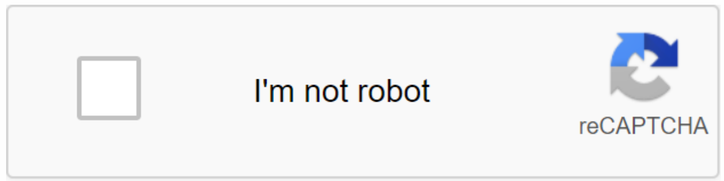

Continue

Endpoint manager mdm client apk

You can add apps directly from the Google Play Store or by uploading custom apps in a repository on all or specific managed Android devices. See the following sections for more details: Add Android apps from the App Store Add custom/enterprise Android apps Add Android apps from the Google Play Store Click App Store > Android Store Click the Add Google Play App button Type the first few letters of the app in the Name field on the form. The endpoint manager will look for compatible apps from the Store. Select the right app from the suggestion list. Then, most of the form will be automatically populated with the Google Play Application app specifications - form type parameter table and text field description type of the name enter the name of the app. Type the first few letters of the app name EM displays matching results Select the app you want to add from the offers After you've selected the app, most other form fields will be automatically populated. Text field version the version number of the application. This field will be automatically populated after you select an app in the Name field. Enter the version number manually if the version number is not fetched automatically. Application ID text field The app ID (package ID). Usually it's in reverse DNS format, for example, 'com.comodo.mobile.comodoantitheft'. In the Google Play Store, the ID is located after '=' in the URL. An example is shown below: click the Help icon next to the Show how to retrieve the package ID for play store apps. This field will be populated automatically when you enter the correct app name in the Name field. License type options button whether the app is free or paid. This option will be preselitated depending on the app selected in the Name field. Drop-down category The category will be selected automatically depending on the app selected in the Name field. The drop-down list also allows you to select the category to which the app belongs. Select the category from the drop-down list if it is not automatically populated. The category of supported devices opens in the category of devices on which to launch the app. This device type will be automatically selected based on the app selected in the Name field. Select the device type from the drop-down list if it is not automatically populated. A description of the Submitted Description text field will be automatically populated with the description of the selected app, from the Google Play Store page. The text field also allows you to edit the description or enter your own description of the app. Mandatory app check box Specify whether the app is a forced installation. If this option is enabled, the app will automatically be rejected to all registered devices. Remove from device when removed from app catalog the app catalog will be removed from devices if it is removed from the EM app The app icon button The app icon will be automatically imported from the Google Play Store for the app selected in the Name field. If you want to change the icon, upload a new icon from your local computer by clicking Browse. The Screenshots button for apps Screenshots of the app will be automatically brought from the Google Play Store for the app selected in the Name field. If you want to add new screenshots from your local computer, upload them by clicking Browse. Click Save after entering the details. The app will be added to the app store and listed in the Market. It will sync with the devices over the next cycle. Click Notify Devices Now if you want to push the app immediately. You can add custom/enterprise Android Apps apps to the store by uploading the app's .apk file. The app information will be brought in automatically by analyzing the file. You'll need to manually enter details that could not be fetched from the .apk file Prerequisite: The app's .apk file had to be saved on your PC or in the network storage accessible through the computer, from which you accessed the Endpoint Manager console. To add custom/enterprise Android apps click Store >Android Store click Add Enterprise App from the top-level options. Click Browse under Source File, navigate to the location of the .apk file for upload, select the file, and click Open. See the previous section if you need advice on the fields on this form. Click Save after entering the details. The app will be added to the store and listed in the Android Store interface. It will be synchronized with registered devices during the next update cycle. Click Update Devices Now if you want to push the app out immediately. Track US Keep employees productive and data more secure with easy-to-set endpoint management for Android, iOS, and Windows 10 devices. Contact Sales View lost phone documentation. Stolen laptop. Things happen. Keep your company's data secure with endpoint management. You can require strong screen locks and passwords, and delete confidential data by deleting a device or selectively deleting an account. Simply allow endpoint management in the Google admin console, and Gmail, Drive and other mobile apps will be better secured and managed. During this time, you can view graphs and reports about mobile use and trends at any time in the reporting section. Help your employees find the work apps they need by distributing business apps from the admin console on Google Play or the Apple App Store. Endpoint management supports and enables BYOD, making it easier to keep your company's data safe while allowing employees to use their preferred personal devices to get work done. Once your employee's device is registered, everything And e-mail configurations, including server-side credentials, are pushed to the device immediately. Agent-free basic management installation offers delete and inventory controls for all devices in your fleet, without user setting or interference. Enhance your employee experience and increase productivity with one-click access to thousands of pre-integrated apps, both in the cloud and on-site. Learn how arrow_forward protect all your user accounts with MFA authentication methods such as push notifications, unable passwords, and dial-up security keys. Learn more arrow_forward access context management endpoint management one entry endpoint (SSO) unified management management HRMS integration management hybrid identities and compatibility technical support QR code connector COMODO security solutions 新版本: 6.16. 0.12 发布日期: August 10, 2020 ITarian End载point Manager (11.37 MB) - The MDM client is the client application of the ITarian Endpoint Manager. ITarian Endpoint Manager The impressions, provisioning, configuration, and manager of the Endpoint Manager by ITarian Schedule and your money in your organization will automate your organization's sign-up, provisioning, configuration, and management options to save your organization time and money. The Endpoint Manager enables seamless remote control over devices, allowing organizations the power to enforce security restrictions to secure company-owned data regardless of which device holds it. To learn more about the endpoint manager by ITarian, see the following page: Mobile Device Management, MDM, EM, IT and Security Manager, Mobile Security, MSM, Mobile Application Management, MAMThis app uses Device Manager permission 分类: 免费版 工具应用 来: 系统要求: 4.1及更高版本+ Endpoint Manager - MDM Client 史版本 Endpoint Manager - MDM Client 6.16.0.12 for Android 4.1及更高版本 version载: 6.16.0.12 for Android 4.1及更高版本 更新日期: 2020-08-10 大载APK (11.37 MB) Endpoint Manager - MDM Client is the client's application for ITarian Endpoint Manager. ITarian Endpoint Manager The impressions, provisioning, configuration, and manager of the Endpoint Manager by ITarian Schedule and your money in your organization will automate your organization's sign-up, provisioning, configuration, and management options to save your organization time and money. The Endpoint Manager enables seamless remote control over devices, allowing organizations the power to enforce security restrictions to secure company-owned data regardless of which device holds it. To learn more about endpoint manager by ITarian, see the following page: Device Management, MDM, Endpoint Management, EM, Mobile Security Management, MSM, Mobile Application Management, MAMThis app uses device manager permission We move sections about older endpoint management releases from what's new in this article. Endpoint Management 20.9.0 the following features are now rolling out to commercial customers. U.S. government customer releases begin inside Months. For feature differences between the U.S. government's commercial offerings, see Endpoint Management Service for the U.S. Government. This release contains improvements that help improve overall performance and stability. Fixed issues managing Endpoint 20.9.0 When an Azure AD user logs into some azure AD joined Windows 10 devices