I'm not a robot

Please turn on JavaScript in your browser and refresh the page to view its content. Mobile device management (MDM) lets you securely and wirelessly configure devices by sending profiles and commands to the device, whether they’re owned by the user or your organization. MDM capabilities include updating software and device settings, monitoring compliance with organizational policies, and remotely wiping or locking devices. Users can enroll their own devices in MDM, and organization-owned devices can be enrolled in MDM automatically using Apple School Manager or Apple Business Manager.There are a few concepts to understand if you’re going to use MDM, so read the following sections to understand how MDM uses enrollment and configuration profiles, supervision, and payloads.Enrollment in MDM involves enrolling client certificate identities using protocols such as Automated Certificate Management Environment (ACME), or Simple Certificate Enrollment Protocol (SCEP). Devices use these protocols to create unique identity certificates for authenticating an organization’s services.Unless enrollment is automated, users decide whether to enroll in MDM, and they can disassociate their devices from MDM at any time. Therefore, you want to consider incentives for users to remain managed. For example, you can require MDM enrollment for Wi-Fi network access by using MDM to automatically provide the wireless credentials. When a user leaves MDM, their device attempts to notify the MDM solution that it can no longer be managed.For devices your organization owns, you can use Apple School Manager or Apple Business Manager to automatically enroll them in MDM and supervise them wirelessly during initial setup; this enrollment process is known as Automated Device Enrollment.An enrollment profile is one of two main ways users can enroll a device into an MDM solution (the other way is to use User Enrollment or account-driven Device Enrollment). With this profile, which contains an MDM payload, the MDM solution sends commands and—if necessary—additional configuration profiles to the device. It can also query the device for information, such as its Activation Lock status, battery level, and name.When a user removes an enrollment profile, all configuration profiles, their settings, and Managed Apps based on that enrollment profile are removed with it. There can be only one enrollment profile on a device at a time.After the enrollment profile is approved, either by the device or the user, configuration profiles containing payloads are delivered to the device. You can then wirelessly distribute, manage, and configure apps and books purchased through Apple School Manager or Apple Business Manager. Users can install apps, or apps can be installed automatically, depending on the type of app it is, how it’s assigned, and whether the device is supervised. For more information, see About Apple device supervision.How you remove profiles depends on how they were installed. The following sequence indicates how a profile can be removed:1. All profiles can be removed by wiping the device of all data.2. If the device was enrolled in MDM using Apple School Manager or Apple Business Manager, the administrator can choose whether the enrollment profile can be removed by the user or whether it can be removed only by the MDM server itself.3. If the profile is installed by an MDM solution, it can be removed by that specific MDM solution or by the user unenrolling from MDM by removing the enrollment configuration profile.4. If the profile is installed on a supervised device using Apple Configurator, that supervising instance of Apple Configurator can remove the profile.5. If the profile is installed on a supervised device manually or using Apple Configurator and the profile has a removal password payload, the user must enter the removal password to remove the profile.6. All other profiles can be removed by the user.An account installed by a configuration profile can be removed by removing the profile. A Microsoft Exchange ActiveSync account, including one installed using a configuration profile, can be removed by Microsoft Exchange Server by issuing the account-only remote wipe command.Important: If users know the device passcode, they can remove manually installed configuration profiles from iPhone and iPad that aren’t supervised, even if the option is set to “never.” Users on Mac can do the same thing only if the user knows an administrator’s user name and password. They can do this using the profiles command-line tool, System Settings (in macOS 13 or later), or System Preferences (in macOS 12.0.1 or earlier). For a Mac with macOS 10.15 or later, as with iOS and iPadOS, profiles installed with MDM must be removed with MDM, or they’re removed automatically upon unenrollment from MDM.Published Date: March 7, 2024 Mobile device management (MDM) lets you securely and wirelessly configure devices by sending profiles and commands to the device, whether they’re owned by the user or your organization. MDM capabilities include updating software and device settings, monitoring compliance with organizational policies, and remotely wiping or locking devices. Users can enroll their own devices in MDM, and