

As Secure As Your Devices Can Get

Scalefusion UEM & Check Point Harmony Mobile

Overview

The Scalefusion and Check Point Harmony Mobile integration offers a unified solution to manage, monitor, control, and protect iOS and Android devices against potential threats. This integration brings together seamless Unified Endpoint Management (UEM) features with robust Mobile Threat Defense (MTD) protection, enhancing security comprehensively.

Benefits

- Get an overview of your device risk status
- Move high-risk devices into specific device groups
- Blocklist suspicious websites and block man-in-the-middle attacks
- Set up multi-layered network settings
- Extensive device protection settings from MDM and MTD

Introduction

As of 2024, there are an estimated 7.07 billion smartphones^[1] worldwide, and this number only increases every year. While smartphone use is a part of daily life, it's also how business happens now. 87% of businesses expect employees to use personal devices for work purposes. Almost 62% of Gen Z workers use smartphones as part of their job^[2].

Smartphone Ownership Statistics (Top Picks)

- There are approximately **6.84 billion** smartphones in the world.
- Worldwide smartphone users have **increased year-over-year** by at least **5%** over the last five years.
- There are upwards of **10.47 billion** IoT connections worldwide
- **China** has the most smartphone users in the world
- **Germany** has the most smartphone usage per capita
- **College graduates** are most likely to own a smartphone
- **Android** is the leading mobile operating system worldwide

Smartphones have become a starter kit for anyone and everyone in the workplace. It is a must-have device that makes day-to-day operations and communication more efficient and convenient. 93% of workers under 50 reported using their smartphones for work-related tasks^[3]. It's a no-brainer why organizations and employees rely on smartphones to get by. However, the advent of smartphones has brought about a new wave of sly threat actors who put personal and corporate devices and data at risk.

Cyberattacks Come in Various Forms, Such as:

Phishing attacks

Phishing is an attempt to steal personal information or break into online accounts using deceptive emails, messages, ads, or sites that look similar to sites you already use.

Ransomware

Ransomware is a form of malware that steals sensitive data or locks a device permanently via malicious apps or drive-by downloads and can only be unlocked after paying a penalty.

Unsecured Wi-Fi networks

Unsecured Wi-Fi networks allow you to connect without a password or authorization. Hackers intercept data units transmitted over unencrypted Wi-Fi networks and decode them to retrieve specific login details or sensitive financial data.

App-based threats

Downloadable (but uncertified) applications can present many security issues for mobile devices. “Malicious apps” may look fine on a download site but are specifically designed to commit fraud. Even some legitimate software can be exploited for fraudulent purposes.

Unified Endpoint Management: Scalefusion UEM

Scalefusion’s UEM solution helps manage and secure all corporate and employee-owned endpoints to safeguard device and data security and confidentiality. Scalefusion helps organizations control, manage, and secure their device fleet and data, ensuring all devices are password-protected, updated, and within secure boundaries.

Scalefusion Unified Endpoint Management Features

1. Cross-platform Solution

In modern enterprises that employ a mix of knowledge and frontline workers, there is considerable diversity in the devices preferred by employees or required for the desired business operations. Understanding the need to facilitate this device diversity, Scalefusion MDM supports multiple OS, Android, iOS, macOS, Windows, and Linux and expands to all device types, such as POS systems, Kiosks, IFPDs, and more.

2. Extensive Security Configurations

IT admins can add devices in different groups and sub-groups based on specific criteria they set and push protocols to bolster device and data security right from enrollment.

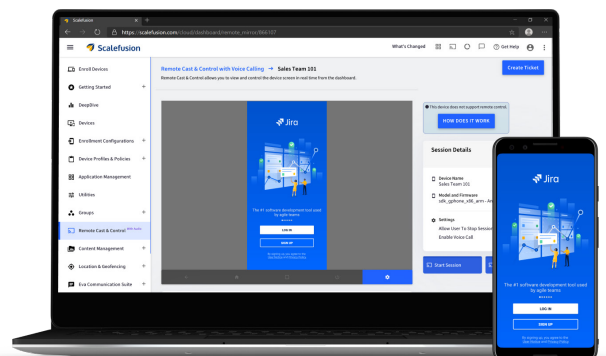
- Enforce password policies
- Enable certificate management
- Prevent factory resets
- Detect failed passcode attempts & SIM swaps
- Disable hardware keys
- Lock/wipe off device data remotely
- Disable device boot in safe mode

3. Application & Content Management

Scalefusion UEM provides extensive content and app management features, enabling IT administrators to selectively organize content across the fleet of managed devices. They can deploy, remove, and configure public and private apps, distribute business-related content files to devices, and remotely update them.

4. Remote Troubleshooting

IT admins can use the Remote Cast & Control feature of Scalefusion to troubleshoot devices and reduce their downtime. IT teams can mirror the device screen and connect to the end-user over a VoIP call to quickly resolve issues or sync files. To support ITSM, admins can take screenshots or screen recordings and create context-aware support tickets directly from the remote session.



Mobile Threat Defense: Check Point Harmony Mobile

Check Point Harmony Mobile is a Mobile Threat Defense (MTD) solution that helps organizations keep critical data stored on corporate and employee-owned devices safe from sophisticated threats like phishing and ransomware. Harmony Mobile gives you a 360° workspace threat prevention from emails, collaboration applications, browsers, unmanaged devices, and everything else that can compromise your security posture. Harmony Mobile ensures your workspace is fully protected against cyber threats.

Mobile Threat Defense Benefits

App and File Protection

Detects and blocks the download of malicious apps in real-time and prevents malware from infecting employee devices.

