Zero-touch device management

The smarter way to manage your endpoints

WHITE PAPER

hexnode

TABLE OF CONTENTS

Introduction

Device management is a blanket term that serves so many purposes. For some, it can be referred to as controlling a group of devices dedicated to a specific use. For others, it could mean managing employee devices in an enterprise or even managing devices used for business purposes. All these devices carry sensitive data, which demands a medium to manage all this.

Not having a centralized platform to monitor all your devices can create operational challenges. Device management tools are the perfect solution to this dilemma; providing comprehensive capabilities to control fleets of devices without compromising employee experience.

Device management solutions took themselves to the next level with the introduction of Zero Touch policies, which enabled devices to be ready for enterprise usage from the first boot. Combined with a suitable Unified Endpoint Management (UEM) solution such as Hexnode, zero-touch management policies can be leveraged to automate a wide range of tasks that take a significant amount of time and resources from IT teams. Let's delve into some important aspects of having zero-touch device management for modern workplaces.

1

Necessity of device management

In 2021, the size of the global device management market was estimated at $3.97 billion. The market is expected to grow at a CAGR of 23.9% from 2022 to 2029, rising from USD 4.75 billion in 2022 to USD 21.30 billion. The market is expanding as more industries, including healthcare, IT & telecommunications, adopt more mobile-related software.

Source: Fortunebusinessinsights

Devices such as smartphones, laptops and tablets are increasingly crucial to the operations of almost every enterprise. If the health of these devices is not kept in check, it can seriously disrupt workflows.

However, setting up and troubleshooting each device is not feasible as it may take up a lot of time. Having the necessary device management tools can significantly reduce the effort by enabling the management of these devices from a centralized platform.

This becomes increasingly important in modern work cultures, such as BYOD (Bring Your Own Device).

STRENGTHENING SECURITY

The first step of configuring enterprise devices is providing employees access to the necessary data and resources. If not handled properly, this can lead to many security concerns. Data breaches can cause plenty of problems for enterprises. Hence, keeping corporate data safe from threats and separated from personal data becomes a necessity. Containerization is a crucial feature that device management solutions leverage to make this happen.

GAINING EFFICIENCY

Since device management solutions are centrally managed, it reduces the time and money spent on IT administration. For example, it might take around 60 minutes to set up a corporate device manually, and a device management solution can reduce this to an average time of 5 minutes. Also, it can automate many other operations, such as application management and software updates. The savings on time can be directly converted to cutting down expenses if we consider the salaries for IT managers or fees for IT service providers.

2

Challenges of device management

The evolution of device management in the corporate scenario has been tremendous. Its features have been highly convenient to workers, as it grants them access to all necessary resources no matter where they are. However, IT administrators are working harder than ever to maintain integrity when securing corporate resources and networks. Let's look at some challenges companies face when performing device management.

MIGRATION

Organizations might have to migrate to other device management solutions from the current one for various reasons—to save on expenses or to have more functionalities. However, migration has its own operational challenges.

In addition to the set-up time, it also comes with a lot of confusion between the employees. Therefore, it is essential to have a solid communication plan to execute a seamless migration. This is one challenge that the administrators must figure out before migrating to a different device management solution.

UNAUTHORIZED ACCESS

Unauthorized access is when a person enters a computer network without permission. This might lead to the theft of corporate intellectual property and can cause severe damage. Cybercriminals often do this to get unauthorized access to operating systems by exploiting the vulnerabilities in the software.

Another way attackers do this is by exploiting features such as Single Sign-On (SSO), which leave the information on the device to allow the user to login to access several services without re-entering authentication factors. During this time, anyone else with access to the device may be able to access unauthorized data.

Newer devices employ advanced security features such as biometrics to prevent this unauthorized access.

ACCOUNTING FOR MULTIPLE DEVICE TYPES

Enterprises use devices that run various operating systems. If the device management capabilities don't accommodate the difference between these devices, that may become a hurdle to the workflow.

Managing the various devices equally will require carefully selecting ideal device management tools.

COMPLIANCE MANAGEMENT

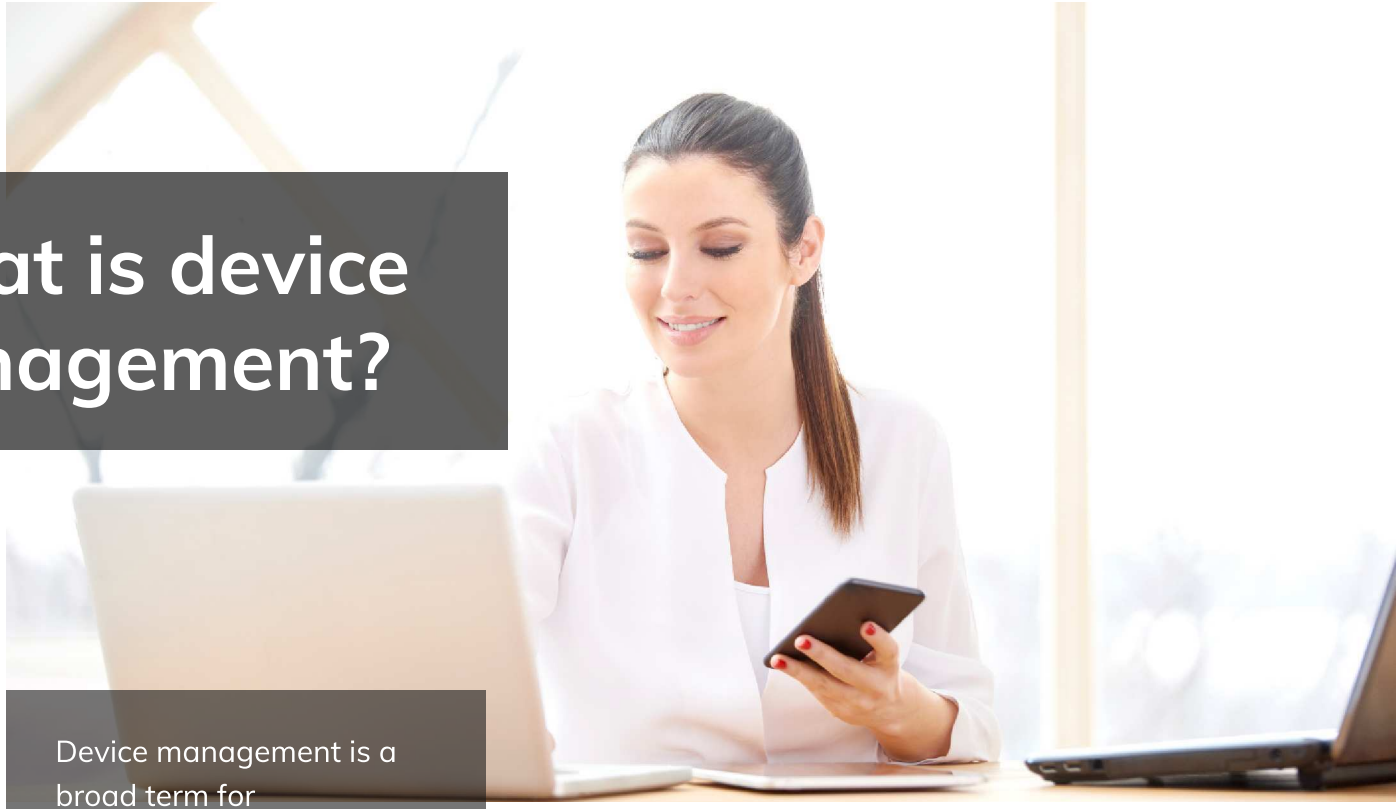
Regulatory compliance is a set of standards that aims to meet the privacy and security requirements of authorities, markets, and clients from a commercial standpoint. As federal government bodies create these, failure to adhere to them will result in hefty fines and penalties. IT teams often use device management tools to ensure the devices are compliant. A robust device compliance policy combined with a device management tool, which is up to date with the device environment, is crucial for organizations to achieve device compliance.