organization-owned devices can be enrolled in MDM automatically using Apple School Manager or Apple Business Manager.There are a few concepts to understand if you’re going to use MDM, so read the following sections to understand how MDM uses enrollment and configuration profiles, supervision, and payloads.Enrollment in MDM involves enrolling client certificate identities using protocols such as Automated Certificate Management Environment (ACME), or Simple Certificate Enrollment Protocol (SCEP). Devices use these protocols to create unique identity certificates for authenticating an organization’s services.Unless enrollment is automated, users decide whether to enroll in MDM, and they can disassociate their devices from MDM at any time. Therefore, you want to consider incentives for users to remain managed. For example, you can require MDM enrollment for Wi-Fi network access by using MDM to automatically provide the wireless credentials. When a user leaves MDM, their device attempts to notify the MDM solution that it can no longer be managed.For devices your organization owns, you can use Apple School Manager or Apple Business Manager to automatically enroll them in MDM and supervise them wirelessly during initial setup; this enrollment process is known as Automated Device Enrollment.An enrollment profile is one of two main ways users can enroll a device into an MDM solution (the other way is to use User Enrollment or account-driven Device Enrollment). With this profile, which contains an MDM payload, the MDM solution sends commands and—if necessary—additional configuration profiles to the device. It can also query the device for information, such as its Activation Lock status, battery level, and name.When a user removes an enrollment profile, all configuration profiles, their settings, and Managed Apps based on that enrollment profile are removed with it. There can be only one enrollment profile on a device at a time.After the enrollment profile is approved, either by the device or the user, configuration profiles containing payloads are delivered to the device. You can then wirelessly distribute, manage, and configure apps and books purchased through Apple School Manager or Apple Business Manager. Users can install apps, or apps can be installed automatically, depending on the type of app it is, how it’s assigned, and whether the device is supervised. For more information, see About Apple device supervision.How you remove profiles depends on how they were installed. The following sequence indicates how a profile can be removed:1. All profiles can be removed by wiping the device of all data.2. If the device was enrolled in MDM using Apple School Manager or Apple Business Manager, the administrator can choose whether the enrollment profile can be removed by the user or whether it can be removed only by the MDM server itself.3. If the profile is installed by an MDM solution, it can be removed by that specific MDM solution or by the user unenrolling from MDM by removing the enrollment configuration profile.4. If the profile is installed on a supervised device using Apple Configurator, that supervising instance of Apple Configurator can remove the profile.5. If the profile is installed on a supervised device manually or using Apple Configurator and the profile has a removal password payload, the user must enter the removal password to remove the profile.6. All other profiles can be removed by the user.An account installed by a configuration profile can be removed by removing the profile. A Microsoft Exchange ActiveSync account, including one installed using a configuration profile, can be removed by Microsoft Exchange Server by issuing the account-only remote wipe command.Important: If users know the device passcode, they can remove manually installed configuration profiles from iPhone and iPad that aren’t supervised, even if the option is set to “never.” Users on Mac can do the same thing only if the user knows an administrator’s user name and password. They can do this using the profiles command-line tool, System Settings (in macOS 13 or later), or System Preferences (in macOS 12.0.1 or earlier). For a Mac with macOS 10.15 or later, as with iOS and iPadOS, profiles installed with MDM must be removed with MDM, or they’re removed automatically upon unenrollment from MDM.Published Date: March 7, 2024 When installing and configuring your MDM solution, consider how you’ll configure the network, Transport Layer Security (TLS), infrastructure services, Apple services, and backup.When you install a locally hosted MDM solution, you need to configure all of the following items. Configure and test each one early in the process to ensure a smooth deployment. If your MDM solution is externally managed or hosted in the cloud, your MDM vendor may handle many of these items on your behalf:DNS: An MDM solution must use a fully qualified domain name that can be resolved from both inside and outside the organization’s network. This lets the server manage devices whether they’re connected locally or remotely. In order to maintain connectivity with clients, this domain name can’t change.IP address: Most MDM solutions require a static IP address. The existing DNS name must persist if the server’s