Network Protection

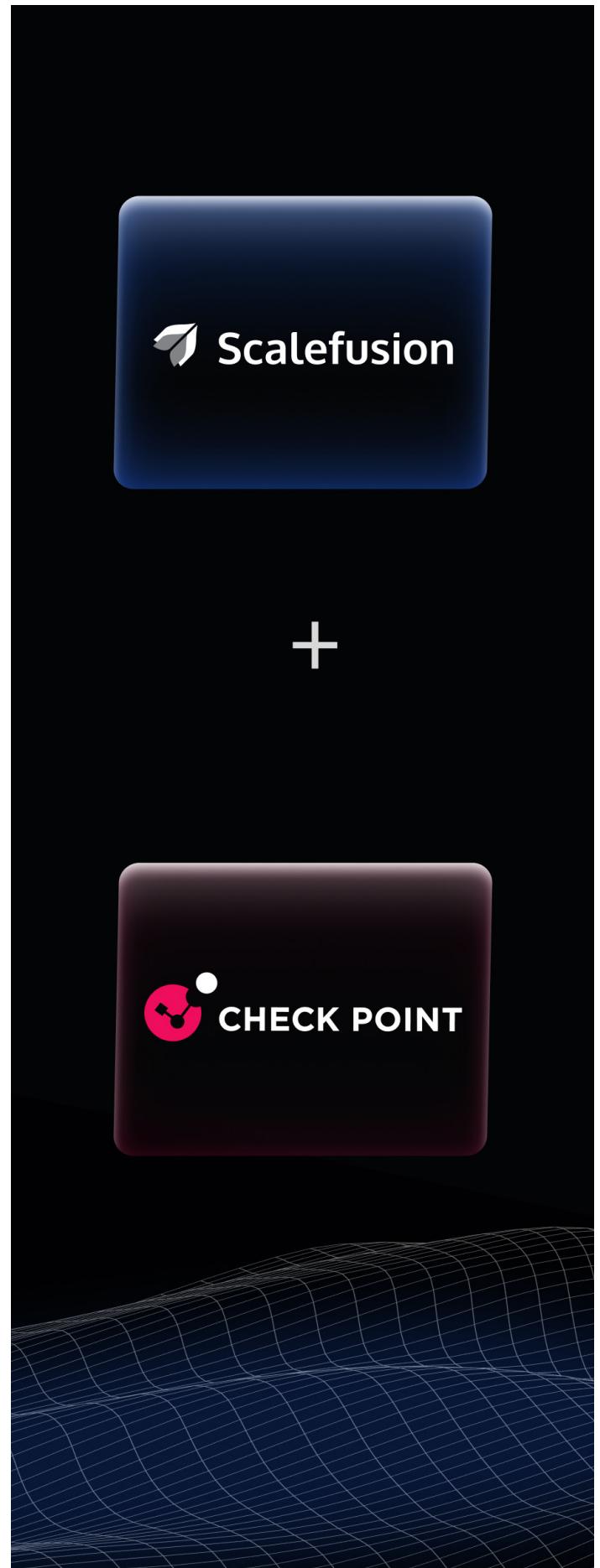
Set Wi-Fi network protection settings with a collection of geolocation, block phishing URLs in SMS, and restrict man-in-the-middle URLs.

OS and Device Protection

By providing real-time risk assessments, devices are shielded from compromise by detecting attacks, managing vulnerabilities (CVE), monitoring configuration changes or insecure settings, and identifying advanced rooting and jailbreaking attempts.

MTD Feature Checklist with Check Point Harmony Mobile

- Blocks malicious apps and file downloads.
- Protects against malware and phishing attacks.
- Eliminates “man-in-the-middle” attacks.
- Prevents infected devices from accessing corporate assets and resources.
- Detects and prevents advanced jailbreaking and rooting techniques.
- Detects operating system vulnerabilities (CVE) and misinformation.



Why UEM & MTD is a Business Essential

Scalefusion’s integration with Check Point Harmony Mobile offers a unified platform to manage, monitor, control, and simultaneously defend and secure your iOS and Android devices against any impending threats. You get an adept combination of seamless UEM and a robust MTD solution, which is what more powerful and comprehensive Unified Endpoint Management is all about!

1. Quick & Seamless Integration

Integrate Check Point Harmony Mobile with Scalefusion in seconds. From auto-installation to silent configuration and publishing, Scalefusion takes care of the rest. Simply integrate Check Point Harmony Mobile from the Scalefusion dashboard.

2. Multiple Security Checkpoints

Define a security policy that covers multiple attack vectors across Android and iOS from the Harmony Mobile portal.

3. Automatic and Updated Risk Scoring

Keep a tab on the device posture by looking at the consolidated summary or device reporting.

4. Automatic Remediation

Set up quarantine groups to automatically restrict device usage or adjust policies based on the risk score.

