modifies the dialed number from an analog device before the gateway sends the call to SIP or to another port. Use it to add a prefix or remove an access code.

For the procedure to create a manipulation rule, see Configure a Number Manipulation Rule on page 100.

7.12.1 Configure a Number Manipulation Rule

Create a number manipulation rule to strip or add digits to a called or caller number during call routing.

1. Navigate to Manipulation and select the required manipulation type.
2. Click Add to create a new rule.
3. Configure matching conditions such as caller prefix or called prefix.
4. Configure the digit manipulation parameters, such as stripping digits or adding a prefix.
5. Save the configuration.
6. Verify the call routing behavior.

Note:

- Incorrect digit manipulation may cause call routing failures.
- Ensure that the numbering format matches the Session Initiation Protocol (SIP) server requirements.
- Test both incoming and outgoing call scenarios after configuration.

7.12.2 IP -> Tel Called

Describes the number manipulation rules applied to the called number for IP-to-Tel calls.

You can set rules for manipulating the called number of IP -> Tel calls.

Table 53: IP - Tel Called

Parameter	Description
Index	Specifies the index for this manipulation rule. The range is 0 to 127, and you cannot reuse an index. An index of 0 has the highest priority.
Description	Describes this manipulation rule so that you can identify it.
Calls From	Specifies whether calls originate from an IP trunk or a Session Initiation Protocol (SIP) server.
Caller Prefix	Specifies a prefix for the caller number. The prefix has fewer digits than, or as many digits as, the caller number, and it helps match the caller number for this call. For example, if the caller number is 2001, the caller prefix can be 200 or 2. Specify "any" to match any caller number.
Called Prefix	Specifies a prefix for the called number. The prefix has fewer digits than, or as many digits as, the called number, and it helps match the called number. For example, if the called number is 008675526456659, the called prefix can be 0086755 or 00. Specify "any" to match any called number.
Calls to	Specifies whether the Analog Gateway routes the call to a port or a port group.
Stripped Digits from Left	Specifies the number of digits to remove from the left of the called number.
Stripped Digits from Right	Specifies the number of digits to remove from the right of the called number.
Prefix to Add	Specifies the prefix to add to the called number after the gateway removes digits.

Parameter	Description
Suffix to Add	Specifies the suffix to add to the called number after the gateway removes digits.
Number of Digits to Leave from Right	Specifies how many digits at the right (end) of the dialed number the system retains during number manipulation. Routing rules use this setting to trim leading digits while preserving the required portion of the number.

7.12.3 Tel - IP/Tel Caller

Explains how to manipulate the caller number of Tel-to-IP/Tel calls.

You can configure rules that manipulate the caller number of Tel -> IP/Tel calls. For the configuration table, see Table 53: IP - Tel Called on page 101.

7.12.4 Tel - IP/Tel Called

Explains how to manipulate the called number of Tel-to-IP/Tel calls.

You can configure rules that manipulate the called number of Tel -> IP/Tel calls. For the configuration table, see Table 53: IP - Tel Called on page 101.

7.13 Management

7.13.1 TR069

Describes the TR-069 remote management parameters configured on the Management > TR069 page.

Note: For security reasons, ensure that TR069 is disabled by default. Enable TR069 only for diagnostic purposes, and disable it again after you complete the diagnostic process.

TR069, short for Technical Report 069 (CPE WAN Management Protocol), provides a commonly used framework and protocol for next-generation network devices.

Under the TR069 network management model, the Auto Configuration Server (ACS) works as a management server responsible for managing Customer Premises Equipment (CPE).

The administrator or Technical Support provides the ACS URL, which usually starts with http:// or https://.

The device uses a user name and password for ACS authentication.

The AG4124/AG4172 uses the ACS user name and password to authenticate with the ACS.

You set the Connect Request user name and password on the AG4124/AG4172 Web Management System.

Table 54: Description of TR069 Parameters

Parameter	Description
TR069	Enables or disables TR069. Disabled is the default.
ACS URL	Specifies the Internet Protocol (IP) address or domain name of the ACS, provided by the service provider.
Username(ACS)	Specifies the user name for the ACS, provided by the service provider.
Password(ACS)	Specifies the password for the ACS, provided by the service provider.
Periodic Inform	Enables or disables Periodic Inform. When enabled, the ACS connects to the CPE at the interval specified in Periodic Inform Interval, for example every 30 seconds.
Periodic Inform Interval	Specifies the interval for periodic connections between the ACS and the CPE.
Username (CPE)	Specifies the user name for the CPE.
Password (CPE)	Specifies the password for the CPE.
Port	Specifies the port used to connect the CPE and the ACS.

7.13.2 SNMP

Describes the Simple Network Management Protocol (SNMP) agent parameters configured on the Management > SNMP page.

SNMP is an Internet-standard protocol for collecting and organizing information about managed devices on Internet Protocol (IP) networks and for modifying that information to change device behavior. Devices that typically support SNMP include routers, switches, servers, workstations, printers, and modem racks.

Network administrators widely use SNMP for network monitoring. SNMP exposes management data in the form of variables on the managed systems, organized in a management information base (MIB) that describes the system status and configuration. Managing applications can then query these variables remotely, and in some cases, modify them.

SNMP has three significant versions. SNMPv1 is the original version of the protocol. The more recent versions, SNMPv2c and SNMPv3, offer improvements in performance, flexibility, and security.

Note: **Security warning:** Mitel does not recommend using SNMPv1 or SNMPv2c because of their poor security controls.

Table 55: SNMP Parameters

Parameter	Description
SNMP	The AG4124/AG4172 Analog Gateway supports three versions of SNMP: V1, V2C, and V3.
Community Configuration	Community configuration exists in V1 and V2C. • Community: type a community name used to read through the SNMP protocol. This value is a character string. • Source: the IP address of the SNMP server. The SNMP server cannot identify packets sent from the AG4124/AG4172 Analog Gateway unless the community configured on the AG4124/AG4172 Analog Gateway matches the community configured on the SNMP server.
Group Configuration	Group configuration exists in V1, V2C, and V3. • Group: type a group name that identifies the group. This value is a character string. • Community: type the name of a community to associate it with this group. You configure read, write, and notify access permissions separately for each group.
View Configuration	View configuration exists in V1, V2C, and V3. • ViewName: type a view name that identifies this view. • ViewType: select Included or Excluded. Included means the view includes the Object Identifier (OID) of the corresponding ViewSubtree. Excluded means the view excludes the OID of the corresponding ViewSubtree. • ViewSubtree: type the OID of the view subtree. • ViewMask: excludes a row of a table, such as an Ethernet port.
Access Configuration	Access configuration applies to V1, V2C, and V3. It sets read, write, or notify permission for a community group. • Group: select a previously configured group name.

Parameter	Description
	• Read: select a read view for the group. • Write: select a write view for the group. • Notify: select a notify view for the group.
Trap Configuration	Trap configuration applies to V1, V2C, and V3. It sends trap alarms. • Trap Type: select V1, V2C, or Inform. • Trap IP: specifies the IP address of the destination SNMP server that receives the trap alarm. • Trap Port: specifies the port of the destination SNMP server that receives the trap alarms. • Trap Community: specifies the community configured on the destination SNMP server.
User Configuration	User configuration applies to V3 only. You must configure this parameter when V3 transmits encrypted SNMP packets. • User: type the user name used for authentication. • AuthType: select Message Digest algorithm 5 (MD5) or SHA as the authentication type. • AuthPassword: specifies the password used for authentication. • Privacy Type: select DES, Advanced Encryption Standard (AES), or AES 128 as the encryption type. • Privacy Password: specifies the encryption password.

7.13.3 Syslog

Describes the syslog parameters configured on the Management > Syslog page.

Syslog is a standard message logging mechanism that separates log generation, storage, and analysis. It configures the gateway to send log messages to an external syslog server for monitoring, troubleshooting, and security auditing.

The Analog Gateway generates standard syslog messages that any server supporting standard syslog protocols can receive and process.

Note:

The Analog Gateway does not include an internal syslog server or local log storage capability. You must deploy an external syslog server separately to collect, store, and analyze the syslog messages that the gateway generates. The external syslog server must support standard syslog protocols and must be reachable from the Analog Gateway network.

Examples of commonly used third-party syslog servers include:

- rsyslog
- syslog-ng
- Kiwi Syslog Server
- Graylog
- Splunk Syslog Collector

Syslog severity levels include: EMERG, ALERT, CRIT, ERROR, WARNING, NOTICE, INFO, and DEBUG.

When the AG4124/AG4172 Analog Gateway registers with a cloud server, local syslog configuration becomes unavailable, and the cloud environment handles the logs. If you require a local syslog server, ensure that you enable Local Syslog when the device operates in non-cloud mode.

The gateway does not support storing syslog files locally, and cloud storage behavior for syslog data is not explicitly documented.

The following table lists the syslog parameters.

Table 56: Syslog

Parameter	Description
Local Syslog	Enables or disables sending log messages to an external syslog server. When enabled, logs are transmitted for monitoring and troubleshooting.
Server Address	Specifies the IP address or domain name of the external syslog server that receives log messages.
Server Port	Defines the port used for syslog communication. Default is 514.
Syslog Level	Specifies the severity level of the logs that the gateway sends. Supported levels include EMERG, ALERT, CRIT, ERROR, WARNING, NOTICE, INFO, and DEBUG.

Parameter	Description
CDR	Enables logging of Call Detail Records (CDR) for tracking call activity.
Signal Log	Enables logging of signaling messages such as Session Initiation Protocol (SIP) transactions for troubleshooting call setup issues.
Media Log	Enables logging of media-related events such as Real-time Transport Protocol (RTP) streams to help diagnose audio issues.
System Log	Enables logging of system-level events such as startup, errors, and internal operations.
Management Log	Enables logging of management actions such as configuration changes and administrative access.

7.13.4 User Management

Describes the administrator and user account parameters configured on the Management > User Manage page.

On the **Management > User Manage** page, you can classify users of the AG4124/AG4172 Analog Gateway into different groups and set a login user name and password for each user.

Note: Mitel recommends that you use the User Manage form to create accounts for all authorized users.

The access that a user receives depends on the selected group type. For example, if you select **Admin** as the **Group** when you create a new user, the user has full read/write access. The following table lists the role-based access for the AG4124/AG4172 Analog Gateway Web Management System.

Table 57: Role-Based Access

Analog Gateway web page	Admin access	Guest access
Management	Read/Write	Read
Security	Read/Write	Read

Analog Gateway web page	Admin access	Guest access
Tools	Read/Write	No Access
Other Pages	Read/Write	Read

7.13.5 RADIUS Parameter

Describes the Remote Authentication Dial-In User Service (RADIUS) authentication parameters configured on the Management > RADIUS Parameter page.

Configures RADIUS authentication for device access. When you enable this feature, the gateway uses a remote RADIUS server to validate user credentials, with optional fallback behavior if the server is unreachable.

The following table lists the RADIUS parameters.

Table 58: RADIUS Parameter

Parameter	Description
Radius	Enables or disables RADIUS authentication for the device.
Local Port	Specifies the local User Datagram Protocol (UDP) port that the gateway uses for RADIUS communication.
Device Behavior Upon RADIUS Timeout	Defines the action taken when the RADIUS server does not respond. For example, verify access locally.
Server IP	Specifies the IP address of the RADIUS server used for authentication.
Server Auth Port	Defines the port used by the RADIUS server for authentication requests. Default is 1645.
Server Key	Specifies the shared secret key used between the gateway and the RADIUS server for secure authentication.

7.13.6 Action URL

Describes the Action URL fields on the Management > Action URL page, which reports Analog Gateway status events to a VoIP platform or server over the Hypertext Transfer Protocol (HTTP).

Action URL lets a VoIP platform or VoIP server learn about the status of the AG4124/AG4172 Analog Gateway. The gateway sends this information through a GET request over HTTP. The GET request can also carry data, such as the Analog Gateway ID, Media Access Control (MAC) address, called or caller number, and Internet Protocol (IP) address, to the VoIP platform or VoIP server.

For information about the data that the GET request can carry, see the notes on the **Management > Action URL** page.

- **Event:** status of the AG4124/AG4172 Analog Gateway that the gateway reports to the VoIP platform or VoIP server.
- **Action URI:** for example, http://host:port/file.php?macaddr=$mac, where host is the IP address or domain name of the HTTP server, port is the listening port of the HTTP server, file.php is the script that processes the request, and $mac is the parameter that the request carries when the gateway sends it.
- **Heartbeat:** heartbeat packets that the AG4124/AG4172 Analog Gateway sends to the URL to check the connection between the AG4124/AG4172 Analog Gateway and the HTTP server.

> **Note**: Mitel recommends that only an administrator use the Action URL feature. Leave the **Startup** field blank if you do not use the Action URL feature.

Table 59: Action URL Event Fields

Event	Description
Startup	Sends the Action URI when the Analog Gateway starts up. Leave this field blank if you do not use the Action URL feature.
Offhook	Sends the Action URI when an analog device goes off-hook.
Onhook	Sends the Action URI when an analog device goes on-hook.
Incoming Call	Sends the Action URI when an incoming call is received.
Outgoing Call	Sends the Action URI when an outgoing call is placed.
Call Build	Sends the Action URI when a call is successfully established.
Call Terminate	Sends the Action URI when a call ends.

Event	Description
Register Status	Sends the Action URI when the SIP registration status of a port changes.
Heartbeat	Sends the Action URI as a periodic heartbeat packet, used to check connectivity between the Analog Gateway and the HTTP server.
Heartbeat Interval	Sets the interval, in seconds, between heartbeat packets. The default value is 10 seconds.

7.13.7 SIP PNP

Describes the Session Initiation Protocol (SIP) Plug and Play (PNP) parameters that you configure on the Management > SIP PNP page.

Configures SIP PNP functionality, which allows the gateway to automatically discover and connect to a provisioning or SIP server. This functionality simplifies deployment by enabling automatic configuration updates from the server.

The following table lists the SIP PNP parameters.

Table 60: SIP PNP

Parameter	Description
PNP Enable	Enables or disables SIP PNP functionality for automatic server discovery and configuration.
Server Address	Specifies the Internet Protocol (IP) address that the gateway uses for SIP PNP discovery or provisioning server communication.
Server Port	Defines the port used for SIP PNP communication. Default is 5060.
Update Interval	Specifies the interval in seconds at which the gateway sends update or discovery messages to the server.

7.14 Security

7.14.1 ACL Configuration for Analog Gateway

Introduces the Web ACL and Telnet ACL, which the Analog Gateway uses to regulate management access from network devices.

The Analog Gateway uses Access Control Lists (ACLs) to regulate access from management systems and network devices. When you enable ACL on the Analog Gateway, configure the following to ensure reliable management access:

- **Web ACL**: when you enable Web ACL, add all management IP addresses, such as ESM, switches, and provisioning systems, to ensure proper access to the gateway's web interface.
- **Telnet ACL**: when you enable Telnet ACL, add the same management IP addresses that you configured in the Web ACL to maintain reliable communication with the gateway.

For the step-by-step procedure to configure the Web ACL, see Configure the Web ACL on page 111. For the step-by-step procedure to configure the Telnet ACL, see Configure the Telnet ACL on page 112.

7.14.1.1 Configure the Web ACL

Configure the Web Access Control List (ACL) to restrict HTTPS/HTTP management access to the Analog Gateway to a defined list of source IP addresses.

The Web ACL governs access to the HTTPS/HTTP management interface of the AG4124/AG4172 Analog Gateway by defining the permitted source IP addresses. You cannot enable the ACL when the IP address list is empty.

Warning: Enabling ACL without adding the required management IP addresses may block access to the gateway. Ensure that your current management system IP address is included in the ACL before you enable it. If you lose access due to incorrect ACL configuration, you might need to perform a factory reset to recover.

Note:

- Mitel strongly recommends using the ACL to restrict access to authorized users.
- Review the ACL regularly to ensure that all IP addresses are valid.

1. Enable **ACL for Web**.
2. Add the IP addresses of the following systems:
   - ESM Server. Connects to the Analog Gateway for management and configuration operations.
   - Switches. Communicates with the Analog Gateway.
   - Any other management, provisioning, or monitoring systems that require access.

   Note:

   If you do not add the required IP addresses to the Web ACL, the gateway might not respond to login attempts. Errors such as *"Unable to log in to the gateway"*, *TLS read failure*, or *"Did not get login page"* may appear in logs or the ESM interface.

7.14.1.2 Configure the Telnet ACL

Configure the Telnet Access Control List (ACL) to restrict Telnet management access to the Analog Gateway to a defined list of source IP addresses.