that are configured to be a kiosk, and kiosk mode is not turned on. [CXM-66123] Immediately after registering a device that is running macOS 10.14+, device properties do not always populate in the Endpoint Management console. Restart the device to view the properties. What are you doing in here? Sometimes deployed resources do not affect macOS 10.14+ devices until the device is restarted. What are you doing in here? Endpoint Management 20.8.0 the following features are now rolling out to commercial customers. Editions for U.S. government customers start within three months. For feature differences between the U.S. government's commercial offerings, see Endpoint Management Service for the U.S. Government. Easier use of the certificate alias in managed Android enterprise configurations. Use the new Certificate Alias setting in the Certificate Device policy with the Android Enterprise Managed Configuration Device policy. This allows apps to authenticate on a VPN without user action. Instead of finding the certificate alias in the application logs, create the certificate alias. Create the alias by typing it in the Certificate Alias field of the configuration device policy managed by an Android organization. Then type the same certificate alias in the Certificate Alias setting in the Certificate Device policy. See Android Enterprise Managed Configurations policy and Certificate Device Policy. Password device policies allow you to view apps and shortcuts on Android devices that don't meet compatibility. The password device policy for your Android organization includes a new setting, show apps, and shortcuts when the passcode doesn't match. Allow the setting to make apps and shortcuts remain visible when your device passcode is no longer compatible. Citrix recommends that you create an automatic action to mark your device as incompatible when the passcode is incompatible. See Password Device Policy. Control Use a single lock setting on Android devices. The new Enable federated passcode setting in the Password Device policy allows you to determine whether a device requires a separate passcode for the device and work profile. Before this setting, users controlled this behavior by using the Use one lock on device setting. When Enable Federated Passcode is enabled, users can use the same passcode for the device as the work profile. If an enabled federated passcode is turned off, users cannot use the same passcode for the device as the work profile. The default is Off. The Enable unified lock setting is available for Android enterprise devices running on Android 9.0 or later. See Install Password Fixed endpoint management issues 20.8.0 if you are aboard Endpoint Management on 19.12.0 or a later version, to remove the Android Enterprise subscription, unsubscribe from your Android organization from the console. Then remove the configuration from Google Play. If you click Remove Organization in the Google Play Store first, your Android subscription will remain active in the Endpoint Management console. [CXM-83601] Endpoint Management 20.7.1 The following features are now rolling out to commercial customers. Editions for U.S. government customers start within three months. For feature differences between the U.S. government's commercial offerings, see Endpoint Management Service for the U.S. Government. Rename the profile on Citrix workspace enrollment screens. When users register their device for endpoint management, the profile name that is currently displayed in the Citrix workspace. You can customize this name and view the name of your organization instead. To customize the name, change the value for the new server property apple.mdm.enrollment.profile.organization.name. See Server Properties. Fixed issues managing endpoint 20.7.1 On some cloud sites, the Endpoint Management Console Monitor page is not loaded. [CXM-83365] When you edit the values in the optional.user.identity.attributes server property and save the changes, you receive an error message. [CXM-84209] Endpoint Management 20.7.0 The following features are now out to commercial customers. Editions for U.S. government customers start within three months. For feature differences between the U.S. government's commercial offerings, see Endpoint Management Service for the U.S. Government. Endpoint management supports authentication with an on-premises Citrix gateway as a preview feature. You can now configure an on-premises Citrix gateway as your identity provider for users who sign up through citrix Secure Hub. For more information, see Authentication with an on-premises Citrix gateway using Cloud Citrix (Preview). Customize the list of optional Active Directory user attributes. A new server property, optional.user.identity.attributes, allows you to remove and restore optional features that Endpoint Management uses to identify a user account in Active Directory. For more information, see Customize Active Directory User Attributes. Fixed issues managing endpoint 20.7.0 Apple iTunes volume purchase applications cannot be synchronized with endpoint management. [CXM-81271] When you install multiple LDAP active libraries (AD) in Endpoint Management by using the Citrix Cloud Connector, only the first installed AD is populated in endpoint management settings. As a workaround, you can test Citrix Cloud. If these domains are marked as unused, mark them manually as used. Marking the domain as used makes it available in endpoint management. [CXM-81697] If you are up for endpoint management on 19.12.0 (December 2019) or a later version: When To add multiple LDAP authentication domains, you cannot change the default domain. [CXM-82952] Endpoint Management 20.6.0 The following features are now rolling out to commercial customers. Editions for U.S. government customers start within three months. For feature differences between the U.S. government's commercial offerings, see Endpoint Management Service for the U.S. Government. If you are on an endpoint management deck after releasing 19.8.0 (August 1, 2019), log on to the Citrix cloud and click on the Endpoint Management Service tile to access the console. All customers on board before 19.8.0 will soon be connected to citrix cloud sign in. To provide enhanced security, Citrix recommends configuring a single logon. For assistance, contact Citrix Technical Support. The Secure Hub Apple Push Notification Service (APNs) certificate for endpoint management expires on July 12, 2020. As a result, the agent message fails and the application push may be delayed on iOS devices. This update restarts the Certificate of Secure Hub APIs, which expire on June 18, 2021. Turn off the ability to print on your Android organization's work profiles or on fully managed devices. In the Install Restrictions policy, the Do not allow printing setting allows you to specify whether users can print to any printer accessible from an Android device. For more information, see Android Enterprise Settings. Configure connection status and network priority for macOS. In the Wi-Fi device policy, enable the Connection Status setting for macOS devices to choose how users join the network. The device can use the system credentials or credentials entered in the logon window to authenticate the user. If you have multiple networks, type a number in the Priority field to set the priority of the network connection. The device selects the network with the lowest number. For more information, see macOS settings in the Wi-Fi device policy. Enable configured proxy on iOS devices. Endpoint management now requires enabling a new client property, ALLOW_CLIENTSIDE_PROXY, if you want to allow iOS users to use proxy servers they configure in Wi-Fi settings > Wi-Fi. For more information, see ALLOW_CLIENTSIDE_PROXY a reference to the Customer property. Fixed issues managing Endpoint 20.6.0 in the Endpoint Management console, you cannot see the package ID for mdx-wrapped iOS and Android applications. [CXM-81021] When Endpoint Management sends the queries for Active Directory group members, the Identity Service runs the queries recursively. These queries consume additional resources. Therefore, sites with many Active Directory users may experience disruption in everyday operations. [CXM-81112] In the Endpoint Management console, some apps are displayed as Pending even though they are already installed. This limitation is due to macOS and is specific to PKG files with different pkg and app [CXM-72203] Endpoint Management 20.5.0 The following features are now rolling out to commercial customers. Editions for U.S. government customers start within three months. For feature differences between the U.S. government's commercial offerings, see Endpoint Management Service for the U.S. Government. Simpler configuration of Intune managed applications when you use Endpoint Management Integration with Microsoft Endpoint Manager. When you configure Intune managed