Scalefusion + Check Point Harmony Mobile: Enhance Your Security Posture

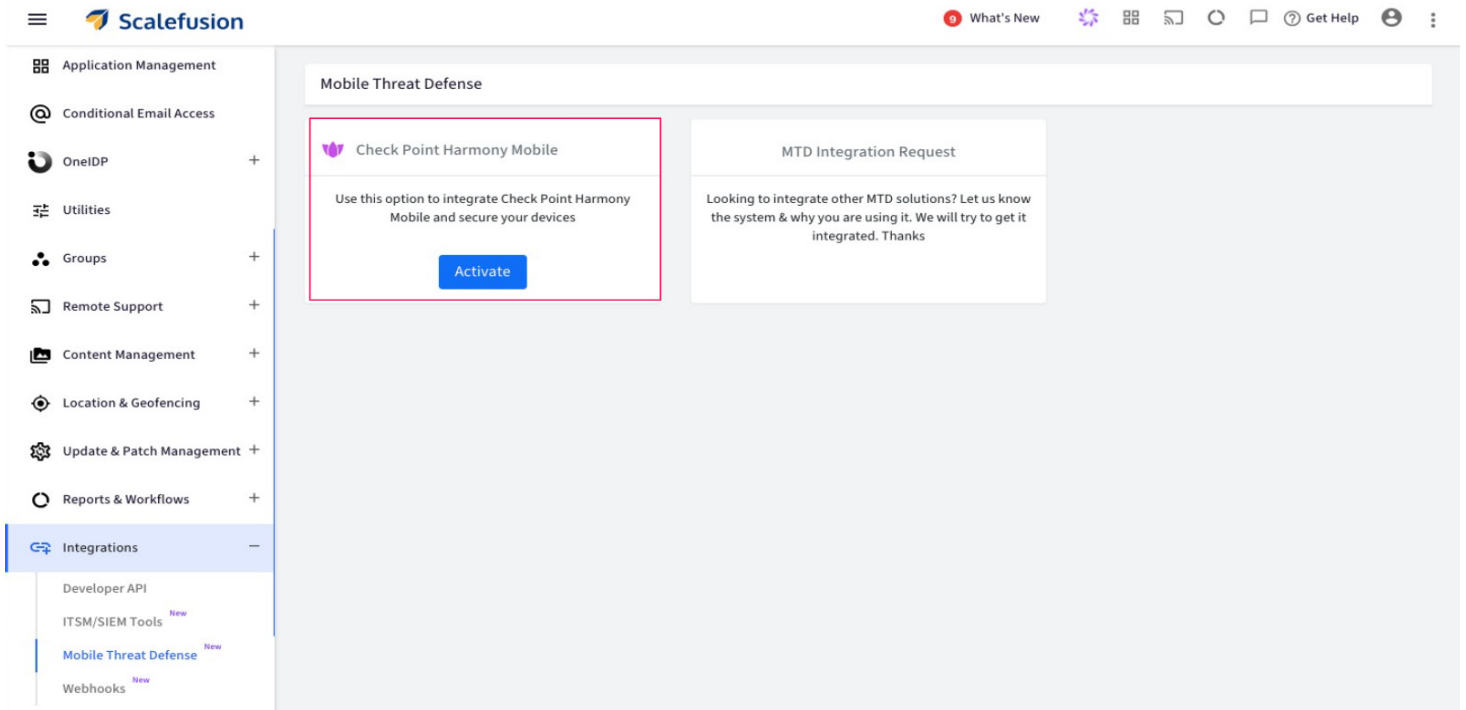
The additional layers of security organizations get with MTD & UEM features when bundled together include:

- Move devices to quarantine groups based on risk status
- Download reports for devices that are at risk
- Get an overview of all the device data and usage on Scalefusion UEM as well as CheckPoint MTD device analysis
- Set “risk status” conditions to OS vulnerability based on security patches, OS versions, and push updates via Scalefusion
- Create an allow list and block list of websites and apps, as well as add detections for man-in-the-middle URLs
- Set Wi-Fi and network settings and enable the collection of the GPS location of a device if a network attack is detected

