A MITEL
TECHNICAL PAPER

MiVoice Business

MiVoice Business Security FAQ

September 2024

Mitel
Powering connections

Notices

Trademarks

Contents

Purpose

The purpose of this document is to answer frequently asked questions regarding security in a Mitel MiVoice Business environment. The security of IP Telephony communications is very important to our customers. Mitel recognizes and addresses these requirements with measures to protect business communications from security threats today, and with ongoing diligence to ensure the security of future communications. Security threats to MiVoice Business implementations are similar to that of any other IP application service and as with other IP applications, Mitel's voice-over-IP (VoIP) applications can also take advantage of the existing security options available within an IP networking infrastructure.

General Security

Q. What are the key security issues for a MiVoice Business deployment?

- **Confidentiality***:* The need to protect transmissions, whether for voice streaming or data services, to prevent eavesdropping or interception of conversations, call control signaling or passwords.
- **Integrity**: The need to ensure that information is not modified by unauthorized users and to unequivocally prove a user or application is actually authorized to perform the task/function they are requesting, be it a voice call or configuration change.
- **Availability**: The need to ensure the operation of the communication system is not adversely affected by directed denial of service attack, an inadvertent network storm or a malicious computer worm or virus.

Q. How does a MiVoice Business solution defend against Security Threats?

Security threats can take many forms such as eavesdropping, toll fraud, and denial of service attacks. Mitel's objective is to develop solutions that inherently defend against attacks and to also share best practices that help users avoid malicious attacks. The operating system (OS) that MiVoice Business uses is not a generic OS and has less of an attack surface due to the hardening of the OS that Mitel has performed, thus making it more difficult for would be attackers than a generic OS.

Encryption

Q. Do Mitel solutions support encrypted call control signaling?

Yes. Encrypted call control signaling (MiNET and SIP) is enabled by default on the MiVoice Business and is available across Mitel's entire current portfolio of IP phones. Call control signaling can be encrypted using Transport Layer Security – TLS version 1.3 or TLS 1.2.

Note: Not all SIP trunk providers encrypt call signaling, so call signaling can also be configured to be unencrypted when working with those vendors.

Q. Do Mitel solutions support encrypted voice?

Yes. Voice streams are encrypted by default using the industry standard of Secure Real Time Protocol (SRTP) using 128-bit Advanced Encryption Standard (AES).

Note: Not all SIP trunk providers encrypt voice, so RTP traffic is not encrypted when working with those vendors.

Q. Is encryption supported by softphones?

Yes, the Mitel MiCollab PC Desktop client and MiCollab Mobile soft phone support encryption with both encrypted call control (minimum TLS 1.2) and encrypted voice (SRTP) using 128-bit AES encryption.

Q. Can I use my company's provided certificate?

Yes, the MiVoice Business allows a customer to upload a certificate to replace the default Mitel self-signed device certificate with a certificate signed by an enterprise or public Certificate Authority (CA). Support for a customer provided certificate by the customer's IP endpoints may vary depending on the model type and should be verified with IP endpoint vendor.

Confidentiality

Q. How does a Mitel voice solution ensure the confidentiality of call control and signaling?

In a MiVoice Business implementation, call-signaling traffic from Mitel's 6900 and 6900w series sets and legacy 5300 series is sent across the network using Mitel's proprietary MiNET protocol secured by TLS. SIP trunks, devices, gateways, and softphones may also use TLS for signaling encryption.

Users should check that their SIP device of choice also supports these capabilities.

In addition, the 6900w phones when connecting to a Wi-Fi network support the Wi-Fi security protocol called Wi-Fi Protected Access - WPA2 Enterprise, WPA2 Personal or WPA3 Personal modes are available.

Q. A malicious user could attempt to use IT network tools to intercept data packets. How does a Mitel voice solution prevent these types of eavesdropping?

