✦ **Scalefusion**

Securing Customer Data on KYC Agent Devices with Mobile Device Management

Overview

Remotely manage and secure all KYC agents' mobile devices (smartphones and tablets) from a centralized console. Enforce stringent security measures like passcode policy, app blocking, peripheral control, and remote lock & wipe to protect sensitive KYC data on devices. Stay compliant with KYC standards and other regional regulations like GDPR.

Benefits

- Ensure bulk out-of-the-box enrollment of devices
- Apply device policies relevant to banking and KYC protocols
- Manage (push/remove) apps and content on KYC agent devices
- Keep track of data consumption patterns to optimize data costs
- Remotely troubleshoot device issues to ensure agent productivity

Introduction

As the BFSI industry undergoes a rapid digital transformation, the advantages and significance of Know Your Customer (KYC) practices in banking have become increasingly apparent. KYC requirements for banks involve a rigorous verification process for their customers, following the well-established 'know your customer' policy. This verification process is often referred to as KYC verification. The specific KYC procedures that a bank implements are established according to the regulations of their region or country.

A key challenge in KYC is ensuring consumer data protection, as regulations strictly mandate it. This means KYC policies, regardless of location, must align with customer data protection regulations like GDPR. A Mobile Device Management (MDM) solution can help BFSI institutions stay compliant with KYC and local data protection regulations through effective device policy administration on agent devices.

Let's take a closer look at the role of Scalefusion MDM in ensuring the integrity of customer data and the streamlined management of agent devices that handle KYC procedures and verifications.

Simplified Bulk Enrollment

A good portion of the BFSI workforce is on-field, with many cross-location transfers and new employees onboarding regularly. As mobile device management begins with enrollment, Scalefusion offers the most simplified bulk, out-of-the-box enrollment without end-user involvement. This means that the field agents don't need to spend any time in the enrollment process and can start using the issued devices straight away. While this is not a mainstay KYC-related feature, it goes a long way in ensuring that the KYC and other regional regulatory protocols are adhered to from the onset when IT admins apply device policies.

For maximum security, Scalefusion offers kiosk mode enrollment of devices where they can only run one app (single-app mode) or a set of apps (multi-app mode) based on the role of the KYC agent. In kiosk mode, the device usage is limited to just the predefined app or apps.
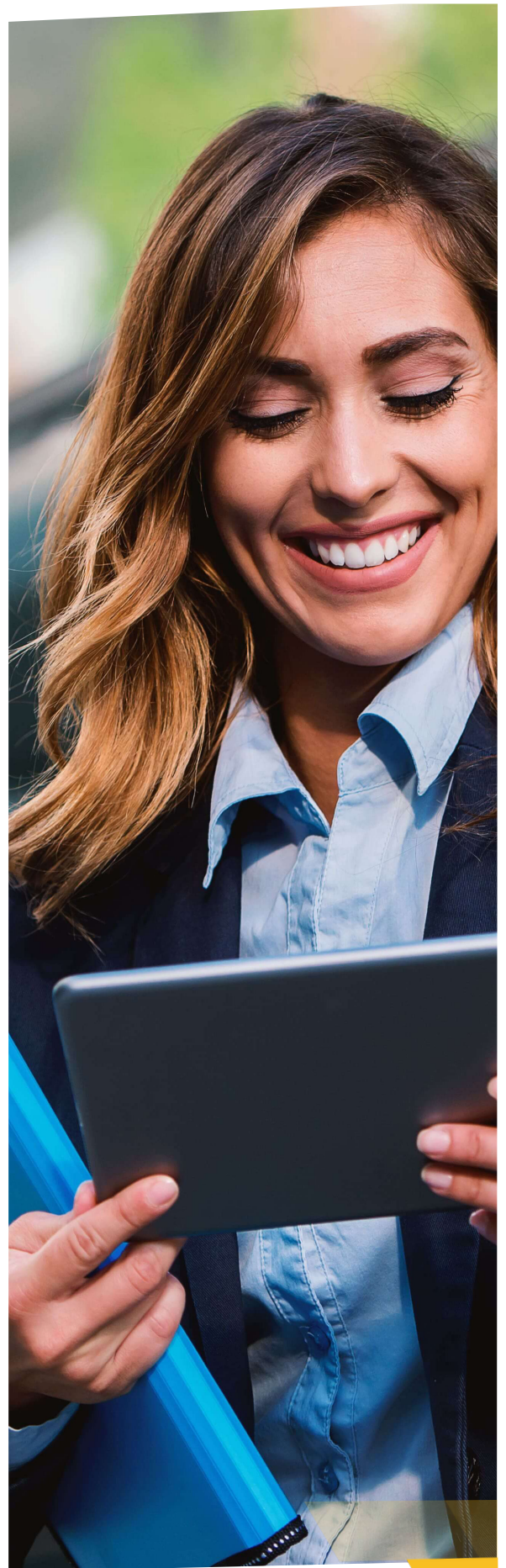
1

Enforce Security Measures

One of the most significant features of Scalefusion, which underscores the need to protect customer (KYC) data, is the capability to enforce security measures on managed agent devices. Based on the KYC compliance and BFSI institution requirements, IT admins can implement a set of security rules or policies. It all begins with a strict passcode policy that highlights the protocols around device passwords. A passcode policy encompasses mandates regarding password length, complexity, change interval, and failed attempts, among others.

In addition to passcode policy, Scalefusion allows IT admins to enforce peripheral control on devices, including USB ports, display, volume, screenshots, and other such device controls. Furthermore, admins can disable device reset through the FRP (factory reset protection) feature. With KYC agents always on the move, device loss or theft is a serious concern. In such scenarios, Scalefusion enables admins to remotely lock the device and wipe the confidential data off it. This safeguards the KYC data from falling into the wrong hands for misuse. BFSI institutions can fortify customer data protection even more by blocking malicious apps that could jeopardize the KYC data that the agent devices contain.