BYOD

Even though Bring Your Own Device (BYOD) policy is proven to have improved productivity, it comes with some challenges.
Managing BYOD devices requires careful consideration, such as more robust security measures, malware protection, efficient password management, and data access control.
There should also be a stringent enrollment and exit strategy to overcome the limitations of these BYOD devices.

3

What is device management?



Device management is a broad term for administering and maintaining devices, including mobile devices, physical computers, IoT devices and other virtual machines. Device management solutions are critical to any enterprise's IT operational strategies.

In the present scenario, as organizations support both on-premises and remote workforces, it becomes crucial to have a robust device management strategy.

FEATURES OF DEVICE MANAGEMENT

- The toolset to remotely configure settings and accounts, deploy and update software, and monitor device statuses.
- Manage devices running different operating systems, such as Windows, Android, macOS, and iOS, from a central platform.
- Automate the deployment of applications.
- Enforce substantial security restrictions.
- Provide conditional access to corporate data.

and many more.

MANAGING HETEROGENEOUS ENVIRONMENTS

Device diversity has long been a problem in the workplace; cross-OS devices, tablets and mobile devices, and personal devices bring different complexity levels to the IT department's device management process. Many organizations have been compelled to reconsider how devices are distributed and controlled due to the workplace's growing device heterogeneity, the COVID-19 pandemic, and the consequent rise in the popularity of remote work.

Although a hurdle, enabling mobile devices is not impossible. All devices brought into the work environment can be separated into groups like BYOD, COBO, COPE, or CYOD. While BYOD, COBO, COPE, and CYOD provide ways to enable mobile endeavors, they differ significantly in fundamental ways that could impact your business and user experience. Therefore, leaders must choose the strategy that best aligns with the culture and needs of the organization.

Bring Your Own Device (BYOD)

Organizations allowing employees to use their personal devices for work is becoming quite common in the corporate world. This is what is known as BYOD - Bring Your Own Device.

To maintain employee trust, BYOD in the workplace often necessitates setting clear boundaries for what will or will not be monitored. It must be clear what the organization can and cannot see if they decide to install an agent on user-owned devices to monitor usage, implement conditional access controls, or for any other purpose. It is not within the corporation's purview to monitor the equipment's personal use.

Corporate Owned Personally Enabled (COPE)

COPE is currently considered a BYOD substitute that maintains business security while also giving employees the flexibility they desire. While employees use equipment provided and authorized by the company, they are also free to use it for non-work-related purposes. For this method, IT loosens the restraints a little bit, but they can still keep an eye on how devices connecting to the network behave. This implies that IT may easily restrict the hardware, services, and apps that employees can use in addition to monitoring and protecting devices. The devices still allow users to publish, tweet, and play games and use them for work. In addition, they can pick from a selection of IT department-approved services and applications. This strategy is far more successful in preventing employees from using applications that might damage hardware and line-of-business resources.

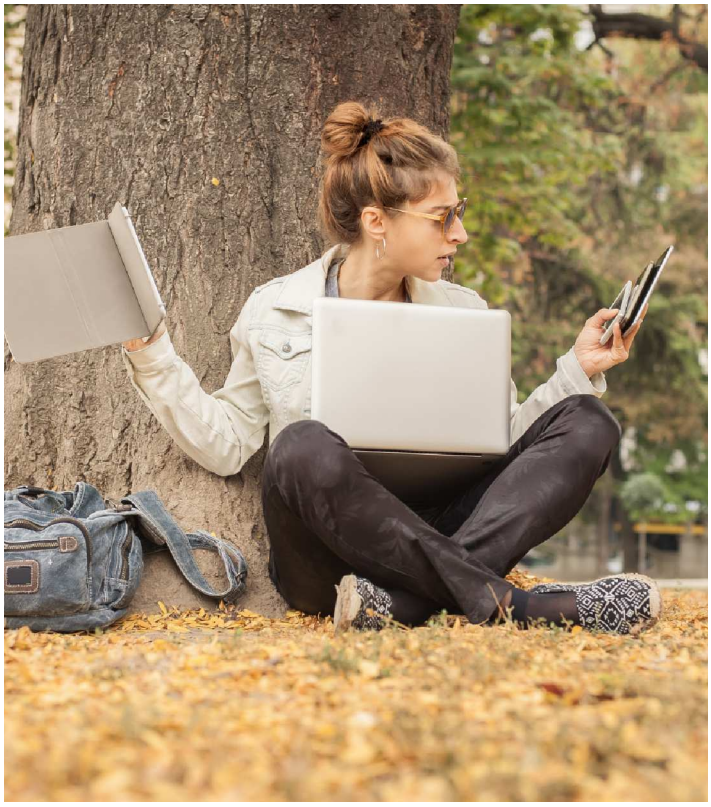
Company Owned Business Only (COBO)