With Mitel IP desk sets and softphones voice traffic is sent encrypted across the network using Secure Real-time Transport Protocol (SRTP) with 128-bit AES encryption. Mitel IP desk sets and softphones will only send and receive voice traffic when instructed to do so by the MiVoice Business through commands sent in the encrypted call control stream. An IP desk set or softphone that is instructed to establish a voice connection receives (over the encrypted call control connection) a unique session encryption key that is used for the encryption of that call. A random SRTP stream sent to an IP set will be ignored. Mitel 6900 and 6900w sets can inform a user that the call is secured end to end with SRTP through the Secure Call Icon on the set.

Integrity

Q. How can an unauthorized set be prevented from connecting to the system?

The MiVoice Business has knowledge of the relationship between MAC Address, IP address, extension numbers and PIN Registration Number if a Mitel IP Phone. This relationship of MAC/IP/Ext/PIN must be valid in order for the MiVoice Business to allow communications to proceed.

SIP devices (including softphones and analog devices connected to analog/SIP gateways) are secured with a unique username/password combination. Complex passwords as per the customer's password policy are recommended.

A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists (ACLs), and firewalls.

Q. How does Mitel prevent modification, alteration or corruption of the voice stream?

Through the use of the encrypted Secure RTP mentioned previously, Mitel is able to ensure that the voice stream is not modified or altered during transmission across the network.

Q. How do you prevent modification, alterations or corruption of the call signaling?

Call-signaling traffic is sent and received using the TLS encrypted Mitel proprietary MiNET protocol.

Secure MiNET traffic is only accepted from devices that have first been authenticated with the MiVoice Business. Each device (i.e. IP phone) sends a unique identifier in the encrypted MiNET call control stream. The MiVoice Business processes the MiNET requests if the unique identifier has been approved and associated with a valid extension in the system. Authorization of the unique identifier is typically done by the system administrator using the MiVoice Business System Administration Tool. The IP phone sends its MAC address as a unique identifier. Note that this identifier is sent in the encrypted MiNET call control stream and not as a Layer 2 transmission, which could possibly be spoofed.

Similarly, SIP desk sets and softphones use TLS-encrypted SIP signaling for call set up, however authentication is performed using username / password that is exchanged across the SIP TLS connection. Complex usernames and passwords should always be used.

Q. How can unauthorized free calls be avoided?

The MiVoice Business Class of Service, Class of Restriction and Interconnect Restriction controls are used to define the available features, dialing restrictions and interconnectivity of devices and trunks in predefined situations. Changes in any of these settings are used the next time the device or user makes a call and allow or bar calls and features. Customers may also want to reference the MiVoice Business Security Guidelines “Prevention of Toll Abuse” section for further detailed information.

Q. On start-up, Mitel IP phone sets download their software via TFTP. What prevents an attacker from substituting their own malicious software load and manipulating the behavior of the phone?

In a MiVoice Business deployment all set software loads are encrypted and tamper-proof to ensure that set will only open the correct load. Upon download and decryption, the sets perform an integrity check to ensure that the software load was not modified.

Q. What intrusion detection utilities are provided or recommended in a Mitel IP telephony environment?

Mitel wants its customers to have maximum choice in their technology decisions and therefore Mitel is agnostic in relation to intrusion detection systems. Information is available in Mitel’s *MiVoice Business Engineering Guidelines* document and your Mitel Systems Engineer can provide additional support regarding the specific ports and protocols utilized by the platform if required.

Authentication

Q. How can users or classes of users be restricted from dialing external or long-distance numbers?

Mitel implements Class of Restriction (CoR) to enable the customer to disallow the dialing of certain external telephone numbers or ranges of numbers (i.e. 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 75 different Classes of Restriction Groups can be specified. An extension user attempting to dial barred numbers will result in them receiving a number unobtainable tone by default. Alternatively, the extension user could be routed to an answer point, such as the switchboard, for the offering of advice. An extension may have a different CoR for use with Day Service, Night 1, and Night 2 services, respectively. Automatic Route Selection Route Plans can also be configured to only allow certain numbers to be dialed based upon the day or week or time of day combination. This would allow users to dial external digit sequences during certain time periods that could be restricted at other times.

