AG4124 (MiVoice 5000) – Personal Data Protection and Privacy Controls

AG4124 Analog Gateway Firmware Release 33.83.11.25

Version 1.1

November 2023

NOTICE

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.

Trademarks

Contents

List of Tables

1 Introduction

1.1 Overview

This document is one in a series of product specific documents that discuss the product security controls and features available on Mitel products.

This particular document will be of interest to AG4124 Analog Gateway and MiVoice 5000 customers that are putting security processes and security controls in place to comply with data security regulations.

This document is intended to assist Mitel AG4124 Analog Gateway and MiVoice 5000 customers with their data security regulations compliance initiatives by:

- Identifying the types of personal data that are processed by the AG4124 Analog Gateway
- Listing the AG4124 Analog Gateway Security Features that customers may require to achieve compliance with security regulations
- Providing a description of the AG4124 Analog Gateway Security Features
- Providing information on where the AG4124 Analog Gateway Security Features are documented

This document is not intended to be a comprehensive product specific security guideline. For information on product security guidelines, product engineering guidelines or technical papers, refer to Mitel's Web Site.

1.2 AG4124 Analog Gateway and MiVoice 5000 Relationship

When the AG4124 Analog Gateway is deployed in conjunction with the MiVoice 5000 management, provisioning of the AG4124 is under the control of the MiVoice 5000. While the AG4124 does support a simple integral call control capability, it is not used. The MiVoice 5000 call control engine is responsible for all call control functions.

The MiVoice 5000 establishes a secure SNMP communication channel with the AG4124 and configures the required AG4124 Web Interface forms. The only personal data transferred from the MiVoice 5000 to the AG4124 are the end user's names and phone numbers.

This document should be used in conjunction with the MiVoice 5000 – Personal Data Protection and Privacy Controls, which can be found on the Mitel Document Center.

1.3 What is New in this Release

Release 33.83.11.25 is the initial release of the AG4124 Analog Gateway.

This is the second version of this document; it has been updated to clarify that this document is only applicable to the AG4124 when the AG4124 is used in conjunction with the MiVoice 5000.

2 Personal Data Collected by the AG4124 Analog Gateway

The AG4124 Analog Gateway is an on-premise offering. The AG4124 Analog Gateway processes only personal data that is required for the delivery of communication services including call control, billing services, and technical support services. There are no end-user opt-in consent mechanisms implemented in the AG4124 Analog Gateway.

During the course of installation, provisioning, operation, and maintenance, the AG4124 Analog Gateway **collects** data related to several types of users, including:

- End users of the AG4124 Analog Gateway, typically Mitel customer employees using Mitel SIP phones, 3rd Party SIP phones and collaboration tools.
- Customers of Mitel customers – for example, call detail recordings (CDR) contain personal content of both parties in the phone call or Fax call.
- System administrators and technical support personnel – Logs and audit trails contain records of the activities of system administrators and technical support personnel.

3 Personal Data Processed by the AG4124 Analog Gateway

The AG4124 Analog Gateway **processes** the following types of data:

- **Provisioning Data:**
  - The end user's name and phone number.
- **Maintenance, Administration, and Technical Support Activity Records:**
  - System and content backups, logs, and audit trails.

Personal data processed by the AG4124 Analog Gateway is required for the delivery of communication services, technical support services or other customer business interests.

There are no end-user opt-in consent mechanisms implemented in the AG4124 Analog Gateway.

4 Personal Data Transferred by the AG4124 Analog Gateway

The types of **personal data transferred** among the AG4124 Analog Gateway and various applications, and services will depend on the specific use requirements of those applications or services, for example:

- Provisioning data, end user's name and end user's phone number
- Maintenance, administration, and technical support activity records, such as system and content backups, logs, and audit trails.

5 How the Security Features Relate to Data Security Regulations

The AG4124 Analog Gateway provides security-related features which allow customers to secure user data and telecommunications data and to prevent unauthorized access to the user's data

Table 1 summaries the security features Mitel customers can use when implementing both customer policy and technical and organizational measures which the customer may require to achieve compliance with data security regulations.

Table 1: The AG4124 Analog Gateway Security Features which customers may require to achieve Compliance with Data Security Regulations.

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
System and Data Protection, Identity and Authentication	Access to personal data is limited with administrative controls on accounts for both personnel and Application Programming Interfaces. Access to the system is limited by allowing only authorized access that is authenticated using a username and password login combination. **WEB Interface** Access to the WEB Interface can be controlled via Access Control Lists supported within the AG4124. The Web Interface supports Role Based Access: • Administrator: Full Access • User: User Files. • Guest: Read Only. The Web Interface has an Inactivity Timer with a default time of 5 minutes. The Web Interface supports access logs. The Web Interface will lock out a user after 5 failed login attempts. The Web Interface password is encrypted with 256 bit AES and stored with the configuration file. Communications to the system are performed over authenticated, encrypted communications channels using HTTPS TLS 1.2. Access to the Telnet Interface can be controlled via Access Control Lists supported within the AG4124. A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists (ACLs) and firewalls. In all cases, physical access to systems should be restricted by the customer.	AG4124 Analog Gateway Administration Guide. Mitel AG4124 Analog Gateway Quick Installation Guide. AG4124 Analog Gateway Security Guidelines.

