

**Modern Client Management and BigFix Mobile
Administrators Guide**



Special notice

Before using this information and the product it supports, read the information in [Notices \(on page clxiii\)](#).

Edition notice

This edition applies to BigFix version 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

- Chapter 1. Modern Client Management and BigFix Mobile..... 6**
 - What’s new in this release 7
 - Features added in the previous releases..... 9
 - Device Enrollment.....16
- Chapter 2. BigFix MCM..... 19**
 - Enrolling Windows devices.....19
 - Enrolling through enrollment URL - Windows.....19
 - Bulk enrollment - Windows.....24
 - Autopilot enrollment - Windows24
 - Autopilot enrollment with Offline Domain Join service.....28
 - Enrollment by non-admin device users.....33
 - SCEP enrollment.....55
 - Enrolling Apple devices.....58
 - Enrolling through enrollment URL - Apple.....58
 - Apple Automated Device Enrollment.....59
 - Apple BYOD enrollments.....60
 - SCEP enrollment.....63
 - Full Disk Encryption.....69
 - Windows BitLocker.....71
 - MacOS FileVault.....72
 - Set up the BES Server Plugin Service (Fixlet 708 in BES Support).....72
 - Recovery Key Escrow Configuration.....73
 - Application management75
 - OS update.....76
 - User management.....76
- Chapter 3. BigFix Mobile.....77**
 - Android mobile management.....77
 - Managed Google Play Accounts enterprise.....81
 - Provisioning Android devices.....82
 - Android policy management.....111

Android device management.....	112
Device trust.....	114
Android device security.....	117
Application management	123
Android Kiosk management.....	130
Android hardware security.....	134
Cross-profile management.....	135
Verify Apps enforcement	137
VPN management.....	138
Wi-Fi configuration management.....	140
Apple mobile management.....	142
Provisioning Apple mobile devices.....	144
Apple mobile policy management.....	145
Chapter 4. Apple VPP Apps and Books.....	146
Chapter 5. SCEP Certificate-based authentication.....	148
Chapter 6. SAML-authenticated enrolment flow.....	150
Chapter 7. Known limitations.....	153
Chapter 8. Troubleshooting.....	154
Verify if PPKG generation point is set for bulk enrollment.....	154
Enrollment fails with 401 authentication error.....	154
Policy is deployed, but is not effective on the device	155
Apple profile displayed as unverified	156
Android Kiosk not connected to Internet.....	157
Endpoint not disconnected from AD after unenrollment.....	158
Health Check MDM Plugin Status is not displayed properly.....	159
Generating Encryption Recovery Key Escrow fails.....	160
Chapter 9. Frequently Asked Questions.....	161
Appendix A. Support.....	162
Notices.....	clxiii
Index.....	

Chapter 1. Modern Client Management and BigFix Mobile

This guide is intended for HCL BigFix Master Operators (MO) and those who administer BigFix deployments. If you are looking for information about using Modern Client Management (MCM) and BigFix Mobile, see the [WebUI User's Guide](#).

MCM and BigFix Mobile is the MDM solution from BigFix to manage devices that run operating systems through a vendor's Mobile Device Manager (MDM) API. With this offering, BigFix can interact with your devices through MDM.

With MCM and BigFix Mobile, organizations can enroll their corporate-owned and employee-owned (BYOD) laptop and mobile devices to monitor, manage, and secure them from a single web console, BigFix WebUI. The MDM server through MDM APIs manages all the actions that you perform through BigFix Console or BigFix WebUI.

BigFix can deploy profiles, custom content, patches, software, and BigFix agents through the BigFix Console or BigFix WebUI. BigFix can also wipe or lock devices remotely if devices get lost or stolen.