The Telnet ACL defines the IP addresses permitted to access the Telnet interface of the AG4124/AG4172 Analog Gateway, and you cannot enable it with an empty IP list. Even when Telnet access is disabled, the Telnet ACL may still affect backend communication used by management tools.

Note:

- Mitel strongly recommends using the ACL to restrict access to authorized users only.
- Allow Telnet access only temporarily, on an as-needed basis, and remove the user's IP address from the ACL after the support or maintenance task is complete.

1. Either enable or disable the Telnet ACL based on the following scenarios:
   a. If Telnet ACL is enabled, add the same IP addresses used in the Web ACL to the Telnet ACL.
   b. If Telnet ACL is disabled, Telnet access is blocked. However, some firmware versions may still require you to configure the IP addresses in both ACLs for successful ESM login.

7.14.2 Passwords

Describes the fields on the Security > Passwords page used to change the Web and Telnet login credentials of the AG4124/AG4172 Analog Gateway.

On this page, you can configure or change the user name and password that you use to log in to the Web Management System and the Telnet interface of the AG4124/AG4172 Analog Gateway.

Note:

- The Web Management System and Telnet user name and password are both admin by default. Mitel recommends that you change them after you first log in, for security reasons.
- Supported characters for password: **· ~ ! @ # ¥ ^ & * ( ) _ + [ ] \ { } | ; ' : " , . ? / - = %**

Table 61: Password Modification Fields

Field	Description
Old Web Username	The current Web Management System username. Default is admin.
Old Web Password	The current Web Management System password.
New Web Username	The new username for the Web Management System.
New Web Password	The new password for the Web Management System.

Field	Description
Confirm Web Password	Re-enter the new Web Management System password to confirm it.
Old Telnet Username	The current Telnet username. Default is admin.
Old Telnet Password	The current Telnet password.
New Telnet Username	The new username for the Telnet interface.
New Telnet Password	The new password for the Telnet interface.
Confirm Telnet Password	Re-enter the new Telnet password to confirm it.

7.14.3 Encrypt

Describes the SIP Encrypt and RTP Encrypt fields on the Security > Encrypt page, used when registering the Analog Gateway to a VOS softswitch.

On this page, you can encrypt Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP) traffic when the AG4124/AG4172 Analog Gateway registers to a VOS softswitch.

Note:

- Mitel does not support VOS. Therefore, ensure that the **SIP Encrypt** and **RTP Encrypt** fields are set to **Disable**.
- You must change the **SIP Encrypt** field to **Enable** only if you want to upload the SIP certificate for Transport Layer Security (TLS) in the **Certificate Manage** page.

7.14.4 Certificate Management

Introduces the Certificate Manage page, where you add, view, and delete SIP Client, SIP CA, and Web Server certificates for the AG4124/AG4172.

On this page, you can add, view, and delete the Session Initiation Protocol (SIP) client certificate or the SIP Certificate Authority (CA) certificate. You can also view, change, and delete the web HTTPS certificate for the AG4124/AG4172.

Note:

- You are not required to upload a SIP CA certificate. However, Mitel recommends it for security reasons. This service has an additional cost.
- Ensure that you have downloaded the SIP CA certificate for the respective Private Branch Exchange (PBX) to your Personal Computer (PC) or laptop. For information about installing a certificate for MiVoice Business, see the *Installing the MiVoice Business Self-Signed Security or Enterprise PKI Certificate* section in the *MiVoice Business System Administration Tool Help* located in MiVoice Business.

7.14.4.1 Add a SIP CA Certificate

Upload a Session Initiation Protocol (SIP) Certificate Authority (CA) certificate to the AG4124/AG4172 Analog Gateway.

To add a SIP CA certificate:

1. In the Web Management System page, navigate to **Security** > **Certificate Manage**.
2. In the page that opens, under **Certificate Upload**, do the following:
   a. In the **File Type** field, select **SIP CA Certificate**.
   b. In the **SIP CA Certificate** field, select **Choose File**.
   c. Select the SIP CA certificate from the local folder.
   d. Click **Upload** to upload the SIP CA certificate.

Note: The file that you upload must be in CA certificate format.

7.14.4.2 Add a SIP Client Certificate

Upload a Session Initiation Protocol (SIP) client certificate and private key to the AG4124/AG4172 Analog Gateway.

To add a SIP client certificate:

1. In the Web Management System page, navigate to **Security** > **Certificate Manage**.
2. In the page that opens, under **Certificate Upload**, do the following:
   a. In the **File Type** field, select **SIP Client Certificate**.
   b. In the **SIP Client Certificate** field, select **Choose File**.
   c. Select the SIP client certificate from the local folder.
   d. In the **SIP Client Private Key** field, select **Choose File**.
   e. Select the private key from the local folder.
   f. Click **Upload** to upload the SIP client certificate and private key.

Note: The file that you upload must be in Certificate Authority (CA) certificate format.

7.14.4.3 Add a Web HTTPS Certificate

Upload a web Hypertext Transfer Protocol Secure (HTTPS) certificate and private key to the AG4124/AG4172 Analog Gateway.

To add a web HTTPS certificate:

1. In the Web Management System page, navigate to **Security** > **Certificate Manage**.
2. In the page that opens, under **Certificate Upload**, do the following:
   a. In the **File Type** field, select **WEB Https Certificate**.
   b. In the **WEB Https Certificate** field, select **Choose File**.
   c. Select the web HTTPS certificate from the local folder.
   d. In the **WEB Https Private Key** field, select **Choose File**.
   e. Select the private key from the local folder.
   f. Click **Upload** to upload the web HTTPS certificate and private key.

Note: The file that you upload must be in Certificate Authority (CA) certificate format.

7.14.4.4 View the SIP Client Certificate

View the details of a Session Initiation Protocol (SIP) client certificate added to the AG4124/AG4172 Analog Gateway.

To view the details of the SIP client certificate that you added:

1. In the Web Management System page, navigate to **Security** > **Certificate Manage**.
2. In the page that opens, under **SIP Client Certificate**, view the following details about the added SIP client certificate:
   - **Awarded**
   - **Issuer**
   - **Start Time**
   - **End Time**

7.14.4.5 View the SIP CA Certificate

View the details of a Session Initiation Protocol (SIP) Certificate Authority (CA) certificate added to the AG4124/AG4172 Analog Gateway.

To view the details of the SIP CA certificate that you added:

1. In the Web Management System page, navigate to **Security** > **Certificate Manage**.
2. In the page that opens, under **SIP CA Certificate**, view the following details about the added SIP CA certificate:
   - **Awarded**
   - **Issuer**
   - **Start Time**
   - **End Time**

Note: The SIP Certificate section displays a maximum of five SIP CA certificates that you added.

7.14.4.6 View the Web HTTPS Certificate

View the details of the web Hypertext Transfer Protocol Secure (HTTPS) certificate installed on the AG4124/AG4172 Analog Gateway.

To view the web HTTPS certificate:

1. In the Web Management System page, navigate to **Security** > **Certificate Manage**.
2. In the page that opens, under **WEB Https Certificate**, view the following details about the installed web HTTPS certificate:
   - **Awarded**
   - **Issuer**
   - **Start Time**
   - **End Time**

Note: The Dinstar self-signed certificate is the default web certificate. You can upload an authenticated certificate to replace it.

7.14.4.7 Delete the SIP Client Certificate

Delete a Session Initiation Protocol (SIP) client certificate added to the AG4124/AG4172 Analog Gateway.

To delete the SIP client certificates that you added:

1. In the Web Management System page, navigate to **Security** > **Certificate Manage**.
2. In the page that opens, under **SIP Client Certificate**, click **Delete** to delete the SIP client certificate.
3. In the **Are you sure to the delete the certificate group?** pop-up message that appears, click **OK** to delete the SIP client certificate.

7.14.4.8 Delete the SIP CA Certificate

Delete a Session Initiation Protocol (SIP) Certificate Authority (CA) certificate added to the AG4124/AG4172 Analog Gateway.

To delete the SIP CA certificates that you added:

1. In the Web Management System page, navigate to **Security** > **Certificate Manage**.
2. In the page that opens, under **SIP CA Certificate**, select the SIP CA certificate that you want to delete.
3. Click **Delete**.
4. In the **Are you sure to the delete the certificate group?** pop-up message that appears, click **OK** to delete the SIP CA certificate.

7.14.4.9 Delete the Web HTTPS Certificate

Delete the web Hypertext Transfer Protocol Secure (HTTPS) certificate installed on the AG4124/AG4172 Analog Gateway.

To delete the web HTTPS certificates that you added:

1. In the Web Management System page, navigate to **Security** > **Certificate Manage**.
2. In the page that opens, under **WEB Https Certificate**, click **Delete** to delete the web HTTPS certificate.
3. In the **Are you sure to the delete the certificate group?** pop-up message that appears, click **OK** to delete the web HTTPS certificate.

7.14.4.10 Enable SIP Encryption

Enable Session Initiation Protocol (SIP) encryption on the AG4124/AG4172 Analog Gateway.

To enable SIP encryption:

1. In the Web Management System page, navigate to **Security** > **Encrypt**.
2. In the page that opens, in the **SIP Encrypt** field, select **Enable** from the list of options to enable SIP encryption.

7.15 Tools

7.15.1 Firmware Upload

Upload firmware and image files to the AG4124/AG4172 Analog Gateway.

Use the Firmware Upload page to upgrade the firmware and image files on the AG4124 and AG4172 Analog Gateways. The upgrade procedure to follow depends on the software version currently installed on the device: some older versions cannot be upgraded directly to newer releases and require intermediate upgrade steps. For a worked example, see Sample Firmware Upload Procedure on page 119.

The following table describes the Firmware Upload fields.

Table 62: Firmware Upload

Parameter	Description
File Type	Select the type of file to upload to the Analog Gateway. The option you select determines which component or function on the Analog Gateway is updated.
Package	Uploads a firmware package (.tar.gz) containing software updates for the Analog Gateway. Package files are commonly used during firmware upgrades and may require a device reboot to complete the update. **Note**: This parameter is displayed when **File Type** is set to **Package**.
Media	Uploads media-related files used by the Analog Gateway. The exact contents and use of this file

Parameter	Description
	type are deployment-dependent, so verify them before use. **Note**: This parameter is displayed when **File Type** is set to **Media**.
DSP Firmware	Uploads firmware for the Digital Signal Processor (DSP), which handles voice and media processing. Some firmware upgrades require a DSP firmware update to maintain compatibility. **Note**: This parameter is displayed when **File Type** is set to **DSP Firmware**.
Tr069 Https Certificate	Uploads a Hypertext Transfer Protocol Secure (HTTPS) certificate used to secure Technical Report 069 (CPE WAN Management Protocol) (TR-069) communication between the Analog Gateway and the Auto Configuration Server (ACS). **Note**: This parameter is displayed when **File Type** is set to **Tr069 Https Certificate**.
Provision Https Certificate	Uploads an HTTPS certificate used to establish secure connections to the provisioning server. **Note**: This parameter is displayed when **File Type** is set to **Provision Https Certificate**.
Kernel	Uploads the operating system kernel image used during device startup and runtime operation. **Note**: This parameter is displayed when **File Type** is set to **Kernel**.
Uboot	Uploads the U-Boot bootloader image used during the device boot process. **Note**: This parameter is displayed when **File Type** is set to **Uboot**.
RootFS	Uploads the root file system image, containing the operating system files, applications, and runtime components required by the Analog Gateway.

Parameter	Description
	Note: This parameter is displayed when **File Type** is set to **RootFS**.
Image	Uploads a complete device image (.bin.ldf) used to update the Analog Gateway software. Depending on the currently installed software version, an intermediate firmware upgrade may be required before you can upload an image file. **Note**: This parameter is displayed when **File Type** is set to **Image**.

7.15.1.1 Sample Firmware Upload Procedure

Purpose and prerequisites for upgrading AG4124 and AG4172 Analog Gateway firmware, image, and DTU firmware.

Purpose

This appendix describes the recommended procedure for upgrading AG4124 and AG4172 Analog Gateway firmware, image, and DTU firmware. Follow the upgrade path that matches the currently installed software version to ensure a successful upgrade.

Prerequisites

Warning:

Some AG41xx software versions cannot be upgraded directly to the target release. Installing firmware packages or image files in an incorrect order may result in upgrade failure or loss of Web Management System access requiring device recovery through Trivial File Transfer Protocol (TFTP).

Before upgrading the Analog Gateway, ensure the following:

- Download the required firmware package, image file, Data Terminal Unit (DTU) firmware (if applicable), and the release notes from the Mitel Software Download Center (SWDL/MOL).
- Verify the currently installed software version on **Status & Statistics > System Information**.
- Determine the required upgrade path using the release notes for the target software version.
- Back up the current device configuration.
- Ensure uninterrupted power during the upgrade.
- Do not close the browser or restart the device while an upload is in progress.

> **Important**:
>
> Follow the upgrade path that matches the current software version installed on the Analog Gateway. Some software versions require one or more intermediate firmware package upgrades before an image file can be uploaded. AG4172 upgrades may also require a DTU firmware update. Refer to the release notes for the target software version.

7.15.1.1.1 Upgrade Path Selection

Supported upgrade paths for the AG4124/AG4172 Analog Gateway, by currently installed software version.

Select the upgrade path that matches the current software version installed on the Analog Gateway.

> **Important**:
>
> Some software versions require one or more intermediate firmware package upgrades before an image file can be uploaded. AG4172 upgrades may also require a Data Terminal Unit (DTU) firmware update. Follow the upgrade path exactly as shown in the following table.

Table 63: Supported Upgrade Paths

Current version	Required upgrade path	Notes
AG4124 33.83.11.xx	1. Upload firmware package **33.83.11.29.tar.gz**. See Upload Firmware Package on page 121. 2. Restart the Analog Gateway. 3. Upload firmware package **33.83.12.08.tar.gz**. See Upload Firmware Package on page 121. 4. Restart the Analog Gateway. 5. Upload image file **Mitel-1215-image.bin.ldf**. See Upload Image File on page 122. 6. Upload firmware package **33.83.12.15T1.tar.gz**. See Upload Firmware Package on page 121. 7. Restart the Analog Gateway.	• Back up the configuration before upgrading. • DTU firmware upgrade is required.
AG4172 33.83.11.30 33.83.12.01	1. Upload firmware package **33.83.12.08.tar.gz**. See Upload Firmware Package on page 121. 2. Restart the Analog Gateway. 3. Upload image file **Mitel-1215-image.bin.ldf**. See Upload Image File on page 122. 4. Upload firmware package **33.83.12.15T1.tar.gz**. See Upload Firmware Package on page 121. 5. Restart the Analog Gateway.	• Back up the configuration before upgrading. • DTU firmware upgrade is required.

Current version	Required upgrade path	Notes
33.83.12.02 - 33.83.12.03	1. Upload firmware package **33.83.12.08.tar.gz**. See Upload Firmware Package on page 121. 2. Restart the Analog Gateway. 3. Upload image file **Mitel-1215-image.bin.ldf**. See Upload Image File on page 122. 4. Upload firmware package **33.83.12.15T1.tar.gz**. See Upload Firmware Package on page 121. 5. Restart the Analog Gateway.	• Back up the configuration before upgrading. • DTU firmware upgrade is required.
33.83.12.04 - 33.83.12.08	1. Upload image file **Mitel-1215-image.bin.ldf**. See Upload Image File on page 122. 2. Upload firmware package **33.83.12.15T1.tar.gz**. See Upload Firmware Package on page 121. 3. Restart the Analog Gateway.	DTU firmware upgrade is re-quired.
33.83.12.10 - 33.83.12.14	1. Upload image file **Mitel-1215-image.bin.ldf**. See Upload Image File on page 122. 2. Upload firmware package **33.83.12.15T1.tar.gz**. See Upload Firmware Package on page 121. 3. Restart the Analog Gateway.	No additional prerequisites.

7.15.1.1.2 Upload Firmware Package

Upload a firmware package to the AG4124/AG4172 Analog Gateway.

1. Log in to the Analog Gateway Web Management System.
2. Navigate to **Tools > Firmware Upload**.
3. Set **File Type** to **Package**.
4. Click **Choose File** and select the required firmware package (.tar.gz).
5. Click **Upload**.
6. Wait until the upload completes successfully.
7. Navigate to **Tools > Device Restart**.
8. Restart the Analog Gateway.
9. Wait until the Analog Gateway returns to service.
10. Verify that the firmware version has been updated successfully on the **Status & Statistics > System Information** page before proceeding to the next upgrade step.

7.15.1.1.3 Upload Image File

Upload an image file to the AG4124/AG4172 Analog Gateway.

Important:

Upload an image file only after all prerequisite firmware package upgrades defined in the required upgrade path have been completed.