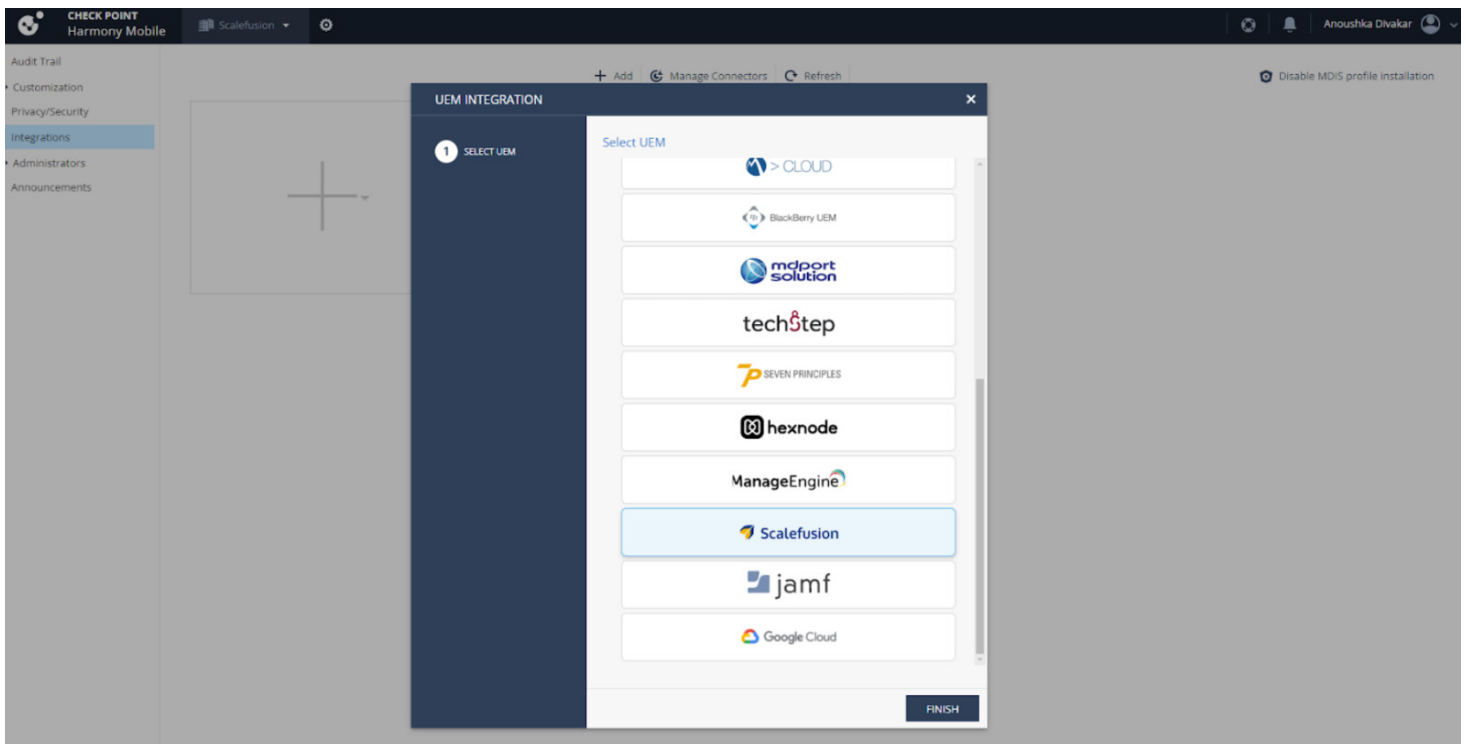


The Integration: Step-by-Step Process

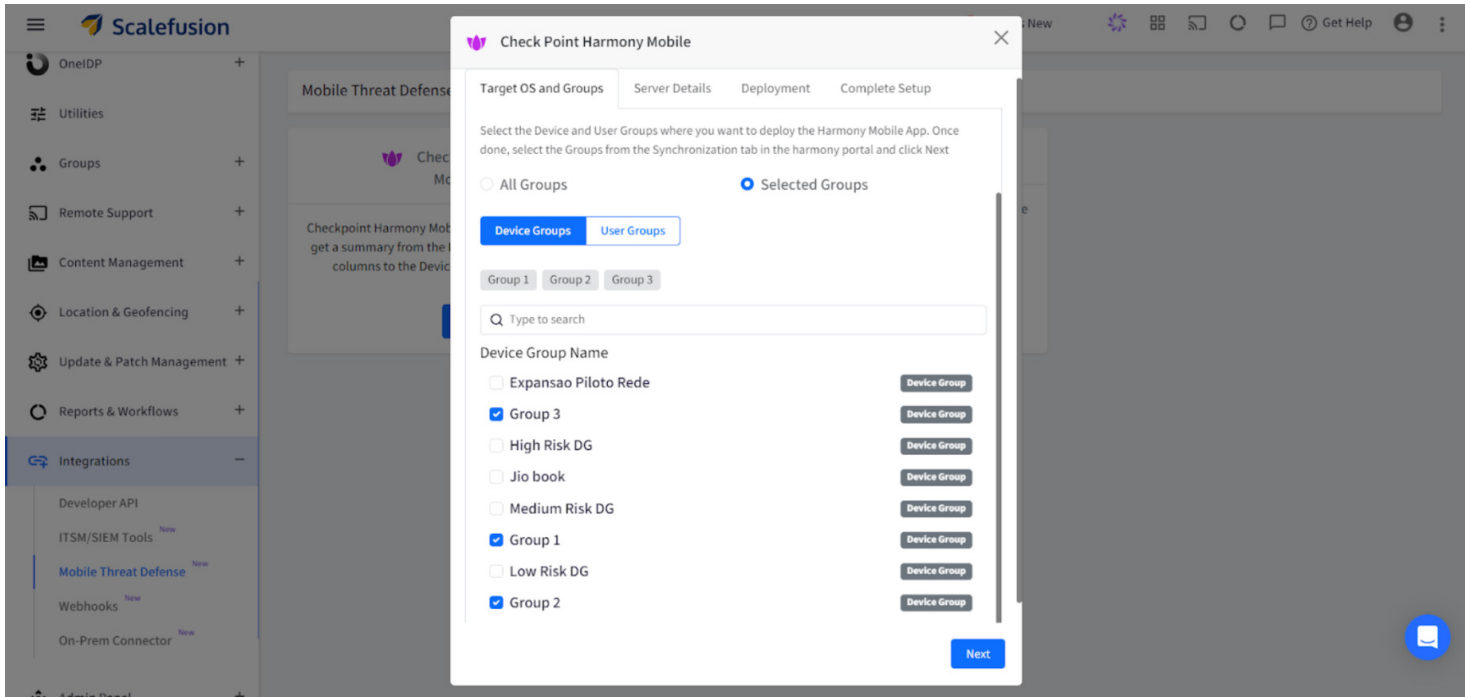
Step 1: Log into your Scalefusion dashboard and head to the integration section. Select Check Point Harmony Mobile and click on “Activate”.