applications, you no longer set the Force app management option in the Endpoint Management console. You will now set the option on the EMS console. Supports restricting web content migration for Managed Intune applications published through Microsoft Edge by integrating endpoint management with Microsoft Endpoint Manager. Integrating endpoint management with Microsoft Endpoint Manager supports the new managed browser policy for Microsoft Edge, restrict web content migration with other applications, in the EMS console. Unlocks a local user account. If a user reaches the maximum number of subsequent invalid logon attempts, the local user account is locked out for 30 minutes. The system rejects all additional authentication attempts until the downout period is complete. To unlock the account in the Endpoint Management console, go to Manage > Users, select the user account, and click Unlock Local User. For more information, see How to unlock a local user account. To change the number of failed logon attempts and lock time, update the local.user.account.lockout.time and local.user.account.lockout.limit server properties. For more information, see Server Properties. The Citrix Content Delivery Network (CDN) now provides enterprise applications for macOS (MDM enrollment). To speed up the delivery of app downloads, CDN sends macOS apps to user devices located near endpoint management servers around the world. For more information, see Migrate enterprise apps from CDN Citrix. Fixed issues with Endpoint Management 20.5.0 administrators with RBAC permission to export sign-up orders can export all enrollment orders, regardless of restrictions. [CXM-79928] Attempts to deploy a PowerShell script to run an automatic operation on Windows devices may fail with an internal 500 server error. The issue occurs if you leave the Description field on the Action Information page blank and select a returned policy value as a trigger. To work around this issue, do not leave the Description field blank when you use a returned policy value as a trigger. [CXM-80997] When you edit an existing iOS restriction policy, an error occurs. [CXM-82180] Endpoint Management 20.4.1 support for the latest HTTP/2-based APIs. Apple's support for apple's legacy binary protocol of Apple's push notification service ends starting in November 2020. Apple recommends that you use the HTTP/2-based APIs instead. Citrix Endpoint Management now supports HTTP/2-based For more information, see the news feed , update apple's push notification service, . For help checking connectivity for APNs, see Connectivity testing. Password requirements for a local user account. When you add or edit a local user account in the Endpoint Management console, make sure that you are following the latest password requirements. For more information, see How to add a local user account. Use the app package ID number to add apps to your app notification device

policy. Click Add New and type the app package ID in the field that appears. For more information, see Install app notification policies. Device policy updates for iOS 13. The iOS 13 device policy now has the following features: Network Usage Policy: We've added additional features to the App Network Usage Policy and renamed it the Network Usage Policy. You can now also configure network usage rules based on SIM ICCIDs on iOS 13 devices. See Network Usage Device Policy Restrictions Policy: Now you can restrict temporary shared device sessions, change eSIM, find my iPhone, and more. For more information, see the iOS Settings section of the Install Restrictions policy. Fixed issues managing Endpoint 20.4.1 with Azure-based Active Directory authentication and device registration, users with Android devices fail to register. An error determines that user authentication does not have access to the device. [CXM-80404] Endpoint Management 20.4.0 web application advertising for Android enterprise in endpoint management console. You no longer have to go managed google play or google developer portal to advertise Android enterprise web applications for endpoint management. When you click Upload B Set > Link > Apps, a managed Google Play Store user interface opens to upload and save the file. The app's certification and advertising can take about 10 minutes. For more information, see Add a Web link. Device policy updates for iOS 13. Device policies for iOS 13 now include the following features: Fixed issues in endpoint management 20.4.0 data visualization charts on the analysis dashboard are not degenerated correctly when you use browser magnification. [CXM-79652] When using MAM-only enrollment, users can still access the Apple Air Sign-up Portal for MDM. [CXM-77449] The selective deletion operation fails when the device is on standby. [CXM-76051] Endpoint Management 20.3.0 The following features are now rolling out to commercial customers. Editions for U.S. government customers start within three months. For feature differences between the U.S. government's commercial offerings, see Endpoint Management Service for the U.S. Government. Enhanced enrollment profiles available for all customers This release enables all customers to have the enhanced enrollment profile features released to some customers in Endpoint Management 20.2.1. For information about this feature, see Configure multiple device and application management modes One environment. Android devices are registered in your Android organization by default starting with this release, Android Enterprise is the default sign-up option for Android devices. If your Android organization is enabled for your endpoint management deployment, all recently registered or re-registered Android devices are registered as Android enterprise devices by default. This change supports the changes Google is making to Android. Google has belittled device management device manager mode and encourages customers to manage all Android devices through the Android organization. (See Driver depreciation in the Google Android Enterprise Developer Guides.) Starting with Endpoint Management 19.11.0, Citrix has moved the actions required to move all Android devices to your Android organization. For more information about supporting endpoint management for switching to an Android organization, see blog, Android enterprise as the default for the Citrix Endpoint Management Service. If your endpoint management deployment includes devices that you must continue to manage in device management mode, create an enrollment profile for these legacy devices. To create an enrollment profile for legacy devices: In the Endpoint Management console, go to Configure different profiles > . To add an enrollment profile, click Add. On the Registration details page, type a name for the sign-up profile. Click Next or select Android under Platforms. The Enrollment Configuration page appears. Set up management to manage a legacy device (not recommended). Click Next. Select Assign (Options). The Assign Delivery Group screen appears. Select the delivery group or delivery groups that contain the administrators who are registered with dedicated devices. Then click Save. To continue managing legacy devices in driver mode, register or re-register them using this profile. You have registered driver devices that are similar to work profile devices by downloading the Secure Hub and providing an enrollment server URL. Fixed issues managing endpoint 20.3.0 attempt to sort devices by last access days or inactivity causes internal server error 500. [CXM-79414] for customers using Amazon's Web services and Citrix's new enhanced sign-up profiles: iOS devices are not registered. As another, create a default enrollment profile that includes all delivery groups. See Through Create an enrollment profile. [CXM-79019] When you deploy a password device policy to macOS devices, the policy applies to the system level instead of to the user level. As a result, users are not asked to change their passcode for hours, or even days. [CXM-75344] Endpoint Management 20.2.1 The following features are now rolling out to commercial customers. Editions for U.S. government customers start within three months. For feature differences between U.S. trade and government proposals, see Endpoint Management For the U.S. government. Configure multiple device and application management modes in one environment about this feature: Improved support for an outbound enrollment profile across two editions. Citrix sends messages about future releases. Until the enhanced sign-up profile feature is available to you, an enrollment profile limits only the number of devices a user can register. You can now configure a single endpoint management site to support multiple enrollment configurations. The role of enrollment profiles has expanded to include device and application management enrollment settings. Enrollment profiles support multiple use cases and device