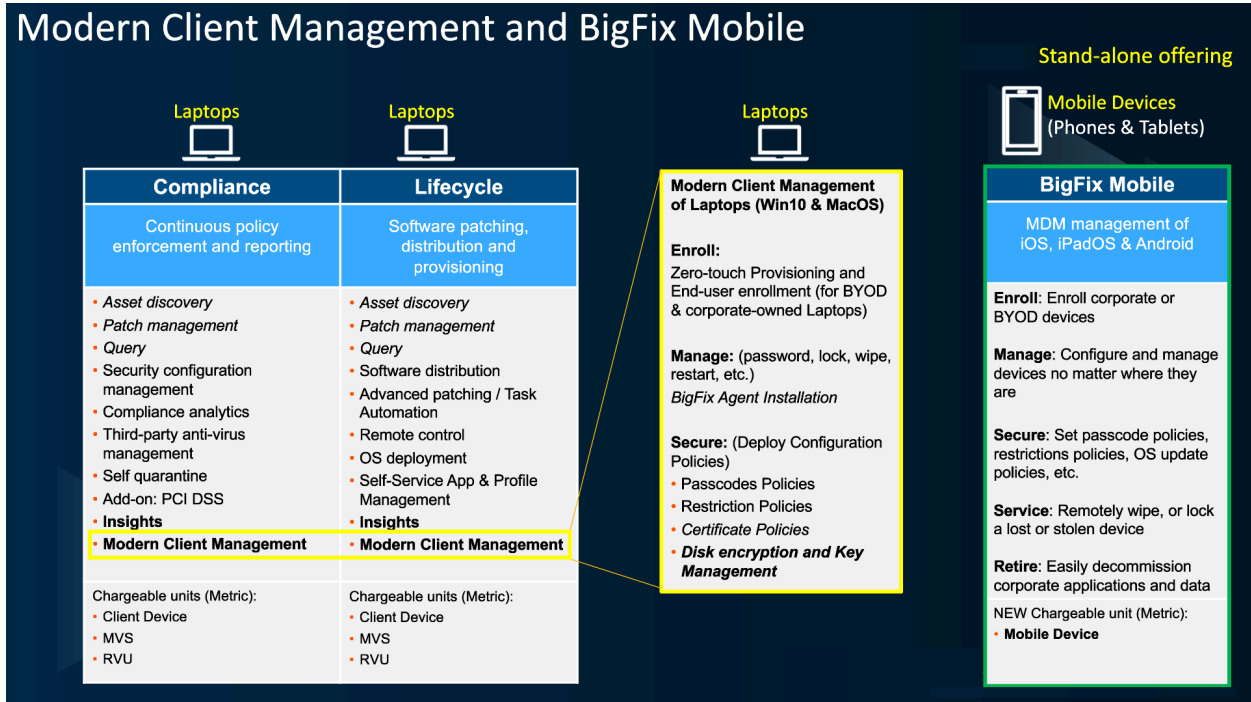
If you have one of the following licenses, you can enroll and manage laptops (Windows and macOS).

- BigFix MCM
- BigFix Mobile
- Lifecycle
- Security and Compliance

If you have the license for BigFix Mobile you can enroll and manage Android, iOS, and iPadOS devices.

If you have license for both MCM and BigFix Mobile, you can enroll and manage laptops as well as Android, iOS, and iPadOS devices.

The following image represents the features available for *MCM* and *BigFix Mobile* individually and as a whole.



Document conventions

Throughout this documentation:

- *MCM* represents features and services available only for laptops (Windows and macOS).
- *BigFix Mobile* represents features and services available only for mobile devices.
- *MCM and BigFix Mobile* represents common features and services available for both laptop and mobile devices.

What's new in this release

Overview of the enhancements made in the current release of MCM and BigFix Mobile.

MCM and BigFix Mobile v3.0 updates

Windows Active Directory and Hybrid Domain Join

BigFix MCM supports Active Directory and Hybrid Domain Join through Offline Domain Join (ODJ) service. Hybrid Domain Join enables organizations to leverage existing on-premises Active Directory infrastructure while taking advantage of the benefits of cloud-based authentication and management. When enabled, users can sign in to their devices using their on-premises credentials, and then access cloud-based resources without having to enter additional credentials. For setup and configuration information, see Domain join installation and configuration.

Custom Templates

With MCM v3.0 release, WebUI provides a set of custom policy templates suitable for Windows, Apple, and Android that you can directly save or modify to create custom policies. For more information on how to create custom policies through available custom templates, see [Custom from Template](#).

User-based endpoint targeting and enrollment

With MCM v3.0, you can target specific set of users and end-user devices to deploy specific MDM policies and actions. BigFix MCM integrates Active Directory Group Membership and Attributes to create Smart Groups. Smart Groups in association with Policy Groups evaluate applicable users and endpoints (based on group membership, attributes, device type, enrollment type and so on) to target and deploy policies and actions during enrollment or post enrollment. For information on how to create Smart Groups through WebUI, see [Smart Groups](#).