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
Communications Protection	Most personal data transmissions use secure channels. Channels that are not secured can be disabled by the Administrator. For system integrity and reliability, all provisioning interfaces use secure channels (TLS 1.2) Analog FXS interfaces do not support encryption. Analog Fax, T.30 G.711 pass through Fax and T.38 Fax do not support encryption. For system integrity and reliability, all provisioning interfaces use secure channels (TLS 1.2)	AG4124 Analog Gateway Administration Guide. Mitel AG4124 Analog Gateway Quick Installation Guide. AG4124 Analog Gateway Security Guidelines.
Access and Authorization	All personal data processing is protected with access and authorization controls, this includes personal data processing by data subjects, Administrators, technical support, and machine APIs. All system data processing and all access to databases, files, and operating systems, are protected with access and authorization controls.	AG4124 Analog Gateway Administration Guide. Mitel AG4124 Analog Gateway Quick Installation Guide. AG4124 Analog Gateway Security Guidelines.
Data Deletion	The system provides an administrator with the ability to erase the end user's personal data. Deleting personal data from the AG4124 is accomplished from the MiVoice 5000 administration tool.	MiVoice 5000 Operating Manual, MiVoice 5000 Manager Operating Manual. MiVoice 5000 User Portal – User Manual MiVoice 5000 Product Guide – Chapter 14 – Security.
Audit	Audit trails are supported to maintain records of log in activities. Call Data Records are managed and stored in the MiVoice 5000 system and can be accessed only by the administrator or by trusted applications.	AG4124 Analog Gateway Security Guidelines. MiVoice 5000 Operating Manual, MiVoice 5000 Manager Operating Manual.
End Customer Guidelines	AG4124 Analog Gateway Security Guidelines are available to assist with securing and maintaining security of the AG4124.	

6 Data Security Regulations

This section provides an overview of the security regulations that <Product Name> customers may need to be compliant with.

6.1 The European Union General Data Protection Regulation (GDPR)

The European Union (EU) General Data Protection Regulation (GDPR) effective on 25 May 2018 replaces the previous EU Data Protection Directive 95/46/EC.

The intent of GDPR is to harmonize data privacy laws across Europe so that the data privacy of EU citizens can be ensured. GDPR requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. GDPR also addresses the export of personal data outside of the EU. Any business that processes personal information about EU citizens within the EU must ensure that they comply with GDPR. Under GDPR, 'processes personal information' means any operation performed on personal data, such as collecting, recording, erasing, usage, transmitting, and disseminating.

6.1.1 What do Businesses need to know about GDPR?

GDPR applies to businesses with a presence in any EU country, and, in certain circumstances, to businesses that process personal data of EU residents even if the businesses have no presence in any EU country.

In order to achieve GDPR compliance, businesses must understand what personal data is being processed within their organization and ensure that appropriate technical and organizational measures are used to appropriately safeguard such data. Table 1 explains what personal data is processed by Mitel's AG4124 Analog Gateway and highlights available security features to safeguard such data.

7 Product Security Information

7.1 Mitel Product Security Vulnerabilities

The Product Security Policy discusses how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how the reporting of security vulnerabilities is performed.

Mitel's Product Security Policy is available at:
https://www.mitel.com/support/security-advisories/mitel-product-security-policy

7.2 Mitel Product Security Advisories

Mitel Product Security Advisories are available at:
https://www.mitel.com/support/security-advisories

7.3 Mitel Security Documentation

Mitel security documentation includes product specific; Security Guidelines, Important Information for Customer GDPR Compliance Initiatives and Data Protection and Privacy Controls. Mitel also has Technical Papers and White papers that discuss network security and data centre security.

Mitel Product Security Documentation is available at:
https://www.mitel.com/en-ca/document-center

8 Disclaimer

THIS SOLUTIONS ENGINEERING DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY. IN NO EVENT WILL MITEL NETWORKS CORPORATION OR ITS AFFILIATES HAVE ANY LIABILITY WHATSOEVER ARISING FROM IN CONNECTION WITH THIS DOCUMENT. You acknowledge and agree that you are solely responsible to comply with any and all laws and regulations in association with your use of the AG4124 Analog Gateway and/or other Mitel products and solutions including without limitation, laws and regulations related to call recording and data privacy. The information contained in this document is not, and should not be construed as, legal advice. Should further analysis or explanation of the subject matter be required, please contact an attorney.