MiVoice Business

RELEASE 10.2
VERSION 1.1

SECURITY GUIDELINES

Mitel®

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 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

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) or its 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.

MiVoice Business
Security Guidelines
Release 10.2
Version 1.1
December 2024

List of Figures

List of Tables

Overview

This document will be of interest to personnel responsible for ensuring the secure deployment and operation of the MiVoice Business (MiVoice Business) system.

Every organization must have a clearly defined IT security policy that defines goals, assets, trust levels, processes, incident handling procedures, and so on. This policy must cover and deploy the security mechanisms available in the MiVoice Business solution.

Security is an integral part of the MiVoice Business system design. This document describes the MiVoice Business security features and provides recommendations on how the administrator should configure them to ensure a secure MiVoice Business deployment.

The MiVoice Business security features are either enabled by default, enabled during the installation/configuration phase, or need to be enabled manually by the system administrator when the MiVoice Business system is initialized.

The MiVoice Business system security measures are mainly based on the following open standard technologies and access mechanisms:

- TLS – Transport Layer Security (TLS) provides secure access to IP phones and secure signaling between IP phones and MiVoice Business Service Nodes. The Transport Layer Security (TLS) provides secure web access to MiVoice Business Service Nodes.
- SSH - Secure Shell (SSH) provides secure console-based access to IP phones and the MiVoice Business System Administration and configuration tools.
- SRTP - Secure Real-time Transport Protocol (SRTP) protects the voice media streams between IP phones and between IP phones and the MiVoice Business.
- Correct identity and access management policies configuration to ensure all end user and administrator accounts, roles, permissions, and password policies.
- OAuth2.0 (Open Authorization) may be used by voice mail to authenticate with other email applications such as Google Apps and Microsoft Office 365.

Other mechanisms that can be employed to protect the MiVoice Business system are based on the following:

- A securely designed corporate Local Area Network (LAN) infrastructure
- Configuration of internal and external public-facing routers and firewalls

In addition to the security recommendations described in this document, several general security aspects need to be covered and addressed by the system administrator and/or the Information Technology (IT) security officer.

An important security measure is to establish and maintain physical security. Only authorized personnel should have access to server locations because many data-exposure attacks can be mounted by unauthorized persons having physical access to a host. Further, the IT data infrastructure must be designed with security in mind, security mechanisms and protocols must be enabled, and all components of the whole system must be correctly configured, maintained, and updated as necessary.

About the MiVoice Business Documentation Set

Documents for MiVoice Business and other Mitel® products are available on the Mitel Document Center web site.

https://www.mitel.com/document-center

The following guides provide complete information about the MiVoice Business:

- *Technician's Handbook:* Installation, upgrade, maintenance, troubleshooting instructions.
- *Hardware Technical Reference Manual*: Hardware specifications.
- *System Administration Tool Help for MiVoice Business:* Programming, maintenance, and troubleshooting.
- MiVoice Business *Resiliency* Guide: This guide provides an overview of the Mitel Resilience solution and the tools to understand, plan, and implement a resilient network.
- *General Information Guide*: General product overview, including deployments, architecture, products, and features.
- *Safety Instructions*: To be read BEFORE installation.
- *Clustering Design and Implementation* (Download document and associated .xls files)): This is a Cluster planning and installation guide for migrating to and using SDS sharing and multi-node Management.
- *Site Planning Guide*: Product installation checklist.
- *Knowledge-Based Article SO4819 - How to enable TLS 1.2 only for MiVB 9.1 Nov 25, 2019*

The following additional information can be found on the powerup.mitel.com website:

- MiVoice Business Controllers Datasheet: Platform capability list.
- Current Product Briefs: Notes on current releases

The following documentation related to comparing and selecting IP phones and peripherals is available on the Mitel Document Center website:

- *Mitel IP Desktop Phones and Peripherals Feature Matrix*
- *Mitel IP Desktop Phones and Peripherals Brochure*
- *IP Desktop FAQ*
- *IP Phone Product Briefs*
- *Product Bulletins*

The following tools related to calculating network powering requirements for IP phones are available:

- *MiVoice Business System Engineering Tool* - located on the powerup.mitel.com website.
- *Mitel Streamline Power Calculator* - located on *the Mitel Document Center website.*

The following documentation is related to deploying IP phones and can be found on the Mitel Document Center website:

- *Mitel IP Sets Engineering Guidelines*
- *Network Engineering for IP Telephony*
- *Wireless Telephony, Planning and Troubleshooting*
- *Ethernet Twisted Pair Cabling Plant, Power, and Grounding Guidelines*

The following document discusses security and toll fraud prevention:

- *Security Toll Fraud and Installation Checklist - EM004472*

The following documents address network and product security:

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

New for this Release

The following security-related changes are included in Release 10.2:

- The EoS components are partially addressed

System Architecture

Mitel® MiVoice Business (MiVoice Business) is the brand name of the call manager software solution. The MiVoice Business solution can be deployed on industry standard servers, in a virtualized computing environment, or on Mitel's SMB Controller or EX Platform.

The MiVoice Business solution delivers sophisticated call management applications and desktop solutions to businesses. The MiVoice Business solution delivers a highly scalable, resilient, and robust call control that fully utilizes the power of IP. The MiVoice Business solution can employ hardware appliances or SIP Gateways to support traditional TDM-based telephony for legacy devices and PSTN connectivity.

MiVoice Business hardware appliances, such as the EX or SMBC, use the IP network to connect IP telephony devices and provides a supplementary TDM (time division multiplexing) subsystem to switch calls between traditional telephone devices. They have the advantage of being able to optimally switch both types of traffic; IP or TDM and provide native call setup, tear down, and signaling between Ethernet IP-connected telephones. For traditional telephony, such as POTS and PSTN trunks, call handling is also handled.

MiVoice Business Security Overview

The MiVoice Business solution has been designed with a security-by-design mindset; the MiVoice Business has security features that address identity, authentication, encryption, access, and authorization. MiVoice Business also supports audit trails, logs, and enterprise security certificates.

The MiVoice Business security features are configured via various management forms, which are accessed with the MiVoice Business System Administration Tool. The MiVoice Business System Administration Tool contains embedded help files with extensive search capabilities that will assist the administrator with forms configuration. The help files also contain documents that discuss maintenance procedures.

MiVoice Business Administration

The MiVoice Business provides personnel with following integral management tools:

- The System Administration Tool
- The Group Administration Tool (not available on all platforms)
- The Desktop Tool (not available on all platforms)

These three different management tools are provided in order to meet the needs of technicians, administrators, and the desktop telephony users themselves. Transport Layer Security protocol (TLS) is used to encrypt the data on the connection between the user's computer and the MiVoice Business management tools over TCP port 443 using the HTTPS protocol.

This document focuses on the forms available within the System Administration Tool that are related to the configuration of security features and mechanisms. The Group Administration Tool and the Desktop Tool forms are not discussed in this document. Details on these tools can be found in the *MiVoice Business System Administration Tool Help files*.

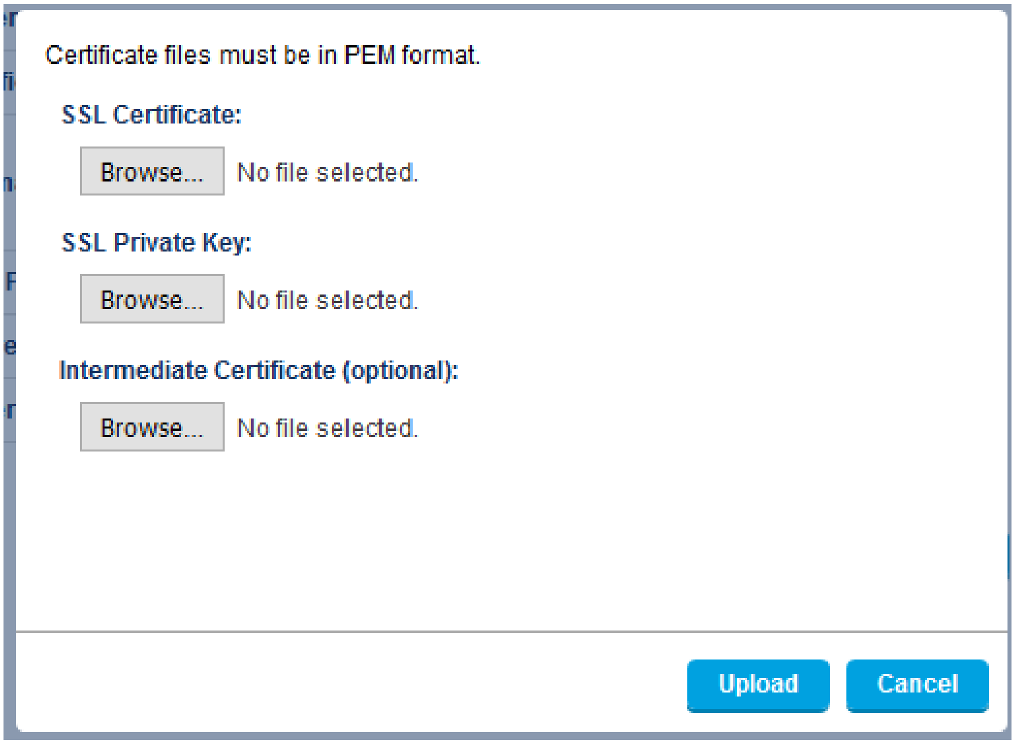
The System Administration Tool uses a browser-based interface. For details on supported browsers, PC requirements, and how to invoke the System Administration Tool, refer to the *System Administration Tool On-Line Help Files*.