App & Content Management

Customer data security is at the top of the checklist in the BFSI industry. However, the productivity and efficiency of the frontline workforce, like KYC agents, can't be overlooked. The agents must be able to access the right apps and resources while on the move. Otherwise, the KYC verification process can upset customers and waste their time as well. Leveraging Scalefusion's app and content management capabilities, IT admins can ensure the agents have seamless access to the required resources. Pushing and removing apps and content remotely is a matter of a few clicks on the Scalefusion dashboard. The dynamic nature of this feature makes it apt for devices used by frontline or non-desk workers like KYC agents.

Remote Troubleshooting

BFSI field agents can ill-afford device downtime during KYC verification. It can disrupt the whole process and lead to customer dissatisfaction. To ensure agent devices are up and running, Scalefusion offers remote troubleshooting in the form of a feature named Remote Cast & Control. IT admins can therefore address device issues remotely by mirroring the screen onto the Scalefusion dashboard. They can also offer VoIP support when field agent intervention is needed.

Compliance Alerts

In case any device or end-user deviates from the set policies based on KYC and other regulations, Scalefusion provides compliance alerts to IT teams. For instance, attempts to open blocked applications or non-adherence to acceptable battery levels. Compliance alerts help admins stay on top of the applied device and security policies. They can flag non-compliance to higher authorities to avoid any impending customer data violations.
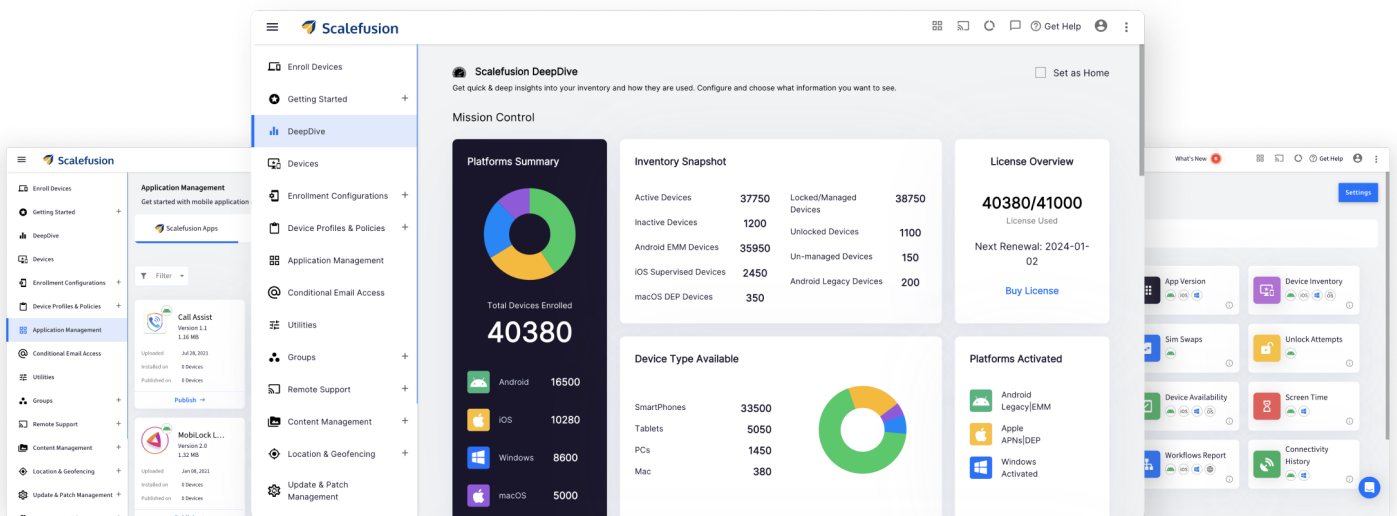
Location Tracking & Geofencing

With Scalefusion, IT can set up geofences for managed agent devices and enable location tracking. Both these features create an additional layer of data and device security. For instance, if, on a given day, field agents are carrying out KYC procedures in a particular location, admins can create geofences and apply them to devices from the Scalefusion dashboard. If an agent breaches the geofence, admins can investigate the cause. Location tracking, on the other hand, lets admins track the devices and take action when they are in a suspicious location where they aren't supposed to be.

Device Reports

Scalefusion provides detailed and comprehensive device reports of agent devices on its dashboard. Device reports allow admins to look into device usage patterns. For the BFSI industry, one important metric of these reports is data consumption. The overview of data consumption helps identify cases of data misuse, if any. This, in turn, can optimize data costs and also identify suspicious internet usage.

Secure Field Agent Devices and Stay KYC-compliant with Scalefusion MDM

An extensive mobile device management software like Scalefusion allows the BFSI industry to manage KYC agents' devices securely. In this highly regulated industry, especially with KYC compliance, customer data protection is of utmost importance, and Scalefusion ensures that through robust security features.

Try it now for free

Register for a free 14-day evaluation at **www.scalefusion.com**

Get a Demo

Request a demonstration and see how Scalefusion can help you in managing your devices and securing your corporate data.

Book a Demo

About Scalefusion

Scalefusion UEM empowers organizations to secure and manage an array of endpoints, such as smartphones, tablets, desktops, laptops, rugged devices, POS systems, and digital signage. With unmatched security and multi-OS support, Scalefusion provides specialized features like OneIdP and AirThink AI backed by a world-class support team—loved by 8000+ global companies across industries.

Enterprise Sales & Partnerships

sales@scalefusion.com

partners@scalefusion.com

Call Us

US: +1-415-650-4500

UK: +44-7520-641664

NZ: +64-9-888-4315

India: +91-74200-76975