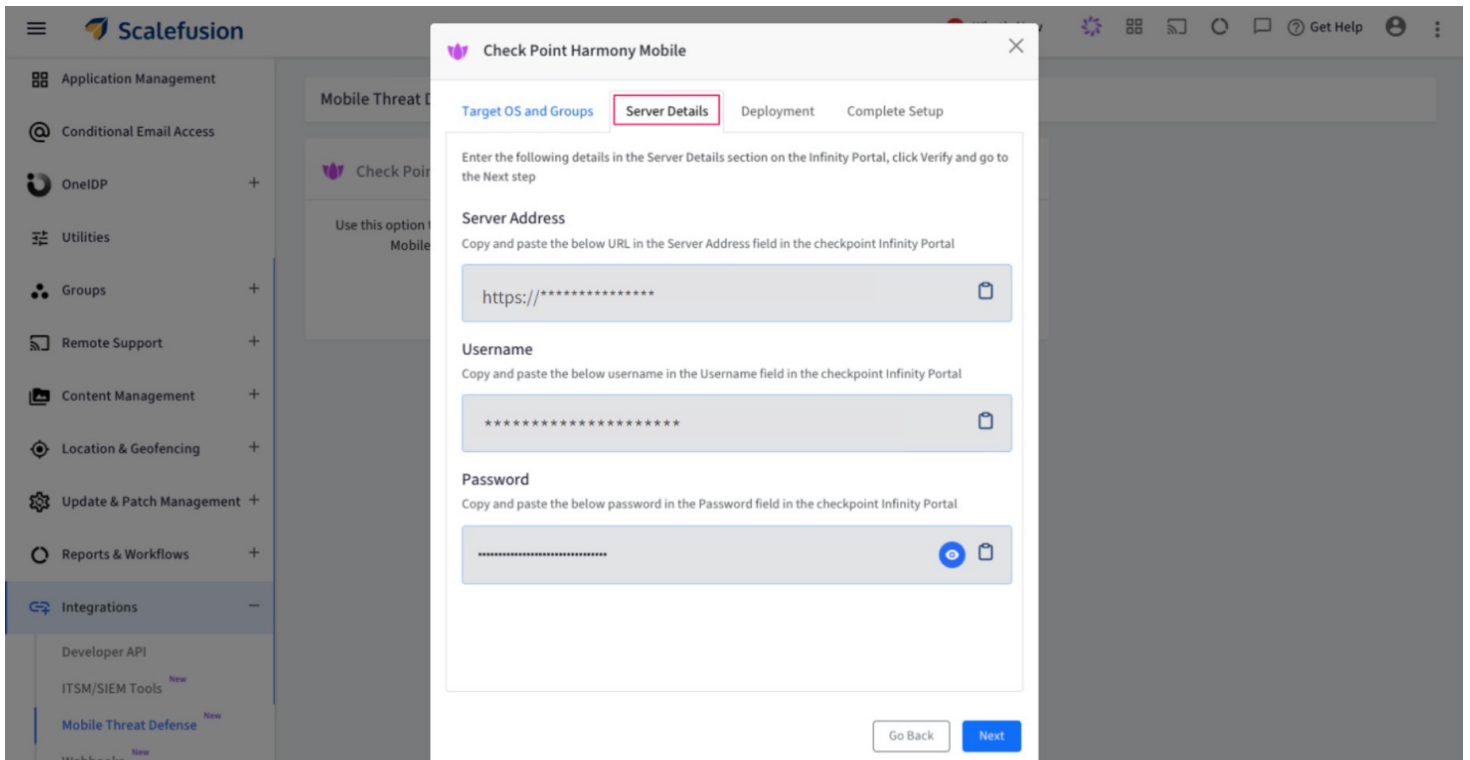
Step 2: Navigate to the Check Point Infinity Portal> head on to Harmony Mobile, select Start a Trial, Sync with UEM, and select Scalefusion.



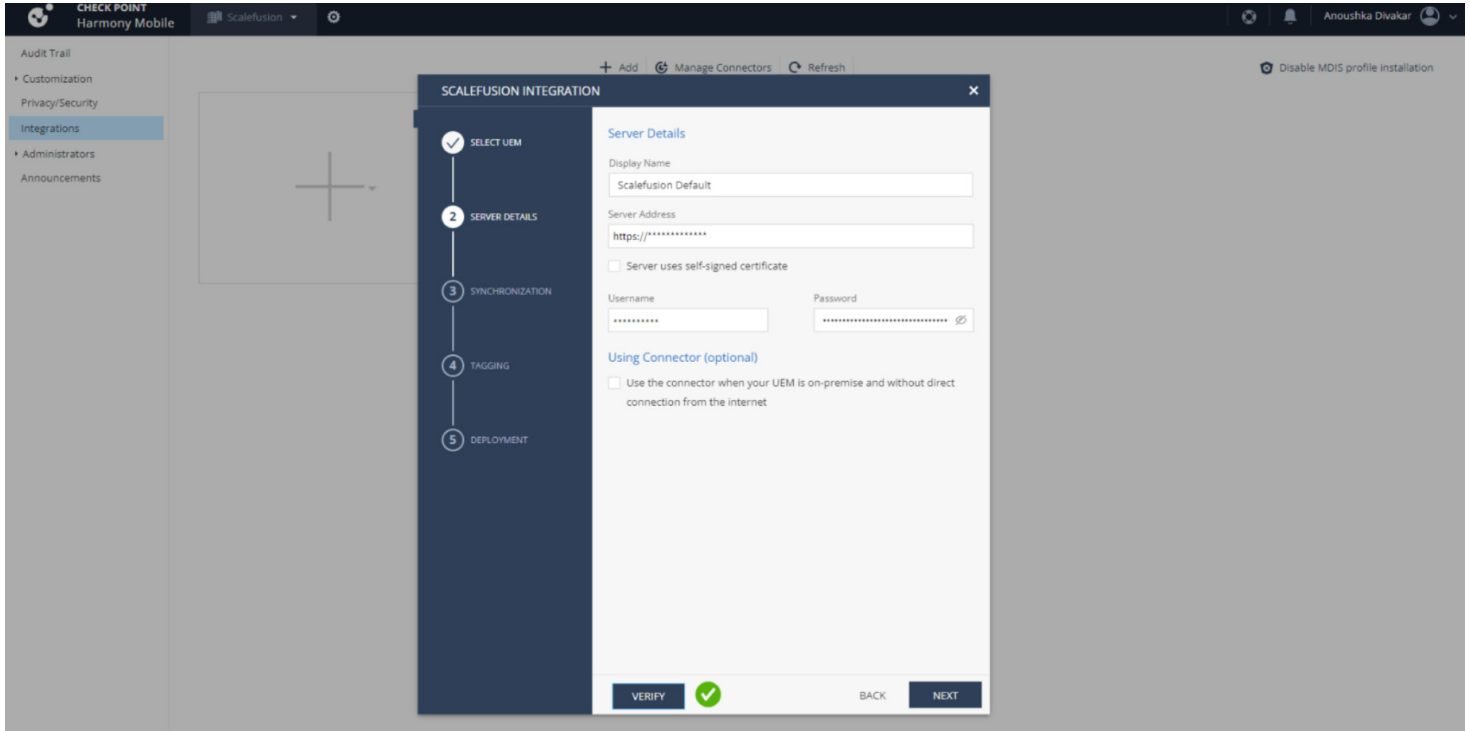
Step 3: Choose the operating system you'd like MTD to target, select the user groups to which this should apply, and click next.