Secure certificate deployment through Simple Certificate Enrollment Protocol (SCEP)

IT admins can now automate issuing certificates to the endpoints to provide access to corporate Wi-Fi, VPN, and secure e-mail through encryption by integrating SCEP with BigFix MCM. To understand the SCEP enrollment flow, see [SCEP enrollment \(on page 55\)](#). To configure SCEP, see [Simple Certificate Enrollment Protocol \(SCEP\) configuration](#).

Apple User Enrollment for BYOD

With MCM v3.0, device users can enroll their own Apple devices. This allows the organizations to securely manage the work profile on those devices while the device users can enjoy the privacy on their personal profile as organizations cannot wipe, lock, or otherwise impose control over their personal profile. For more information, see [Apple BYOD enrollments \(on page 60\)](#).

Apple VPP Apps and Books Support

IT Admins can manage custom apps, Apple Appstore apps to User Enrolled devices, and company licensed-app store apps on all MCM enrolled Apple devices, as MCM is now integrated with the Apps and Books (VPP) capabilities in Apple Business Manager. For more information, see [Apple VPP Apps and Books \(on page 146\)](#).

SAML-authenticated enrollment

BigFix MCM and BigFix Mobile support Security Assertion Markup Language (SAML) authentication to enroll devices. The user's SAML credentials are used to authenticate their identity to complete the enrollment process. With MCM v3.0 release, Okta is tested and supported as a SAML identity provider with AD/Open LDAP and Azure AD as identity services. For more information, see [SAML-authentication configuration](#).

Android - Additional features supported

Cross-profile management: BigFix Mobile supports Android crossprofile management through which organizations can protect and control data sharing from work profile to personal profile in the same device. For more information, see [Cross-profile management \(on page 135\)](#).

Password Wipe: From MCM v3.0 onwards, Password Wipe support is extended for Android mobile devices. For instructions, see [Passcode Wipe](#).

Other enhancements

- **Primary User Assignment:** You can now assign or modify primary user for a device through User Assignment action. When a device has primary user info, it can be easily managed through Smart Groups. If you want to assign primary user for huge number of devices, contact HCL Support at BigFixServices@hcl.in
- **Enrollment UI Rebranding:** You can change the appearance of the Enrollment UI and Android Server Configuration UI by changing the color, image, logo, brand name and so on. For instructions, see Rebranding user interfaces.

Upgrade

For all the MCM v3.0 features to work, upgrade BigFix Plugin Portal to 10.0.8 or later. You can find instructions to upgrade MDM components at On-premises Upgrade.

Features added in the previous releases

Overview of the enhancements made in the previous releases of MCM for BigFix 10.

MCM and BigFix Mobile v2.1.3 updates

MCM Admin UI password must be set with high complexity

MCM Admin UI password must be set with high complexity. This enables the application to restrict the user to log in if the user enters wrong credentials five times consecutively. If the password is not set with high complexity, then the user can make unlimited failed attempts to log on to Admin UI.

Improved unenrollment behavior

With BigFix Platform versions earlier than 10.0.8, when a device is unenrolled and then re-enrolled, WebUI and Console displayed multiple devices with unique computer IDs creating confusions.

With BigFix Platform 10.0.8 release, when you unenroll an MDM device, it deletes the device from the root server, Console, and WebUI. To enable this feature, upgrade BigFix Platform to 10.0.8 or later; no MCM upgrade is required to enable this.

For the steps to unenroll an MDM device, refer to Unenroll devices.

MCM and BigFix Mobile v2.1.1 updates

This section lists updates on features that are applicable for both MCM and BigFix Mobile in this release.

Create PPKG with Expiration Time

PPKG creation is made simpler and more secure with this release. Admins can configure expiration time for their PPKG, which stops enrolling Windows devices through that PPKG beyond the specified expiration time. Also, WebUI internally creates a unique token for every PPKG that gives more control to

prevent unwanted usages of the PPKG. For information about how to create a timestamped PPKG, see [Bulk enrollment - Windows](#)

Upgrade Considerations:

- If you want to deploy timestamped PPKG on to an MDM server, ensure the MDM server is upgraded to v2.1.1 or later.
- PPKG files created without expiration time (created through older version of BigFix MCM) do not work as expected in MDM server v2.1.1 or later. Therefore, you need to create PPKG again and deploy.