COBO extends COPE by forbidding personal use of the equipment. The popularity of the BlackBerry among businesses as an enterprise-grade mobile device persisted for a while and is still very much present in COBO strategies. Devices categorized as COBO are frequently kiosk tablets, Zoom Room controllers, and other items used by the entire company rather than just a single person. However, it is feasible for people to own COBO equipment, such as a smartphone provided by their employer but with rules against personal use.

Although COBO devices are excellent for tracking corporate productivity and security, they severely restrict users and prevent them from using a single device for work and personal use. Nevertheless, COBO is a suitable solution for businesses wishing to improve security and compliance or struggling to keep personal and business data separate.

Choose Your Own Device (CYOD)

Through CYOD, employees are given a selection of devices to pick from. As long as they do so within the confines of the device management policy that IT has already created, this provides employees more freedom and flexibility to select the device that works best for them. In addition, the managed approach reduces the cost of support. Fewer device kinds and configurations mean cheaper and simpler support, and support staff only need training on a few devices.



In some circumstances, employees have the choice to decide and pay for the selected equipment, transferring ownership to them in the process. This strategy is a middle ground between the conventional BYOD and COD approaches.

COMPONENTS OF DEVICE MANAGEMENT

Enrolling and provisioning

The First phase of managing any device involves enrolling it and then provisioning it with the necessary configurations. Enrollment is the first step in the UEM lifestyle. Enrolling the device onboards it into the UEM solution. Android, iOS, macOS, and Windows all have different ways of enrolling devices. The next stage in the lifecycle is the provisioning of devices. The provisioning phase is where the devices are made work-ready.

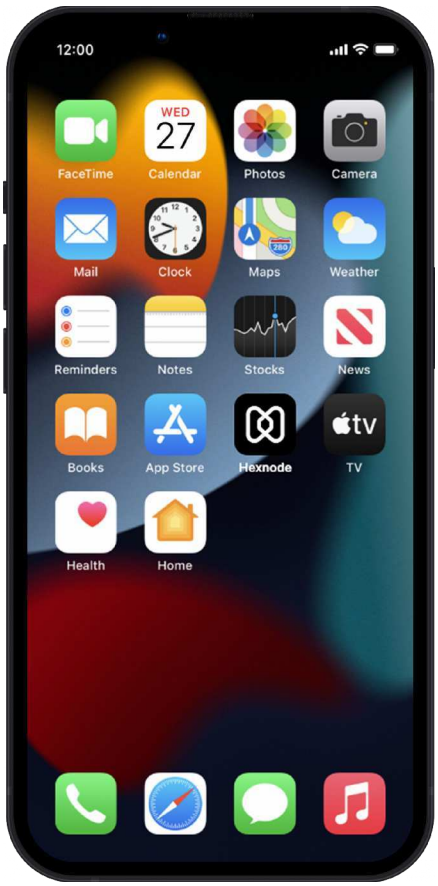
The policies that enable the IT teams to ensure the devices adhere to the guidelines outlined by the authorities are pushed to the devices. Today, the admins can provision the devices to allow them access to fix any issue on the device remotely. The various methods used for the purpose can be either semi-automatic or fully automatic. While semi-automatic enrollment methods require some level of user intervention, fully automatic enrollment methods require zero involvement from the user's side.

App management

One of the most common interactions anyone can have with a device involves apps. Therefore, app management is an essential component of device management that refers to the suite of features employed to manage apps on a device. Essentially, app management allows the admins to push, configure, secure, monitor and update apps for the enrolled devices. In addition, administrators are responsible for ensuring end users have access to the applications they require for their tasks. Challenges faced here include:

- There are many different sorts of devices and apps.
- Organize apps on both company and user-owned devices.
- Make that the network and data are secure.

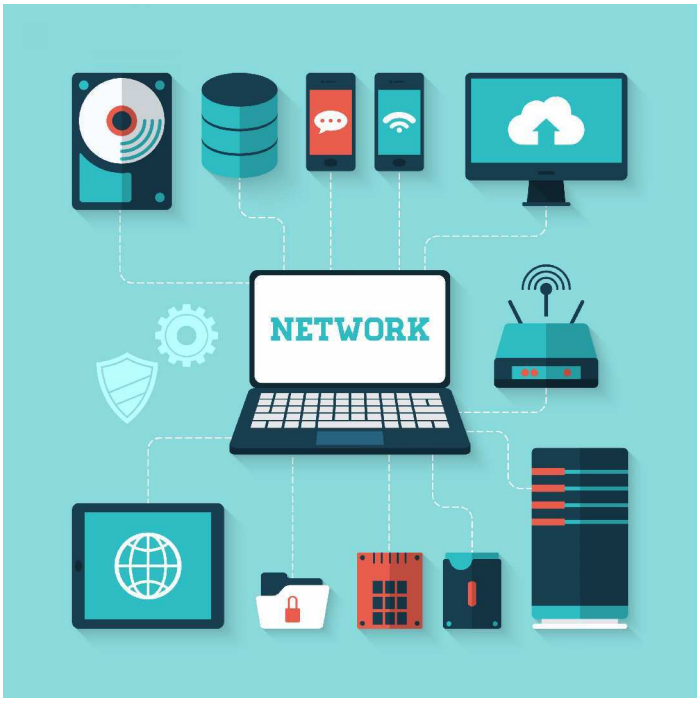
App management typically enlists whitelisting and blacklisting features to ensure the devices only have the work-essential apps.