The following sections of this document discuss the security-related forms that are used to configure the MiVoice Business security features that should be employed to help guard your system against unauthorized access and privacy violations.

Web Server Certificate

The MiVoice Business by default creates a self-signed certificate for authentication of the MiVoice Business system to web browsers. However, self-signed certificates are inherently untrusted by the web browser and a warning will be shown.
This can be mitigated by installing the self-signed certificate on the local computer or bypassed by making an exception.

Figure 1 Installing Certificates



Certificate files must be in PEM format.

SSL Certificate:

No file selected.

SSL Private Key:

No file selected.

Intermediate Certificate (optional):

No file selected.

The recommendation though is to install a certificate obtained from a Certificate Authority (CA) that the customer already owns (that is, an enterprise CA). The web browser will then trust the MiVoice Business access. Note that certificates do expire and therefore, the customer must be aware of the expiry date and renew it when needed.

Administration Encryption

The administration is accessed through HTTPS on TCP port 443, which must be allowed through any data network local access control list or firewall. MiVoice Business 9.1 and greater utilizes Transport Layer Security (TLS) version 1.x.

For Release 10.1, the system can be configured to support TLS 1.2 and TLS 1.3. If TLS 1.2 and TLS 1.3 are enabled on the MiVB, the MiVB will attempt to connect to the endpoint with TLS 1.3. If the endpoint does not support TLS 1.3, the MiVB will negotiate down to TLS 1.2 and attempt to communicate.

The following encryption modules for TLS 1.2 are available in the Cipher Suite of MiVoice Business 9.0 and greater.

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- AES256-GCM-SHA384
- AES256-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- AES128-GCM-SHA256
- AES128-SHA256

The following encryption modules for TLS 1.3 are available in the Cipher Suite of MiVoice Business 10.1 and greater.

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

In the unlikely situation of needing a cipher removed, contact Mitel Technical Support.

Identity and Authentication

To ensure privacy and maintain system integrity, access to the MiVoice Business is restricted by a login password to those users who can be identified and authenticated.

Users logging in to the System Administration Tool for the first time after installation must change the default password. The password strength and the user session inactivity timer are both configurable.

If a user fails to log in after three consecutive attempts, the event is recorded in the maintenance log, and the user is locked out of the system for a period of time.

The passwords used to log in to the MiVoice Business System Administration tool (or Embedded System Management tool (ESM)) are stored securely using strong encryption. The encryption mechanism used is OpenSSL's Advanced Encryption Standard - AES 256-bit encryption.

In the *MiVoice Business System Administration Tool*, the *System Security Management* Form is the form that is used to configure the following login password settings:

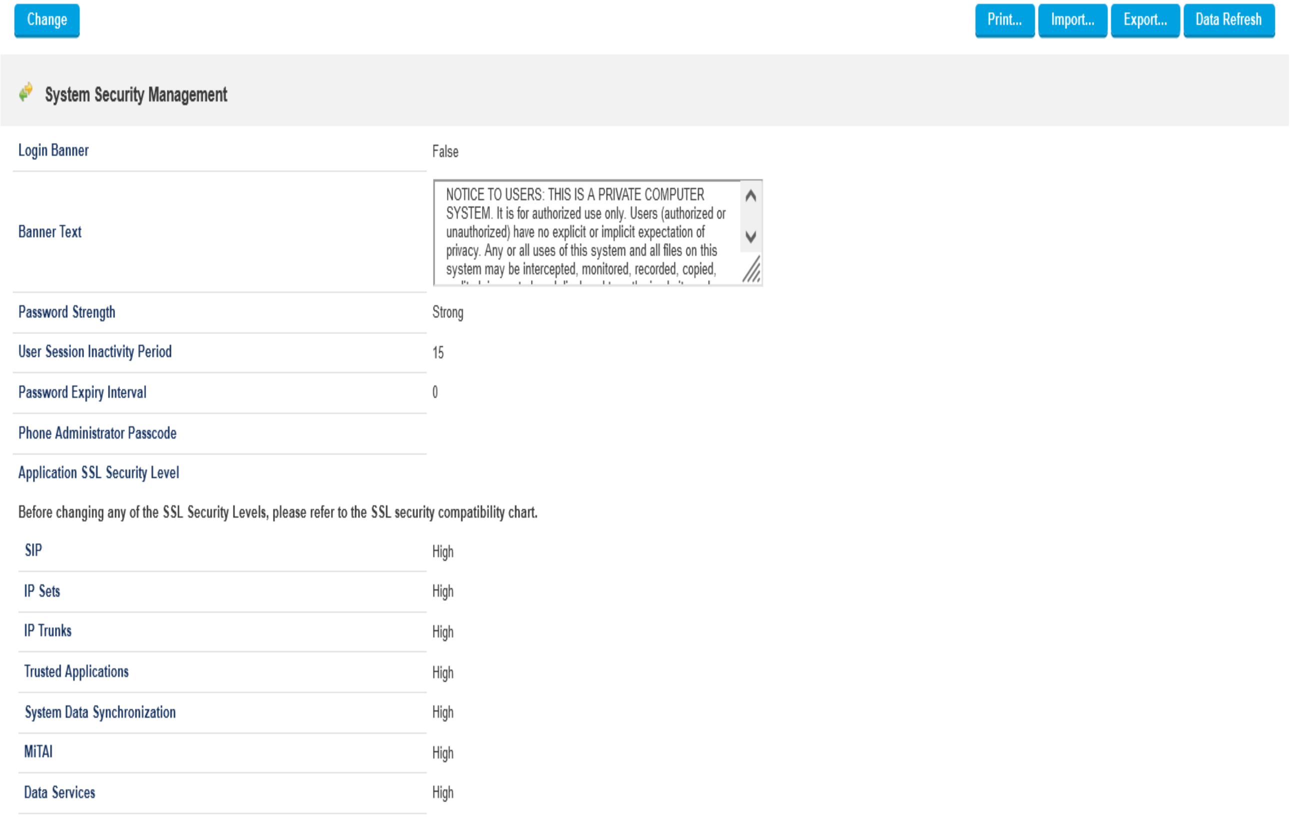
- Set/reset the password
- Establish the password strength rules
- Set the user session inactivity timer
- Set the password expiry interval
- Enable/disable the Login Banner
- Set the Phone Administrator's Password

System Security Management

The security features configured under the *System Security Management* form are described in the following sections. For additional details, refer to the MiVoice Business System Administration Tool Help files.

The following figure shows the new capability that supports the configuration of different TLS security levels.

Figure 2 TLS Security Levels



System Security Management

Login Banner	False
Banner Text	NOTICE TO USERS: THIS IS A PRIVATE COMPUTER SYSTEM. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied,
Password Strength	Strong
User Session Inactivity Period	15
Password Expiry Interval	0
Phone Administrator Passcode	
Application SSL Security Level	

Before changing any of the SSL Security Levels, please refer to the SSL security compatibility chart.

SIP	High
IP Sets	High
IP Trunks	High
Trusted Applications	High
System Data Synchronization	High
MiTAI	High
Data Services	High

Purpose

This form is used to set the strength of the password used to log in to the System Administration Tool and the duration of the session inactivity timer, which automatically logs out the user after a period of inactivity. It can also be used to configure a Login Banner to warn users against unauthorized system access or use.