MCM and BigFix Mobile v2.1 updates

This section lists updates on features that are applicable for both MCM and BigFix Mobile in this release.

Added operating systems Support

This version additionally supports the following operating systems:

- Android 12
- iOS/iPadOS 15
- Windows 11
- macOS Monterey 12

MCM 2.1 Updates

This section lists updates on features that are applicable for MCM in this release.

OS update for MacOS

BigFix MCM 2.1 includes an action to update the system software in macOS devices. For instructions and more information, see OS Update section of Deploy MCM actions of WebUI User Guide.

System Extension Whitelist for MacOS

With BigFix MCM 2.1, you can create system extension policy. System extensions allow software like network extensions and endpoint security solutions to extend the functionality of macOS without requiring kernel-level access. For instructions, see System Extension Whitelists.

BigFix Mobile 2.1 Updates

This section lists updates on features that are applicable for BigFix Mobile in this release.

Android dedicated device support

From UEM 2.1 release, BigFix Mobile supports Android dedicated devices. Now, you can enroll and manage company-owned devices in Kiosk mode. For more information, see Dedicated device management section in [Android mobile management \(on page 77\)](#).

Android Advanced feature set support

This release supports the following Android features:

- **Verify Apps enforcement** - Scans all the apps installed on Android device for harmful software before and after they are installed to ensure that malicious apps can not compromise corporate data. For more information, see [Verify Apps enforcement \(on page 137\)](#).
- **VPN Management:** Allows IT admins to ensure that data from certain apps always goes through the VPN specified. They can also apply a setting such that device is connected to the network only when VPN is connected. For more information, see [VPN management \(on page 138\)](#)
- **WiFi Configuration management:**
 - Allows IT admins to silently provision enterprise WiFi configuration on managed devices.
 - Allows IT admins to lock down WiFi configurations on managed devices, restricting the users from creating new configurations or modifying the existing corporate configurations.

For more information, see [Wi-Fi configuration management \(on page 140\)](#).

- **Private app management:** IT Admins can add and manage private apps for Android Enterprise devices via Managed Google Play. For more information see, [Private app deployment \(on page 127\)](#).
- **Hardware Security management:** IT Admins can lock down hardware elements of a company-owned device to ensure data and device security. For more information see, [Android hardware security \(on page 134\)](#)

Advanced Android Zero Touch enrollments

- Android Zero Touch enrollments are made much more easier with Zero Touch Automatic configurations. Also, IT admin to automate much of the device enrollment process. See [Automatic zero-touch configuration \(on page 98\)](#).
- With Sign-in URLs, IT admins can limit enrollments to specific accounts or domains. See [User-authenticated zero-touch enrollment configuration \(on page 104\)](#).

EMM Managed Android Enterprise account

Creating Android Enterprise account is simpler than before, as the organizations do not need a Google account. For more information, see [Managed Google Play Accounts enterprise \(on page 81\)](#).

Clear passcode for iOS/iPadOS

UEM 2.1 release includes a WebUI action to facilitate system admins to remotely wipe passcode on iOS and iPadOS devices. If device users forget their Apple device password, this feature helps them to get back and use the devices, For instructions, see Deploy MCM actions of the WebUI User Guide.

BigFix Mobile and MCM v2.0 updates

BigFix Mobile

With this release, BigFix introduces BigFix Mobile. BigFix Mobile comes with a host of new features to enroll, manage, secure, service and retire iOS/iPadOS and Android devices. With BigFix Mobile, you can automate enrollment, configuration, remediation, compliance, and advanced analytics. To learn more about this solution and the supported features, see [BigFix Mobile \(on page 77\)](#).



Important:

- BigFix Mobile is a separate offering for managing mobile phones and tablets that comes with its own license. You need to buy the BigFix Mobile license to enroll or manage mobile devices. If you do not have the BigFix Mobile license, the WebUI will not show any references to Android, iOS or iPadOS workflows, and will only support Windows (Windows 10 and Windows 11) and macOS workflows.
- The BigFix Mobile license is only for Mobile Device Support, which does not include Windows or macOS MDM Management. However, due to some dependencies, MDM control of these platforms will technically work for BigFix Mobile - only customers until the end of 2021.