IP address is changed.Configure MDM with TLS: All communications between Apple devices and the MDM solution are encrypted with HTTPS. A TLS (formerly SSL) certificate is required to secure these communications. Don’t deploy devices without a certificate from a well-known certificate authority (CA). Note the expiration date and make sure to renew the certificate before it expires.Firewall ports: To enable both internal and external access to the MDM solution, certain firewall ports must be open. Most MDM solutions accept inbound connections using HTTPS on port 443. Both the MDM solution and the devices must communicate with the Apple Push Notification service. Prior to November, 2020, MDM solutions used ports 2195 and 2196 with APNs; clients use port 5223. After November 2020, MDM solutions use port 2197.Tip: Your MDM solution may host Activation Lock escrow keys and bypass codes, macOS bootstrap tokens, and other unique pieces of data important to continuity of device access. For this reason, make sure you have a robust disaster recovery strategy for your on-premises MDM installation. It’s recommended that backups and restores be tested regularly. Mobile Device Management (MDM) for Apple devices simplifies the task of managing and securing iOS, iPadOS, macOS, and tvOS devices in organizations. MDM allows IT administrators to wirelessly configure settings, deploy apps, and enforce security policies across multiple Apple devices. Apple’s MDM framework provides powerful tools for device enrollment, configuration profile installation, and remote management. Learn how to use MDM to set up email accounts, Wi-Fi networks, and VPN connections on company devices. You can also use MDM to push apps, restrict certain device features, and locate lost or stolen devices. Recent updates to Apple’s MDM capabilities include declarative device management. This new approach offloads some management tasks to the devices themselves, reducing server load and improving responsiveness. When choosing an MDM solution, consider factors like ease of use, scalability, and integration with your existing systems. MDM FeatureBenefitsRemote configurationEasily set up devices without physical accessApp deploymentPush required apps to all managed devicesSecurity enforcementApply passcode policies and encryption settingsAsset trackingLocate and manage your organization’s Apple devices Mobile Device Management (MDM) has become essential for organizations of all sizes that utilize Apple devices. With iPhones, iPads, and Macs increasingly prevalent in the workplace, MDM solutions provide the tools necessary to secure, manage, and support these devices efficiently. This article explores the key aspects of MDM for Apple devices, covering its benefits, features, and considerations for implementation. Apple MDM refers to the use of third-party software or built-in Apple tools to manage and control Apple devices. It allows IT administrators to configure device settings, deploy applications, enforce security policies, and remotely troubleshoot issues. This centralized management simplifies the administration of large deployments of Apple devices, ensuring consistency and security across the organization. Implementing an MDM solution for Apple devices offers numerous advantages: Enhanced Security: MDM allows for the enforcement of passcodes, encryption, and other security policies to protect sensitive data. It also enables remote wiping of lost or stolen devices, preventing unauthorized access. Streamlined Device Deployment: MDM simplifies the setup process for new devices, allowing for automated configuration and application installation. This reduces the time and effort required by IT staff and end-users. Improved Productivity: By providing easy access to necessary resources and applications, MDM can enhance employee productivity. It also allows for the distribution of company-approved apps and content. Reduced IT Costs: MDM automates many administrative tasks, freeing up IT staff to focus on other priorities. It also reduces the need for manual device configuration and troubleshooting. Centralized Management: MDM provides a single console for managing all Apple devices within the organization. This simplifies device tracking, policy enforcement, and software updates. BYOD Support: MDM can be used to manage employee-owned devices (BYOD) while respecting user privacy. It allows for the separation of work and personal data, ensuring that corporate information is secure. Effective Apple MDM solutions typically offer the following features: Device Enrollment: Streamlined enrollment of devices, including automated enrollment for corporate-owned devices. Configuration Profiles: Ability to create and deploy configuration profiles to enforce settings like Wi-Fi, VPN, and email accounts. Application Management: Distribution and management of apps, including both in-house developed apps and apps from the App Store. Security Policies: Enforcement of security policies, such as passcode requirements, encryption, and remote wipe. Remote Control: Ability to remotely troubleshoot device issues, including screen sharing and remote support. Inventory Management: Tracking of device inventory, including hardware and software