As of Release 9.1 SP1, this form allows the Administrator to configure the TLS security level used by the applications and interfaces.

Conditions

The following conditions and rules are associated with the security settings found under the *System Security Management* form.

- Users will be forced to change the factory default password to a password of their choice.
- Forced password changes do not apply to Mitel Extensible Markup Language (MiXML), FTP, and the Real Time Controller (RTC) shell logins. Users can log in with the factory default password until it is changed from the System Administration Tool login page.
- A particular-strength password will also be valid on systems requiring lower-strength; a medium-strength password will also be valid on a "weak" system; a "strong" password will be valid on any system - regardless of the password strength setting.
- Logging in to the system using MiXML with the factory default password generates a security login/logout log.
- The number of consecutive failed login attempts allowed is hardcoded at three.
- The passwords in MiVB are now AES-encrypted

Login Banner

This setting determines whether users will be presented with a message warning against unauthorized system access or use. The message is displayed on the System Administration Tool home page and requires the user's acknowledgment (via an Accept button) before proceeding to the login page. It is displayed again on logout. The default setting is false, which means that no banner will be displayed.

Recommendation: It is recommended that a login banner is used. Actual text will come from the company’s security policy.

Password Strength

Determines the rules users must follow when creating a password, the default setting is for a weak password.

Recommendation: It is recommended that a strong password setting be used.

The basic rules for a strong password are as follows (additional rules are described in the *MiVoice Business System Administration Tool Help files*):

*15 to 20 characters using at least two characters from each of the four character sets, that is: upper-case letters (A-Z), lower-case letters (a-z), numbers (0-9), and special characters (` ~ ! @ # $ % ^ & * ( ) - _ = +).*

User Session Inactivity Period

The number of minutes of inactivity that must elapse in the current System Administration Tool session before the session is automatically terminated. The default setting is for 15 minutes.

Recommendation: The administrator should determine a value that provides a good balance between security and usability.

Password Expiry Interval

Specify the number of days in the range 0 to 365 before the password expires and is no longer valid. If a user attempts to log in after the password has expired, the system prompts for a new password before the user is allowed in. The default setting is 0, indicating that the password will never expire.

Recommendation: The password expiry must be set to the customer's IT department's existing password expiration polices.

Phone Administrator Passcode

The Phone Administrator Passcode is used to secure access to the advance settings on 69xx phones.

The field accepts digits 0 to 9 only. The minimum passcode length is four, the maximum is 10.

See the *69xx Administrator's Guide* on the Mitel Document Center website for more information about the advanced settings. Default setting is blank.

Recommendation: It is recommended that this be set so that access to advanced settings on the 69xx phones is secured by a passcode. When choosing a passcode, it is recommended that the full 10 characters be utilized, and simple pass codes such as 1111 or 1234 not be used.

Application TLS Security Level

These settings allow the administrator to set the TLS security levels for the following applications: SIP communications, IP Sets, IP trunks, Trusted Applications, System Data Synchronization, MiTAI, and Data Services.

Each application may be independently set to High, Low or Legacy; the default settings for all applications is High, which enables both TLS 1.2 and TLS 1.3.

When the TLS security level is set to High, the usage of TLS 1.2 or TLS 1.3 will depend on which version of TLS that the client requests.

Recommendation: It is recommended that the TLS security levels be set to High; however, in certain cases such as interfacing to an older system, it may be necessary to select Low or Legacy. For more information, refer to the MiVoice Business System Administration Tool Help files.

Access and Authorization

For privacy, all personal data processing is protected with role-based access and authorization controls. This includes personal data processing by data subjects, administrators, technical support, and machine APIs.

For system integrity and reliability, including the controls that protect privacy, all system data processing and all access to databases, files, and operating systems is protected with role-based access and authorization controls.

In the MiVoice Business System Administration Tool, two forms are used to administer access and authorization: the *User Authorization Profiles* form and the *Admin Policies* form. A description of these two forms follows.

User Authorization Profiles

Purpose

The *User Authorization Profiles* form is used by the administrator of the system to create, modify, and delete additional user profiles. The user profiles are required to access the following MiVoice Business management interfaces.

- System Administration Tool
- Group Administration Tool
- Desktop Tool (allows users to access the Desktop Tool for configuring their IP phones
- Application (allows access to the MiXML management forms)

The administrator uses the *User Authorization Profiles* form when performing the following tasks:

- Creating user profiles
- System Access Authorization

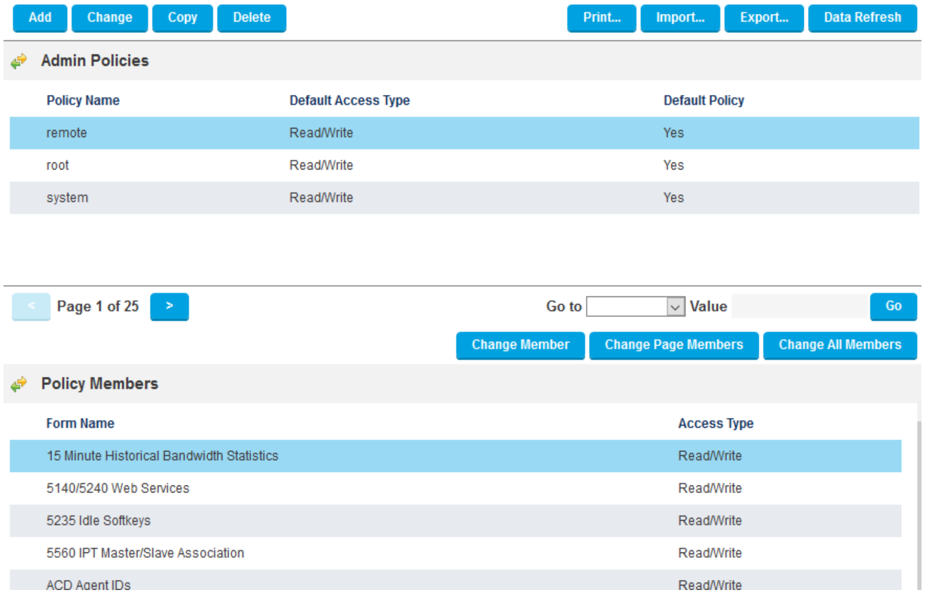
Admin Policies

Purpose

The *Admin Policies* form is used to add, modify, and delete policies that are used to establish permissions for the various user accounts. These permission policies dictate which System Administration Tool forms a user is allowed to access and/or modify.

The top portion of the form lists the currently defined policies, beginning with the four default policies: REMOTE, ROOT, NO ACCESS, and SYSTEM. The ROOT policy cannot be changed, deleted, or copied. The SYSTEM, REMOTE, and NO ACCESS policies can be changed and copied but not deleted.

Figure 3 Admin Policies Form



Admin Policies

Policy Name	Default Access Type	Default Policy
remote	Read/Write	Yes
root	Read/Write	Yes
system	Read/Write	Yes

Policy Members

Form Name	Access Type
15 Minute Historical Bandwidth Statistics	Read/Write
5140/5240 Web Services	Read/Write
5235 Idle Softkeys	Read/Write
5560 IPT Master/Slave Association	Read/Write
ACD Agent IDs	Read/Write

For each policy, the form shows the Default Access Type (Read/Write, Read Only, and No Access) granted to all the forms that the policy controls and whether the policy is a Default Policy— that is, created by Mitel (Yes) or by the user (No).

The lower portion of the form shows the access permissions defined for the forms that the selected policy controls. The permissions are as follows:

- Read - enables the form to be viewed but not changed.
- Read/Write - enables the form to be viewed and changed.
- No Access - hides the form from view.

The *Admin Policies* form is displayed only when logging in to the System Administration Tool using the ROOT policy account. All forms that MiVoice Business supports regardless of the type of MiVoice Business (SMBC, EX, virtual and so on) and type of licenses purchased are displayed.

Recommendations:

- It is recommended that the administrator create a user authorization policy. The administrator should establish MiVoice Business user authorization profiles that comply with the company policy and business requirements.
- Should temporary profiles be created to support maintenance and/or troubleshooting activities the profiles must be deleted after the activities have been completed
- When a user leaves the employ of the company, the administrator must delete all profiles associated with that user.