MCM and BigFix Mobile v2.0 updates

This section lists updates on features that are applicable for both MCM and BigFix Mobile in this release.

• WebUI user experience updates

- Mobile support: If you have the BigFix Mobile license, you can manage mobile devices with WebUI. WebUI dynamically displays UI according to your license.
- MCM Dashboard: Modern Client Management dashboard provides insights into every aspect of device management, device security, and device encryption.
- Jump To: This drop down provides quick links to navigate to different pages within the MCM application.
- Admin section: You can now Install MDM servers, Plugins, and do operational tasks from Admin section.
- Policy Group: Create a default policy that gets deployed to MDM endpoints at enrollment time by combining MDM policies, custom policies, apps, and BigFix Agents. For more details, see Policy Groups
- Health Check: Extended health check to monitor the BigFix Mobile environment and disk encryption. For more details, see Health Check.

• Apple Bootstrap token support

MCM now supports MDM operations that require use of the bootstrap tokens. For more information, see [Bootstrap tokens for Apple devices](#).

• New Fixlet - Update Apple Enrollment Certificate before expiration

This release introduces a Fixlet to renew Apple Device Identity Certs that are assigned to an Apple device at the time of MDM enrollment. For more details, see [Update Apple Enrollment Certificate before expiration](#).

- **MDM-debug tool**

This tool can be used to set log levels for individual/group/all MDM modules, execute commands and update policy settings on the MDM enrolled devices using REST APIs. This will be helpful to quickly debug production issues when there is a communication failure at different MDM layers and to trace the execution work flows, requests, and endpoint responses. For instructions on how to use it, see [MDM debug tool](#)

- **Autopilot cli for enrollment of Windows 10 devices**

This release introduces a command line utility to set up and trigger Autopilot enrollment of Windows 10 devices. For a complete step-by-step procedure and instructions, see [Autopilot enrollment](#).

- **Enrollment by non-admin Windows 10 device users**

Windows 10 device users without admin credentials can now enroll devices to BigFix MCM. They can enroll a single device over-the-air or automatically bulk enroll multiple devices without admin rights and manage them through BigFix MCM. For more details, see [Enrollment by non-admin device users \(on page 33\)](#)

- **Full Disk Encryption**

MCM v2.0 introduces the [Full Disk Encryption \(on page 69\)](#) feature to centrally manage the native full-disk encryption technologies of Windows (BitLocker) and macOS (FileVault2) to secure data at rest.

- **WNS credentials**

The communication between Windows Notification Services (WNS) and the MDM server is securely established using WNS credentials. Windows now requires customer specific WNS credentials to be procured and provided at the time of all installs and upgrades that include a Windows MDM server. For more information about how to generate WNS credentials, see [Generating WNS credentials](#). Users can upload WNS credentials through BESUEM Fixlets or through WebUI.

- **Performance enhancements**

This release includes a number of stability and performance enhancements and fixes. For capacity planning and configuration recommendations, see [BigFix Capacity Planning documentation at BigFix Performance & Capacity Planning Resources](#).

- **Addressed security vulnerabilities**

Product security vulnerability issues from MCM v1.1 are addressed in this release.

Update considerations

MCM v1.1 updates

- **Apple Automated Device Enrollment**

MCM v1.1 introduces a feature that helps you to set up and pre-configure new or factory reset macOS devices automatically. For complete information and setup instructions, see [Apple Automated Device Enrollment \(on page 59\)](#).

- **Autopilot enrollment of Windows 10 devices**

This release introduces the Autopilot feature that helps you to set up and pre-configure new or factory reset Windows 10 devices automatically. For complete information and setup instructions, see [Autopilot enrollment](#).

- **Bulk enrollment of Windows 10 devices**

The Bulk enrollment feature in MCM v1.1 facilitates you to enroll a large number of BigFix managed Windows 10 devices to MDM server within minutes. For more information, see [Bulk enrollment - Windows \(on page 24\)](#).