1. Verify that all prerequisite firmware package upgrades have been completed. See Sample Firmware Upload Procedure on page 119.
2. Log in to the Analog Gateway Web Management System.
3. Navigate to **Tools > Firmware Upload**.
4. Set **File Type** to **Image**.
5. Click **Choose File** and select the required image file.
6. Click **Upload**.
7. Wait until the upload completes successfully.
8. If prompted, restart the Analog Gateway.
9. Wait until the Analog Gateway returns to service.
10. Verify that the image upgrade has completed successfully on the **Status & Statistics > System Information** page before proceeding to the next upgrade step.

7.15.1.1.4 Upload DTU Firmware (AG4172 Only)

Upload DTU firmware to the AG4172 Analog Gateway.

Important:

Perform a Data Terminal Unit (DTU) firmware upgrade only when it is required by the applicable upgrade path in the release notes.

1. Log in to the Analog Gateway Web Management System.
2. Navigate to **Tools > Firmware Upload**.
3. Set **File Type** to **DSP Firmware**.
4. Click **Choose File** and select the required DTU firmware file.
5. Click **Upload**.
6. Wait until the upload completes successfully.
7. Navigate to **Tools > Device Restart**.
8. Restart the Analog Gateway.
9. Wait until the Analog Gateway returns to service.
10. Verify that the DTU firmware version has been updated successfully on the **Status & Statistics > System Information** page.

Note:

Failure to install the required DTU firmware may result in hardware compatibility issues after the software upgrade.

7.15.1.1.5 Verify the Firmware Upgrade

Verify that the Analog Gateway firmware upgrade completed successfully.

1. Log in to the Analog Gateway Web Management System.
2. Navigate to **Status & Statistics > System Information**.
3. Verify the following information:
    - Software Version
    - Kernel Version
    - RootFS Version
    - DMS Version
    - DTU Version (AG4172 only, if applicable)
4. Verify that the Analog Gateway has completed startup successfully and is operating normally.
5. Verify that all configured ports and Session Initiation Protocol (SIP) services have registered successfully.
6. Place a test call to verify normal call processing.

7.15.1.1.6 Firmware Upload Troubleshooting

Recommendations for resolving a firmware or image upload that did not complete successfully.

If an upgrade does not complete successfully, refer to the following recommendations before retrying the upgrade:

- If a firmware package or image file upload fails, restart the Analog Gateway before attempting the upload again.
- Do not extract the firmware package (.tar.gz) before uploading it. Upload the package file exactly as downloaded from the Mitel Software Download Center.
- Complete multi-stage upgrades in the order specified by the required upgrade path. Do not skip intermediate firmware package or image upgrades.
- If the Web Management System is inaccessible after an upgrade, recovery through Trivial File Transfer Protocol (TFTP) may be required.
- On AG4124, image uploads may fail because of limited memory resources. If this occurs, restart the Analog Gateway and retry the image upload.
- Before uploading firmware packages, image files, or Data Terminal Unit (DTU) firmware, verify that the selected files match the required upgrade path for the currently installed software version.

7.15.2 Data Backup

Back up configuration data, Analog Gateway status, and summary messages to the local computer.

Use the **Tools** > **Data Backup** page to download and save a copy of the configuration data, Analog Gateway status, and summary messages to your local computer.

Note: The AG4124/AG4172 device backup does not include Session Initiation Protocol (SIP) or web server certificates.

7.15.3 Data Restore

Restore configuration data on the Analog Gateway from a data file uploaded from the local computer.

Use the **Tools** > **Data Restore** page to restore configuration data by uploading a data file from your local computer. The restored configuration takes effect after the Analog Gateway restarts.

Note: The AG4124/AG4172 device backup does not include Session Initiation Protocol (SIP) or web server certificates.

7.15.4 Perform a Ping Test

Use Ping to check whether a network is working normally by sending test packets and measuring response time.

Ping checks whether a network is working normally by sending test packets and measuring response time.

To use Ping:

1. Enter the Internet Protocol (IP) address or domain name of a network, a website, or an Analog Gateway in the Ping input box, and then click **Start**.

   Table 64: Ping Test Fields

Parameter	Description
Destination	The IP address or domain name to ping.
Number of Ping (1-100)	The number of ping requests to send. Range: 1 to 100.
Packet Size (56-1024 bytes)	The size of each ping packet, in bytes. Range: 56 to 1024.

2. Review the ping results.

   Receiving reply messages indicates the network is working normally; if no replies are received, the network is down.

The end-to-end delay for a voice call should not exceed 50 ms.

For details on using Ping to determine whether the Ethernet Local Area Network (LAN) is suitable for transporting voice and fax traffic, see Network Engineering for IP Telephony, in the section "Maintaining Voice Quality of Service."

7.15.5 Perform a Tracert Test

Use Traceroute to track the route from one IP address to another.

Tracert is short for traceroute. It tracks the route from one Internet Protocol (IP) address to another.

To use Traceroute:

1. Enter the IP address or domain name of the destination Analog Gateway, and the maximum number of hops.
2. Click **Start**.
   - **Destination:** the IP address or domain name of the destination Analog Gateway to track.
   - **Max Hops:** the maximum number of hops to search for the specified IP address or domain name. For example, if Max Hops is set to 30 and the configured IP address or domain name cannot be reached within 30 hops, the IP address or domain name is presumed unreachable.
3. View the route information in the returned message.

7.15.6 Perform the Outward Test

Diagnose the physical function of an FXS port using the GR-909 standard outward test.

The outward test lets you diagnose the physical function of a Foreign Exchange Station (FXS) port. It follows the Generic Requirement 909 (Telcordia loop-test standard) (GR-909).

Note: To run the outward test, an analog device must be connected to the port being tested. If the analog device is an analog phone, the phone must be on-hook.

To start the outward test:

1. Select the FXS ports to test.
2. Click **Start**.

   The test may take a few minutes to complete.

Test results:

- **OK**: The tested FXS ports are working correctly.
- **FAIL**: The tested FXS ports are not functioning correctly.

7.15.7 Perform a Network Capture

Capture network traffic on the available network ports of the Analog Gateway for diagnostics.

Network capture is an important diagnostic tool for maintenance. Use it to capture data packets on the available network ports.

Note:

- Mitel recommends that you delete all capture records once system diagnosis or maintenance is complete.
- Captured files download automatically to the default download location configured in the web browser.
- Running simultaneous real-time captures for multiple Analog Gateway devices in the same browser instance may result in incomplete or missing capture files. Mitel recommends that you perform only one real-time capture at a time per browser session.

To perform a network capture:

1. Log in to the Analog Gateway Web Management System.
2. Navigate to **Tools > Network Capture**.
3. Select the capture options described in the following table.

Table 65: Network Capture

Parameter	Description
>Type	Select the capture type to use for troubleshooting and diagnostics. The following capture types are available: • **Network package** - Captures network traffic exchanged between the Analog Gateway and connected devices, such as Session Initiation Protocol (SIP) servers, gateways, and management systems. • **PCM** - Captures Pulse Code Modulation (PCM) audio data from a selected analog port for voice and media troubleshooting. • **Syslog** - Captures syslog messages generated by the Analog Gateway for system and fault analysis. Syslog capture requires Syslog to be enabled on the Analog Gateway. • **DSP** - Captures voice stream data processed by the Digital Signal Processor (DSP) chipset for media and audio troubleshooting. **Note**: This option applies only to the AG4124.
>UserCard	Select the UserCard from which to capture network traffic. Determine the correct UserCard based on the port being investigated. Use **Status & Statistics > Port Status** to identify the affected port, and **Status & Statistics > UserCard Status** to identify the corresponding UserCard. Selecting the correct UserCard ensures that the capture contains traffic associated with the target port. **Note**: This parameter applies only to the AG4172.

Parameter	Description

>Select Type	Select how PCM audio data is captured.
	
	• **According slot** - Captures PCM audio data for the selected UserCard slot.
	  • **Slot** - Select the UserCard slot to capture. On the AG4172, identify the appropriate UserCard using **Status & Statistics > UserCard Status**. If you are troubleshooting a specific analog port, use **Status & Statistics > Port Status** to determine the associated UserCard.
	  • **Port** - Select the analog port associated with the selected UserCard.
	• **According port** - Captures PCM audio data for a specific analog port.
	  • **Port** - Select the analog port to capture. You must select a port before starting a PCM capture.
	
	Note: This parameter applies only to the AG4172.
	
	This field appears when **Type** is set to **PCM**.

>Port	Select the analog port from which to capture PCM audio data. You must select a port before starting a PCM capture. Use this option when troubleshooting audio issues associated with a specific analog device or extension. **Note**: This parameter is displayed only when **Type** is set to **PCM**.
>Real-time Capture	Enable real-time capture and set limits for the generated capture file. Set the following parameters: • **Time Limit (0: No Limit)** - Specifies the maximum capture duration, in minutes. • **Size Limit (0: No Limit)** - Specifies the maximum capture file size, in MB. Setting a value of **0** disables the corresponding limit. **Note**: While Real-time Capture is enabled, the other capture options are unavailable until the capture operation completes.

4. Click **Start**.

   The recording starts, and the capture file (log file) download begins.
5. Reproduce the issue or activity that you want to capture.

6. Click **Stop**.

   The recording ends, and the file downloads to your default download location. Captured files are saved in Packet Capture (PCAP) format and can be analyzed using packet analysis tools such as Wireshark.

7.15.8 Analog Gateway Restart

Restart the Analog Gateway to apply configuration changes.

Some parameter changes do not take effect immediately. If you change a setting that requires it, restart the Analog Gateway so the new configuration is applied.

Configurations With PBX 8

This chapter contains the following section(s):

- Configuring Analog Gateway With MiVoice Business
- Configuring Analog Gateway With MiVoice MX-ONE
- Configuring Analog Gateway With MiVoice 5000
- Configuring OpenScape Business for Use With the Mitel AG4124/AG4172 Analog Gateway
- Configuring OpenScape 4000 for Use With the Mitel AG4104/AG4108 Gateway

PBX integration guides for the Mitel AG4124/AG4172 Gateway.

8.1 Configuring Analog Gateway With MiVoice Business

Configuring MiVoice Business for Use With Mitel AG4124/AG4172 Gateway (Single Line). Entry point for the topics covering MiVoice Business integration with the Mitel AG4124/AG4172 Gateway.

8.1.1 Overview

Reference for configuring MiVoice Business to host the Mitel AG4124/AG4172 Gateway.

This section gives Mitel Authorized Solutions Providers a reference for configuring MiVoice Business Release 10.2 (and later) to host the Mitel AG4124/AG4172 Gateway. You can configure the devices in a range of arrangements, depending on your VoIP solution. The AG4124/AG4172 Gateway devices use single line user licenses on MiVoice Business. This section covers a basic Mitel AG4124/AG4172 Gateway setup as a SIP endpoint with the required setup options.

8.1.1.1 Supported Software Versions

Software versions of MiVoice Business and the Mitel AG4124/AG4172 Gateway that support basic SIP calls.

The following table shows the product software versions that support basic SIP calls between the Mitel AG4124/AG4172 Gateway and MiVoice Business.

Product	Version
MiVoice Business	All versions
AG4124	v33.83.11.29 or above
AG4172	v33.83.12.08 or above

8.1.1.2 Supported Features

Features supported when the Mitel AG4124/AG4172 Gateway is connected to MiVoice Business.

The following table lists the features supported when the Mitel AG4124/AG4172 Gateway is connected to MiVoice Business.

Feature	Feature description
Basic Call	Making and receiving calls
Registration/Authentication	Device registration and authentication
DTMF Signal	Sending Dual-Tone Multi-Frequency (DTMF) signals after call setup (for example, a mailbox password)
Call Hold	Placing a call on hold
Call Transfer	Transferring a call
Call Forward	Forwarding a call
Conference	Conferencing multiple calls together
Redial	Last Number Redial
Personal Ring Group	Multiple sets ring when one number is dialed
MWI	Message Waiting Indicator (MWI)
FAC	Testing call park/retrieve, Do Not Disturb (DND), and similar features by using a Feature Access Code (FAC)
Long Duration Calls	Basic incoming and outgoing long-duration calls

8.1.1.3 Device Limitations

Features not supported when the Mitel AG4124/AG4172 Gateway is connected to MiVoice Business.

The following table lists the features that are not supported when the Mitel AG4124/AG4172 Gateway is connected to MiVoice Business.

Feature	Problem description
Video Calls	The Mitel AG4124/AG4172 Gateway does not support video calling.
G.722 Codec	The Mitel AG4124/AG4172 Gateway does not support calls using the G.722 codec.

8.1.1.4 Network Topology

Deployment topology for the Mitel AG4124/AG4172 Gateway with MiVoice Business, on premise or at a remote site.

The AG4124/AG4172 Analog Gateway provides connectivity and protocol conversion between SIP devices on the customer's Local Area Network (LAN) and the analog phones and fax machines connected to the AG4124/AG4172.

The AG4124/AG4172 can be deployed on premise at the main site, or off premise at a branch office or remote site.

- When deployed on premise at the main site, the AG4124/AG4172 connects the analog phones to the customer's LAN. The MiVoice Business SIP Call Server and the SIP phones also connect to the customer's LAN.
- When deployed off premise at a remote site, the AG4124/AG4172 connects the analog phones to the remote site's LAN. The remote site connects to the main site over the Internet, letting the phones connect to the MiVoice Border Gateway (MBG) and register with MiVoice Business as teleworker phones.

Note: To keep the deployment secure:

- The AG4124/AG4172 must never connect directly to the Internet; it must connect to the Internet through a firewall.
- The MiVoice Border Gateway must never connect directly to the Internet; it must connect to the Internet through a firewall.

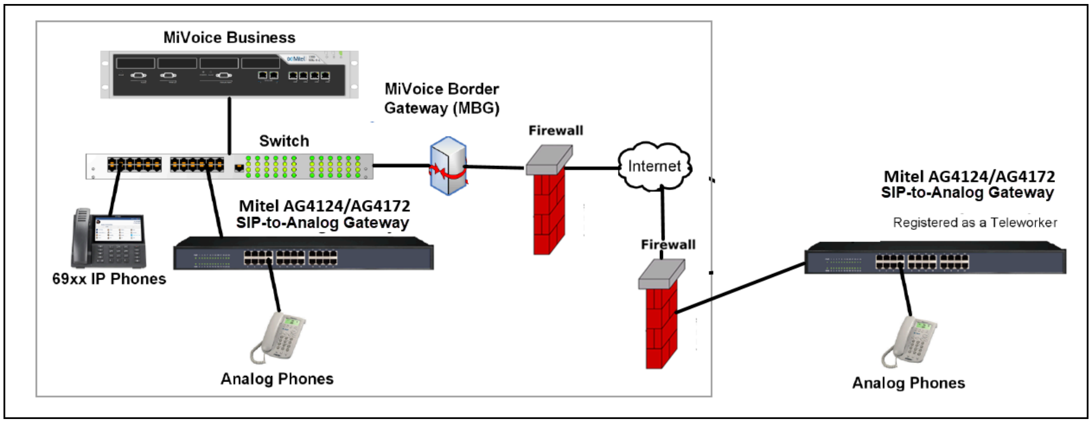

Figure 7: Network Topology

8.1.2 MiVoice Business Configuration Notes

Steps for programming a MiVoice Business to connect with the Mitel AG4124/AG4172 Gateway.

The following topics describe the steps for programming a MiVoice Business system to connect with the Mitel AG4124/AG4172 Gateway.

8.1.2.1 Assumptions for the MiVoice Business Programming

Bandwidth prerequisite for connecting the Mitel AG4124/AG4172 Gateway to MiVoice Business.

Sufficient bandwidth must be available to support Voice over IP. For more information, see Bandwidth considerations (voice and signaling encryption).

8.1.2.2 Verify SIP Software Licensing

Verify that MiVoice Business has adequate Single Line Users licenses for connecting SIP endpoints.

Verify that MiVoice Business has adequate **Single Line Users** licenses for connecting SIP endpoints.

1. Log in to the MiVoice Business System Administrator Tool.
2. Navigate to the **Licenses** > **License and Option Selection** form.
3. Verify that MiVoice Business has adequate single-line licenses for connecting IP devices.

8.1.2.3 Configure the Single-Line IP Set

Program a Generic SIP Device on MiVoice Business as a single-line SIP phone for the Mitel AG4124/AG4172 Gateway.

On MiVoice Business, a Generic SIP Device is programmed as a Generic SIP Phone in the **User and Services Configuration** form for each analog phone.

To program the SIP device as a Generic SIP Phone, do the following:

1. Log in to the MiVoice Business System Administrator Tool.
2. Go to **Users and Devices** and select the **User and Services Configuration** form.

