Mitel Performance Analytics (MPA) 3.3 Security Summary

Introduction

Mitel Performance Analytics (MPA) supports several different deployment architectures. The security principles and the available tools vary, depending on the architecture.

On Premises - If a customer chooses to deploy MPA on premises, the MPA server and corresponding modules are subject to the customer's own network security. In this model, the MPA server typically sits behind the customer's firewall and is governed by that company's security policies. Please see the Mitel Performance Analytics Engineering Guidelines for information about open port requirements.

On Premises - Air Gapped. Air-gapped systems are similar to on-premises systems; however, in air-gapped systems there is no possible connection to external networks such as the internet, and thus no way to remotely administer the MPA installation. This architecture also follows the customer's security policies.

Cloud - MPA servers are managed by the Martello Operations team, and are hosted in Amazon Web Services in a geographical region close to the customer. This deployment uses industry-standard security policies and procedures to ensure the application is 100% secure.

Except where otherwise specified, this document will address the **Cloud** deployment option.

Mitel
Powering connections

Data storage

Mitel Performance Analytics is hosted on Amazon Web Services. Martello uses industry accepted best practices to keep this deployment secure. These practices include Amazon security groups, firewalled ports, ssh-key based machine logins, and key rotation.

Data access is restricted solely to Martello employees, all of whom are under strict confidentiality agreements. Only key engineers may access production data, and then only for the purpose of debugging data-related issues as a last resort. In addition, Martello Support may access your web console to provide guidance as a result of specific incidents or requests.

Audit Log

The audit log file contains records of all actions performed on MPA, when they were performed, who performed them, and where they were performed from. The .csv format audit log can be downloaded for review.

What is logged:

- All instances when devices were created, updated, or deleted.
- All remote access sessions.
- Admin user login.
- User failed login (any user).
- MiXML custom command (no details)
- MIB browser (no details)
- Connectivity test
- User edits (no details)

What is not logged:

- User log out
- Query viewing

Two-Factor Authentication

Two-factor authentication (2FA) provides an extra layer of security for Mitel Performance Analytics systems beyond your user id and password. As a second factor, MPA uses a time-limited passcode generated by another application, with no network interaction. This decreases the risk of hackers compromising your Mitel Performance Analytics account.

With 2FA enabled, users must authenticate themselves using a Time-based One-Time Password algorithm (TOTP) based application, in addition to their username and password, before being allowed to login to Mitel Performance Analytics.

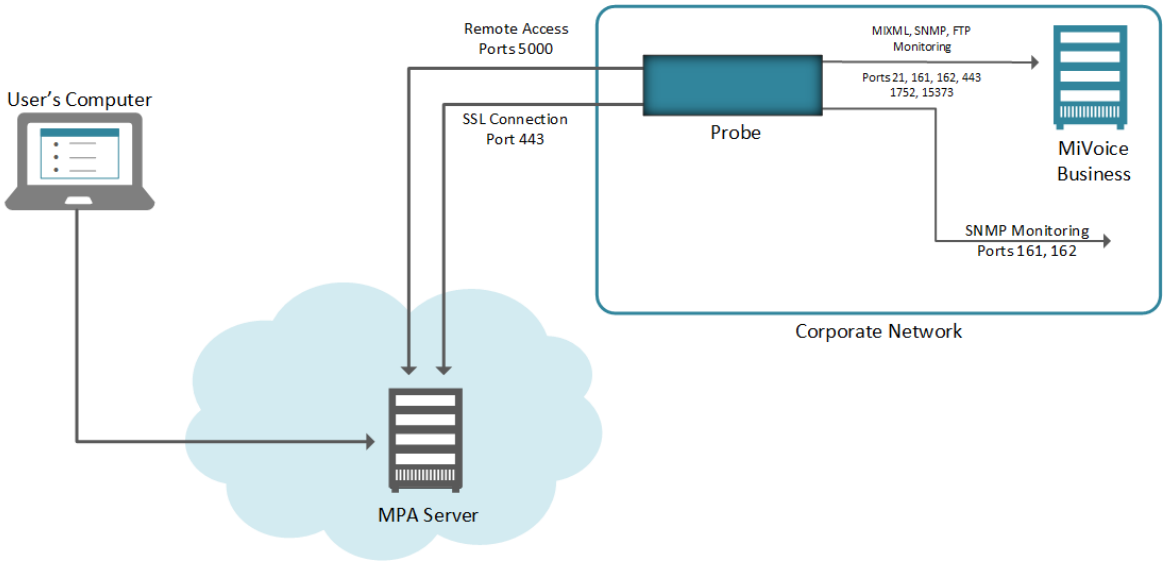
Remote Access Connection Security Features

The Mitel Performance Analytics Remote Access service uses standard IP security mechanisms. The communication links are secured using industry-standard encryption and authentication mechanisms.