migration routes within a single endpoint management console. Use cases include: Mobile Device Management (MDM only) MDM + Mobile Application Management (MAM) MAM only owned by byod sign-up company (ability to opt out of MDM enrollment) Transfer of Android Device Manager registrations to Android Enterprise Enrollment (fully managed, work profile, dedicated device) registration profiles to replace the server property is now not used, xms.server.mode. This change does not affect the existing delivery groups and listed devices. The following table shows the automatic migration path and property status of the existing server to the new sign-up profile feature: Existing server property and new management mode ENT mode (iOS) signing up an Apple device with Citrix MAM ENT mode (Android) legacy device manager with Citrix MAM ENT mode (Android organization) working profile on a fully managed, With MAM Citrix Mode (iOS and Android) Citrix MAM MDM Mode (iOS) Apple Device Registration MDM Mode (Android) Legacy Device Manager MDM (Android Enterprise) Work Profile In full procedure when you create a delivery group, you can attach a group enrollment profile. If you do not attach an enrollment profile, endpoint management attaches the global enrollment profile. Sign-up profiles provide the following device management features: easier transfer from Android Device Manager (DA) mode to Android Enterprise. For Android enterprise devices, settings include device status such as: fully managed, fully managed, or dedicated work profile. For more information, see Android Organization. For this upgrade, the current endpoint management configurations for Server Status > Android Enterprise Map to the new sign-up profile settings follows. Set current configuration management set to owner mode of Citrix MAM device setting MDM; Managed Google Play (Android Enterprise) Android Enterprise Enterprise enterprise is fully managed off MDM; G Suite (Legacy DA) legacy DA not being available outside of MAM does not manage devices that are not apply to MDM + MAM; Managed Google Play (Android Enterprise) Android Enterprise * Work profile on fully managed on MDM + MAM; Legacy DA Suite* is not available on * Required, allow users to turn device management off. After the upgrade, your current enrollment profiles reflect these mappings. Consider whether you want to create other enrollment profiles to handle new usage cases when switching from legacy to crisd. If you are on board for managing endpoint 19.12.0 or later, the global enrollment profile has these predefined settings. IOS management is easier. For iOS devices, settings include choosing between registering devices as managed or unmanaged. For this upgrade, map your previous configurations to the new enrollment profile settings as follows. Set the Citrix MAM server mode management setting to MDM device enrollment setting off MAM does not manage devices in MDM + MAM device enrollment in if registration is required, allow users to reject device management off. If you are on board for managing endpoint 19.12.0 or later, the global enrollment profile has these predefined settings. Allow Windows 10 devices to automatically register in the Citrix workspace app. For this upgrade, the previous MDM configuration maps for the new enrollment profile setting are fully managed. If you are on board for managing endpoint 19.12.0 or later, the global enrollment profile has these predefined settings. The following limitations exist for enhanced enrollment profiles: The enhanced enrollment profile feature does not work for iOS and Android devices when endpoint management is integrated with the Citrix workspace. The enhanced sign-up profile feature is not available for invitations to register a one-time PIN number or two-stage verification. For more information, see Enrollment Profiles. Simple registration of dedicated Android Enterprise (COSU) devices. Endpoint Management now allows you to register dedicated Android enterprise devices (also called COSU devices) by creating an enrollment profile. No individual is no longer required to create a role-based access control (RBAC) role for registering dedicated devices. See Assign resources to dedicated Android enterprise devices. Turn off biometric authentication on Android devices using keyguard management policies. Keyguard Management Device Policy now allows you to disable fingerprint locking, facial authentication, iris authentication, or any biometric authentication for devices running Android 9.0 or higher. Get guidance in the Resource Center. Use the Resource Center to access data within the product. For dashboard guidance, click the icon in the lower-right corner. Fixed issues managing endpoint 20.2.1 Previously you needed permissions to edit devices before you could use the Endpoint Management API to send messages to devices. You now need send message permissions to send messages. [CXM-76689] When you register a Windows desktop/tablet device that supports WEM and then register the same device in an MDM, the Endpoint Management Console displays two separate values for the device. [CXM-77412] Endpoint 20.1.0 The following features are now rolling out to commercial customers. Editions for U.S. government customers start within three months. For feature differences between the U.S. government's commercial offerings, see Endpoint Management Service for the U.S. Government. Support for Android enterprise COPE devices. Endpoint Management supports fully managed Android enterprise devices with work profiles. Google has previously called these devices AS COPE (enterprise-owned and personally operated). Fully managed Android Enterprise devices have a device profile and a work profile. You can apply separate policy settings to your device and work profile. For this release: You can apply a separate setting to the device and work profile by using these device policies: Certificates, Keyguard Management, Passcode, and Restrictions. You can apply the location mode setting of the location device policy to the COPE device itself, but not to the COPE device work profile. Other settings in the location device policy are not available for COPE devices. See the location device policy. You can apply the Lock separately security action to the device or work profile. Automatically sign up for Windows 10 devices using the Citrix workspace app. Endpoint management can now automatically register your Windows 10 desktops and tablets using the Citrix Workspace app. For more information about this feature, see Integrate with the Citrix workspace experience. Fixed issues managing endpoint 20.1.0 > Apple Deployment Plan settings do not include hop options for the new iOS 13 Setup Assistant screens. During sign-up, users must click through screens for Get Started and Appearance. [CXM-71370] Filters tab is open by default for Management > Devices. [CXM-75823] Single Sign-on ShareFile (SSO) fails for multiplayer clients in the same set of virtual machines. [CXM-75886] Endpoint Management 19.12.0 The following features are now rolling out to commercial customers. Editions for U.S. government customers start within three months. For feature differences between the U.S. government's commercial offerings, see Endpoint Management Service for the U.S. Government. You can now configure delivery groups for Windows devices based on device properties. (Preview) This feature is available only for Windows desktops and tablets. To request access to this preview feature, contact your Citrix sales or support representative. For more information about this feature, see How to add a delivery group (preview). Import Group Policy objects (GPOs) into endpoint management and deploy them directly to Windows 10 devices. Instead of relying on an AD administrator to deploy GPOs from the Group Policy Management Console, you can import and deploy Group Policy objects by using the Endpoint Management Console. See Windows GPO Configuration Policy. Install EXE apps for Windows desktops and tablets. You can now upload EXE applications as enterprise apps for Windows desktops and tablets. For more info, see Add Win32 apps as enterprise apps. Users can no longer remove policies from iOS devices. Some device policies no longer allow users to remove the policy from iOS devices. The Allow user to remove policy setting has been removed for iOS from the following policy: APN policy, mail policy, password policy, profile provisioning policy, proxy policy, and VPN policy. Fixed issues managing endpoint 19.12.0 if you update an application version number with the PUBLIC REST ENDPOINT Management API, and then by using the console: The app version is not updated. [CXM-69216] Sometimes Endpoint Management cannot install EXE applications on Windows devices because the file hash is incorrect. [CXM-75506] Endpoint Management 19.11.0 The following features are now rolling out to commercial customers. Editions for