3. On the page that opens, click **Add**.
4. Select **Default User and Device**.
5. On the page that opens, click the **Service Profile** tab.
6. In the **Number** field, enter the directory number. For example, 2222.
7. In the **Device Type** field, select **Generic SIP Phone** from the list of options.
8. Select the **Single Line Phone** option.
9. Click the **Access and Authentication** tab.
10. On the page that opens, enter the SIP password in the **SIP Password** field, and reenter it in the **Confirm SIP Password** field.
11. Click **Save Changes** to save the changes.

Note: The SIP password is the SIP authentication password, and the Number is the directory number (DN, a telephone number). Program all other fields according to the site requirements, or leave them at their default values.

8.1.2.4 Configure Class of Service Assignment

Configure Class of Service options on MiVoice Business for a Generic SIP Phone connected through the Mitel AG4124/AG4172 Gateway.

The **Class of Service Options** form creates or edits a Class of Service and specifies its options. Classes of Service, identified by Class of Service numbers, are referenced by the **Station Attributes** form for the SIP device.

Your site deployment may require various options to be set. For a Generic SIP Phone to work with MiVoice Business, do the following in the **Class of Service Options** form:

1. In the MiVoice Business System Administrator Tool, navigate to
   System Properties > **System Feature Settings** and select **Class of Service Options**.
2. Select the Class Of Service Number entry from the table and click
   Change.
3. Under
   General Tab, do the following:
   a. Set **Public Network Access via DPNSS** to **Yes** in the Class of Service for the SIP phones, to allow calls over trunks (including SIP trunks).
   b. Set **Force Device Busy If Any Line In Use** to **Yes** to prevent phones from receiving calls while they are already on a call.
   c. Disable **Auto Camp-on Timer** so devices hear a busy tone when calling busy extensions.
4. Click
   Save to save the changes.

For detailed information on Class of Service settings, see the *Class of Service Options* section in the *MiVoice Business System Administration Tool Online Help*, available on the MiVoice Business documentation page.

8.1.2.5 Configure TLS for the Mitel AG4124/AG4172 and MiVoice Business

Program a SIP Device Capabilities Number for TLS on MiVoice Business, and configure the corresponding SIP Server settings for TLS transport on the Mitel AG4124/AG4172 Gateway.

The **SIP Device Capabilities** form on MiVoice Business defines a SIP profile that grants a SIP device, such as the Mitel AG4124/AG4172 Gateway, alternate capabilities, as recommended in the *Mitel Interoperability Reference Guide*.

> **Note**: Mitel recommends configuring the SIP Device Capabilities Number for Transport Layer Security (TLS) on the Mitel AG4124/AG4172 Gateway.

This procedure has two parts: programming the SIP Device Capabilities Number for TLS on MiVoice Business, and configuring the matching SIP Server settings for TLS on the Mitel AG4124/AG4172 Gateway.

1. On MiVoice Business, in the **SIP Device Capabilities** form:
1. In the MiVoice Business System Administrator Tool, navigate to **System Properties** > **System Feature Settings** and select **SIP Device Capabilities**.
2. On the page that opens, click **Change**.

> **Note**: Mitel recommends using the default values; change them only if necessary.

3. Update the SIP device capabilities according to the site requirements.
4. Click **Save**.
2. On the Mitel AG4124/AG4172 Gateway, in the Web Management System:
5. Log in to the Web Management System.
6. Navigate to **SIP Server**.
7. In the

   SIP Server field, enter the SIP server details, such as a MiVoice Business IP address or Fully Qualified Domain Name (FQDN).
8. In the

   SIP Server Port (Default: 5060) field, enter **5061**.
9. In the

   Primary Outbound Proxy Port field, enter **5061**.
10. In the

    Secondary Outbound Proxy Port field, enter **5061**.
11. In the

    SIP Transport Type field, select **TLS** from the list of options.
12. In the

    SIP UDP/TCP Local Port field, enter **5061**.
13. In the

    SIP TLS Local Port field, enter **5061**.
14. Click

    Save to save the changes.

8.1.2.6 Configure UDP for the Mitel AG4124/AG4172 and MiVoice Business (Optional)

Program a SIP Device Capabilities Number for UDP on MiVoice Business, and configure the corresponding SIP Server settings for UDP transport on the Mitel AG4124/AG4172 Gateway.

The **SIP Device Capabilities** form on MiVoice Business defines a SIP profile that grants a SIP device, such as the Mitel AG4124/AG4172 Gateway, alternate capabilities, as recommended in the *Mitel Interoperability Reference Guide*.

Important: This procedure is optional. Mitel does not recommend configuring the SIP Device Capabilities Number for User Datagram Protocol (UDP) as the default setting on the Mitel AG4124/AG4172.

This procedure has two parts: programming the SIP Device Capabilities Number for UDP on MiVoice Business, and configuring the matching SIP Server settings for UDP on the Mitel AG4124/AG4172 Gateway.

1. On MiVoice Business, in the **SIP Device Capabilities** form:
1. In the MiVoice Business System Administrator Tool, navigate to **System Properties** > **System Feature Settings** and select **SIP Device Capabilities**.
2. On the page that opens, click **Change**.
3. Click the **SDP Options** tab.
4. On the page that opens, do the following:
   a. Set the **Allow Device To Use Multiple Active M-Lines** field to **Yes**.
   b. Set the **Force Sending SDP in Initial Invite Message** field to **Yes**.
   c. Set the **Prevent the Use of IP Address 0.0.0.0 in SDP Messages** field to **Yes**.
5. Click the **Signaling and Header Manipulation** tab.
6. On the page that opens, set the **Allow Display Update** field to **Yes**.
7. Click the **Timers** tab and click **Change**.
8. On the page that opens, in the **Session Timer** field, enter **1800**.

Note: Mitel recommends using the default values for other parameters; change them only if necessary.

9. Click **Save**.
2. On the Mitel AG4124/AG4172 Gateway, in the Web Management System:
10. Log in to the Web Management System.
11. Navigate to **SIP Server**.
12. Configure the
    SIP Server settings:
    a. Set **SIP Server** to the MiVoice Business IP address or Fully Qualified Domain Name (FQDN).
    b. Set **SIP Server Port (Default: 5060)** to **5060**.
    c. Set **Registration Expires (Default: 300)** to **300**.
    d. Clear the **Heartbeat** checkbox.
13. Configure the
    Primary Outbound Proxy settings:

a. Set **Primary Outbound Proxy Port Address** to a site-specific value.
b. Set **Primary Outbound Proxy Port** to **5060**.

14. Configure the

    Registration settings:

    a. Set **Re-registration Percent(Expires)(0: means random, range: 25%-75%)** to **0**.
    b. Set **Retry Interval when Registration Failed** to **30**.
    c. Set **Registration Limit (counts/time, time: 0 means unlimited)** to **1/0**.
    d. Clear the **Send SIP Unregistration Request when the Device Restart** checkbox.

15. Clear the

    Music on Hold (MOH) checkbox.

16. Set **SIP Transport Type** to **UDP**.
17. Configure the **Local SIP Port**:

    a. Clear the **Use Random Port** checkbox.
    b. Set **SIP UDP/TCP Local Port** to **5060**.

18. Click

    Save to save the changes.

For information about SIP Device Capabilities settings, see the *SIP Device Capabilities* section in the *MiVoice Business System Administration Tool Online Help*, available on the MiVoice Business documentation page.

8.1.2.7 Configure SRTP

Enable voice and video SRTP encryption on MiVoice Business for use with the Mitel AG4124/AG4172 Gateway.

1. In the MiVoice Business System Administrator Tool, navigate to **System Properties** > **System Feature Settings** and select **System Options**.
2. On the page that opens, click **Change**.
3. Set the **Voice Encryption Enabled** field to **Yes**.
4. Set the **Voice/Video SRTP Encryption Enabled** field to **Yes**.
5. Click **Save**.

8.1.2.8 Configure Station Attributes

Assign the previously configured Class of Service and SIP Device Capability number to the Mitel AG4124/AG4172 Gateway on MiVoice Business.

Use the **Station Attributes** form to assign the previously configured Class of Service and SIP Device Capability number to each Mitel AG4124/AG4172 Gateway in MiVoice Business. This form uses Range Programming. To do so:

1. In the MiVoice Business System Administrator Tool, navigate to

   Users and Devices > **Advanced Configuration** and select **Station Attributes**.

2. Select the Mitel AG4124 Gateway number and then select **Change**.
3. Enter the previously configured SIP Device Capability number (**30**) and the Class of Service for Day, Night 1, and Night 2 (**10**). See the *Station Attributes* form for more details.
4. Click

   Save to save the changes.

8.1.3 Mitel AG4124/AG4172 Configuration Notes

Sample configuration settings for connecting the Mitel AG4124/AG4172 Gateway to MiVoice Business.

The following sections show sample configuration settings for connecting the Mitel AG4124/AG4172 Gateway to MiVoice Business.

8.1.3.1 Configure Settings Using the Web Management System

Configure the Mitel AG4124/AG4172 Gateway Web Management System settings to connect with MiVoice Business (MiVB).

To configure the settings using the Web Management System, do the following:

1. Log in to the Web Management System.
2. Go to **Network** > **Local Network** and in the page that opens, do the following:
   a. In the **IP Protocol** field, select **IPv4**.
   b. Under **Network Configuration**, do the following:
      i. Select the **Use the following IP address** option.
      ii. Enter appropriate values in the **Static IP address**, **Subnet Mask**, and **Default Gateway** fields.
   c. Under **DNS Server**, do the following:
      i. Select **Use the following DNS server address**.
      ii. In the **Primary DNS Server** field, enter the Internet Protocol (IP) address of the Domain Name System (DNS) server.
      iii. Optional: In the **Secondary DNS Server** field, enter the IP address of the secondary DNS server.
   d. Click **Save** to save the changes.
3. Go to **SIP Server**. In the page that opens, do the following:
   a. In the **SIP Server** field, enter the SIP Server details, such as a MiVB IP address or a Fully Qualified Domain Name (FQDN).
   b. In the **SIP Server Port (Default: 5060)** field, enter **5061**.
   c. In the **Primary Outbound Proxy Port** field, enter **5061**.
   d. In the **Secondary Outbound Proxy Port** field, enter **5061**.
   e. In the **SIP Transport Type** field, select **TLS** from the list of options.
   f. In the **SIP UDP/TCP Local Port** field, enter **5061**.
   g. In the **SIP TLS Local** Port field, enter **5061**.
   h. Click **Save** to save the changes.
4. Go to **Port** and do the following:
   a. Click **Add**.
   b. In the **Start Port** and **End Port** fields, enter the appropriate port number for the extension being programmed.
   c. In the **Registration** field, select the **Enable** option.
   d. In the **Profile** field, set the value based on the Message Waiting Indicator (MWI) that the phone has.
   e. In the **SIP User ID**, **Authenticate ID**, and **Authenticate Password** fields, enter the user details that are configured on the MiVB system.
   f. Click **Save** to save the changes.

> **Note**: You must repeat this for each analog phone connected to the AG4124/AG4172 Gateway.

5. Go to **Status & Statistics** > **Port Status** to view the port status.
6. Go to **Advanced** > **Line Parameter**. In the page that opens, verify/edit the details as required and click **Save**.
7. Go to **Advanced** > **FXS Parameter**. In the page that opens, verify/edit the details as required and click **Save**.
8. Go to **Advanced** > **Media Parameter**. In the page that opens, verify/edit the details as required and click **Save**.

> **Note**: Under **Media Parameters**, set the **SRTP Mode** field to **AUTO**. By default, in the **System Administration Tool (MiVB)**, the **Voice/Video SRTP Encryption Enabled** field (**System Properties > System Feature Settings > System Options**) is set to **Yes**.

If the Media Parameter SRTP Mode field is set to Disable, the MiVB System Options SRTP field must also be set to Disable.

9. Go to **Advanced** > **Service Parameter**. In the page that opens, verify/edit the details as required and click **Save**.

> **Note**: The Voicemail User ID should not exceed 32 characters.

10. Go to **Advanced** > **SIP Compatibility**. In the page that opens, verify/edit the details as required and click **Save**.
11. Go to **Advanced** > **Feature Code**. In the page that opens, verify/edit the details as required and click **Save**.

> **Note**: All feature codes are disabled by default, except for the following fields:
> - **Inquiry LAN IP**
> - **Inquiry IP Phone Number**
> - **Inquiry PortGroup Number**

12. Go to **Advanced** > **System Parameter**. In the page that opens, verify/edit the details as required and click **Save**.
13. Go to **Advanced** > **Media Parameter**. In the page that opens, do the following:
    a. In the **SRTP Mode** field, select **Force** for the Transport Layer Security (TLS)/Secure Real-time Transport Protocol (SRTP) configuration.
    b. Click **Save** to save the changes.

> **Note**: To enable forced calls, you must select **Enable** in the **SRTP Mode** field.

8.1.4 MiVoice Border Gateway Setup Notes

Steps for programming the MiVoice Border Gateway (MBG) to enable connections between the Mitel AG4124/AG4172 Gateway and MiVoice Border Gateway.

The following sections describe the steps for programming the MiVoice Border Gateway (MBG) server to enable connections between the Mitel AG4124/AG4172 Gateway and the MBG.

8.1.4.1 Set up MiVoice Business in MiVoice Border Gateway

Configure the MiVoice Border Gateway to communicate with MiVoice Business.

To configure the MiVoice Border Gateway to communicate with MiVoice Business:

1. Log in to the MiVoice Border Gateway application.
2. Navigate to **Network > ICPs**.
3. On the page that opens, click **+ (Add an ICP)**.
4. On the page that opens, enter the ICP information (**Name**, **Type**, **SIP capabilities**, and **Hostname or IP address**) and click **Save**.

8.1.4.2 Add SIP Devices to MiVoice Border Gateway

Add a SIP device to the MiVoice Border Gateway (MBG) for teleworker connections to the Mitel AG4124/AG4172 Gateway.

To add a SIP device:

1. In the MBG application, navigate to **Teleworking > SIP**.
2. On the page that opens, under **SIP profile information**, click **+ (Add)** to add a SIP device.
3. On the page that opens, under
   Manage SIP profile, enter the data to create the new SIP device in MBG.
4. Enter all the required information in the
   Profile, **Connection**, **Set-side Authentication**, and **ICP-side Authentication** fields.

> **Note**: The Set-side credentials must match the username and password provisioned on the phone.
> The ICP-side credentials must match the Login PIN and Number provisioned on MiVoice Business.
> Provisional Response Acknowledgement (PRACK) support in SIP signaling is disabled by the global setting; by default, PRACK support in the Manage SIP Profile section is set to Use global setting. If PRACK is enabled on MiVoice Business, you must also enable it in the Manage SIP Profile section when adding a SIP user (that is, change the setting from Use global setting to Enabled).

5. Click **Save** to save the changes. Once these steps are complete, the MBG server allows connections to be made between the Mitel AG4124/AG4172 Gateway and the MBG.

8.1.5 Configuring AG Connectivity to MiVB Through MBG (Teleworker Mode)

Prerequisites and notes for connecting the Analog Gateway to MiVoice Business through MiVoice Border Gateway in Teleworker mode.

Prerequisites

Before connecting the Analog Gateway (AG) to MiVoice Business (MiVB) through MiVoice Border Gateway (MBG), confirm the following:

- MiVoice Business
  - The MiVB system is deployed and reachable from the MBG.

  - A generic SIP device is created for each Analog Gateway port.
- MiVoice Border Gateway
  - The MBG is deployed and reachable from the Analog Gateway.
  - The Local Area Network (LAN, internal) and Wide Area Network (WAN, external) interfaces are configured.
- Analog Gateway
  - The Analog Gateway is powered on and reachable over the network.
  - SIP communication uses Transport Layer Security (TLS), port 5061.
  - The firmware version supports MBG connectivity (Release 5, version 33.83.12.21 or higher).

Notes

- The AG connects to the MiVB through the MBG; it does not connect directly.
- SIP authentication settings must match across the MiVB, the MBG, and the AG.
- Call recording using MIR is supported only when the AG connects through the MBG.
- A direct AG-to-MiVB connection does not support call recording.

8.1.5.1 MiVB Configuration for Teleworker Mode

Create the generic SIP devices and network elements MiVoice Business (MiVB) needs for AG connectivity through MiVoice Border Gateway (MBG).

To create the generic SIP devices:

1. Log in to the MiVB Web GUI.
2. Navigate to **Users and Devices > Users and Services Configuration**.
   a. Create a generic SIP device for each AG port.
      i. Under **Service Details**, ensure that **SIP Device Capabilities** is set to **85 Analog-AG**.
   b. Navigate to **SIP Device Capability**, and ensure that **Replace System based with Device based In-Call Features** is set to **No**.
   c. Save the configuration.
3. Navigate to **Voice Network > Network Elements**.
   a. Click **Add** to add the MiVB systems as network elements.
   b. Configure the parameters and ensure that **Data Sharing** is set to **YES**.
   c. Save the configuration.