In addition, the utilization of account codes provides extra control options.

- Verified Account Codes allow users to utilize features that are not normally available at an extension. These Account Codes can be used to change the Class of Service (features) and Class of Restriction (barring) parameters of the extension.
- Non-Verified Account Codes allow the extension user to enter codes in Mitel's call reporting utility, the SMDR, relating to billing and/or call management.
- System Account Codes can also be added and automatically dialed by the system when outgoing calls are made on network services that have such a requirement.

Mitel systems are, of course, configurable such that all legally required emergency numbers can be dialed at any time with or without a prefix.

Q. 802.1X is a network access control standard that addresses how to keep a user from gaining access to the network by plugging an unauthorized device into a corporate network. How does Mitel address 802.1X with respect to softphones and desktops?

Mitel 5300 and 6900(w) IP sets include support for 802.1X in their firmware. With 802.1X enabled, the phones support EAP-PEAP, EAP-MD5 or EAP-TLS. Additional details of what set type supports which 802.1X capabilities are available in the Mitel IP Sets Engineering Guidelines document.

The 6900w phones also support the wireless network security protocol Wi-Fi Protected Access WPA2 Enterprise, WPA2 Personal or WPA3 Personal modes. WPA2 Enterprise uses IEEE 802.1X, which offers enterprise-grade authentication. WPA2 Personal and WPA3 Personal use pre-shared keys (PSK) and are designed for home or SoHo use.

Mitel's primary softphone is called MiCollab Client. It is available as an application on a Windows PC, macOS, Android device or Apple iOS as well as supporting WebRTC. A softphone takes advantage of 802.1X settings configured in the underlying operating system. For instance, if MiCollab Client Softphone is installed on a Windows 11 laptop, that laptop would use the included 802.1X supplicant to connect to the network before MiCollab Client Softphone can connect.

Q. How are Mitel phones authenticated when installed or deployed?

The MiVoice Business has knowledge of the relationship between MAC Address, IP address, extension numbers and PIN Registration Number. This relationship of MAC/IP/Ext/PIN must be valid in order for the MiVoice Business to allow communications to proceed.

Each set has a unique identifier that is sent in the encrypted call control stream and is mapped in the MiVoice Business to an extension which has a Class of Service and Class of Restriction that determines the features the set is allowed to use, and the dialing level permitted.

Q. Do Mitel phones need to authenticate to place each call?

For each call that is made the phone's programmed capabilities e.g. (Class of Service (CoS), Class of Restriction (CoR) and Interconnect Restrict) in the MiVoice Business are consulted. For example, if a change in the IP set's CoR was made the new call barring rules would be applied on the next call made. However, the phones do not need to re-authenticate to the MiVoice Business for each call as the MiNET call control signaling connection is always providing secure heartbeat communications between the MiVoice Business and the Mitel IP sets.

In addition, Mitel has support for account codes that would require a phone user to enter a valid PIN code before any call is made.

Q. Can a H.323, MGCP or SIP client place an unauthorized external call?

The MiVoice Business solution does not support H.323 or MGCP and therefore no H.323 or MGCP device can connect to it.

MiVoice Business supports SIP and encrypted SIP for devices and trunks. SIP devices may place calls (internal or external) only once authorized on the MiVoice Business system. Authorization requires that a user is preprogrammed on the system with a matching combination of username and password. Mitel recommends the strongest usernames and passwords be used that each end supports.

MiVoice Business also supports SIP trunks, and these are subject to the same restrictions as legacy TDM trunks plus the SIP peer is sent to a preprogrammed IP address and can also be protected by a username / password. Mitel recommends the strongest usernames and passwords be used that each end supports.