U.S. government customers start within three months. For feature differences between the U.S. government's commercial offerings, see Endpoint Management Service for the U.S. Government. Apple Volume Purchase Program Migration Apple Business Manager (ABM) and Apple School Principal (ASM) companies and institutions through the Apple Volume Acquisition Program (VPP) should switch to apps and books in Apple Business Manager or Apple School Principal before December 1, 2019. Before migrating VPP accounts in Endpoint Management, see this Apple support article. If your organization or school uses only a volume purchase program (VPP), you can register with ABM/ASM and then invite existing VPP buyers to your new ABM/ASM account. For ASM, navigate to . For ABM, navigate to . To update the volume purchase account (formerly VPP) in Endpoint Management: In the Endpoint Management console, click the gear icon in the upper-right corner. The Settings page appears. Click Purchase Volume. The Volume Purchase Configuration page appears. Make sure your ABM or ASM account has the same app configuration as your previous VPP account. On the ABM or ASM portal, download an updated token. In the Endpoint Management console, do the following: Edit the existing volume purchase account with the updated token information for this location. Edit the ABM or ASM certificates. Do not change the extension. Click Save twice. For more information, see: Sign-up profiles control sign-up options for Android device sign-up profiles now control how Android devices register if your Android organization is available for your endpoint management deployment. Sign-up profiles determine whether Android devices are listed in the default Android Enterprise mode (fully managed or in a work profile) or legacy (driver) mode. By default, the global enrollment profile is registered in the new and Android factory reset Devices as fully managed devices and registering BYOD Android Enterprise devices as work profile devices. For more information, see Android Organization. Preparing legacy Android devices for android enterprise by default Google is disparaging device manager mode of device management and encouraging customers to manage all Android devices in device owner mode or profiled mode. (See Driver depreciation in the Google Android Enterprise Developer Guides.) To support this change, Citrix will make your Android organization the default sign-up option for Android devices. This change means that if your Android organization is enabled for your endpoint management deployment, all recently registered or re-registered Android devices are registered as Android enterprise devices. So you can prepare for this change, endpoint management now allows you to create sign-up profiles to control how Android devices are recorded. Your organization might not be ready to start managing legacy Android devices in device or profiled mode. In this case, you can continue to manage them in driver mode. Create an enrollment profile for legacy devices and re-register for all legacy registered devices. To create an enrollment profile for legacy devices: In the Endpoint Management console, go to Configure different profiles > . To add an enrollment profile, click Add. On the Registration details page, type a name for the sign-up profile. Click Next or select Android under Platforms. The Enrollment Configuration page appears. Set up management to manage a legacy device (not recommended). Click Next. Select Assign (Options). The Assign Delivery Group screen appears. Select the delivery group or delivery groups that contain the administrators who are registered with dedicated devices. Then click Save. To continue managing a legacy device in driver mode, register or re-register them using this profile. You have registered driver devices that are similar to work profile devices by downloading the Secure Hub and providing an enrollment server URL. For more information about supporting endpoint management for switching to an Android organization, see blog, Android enterprise as the default for the Citrix Endpoint Management Service. Fixed issues managing endpoint 19.11.0 when you search for a Google Play Store app in the Endpoint Management console, where the app is empty. You can enter the name manually to save the app. Until the problem is fixed, go to the managed Google Play Store to manually approve and save the app. [CXM-73398] for iOS, location tracking does not work if you do the following: configure and deploy location policies, enable tracing from device security operations, and then delete the deployment Policy and create a new one. [CXM-73470] Users with adposy in their user names cannot register their devices when their user name is imported from LDAP. [CXM-73780] Endpoint Management 19.10.0 The following features are now rolling out to commercial customers. Editions for U.S. government customers start within three months. For feature differences between the U.S. government's commercial offerings, see Endpoint Management Service for the U.S. Government. Extended support for Zebra OEMConfig. Endpoint Management now supports zebra device management using the Zebra Technologies Zebra OEMConfig management tool. (For information, see zebra technologies website.) To manage devices using the Zebra OEMConfig app, publish the app and configure android enterprise managed configuration device policies. Content delivery network (CDN) availability for Windows apps. You can now deploy Windows apps using a content delivery network. See Migrate enterprise apps from the Citrix CDN. Group invitation support for users whose names include special characters. When you select a group to accept enrollment invitations, Endpoint Management now receives the list of users from Active Directory. The list includes users whose names contain special characters. See Registration invitations. Fixed issues managing endpoint 19.10.0 After you register a new device or re-register an old device, an error message is displayed intermittently on Management > Devices. [CXM-72634, CXM-73077] When you select a Chrome device or workspace hub in Device Management > > Registered devices, and then click Edit, you receive the following message: A configuration error has occurred. Please try again. This message also appears when you go to those devices in the device list and click View More. Either way, click OK to continue. [CXM-73010] Endpoint Management 19.9.1 support for encryption management for iOS and Android. When you add MDX apps, you can now choose whether MDX or the device platform encrypts data on your device. When you switch to platform-based encryption, compatibility checks work before each app starts. If compatibility checks pass, the app is running and protected by platform encryption. Analysis > Reporting now includes a report of incompatible devices, such as devices that are jailbroken or do not have a passcode. When adding an app, select encryption type: MDX encryption: MDX encrypts the data. MDX does not enforce compatibility. For existing apps, the default is MDX encryption. Platform encryption with compatibility enforcement: The device platform encrypts the data. You choose how compatibility enforcement applies. For new apps, the default is platform encryption with compatibility enforcement. For more information about MDX policies, see MDX policies for third-party apps for iOS and MDX policies for third-party apps for Android. Support for iPadOS. Citrix Endpoint Management Supports 13.x. The device policy for iOS applies to devices running iPadOS. If you plan to register iPadOS devices by sending an invitation link to users, see the Citrix CTX261981 support article. Simpler app management for your Android organization. You should no longer switch to google play managed or google developer portal to approve or publish apps for endpoint management. As a result, the app's certification and advertising take about 10 minutes rather than hours. Approve Android enterprise apps for the Public App Store in the Endpoint Management console. You can now approve managed Google Play Store apps without leaving the endpoint management console. After you enter an app name in the search field, the managed Google Play Store user interface opens with the instructions for approving and saving the app. Your app then populates the results and allows you to configure its details. See Add an app to an app store public app. Approve the MDX apps for an Android organization in the Endpoint Management console. You can now approve managed Google Play Store apps for an Android organization without leaving the Endpoint Management Console. After uploading the MDX file, the Managed Google Play Store user interface opens with the instructions for approving and saving the app. See Add an MDX app. Publish enterprise apps for your Android organization in the Endpoint Management console. You should no longer