- **Certificate management**

MCM v1.1 introduces the ability to deploy certificate policies on MDM endpoints for both macOS and Windows to make it much easier for you to manage certificates. For instructions, see [Certificates Policy](#)

- **Configure and Manage BigFix MCM through WebUI**

This release includes the ability to configure and manage BigFix MCM through WebUI. You can easily install MCM components, upgrade, and uninstall through WebUI. For detailed instructions, see [MCM User Guide](#).

- **Deploy software to MDM endpoints**

With this release, you can deploy software applications to MDM endpoints via MDM APIs through WebUI quickly. For instructions, see [Prestage an Application](#)

- **Restriction profiles**

With MCM v1.1, you can create restrictions profiles for both Windows and macOS. Configuring many settings like privacy and user experience on MDM endpoints is straightforward and simple.

- **LDAPS utility**

MCM v1.1 introduces a command line utility through which you can quickly troubleshoot LDAPS issues.

- **Unenroll**

From this release, if you want to unenroll your devices from MCM, you can do it through WebUI. For instructions, see [Unenroll devices](#).

- **Fixlets to upgrade MCM components**

With MCM v1.1 release, you can update MDM Enrollment Profile for Apple devices. Take a look at the BESUEM site for the relevant Fixlets.

- **Performance enhancements**

This release includes a number of stability and performance enhancements and fixes. For capacity planning and configuration recommendations, see BigFix Capacity Planning documentation at [BigFix Performance & Capacity Planning Resources](#).

- **Addressed security vulnerabilities**

Product security vulnerability issues from MCM v1.0.1 are addressed in this release.

MCM v1.0.1 updates

- **Support for the BigFix Work from Home Solution**

MCM v1.0.1 supports the BigFix Work from Home Solution. For complete information about the BigFix Work from Home Solution, read [The BigFix Work from Home Solution Guide](#).

- **Performance enhancements**

This release includes a number of stability and performance enhancements and fixes. For capacity planning and configuration recommendations, see BigFix Capacity Planning documentation at [BigFix Performance & Capacity Planning Resources](#).

- **Extended operating system support**

- The MCM solution supports RHEL 8 on MDM Server and Plugin Portal servers with a workaround to install Docker CE. For more information, see [Installing Docker CE and Docker compose on RHEL8](#)
- The MCM solution supports Windows 10 (Pro, Enterprise, and Home) running on MCM endpoints.



Note: Only certain Windows editions support all available operating system features that are configured through MDM. For complete information, see the Windows [Configuration service provider \(CSP\) reference](#) document. Each CSP highlights which Windows editions are supported.

- **Fixlets to upgrade MCM components**

With MCM v1.0.1 release, you can upgrade the MCM components by using Fixlets that are available through the BigFix Console. Take a look at the BESUEM site for the relevant Fixlets.

- **WebUI Health Checks dashboard for MCM serviceability**

The WebUI Health Checks dashboard is available to monitor the health of your BigFix MCM deployments. For more information, see [Health Checks](#).

- **Addressed security vulnerabilities**

Product security vulnerability issues from MCM v1.0.0 are addressed in this release.

Device Enrollment

You must enroll your devices to manage them with MCM and BigFix Mobile. MDM servers interact with the enrolled devices through MDM APIs.

MCM and BigFix Mobile support multiple enrollment methods based on the device's operating system and the requirements in an organization. You have options to allow device users to self-enroll devices or let admin users configure settings to automatically enroll devices in large numbers.

Apple device (iPhone, iPad, and Mac) enrollment management

If you are managing iOS, iPadOS, and macOS devices, you will come across [Apple Business Manager](#) and [Apple School Manager](#) that include Device Enrollment (formerly known as DEP) and Volume Purchase Program. Apple Business/School Manager is Apple's web portal, where IT admins can enroll their Apple devices and manage applications and licenses through VPP.

Android device enrollment

To automate the enrollment of Android smart phones and tablets, you can utilize built-in device management platforms. For managing software licenses and app installations, organizations can use the [Managed Google Play Store](#).

The following table shows the different combinations of enrollment methods and operating systems along with the scenarios.

