AVG Business

DATASHEET

Mobile Device Management (MDM)

Mobile, Managed.

Mobile Device Management gives organizations the tools to implement their mobile strategy and manage the mobile experience for end users. Available as part of AVG Managed Workplace®, the features within MDM streamline security, administration, and performance of mobile devices – including organizational assets and devices owned by end users. MacBook® notebooks, iPads®, iPhones® and Android™ devices can all be monitored and managed through a single web-based dashboard. This lets you remotely monitor issues, receive alerts, and respond rapidly to issues from anywhere with an Internet connection, even from smartphones and tablets.

By design, MDM gives you the control to provision, configure, monitor, track, and secure mobile devices – and ultimately protect corporate and personal data in the process.

Benefits

AVG Managed Workplace helps you;

- **Manage large-scale deployments** of mobile devices to ensure adherence to organizational usage and security policies.
- **Protect** personal and corporate data by remotely locking and/or wiping lost or stolen devices.
- **Configure** devices remotely, including standardized implementation of security policies for devices, such as password rules, permissible apps, plus network and email settings.
- **Apply rapid remediation** with the ability to act on availability and security alerts for mobile devices by accessing AVG Managed Workplace on your own device.
- **Manage the end user experience** with monitoring capabilities that ensure ongoing compliance with organizational policies.
- **View a complete inventory** of all managed smartphones and tablets in the organization, drill down to details on individual devices, and take remedial measures when required.

AVG Business Managed Workplace®

Capabilities of MDM Include . . .

Centralized View and Provisioning

With a single web-based dashboard, you can monitor and manage all Android and iOS smartphones and tablets alongside all of your organization's IP-based assets. This centralized view also provides the deeper functionality for rolling out large-scale deployments of mobile devices – all configured for corporate usage and security policies.

Monitoring and Alerting

With AVG Managed Workplace, you can run a network audit and view a detailed list of OS X, iOS, and Android devices. From there, you can create alerts based on availability and security issues, such as when:

- A device is unavailable for a specified period of time. or an Android device has been "rooted.";
- A SIM card has been changed;
- A device "roams" or changes mobile networks (which can raise costs or create issues with billing).

Security

- Rapidly protect sensitive data – including personal data for users and corporate data for your organization. Take the actions you need when a device is lost or stolen.
- Set alerts that notify you when a lost or stolen device is powered on.
- Configure which actions will automatically take place when the "lost" device checks in.
- Lock out access, reset the passcode, wipe the device, or restore it to factory defaults, even disable specific applications, like cameras on devices that are used in highly secure environments.
- Use "selective wipe" to limit the removal to corporate data.

Additional Email Security

- Removing the email configuration profile from a personal mobile device offers additional "end of life" security benefits as well. When user leaves the organization with a personal device, removing the email configuration profile also deletes all corporate mail data from the device.

CANADA / US

☎ **855-254-6989**
✉ **casales@avg.com**

Policies

- Configure security and usage policies then deploy them to customized groupings of managed mobile devices. Also, automatically deploy appropriate configuration profiles when users enroll additional devices.
- Passcode settings for Apple devices such as length, complexity, locking, and the number of failed attempts allowed.
- Network settings for proxy connections, encryption, and more.
- Security and privacy settings, plus limits on data usage.
- Virtual Private Network (VPN) settings that make it easier for iOS and OS X users to connect to the secure network.
- Specific to OS X, you can configure profiles for energy savings, parental controls, restrictions, and software updates, profiles for Exchange, mail, and restrictions.
- Similar configuration profiles are available for Android devices.

Reporting

- AVG Managed Workplace provides a set of reports that provide a comprehensive overview of the mobile environment.
- A device summary that shows the hardware, software, alerts, and traffic information associated with each mobile device.
- A profile configuration that summarizes all mobile device configurations.
- An inventory that breaks down all devices managed by MDM, including summaries by device platform, carrier, and other individual device details.

AVG *Business* Managed Workplace®