Application - Login Security

Mitel XML (MiXML) applications are used to access the MiVoice Business database; for example, synchronizing programming data with MiContact Center Business. MiXML requires a user be set up in the User Authorization Profiles form and also requires a certificate to access to MiVoice Business systems. Accessing the system using MiXML generates events that are recorded in the Audit log system.

For additional information about securing MiXML accesses, refer to the System Administration Tool Help Files; in particular see the *MiXML Applications* form and the *System Security Management* form. Applications require a certificate as well as the credentials for a User Authorization Profile with Application access defined.

Access to the FTP Server is accomplished with secure FTP (SFTP).

Audits and Logs

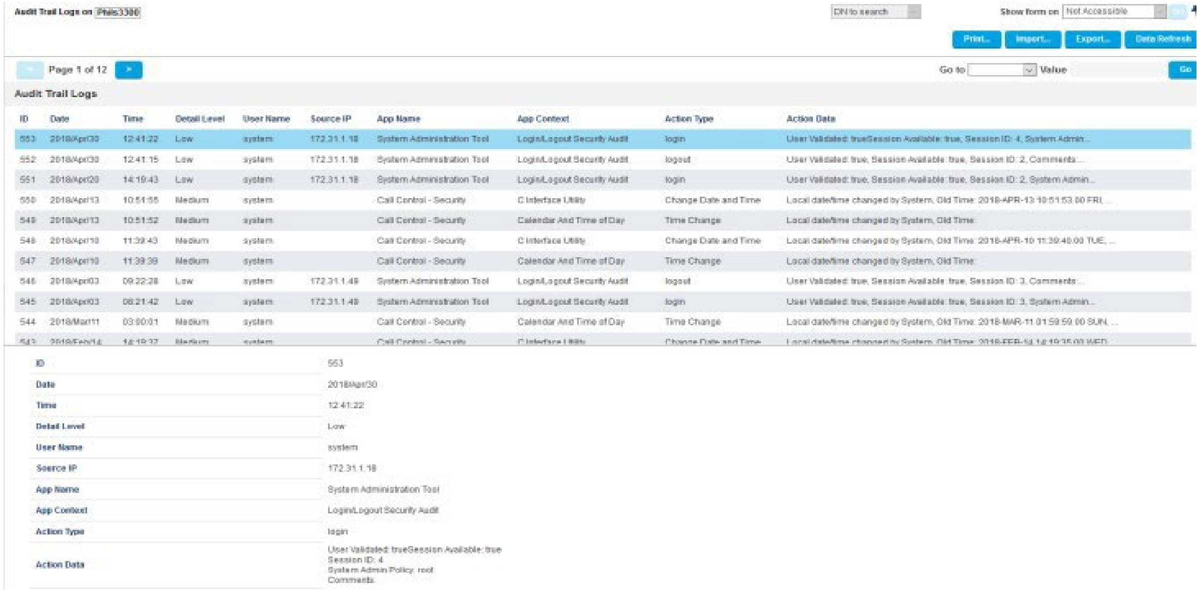
Several audit trails and event logging capabilities are supported to maintain records of data processing activities and system accesses.

Audit Trails Logs

Purpose

The *Audit Trails Logs* form provides a historical record of changes made to the system from the System Administration Tool and various other user interfaces and applications.

Figure 4 Audit Trails Logs Form



Audit Trail Logs on Phils3300

Show form on: Not Accessible

Audit Trail Logs

ID	Date	Time	Detail Level	User Name	Source IP	App Name	App Context	Action Type	Action Data
553	2018/Apr/30	12:41:22	Low	system	172.31.1.18	System Administration Tool	Login/Logout Security Audit	login	User Validated: trueSession Available: true, Session ID: 4, System Admin...
552	2018/Apr/30	12:41:15	Low	system	172.31.1.18	System Administration Tool	Login/Logout Security Audit	logout	User Validated: true, Session Available: true, Session ID: 2, Comments:...
551	2018/Apr/20	14:19:43	Low	system	172.31.1.18	System Administration Tool	Login/Logout Security Audit	login	User Validated: true, Session Available: true, Session ID: 2, System Admin...
550	2018/Apr/13	10:51:55	Medium	system		Call Control - Security	C Interface Utility	Change Date and Time	Local date/time changed by System, Old Time: 2018-APR-13 10:51:53.00 FRI, ...
549	2018/Apr/13	10:51:52	Medium	system		Call Control - Security	Calendar And Time of Day	Time Change	Local date/time changed by System, Old Time:
548	2018/Apr/10	11:39:43	Medium	system		Call Control - Security	C Interface Utility	Change Date and Time	Local date/time changed by System, Old Time: 2018-APR-10 11:39:40.00 TUE, ...
547	2018/Apr/10	11:39:39	Medium	system		Call Control - Security	Calendar And Time of Day	Time Change	Local date/time changed by System, Old Time:
546	2018/Apr/03	09:22:28	Low	system	172.31.1.49	System Administration Tool	Login/Logout Security Audit	logout	User Validated: true, Session Available: true, Session ID: 3, Comments:...
545	2018/Apr/03	08:21:42	Low	system	172.31.1.49	System Administration Tool	Login/Logout Security Audit	login	User Validated: true, Session Available: true, Session ID: 3, System Admin...
544	2018/Mar/11	03:00:01	Medium	system		Call Control - Security	Calendar And Time of Day	Time Change	Local date/time changed by System, Old Time: 2018-MAR-11 01:59:59.00 SUN, ...
543	2018/Feb/14	14:19:37	Medium	system		Call Control - Security	C Interface Utility	Change Date and Time	Local date/time changed by System, Old Time: 2018-FEB-14 14:19:35.00 WED

ID	553
Date	2018/Apr/30
Time	12:41:22
Detail Level	Low
User Name	system
Source IP	172.31.1.18
App Name	System Administration Tool
App Context	Login/Logout Security Audit
Action Type	login
Action Data	User Validated: trueSession Available: true Session ID: 4 System Admin Policy: root Comments:

- In general, all login/logout attempts and any action from any user interface or application connected to MiVoice Business that results in a change to the system database is logged.
- Audit trails are presented in this form for viewing, printing, and exporting. The information logged includes the user who performed the operation, operation type (Add, Change, Submit, and so on), date/time, application involved, and actual data changed.
- Logs can be viewed in this form as a continuous file going back 5000 log entries. Older entries are archived in xml files that can be exported for off board viewing.
- Audit Trail Logs are included in the system backup.

The user interfaces and applications audited for database changes and logins/logouts are as follows:

- System Administration Tool
- Group Administration Tool
- Desktop Tool
- Mitel Integrated Configuration Wizard
- MiVoice Business Software Installer
- MiXML interfaces (internal and external)
- Maintenance commands from the CDE interface
- Integrated Directory Services

The user actions that are audited are:

- Logins and logouts, both successful and unsuccessful attempts
- Provisioning operations
- Maintenance operations
- Scheduler operations
- Integrated Directory Service synchronization

Refer to the MiVoice Business System Administration Tool Help file for the *Audit Trails Logs* form for additional information about types of login/logouts that are audited and the log file size and location.

Under the MiVoice Business System Administration Tool Help file, refer to the *Auditing Logins and Logouts* procedure for guidance on how to use the *Audit Trails Logs*.

SMDR Options

Purpose

The *SMDR Options* form (Station Management Detail Recording) is used to select the following SMDR options.

- Station Message Detail Recording
- Program External SMDR
- Program Internal SMDR
- Location Based Accounting

Within the *SMDR Options* form, if no entry is made for a given option that requires a "Yes/No" value, the default value "No" will be applied; if no entry is made for an option that requires another kind of value, the entry will default to blank.

Call accounting systems and other applications connect to the SMDR raw ASCII output on TCP port 1752.

Recommendation: The administrator should carefully review this form and set the reporting controls as required. The application vendor collecting SMDR information will have recommended values.

To restrict access to SMDR raw information, create an Access Control List (ACL) on the Ethernet switch port that the MiVoice Business is connected to and allow only the permitted applications to connect in 1752.

PMS Logs (Property Management System)

Purpose

A Property Management System (PMS) provides a center for managing a hotel/motel hospitality business. It may also be referred to as a Front of House (FOH) system and can interface with a front desk system to provide reservation control, centralized accounting and billing, and call logging.