information. Reporting and Analytics: Generation of reports on device usage, compliance, and other metrics. Selecting the right MDM solution depends on the specific needs of your organization. Consider the following factors: Scalability: Choose a solution that can scale to accommodate your current and future device deployments. Features: Evaluate the features offered by different solutions and choose one that meets your requirements. Ease of Use: Select a solution that is easy for IT staff to use and manage. Integration: Ensure the MDM solution integrates with your existing IT infrastructure. Pricing: Compare the pricing of different solutions and choose one that fits your budget. Support: Look for a vendor that offers excellent customer support. Apple offers two programs that work in conjunction with MDM solutions: Apple Business Manager (ABM) and Apple School Manager (ASM). These programs provide additional features for managing Apple devices in organizations and educational institutions, including automated device enrollment and volume purchasing of apps. When implementing an MDM solution, it’s crucial to address user privacy concerns. Be transparent with employees about what data is being collected and how it is being used. Ensure that the MDM solution respects user privacy and complies with relevant regulations. Plan carefully: Before implementing an MDM solution, carefully plan your deployment strategy. Communicate clearly: Communicate with employees about the benefits of MDM and address any concerns they may have. Test thoroughly: Test the MDM solution in a pilot environment before deploying it to all devices. Provide training: Provide training to IT staff and end-users on how to use the MDM solution. Stay up-to-date: Keep your MDM solution up-to-date with the latest security patches and features. The field of Apple MDM is constantly evolving. New features and capabilities are being developed all the time. Staying informed about the latest trends and advancements will help you make the most of your MDM solution. While MDM focuses on managing the entire device, Mobile Application Management (MAM) focuses specifically on managing applications. MAM allows IT administrators to control which apps are installed on devices, configure app settings, and secure app data. MAM can be used in conjunction with MDM to provide a more granular level of control over mobile devices. This is particularly useful in BYOD environments where organizations may not want to manage the entire device, but still need to secure corporate data within specific applications. MAM solutions often provide features like app wrapping, which allows for the addition of security policies to existing apps without requiring code changes. This can be a valuable tool for protecting sensitive data in third-party applications. MAM offers a more targeted approach to mobile management, allowing organizations to balance security and user privacy. Apple offers powerful mobile device management (MDM) tools for organizations to control and secure their devices. These solutions provide robust features for device configuration, app deployment, and security enforcement across Apple’s ecosystem. MDM for Apple devices allows secure wireless configuration of iOS, iPadOS, macOS, and tvOS. It uses configuration profiles to manage settings and restrictions. MDM solutions can distribute apps, configure Wi-Fi and VPN settings, and enforce passcode policies. Key capabilities include: Remote device lock and wipe App and content management Inventory and reporting Security policy enforcement MDM works through a client-server model. The MDM server sends commands and configuration profiles to managed devices. Devices then report status information back to the server. Apple’s MDM framework offers unique capabilities tailored to its operating systems. You can leverage education-centric or business-focused functionality depending on your needs. Some Apple-specific MDM features include: Automated Device Enrollment Managed Apple IDs Classroom app for iPad Lost Mode for iOS devices Activation Lock management Apple School Manager and Apple Business Manager integrate with MDM to streamline device deployment and app distribution. These services allow you to purchase and assign apps in bulk. Device enrollment connects Apple devices to your MDM solution. You have several enrollment options: User Enrollment: For BYOD scenarios Device Enrollment: For organization-owned devices Automated Device Enrollment: Zero-touch setup Automated Device Enrollment is the most seamless method. It automatically configures devices during setup without IT interaction. This process uses your MDM server and Apple Business Manager or Apple School Manager. Enrollment TypeBest For Key BenefitsUserBYODPrivacy, limited managementDeviceShared devicesFull control, supervisionAutomatedNew deploymentsZero-touch, always managed After enrollment, your MDM pushes initial settings and apps to devices. You can then manage them throughout their lifecycle. Apple’s mobile device management (MDM) offers robust security features and compliance tools. These help protect sensitive data and ensure devices meet organizational standards. MDM solutions can query Apple devices for compliance