Network management

Network management is setting up, keeping track of, and controlling a network's functioning. The three most important capabilities of a network management tool are directly related to how well that platform unifies sites and remote workers when managing a complicated or highly scattered network:

- The value that IT teams will derive from the solution is directly impacted by its ease of adoption and deployment.
- A platform that can control the entire network's breadth, from access to WAN to IoT.
- No matter how you decide to deploy, admins must give the security, control, and handling of network data equal attention.



Network management has developed over the last ten years to support IT teams to operate more quickly. It now incorporates advanced analytics, machine learning, and intelligent automation to improve network performance continuously. In addition, these network management tools are being used more frequently in the cloud and hosted environments as businesses adjust to a more distributed workforce.

Content management

Every company has a lot of information, but not all of it may be accessible to all personnel. Larger corporations have a lot of data and numerous people, necessitating multiple security levels. The current situation calls for distributing the appropriate content to the appropriate audiences, and Mobile Content Management (MCM) provides the answer.
MCM is the term used to describe the quick and secure transfer of data to and from devices owned by authorized personnel. Unified Endpoint Management (UEM) solutions provide content management capabilities like data uploading, file distribution to particular users, and secure repository storage.

Other features provided by MCM include the ability to collaborate with other users to edit files saved in the cloud. This allows staff members to work together and access business information from anywhere.

Device security management

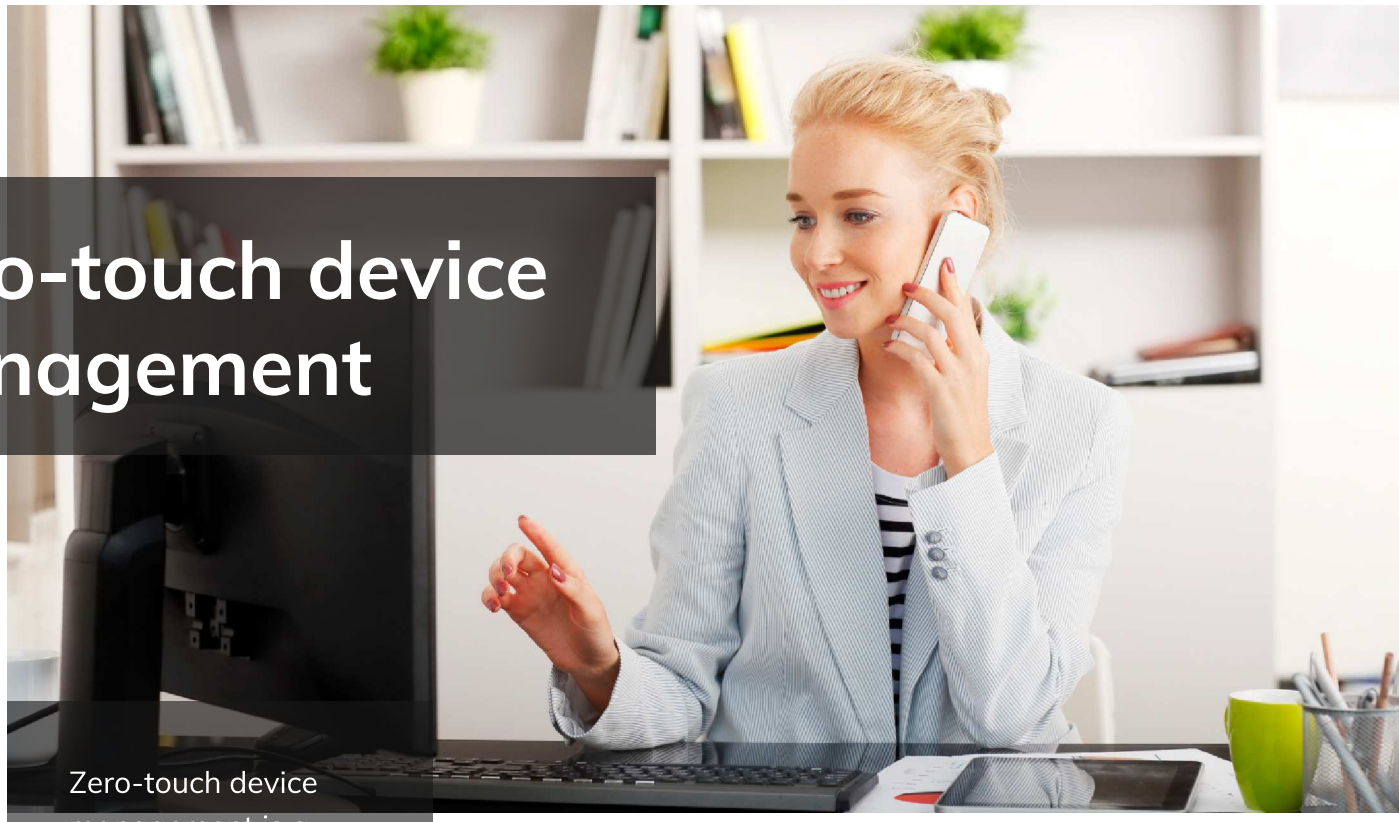
Device security management is the term used to describe the safeguards used to guard sensitive data transmitted and stored on computers, smartphones, tablets, wearables, and other portable devices. The primary objective of mobile device security is to prevent unauthorized users from entering the corporate network.

Given that more than half of business PCs are now portable, network security must consider all the locations and usage employees require of the corporate network. Malicious mobile apps, phishing scams, data leaks, malware, and insecure Wi-Fi networks are a few potential smartphone hazards. Additionally, businesses must plan to risk a mobile device being stolen or lost by an employee. Therefore, companies should take specific preemptive measures to lessen the risk of averting a security breach.

Investment in UEM solutions and a multi-layered strategy are necessary for mobile device security. Each firm must choose which ones work best for their network.

4

Zero-touch device management



Zero-touch device management is a fleet management solution that stormed the IT market during the recent pandemic. Zero-touch is a subdivision of remote device management meant to manage devices remotely. An efficient device management solution that requires no intervention from the user's end is what zero-touch offers.

WHAT IS ZERO-TOUCH ENROLLMENT AND PROVISIONING?