The PMS can interface with MiVoice Business to seamlessly enable guest room telephone services based on the room's status.

When information about a guest is changed at the front desk, messages are sent to MiVoice Business via the PMS. Similarly, when information about a guest is changed on the MiVoice Business system, messages are sent via the PMS to the front desk system.

There are a number of different logs maintained in the MiVoice Business System Administration Tool, located under PMS logs. The logs of interest from a security perspective are the Occupancy Logs.

Occupancy Logs

If the Property Management System is operational, it will generate occupancy logs and the MiVoice Business will not generate occupancy logs. If the Property Management System is unavailable, or the communication link between the PMS and the MiVoice Business becomes unavailable, the MiVoice Business will generate occupancy logs.

Occupancy logs may contain the customer's name, room number, phone call records, and customer's affiliation, check in and check out times, the date and time that the logged event occurred, and the customer's credit limit.

To access the command-line-interface so that PMS logs may be viewed or deleted:

> Login to the Linux Shell via SSH and run */sysro/bin/mtce-term* to get access to the MTCE shell.
>
> The maintenance command to view PMS Logs is:
>
> *LOGS READ HOTEL [ALL | NEW <number> | OLD <number>] [MATCH <string>]*
>
> The maintenance command to delete PMS Logs is:
>
> *LOGS PURGE HOTEL [ALL | NEW <number> | OLD <number>]*
>
> Deleting PMS logs cannot be filtered by room number or customer name (the system can purge only all new or old printed logs).

Note: The MiVoice Business does not allow the administrator to delete logs that may be kept on a third-party Property Management System. For purging PMS logs from third-party Property Management Systems, refer to the PMS vendor's documentation.

Note: The MiVoice Business supports integration between the Property Management System and the MiVoice Business voice mail system; this allows management of the voice mail system to be automated by the PMS. For details, refer to the MiVoice Business System Administration Tool Help file, see the topic *Voice Mail and PMS Integration* form.

Recommendation: To restrict access to PMS raw information, create an Access Control List (ACL) on the Ethernet switch port that the MiVoice Business is connected to and allow only the permitted applications to connect on 1753.

Local Area Network (LAN) Security

The MiVoice Business, IP phones, and associated components communicate using the corporate network infrastructure.

Network Access Security

It is recommended that the Ethernet LAN switches used to provide IP phones with LAN connectivity be managed, enterprise-grade switches that include integrated access control measures. It is also recommended that the system administrator ensure that the switch access control measures are properly configured and maintained.

Wireless networks should also employ access control measures and user authentication mechanisms with a minimum of WPA2 encryption and a separate SSID for voice applications. SSID to VLAN mapping is recommended.

Using VLANs to Assist with Security

To make eavesdropping attacks or Denial of Service attacks more difficult, or less effective, traffic on the LAN should be grouped according to traffic types and trust levels. This can be achieved with the use of Virtual LANs. VLANs can be used to segregate controller-to-controller signaling, controller-to-phone signaling, and voice traffic.

When VLANs are used to provide isolation between traffic types, it will make the solution more robust against virus-based attacks and network flooding attacks. In particular, if Voice over Internet Protocol (VoIP) traffic is grouped into a single VLAN, and the nodes on this VLAN are strongly protected, a worm-based attack causing network overload that originated on a node located on another VLAN might only marginally affect the VoIP LAN.

As an example, traffic types could be segregated as follows:

1. One VLAN grouping all of the call control engines together
2. One or several VLANs grouping all of the IP phones together
3. One or several VLANs for supporting the data traffic

When the traffic types have been segregated by VLAN, hosts or devices belonging to different VLANs can communicate only through a Layer 3 switch or router that connects the two VLANs. This means that broadcast traffic is blocked across VLANs, preventing broadcast storms from propagating network wide.

Additionally, many modern routers offer Intrusion Detection/Prevention Systems (IDS/IPS), which are able to detect and/or block more advanced types of attacks.

Creating network trust zones for security purposes and the usage of Intrusion Detection and Prevention Systems (IDPS) are discussed in detail in the Mitel Technical Papers - *Intrusion Detection and Prevention Systems* and *Securing Mitel Cloud Based Unified Communications*.

Securing Controller to Controller Traffic

In a modern IT infrastructure, servers and controllers are generally connected at the network core, and they are also usually placed in a common physical location. This location needs to be physically protected, and only authorized personnel should be allowed to access this area.

When servers and controllers are deployed in this way, traffic among the servers is likely to never leave the physical locations where servers are stored. Some Layer 2 and Layer 3 network devices are also located in the same locations and contribute to guarantee the physical separation of server traffic from other kinds of network traffic. Access control measures should be enabled on L2 switches housed in this location, and IDPS technology should be deployed to protect the core elements.

As a further measure to protect controller to controller traffic, it is recommended that a specific VLAN be used just for connecting servers and controllers.

If servers or call control engines are located at remote locations, it is highly recommended to connect these devices to the main location via a Virtual Private Network (VPN), and to employ firewalls with integrated IDPS to protect and monitor the traffic on these external connections.

Controller to Controller Authentication

The Device Certificate is the certificate that is used to authenticate the identity of MiVoice Business systems interacting with each other. The Device Certificate form is accessed with the System Administration Tool.

By default, the MiVoice Business uses the Mitel legacy certificate. You can replace the default Mitel legacy certificate with a self-signed certificate, a certificate signed by an enterprise or public Certificate Authority (CA) obtained through a Certificate Signing Request (CSR).

Alternatively, you can also use the Web Server certificate from the Server Manager as a device certificate.

Streaming Voice to a PSTN Gateway

When streaming voice traffic to an external gateway PSTN connection, the voice media path is established between the IP phone and the IP/TDM Gateway. This might be the local 3300 ICP, EX Gateway, SMBC, or another unit dedicated to this function connected via IP Networking. IP connections will be established as secure where possible.

Streaming Voice to TDM Connections

When a 3300 ICP has TDM connected devices, calls to these devices from an IP device will be via the integral IP/TDM gateway. Signaling and media security applies to the IP portion of the connection, and so the IP path to the gateway will be secure. The connection on the TDM side will continue, as it always has, to use a dedicated connection to the end device.

Similarly signaling and media IP connections to MiVoice Business running on SMBC and EX Gateway will be encrypted as well as the connections to external SIP /Analog gateways. However, the analog connection will continue, as it always has, to use a dedicated connection to the end device.

Streaming Voice to Internal Voice Mail, Record-A-Call and Conferences

When there are internal features such as voice mail, Record-a-Call, or conference enabled on the 3300 ICP, these are considered TDM devices. Encryption applies to the IP-based part of the connection so that the IP path to the gateway will be secure. The connection to the TDM devices will remain a dedicated connection to the requested service.

A conference call with a number of users requires multiple connections to the conference bridge. Connections between the IP end device and this gateway will be encrypted. Connections to the conference bridge are established over the 3300 ICP's internal TDM infrastructure.

PSTN connections or TDM devices connected to this bridge will not use encryption but will connect via dedicated circuits.

MiVoice Business on other platforms, including the EX Gateway and SMBC, have a different internal architecture and TDM devices or trunks are converted to SIP in the gateway.

IP Ports

The administrator and/or network engineer will need to open specific IP ports in the network firewalls to allow the MiVoice Business to communicate with IP phones and other components of the MiVoice Business solution. For a list of the IP ports that to be opened on network firewalls, refer to the *MiVoice Business Engineering Guidelines*.

MiVoice Business 3300 ICP WAN Port Settings

The MiVoice Business 3300 ICP hardware platforms provide a wide area network interface and as a result, they have security-related network settings. These settings are discussed in this section.

These network settings are applicable only to the following platforms:

- AX Controller
- CX-II and CXi-II Controllers
- MXe III Base and MXe III Expanded Controllers

WAN Settings

Purpose

The *WAN Settings* form is used to enable and configure the WAN interface. The *WAN Settings* form also provides WAN status information when a link to the internet is established.

Note: The default setting for WAN Access is 'Enabled'.

If the WAN interface is going to be used, the administrator will need to determine how the WAN interface will obtain an IP address. The possible methods for obtaining an IP address are, DHCP, PPPoE or, Static configuration.

Refer to the Help Files for the *WAN Settings* form for details on selecting how an IP address will be obtained, authentication, and passwords.

Recommendation: If the WAN interface is not going to be used, then the interface should be set to 'Disabled'.