data. This includes device details, network info, and app usage. You can set how often the MDM gathers this data. Compliance checks ensure devices follow your policies. MDM can monitor: Software versions Installed apps Device settings Encryption status If a device falls out of compliance, MDM can take action. This may include sending alerts or restricting access to company resources. Apple MDM includes several features to safeguard your data: MDM can enforce passcode policies and enable remote wipe capabilities. This protects data if a device is lost or stolen. For BYOD scenarios, User Enrollment keeps work and personal data separate. It uses cryptographic separation to protect company information. FeatureBenefitFileVaultEncrypts Mac hard drivesHTTPSSecures MDM communicationUser EnrollmentSeparates work/personal data These tools help you maintain a strong security posture while managing Apple devices in your organization. Mobile device management for Apple devices offers powerful tools for configuration and oversight. It enables organizations to efficiently manage devices at scale while maintaining security. MDM systems allow administrators to send commands and profiles wirelessly to Apple devices. This includes actions like: • Configuring settings• Installing apps• Locking or wiping devices• Querying device information Administrators can view reports on device status, compliance, and usage. This helps track inventory and ensure policy adherence. MDM solutions offer query services to gather data like: • Installed apps• Device location• OS version• Security status Many integrate with Active Directory for user account management. This simplifies provisioning and access control. MDM platforms provide options for deployment and hosting: Hosting TypeDescriptionCloudManaged by vendor, quick setupOn-premisesLocal control, higher securityHybridMix of cloud and local servers Vendor support is crucial for successful MDM implementation. Look for providers offering: • Setup assistance• Training resources• Ongoing technical support Integration with existing IT systems improves workflow efficiency. Consider how the MDM solution connects with: • Help desk software• Asset management tools• Security information systems Choose a platform that aligns with your organization’s needs and technical capabilities. Proper integration ensures smooth device management and support processes. Apple’s mobile device management (MDM) solutions offer specialized features for both educational institutions and businesses. These tools help streamline device deployment, enhance productivity, and ensure security across various environments. Apple School Manager provides education-centric functionality to simplify device management in schools. This platform allows IT administrators to create managed Apple IDs for students and staff. It integrates with Student Information Systems for easy account creation. Classroom app lets teachers guide learning, share work, and manage student devices. Teachers can launch apps, websites, or books on all devices simultaneously. They can also view student screens and lock devices to maintain focus. Schoolwork app helps teachers and students track assignments and progress. It integrates with popular educational apps to streamline workflows. Teachers can send handouts, view student progress, and provide feedback all in one place. Shared iPad enables multiple students to use the same device while keeping their data separate and secure. This feature is ideal for schools with limited budgets or shared device setups. Apple Business Manager offers device enrollment and app distribution for corporate environments. It allows IT teams to automate device setup and remotely configure settings. App Assignment lets administrators distribute and manage apps across employee devices. This ensures all team members have access to necessary tools and software. MDM solutions support various device types including iPhones, iPads, Macs, and Apple TVs. This cross-platform support simplifies management for diverse work environments. Hardware Serial Number tracking helps businesses maintain inventory and manage device lifecycles. IT can easily identify and locate devices within the organization. FeatureEducationBusinessUser ManagementManaged Apple IDsCorporate accountsApp DistributionSchoolworkApp AssignmentDevice SharingShared iPadN/AEnrollmentApple School ManagerApple Business Manager Pricing for MDM solutions varies based on features and scale. Many providers offer tiered plans to fit different organizational needs. Mobile device management (MDM) for Apple devices offers powerful tools for businesses. These FAQs address key aspects of MDM integration, benefits, and user control. Apple Business Manager seamlessly connects with MDM solutions. You can automatically enroll devices and purchase apps in bulk. This integration streamlines device setup and management for your organization. MDM for iPhones provides remote device control and app management. You gain visibility into device states and can automate OS updates. MDM ensures compliance with company policies without hands-on IT involvement. Users cannot disable MDM on corporate-owned iPhones. Only IT administrators can remove MDM profiles. This