8.1.5.2 Configure the MBG for Teleworker Mode

Configure MiVoice Border Gateway (MBG) certificates and teleworker SIP profiles for Analog Gateway (AG) connectivity.

To configure the MBG:

1. Log in to the MBG Web Graphical User Interface (GUI).
2. Configure the Certificate Authority (CA) certificate:
   a. Navigate to **System > Settings** > **SIP options**.
   b. Under **SIP support > Certificate**, click **Export root cert** to download the certificate.
   c. Use this certificate for the AG configuration (see Certificate Management on page 113).
3. Configure the web server certificate:

a. Navigate to **Security > Web Server**.
b. Under **Manage Web Server Certificate**, click **Get Certificate** to download the certificate.
c. Use this certificate for the AG configuration (see Certificate Management on page 113).

4. Configure the teleworker SIP profiles:
   a. Navigate to **Network > ICPs**, and ensure the MiVoice Business (MiVB) devices are configured.
   b. Navigate to **Teleworking > Manage**.
   c. Under SIP profiles and devices, ensure the SIP profiles are created.
5. Save the configuration.

8.1.5.3 Configure the AG for Teleworker Mode

Configure the Analog Gateway (AG) SIP Server and Port settings for connectivity through MiVoice Border Gateway (MBG).

To configure the AG:

1. Log in to the AG Web Graphical User Interface (GUI).
2. Navigate to **SIP Server**.
   a. Under **SIP Server**, set the **SIP Server IP address** to match the MBG IP address (**WAN interface**).

   > **Note**: If you want to connect to multiple MBGs (for resiliency), configure the **Primary Outbound Proxy** and the **Secondary Outbound Proxy**.

   b. Under **Registration**, ensure that the **Registration Limit (counts/time, time:0 means unlimited)** is configured, for example, 24 ports per 30 seconds or 72 ports per 30 seconds, depending on the model.
   c. Set the SIP Transport Type to TLS.
      i. Ensure that **SIPS URL** is enabled.
      ii. Ensure that **Contact Uses the Local Connection Port** is enabled.
   d. Save the configuration.
3. Navigate to **Ports**.
   a. Ensure the values match the SIP profile configured on MiVoice Business (MiVB).
   b. Save the configuration.

Verify the following:

- On the AG, Port Status → Ports should show Registered.
- On the MBG, Teleworker status → Devices should show Connected.

8.1.6 Data Encryption

Overview of the voice and signaling encryption architecture used across MiVoice Business and its connected devices.

Encryption hides both the signaling information and the voice streaming. The network connection, or path, remains the same whether the data in the payload is secured or not. Both secure and non-secure devices use the same network paths to establish voice connections. Data encryption involves two main aspects:

- key exchange
- data encryption and decryption

Encryption scrambles the data using the available key information such that it cannot be easily read and decoded by a third party. Only the endpoints have the necessary key information to encode and decode the data correctly. The method used to pass this key information between endpoints is known as the key exchange.

There are a number of standard methods to encrypt data. These are very secure in their coding, and have been field tested over a number of years with critical information such as financial and personal data. From a user view, all that is important is to know is that the data is secured. The method used to encrypt the data is negotiated by the endpoints. If one or both endpoints do not support encryption, the connection may still be established, but it is unsecured. That is, a voice call can still be established with equipment that does not support encryption methods.

Bandwidth Considerations (Voice and Signaling Encryption)

The secure connection uses data encryption to modify the contents of the payload so that someone collecting data packets will be unable to read the contents. It does not modify the contents of the IP header, since the header is still needed to pass data over the existing Layer 3 routers and Layer 2 network switches. If the headers were also encrypted, then every router in the path would need to know how to decipher the information.

The data in the payload is intended for a particular application. It is the application that knows how to decode the information. For the Voice over IP application, this payload contains the signaling information or voice streaming.

When the data is encrypted, it is simply replaced with a scrambled version. This is a 1 for 1 transformation, so there are no additional bytes. As a result, the bandwidth is the same for encrypted or non-encrypted information. This is not true for Secure RTP (SRTP), which appends either 4 or 10 bytes to the voice payload depending on the cipher mode used. Voice streaming security (SRTP)

For the signaling information, there are some additional messages related to setting up the secure connections. However, these are minimal when compared to the remainder of the signaling bandwidth, which is already quite low. For voice information the bandwidth remains the same for both encrypted and unencrypted payloads.

As an analogy, the encryption can be considered simply another voice codec, or an additional process in the voice-streaming path. G.711 and G.729 codecs are often used for voice streaming. Encryption merely makes these secure, so the result is a secure-G.711 or secure-G.729 codec. The bit rate and network bandwidth requirements remain the same.

Figure 8: Unsecured Vs. Secured Connection

Signaling and Media Paths

Media and signaling path encryption is supported for all of Mitel's IP phones on MiVoice Business.

Media path encryption is accomplished with Secure RTP using 128-bit Advanced Encryption Standard (AES). Encryption is backward-compatible to support both currently shipping desktops and previously deployed Mitel IP desktops. Mitel provides encryption of the media path between multiple 3300 ICPs using a Secure Sockets Layer (SSL) protocol. This allows scalability of applications by configuring 3300 ICPs into clusters or deploying them as part of a centrally managed but distributed architecture.

The signaling path is generally between the controller and the IP Phone or other end-device. This path is established as a secure connection. Signaling information is interpreted within the controller. Where a message needs to be sent to another controller, such as with IP Networking, or to another end device, an independent secure connection is used. A call between two phones on two controllers therefore requires the establishment of three secure signaling channels: a secure connection at each controller and one between the controllers.

Figure 9: Media and Signaling Path Encryption

Secured signaling paths do not take different network routes than paths without security. The only difference is that the contents of the payload are encrypted. The only additions for security are the messages needed to establish the point-to-point secure connections and to negotiate the secure voice connection. The signaling itself is secured: MiNET becomes Secure-MiNET, and MiTAI becomes Secure-MiTAI.

Once the signaling paths are established and a voice connection can be made, the two end devices negotiate the keys and method of voice encryption. Once they agree, voice streams directly between the two devices. This is the same as the unencrypted case; only the voice data is encrypted.

Voice Streaming Security (SRTP)

Mitel controllers and selected IP sets and applications support the RFC 3711 standard for Secure RTP. This provides added confidentiality, message authentication, and replay protection over the standard RTP protocol. A call is encrypted and uses the most secure method available if both ends support encryption. Calls initiated on a controller, an IP phone, or an end device that does not support encryption are still supported, but are not encrypted.

SRTP is enabled by default on all x86 systems (EX and servers) as of MiVB release 9.4.

Media (voice) streaming between Mitel sets and controllers uses a version of SRTP with a predefined algorithm (Mitel SRTP), so negotiation of the secure connection is fast. Mitel products that connect to third-party equipment must negotiate the key exchange for the security algorithm, which is more processor-intensive.

Signaling Security

Two main methods are used to secure a signaling channel. These are:

- Transport Layer Security (TLS), an open standard
- Secure MiNET, a Mitel proprietary standard

Mitel's Secure MiNET protocol uses the Advanced Encryption Standard (AES) to encrypt call control packets. Using secure MiNET ensures that call control signaling packets between the IP phones and the 3300 ICP are protected from eavesdropping. Using secure MiNET also protects the 3300 ICP from unauthorized control packets.

Secure MiNET uses a predefined algorithm to encode the signaling messages. Negotiation of the encryption method is not needed, so this provides a simpler and faster method for establishing secure connections with third-party applications. Some SIP phones may also use TLS, which is an updated and more open version of the SSL standard. Because the encryption algorithms for SSL and TLS are not predefined as they are with Secure MiNET, the endpoints must negotiate the security for each connection, and performance may be impacted somewhat. Factor this into capacity planning for SIP-TLS deployments.

In addition to Secure MiNET, a standard encryption method that uses SSL is also available on certain end devices. SSL is used to negotiate which encryption method to use at the endpoints. This standard allows interaction with third-party applications.

As of MiVB release 7.1, a third option for signaling encryption is available between controllers and selected phone set types: the Protected Extensible Authentication Protocol (PEAP), a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated TLS tunnel.

Mitel 53xx series IP phones are enhanced to support 802.1x with PEAPv0-MSCHAPv2 authentication. The existing EAP-MD5 authentication mode continues to be supported for backward compatibility.

- Supported set types are 5360, 5340e, 5330e, 5320e, 5324, 5312, 5304, and 69xx series.
- 5340, 5330, and 5320 do not support PEAP authentication.
- Firmware required is version 6.3.0.12 (released with MiVB 7.1) or higher.
- These sets automatically trust the server certificate for TLS connection.
- The configuration of username and password on these IP sets remains unchanged.

The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. SSL prevents unauthorized access to administrative functions and encrypts all traffic on the link to prevent the sniffing of usernames and passwords.

IP phones determine which secure method to use, first trying SSL, then Secure MiNET; if neither is supported, the call goes unsecured.

The ICP uses multiple IP ports to differentiate these protocols (6800, 6801, 6802) as defined in the IP port information. If the relevant port is blocked with a firewall or a router, for instance, the negotiation may fail and a connection may not be established.

IP Networking communication between ICP controllers and gateways uses only SSL or no encryption at all. MiNET encryption is not supported.

Voice Streaming to External Gateway PSTN Connection

In voice streaming to an external gateway PSTN connection, the voice path is established between the IP phone and the IP/TDM gateway. This might be the local ICP, or another unit dedicated to this function and connected through IP Networking. There is no difference in the connection path between secure and non-secure call establishment. Connections are established as secure where possible.

Voice Streaming to TDM Connections

Where an ICP has a number of TDM-connected devices, calls to these devices are routed through the local IP/TDM gateway. Encryption applies to the packet part of the connection, so the IP path to the gateway is secure where possible. The connection on the TDM side continues, as it always has, to use a dedicated connection to the end device.

Voice Streaming to Internal Voice Mail, Record a Call and Conference

Where there are internal features like voice mail, Record-a-Call, or conference at the ICP, these are considered TDM devices. Encryption applies to the packet part of the connection, so the IP path to the gateway is secure where possible. The connection on the TDM devices remains a dedicated connection to the requested service.

A conference call with a number of users requires multiple connections to the IP gateway. Connections between the IP end device and this gateway are encrypted where possible. Connections to the conference bridge are established over the internal TDM infrastructure.

PSTN connections or TDM devices connected into this bridge do not use encryption but maintain their normal dedicated connections.

Voice Streaming to Applications

A number of applications and end devices support encryption; some, however, do not. Connections to devices that do not support encryption are established without it. See your MiVoice Business documentation for the current list of devices and applications that support encryption.

End devices that connect to the external port of the MiVoice Border Gateway (formerly the Teleworker solution) are secure, but when similar end devices are used within the LAN environment, they may not be fully secured.

For further details, see the MiVoice Border Gateway Engineering Guidelines. The MiVoice Border Gateway also terminates both internal and external secure connections, which allows for different encryption methods: an external secure connection and an unsecured internal connection.

MiCollab Client provides a softphone with an encrypted call path and call signaling, plus secure instant messaging that keeps IM traffic encrypted and inside the network.

The SpectraLink wireless phones and the Mitel WLAN stands may use security on the air access interface (radio link), such as WEP or WPA2. However, this covers only the wireless connection, not necessarily the rest of the connection across the remaining network infrastructure.

Worm and Virus Protection

The 3300 ICP uses an embedded real-time operating system that is less susceptible to the viruses and worms typically found on networks and the internet. This also makes it difficult for an attacker to write a virus targeted at generic VxWorks implementations.

Application servers based on Windows must be properly maintained with current operating system security updates. Mitel products based on Windows include the Contact Center Solutions, Speech Server, and Messaging Server systems. These key application servers must be kept up to date with the latest Microsoft security updates and worm protection.

Prevention of Toll Abuse

Any communication system that combines Direct Inward System Access (DISA), an integrated auto attendant or RAD groups, and a peripheral interfaced auto attendant or voice mail can be susceptible to toll abuse. It is therefore important to assign appropriate telephone privileges and restrictions to devices. In addition, deny public telephones toll access unless authorized through an attendant.

The 3300 ICP system has comprehensive toll control as an integral part of call control. It lets you restrict user access to trunk routes, specific external directory numbers, or both. It also provides Class of Restriction (COR) and Class of Service (COS) features that can substantially reduce the risk of toll abuse.

As a deterrent to toll abuse by internal callers, use Station Message Detail Recording (SMDR) to track calls from within your company; it provides detailed information such as the originating extension number, time, duration, and number dialed. Restrict SMDR record access as you would for any other function.

Secure Management Interfaces

The 3300 ICP includes a fully integrated set of management tools designed to install, manage, and administer 3300 ICP systems. Three levels of access meet the needs of system technicians, group administrators, and desktop telephony users themselves. All of these integral management tools use SSL security for data encryption. A login and password control user access to the management tools. After a user logs in to the 3300 ICP, the system displays a menu of the specific tools to which they have been granted access. Mitel also offers the Management Access Point, which provides secure remote administration for VPN or dial-up access.

8.1.7 MiVoice Business Resiliency Configuration

Prerequisites, notes, and limitations for configuring MiVoice Business (MiVB) resiliency with the Analog Gateway.

Prerequisites for MiVB

Before configuring resiliency for MiVoice Business (MiVB) with the Analog Gateway (AG), ensure the following:

- The AG is running the current supported release. At present, the supported releases are **v33.83.11.29 (AG4124)** and **v33.83.12.08 (AG4172)**. Earlier releases are not supported.
- Two MiVB systems (primary and secondary) are deployed and properly clustered with data sharing enabled.

> **Note**:
>
> The Primary and Secondary Outbound Proxy configuration on the Analog Gateway must match the corresponding Home Element and Secondary Element configuration in MiVB.

- IP trunking is configured between the MiVB systems.
- Analog Gateways are reachable over the network.
- The certificates required for AG integration are installed in MiVB, and the root certificate is trusted.
- The Analog Gateway is already added and integrated with MiVB. For integration steps, see Configuring Analog Gateway With MiVoice Business on page 129.
- SIP device capabilities are verified and modifiable (version dependent).

For MiVB configuration details, see the latest **MiVB System Administration Tool Online Help** ZIP file, available on the MiVoice Business documentation page.

Notes

- Resiliency requires configuration on both MiVB and the AG; it is not automatic.
- All Analog Gateway ports must be configured for resiliency. If any port on the Analog Gateway is not configured for resiliency, the Analog Gateway fails to register correctly with the secondary MiVB system during failover.
- During failover, some features (for example, voicemail) may not be available, depending on the system design.
- Ongoing calls may drop during failover. Call survival is not supported for AG devices.
- Session timers (default approximately 1800 seconds) may delay failover behavior in some cases.
- You must reboot the Analog Gateway after configuration changes.

- Registration rate limits are required for resiliency deployments and must be configured according to the deployment size.

Limitations

- The Analog Gateway Server configured in the primary MiVB system is not replicated to the secondary MiVB system.
- Only Analog Gateway ports configured for resiliency are replicated to and visible on the secondary MiVB system.

8.1.7.1 Configure MiVB for Resiliency

Configure MiVoice Business (MiVB) to support Analog Gateway resiliency.

1. Log in to the MiVB GUI.
2. Add the Analog Gateway server.
   a. Navigate to **Analog Gateway Servers** (using search or the menu).
   b. Click **Add** to add the AG server.
   c. Configure the AG server parameters.
   d. Click **Save**.
3. Configure the Analog Gateway ports.
   a. Navigate to **Analog Gateway Ports** (using search or the menu).
   b. Select the AG server that you added.
   c. Click **Change**.
   d. Configure the AG port parameters.
   e. Click **Save**.
4. Configure SIP Device Capabilities (using search or the menu).
   a. Navigate to **SIP Device Capabilities**.
   b. Verify the Analog Gateway capability settings.
      i. Under **Basic** configuration, ensure that the **Replace System based with Device based In-Call Features** value is set to **No**.
   c. Click **Save**.
5. Assign the SIP Device Capability to ports.
   a. From the menu, navigate to **Users and Devices > Users and Services Configuration**.
   b. Search for the **SIP User ID**. For example, 167201.
   c. Click the result.
      i. Under **Service Profile**, ensure that **Device Type** is set to **Analog-AG**.
      ii. Under **Service Profile**, set **Home Element** to the primary MiVB system.
      iii. Under **Service Profile**, set **Secondary Element** to the secondary MiVB system.
      iv. Under **Device Details**, ensure that **Endpoint ID** is set to the AG that you added earlier in the Analog Gateway Server configuration.

