Solution overview

Until recently, the Android ecosystem lacked consistent management capabilities for efficient device management across all manufacturers. Securing and separating personal and work data, deploying apps and configurations remotely and silently, and applying policy controls and restrictions on Android devices have been limited and manufacturer-specific.

With Miradore Online and our Android Enterprise solution, companies can securely enable company resources on user-owned (BYOD) devices and fully manage company-owned devices efficiently with a broad set of features on most Android devices running version 5.0 or newer.

<table>
<thead>
<tr>
<th>Features</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic device set-up</td>
<td>Get business apps and configurations easily set-up on any number of devices when the device is powered on for the first time.</td>
</tr>
<tr>
<td>Safeguard data, apps, and device</td>
<td>Business data is separated from personal data in a work profile or protected device-wide on work-managed devices. Utilize VPN and encryption to protect data. IT Administrators can prevent installation of apps and apply app configurations for full control over application usage.</td>
</tr>
<tr>
<td>Manage company apps centrally</td>
<td>IT Administrators can use Managed Google Play to get work apps purchased and published for self service or installed silently. Any apps needed for work are preapproved by the IT administrator.</td>
</tr>
</tbody>
</table>

Benefits

- Use any Android device securely
- Separate business and personal apps and content
- Easy device set-up
Work Profile Solution

The work profile solution is intended mainly for BYOD devices, allowing administrators to manage a self-contained work profile on a user’s personal device. Corporate apps, data, and management policies are restricted to the work profile, keeping them secure and separate from personal data, while maintaining user privacy. Users maintain full access and control of personal information and their device.

Typical use cases for the Work Profile solution:
1. Company-owned, personal use enabled (COPE) device with personal apps and content, company resources isolated in the work profile.
2. Device is owned by the user (BYOD), company resources are enabled and secured in the work profile.

About the Work Profile:
- Isolated and encrypted area for business apps and data
- Access control with a separate passcode
- Remotely managed by IT Administrators using Miradore
- The Work Profile can be removed by the user
- Managed Google Play store with only approved apps available

Work Managed Solution

The work-managed solution is designed for corporate-owned devices that are managed centrally. This allows administrators to secure the entire device and enforce an extended range of policy controls unavailable to work profiles.

Typical use cases for the Work Managed solution:
1. Company-owned device, purpose-built and restricted
2. Company-owned, personal use enabled (COPE) device, company has full access, user is granted limited access

About the Work Managed Solution:
- Device apps and settings fully managed by IT Administrators using Miradore
- User access to the device apps and settings can be limited
- User cannot remove remote management (MDM or EMM) features
- Managed Google Play store with only approved apps available
Delivery specifications

- The Android Enterprise solution is available on the Miradore Online Enterprise Plan.
- Navigate to www.miradore.com and click ‘Get Started.’
- Provide your Company name, login name, and password to create your EMM site.
- You may start to add smartphones and tablets immediately to the service and start securing, controlling and managing your mobile devices.

Requirements

- The Android Enterprise solution requires Android 5.0 or newer.
- A network connection (mobile data, WiFi) must be available.

For more information

For additional information, visit miradore.com/enterprise-mobility-management/