ensures consistent security and management across company devices. MDM offers wireless configuration through profiles and commands. You can update software, adjust settings, and monitor devices remotely. MDM also enables app distribution and security policy enforcement. Removing MDM from a corporate iPhone without permission is not recommended. It may violate company policies and compromise device security. Always consult your IT department before attempting to remove MDM. MDM settings are typically found in the “Profiles” section of the iPhone’s Settings app. You may see installed configuration profiles and certificates here. Contact your IT support for specific guidance on accessing MDM features. MDM FeatureBenefitRemote ConfigurationEasy device setupApp ManagementControl over softwareSecurity EnforcementEnhanced data protectionOS UpdatesConsistent system versionsInventory TrackingAsset management Mobile device management (MDM) lets you securely and wirelessly configure devices by sending profiles and commands to the device, whether they’re owned by the user or your organization. MDM capabilities include updating software and device settings, monitoring compliance with organizational policies, and remotely wiping or locking devices. Users can enroll their own devices in MDM, and organization-owned devices can be enrolled in MDM automatically using Apple School Manager or Apple Business Manager.There are a few concepts to understand if you’re going to use MDM, so read the following sections to understand how MDM uses enrollment and configuration profiles, supervision, and payloads.Enrollment in MDM involves enrolling client certificate identities using protocols such as Automated Certificate Management Environment (ACME), or Simple Certificate Enrollment Protocol (SCEP). Devices use these protocols to create unique identity certificates for authenticating an organization’s services.Unless enrollment is automated, users decide whether to enroll in MDM, and they can disassociate their devices from MDM at any time. Therefore, you want to consider incentives for users to remain managed. For example, you can require MDM enrollment for Wi-Fi network access by using MDM to automatically provide the wireless credentials. When a user leaves MDM, their device attempts to notify the MDM solution that it can no longer be managed.For devices your organization owns, you can use Apple School Manager or Apple Business Manager to automatically enroll them in MDM and supervise them wirelessly during initial setup; this enrollment process is known as Automated Device Enrollment.An enrollment profile is one of two main ways users can enroll a device into an MDM solution (the other way is to use User Enrollment or account-driven Device Enrollment). With this profile, which contains an MDM payload, the MDM solution sends commands and—if necessary—additional configuration profiles to the device. It can also query the device for information, such as its Activation Lock status, battery level, and name.When a user removes an enrollment profile, all configuration profiles, their settings, and Managed Apps based on that enrollment profile are removed with it. There can be only one enrollment profile on a device at a time.After the enrollment profile is approved, either by the device or the user, configuration profiles containing payloads are delivered to the device. You can then wirelessly distribute, manage, and configure apps and books purchased through Apple School Manager or Apple Business Manager. Users can install apps, or apps can be installed automatically, depending on the type of app it is, how it’s assigned, and whether the device is supervised. For more information, see About Apple device supervision.How you remove profiles depends on how they were installed. The following sequence indicates how a profile can be removed:1. All profiles can be removed by wiping the device of all data.2. If the device was enrolled in MDM using Apple School Manager or Apple Business Manager, the administrator can choose whether the enrollment profile can be removed by the user or whether it can be removed only by the MDM server itself.3. If the profile is installed by an MDM solution, it can be removed by that specific MDM solution or by the user unenrolling from MDM by removing the enrollment configuration profile.4. If the profile is installed on a supervised device using Apple Configurator, that supervising instance of Apple Configurator can remove the profile.5. If the profile is installed on a supervised device manually or using Apple Configurator and the profile has a removal password payload, the user must enter the removal password to remove the profile.6. All other profiles can be removed by the user.An account installed by a configuration profile can be removed by removing the profile. A Microsoft Exchange ActiveSync account, including one installed using a configuration profile, can be removed by Microsoft Exchange Server by issuing the account-only remote wipe command.Important: If users know the device passcode, they can remove manually installed configuration profiles from iPhone and iPad that aren’t supervised, even if the option is set to “never.” Users on Mac can do the same thing only