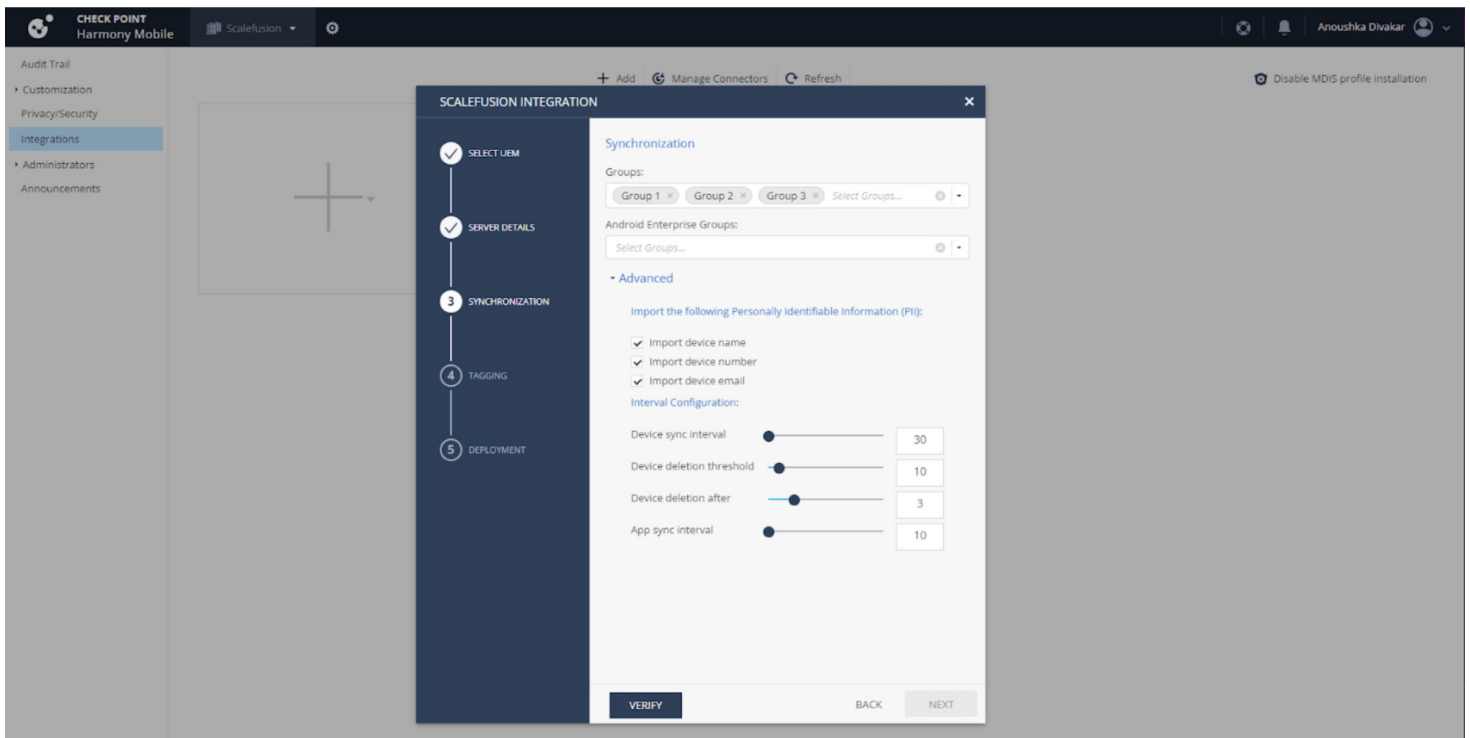
Step 4: Copy the server details provided on the Scalefusion dashboard and apply them to the Check Point Infinity Portal.