      > **Note**: The **Endpoint ID** is configured automatically during integration.

      v. Click **Save**.
      vi. Repeat the resiliency configuration for every Analog Gateway port.
      vii. Verify that all Analog Gateway ports are configured consistently for resiliency before completing the deployment.

> **Important**:
>
> Configure resiliency for every port on the Analog Gateway. If one or more ports are not configured for resiliency, the Analog Gateway may not register correctly with the secondary MiVB system during a failover event.

8.1.7.2 Configure the AG for Resiliency

Configure the Analog Gateway to support resiliency with MiVoice Business (MiVB).

1. Log in to the Analog Gateway (AG) web UI.
2. Configure the SIP server settings.
   a. Navigate to **SIP Server** settings.
   b. Do not configure the **SIP Server** field.
   For example, the following parameter values should be empty:
      - SIP Server
      - SIP Server Port (Default: 5060)
      - Registration Expires (Default: 300)
      - Heartbeat **(Disabled)**
   c. Set the **Primary Outbound Proxy**:
      - Set **Primary Outbound Proxy Address** to the primary MiVB IP address or FQDN.
      - Set **Primary Outbound Proxy Port** to **5061** (TLS recommended).
   d. Set the **Secondary Outbound Proxy**:
      - Set **Secondary Outbound Proxy Address** to the secondary MiVB IP address or FQDN.
      - Set **Secondary Outbound Proxy Port** to the same value as the primary port.
   e. Set the **SIP Transport Type**:
      i. Set **SIP Transport Type** to **TLS**.
      ii. Enable the **SIPS URL**.
      iii. Configure **Contact Uses the Local Connection Port** according to the deployment:
         - Set to **Disable** for resiliency deployments and direct MiVB connections.
         - Set to **Enable** for direct MiVoice Border Gateway (MBG) connections.
   f. Click **Save**.
3. Configure **Registration**.
   a. Configure the **Registration Limit (counts/time, time: 0 means unlimited)** parameter. For example, 24 ports per 30 seconds or 72 ports per 30 seconds, depending on the model.
      - Configure the registration rate limit based on the deployment size.
      - This setting is required for resiliency deployments to control the registration rate during failover.

> **Note**:
>
> For recommended values, see the deployment sizing guidelines.

4. Restart the Analog Gateway.
   a. Navigate to **Tools > Device Restart**.

> **Important**: Service is impacted for 10 minutes during the restart.

b. Allow 5 to 10 minutes for full recovery and registration.

8.1.7.3 Verify the MiVB Resiliency Configuration

Verify that Analog Gateway ports fail over correctly to the secondary MiVoice Business (MiVB) system.

1. Shut down the primary MiVB server.

   Wait up to 10 minutes.
2. Log in to the Analog Gateway (AG) web GUI.
3. Navigate to **Status & Statistics > Port Status**.
4. Verify that the ports automatically register with the secondary MiVB system (see the **Server** parameter).

   After the primary MiVB system is restored, the ports automatically re-register with the primary MiVB system.

8.1.8 Analog Gateway Behavior When the SIP Server Is Unavailable

Describes Analog Gateway telephony behavior in Standalone Mode when the MiVoice Business SIP server is unreachable, and how to identify and recover from an outage.

This topic describes the Analog Gateway's telephony capabilities when the MiVoice Business (MiVB) Session Initiation Protocol (SIP) server becomes unreachable due to a network failure, server outage, or maintenance window.

When the Analog Gateway loses connectivity to the MiVB SIP server, all ports transition to an Unregistered state. You can verify this on the **Status & Statistics** > **Port Status** page of the Analog Gateway web interface. During this time, the Analog Gateway operates in a limited standalone mode (Standalone Mode).

Standalone Mode — Supported Functionality

When the SIP server is unavailable, the Analog Gateway supports inter-port calling only:

- Analog phones connected to Foreign Exchange Station (FXS) ports on the same Analog Gateway unit can place and receive calls to and from each other.
- Inter-port calling is handled locally by the Analog Gateway's internal switching logic and does not depend on SIP registration.
- Standard analog call operations between local ports, such as placing a call, answering, and hanging up, continue to function.
- Caller ID delivery between inter-port calls may be limited depending on the port configuration.

  For example,

  On an AG4124 unit with ports 1–24 configured, a phone on port 3 can dial and connect to a phone on port 10 even when the SIP server is down. The call is switched locally within the AG unit.

Standalone Mode — Unsupported Functionality

The following features do not work when the SIP server is unavailable, because they require SIP signaling, server-side routing, or media server resources:

Table 66: Unsupported Standalone Mode Features

Feature	Reason unavailable
Calls between different AG units	The AG has no IP routing or account data for ports on other Analog Gateway units; all inter-unit call routing is handled by MiVB.
Call transfer (blind)	Requires SIP REFER signaling through the SIP server.
Call transfer (attended/consultative)	Requires SIP server involvement to bridge the consultation and transfer legs.
Three-way conference	Requires SIP server or media server resources to mix audio streams.
Call forwarding (all types: CFU, CFB, CFNRy)	Call forwarding rules are stored and executed on the SIP server.
Call hold/retrieve	SIP re-INVITE handling through the server is re-quired.
Message Waiting Indicator (MWI)	MWI notifications are sent by the SIP server or voicemail system using SIP NOTIFY.
Voicemail access	Requires connectivity to the voicemail system through MiVB.
Feature Access Codes (FACs)	FACs are interpreted and executed by the SIP server. The AG does not process FAC digit strings locally.
Do Not Disturb (DND)	DND state is managed by the SIP server.
Call pickup (group/directed)	Requires SIP server signaling to redirect the ring-ing call.
Speed dial/abbreviated dialing	Speed dial mappings are stored on the SIP server.

Feature	Reason unavailable
Outbound PSTN/external calls	All external call routing goes through MiVB trunk resources.
Inbound external calls	Incoming calls from the Public Switched Telephone Network (PSTN) or SIP trunks are routed by MiVB and cannot reach AG ports when the server is down.

Identifying a SIP Server Outage

Administrators can identify a SIP server connectivity issue by checking the following indicators:

- **Port Status page**: navigate to **Status & Statistics** > **Port Status**. If all ports show a registration status of **Unregistered**, the AG has lost contact with the SIP server.
- **Syslog messages**: review syslog entries for SIP registration failure messages or TCP/UDP connection timeout errors to the configured SIP server IP address.
- **Network connectivity**: verify IP connectivity between the Analog Gateway and the MiVB server using standard network diagnostic tools, such as ping and traceroute.

Recovery

When the MiVB SIP server becomes available again:

- The Analog Gateway automatically re-registers all configured ports with the SIP server.
- Port status on the Port Status page returns to **Registered**.
- All SIP-dependent features, such as call transfer, conference, forwarding, MWI, and FACs, resume normal operation.
- No manual intervention on the Analog Gateway is required for recovery, provided the SIP server address and credentials remain unchanged.

Planning Considerations

The Analog Gateway is not designed to operate as a standalone PBX. The inter-port calling capability during SIP server outages is a limited, best-effort function intended to preserve basic local connectivity only.

For production environments that require continued full-featured telephony during a SIP server outage, configure MiVoice Business Resiliency with a secondary MiVB system. See MiVoice Business Resiliency Configuration for setup instructions.

In multi-AG deployments, phones on different AG units cannot call each other during a SIP server outage, even if the AG units are on the same network.

Applicability

This behavior applies to:

- AG4124 (all firmware versions)
- AG4172 (all firmware versions)
- All SIP server registration modes: User Datagram Protocol (UDP) and Transmission Control Protocol (TCP)

8.2 Configuring Analog Gateway With MiVoice MX-ONE

Configuring MiVoice MX-ONE for Use With Mitel AG4124/AG4172 Gateway.

8.2.1 Overview

Reference for configuring MiVoice MX-ONE to host the Mitel AG4124/AG4172 Analog Gateway.

This appendix is a reference for Mitel Authorized Solutions Providers who are configuring MiVoice MX-ONE to host the Mitel AG4124/AG4172 Analog Gateway. It covers a basic AG4124/AG4172 Analog Gateway setup as a Session Initiation Protocol (SIP) endpoint, including the required options.

8.2.1.1 Supported Software Versions

Software versions of MiVoice MX-ONE and the Mitel AG4124/AG4172 Gateway that support basic SIP calls.

The following tables list the software versions of MiVoice MX-ONE and the Mitel AG4124/AG4172 Gateway that support basic Session Initiation Protocol (SIP) calls between the two products.

Table 67: AG4124

Product	Version
MiVoice MX-ONE	7.6 and later
AG4124	Mitel v33.83.11.28 and later

Table 68: AG4172

Product	Version
MiVoice MX-ONE	7.8 SP2 and later
AG4172	Mitel v33.83.12.15 and later

8.2.1.2 Supported Features

Features supported when the Mitel AG4124/AG4172 Gateway is connected to MiVoice MX-ONE.

The following table lists the features supported when the Mitel AG4124/AG4172 Gateway is connected to MiVoice MX-ONE.

Feature	Feature description
Basic Call	Making and receiving calls
Registration/Authentication	Device registration and authentication
Dual-Tone Multi-Frequency (DTMF) Signal	Sending DTMF after call setup (for example, a mailbox password or a service code used to invoke a specific feature)
Call Hold	Putting a call on hold
Call Transfer	Transferring a call to another destination
Call Forward: Direct/On Busy/On No Answer	Forwarding a call to another destination
Conference	Conferencing multiple calls together
Redial	Last number redial
Redundancy	Maintaining service availability by activating a secondary instance when the primary instance becomes unavailable
Call Pickup	A member of a group can pick up calls to other members of the same group
Message Waiting Indicator (MWI)	Message waiting indication
Transport Layer Security (TLS)/Secure Real-time Transport Protocol (SRTP)	Making and receiving calls using TLS/SRTP
Call Park/Retrieve	Parking and retrieving a call using a service code

Feature	Feature description
Long Duration Calls	Basic incoming and outgoing long-duration calls

8.2.1.3 Device Limitations

Features not supported when the Mitel AG4124/AG4172 Gateway is connected to MiVoice MX-ONE.

The following table lists the features that are not supported when the Mitel AG4124/AG4172 Gateway is connected to MiVoice MX-ONE.

Feature	Problem description
Video Calls	The Mitel AG4124/AG4172 Analog Gateway does not support video calling.
G.722 Codec	The Mitel AG4124/AG4172 Analog Gateway does not support calls using the G.722 codec.

8.2.1.4 Network Topology

Deployment topology for the Mitel AG4124/AG4172 Gateway with MiVoice MX-ONE.

The AG4124/AG4172 Analog Gateway provides connectivity and protocol conversion between Session Initiation Protocol (SIP) devices on the customer's Local Area Network (LAN) and the analog phones and fax machines connected to the AG4124/AG4172.

The AG4124/AG4172 is deployed on the premises, at the main site. In this deployment, the AG4124/AG4172 connects the analog phones to the customer's LAN. The MiVoice MX-ONE SIP Call Server and the SIP phones are also connected to the customer's LAN.

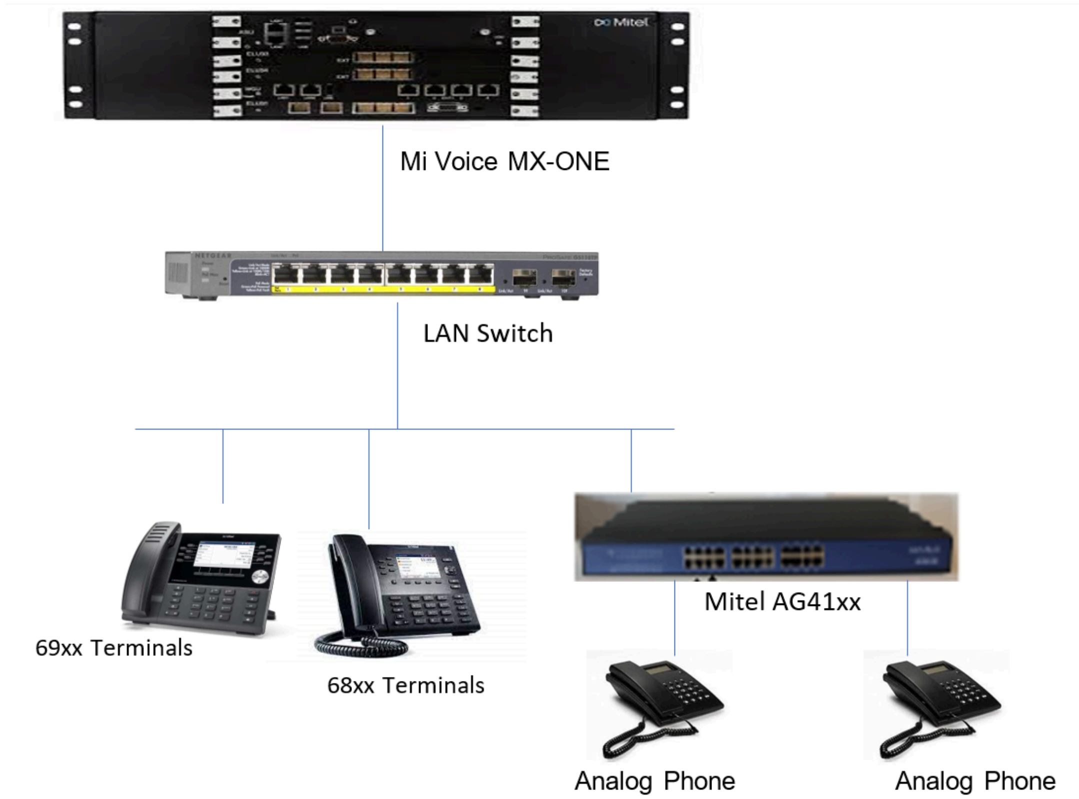

Figure 10: Network Topology

8.2.2 MiVoice MX-ONE Configuration Notes

Steps for programming a MiVoice MX-ONE to connect with the Mitel AG4124/AG4172 Gateway.

The following sections describe the steps for programming a MiVoice MX-ONE to connect with the Mitel AG4124/AG4172 Gateway.

8.2.2.1 Assumptions for the MiVoice MX-ONE Programming

SIP signaling port assumptions for connecting the Mitel AG4124/AG4172 Gateway to MiVoice MX-ONE.

These configuration notes assume the following about the Session Initiation Protocol (SIP) signaling connection between the gateway and MiVoice MX-ONE:

The SIP signaling connection uses Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) on port 5060.

The SIP signaling connection uses Transport Layer Security (TLS) on port 5061.

8.2.3 Mitel AG4124/AG4172 Configuration Notes

Sample configuration settings for connecting the Mitel AG4124/AG4172 Gateway to MiVoice MX-ONE.

The following sections present sample configuration settings for connecting the Mitel AG4124/AG4172 Gateway to MiVoice MX-ONE.

8.2.3.1 Log in to the Mitel AG4124/AG4172 Gateway Using the Default IP Address and Credentials

Log in to the Mitel AG4124/AG4172 Gateway using its default IP address and credentials.

The Mitel AG4124/AG4172 Gateway ships pre-configured with the following default settings:

Internet Protocol (IP) address: **192.168.11.1**

User name: **admin** / Password: **admin**

To log in to the Mitel AG4124/AG4172 Gateway:

1. Open a supported web browser and direct it to the IP address of the Mitel AG4124/AG4172 Gateway. For example, enter the following Uniform Resource Locator (URL): http://192.168.11.1

   The browser prompts for authentication.
2. Enter the default user name and password (**admin/admin**). After authentication succeeds, you are redirected to the Web Management System home page.

8.2.3.2 Configure the Settings Using the Web Management System

Configure the Mitel AG4124/AG4172 Gateway Web Management System settings to connect with MiVoice MX-ONE.