Availability

Q. How is a MiVoice Business solution protected against virus attacks and/or worms?

MiVoice Business does not use a generic operating system but uses a Linux variant known as Mitel Standard Linux (MSL) which has unnecessary packages removed and certain services replaced. Compared to more common operating systems, MSL provides a reduced attack surface. In addition, only Mitel applications are installed on the MSL server and installation of non-Mitel endorsed applications is not supported, thereby reducing the accidental installation of malware. MSL is also configured so that unnecessary IP Ports are closed.

While it would still be theoretically possible for an attacker to write a virus targeted at Mitel's specific Linux implementation, the reality is that it would be extremely difficult for such a virus to propagate, as the means to introduce it into a network would be severely limited.

A similar statement could be made about the operating system used in Mitel IP phones. Here the risk is even lower because of the limited memory available in a phone limits how sophisticated a program can be run inside of the device.

Q. How is the Mitel solution protected against denial of service (DOS) attacks?

The comments made above in relation to viruses apply to DoS threats as well. Given that the MiVoice Business and Mitel's IP Phones do not use general-purpose operating systems, they are not vulnerable to the entire class of DoS attacks against the components of those operating systems. However, many DoS attacks are against the TCP/IP networking layer itself and so attack any IP-connected device. With each release of the MiVoice Business and Mitel's IP desktops, Mitel continues to harden the systems against DoS attacks. Hardening is a continuous process and high priority at Mitel to ensure our customers are protected against attackers who unfortunately are constantly coming out with new DoS attacks.

General Network Questions

Q. Mitel phones generally include a second Ethernet port that is often used to support a user's PC. How is that port secured?

The PC port on a Mitel desktop is a simple Ethernet switch that provides basic Layer 2 connectivity to whatever device is plugged into the PC port. The PC port can be enabled or disabled in the MiVoice Business system programming as desired. When enabled it passes all traffic through to the network switch to which the IP set is connected. Any additional network authentication is handled by the network switch and network authentication services.

Q. What security is available for wireless phones?

Mitel 6900w sets are wireless network capable and support Wi-Fi Protected Access 2 (WPA2) Personal and Enterprise modes and WPA 3 Personal mode. 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, WPA2 Personal or WPA3 Personal. WPA2 Personal and Enterprise differ in the authentication stage. WPA2 Enterprise uses IEEE 802.1X, which offers enterprise-grade authentication. WPA2 Personal and WPA3 Personal use pre-shared keys (PSK) and are designed for home or SoHo use.

The Mitel Wireless LAN Adapter is available to convert Ethernet only devices to Wi-Fi and is supported on the 6900, 6800, 5300 series of IP Phones. The wireless LAN adapter supports WEP, WPA-PSK, and WPA2-PSK (AES). It also supports IEEE802.1X authentications. More details are available in the *Mitel WLAN Administrators Guide.*

The Mitel 5634 voice over Wi-Fi phone is a portable device that supports WPA and WPA2 PSK in addition to EAP-TLS.

Q. Is it possible for incoming connections on the TDM side of a MiVoice Business to somehow gain access to data network on the IP side of the system, i.e. is there a potential for someone calling in on a PSTN trunk line to gain access to the corporate data network? Or vice versa?

No. This question is applicable to cases where the MiVoice Business is installed on Mitel appliances that support TDM interfaces, such as the SMBC, EX or 3300 ICP hardware platforms. While the MiVoice Business appliances provide a gateway between TDM and IP, all TDM connections are terminated on the TDM side of the MiVoice Business, and all IP connections are terminated on the IP side. A connection over a (TDM) trunk line to an IP phone would be terminated within the MiVoice Business and a new IP connection made from the MiVoice Business to the IP phone. Likewise, in a call from an IP phone to a trunk line or other TDM set, the IP connection would be terminated within the MiVoice Business and a new TDM connection made over the appropriate trunk to the appropriate set. When using external analog to SIP gateways or analog terminal adapters (ATA), such as Mitel's AG41XX series, the same process

occurs in the device. Note that in this IP-to-TDM translation process there is no noticeable impact for the user.