if the user knows an administrator’s user name and password. They can do this using the profiles command-line tool, System Settings (in macOS 13 or later), or System Preferences (in macOS 12.0.1 or earlier). For a Mac with macOS 10.15 or later, as with iOS and iPadOS, profiles installed with MDM must be removed with MDM, or they’re removed automatically upon unenrollment from MDM.Published Date: March 7, 2024 Please turn on JavaScript in your browser and refresh the page to view its content. Mobile device management (MDM) lets you securely and wirelessly configure devices by sending profiles and commands to the device, whether they’re owned by the user or your organization. MDM capabilities include updating software and device settings, monitoring compliance with organizational policies, and remotely wiping or locking devices. Users can enroll their own devices in MDM, and organization-owned devices can be enrolled in MDM automatically using Apple School Manager or Apple Business Manager.There are a few concepts to understand if you’re going to use MDM, so read the following sections to understand how MDM uses enrollment and configuration profiles, supervision, and payloads.Enrollment in MDM involves enrolling client certificate identities using protocols such as Automated Certificate Management Environment (ACME), or Simple Certificate Enrollment Protocol (SCEP). Devices use these protocols to create unique identity certificates for authenticating an organization’s services.Unless enrollment is automated, users decide whether to enroll in MDM, and they can disassociate their devices from MDM at any time. Therefore, you want to consider incentives for users to remain managed. For example, you can require MDM enrollment for Wi-Fi network access by using MDM to automatically provide the wireless credentials. When a user leaves MDM, their device attempts to notify the MDM solution that it can no longer be managed.For devices your organization owns, you can use Apple School Manager or Apple Business Manager to automatically enroll them in MDM and supervise them wirelessly during initial setup; this enrollment process is known as Automated Device Enrollment.An enrollment profile is one of two main ways users can enroll a device into an MDM solution (the other way is to use User Enrollment or account-driven Device Enrollment). With this profile, which contains an MDM payload, the MDM solution sends commands and—if necessary—additional configuration profiles to the device. It can also query the device for information, such as its Activation Lock status, battery level, and name.When a user removes an enrollment profile, all configuration profiles, their settings, and Managed Apps based on that enrollment profile are removed with it. There can be only one enrollment profile on a device at a time.After the enrollment profile is approved, either by the device or the user, configuration profiles containing payloads are delivered to the device. You can then wirelessly distribute, manage, and configure apps and books purchased through Apple School Manager or Apple Business Manager. Users can install apps, or apps can be installed automatically, depending on the type of app it is, how it’s assigned, and whether the device is supervised. For more information, see About Apple device supervision.How you remove profiles depends on how they were installed. The following sequence indicates how a profile can be removed:1. All profiles can be removed by wiping the device of all data.2. If the device was enrolled in MDM using Apple School Manager or Apple Business Manager, the administrator can choose whether the enrollment profile can be removed by the user or whether it can be removed only by the MDM server itself.3. If the profile is installed by an MDM solution, it can be removed by that specific MDM solution or by the user unenrolling from MDM by removing the enrollment configuration profile.4. If the profile is installed on a supervised device using Apple Configurator, that supervising instance of Apple Configurator can remove the profile.5. If the profile is installed on a supervised device manually or using Apple Configurator and the profile has a removal password payload, the user must enter the removal password to remove the profile.6. All other profiles can be removed by the user.An account installed by a configuration profile can be removed by removing the profile. A Microsoft Exchange ActiveSync account, including one installed using a configuration profile, can be removed by Microsoft Exchange Server by issuing the account-only remote wipe command.Important: If users know the device passcode, they can remove manually installed configuration profiles from iPhone and iPad that aren’t supervised, even if the option is set to “never.” Users on Mac can do the same thing only if the user knows an administrator’s user name and password. They can do this using the profiles command-line tool, System Settings (in macOS 13 or later), or System Preferences (in macOS 12.0.1 or earlier). For a Mac with macOS 10.15 or later, as with iOS and iPadOS, profiles installed with MDM must be removed with MDM, or they’re removed automatically upon unenrollment from MDM.Published Date: March 7, 2024