sign up for a Google Play developer account when adding a private Android app. The Citrix Endpoint Management Console opens a managed Google Play Store user interface so that you need to upload and publish the APK file. See Add an enterprise app. Additional certificate management features for Android enterprise devices in work profile mode or in fully managed mode. In addition to installing certification authorities in the managed key store, you can now manage the following features: configuring the credentials used by specific managed applications. The certificate device policy for an Android organization now includes setting up apps to use certificates. You can specify the apps to use the user credentials issued by the certification provider selected in this policy. Apps are given quiet access to credentials during runtime. To use credentials for all apps, leave the app list blank. See Certificate Device Policy. Quietly remove certificates from the managed key store or uninstall all non-system CA certificates. See Certificate Device Policy. Prevent users from changing certificates stored in the managed key store. The Install restrictions policy for an Android organization now includes the Allow user to configure user credentials setting. By default, this setting is Enabled. See Install restrictions policy. Location device policies are now available for your Android organization. You can set location settings for Android enterprise devices that are managed or run in managed profile mode. Android location tracking requires Android 8.5 and See Location Device Policy. Easy access to BitLocker recovery keys. If a user loses the BitLocker recovery key, unlocking their device can be a challenge. Endpoint Management now displays the BitLocker recovery key for Windows desktops and tablets under device information. See BitLocker Recovery Key. Fixed issues managing endpoint 19.9.1 After you add a custom property with a special character, administrators cannot access the Devices page in the XenMobile console. [CXM-57322] RBAC Tier 2 techs role cannot create user group sign-up invitations with more than 2000 users. Only full administrative users can create the invitations. [CXM-72086] On iOS devices, administrators may lose the ability to send a device unlock command to a password-protected device after upgrading the device to iOS 13.1.x . [CXM-73151] Endpoint Management 19.9.0 keyguard feature management for Android enterprise work profile and fully managed devices. Android Key Protector manages the device and challenges job lock screens. Use the Keyguard Management Device policy to control: Manage Keyguard on work profile devices. You can specify the features available to users before unlocking the device key protector and the Job Challenge Key Protector. For example, by default users can use a fingerprint and display of uns censored messages on the lock screen. Manage Keyguard on fully managed and dedicated devices. You can specify the available features, such as trust agents and a secure camera, before unlocking a keyguard screen. Alternatively, you can choose to disable all keyguard features. See Keyguard Management Device Policy. Samsung Knox Password Reset Container. The Reset Password Container security operation is no longer available for Samsung Knox Enterprise Android devices. Use the Container Lock security action to reset passwords for Samsung Knox containers. The Reset Container Password security operation is still available for Samsung devices in driver mode. Configure the product route for your Android Enterprise apps. When you add a public store app or MDX app for an Android organization, set the product route you want to push to user devices. For example, if you have a track to test, you can select and assign it to a specific delivery group. To learn more about deploying distribution, see the Google Play Help Center. For information about configuring a product track, see Add an MDX app or Add an app store public app. The Windows GPO configuration policy is automatically enabled. The Windows GPO configuration policy automatically allows you to export a Citrix workspace management site to the Citrix cloud. For more information, see Windows GPO Configuration Device Policy. Managed Mobile Device Management (MDM) and Workspace Management (WEM) devices are merged in Terminal. If a device is managed by MDM and managed by WEM, it is now displayed as one device in the Endpoint Management console. The device label in the console is MDM, WEM. Previously, the device was displayed as two different devices. You can also delete devices that are currently managed by MDM and WEM. Fixed issues managing Endpoint 19.9.0 After you deploy the App Access device policy, incompatible devices do not run the configured operation. [CXM-69842] You cannot configure G Suite administrator credentials for Chrome operating system devices. [CXM-71665] Connectivity between endpoint management and Apple's school principal fails. [CXM-71844] MAM devices delete apps and app data due to a failure to complete user domain information. As a result, the device considers the user deleted. [CXM-72093] After you register a new device or re-register an old device, an intermittent error message is displayed on the Management tab. [CXM-72224] Manage Endpoint 19.8.0 for existing clients: Limited port access to the Endpoint Management Console and self-help portal: For customers who were on board before Endpoint Management 19.8.0 (August 1, 2019): You can require that administrators sign the Citrix Cloud console for SSO access to the Endpoint Management console. Citrix strongly recommends all access to the console through Citrix Cloud. Set the new enable.cloud.console.sso server property to True, which means you cannot directly access the Endpoint Management console. Attempts to access the endpoint management console directly on port 4443 cause error 500. Access to the self-help portal is available only through port 443. An attempt to access through port 4443 has now been denied an Access message. For customers who take starting Endpoint Management 19.8.0 (August 1, 2019): New clients log on to the Citrix cloud console for SSO access to the Endpoint Management console. Accessing the Self-Help portal requires a change to the server property. By default, new clients cannot access the self-help portal. To give your users access to the self-help portal, update shp.console.enable to True. Fixed issues managing endpoint 19.8.0 When you import a CA certificate, the console does not display an updated or new certificate under PKI entities. [CXM-68419] When you configure the VPN device policy for iOS to use the Citrix SSO protocol: After you enable the Request PIN option when you connect the setting and save the policy, this setting returns to off. [CXM-68523] For customers migrated from earlier versions, opening the Management tab in the console displays an error if the device enrollment profile has been deleted. [CXM-69750] Endpoint Management 19.7.1 access to all Google Play apps in the managed Google Play Store. Access All apps in the Managed Google Play Store Server feature makes all apps from the Public Google Play Store accessible from the Google Play Store managed. Setting A true feature enables the public Google Play Store apps for all Android users. Administrators can then use the Install Restrictions policy to control access to these apps. Enable system apps on Android devices. To allow users to run preinstalled system apps in Android enterprise work profile mode or in fully managed mode, set the Install Restrictions policy. This configuration gives the user access to default device apps, such as camera, gallery, and others. To restrict access to a particular app, set app permissions using the Android App Permissions policy. Fixed issues managing endpoint 19.7.1 When you send an enrollment link by using SMTP/SMS, the sending link does not work. [CXM-67458] When you try to update a public iOS application by using an endpoint management console, a configuration error is displayed. [CXM-69190] Some third-party volume purchase apps fail to update automatically. This issue occurred because of blocked host names. For more information, see . [CXM-69341] When you add Microsoft Word or PowerPoint for iOS to the cloud app library, the app is failed to assign to a group of users. You must delete and re-add all Intune apps that have encountered this issue. [CXM-69349] Location Device Policy 19.6.1 Endpoint Management now enables device tracking for Android. You can now turn device tracking into questioning specific devices at the frequency you set. You can use this policy to track delivery personnel for more accurate delivery estimates, track lost or stolen devices, or enforce geographic boundaries. For more information, see Location Device Policy. Fixed issues with the Endpoint Management App icons 19.6.1 are not displayed in the