MITEL PERFORMANCE ANALYTICS

RELEASE 3.5

SECURITY SUMMARY

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

Mitel Performance Analytics Security Summary
Release 3.5 - November 6, 2024

INTRODUCTION

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

On Premises—When deployed on premises, the Mitel Performance Analytics 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 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 Mitel Performance Analytics installation. This architecture also follows the customer's security policies.

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

Unless otherwise specified, this document addresses the Cloud deployments.

REVISION HISTORY

DOCUMENT DATE	DESCRIPTION
November 6, 2024	Mitel Performance Analytics R3.5 General Availability

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 log-ins, 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 Mitel Performance Analyticswhen 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)
- Device operations, including backups and upgrades
- 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, Mitel Performance Analytics 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.

HTTPS AND SECURE COMMUNICATION

Mitel Performance Analytics ensures secure communication by redirecting all HTTP requests to HTTPS. The only exception to this rule is for specific internal operations involving Network Testing, which is a background process that users do not directly interact with.

This exception does not raise security concerns because the network testing processes operate strictly within your secure network environment and do not expose vulnerabilities to the external network, ensuring the security of your data.

HSTS (HTTP Strict Transport Security) is intentionally not configured on theMitel Performance Analytics server to avoid disrupting remote access functionality. Configuring HSTS may cause the MPA Probe to not function as intended. Users must also accept a certificate warning from their browser to allow it.

TLS V1.3 ENCRYPTION

Mitel Performance Analytics uses the TLS v.1.3 encryption protocol and includes the following:

- TCP traffic between the probes and the Mitel Performance Analytics server use TLS v.1.3 wherever possible. Older probes that do not support TLS v1.3 continue to use TLS v1.2 or earlier.
- Probes can be configured to monitor SIP Publish voice quality data using TLS v1.3. To configure a probe to use TLS 1.3, refer to the *Probe Installation and Configuration Guide*, on the Probe Configuration topics in Mitel Performance Analytics *Online Help*.

Note: TLS v1.3 is not supported for Windows probes.

SNMP V3

Simple Network Management Protocol, or SNMP, allows for the secure monitoring and management of devices on a local or wide area network. SNMP v3 includes both encryption and authentication, which can be configured for use either together or separately.

In Mitel Performance Analytics, SNMP v3 can be configured on most devices for the retrieval of device information. SNMP v3 can also be configured as a recipient type when configuring alert profiles.

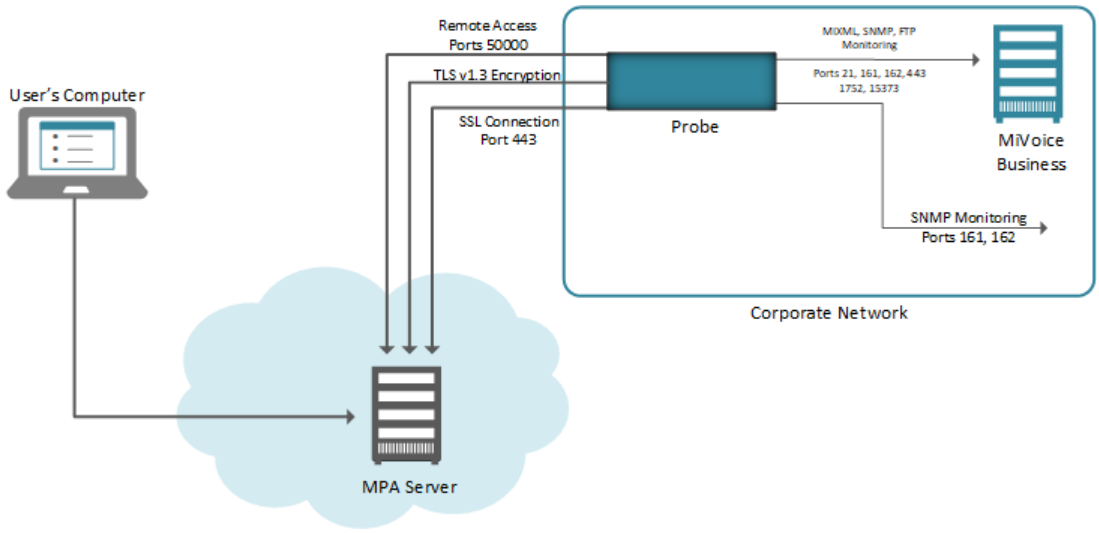
REMOTE ACCESS CONNECTION SECURITY FEATURES

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 oMitel Performance Analytics use an SSL certificate signed by an industry-trusted certificate authority. On-premises installations of Mitel Performance Analytics 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 Mitel Performance Analytics 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.

BROWSER 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.

REMOTE ACCESS SECURITY

The Remote Access Port Forward dashboard panel allows a user to select from a variety of protocols or to specify their own port to connect to monitored devices. Mitel cautions against the use of protocols like HTTP, Telnet, and FTP 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 Dependabot scans on its environments and documents the results. Any vulnerabilities discovered by the scans are dealt with in accordance with a strict security policy.

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 SCANS

Intruder performs scans to check for the following types of vulnerabilities:

- Software and services which are not recommended to be exposed to the internet.
- Information leakage which could be used by hackers to mount further attacks.
- Weaknesses in SSL/TLS implementations.
- Misconfigurations, security best practices, and common mistakes such as exposing code repositories.
- Software with publicly known vulnerabilities.

Intruder also includes internal endpoint scanning for Linux, Windows and macOS devices. The following device checks are performed:

- Local misconfigurations and mistakes such as using default passwords, exposed admin pages, and disabled encryption.
- Internal targets for vulnerable versions of software packages, frameworks and components, including OS patches, software updates and missing server packages.

Intruder also executes penetration tests to identify vulnerabilities that could allow a remote hacker to control or access sensitive data on a system.

Martello runs Intruder scans weekly and the results of these tests may be requested.

DEPENDABOT 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 Dependabot as part of our development process.

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