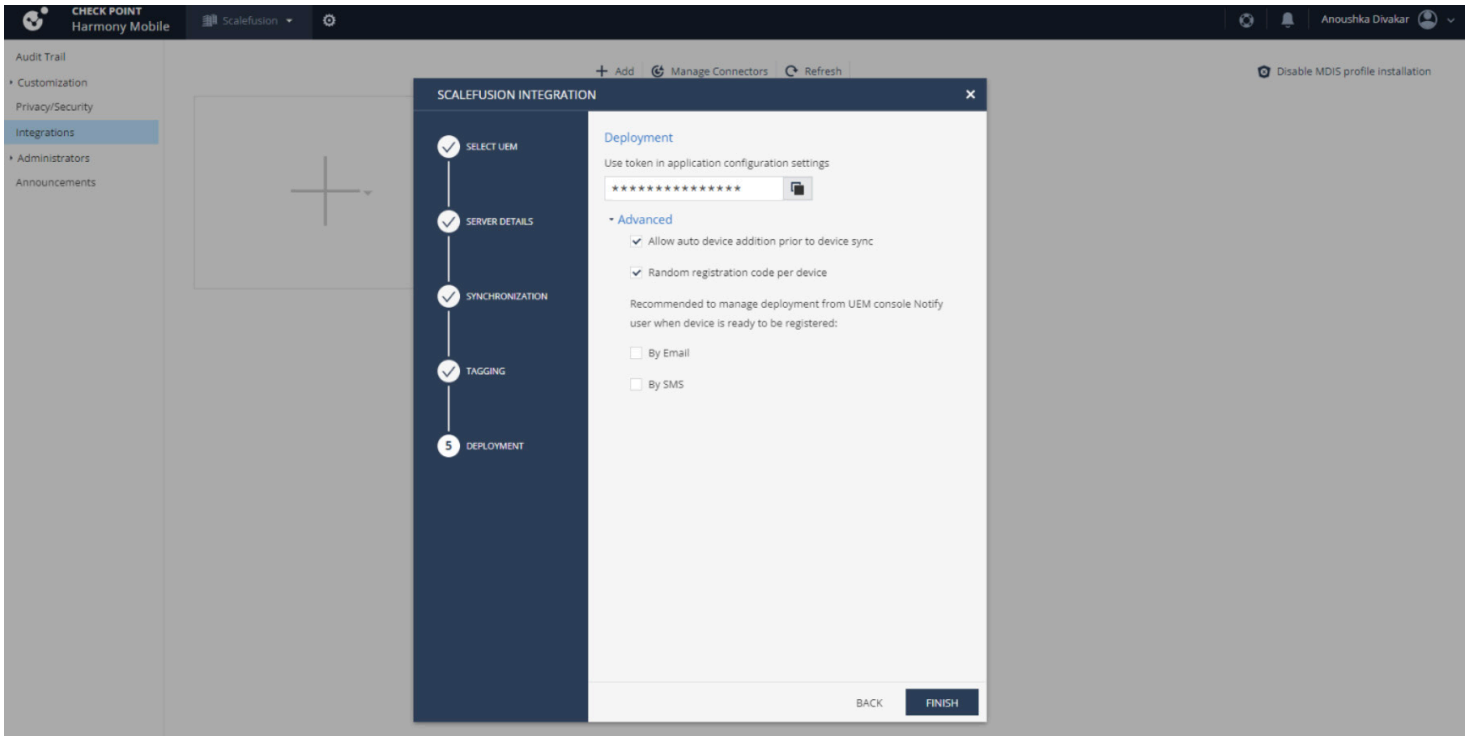
Step 5: Paste the server details in the Server Details section of the Check Point Infinity Portal dashboard.



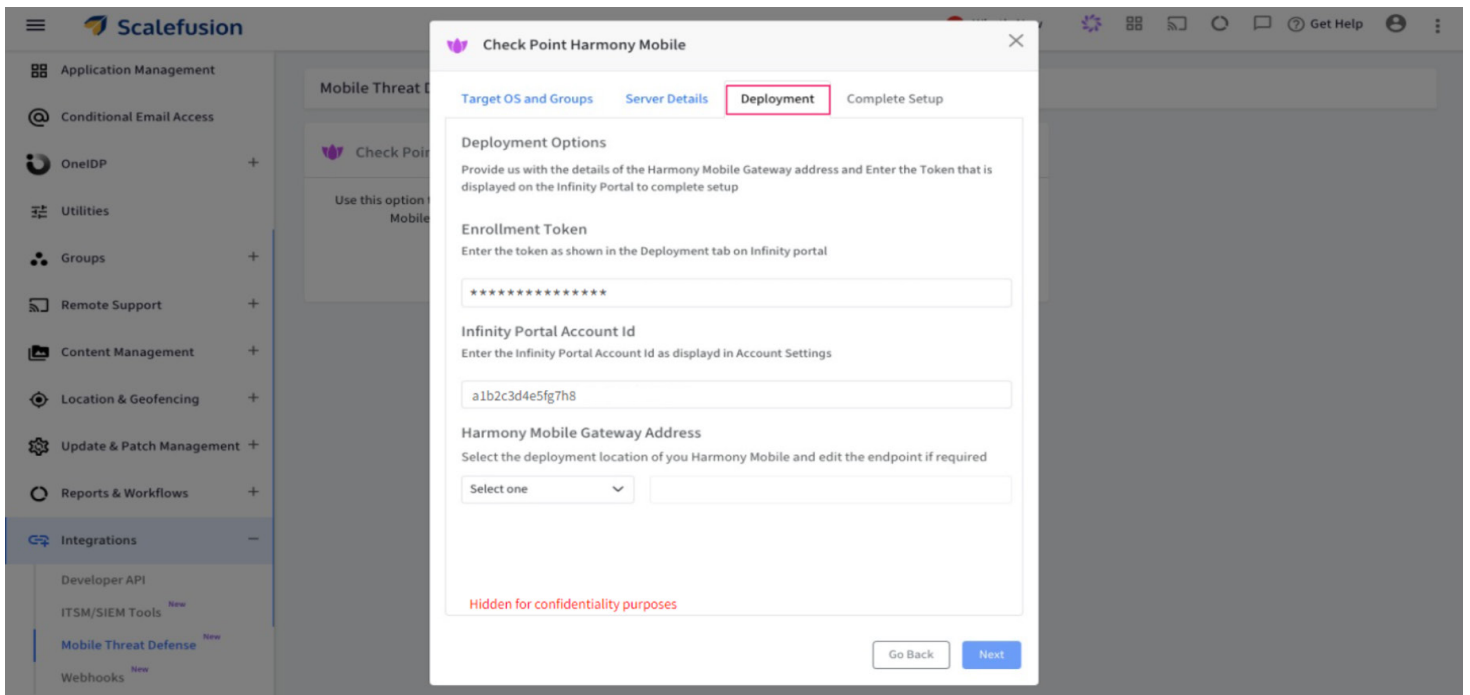
Step 6: Now, similar to the target OS and user group settings chosen on Scalefusion’s dashboard, apply the same in the following step after the server details. This synchronization step helps align the settings chosen on both dashboards. Once selected, click apply.