Endpoint Management console for automatically uploaded apps. [CXM-66444] After the time period on bulk.enrollment.fetchRosterInfoDelay ends and the Apple School Manager device synchronizes with the server: the Apple School Administrator user account is deleted from the server and the device goes anonymous. [CXM-67913] Users with German special characters, such as umlauts, in their display name cannot register. [CXM-68097] The following error message is displayed when you try to configure a public application by using the URL of the new app from the Apple Store. The app you entered could not be found. Check the URL and try again. [CXM-68537] Managing Endpoint 19.6.0 Automatic Updates for Apple Volume Purchase Apps. When you add a volume purchase account (Settings > iOS), you can now enable automatic updates for all iOS apps. Check the app's automatic update setup for apple volume purchases. Fixed issues managing endpoint 19.6.0 The following error is displayed when you add a registry key to a Windows Embedded Compact 2008 policy if the registry value length exceeds 2048 characters: Terminal Error: A statement could not be executed; SQL [n/a]; A lamented exception is A statement could not be executed. [CXM-59446] During profile installation on an iOS device, unverified appears in the profile information. [CXM-64486] When an Azure AD user logs on to certain Windows 10 Azure AD devices and joins devices that are configured as kiosks, kiosk mode is not turned on. This issue does not occur if you understand the Azure AD user name in azuread\user format. For more information, see Kiosk Device Policy. [CXM-66123] App icons are not displayed in the Endpoint Management console for automatically uploaded apps. [CXM-66444] When you add a volume purchase account (Settings > iOS settings), the following message appears if the token exceeds 350 characters: The company token entered is invalid, please enter a new token. [CXM-68113] Change the endpoint management MDM enrollment workflow to iOS 19.5.0. To improve platform security by reducing misleading profile installations, Apple has released a new workflow to manually register devices in MDM. This new workflow affects all MDM solutions, including Citrix Endpoint Management. There is no change for MDM enrollment to servers assigned to Apple Business Manager or apple's school principal. The workflow changes are only for manual enrollment in MDM. Citrix also simplified enrollment. Previously, iOS device users receive two requests during enrollment: a request for the root CA and a request for approval of the MDM device. Because all Citrix cloud deployments use trusted certificates, the root CA is no longer needed. iOS device users receive only the MDM device certificate request during enrollment. This request is marked XenMobile service profile. To support this change, Citrix has changed the value of the server property, ios.mdm.enrollment.installRootCaIfRequired, to false. The Safari window opens during MDM enrollment to simplify profile installation for users. For more information, see Register iOS devices and the following YouTube video: Changes for new customers to manage endpoints: Workspace experience deployment. You can create a separate delivery group called Workspace to start deploying the workspace experience to new devices. With the Workspace delivery group, you can provide the workspace experience to a small group without disrupting all users. See Integration with the Citrix workspace experience. Policies and apps that you predefine for new endpoint Management 19.5.0 customers. If you're connected to a deck starting with 19.5.0 or later, we're preconfiguring several device policies and mobile productivity apps. This configuration allows you to instantly deploy basic functionality to device users. See Default mobile device and productivity apps policies. You can now enter the KPE Premium and Standard licensing keys for Android Devices running Knox version 3.0 or later. For information, see Knox Device Policy for Enterprise Devices. Public operating device policy for chrome operating system. You can now configure Chrome os devices to support guest sessions. For information about configuring this policy, see Public Session Device Policy. RBAC permission changes. The LOCAL USER ADD/DELETE RBAC permission is now divided into two permissions: adding local users and deleting local users. Fixed issues with Enterprise Endpoint Management 19.5.0 apps do not quietly upgrade on monitored devices running iOS 11.4 or later. What are you doing in here? When you edit a device policy, you receive the following error message: A configuration error occurred. Please try again. [CXM-66370] Managing Endpoint 19.4.1 By using Endpoint Management (WEM) Integration, you can manage all supported Windows devices that came with the domain. This combination offers the following benefits and features: With WEM only, MDM deployments are not possible. When you only manage an endpoint, you're limited to managing Windows 10 devices. By combining the two products: WEM can access MDM features You can manage a wider spectrum of Windows operating systems by managing endpoints Management This takes the form of configuring Windows GPOs objects. Now, administrators are importing an ADMX file to manage Citrix endpoints and pushing it to Windows 10 desktops and tablets to configure specific applications. With the Windows GPO Configuration Device Policy, you can configure Group Policy objects and push changes to the WEM service. The WEM agent then applies the Group Policy objects to devices and their applications. Any device that WEM supports can cause GPO configurations to be pushed to it, even if Endpoint Management does not natively support that device. For a list of supported devices, see Operating system requirements. Devices that accept the Windows GPO Configuration Device policy are running in a new endpoint management mode called WEM. In the Manage > Registered Devices list, the Status column for WEM-managed devices lists WEM. For more information, see Windows GPO Configuration Device Policy. CDN delivery of enterprise apps is now the default for new Endpoint Management 19.4.1 multi-lease customers. If you are a new customer in the Asia Pacific region, contact your Citrix support representative to enable CDN shipping. In all regions, existing customers who want to provide enterprise apps through CDN must reload existing apps after enabling the feature. See Migrate enterprise apps from the Citrix CDN. Support for web apps and SaaS and web links for your Android organization. Endpoint management now supports providing links for web apps or SaaS and Web links to Android enterprise devices. Web apps and SaaS and other web links for your Android organization in the same way they're added for others See Add a web app or SaaS and Add a web link. Additional restrictions for Chrome os devices: View instructions on disabled devices. You can now add a custom message to display on disabled Chrome operating system devices. Allow users to install specific add-ons, apps, and themes. Enter the list of URLs to allow download from these sources. For more information, see Chrome OS Settings. Fixed issues managing Endpoint 19.4.1 on Android enterprise devices, the following app canvases may not appear in Secure Hub: Public App Store apps configured on the Google Play platform and enterprise apps configured on the Android platform. [CXM-63638] Android enterprise apps don't appear for devices until they're registered and registered again. Apps appear even if you update them in their shipping groups. [CXM-64670] Automatic operations may not be deployed to Android enterprise devices. [CXM-64950] Your Android Enterprise name and owner may not display correctly in the Google Play Store Manager console. [CXM-65647] Endpoint Management 19.3.1 Fixed issues managing Endpoint 19.3.1 if you deployed a Store device policy for Windows 10 desktop and tablet devices before releasing 19.3.1: When a user clicks the Windows Store link on the Start menu, You receive a message: 500 Internal Server Error or HTTP Status 404 - You have reached an old URL or this device is not registered. To resolve this issue, you must recreate and deploy your Store Device policy. [CXM-61785] If an Active Directory user group is assigned to RBAC role permissions, you cannot delete the LDAP configuration that contains that user group. As a workaround, if you unassign the appropriate Active Directory group from the RBAC, you can delete the domain. [CXM-62737] Endpoint Management 19.3.0 support for Samsung Knox on Android Enterprise Policy Consolidation. For Android enterprise devices running Samsung Knox 3.0 or later and Android 8.0 or later: Knox and Android Enterprise are integrated into a unified device and profile management solution. Configure Knox settings on the Android Organization page of the following device policy: Install