System Authentication: Mitel Performance Analytics uses a 2048-bit security certificate and authenticates all connection requests.

SSL: All SSL sessions to Mitel Performance Analytics are encrypted and authenticated using RSA-2048 for key exchange and AES 128 for encryption. Cloud installations of MPA use an SSL certificate signed by an industry-trusted certificate authority. On-premises installations of MPA generate a unique self-signed certificate but can be replaced with a customer-provided certificate.

SSH: All SSH sessions are encrypted and authenticated using RSA-1024 with rotation for key exchange and AES 128 for encryption. Key Rotation is enabled generating a new key for each session. Firewall rules for our Cloud deployments block SSH connections from everywhere except for Martello Technologies offices, and only Martello Operations staff have credentials to access MPA servers.



Remote Access Control Settings: Mitel Performance Analytics provides controls for the Remote Access feature through the Probe Settings page. Users can configure the Probe to:

1. Never allow port forwarding, thereby blocking all remote access capabilities.
2. Allow port forwarding only to those devices monitored by the Probe.
3. Allow port forwarding for all devices on the subnet the Probe is connected to, thereby allowing remote access to devices not monitored by the Probe. The Remote Access panel for the Probe provides information on all active remote access sessions.

Source IP Address Restriction

Mitel Performance Analytics only accepts incoming remote access packets with the source IP address of the user who requested the Remote Access session.

Audit Log Remote Access Records

Mitel Performance Analytics maintains an Audit Log for all Remote Access sessions. The Audit Log records the name of the Mitel Performance Analytics user that initiated the connection, and the IP address of the remote device.

User IP Protocol Security

The link between the user's PC and the Mitel Performance Analytics system uses internet connectivity for cloud-hosted Mitel Performance Analytics. Therefore, any traffic that is sent over this link is encrypted for security.

SSL/HTTPS is used for all connections to Mitel Performance Analytics web portals with security provided by RSA-2048 for key exchange and AES 128 for encryption.

The following table lists commonly used TCP/IP protocols and their encryption levels:

PROTOCOL	SECURE	APPLICATION
HTTP	No	Web
HTTPS	Yes	Web
SCP	Yes	File Transfer
SFTP	Yes	File Transfer
SSH	Yes	Secure Session
Telnet	No	Terminal Session
FTP	No	File Transfer

Mitel cautions against the use of HTTP, Telnet and FTP when using Mitel Performance Analytics Remote Access because the segment of the connection between the user's PC and the Mitel Performance Analytics server is not secured

AWS Security Practices

Mitel Performance Analytics resides in Amazon Web Services (AWS) and is governed by AWS security practices. For more information about AWS, please see:

https://aws.amazon.com/security/
https://aws.amazon.com/professional-services/CAF/#Security_Perspective

Martello Internal Security Audits

Martello has been dedicated to internal security audits and tests since its inception and continues to perform its due diligence in the areas of security vulnerabilities. Martello regularly performs both Intruder and Mend Scans on its environments and documents the results. If at any time a Mitel partner or customer has questions or concerns regarding the latest test results, they simply need to submit a request to support@martellotech.com and a Martello support representative will be happy to discuss our results with them.

Intruder Scan

Intruder allows scans for the following types of vulnerabilities:

1. Vulnerabilities that allow a remote hacker to control or access sensitive data on a system.
2. Misconfiguration, such as open mail relay or missing patches.
3. Default passwords, a few common passwords, and blank/absent passwords on some system accounts.
4. Identification of systems and software which do not need to be exposed to the Internet, such as network monitoring software and administrative interfaces.
5. Encryption weaknesses, including SSL certificate misconfigurations and identification of unencrypted services, such as FTP.
6. Information leaks.

Martello performs Intruder scans weekly and the results of these tests may be requested. You can see an example of Intruder scan results at the end of this document.

Mend Scans

Mitel Performance Analytics includes open-source software, such as third-party libraries. Because of this, it is necessary to continually evaluate the security of the open-source software that we depend on. To ensure the security of Mitel Performance Analytics, we use Mend as part of our development process.

Mend is a vulnerability detection and prioritization software tool that helps developers identify software risks in both open source and proprietary code. Mend is integrated into the software development environment and continuously identifies potential issues as the code is developed and provides automated remediation workflows. Potential risks are identified, prioritized, and resolved as part of every Mitel Performance Analytics release cycle.

MPA-3.3 GA Scan Results

The following images show the results of the Intruder internal scan results for the MPA server.