To configure the settings using the Web Management System, do the following:

1. Log in to the Web Management System.
2. Go to **Network > Local Network**.
3. Set the parameter **IP Protocol** to **IPV4**.
4. Under **Network Configuration**, select **Use the following IP address** and manually enter the parameters **Static IP address**, **Subnet Mask**, and **Default Gateway**.
5. Click the **Save** button.
6. Go to **SIP Server**.
7. Under **SIP Server**, manually enter the SIP Server details for the MiVoice MX-ONE Internet Protocol (IP) address or Fully Qualified Domain Name (FQDN).
8. Set the parameter **SIP Transport Type** to **UDP/TCP** or **TLS** according to your settings.
9. Set the parameter **SIP UDP/TCP Local Port** to **5060**.
10. Set the parameter **SIP TLS Local Port** to **5061**.
11. Click the **Save** button.
12. Go to **Port**.
13. Click the **Add** button.
14. Select the checkbox for the parameter **Registration** to enable registration.
15. Provide the user details that are configured on the MiVoice MX-ONE:
    a. **Display Name**
    b. **SIP User ID**
    c. **Authenticate ID**
    d. **Authenticate Password**

16. Click the **Save** button.
17. Check that the user is properly registered:
    a. Go to **Status & Statistics > Port Status**.
    b. You can see the users, their port number, and whether they are registered.
18. Check that the following parameters are configured as follows:
    a. Menu **Advanced > Media Parameter**

    > **Note**: For a Transport Layer Security (TLS)/Secure Real-time Transport Protocol (SRTP) configuration, whether the parameter **SRTP mode** is set to **Force** or **Auto** depends on customer requirements. If the AG4124/AG4172 is configured with SRTP mode set to "Force", update the Mitel-AG-GW user profile in MX-ONE in the file **"/etc/opt/eri_sn/sip_user_agents/mitel.conf"** with root access. Add the line **UserAgent:Mitel-AG-GW:CryptoOfferMethod: "SAVP"** in the Mitel-AG-GW section, and reload the SIPLP program unit.

    b. Menu **Advanced > Service Parameter**. See Service Parameters on page 77 for field details.
    c. Menu **Advanced > SIP Compatibility**. See SIP Compatibility Parameters on page 80 for field details.
    d. Menu **Advanced > System Parameter**. See System Parameters on page 90 for field details.
19. Go to **Advanced > Feature Code**.
    a. In the Status column, check that the feature codes are all disabled. See Feature Codes on page 89 for the full list of feature codes.
20. Go to **Security > Certificate Manage**.
    a. Under **Certificate Upload**, click **Choose File** to upload the MX-ONE Certificate Authority (CA) certificate (the *CA.pem* file).
21. Restart the Analog Gateway to apply all the changes:
    a. Go to **Tools > Device Restart**.
    b. Click the **Start** button to reboot the Analog Gateway.

> **Note**: During the reboot, the RUN indicator turns off and all the Foreign Exchange Station (FXS) port indicators turn on. The Analog Gateway is ready to use when:
> - The RUN indicator turns on.
> - The unused FXS port indicators turn off.

8.3 Configuring Analog Gateway With MiVoice 5000

Pointer to the MiVoice 5000 installation and configuration documentation for the Mitel AG4100/TA7100.

To configure the AG4124/AG4172 Analog Gateway with MiVoice 5000, see *Mitel EX Controller Mitel GX Gateway Mitel AG4100 and TA7100 - Installation and Configuration* in Technical Documentation.

8.4 Configuring OpenScape Business for Use With the Mitel AG4124/AG4172 Analog Gateway

Reference information for Mitel Authorized Solutions Providers on configuring OpenScape Business to host the Mitel AG4124/AG4172 Analog Gateway as a Session Initiation Protocol (SIP) endpoint.

This topic describes the basic setup required to connect the Mitel AG4124/AG4172 Analog Gateway to OpenScape Business as a SIP endpoint, along with the required option settings. When integrated with OpenScape Business, the AG4124/AG4172 Analog Gateway supports the following features:

- Outgoing calls from analog to SIP
- Incoming calls to analog from SIP
- Outgoing calls from analog to HFA (a Mitel proprietary IP phone signaling mode)
- Incoming calls to analog from HFA
- Consult retrieve
- Consult transfer
- Blind transfer
- Camp-on call (call waiting)
- Conference
- Long duration call
- Dual-Tone Multi-Frequency (DTMF) signaling
- Voicemail check
- SIP protocols: Analog (Transport Layer Security (TLS), User Datagram Protocol (UDP)), SIP (TLS, UDP)
- Codec support (G.711A/µ law, G.729A/B)
- Hunt group (group, linear, cyclical)
- Speed dial
- Redial key
- Do Not Disturb (DND) status
- Call Forward No Reply
- Call Forward Unconditional
- Call Forward on Busy
- Feature code activation/deactivation on the analog phone

8.4.1 Using the AG4124 and AG4172 LAN Port (OpenScape Business)

LAN port options for connecting a management Personal Computer (PC) to the Mitel AG4124/AG4172 Analog Gateway.

The management PC can access the AG4124 Web Management System through LAN0, LAN1, or LAN3. Enabling or disabling Virtual Local Area Networks (VLANs) does not change this behavior. Connect the AG4124 to the management PC using Category-5 Unshielded Twisted Pair (UTP) cabling.

You must connect the AG4172 to the customer's Local Area Network (LAN), the management PC, or both, using LAN0 or LAN1. Enabling or disabling VLANs does not change this behavior. Connect the AG4172 to the management PC using Category-5 UTP cabling.

8.4.2 Prepare to Log in to the Analog Gateway (OpenScape Business)

Connect and identify the Mitel AG4124/AG4172 Analog Gateway before logging in to the Web Management System for use with OpenScape Business.

1. Connect the Analog Gateway to the network and connect a telephone to the port.
2. Dial *158# to query the Internet Protocol (IP) address of the LAN port (the default IP address is 192.168.11.1).
3. Change the IP address of the Personal Computer (PC) so that it is on the same network segment as the LAN port of the Analog Gateway.
4. Check the connectivity between the PC and the Analog Gateway.
5. At a command prompt on the PC, run ping 192.168.11.1 to verify the IP address and connection information.

After the AG4124/AG4172 Analog Gateway is fully commissioned and the administrative accounts are established, you should establish access controls on the port's management capabilities.

8.4.3 Log in to the Web Management System (OpenScape Business)

Log in to the Web Management System on the Mitel AG4124/AG4172 Analog Gateway.

> **Note**: When you access the AG4124/AG4172 Web Management System by entering the unit's name or IP address, the system uses Hypertext Transfer Protocol Secure (HTTPS) for enhanced security. If you instead enter a specific page name directly into your browser's address bar, the system might revert to Hypertext Transfer Protocol (HTTP), which is not secure. To avoid this, log in by entering only the unit's name or IP address into your browser so that the system uses HTTPS, then navigate from there to the login page.

1. Open a web browser and enter the IP address of the LAN port (the default IP address is 192.168.11.1).
2. Enter the user name and password.
3. Click
   Login.

Both the default user name and the default password are "*admin*".

For security, change the user name and password at first login.

8.4.4 Configure Basic Settings (OpenScape Business)

Configure the Mitel AG4124/AG4172 Analog Gateway's network and Session Initiation Protocol (SIP) server settings for use with OpenScape Business.

1. Click
   Quick Setup Wizard.
2. In the
   Setup Wizard - Local Network page that opens, do the following:
   a. If needed, in the **WAN Dual Mode** field, select **Separation** from the drop-down list.
3. Under

Network Configuration, do the following:

a. Select the **Use the following IP address** option.
b. In the **IP Address** field, enter the address used to access the gateway on your network. This Internet Protocol (IP) address must be in the same subnet as OpenScape Business.
c. Enter the **Subnet Mask** and **Default Gateway**.

4. Under

Manage Address, do the following:

a. Enter 192.168.11.1 in the **IP Address** field.
b. Enter 255.255.255.0 in the **Subnet Mask** field.

5. Under

DNS Server, do the following:

a. Select the **Use the following DNS Server address** option.
b. Enter the value for **Primary DNS Server**. This value should match the Domain Name System (DNS) address configured for OpenScape Business.

6. Click

Save and Next. See Local Network on page 48 for field details.

7. In the

Setup Wizard - SIP Server page that opens, do the following:

a. Enter the OpenScape Business IP address in the **SIP Server** field. See SIP Server on page 56 for field details.

8. Click

Next.

9. In the

Setup Wizard - Port page that opens, click **Next**.

10. Click

Complete.

11. If needed, navigate to the

SIP Server tab.

a. Select either **UDP/TCP** or **TLS** in the **SIP Transport Type** field.

   i. Set the **SIP UDP/TCP Local Port** field to 5060.
   ii. Set the **SIP TLS Local Port** field to 5062.

12. Click

Save.

8.4.5 Using the AG4124/AG4172 Management Port (OpenScape Business)

Purpose and behavior of the Mitel AG4124/AG4172 management port for use with OpenScape Business.

The AG4124/AG4172 management port is useful for accessing the Web Management System when the customer's network Dynamic Host Configuration Protocol (DHCP) server is having problems and the AG4172 is relying on DHCP to obtain an Internet Protocol (IP) address.

The AG4124/AG4172 management port is a dedicated Ethernet port for accessing the Web Management System. It can be reached only from a Personal Computer (PC) residing on the same subnet as the AG4124/AG4172.

If the AG4124/AG4172 management port has previously been configured with a static IP address, you can still access the Web Management System through the management port if the DHCP server fails.

To allow a PC to access the Web Management System through the management port, you must properly configure the AG4124/AG4172.

8.5 Configuring OpenScape 4000 for Use With the Mitel AG4104/AG4108 Gateway

Reference for Mitel Authorized Solutions Providers for configuring OpenScape 4000 to host the Mitel AG4104/ AG4108 Analog Gateway.

This topic is a reference for Mitel Authorized Solutions Providers who need to configure OpenScape 4000 to host the Mitel AG4104/AG4108 Analog Gateway. It covers a basic setup of the Analog Gateway as a Session Initiation Protocol (SIP) endpoint, including the options required for that setup.

The Mitel AG4104/AG4108 gateway supports the following features:

- Outgoing call from analog to SIP
- Incoming call to analog from SIP
- Outgoing call from analog to HFA, a Mitel proprietary IP phone signaling mode
- Incoming call to analog from HFA
- Consult retrieve
- Consult transfer
- Blind transfer
- Camp-on call (call waiting)
- Conference
- Long duration call
- Dual-Tone Multi-Frequency (DTMF)
- Voicemail check
- SIP protocol support -- analog side using Transport Layer Security (TLS) or Transmission Control Protocol (TCP)/User Datagram Protocol (UDP); SIP side using TLS or TCP/UDP
- Codec support (G.711A/μ law, G.729A/B)
- Hunt group (group, linear, cyclical)
- Speed dial
- Redial key
- Do Not Disturb (DND) status
- Call Forward No Reply
- Call Forward Unconditional
- Call Forward on Busy
- Outgoing fax
- Incoming fax
- Feature code activation/deactivation on analog phone

8.5.1 Using the AG4104 and AG4108 LAN Port

A management Personal Computer (PC) can reach the AG4104/AG4108 Web Management System through either LAN0 or LAN1. Enabling or disabling Virtual Local Area Networks (VLANs) does not affect this access.

The AG4104/AG4108 must be connected to the customer's Local Area Network (LAN) or to the management PC using LAN0 or LAN1. As with Web Management System access, enabling or disabling VLANs does not change this connection requirement.

8.5.2 Log in to the Web Management System

Log in to the Web Management System for the Mitel AG4104/AG4108 gateway.

Note: When you access the AG4104/AG4108 Web Management System by entering the unit's name or Internet Protocol (IP) address, the system uses Hypertext Transfer Protocol Secure (HTTPS) for enhanced security. If you instead type a specific page name directly into your browser's address bar, the system might fall back to unsecured Hypertext Transfer Protocol (HTTP). To avoid this, log in by entering only the unit's name or IP address into your browser so that HTTPS is used, and then navigate to the login page from there.

1. Open a web browser and enter the IP address of the Local Area Network (LAN) port. The default IP address is 192.168.11.1.
2. Enter your user name and password.
3. Click **Login**.

The default user name and password are both "*admin*".

For security, change the user name and password the first time you log in.

8.5.3 Configure Basic Settings for the AG4104/AG4108 Gateway

Configure the Mitel AG4104/AG4108 gateway network and SIP server settings for use with OpenScape 4000.

1. Click **Quick Setup Wizard**.
2. On the **Setup Wizard - Local Network** page that opens, if needed, select **Separation** from the **WAN Dual Mode** drop-down list.
3. Under **Network Configuration**, do the following:
   a. Select the **Use the following IP address** option.
   b. Enter the **IP Address** to use for accessing the gateway on your network. The IP address must be in the same subnet as OpenScape 4000.
   c. Enter the **Subnet Mask** and **Default Gateway**.
4. Under **Manage Address**, do the following:
   a. Enter 192.168.11.1 in the **IP Address** field.
   b. Enter 255.255.255.0 in the **Subnet Mask** field.
5. Under **DNS Server**, do the following:
   a. Select the **Use the following DNS Server address** option.

b. Enter the **Primary DNS Server** address. This value should match the DNS address used by OpenScape 4000.

6. Click **Save and Next**.

   See Local Network on page 48 for field details.

7. On the **Setup Wizard - SIP Server** page that opens, enter the OpenScape 4000 gateway's Internet Protocol (IP) address in the **SIP Server** field.

   See SIP Server on page 56 for field details.

8. Click **Next**.
9. On the **Setup Wizard - Port** page that opens, click **Next**.
10. Click **Complete**.
11. If needed, go to the **SIP Server** tab.
    a. Select either **UDP/TCP** or **TLS** in the **SIP Transport Type** field.
       i. Enter 5060 in the **SIP UDP/TCP Local Port** field.
       ii. Enter 5061 in the **SIP TLS Local Port** field.
    b. Click **Save**.
12. Click **Save**.

8.5.4 Using the AG4104/AG4108 Management Port

The AG4104/AG4108 Management Port provides a useful way to reach the Web Management System when the customer's network Dynamic Host Configuration Protocol (DHCP) server is having problems and the AG4104/AG4108 depends on DHCP to obtain an Internet Protocol (IP) address.

The Management Port is a dedicated Ethernet port used specifically for accessing the Web Management System. It can be accessed only from a Personal Computer (PC) residing on the same subnet as the AG4104/AG4108.

If the Management Port has already been configured with a static IP address, you can still access the Web Management System through the Management Port even if the DHCP server fails.

To allow a PC to access the Web Management System through the Management Port, you must configure the AG4104/AG4108 correctly.

8.5.5 Configure TLS for the SIP Server

Configure the Mitel AG4104/AG4108 gateway to register SIP users over TLS with OpenScape 4000.

To register users over Transport Layer Security (TLS), set or verify the following:

1. On the Session Initiation Protocol (SIP) server, set the SIP server port to 5061 and set **SIP Transport Type** to **TLS**.

   See SIP Server on page 56 for field details.

2. On the **Certificate Manage** page, upload the **SIP CA Certificate** and **SIP Client Certificate**.

   See Certificate Management on page 113 for the certificate upload procedures.

3. To register clients, on the **Port** configuration page, enter the **Authenticate ID** and **Authenticate Password**. An empty ID or password is not supported.

   See Port on page 67 for field details.

Compliances 9

This chapter contains the following section(s):

- Configure the AG for Australian Regulatory Compliance

Lists the regulatory compliance standards the AG4124/AG4172 Analog Gateway meets.

The Mitel AG4124 and AG4172 Analog Gateways comply with the following regulations:
- All applicable European CE marking directives
- NRTL certification for distribution in North America
- FCC Part 15 and Part 68 and ISED equivalents

Note: For more information, see Mitel Regulatory Declarations.

9.1 Configure the AG for Australian Regulatory Compliance

Configure the Analog Gateway to comply with Australian regulatory requirements.

To configure the AG for Australian regulatory compliance:

Note:
- This appendix is only for the users in Australia.
- This section describes only the mandatory parameter configuration.
- Configure the other parameters either using default values or the site specific values.

1. Log in to the AG Web Management System.
2. Navigate to the **Advanced > FXS Parameter**.
   a. On **Detect Hook Flash**, set **Min Time** as **20**.
   b. Set **SLIC Setting** as **220 Ohm +(820 Ohm || 120nF)**.
   c. Click **Save**.
3. Navigate to the **Advanced > Line Parameter**.
   a. Set **Call Progress Tone** as **AUSTRALIA**.
   b. Set **Config Mode(Gain)** as **Advanced** and configure the following parameters:
      i. Set **Tx Gain(IP->PSTN)** as **-6dB**.
      ii. Set **Rx Gain(PSTN->IP)** as **-1dB**.
      iii. Set **DSP Tx Gain(IP->PSTN)** as **+4dB**.
      iv. Set **DSP Rx Gain(PSTN->IP)** as **-4dB**.
   c. Click **Save**.
4. Navigate to the **Advanced > Media Parameter**.
   a. Add only the following entry in **Preferred Vocoder**:

i. **Coder Name** as **G.711U**, **Payload Type** as **8**, and **Packetization Time** as **20**. Keep other parameters as default or site specific values.

> **Note**: Delete other entries if already present.

ii. Click **Save**.