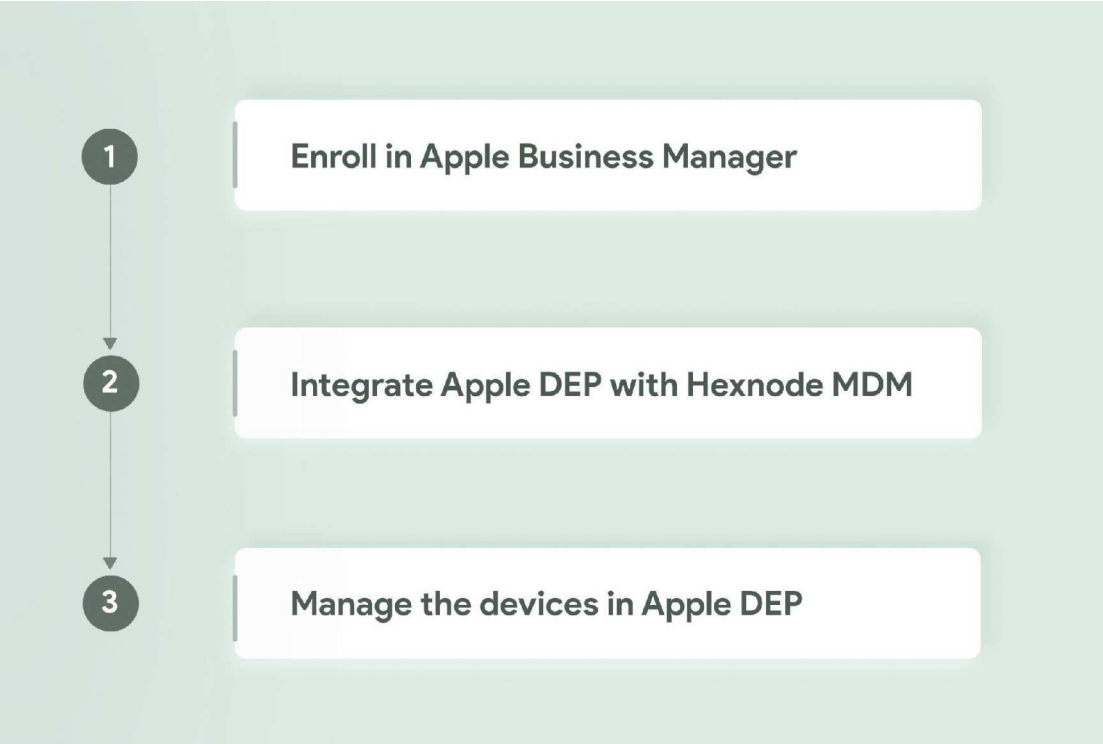
Zero touch enrollment and provisioning or zero touch deployment refer to the process where the essential configurations, settings, and apps are automatically made available on the devices without the need for IT involvement, making it usable for employees as soon as they unbox it.

Different platforms offer different zero touch deployment methods for their devices. For example, Apple has its own deployment method called Automated Device Enrollment, Android has Zero Touch Enrollment and Android ROM enrollment, Samsung devices have Samsung Knox Mobile Enrollment, and Microsoft has Autopilot to enroll Windows devices. Hexnode UEM supports all of these zero touch enrollment methods, and let's see them one by one.

Apple's Automated Device Enrollment

Apple's Automated device enrolment, earlier known as Device Enrollment Program (DEP), simplifies the deployment of Apple devices purchased in bulk from Apple or an authorized reseller by automatically installing the basic settings and configurations on the devices from the start. ABM/ASM streamlines Apple device administration in the workplace by combining DEP and VPP (Volume Purchase Program) into one site. The corporate-owned device registration starts when the user picks the necessary language and connects to the network.

The first step in enrolling your Apple devices via DEP is to ensure that the APNs or Apple Push Notification service certificate is configured in the MDM server. APNs is the messenger between the MDM and the Apple device. Enrolling Apple devices using ADE helps IT admins unlock a lot of additional features, like enabling supervision on devices as soon as it is enrolled. Supervision of Apple devices gives you more control over the devices and also lets you configure additional restrictions.



Supported devices:

- iOS 7.0.4 and above
- OX S 10.9 and above
- tvOS 10.2 and above
- iPad OS 13.1 and above

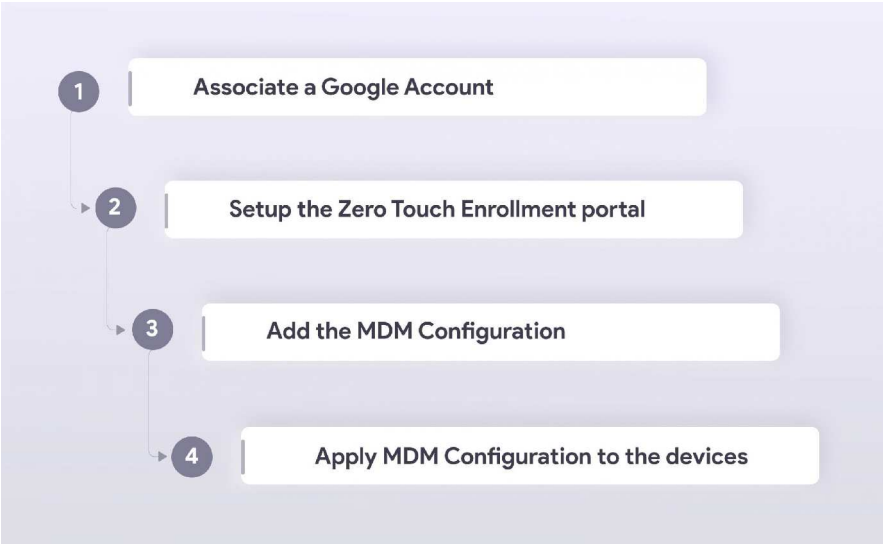
Android Device Enrollment

Android devices have multiple zero touch deployment options, like Android Zero Touch Enrollment (ZTE) for non-Samsung devices, Samsung Knox Mobile Enrollment for Samsung Knox devices and Android ROM Enrollment for all Android devices.