Remote Access (PPTP)

Purpose

The *PPTP* form is used to program the Internet gateway as a Point-to-Point Tunneling Protocol (PPTP) server for a remote client on the Internet.

The default setting for PPTP is disabled and the default password setting is blank. If the administrator decides to enable PPTP access, then a strong password should be used.

Firewall Control

Purpose

The *Firewall Control* form is used to program the firewall settings for the Internet gateway (WAN interface). The firewall examines all packets attempting to access the internal network from the Internet. Unless a packet is part of an existing connection or matches a specific TCP or UDP port that has been programmed for forwarding, it is declared as "unknown". All unknown packets are logged in System Diagnostics and then rejected.

The firewall can also be programmed to allow outbound Virtual Private Network (VPN) tunnels with PPTP and IPSec pass-through and inbound connections with IP Port Forwarding.

For further details, refer to the Help Files for the *Firewall Control* form.

Port Forward Table

Purpose

The *Port Forward Table* form allows predefined external traffic to reach its destination on the internal network. The Port Forward Table can contain up to 40 entries. Each entry consists of a protocol (TCP or UDP) and port number combination on the Internet Gateway (WAN interface) as well as an IP address and port number combination on the internal network.

After an entry has been added to the table, a host on the internet can send a packet to the ICP WAN interface for the specified protocol/port number combination. The firewall re-addresses the packet and sends it to the IP address/port number combination of the actual resource or service on the internal network.

Recommendation: If the ICP WAN interface is to be used, it is recommended that the administrator use the Port Forward Table to block unwanted traffic originating from the internet.

Endpoint Security

Devices in the Mitel IP phone product range include the following measures to ensure VoIP security:

- Network access authentication protocol (802.1X)
- Encryption of voice and call signaling streams
- Authentication to call control
- Digitally signed firmware upgrade files

Network access authentication is used to ensure that only authorized users are allowed access to the network. Encryption is used to conceal the information that is being exchanged from unauthorized users and applications.

Network Access Authentication (802.1X)

Most enterprise grade L2 switches support 802.1X access authentication on their network ports. A device that connects to one of these ports needs to be authenticated as valid before full network connections can be established.

Mitel IP phones support the IEEE 802.1X authentication protocol. Depending on the phone model, there will be support for EAP-MD5, PEAP and proxy logoff. Users authenticate through the phone interface by entering a username and password. For details regarding which protocols a phone supports, refer to the *Mitel IP Sets Engineering Guidelines*.

The username / password authentication combination used with 802.1X is entered into the IP set interface through the telephone keypad where it is stored in flash memory.

Recommendation: It is recommended that the L2 switches used throughout the LAN support the IEEE 802.1X protocol and that this capability be enabled by the administrator.

The 53xx and 69xx series of phones support IEEE 802.1X proxy logoff. This logoff feature will become enabled when 802.1X is enabled on the phone. With proxy logoff, when a PC is physically disconnected from the phone's PC Ethernet port, the phone's PC Ethernet port will be reset. Once the PC Ethernet port has been reset, if a PC is reconnected to the phone's PC port, the PC will have to re-authenticate before being allowed access to the network.

Alternatively, some networks utilize MAC authentication to ensure only Mitel devices can access the voice VLAN.

Phone Authentication via Call Control

Mitel IP phones are available using two protocols:

1) MiNET – an encrypted proprietary stimulus-based protocol. For a Mitel set to register with the MiVoice Business call control the set type, the PIN number and MAC address must be accepted by the system. This information is entered by the administrator (it may bulk entered too). After registration, the MiVoice Business call control has knowledge of the relationship between MAC address, IP address, extension number, and PIN Registration Number. This relationship of MAC/IP/Ext/PIN must be valid for the MiVoice Business to allow communications to proceed.

2) Session Initiation Protocol (SIP) – MiVoice Business supports SIP stations that have been tested successfully through an interoperability process run by the SIP Center of Excellence team at Mitel. The SIP set must use a username and password combination to successfully register. This may be encrypted for additional security – assuming the SIP endpoint supports encryption.

Encryption - Secure Connections

In an IP-enabled network, secure connections between IP endpoints such as IP phones, are required and can be achieved in the following ways:

- Call signaling security ensures all signaling messages transmitted over an IP network are encrypted.
- Voice streaming (media) security ensures all voice packets transmitted over an IP network are encrypted.

Media and signaling path encryption is provided for all of Mitel's IP phones that are supported on the MiVoice Business. For additional details refer *to* the *Mitel IP Sets Engineering Guidelines* and the 69xx Security Guidelines.

MiVoice Business running on all hardware platforms and in virtualized environments supports TLS and secure MiNET signaling, encrypted SIP signaling and voice encryption. Media stream encryption may have impacts on the supported capacity of the controllers; for details refer to the document called *Mitel MiVoice Business - Engineering Guidelines*.

Secure Call Icon

The MiVB has the ability to inform a phone if a call is secured end-to-end with SRTP. This feature works with the following MiNET sets.

- 6905
- 6910
- 6920 and 6920w
- 6930 and 6930w
- 6940 and 6940w
- 6970
- 6915
- 6915 V2

To enable the Secure Call Icon, the Administrator must enable the feature. The feature is enabled via the MiVoice Business System Administration Tool. Within the System Administration Tool, the system option called, Voice/Video SRTP Encryption Enabled field, must be set to Yes for the SRTP security to be negotiated.

When the Secure Call Icon feature is enabled, the MiVB will send an indication to the MiNET set that the call is secured with SRTP end-to-end and the MiNET set will turn on the Secure Call Icon. The Secure Call Icon will persist for the duration of the encrypted call stream.

Call Signaling Security – Mitel MiNET Sets

Two main protocols are supported and either protocol may be used to secure a signaling channel. These are:

- **Secure MiNET, which is a Mitel standard**

  When using Secure MiNET, the phone will use a local port in the range of TCP 6900-6999 and the MiVB will use TCP Port 6802.

- **TLS (Transport Layer Security), which is an open standard**

  When using TLS, the phone will use a local port in the range of TCP 6900-6999 and the MiVB will use TCP Port 6801.

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 MiVoice Business are protected from eavesdropping. Using secure MiNET also protects the call control engine from unauthorized control packets.

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

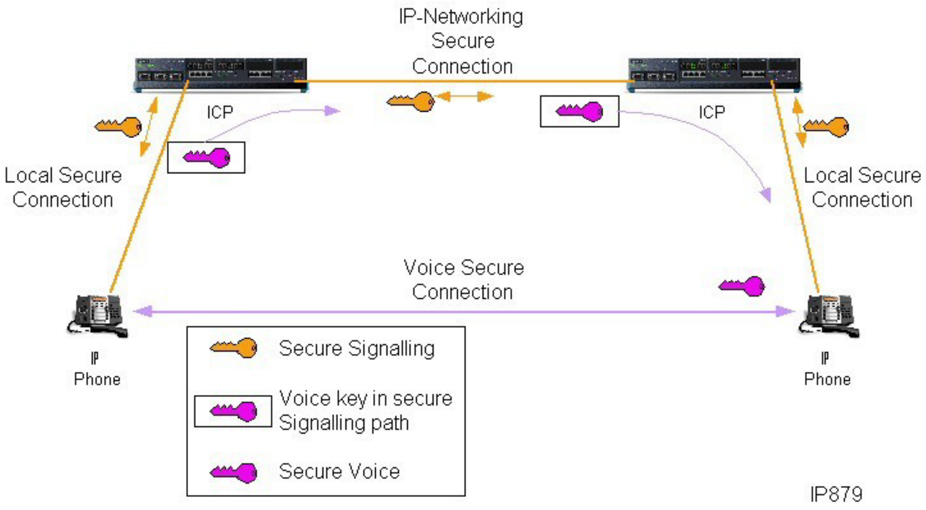
For Release 9.1 the system can be configured to only support TLS 1.2, for details refer to the *Knowledge Based Article SO4819 - How to enable TLS 1.2 only for MiVB 9.1.*

For Release 10.1 the system can be configured to support TLS 1.2 and TLS 1.3. If TLS 1.2 and TLS 1.3 are enabled on the MiVB, the MiVB will attempt to connect to the endpoint with TLS 1.3, if the endpoint does not support TLS 1.3, the MiVB will negotiate down to TLS 1.2 and attempt to communicate.