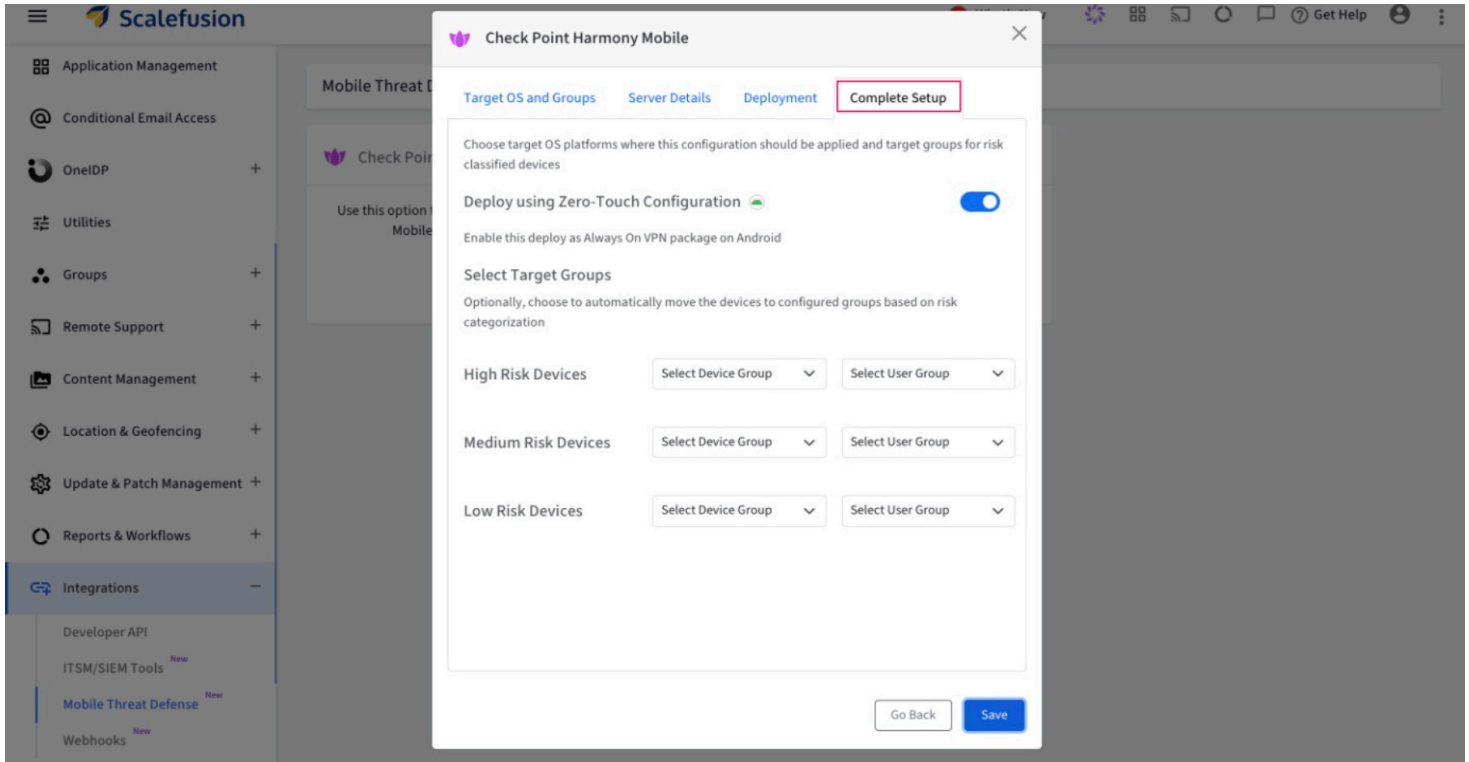
Step 7: The final step on the Check Point dashboard will give you a deployment token ID. Copy this ID and switch to the Scalefusion dashboard. You can now click apply on the Check Point dashboard as this completes the final step.



Step 8: On the Scalefusion dashboard, the next step is Deployment. Apply the copied deployment ID received from the Check Point dashboard into the Enrollment Token section on the Scalefusion dashboard. Next, input your Check Point Portal Account ID found within the Check Point dashboard: Settings>General. You can also define the region where the MTD is to be deployed or you can select Others and provide your custom URL. Then click next.



Step 9: Now head on to the last formalities of the set up and click “Save”. You’re all done.



Summary

You need to gear up for data and device risks as digital transformation becomes more widespread than before. You must ensure your IT infrastructure has no gaps that allow data mishaps. Endpoints must be well-secured to make critical information unavailable for malicious use. MTD from Check Point Harmony Mobile is ideal to ensure your devices have an elevated security posture. At the same time, a UEM solution like Scalefusion can ensure your devices are managed, updated, controlled, and monitored via the latest device management capabilities.

Reference:

1. Exploding Topics
2. & 3. Gitnux



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, laptops, rugged devices, POS systems, and digital signage, all from a single dashboard. It supports multi-OS, giving IT admins a one-stop solution. With unmatched security and compliance, Scalefusion provides specialized features like OneldP 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

Copyright© 2024 ProMobi Technologies. All rights reserved. Scalefusion, the Scalefusion logo, and other marks appearing herein are property of ProMobi Technologies Pvt. Ltd. All other marks are the property of their respective owner/s.

Call Us

US: +1-415-650-4500
 UK: +44-7520-641664
 NZ: +64-9-888-4315
 India: +91-74200-76975