5. Perform the following procedure in the command line interface.
   a. Log in to the command line interface using the following credentials.
      - **User name:** admin
      - **Password:** admin@123#
   b. Enter the following commands.

```
enable
```

```
aos
```

   c. Log in again using the credentials used to log in to the AG41x Web Management System to enter shell mode.
   d. Enter the following commands.

```
enable
```

```
dsp
```

   e. Press **Enter** to move to the **DSP signal test mode** parameter.
   f. Set **DSP signal test mode** value to **2** (CLEARMODE).
   g. After updating the value, keep pressing **Enter** (leaving other parameters at their default values) until you reach the **Apply the modified configuration (Y/N)** prompt.
   h. Type **Y** and press **Enter** to save the changes.
   i. Restart the AG system to complete the configuration.

Glossary 10

This chapter contains the following section(s):

- Media Access Control (MAC)
- MiVoice Border Gateway (MBG)
- Message Digest Algorithm 5 (MD5)
- Music on Hold (MOH)
- Maximum Transmission Unit (MTU)
- Message Waiting Indicator (MWI)
- Network Address Translation (NAT)
- Network Time Protocol (NTP)
- Object Identifier (OID)
- Private Branch Exchange (PBX)
- Personal Computer (PC)
- Packet Capture (PCAP)
- Pulse Code Modulation (PCM)
- Protected Extensible Authentication Protocol (PEAP)
- Plug and Play (PNP)
- Provisional Response Acknowledgement (PRACK)
- Public Switched Telephone Network (PSTN)
- Remote Authentication Dial-in User Service (RADIUS)
- Random Access Memory (RAM)
- Request for Comments (RFC)
- Real-Time Transport Protocol (RTP)
- Session Description Protocol (SDP)
- Session Initiation Protocol (SIP)
- Secure SIP (SIP Over TLS) (SIPS)
- Subscriber Line Interface Circuit (SLIC)
- Station Message Detail Recording (SMDR)
- Simple Network Management Protocol (SNMP)
- Secure Real-Time Transport Protocol (SRTP)
- Service (As in a DNS SRV Record) (SRV)
- Secure Shell (SSH)
- Secure Sockets Layer (SSL)
- Session Traversal Utilities for NAT (STUN)
- Transmission Control Protocol (TCP)
- Time-Division Multiplexing (TDM)
- Trivial File Transfer Protocol (TFTP)
- Transport Layer Security (TLS)
- Technical Report 069 (CPE WAN Management Protocol) (TR-069)
- User Agent (UA)
- User Datagram Protocol (UDP)
- User Interface (UI)
- Uniform Resource Identifier (URI)
- Uniform Resource Locator (URL)
- Unshielded Twisted Pair (UTP)
- Vendor Class Identifier (VCI)
- Virtual Local Area Network (VLAN)

- Virtual Private Network (VPN)
- Wide Area Network (WAN)

10.1 Access Control List (ACL)

A list of rules that permits or denies network traffic based on criteria such as source IP address or protocol. The Analog Gateway uses ACLs to restrict access to management interfaces such as Telnet or the web interface.

10.2 Auto Configuration Server (ACS)

A server that uses TR-069 to remotely provision and manage devices such as the Analog Gateway.

10.3 Advanced Encryption Standard (AES)

A widely used symmetric encryption algorithm, used in this guide for securing voice and signaling traffic, such as SRTP media encryption.

10.4 Address Resolution Protocol (ARP)

A protocol that resolves an IP address to the physical (MAC) address of a device on the same LAN.

10.5 Automatic Route Selection (ARS)

A PBX feature that automatically selects the most appropriate outbound route for a call based on the dialed digits and configured routing rules.

10.6 Certificate Authority (CA)

An entity that issues digital certificates used to establish trust in TLS/SSL connections. The Analog Gateway trusts a Certificate Authority's root certificate to validate the identity of servers it connects to.

10.7 Call Detail Record (CDR)

A record generated for each call, containing details such as calling and called numbers, start time, and duration.

10.8 Called Station Identification (Fax Answer Tone) (CED)

The distinctive tone a fax machine sends after answering a call, which senders and gateways use to detect that a fax session is starting.

10.9 Caller ID (CID)

A service that delivers the calling party's number, and often name, to the called party before or during call setup.

10.10 Calling Line Identification (CLI)

The information, typically a phone number, that identifies the calling party; closely related to Caller ID.

10.11 Calling Tone (Fax Calling Signal) (CNG)

The distinctive tone a fax machine sends when placing a call, signaling to the receiving end that a fax transmission is being attempted.

10.12 Class of Service (COS)

A set of permissions and restrictions, such as which types of calls a line is allowed to make, assigned to a line or device.

10.13 Customer Premises Equipment (CPE)

Telecommunications equipment located at the customer's site rather than at the service provider's facility; the Analog Gateway is an example of CPE.

10.14 Comma-Separated Values (CSV)

A plain-text file format that stores tabular data with commas separating fields, used for importing or exporting configuration data such as port settings.

10.15 Dynamic Host Configuration Protocol (DHCP)

A protocol that automatically assigns IP addresses and other network settings to devices when they join a network. The Analog Gateway can obtain its network configuration from a DHCP server.

10.16 Do Not Disturb (DND)

A phone or PBX feature that suppresses incoming call alerts, typically sending calls straight to voicemail or a busy signal.

10.17 Domain Name System (DNS)

The system that translates domain names, such as a SIP server's hostname, into IP addresses.

10.18 Differentiated Services Code Point (DSCP)

A field in the IP header used to mark packets for a particular class of Quality of Service treatment, such as prioritizing voice traffic.

10.19 Digital Signal Processor (DSP)

A specialized processor that handles real-time audio processing tasks, such as voice encoding, echo cancellation, and tone detection, on the Analog Gateway.

10.20 Dual-Tone Multi-Frequency (DTMF)

The tone signaling standard used for telephone keypad input, such as entering a mailbox password after a call is answered.

10.21 Data Terminal Unit (DTU)

A hardware module on certain Analog Gateway models responsible for specific data-handling functions; DTU firmware is upgraded separately from the main system firmware.

10.22 Extensible Authentication Protocol (EAP)

A framework that supports multiple authentication methods for network access, often used together with 802.1X.

10.23 Error Correction Mode (ECM)

A fax transmission mode that detects and retransmits corrupted data, improving reliability over noisy connections.

10.24 Feature Access Code (FAC)

A short digit sequence dialed from a phone to activate a PBX feature, such as call park, retrieve, or Do Not Disturb.

10.25 Fully Qualified Domain Name (FQDN)

A complete domain name that specifies a host's exact location in the DNS hierarchy, such as sipserver.example.com, as opposed to a bare IP address.

10.26 Frequency-Shift Keying (FSK)

A modulation method that encodes digital data as changes in frequency; used, for example, to deliver Caller ID information over an analog line.

10.27 Foreign Exchange Office (FXO)

An analog interface that connects to a telephone line the way an analog telephone does, allowing a device to place or receive calls over the public telephone network or a PBX trunk.

10.28 Foreign Exchange Station (FXS)

An analog interface on the Analog Gateway that supplies dial tone, ring voltage, and battery current to a connected analog device, such as a telephone or fax machine, the same way a telephone company central office would.

10.29 Generic Requirement 909 (Telcordia Loop-Test Standard) (GR-909)

A Telcordia (now iconectiv) test standard for verifying the electrical condition of analog telephone lines, such as loop resistance and voltage.

10.30 Graphical User Interface (GUI)

A visual, typically browser-based interface for configuring and monitoring a device, such as the Analog Gateway's Web Management System.

10.31 Gateway (GW)

A device that connects two different types of networks or media, such as the Analog Gateway, which connects analog telephone devices to an IP-based SIP network.

10.32 HFA

A Mitel-proprietary IP endpoint signaling mode used for call handling between the Analog Gateway and MiVoice Business. The source documentation for this guide does not spell out what the letters stand for, and no independently verifiable expansion was found, so this guide uses HFA as a name rather than an expandable acronym.

10.33 Hypertext Transfer Protocol (HTTP)

The protocol used to transfer web pages and other resources; used by the Web Management System when accessed without encryption.

10.34 Hypertext Transfer Protocol Secure (HTTPS)

HTTP secured with TLS/SSL encryption. The Web Management System uses HTTPS by default for enhanced security.

10.35 Integrated Communications Platform (ICP)

A Mitel PBX platform, such as the 3300 ICP, that provides call control and telephony features. The MiVoice Border Gateway uses the term ICP to refer to the systems it connects to.

10.36 IP Multimedia Public Identity (IMPU)

A public identity, such as a SIP URI, used to identify a user within an IP Multimedia Subsystem (IMS) network.

10.37 Internet Protocol (IP)

The network-layer protocol that routes data packets between devices on a network using IP addresses. Nearly every service on the Analog Gateway, including SIP signaling and voice media, is carried over IP.

10.38 Layer 2 (Data Link Layer) (L2)

The data-link layer of the OSI networking model, responsible for node-to-node data transfer using addresses such as MAC addresses; Ethernet switching operates at Layer 2.

10.39 Layer 3 (Network Layer) (L3)

The network layer of the OSI networking model, responsible for routing packets between networks using IP addresses.

10.40 Local Area Network (LAN)

A network that connects devices within a limited area, such as an office or building. The Analog Gateway connects to a LAN to reach the SIP server, PBX, or Web Management System.

10.41 Media Access Control (MAC)

A hardware address that uniquely identifies a network interface, used for addressing at the data-link layer and often as a device identifier.

10.42 MiVoice Border Gateway (MBG)

A Mitel product that provides secure remote (teleworker) connectivity and session border control between endpoints, such as the Analog Gateway, and MiVoice Business.

10.43 Message Digest Algorithm 5 (MD5)

A cryptographic hash function historically used for password storage and integrity checks; considered weak for security-critical uses today but still referenced in some legacy authentication schemes.

10.44 Music on Hold (MOH)

Audio played to a caller who has been placed on hold.

10.45 Maximum Transmission Unit (MTU)

The largest packet size, in bytes, that a network link can carry without fragmentation.

10.46 Message Waiting Indicator (MWI)

A notification, typically a stutter dial tone or a lamp, that tells a user a voicemail message is waiting.

10.47 Network Address Translation (NAT)

A technique that maps private IP addresses to a public IP address (or vice versa) as traffic crosses a network boundary. NAT settings on the Analog Gateway affect how its SIP messages report addresses to devices on the other side of a firewall or router.

10.48 Network Time Protocol (NTP)

A protocol used to synchronize a device's clock with a reference time source over a network.

10.49 Object Identifier (OID)

A globally unique identifier used in SNMP and other protocols to name a specific object or data element in a structured hierarchy.

10.50 Private Branch Exchange (PBX)

A telephone switching system used within an organization to route calls between internal extensions and to outside lines. MiVoice Business, MiVoice MX-ONE, MiVoice 5000, OpenScape Business, and OpenScape 4000 are all examples of PBX systems the Analog Gateway can connect to.

10.51 Personal Computer (PC)

A general-purpose computer, referenced in this guide chiefly as the device used to connect to and manage the Analog Gateway.

10.52 Packet Capture (PCAP)

A file format and technique for recording network traffic for later analysis, used when troubleshooting the Analog Gateway.

10.53 Pulse Code Modulation (PCM)

A method of digitally representing an analog voice signal by sampling its amplitude at regular intervals.

10.54 Protected Extensible Authentication Protocol (PEAP)

An authentication protocol that encapsulates EAP within an encrypted and authenticated TLS tunnel, used for network access authentication such as 802.1X.

10.55 Plug and Play (PNP)

A mechanism that lets a device automatically discover its configuration server and download its configuration when it first connects to the network.

10.56 Provisional Response Acknowledgement (PRACK)

A SIP method (defined in RFC 3262) used to reliably acknowledge provisional (1xx) responses during call setup.

10.57 Public Switched Telephone Network (PSTN)

The traditional circuit-switched telephone network. Analog devices connected to the Analog Gateway's FXS ports typically place calls that ultimately reach the PSTN through a SIP trunk or PBX.

10.58 Remote Authentication Dial-in User Service (RADIUS)

A protocol for centralized authentication, authorization, and accounting, which the Analog Gateway can use to authenticate administrative logins against a central server.

10.59 Random Access Memory (RAM)

The volatile memory a device uses to run its operating software; distinct from the persistent flash storage that holds firmware.

10.60 Request for Comments (RFC)

A publication from the Internet Engineering Task Force (and, for some numbers, other standards bodies) that defines an internet protocol or standard, such as RFC 3261 for SIP.

10.61 Real-Time Transport Protocol (RTP)

A protocol used to carry voice and other real-time media over an IP network. SIP negotiates the connection; RTP carries the actual voice stream.

10.62 Session Description Protocol (SDP)

A format used within SIP messages to describe media sessions, such as the codecs, IP addresses, and ports to use for a call's voice stream.

10.63 Session Initiation Protocol (SIP)

An application-layer signaling protocol used to establish, modify, and terminate real-time communication sessions, such as voice calls, between devices on an IP network. The Analog Gateway uses SIP to register its ports with, and exchange call-control signaling with, a connected PBX, session border controller, or gateway.

10.64 Secure SIP (SIP Over TLS) (SIPS)

A SIP URI scheme that indicates SIP signaling must be carried over an encrypted transport such as TLS.

10.65 Subscriber Line Interface Circuit (SLIC)

The electronic circuit that provides the electrical interface, such as ring voltage and battery current, between an FXS port and an analog telephone line.

10.66 Station Message Detail Recording (SMDR)

A record of call activity, such as originating extension, time, duration, and number dialed, used to track usage and deter toll abuse.

10.67 Simple Network Management Protocol (SNMP)

A protocol used by network management systems to monitor and, in some cases, configure network devices.

10.68 Secure Real-Time Transport Protocol (SRTP)

An encrypted version of RTP that protects voice media from eavesdropping and tampering.

10.69 Service (As in a DNS SRV Record) (SRV)

A DNS record type that specifies the hostname and port for a particular service, such as a SIP server, allowing a client to discover it automatically.

10.70 Secure Shell (SSH)

An encrypted protocol for secure remote command-line access to a device.

10.71 Secure Sockets Layer (SSL)

The predecessor to TLS; a protocol that encrypts data sent over a network connection. The term is still used in some interfaces and documentation even where TLS is the protocol actually in use.

10.72 Session Traversal Utilities for NAT (STUN)

A protocol that helps a device discover its public IP address and the type of NAT it is behind, used to assist with NAT traversal for SIP and media traffic.

10.73 Transmission Control Protocol (TCP)

A connection-oriented transport protocol that guarantees ordered, reliable delivery of data. Some Analog Gateway services, including certain SIP transport modes, can use TCP.

10.74 Time-Division Multiplexing (TDM)

A method of carrying multiple signals over a single channel by allocating each signal a recurring time slot, used in traditional PBX and telephone network trunking.

10.75 Trivial File Transfer Protocol (TFTP)

A simple file transfer protocol, sometimes used to distribute firmware or configuration files to network devices.

10.76 Transport Layer Security (TLS)

A cryptographic protocol that encrypts and authenticates data sent over a network connection. The Analog Gateway can use TLS to secure SIP signaling between itself and a PBX or gateway.

10.77 Technical Report 069 (CPE WAN Management Protocol) (TR-069)

A Broadband Forum standard that defines a protocol for remote management of customer-premises devices by an Auto Configuration Server.

10.78 User Agent (UA)

A SIP endpoint, such as the Analog Gateway or a SIP phone, that originates or terminates SIP signaling on behalf of a user.

10.79 User Datagram Protocol (UDP)

A lightweight, connectionless transport protocol. SIP and RTP can both be carried over UDP, which offers lower overhead than TCP but no built-in reliability or ordering.

10.80 User Interface (UI)

The means by which a user interacts with a device, such as the Analog Gateway's web-based User Interface.

10.81 Uniform Resource Identifier (URI)

A string that identifies a resource; a SIP address (such as a phone number or username at a domain) is expressed as a URI.

10.82 Uniform Resource Locator (URL)

The address used to locate a resource, such as a firmware image or a web page, typically over HTTP or HTTPS.

10.83 Unshielded Twisted Pair (UTP)

A common type of copper network cable, such as Category 5e or 6, used to connect the Analog Gateway to a LAN.

10.84 Vendor Class Identifier (VCI)

An optional DHCP field that identifies the vendor or type of a requesting device, which a DHCP server can use to apply vendor-specific configuration.

10.85 Virtual Local Area Network (VLAN)

A logical subdivision of a physical network that isolates traffic, such as voice traffic, from other traffic on the same physical LAN.

10.86 Virtual Private Network (VPN)

An encrypted network connection that extends a private network across a public network, used in this guide chiefly for secure remote administration.

10.87 Wide Area Network (WAN)

A network that spans a larger geographic area than a LAN, typically connecting multiple sites or connecting a site to the internet.