The IP phones will determine which secure method to use, first trying TLS, then secure MiNET.

The signaling path is between the call control and the IP phone or other endpoint device. This path is established as a secure connection. Signaling information is interpreted within the controller. As shown in the following diagram, when a message needs to be sent to another controller or to another end device, an independent secure connection is used. Thus, a call between two phones which are associated with two different controllers will require the establishment of three secure signaling paths, that is, a secure connection at each controller and one between the controllers.

Figure 5 Media and Signaling Path Encryption



The only overhead for supporting security are messages to establish the point-to-point secure connections and the negotiation of the secure voice connection.

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

Voice Streaming (Media) Security

Phone Streaming

Media path security between IP phones or between an IP phone and a controller is accomplished with either the Secure Real Time Protocol (SRTP), which is a standards based protocol described by RFC 3711, or a Mitel variation of SRTP termed Mitel SRTP, both using the 128-bit Advanced Encryption Standard (AES). Mitel-SRTP uses the same encryption algorithm as SRTP.

The MiVoice Business controller specifies streaming connections using SRTP or Mitel-SRTP based on whether SRTP is enabled on the MiVoice Business and the capabilities of the connection endpoints, including Mitel and third-party phones. If SRTP is enabled and supported by both endpoints, SRTP is chosen; if not, Mitel SRTP is chosen. Connections to third-party equipment must use SRTP; some older models of Mitel phones only support Mitel SRTP. For details, refer to the *Mitel IP Sets Engineering Guidelines.*

Controller to Controller Streaming

Scalability of the MiVoice Business solution is achieved by configuring MiVoice Business systems into clusters or deploying them as part of a centrally managed but distributed architecture.

Mitel provides encryption of the media path between multiple MiVoice Business systems using SRTP or Mitel-SRTP. TLS is used to encrypt the signaling path between multiple MiVoice Business systems.

Dual Port Phones

A number of Mitel's IP phones are dual port, meaning that there are two Ethernet ports on the phone. One Ethernet port is used to connect to the LAN. The other Ethernet port can be used to connect a PC to the network via the phone's integral L2 switch; this capability is useful in environments where the phone and the PC need to share a single Ethernet connection.

MiVoice Business supports a Class of Service (CoS) option that can be used by the system administrator to disable the second Ethernet port on dual port phones, which in turn will bar access at the second Ethernet port. The default condition is for all second Ethernet ports to be enabled.

For all IP endpoints there are three main settings that are applied to them

1) Class of Restriction (CoR) – the call barring level that the set or user is allowed to make externally; for example, all phones are allowed to dial an emergency number (999, 112, 911), but only the executive staff can dial international calls. CoR can be set at a time of day and day of week granularity level per user if preferred.

2) Class of Service (CoS) – the features allowed by the user or device; for example, silent monitor allowed. This is also where the IP phone's expansion Ethernet port can be disabled so that a PC plugging into the back of the IP phone is not connected to the network at all.

3) Interconnect Restrict – the ability to stop devices and users from being able to call other devices and users connected to the same system; for example, user 1234 can be barred from calling extension 1235.

Wi-Fi Capable Phones

The 6900w family of IP phones have an embedded IEEE 802.11a/b/g/n Wi-Fi interface.

The 6900w phones support a Wi-Fi security protocol called Wi-Fi Protected Access 2 (WPA2). There are two versions of WPA2 supported on the 6900w IP phones, Personal and Enterprise. Both the Personal and Enterprise versions use AES-CCMP to encrypt transmitted data.

WPA2 Personal and Enterprise differ in the authentication stage. WPA2 Enterprise uses IEEE 802.1X, which offers enterprise-grade authentication. WPA2 Personal uses pre-shared keys (PSK) and is designed for home or SoHo use.

When Wi-Fi is enabled on a 6900w IP phone, the phone will use information from the Wi-Fi Access Point to determine if the Access Point is running WPA2 Enterprise or Personal.

When a 6900x IP phones connects to an Access Point, the phone will display a password prompt if WPA2 Personal was detected, or a username prompt followed by a password prompt if WPA2 Enterprise was detected.

Mitel Endpoint Internal Security Capabilities

69xx IP Phones

The 69xx series of IP phones have an integrated L2 switch that provides protection against unexpected levels of network activity, the L2 switch will also restrict traffic according to built-in rules; these rules are not configurable. All packets blocked by the L2 switch will be discarded transparently at the Ethernet layer without the phone's upper layers being affected in any way.

52xx and 53xx IP Phones

A number of IP phones from the 52xx, 53xx and 55xx series use an integral micro-firewall to protect against unexpected levels of network activity, the micro-firewall will also restrict traffic and responses according to built-in rules; these rules are not configurable.

The following IP phones support the Integral micro-firewall:

5212	5304	5324	5340e	MiVoice Video/Conference
5215 Dual Mode	5312	5330	5360	
5220 Dual Mode	5320	5330e	5505	
5224	5320e	5340	5540	

Table 1 IP Sets with Integral Micro-Firewall

The micro-firewall blocks all undesirable packets (such as ARP packets that are not for the phone).

Packet Type	Rate (Packet/Second)	Burst Handling (Packets)
CDP, STP, LLDP	5	25
DNS	30	20
ARP, ICMP	5	50
RTP (per stream)	110	0

Table 2 IP Sets Micro-Firewall – Packet Rates

The micro-firewall uses a "credit" system to limit unexpected packet rates and will discard packets if these limits are exceeded. This may occur during an attack, but may also occur for certain protocols where there are large subnets. Subnets greater than 1022 (/22) are not encouraged, the normal being 254 (/24).

The micro-firewall will filter the packets and allow bursts up to the "credit" limit shown above. After a protocol type has exhausted its credits with a burst that reached the prescribed limit, the credits are added back at prescribed rates. For instance, the micro-firewall may allow up to 50 ICMP packets in a burst, and then discard any additional ones that arrive before the micro-firewall will begin adding credits at the rate of 5 a second.

All packets blocked by the micro-firewall will be discarded transparently at the Ethernet layer without the phone's upper layers being affected in any way.

MiVoice Business Console

To ensure security, the voice (media) and signaling paths between the MiVoice Business Console (MiVoice Business-C) and the MiVoice Business can be encrypted.

To ensure that the communication paths between the MiVoice Business-C and the MiVoice Business are secured, the administrator will need to run the MiVoice Business-C Configuration Wizard when the MiVoice Business-C is first installed or when an upgrade is taking place, for details refer to the MiVoice Business-C Installation Guide.

When running the Configuration Wizard, the Wizard will attempt to secure the signaling path between the MiVoice Business-C and the MiVoice Business with TLS. If securing the path with TLS cannot be accomplished, the Wizard will then try using Secure MiNET to secure the signaling path.

Media path security between the MiVoice Business-C and the MiVoice Business is accomplished with either the Secure Real Time Protocol (SRTP), which is a standards based protocol described by RFC 3711, or a Mitel variation of SRTP termed Mitel SRTP, both using the 128-bit Advanced Encryption Standard (AES). Mitel-SRTP uses the same encryption algorithm as SRTP, but with a Mitel packet.

The MiVoice Business-C screen has an icon in the lower right corner that will indicate if the connection to the MiVoice Business is successfully secured. When the solution is operating with MiVoice Business resiliency, the security status of both the Primary and Secondary MiVoice Business will be indicated, for further information refer to the MiVoice Business-C documentation.

Embedded Voice Mail

The Embedded System Management (ESM) tool has a VM Options form that is used to configure Voice Mail security features. The Embedded Voice Mail passcode can be set to between 4 and 10 digits. The Mailbox lockout timer can be set from 0 to 60 minutes, where 0 refers to lock mailbox “forever”.

The Voice Mail passcode is encrypted using OpenSSL’s AES 256-bit encryption.

When a Mailbox has been locked forever, it can be unlocked by resetting the passcode using the Desktop Tool, or the Voice Mail Mailboxes or User and Services Configuration form. The default value for the Mailbox lockout timeout is 3 minutes.

The forward to email feature which forwards a voicemail message to the user’s email account supports the following transmission and authentication methods:

- A non-secure / Cleartext method of forwarding to email via Port 25. This method is not supported in the MiCloud Flex Solution. It is available only with the MiVB Enterprise solutions.

- The STARTTLS method of authentication for forwarding to email via Port 587. This method is supported for MiVB Enterprise solutions and MiCloud Flex solutions.