Zero-Touch Enrollment (ZTE)

Zero Touch Enrollment (ZTE) makes it easier to enroll corporate-owned Android devices in bulk. In terms of security, this zero-touch Android device deployment approach may be pretty intense because it lowers the dangers accidentally produced by users who may set up the wrong settings. To enroll your Android devices in your MDM using ZTE, you must first make sure that the devices are purchased from either a zero-touch reseller partner or a Google partner. You must also have a Google account associated with your corporate email to enroll your device using ZTE. Once the Google account is set, you can set up a zero-touch portal using that account and, in the portal, you can add the MDM configuration file in the Configuration tab. You can get the configuration file for the MDM provider. Once all these are set up, you can push the configuration to the devices through the zero-touch portal.

Once enrolled with ZTE, organizations have total control and efficient management of corporate-owned devices. Once the devices have been registered via zero-touch, administrators may mandate the automated installation of apps, and corporate users can immediately begin utilizing devices that have already been configured with the relevant rules and configurations by the organization's MDM supplier.



Supported devices:

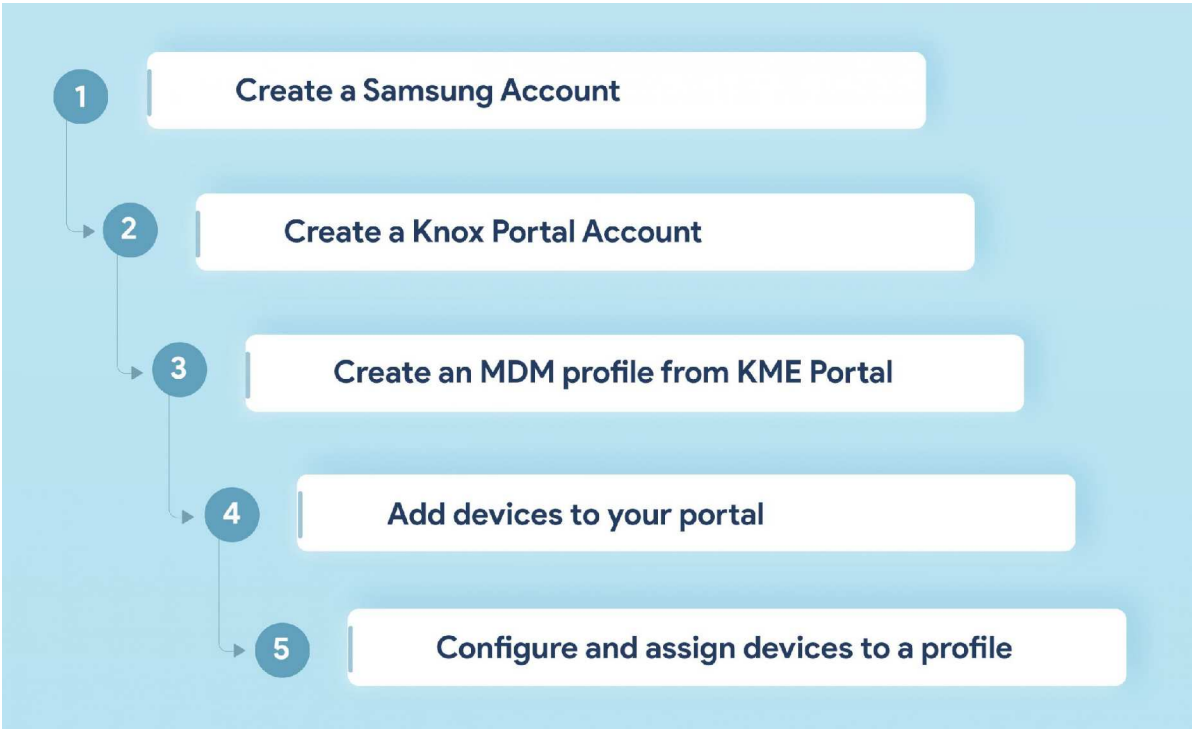
- Compatible device running Android 8.0 and above
- Pixel phone with Android 7.0

Samsung Knox Mobile Enrollment (KME)

Zero Touch Enrollment (ZTE) makes it easier to enroll corporate-owned Android devices in bulk. In terms of security, this zero-touch Android device deployment approach may be pretty intense because it lowers the dangers accidentally produced by users who may set up the wrong settings.

To enroll your Android devices in your MDM using ZTE, you must first make sure that the devices are purchased from either a zero-touch reseller partner or a Google partner. You must also have a Google account associated with your corporate email to enroll your device using ZTE. Once the Google account is set, you can set up a zero-touch portal using that account and, in the portal, you can add the MDM configuration file in the Configuration tab. You can get the configuration file for the MDM provider. Once all these are set up, you can push the configuration to the devices through the zero-touch portal.

Once enrolled with ZTE, organizations have total control and efficient management of corporate-owned devices. Once the devices have been registered via zero-touch, administrators may mandate the automated installation of apps, and corporate users can immediately begin utilizing devices that have already been configured with the relevant rules and configurations by the organization's MDM supplier.



Supported devices:

- Samsung Knox devices running on Knox version 2.4 or higher

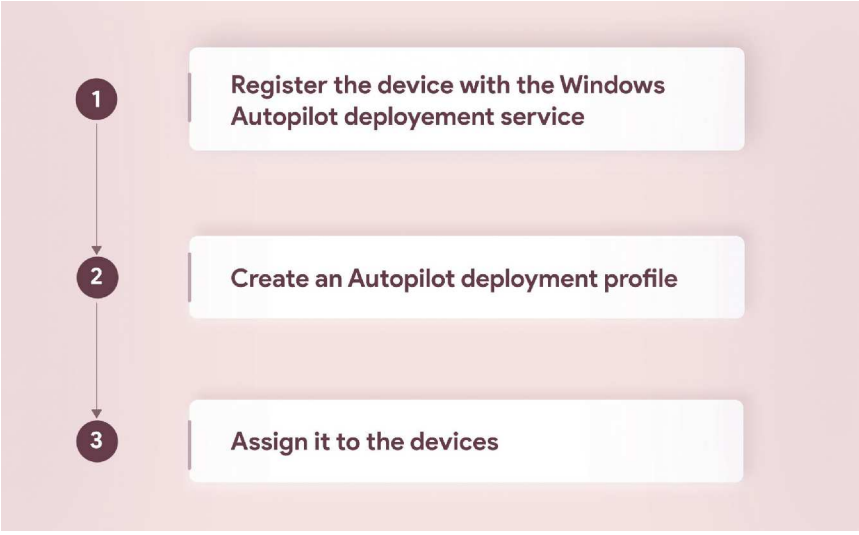
Android ROM Enrollment

This enrollment is usually preferred by organizations that have partnerships or collaborations with OEM vendors. Here what the OEM vendor does is the ROM is flashed with a custom ROM during the manufacturing process. The custom ROM is designed in such a way that the UEM/MDM app is added as a system app with all the permissions and privileges granted to the app. When adding the MDM app, make sure that the app's APK file is added to the system/priv-app folder so that the MDM app will be silently installed and make it non-removable. Once the ROM is flashed, no further change can be made on the UEM/MDM app unless the OEM vendor re-signs the ROM.

Windows Autopilot

Windows Autopilot is a cloud service provided by Microsoft that makes zero touch deployment of Windows devices possible. Before Autopilot, admins had to manually design custom images and set up an infrastructure to manage the images to deploy Windows devices. The main drawbacks to this were, a lot of manual work was required here, also a new image had to be deployed whenever Microsoft released a new update.

With Windows Autopilot, devices can be set up and deployed easily without the IT admin having to touch the device. For this, the device must be first registered with the Windows Autopilot deployment service and then create a deployment profile with all the necessary configurations. Once the profile is set up, you can assign it to the devices. The device will enroll and be set up in accordance with your settings as soon as it is powered on and connected to the network after the profile has been assigned.



Supported devices:

- Windows 10 version 1703 and above
- Supported editions: Pro, Pro Education, Pro for Workstations, Enterprise, Education

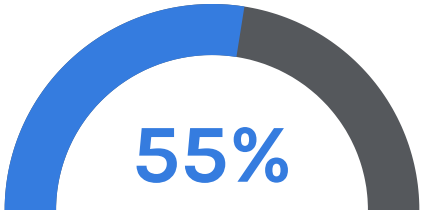
WHAT IS ZERO-TOUCH AUTOMATION?

Zero-touch automation (ZTA) coordinates automated operations using a SaaS management platform to eliminate all manual IT touchpoints. As a result, it makes it possible to avoid human mistakes as a potential system disruptor.

The ZTA actions can be simple, like restarting a server, or complex, like disaster recovery. Using ZTA, a company may boost productivity, lower costs, predictability, and agility, leading to greater service health and availability and improving customer satisfaction.

How can the IT environment be protected with zero-touch automation?

Zero-touch automation can be helpful for a wide range of tasks depending on the procedures that consume the most time and resources for the IT department. This task category may also include onboarding and offboarding. Businesses that embrace an automation-first attitude may save significant time and resources, allowing their IT teams to focus on higher-value tasks rather than repetitive responsibilities.



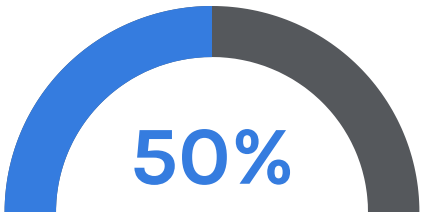
of programs support zero-touch automation

A case study by Infosys revealed that Zero-touch automation and continuous testing framework help US bank soft save $14+ million.

60%–80%

Decrease in regression cycle time using ZTA

Manual methods are sometimes expensive, dangerous, and demanding. Many repetitive duties can quickly become tedious or annoying and don't always make the best use of an employee's abilities. On the other hand, zero-touch will facilitate procedures, protect employees, and enhance the quality of products. Aiming for zero-touch automation is a feasible endeavor that has the potential to save a lot of money, maximize the use of IT resources, and benefit the entire business.



reduction in the number of employees needed for testing

Source: Infosys

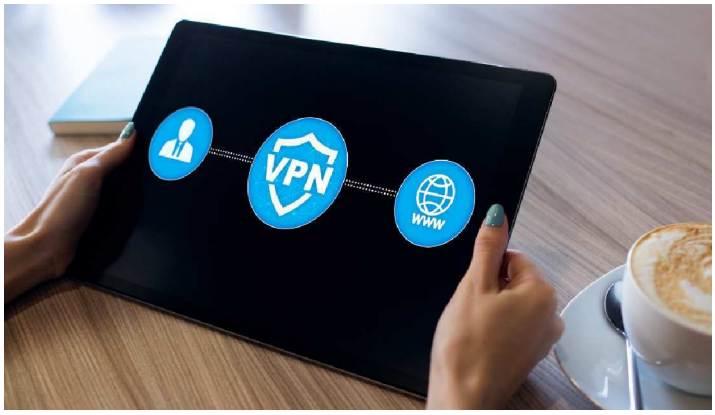
It is simpler to accomplish your company's objectives when your infrastructure is well-managed and under your control through ZTA. Additionally, there are intangible advantages, such as understanding who genuinely utilizes the infrastructure and allowing operators to concentrate their efforts more on creative solutions.

Dynamic grouping and geofencing features are also available with zero-touch automation. Dynamic groups automatically change the member devices based on some predefined criteria. During the periodic group sync, devices that use dynamic grouping enter and exit the group. It is preferable to manual grouping since it can be accomplished with only a small amount of manual work.

A virtual fence may be built around a specific geographic area using the location-based service known as geofencing. By setting up geofences, administrators may dynamically link policies or unlink them from devices inside or outside a given area. This capability may be combined with dynamic grouping and applied to various use cases, such as making corporate resources and device settings available based on device location or developing a compliance-based warning system for devices found to be beyond the geofence.

WHAT IS A ZERO-TOUCH NETWORK?

Zero-touch networks (ZTN) are autonomous systems that can repair and modify themselves depending on signals in the data gathered and examined from all network activities. The foundation of zero-touch networks is cutting-edge machine learning technology, which detects abnormalities and offers autonomous repair through strong correlations and root cause analysis.