Teleworker / Remote Worker Support

Q. How does Mitel address the issue of secure traversal of firewalls?

The Mitel Teleworker Solution uses a MiVoice Border Gateway (MBG) server that resides on the edge of a corporate network behind a customer firewall in a DMZ and allows Mitel phones to be securely located anywhere across the Internet. The MBG teleworker solution maintains an encrypted call control link to the remote phone and dynamically opens and closes firewall pinholes on the MBG when a secure voice connection is made. The Teleworker Solution can work with all current Mitel IP Phones as well as third party SIP sets that have been tested and certified by Mitel for interoperability.

Q. Can remote phones be located behind firewalls/gateways that perform Network Address Translation (NAT)?

Yes, remote phones can be located on any type of broadband connection and can be behind one or multiple layers of NAT.

Q. How secure is the Teleworker Solution?

The Mitel Teleworker Solution supports a minimum of TLS 1.2 encrypted MiNET call control and 128-bit AES-encrypted Secure RTP. Only authorized devices can connect, and it dynamically opens and closes firewall pinholes when a secure voice connection is made.

Q. Can a remote user plug a PC into the second Ethernet port on the back of the teleworker set and connect into the corporate network?

No. The second Ethernet port, when enabled, merely provides any device plugged into it with connectivity to the local Ethernet network. It does not provide any mechanism for a device to connect across the secure connection established between the remote set and the Teleworker MBG server located at the corporate office or data center. Any such data connections would require the use of a separate data VPN system by the device that is attached.

Management

Q. How does Mitel prevent unauthorized access to the web management interface of the MiVoice Business?

Mitel implements TLS to defend against “sniffing” of usernames and passwords. Access to the management interface requires a username and password. Password strength is configurable in the MiVoice Business under System Security Management as are the session inactivity time (default is 15 minutes), Password Expiry Interval and other settings. If an incorrect username/password is entered three times in a row, the system will prevent further login attempts for 15 minutes.

The underlying Mitel Standard Linux (MSL) operating system allows administrators to be limited to specified IP addresses, or IP address ranges, only accepting TLS based web connections from the permitted IP address source(s). Linux shell access is only available via SSH, which is disabled by default and also supports the source IP address restrictions, ensuring that the platform rejects any non-authorized connections.

Further safeguarding is afforded by providing multiple levels of access control. A customer can further protect by using Access Control Lists (ACL) or firewall capabilities of the switch device the MiVoice Business is connected to.

Q. How do you prevent modification, alterations, or corruption of the management commands?

All web interfaces implement TLS and are password protected to ensure secure access.

Q. Are multiple levels of administrative access supported?

The MiVoice Business supports three levels of embedded administration tools. One level is for system administration, one is for group administration, and one is for end users to directly control their desktop device. All are web based and secured via TLS. Administration levels can be further customized by allowing and barring Read or Write access into specific programming forms.

Q. Are there limits on the number of simultaneous users that can access the embedded administration tool?

Yes. There can be a total of up to fifty simultaneous system users, of which five may be concurrent system admin users and five may be concurrent group admin users. Sessions will time out after 15 minutes of inactivity by default (configurable).

Additional Information, Support, Services

Q. Where can I find more information such as guidelines and best practices for implementing effective security in a Mitel IP-telephony environment?

Users can access technical and security documentation and engineering guidelines using the Mitel Document Center web site (https://www.mitel.com/document-center).

Q. Does Mitel offer security patches for Mitel IP telephony solutions?

Yes. Generally, distribution of security patches is available using a software download. Customers can sign up to be notified of security advisories at https://www.mitel.com/support/security-advisories.

Q. Where can I obtain access to pre- or post-sales, on-site, professional security assessment/planning services?

Mitel's resellers and professional services organization offer network assessment/planning services. Please contact your sales representative for more information.