app inventory policies for your Android organization. You can now inventory Android enterprise apps on managed devices. For more information, see Install app inventory policies. File device policy for Android enterprise. You can now add endpoint management scripts to perform functions on Android enterprise devices. See File Device Policy. Lock and reset the password for your Android organization. Endpoint Management now supports password locking and reset security operation for Android enterprise devices registered in work profile mode running Android 8.0 and a larger version. See Security actions. Active Azure Guide support at the kiosk on Windows 10 desktop and tablet devices. You can now add Azure AD devices that are joined to a domain in kiosk mode. See Device policy. For endpoint management customers when the workspace experience is enabled: Citrix Endpoint Management supports one-way authentication in the Workspace app on iOS and Android. This feature does not support Azure Active Directory. For information, see Change authentication to workspaces. Change the PUBLIC REST API. The Public Endpoint Management API for REST Services now includes a platform information editing API within the container for MDX applications. See section 3.15.2.4 update platform information within the container for MDX applications in PDF, Public API for REST Services. Fixed issues managing endpoint 19.3.0 locking fully managed remote Android enterprise devices through locking with password security operation may fail without notifying you of the failure. To make sure a device is locked, set Lock with passcode twice. The device locks with the second passcode you set. [CXM-61095] If your organization is deleted from a managed and updated Google Play on an endpoint management server, Android enterprise devices cannot be registered at times. [CXM-62769] for integrating Citrix Endpoint Management with Microsoft Endpoint Manager: Changes made to the Intune Store app name or description are lost. [CXM-62842] After editing the iOS Intune app, the app will not install from the Microsoft Company Portal app. [CXM-62972] If you are assigned permission as a custom Citrix Cloud administrator instead of as a full administrator, you cannot click the Manage button to navigate resources. [CXM-63433] Depreciation of TLS versions To improve the security of the Citrix Endpoint Management Service, Citrix is currently blocking all communications through Transport Layer Security (TLS) 1.0 and 1.1. As a result of the weakening of security, the PCI Board disparages TLS 1.0. How this change affects you If you use Mobile Application Management by using the On-Premises Citrix Gateway (NetScaler Gateway), you must update your Load Balancer service to enable TLS 1.2. Older versions of the following connectors support TLS 1.0 only: Endpoint Management Connector for Exchange ActiveSync Citrix Gateway Connector for Exchange ActiveSync Upgrade your connector as follows: If you use the Endpoint Management Connector for Exchange ActiveSync build 10.1.3 or lower, upgrade to build 10.1.4 or higher. If you use the Citrix Gateway connector for Exchange ActiveSync to build 8.5.0 or lower, upgrade to build 8.5.1.11 or higher. What to do If you are using a local Citrix gateway (NetScaler gateway), enable TLS 1.2 in your load balancer service. For information, see . To download one of the Members of Exchange ActiveSync: 1. Go to <https: www.citrix.com/downloads=>. 1. Navigate to **Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (On-Premises) > Software Product > XenMobile Server 10 > Server Components**. 1. Locate the connector tile </https:>Then click **Download File**. Manage Endpoint 19.2.1 Run multiple apps at a kiosk on Chrome devices. You can now add multiple apps to a kiosk policy for the Chrome operating system. You can start apps automatically when the user starts the device. See the Kiosk device policy. Fixed issues managing Endpoint 19.2.1 After an Android organization is not registered and then re-enrolled, approved applications do not appear on devices that are listed in work profile mode. [CXM-59994] When users first start secure mail in Intune MDM+MAM, the installation takes users through a workflow to select Intune MAM/XenMobile. [CXM-31272] Manage Endpoints 19.2.0 Enterprise Application Provider from a Content Delivery Network (CDN). When a user is not located near an endpoint management server, delivery of enterprise applications can take some time. For faster app downloads, you can instead get enterprise apps from content delivery network (CDN) locations around the world. CDN support for enterprise apps is available for iOS apps (MDM or MAM sign-up) and Android apps (MDM or MAM sign-up). CDN support for enterprise apps is not available for Windows apps. To get started, see Migrate enterprise apps from the Citrix CDN. Change DEP device enrollment for the Citrix workspace. If endpoint management is integrated with the Citrix workspace, the workspace application is included in the DEP deployment package as a required application. This feature requires that you configure your DEP account settings for iOS when the required credentials are set to off. Secure Hub prompts users to register the device in the Citrix workspace before signing up for endpoint management. The ios.mdm.enrollment.installRootCaIfRequired server property is currently set to false. Endpoint management uses a trusted public certificate chain, so you don't need to push a root certification authority to devices. As a result, iOS device users no longer receive a request to install an underlying certification

authority during enrollment. The WiFi policy and certificates now support Apple TV OS. For more information, see the Policies for a Wi-Fi device, certificates, and AirPlay security device. Location device policies are now available for your Android organization. You can set location settings for Android enterprise devices that are managed or run in managed profile mode. See Location Device Policy. Improved support for Alexa for Business. Endpoint management now includes support for Alexa for business conferencing, adding Alexa skills to your organizations, editing skill sets. Look for Alexa for business. Automatic actions for the Windows Agent policy. With the Windows Agent policy, you can automate actions to run on Windows desktops and tablets based on registry entries. For more information, see the Windows Device Policy and Automatic Actions articles. For Android Enterprise, No The option for required characters in passcode is currently unavailable. Android enterprise devices running Android 7 or higher no longer support passcode generated without character restrictions. If you previously set required characters without restrictions, this update changes this value to numbers only. This change does not affect the user's current signing experience. For more information, see Android Enterprise Settings. Fixed issues managing Endpoint 19.2.0 When an app is deleted from an Intune library, and a user tries to delete it from a Citrix cloud library, they cannot delete it. [CXM-61645] After uploading the Google Play app in the Endpoint Manager console without adding an app icon image: If you later upload a photo for the app, the image won't appear in the App list. [CXM-60965] Device Policy 19.1.2 Endpoint Management Files is now available for Android Enterprise. You can add endpoint management scripts to perform functions on Android enterprise devices. See File Device Policy. Configures time zone settings for Chrome operating system devices. You can now select a time zone for your Chrome device and specify how to identify the time zone. For more information, see Install restrictions policies. RBAC administrator group permissions now restrict user information displayed on the User Orders and Registration Invitations pages. Previously, the Endpoint Management Console included information for all local users and domain users on the Manage > Users and Management pages > Enrollment invitations. To specify which user groups the RBAC administrator has permission to view and manage, edit the administrator role and specify the user groups. For more information, see Configure roles using the RBAC. Launch third-party apps from the Workspace app. For customers with a Citrix workspace enabled: Before deploying new apps to users, you can add a comma-separated list of URLs to run the apps from the Workspace app. For more info, see Add apps. Fixed issues with Endpoint Management 19.1.2 You cannot upload APK versions to Google Play Services later than 11.5.09 in the Endpoint Management Console. [CXM-59492] Edit windows desktop and tablet apps B Set > Apps > Public App Store causes this message: App search failed. Searching for these apps result in this message: Error connecting to Windows desktop store URL: Failed to retrieve public app information. [CXM-61686] [CXM-61686]