- The SSL / TLS method of authentication for forwarding to email via Port 465. This method is supported for MiVB Enterprise solutions and MiCloud Flex solutions.

Prevention of Toll Abuse

Any communication system that has a combination of Direct Inward System Access (DISA) integrated auto attendant, Recorded Announcement Devices groups, an auto attendant or voice mail can be susceptible to toll abuse. Therefore, it is important to assign appropriate telephone privileges and restrictions to devices. In addition, publicly accessible telephones should be denied toll access unless authorized through an attendant.

The 3300 ICP/MiVoice Business system provides comprehensive toll control as an integral part of the call control engine.

The MiVoice Business call control gives the administrator the ability to restrict a user's access to trunk routes and/or specific external directory numbers.

The MiVoice Business call control offers several Class of Restriction (CoR) and Class of Service (CoS) capabilities, that when used correctly can substantially reduce the risk of toll abuse by disallowing the dialing of certain external telephone numbers or ranges of numbers (Call Barring).

This is achieved by associating in software each extension and trunk with a CoR and providing specific barring plans with each CoR.

Mitel’s implementation of CoR affords great flexibility. Up to 64 different Classes of Restriction can be specified. An extension user attempting to dial barred numbers will result in them receiving a number unobtainable tone.

As a deterrent to toll abuse by internal callers, Station Message Detail Recording (SMDR) logs can be used to track calls from within your company, providing detailed information such as the originating extension number, time, duration, and number dialed. SMDR record access should be restricted as with any other function.

Knowledge Articles

The following articles discuss the prevention of toll fraud, these Knowledge Management System (KMS) articles can be found on the Knowledge Management System.

- HO1180 - Simple SIP Passwords and Impersonation
- HT4607 - Using CDE to Prevent Toll Fraud on the Mitel 3300 ICP
- HT5320 - Potential credit card scam when outside callers are calling Hotel Guests via Embedded voicemail
- HO916 - General Guidelines to Secure SIP trunks for Toll Fraud prevention
- HT461 - Preventing Toll Fraud MiVoice Business
- HT53 - For security and/or Toll Fraud concerns, Hot Desk User PIN should be updated regularly

The Mitel Knowledge Based articles HO745, HO1178, HO767 and HO916 also discuss the prevention of toll abuse, to access these documents, contact Mitel Professional Services.

Technical Bulletins

Technical Bulletin Article # 13-5191-00310 provides some general guidelines to prevent SIP trunks from being accessed for unauthorized use of phone service or SIP trunk resources (a.k.a. Toll Fraud).

Mitigation of Telephony Denial of Service

Areas that might be subject to Telephony Denial of Service (TDoS) within the system include:

- User end-devices and telephone extensions
- IP to TDM gateway
- Trunk interface to PSTN or SIP service provider

Most attacks for TDoS on the phones are targeted at the IP interface. Mitel phones include a micro-firewall or L2 traffic controls on this IP interface, which applies rate limits to different protocols, including the voice streaming connections. Unexpected packets and packets over and above expected limits are throttled and rejected. Note that non-Mitel phones connected to the system, such as third-party SIP devices, may not include this functionality.

The IP to TDM gateway provides the connections between the IP and TDM networks. The primary function is conversion of the voice streams between these networks. Streams with excessive packets are rejected. IP ports for streaming are opened only as required and closed on call completion. Streaming to an unopened IP port will result in that stream being dropped. Call setup rates are limited in line with the expected number of channels and calls through the gateway.

Primary connections to the PSTN or SIP service provider are via digital trunks or IP/SIP trunks. Digital trunks are limited due to the number of physical channels that can be accessed at any time. The signaling channel and call handling can also be configured for rate limiting.

IP/SIP trunks can handle many trunks and also high call rates. In order to ensure minimal impact due to TDoS, both the end-user system and the connections to the SIP Service Provider need to be balanced. The number of trunk connections on the end-user system is limited due to licensing and configurations settings. The service provider connections should be arranged to match the number of channels in a similar manner. Controllers and gateways can also be IP networked to provide load distribution in situations where high traffic levels need to be handled, as in call centers.

LAN Quality of Service

For ensuring voice and video quality across a network, Mitel recommends that specific IEEE 802.1p Quality of Service (QoS) settings be used to ensure that the networking equipment treats voice, video and signaling packets with higher priorities than other traffic.

Following these recommendations may increase the possibility that voice, video and signaling packets will be more resistant to a DoS attack. For recommended QoS settings, refer to *Mitel IP Sets Engineering Guidelines.*

Miscellaneous Information

System Options

Purpose

The *System Options* form is used to specify parameters that are used system-wide during call processing and data switching, the form also contains a number of security related settings, and they are described below.

- **Call History - Disable Record Generation:** The default setting is "No", meaning that call history records will be stored.
- **Call History - Default Call History Records:** This is used to set how many call history records the set can store.
- **DISA Failed Attempts before Lock-Out:** This sets the number of invalid PINs that a user is allowed to enter within five minutes.
- **DISA Number Lock-Out Timer:** This sets the amount of time a user is locked out after exceeding the number of invalid PIN entries.
- **Send Welcome Email:** Selecting "Yes" will send newly provisioned users a welcome email containing their login credentials and other service information.
- **Set Registration Access Code:** This code is used when registering a new IP telephone.
- **Set Registration Security:** This is used to set the number of attempts that a user has to register an IP telephone.
- **Voice Encryption Enabled:** The default setting is "Yes'.
- **Voice/Video SRTP Encryption Enabled:** The default setting for MiVoice Business 7.0 and later installations is "Yes", which will enable Secure Real-time Protocol (SRTP) media encryption. If this is set to "No", while the option *Voice Encryption Enabled* is set to "Yes", then Mitel's Encryption solution (not SRTP) is used to provide media security. If the option *Voice Encryption Enabled* is set to "No", then this option becomes inactive (grayed out) and no media security is applied to any calls.

Recommendation: It is recommended that the administrator review all of these options and set the controls as appropriate for their particular network.

Recommendation: It is recommended that the administrator enable voice encryption and enable the use of SRTP.

Antivirus Protection

Applications such as MiVoice Business must process data in real-time. Real-time applications require unfettered access to processor resources, memory systems, and to disk drive accesses and network communications. When MiVoice Business is deployed on proprietary hardware, industry standard servers or virtual machines - as per Mitel's MiVoice Business Engineering Guidelines - the machine's resources will have been sized to ensure that the applications will have unrestricted and timely access to the resources that they require.

Because these real-time data processing applications are executed on carefully sized computing platforms, the installation of antivirus software is not recommended.

Securing Mitel Standard Linux

Mitel's MiVoice Business software is installed on top of the Mitel Standard Linux (MSL) operating system. Compared to more common operating systems, MSL provides a reduced attack surface. This reduced attack surface is the result of the following MSL characteristics:

- MSL does not support email
- MSL does not support internet Web browsing
- Users with write permissions are limited and access is strictly controlled
- Mitel has removed unnecessary files and packages from MSL
- Mitel has closed unnecessary IP Ports

Additional measures can be taken to secure the MSL platform and the MiVoice Business application executing on the platform, these measures are based on well-known network security best practices.

In general, a platform that is both physically secure and installed in network that has been securely designed will have a low likelihood of being infected compared to a platform that that lacks physical security and/or is installed in a network lacking security controls.

Use of Antivirus Software

While the use of antivirus software is widely accepted in the IT industry for use on servers, end user mobile platforms and desktops, running antivirus software on a real-time computing platform will be problematic.

Because MiVoice Business is a real time application, Mitel cannot guarantee that third-party antivirus software will not affect the performance of the MiVoice Business application, and Mitel does not offer any endorsements of antivirus software vendors, or evaluations of particular antivirus products.

Should a customer require technical support from Mitel related to a system that has antivirus software installed, Mitel may require that the software be removed before Mitel can start troubleshooting the problem.

Software Patch Management Policy

It is necessary for the administrator to ensure that the MiVoice Business systems are always updated and equipped with all critical patches to guarantee the highest level of security. Mitel has developed best practices for the management and installation of security patches released by the operating system vendors aiming to guarantee the highest level of security and the correct functioning of the system.

Product Security Information

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

Mitel Product Security Advisories

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

Mitel Security Documentation

Mitel security documentation includes product-specific Security Guidelines and 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

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 MiVoice Business 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.