Although zero-touch technologies are still in their infancy, there is a rising expectation that network monitoring and alerting systems can perform the remediation process without involving a human. The remediation process is a mechanism that corrects or eliminates problems that have been identified.

It includes:

- finding vulnerabilities through scanning and testing,
- prioritizing,
- fixing and
- monitoring vulnerabilities.

Cloud infrastructure, Software-Defined Networking (SDN), Network Function Virtualization (NFV), machine learning, and 5G developments can be used to develop the zero-touch network. This connects to the 5G revolution in networking, which is now being developed and will deliver more bandwidth, capacity, and growth for subsequent improvements. Machine learning can also further increase the intelligence of ZTN by extracting information from the repository of data created by a network and making decisions based on data. Moreover, network management solutions are automatically secured through zero-touch networks.

ZTN will have quick turnaround times and returns on investment, making it simple to meet various and novel company advancements, corporate groups, customers, and industry segments. In addition, ZT networks are greatly facilitated by automation. This is because automation allows us to set up various components automatically and modify the status of a service that is already deployed without manually entering instructions or restarting a server.

Zero-Touch Operations (ZTO)

The concept of Zero-touch operations (ZTO) was brought to the networks. It is emerging as a crucial enabler for safeguarding the future of dependable and successful network operations in a world where the requirement to handle escalating data demands effectively is higher than ever.

The best strategy to guarantee error-free business procedures that may increase income while offering excellent service is to use zero-touch operations. It is the appropriate strategy for managing IT operations and reducing risk.

From an operator executive's perspective, the ZTO will be implemented in the following five areas in the companies:

- Network deployment and upgrades: includes automatic software updates, site assessments, zero-touch integration, etc.
- Network optimization: includes performance accelerators, power-saving measures, virtual drive evaluations, etc.
- Network healing: includes cell outage compensation, incident management and recovery, and zero-touch assurance.
- Network evolution: includes planning for capacity, handling security incidents, intent-based automation, and other concepts.
- Self-service and on-demand services: Business websites and mobile applications let users alter their services.

Almost all businesses are employing cloud enablement services and embracing cloud infrastructure. Some businesses, however, employ infrastructure that is not cloud-native. ZTO is also feasible for these networks, especially when a hybrid environment is built.

5

Zero-touch and UEM

The approach of centrally managing endpoint devices from a single place is known as Unified Endpoint Management (UEM). Examples of endpoints are mobile, desktop PCs, laptops, tablets, wearables, and other intelligent devices that access networks or resources within an enterprise

HOW ZERO-TOUCH WORKS USING A UEM?

UEM solutions, viewed as the next generation of mobility software, combine numerous existing Enterprise Mobility Management (EMM) technologies, such as mobile device management (MDM) and Mobile Application Management (MAM), with some of the tools used to protect desktop PCs and laptops.

In addition, UEM combines the different aspects of EMM suites with Client Management Tools (CMT) features, which monitor desktop PCs and laptops on a corporate network. Routine activities, such as device scans and health checks, place a significant burden on the IT staff and are vulnerable to human mistakes. These sorts of everyday chores should be automatable by zero-touch management systems. Automating these procedures helps to minimize these human errors.

How UEM helps in managing devices

Hexnode UEM is a cloud-based management system that offers more secure, adaptable, and comprehensive management services than any other vendor on the market. Hexnode UEM uses a top-tier EMM solution to protect, track, and manage corporate and personal devices. In addition, you may set up platform-independent policies, install apps and content, and configure your devices to operate in purpose-specific kiosk modes. It provides full mobility management software compatible with all major platforms, including Android, Windows, iOS, macOS, Fire OS, and Apple TVs.

UEM systems also encourage strict and consistent security rules across the enterprise. It has various application and device management features that enable consistent application and content access throughout all endpoints and boost workplace productivity. All of the devices handled by the company could be handled from a single place, regardless of platform.

Zero-touch features of Hexnode

Hexnode UEM supports multiple zero-touch features, which begins with the various device enrollment method. Apple, Google, Samsung, and Windows all have zero-touch deployment systems, and Hexnode assists in making the most effective use of enrollments for all but Windows.

Hexnode allows IT administrators to automate policies and configurations and enforce limitations on managed devices to help govern end-user access. Administrators may define various rules and conditions for regulating devices and verifying compliance.
Hexnode UEM interacts with many directory services, allowing administrators to export users and user groups from these services to the UEM interface. It also gives settings and control privileges to managed apps installed in bulk on end-user devices.
Configuring dynamic groups and implementing rules and conditions that, when fulfilled, trigger pre-defined actions such as policy allocation, auto lockout, and more are also part of the zero-touch deployment.

Hexnode could also assist IT teams in automating a wide range of functions, such as locking down or turning off devices when they're not being used, clearing a device's internet history, automatically adjusting device settings based on the device's location, and much more, with the help of features such as custom script execution and geofencing. Geofencing is a Hexnode feature that allows you to automatically associate rules with devices based on whether they are within or outside of a given location.

Conclusion

Zero-touch management has made it easy to enroll devices in mass. The gadgets are safeguarded against numerous threats and breaches. Finding a replacement device is never an issue if the equipment stops operating. If you pick a device management application that does not adapt to your company's particular demands, device management might be a headache. So, while selecting a Zero-touch management solution for your purposes, be sure it meets all of your requirements.

With Hexnode UEM, you can use a single policy to specify configurations and limits for your iOS, Android, Windows, Mac, and Apple TV devices. When looking to develop your organization, the number of endpoints to manage will depend on various factors, including the number of user accounts, personnel, and devices. The fundamental notion of device management is to give solutions for simply managing devices.

However, looking ahead in time, one can state with absolute certainty that the number of devices requiring administration will rise. Therefore, integrating zero-touch with the never-ending work of device management is quickly becoming less of an option and more of a must. A zero-touch device management solution with a UEM for your devices would make life easier for the entire organization. Implementing a zero-touch solution is a critical decision that might help your firm expand more quickly.

Mitsogo Inc., United States (HQ), 111 Pine St #1225,
San Francisco, CA 94111
Tel: Intl +1-415-636-7555, Fax: Intl +1-415-646-4151