Android Enterprise
Case Study

Indigo Industries

Meet Shelby Council

Shelby is the Head of Mobility for Indigo Industries and has been with the company for seven years, starting as an IT Analyst in the healthcare business unit. They have built a team of 11 people representing the various business units of Indigo. Shelby reports to the Director of End User Computing, Edna Luna.

Shelby considers themselves an Android champion and typically tests the latest devices from top manufacturers. They also keep late model devices of every modern OS on hand for testing purposes. A year ago, Shelby created a strategy to incorporate the latest Android management capabilities into Indigo's IT environment. Their primary goal is to offer her business stakeholders and users choices. Indigo has a reputation for innovation but Shelby has been burned by "science experiments" before and wants to make sure this goes well.

About Indigo Industries

Indigo Industries is a multinational conglomerate incorporated in the U.S. with headquarters in New York, London and Hong Kong. As of this summary, the company operates in the following market segments: healthcare, power, manufacturing, finance, transportation, and oil and gas. Indigo is ranked among the top 2000 companies globally by gross revenue and has locations in 26 countries.

Business problems: Knowledge worker woes

The first business units Shelby is targeting are healthcare and finance. Hayden (Healthcare) and Farah (Finance) are the primary representatives and business stakeholders. They have approximately 20K devices between them. After some inquiry Shelby gives you these stats:

- 5,000 Android
- 15,000 other OS

Hayden and Farah believe they also need to do refreshes in the US and EMEA and would like to focus on lower cost options that can replace expensive devices, with a few Google recommended flagship devices with consistent experiences thrown in. They are unsure which devices they should support and purchase going in the new deployment.

Both business units have dedicated support technicians servicing the users but would like to minimize deployment costs by sending company-owned devices directly to the user, ideally to be provisioned out of the box.

Shelby has had a tough time convincing the Finance steering committee (led by Farah) that Android is a secure solution that can be approved for use within their business unit. Their primary worries are about unsafe applications and frequency of security patches.

Both business units have the same cloud-based EMM provider with different tenants. They are open to considering new providers but do not want Google having access to user identities. They value user privacy on personal devices but need full device control on company-owned devices. Their primary security concerns are data-loss prevention, complex passwords and rooting of devices.

Between the two business units, they have multiple Android and iOS custom business critical apps (3 years old), that were formerly wrapped using the MDM SDK and deployed via the MDM app catalog. They also have a number of key application use cases and security requirements. Indigo is an Exchange Microsoft 365 shop.

Shelby would like a solution document presented within the next two days.

Android Enterprise
Case Study

Indigo Industries

Requirements

- Select minimum OS to determine supported personally-owned (BYOD) and company-owned devices
- Refresh company-owned devices (5K devices in NY and London)
- Convince finance stakeholders that Android is secure
- Identify model that provides anonymized user accounts, dynamically provisioned by the EMM.
- Support personally-owned (BYOD) and company-owned devices
- User-driven provisioning for BYOD; out of the box for company-owned devices

Important policies

Prevent work to personal copy/paste (BYOD)
Disable unknown sources and USB debugging
6-digit work application password (BYOD)
4-digit device PIN security

Key applications

Messaging client
File viewer and editor
Secure browsing
VPN
Camera
Contacts
Email

Android Enterprise
Case Study

Indigo Industries

Case study details for Module 2: EMM, Identity, and Provisioning

Policy groups

1. Finance
2. Healthcare

Identity model

Identify model that provides anonymized user accounts, dynamically provisioned by the EMM.

Use case #1: Personally-owned (BYOD) devices

Solution set: Work profile

Policies

1. Prevent work to personal copy/paste (BYOD)
2. Disable unknown sources and USB debugging
3. 6-digit work application password (BYOD)
4. 4-digit device PIN security

Provisioning method

User-driven

Use case #2: Company-owned devices

Solution set: Fully managed device

Policies

1. Disable unknown sources and USB debugging
2. 4-digit device PIN security

Provisioning method

Seamless device setup, out of the box