Enrollment method	Operating System	Scenario
Enrolling through enrollment URL <ul style="list-style-type: none"> • Windows (on page 19) • macOS, iOS, and iPadOS (on page 58) • BYOD Android devices - provisioning with the enrollment URL (on page 84) • BYOD Apple devices- provisioning with the enrollment URL (on page 60) 	Windows, macOS, iOS, iPadOS, and Android	<ul style="list-style-type: none"> • The devices are already with the employees. • The number of devices to be enrolled are relatively less. • User can initiate enrollment.

Enrollment method	Operating System	Scenario
<ul style="list-style-type: none"> • BYOD Android devices - QR code enrollment (on page 88) • Fully-managed Android devices - QR code enrollment (on page 93) 	Android	<ul style="list-style-type: none"> • The devices are already with the employees. • The number of devices to be enrolled are relatively less. • Admin authenticates after which user can initiate enrollment with QR code.
Bulk enrollment	Windows 10, Windows 11	<ul style="list-style-type: none"> • Large number of Windows 10 and Windows 11 devices to be enrolled with MDM Server. • The enrollment needs to be automated without user intervention. • The devices have BigFix agent installed already.
Autopilot enrollment - Windows (on page 24)	Windows 10 and Windows 11	<ul style="list-style-type: none"> • Large number of company-owned Windows 10 and Windows 11 devices that need initial OS setup to be enrolled with MDM Server. • The enrollment needs to be automated without user intervention.
Autopilot enrollment with Hybrid Domain Join - Windows (on page 28)	Windows 10 and Windows 11	<ul style="list-style-type: none"> • The organization has an on-premises Active Directory Domain Services (AD DS) environment, and you want to join your Azure AD joined Windows laptops to your AD DS domain. • Large number of company-owned Windows 10 and Windows 11 de-

Enrollment method	Operating System	Scenario
Apple Automated Device Enrollment <i>(on page 59)</i>	macOS, iOS, iPadOS	<p>vices that need initial OS setup to be enrolled with MDM Server.</p> <ul style="list-style-type: none"> The enrollment needs to be automated without user intervention. Large number of company-owned Apple devices (macOS, iOS, iPadOS) that need initial OS setup to be enrolled with MDM Server. The enrollment needs to be automated without user intervention.
Zero-touch enrollment <i>(on page 95)</i>	Android	<ul style="list-style-type: none"> Large number of company-owned Android devices that need initial OS setup to be enrolled with MDM Server. The enrollment needs to be automated without user intervention.
Secure certificate deployment and enrollment using SCEP <i>(on page 55)</i> When the SCEP environment is set up, the following methods of enrollment are supported for certificate enrollment using SCEP: <ul style="list-style-type: none"> OTA enrolment Bulk enrollment Autopilot enrollment 	Windows 10, Windows 11, macOS, iOS, iPadOS	IT administrator can automatically enroll every managed device for a client certificates without requiring any end user interaction.
SAML-authenticated enrollment <i>(on page 150)</i>	Windows 10, Windows 11, macOS, iOS, iPadOS, Android	To authenticate the user via the identity provider before proceeding with the enrollment process.

Chapter 2. BigFix MCM

Read this section to learn enrolling and managing Windows and macOS desktop and laptop devices.



Important: Ensure all the operating system specific analyses are activated through [WebUI Health Check](#) for MCM app to work as expected.

Supported Operating Systems and versions

- Windows 10
- Windows 11
- macOS 10.14 and later

Related information

Enrollment methods

[Full Disk Encryption \(on page 69\)](#)

[Application management \(on page 75\)](#)

Enrolling Windows devices

You can get Windows 10 and Windows 11 devices enrolled in BigFix MCM in many ways.

- [Enrolling through enrollment URL - Windows \(on page 19\)](#): Users can self-enroll their Windows desktops.
- Bulk enrollment: MCM Admins can enroll large numbers of Windows devices with the same configuration all at once. For this, MCM Admin configures policies through the Windows provisioning tool and triggers enrollment through BigFix WebUI.
- [Autopilot enrollment - Windows \(on page 24\)](#): MCM Admins can configure the Autopilot settings in Azure Active Directory (Azure AD). The devices configured to be enrolled with Windows Autopilot are automatically enrolled in BigFix MCM on first boot up.
- [Enrollment by non-admin device users \(on page 33\)](#): You can also enroll your devices to BigFix MCM without admin credentials. You can enroll a single device over-the-air or automatically bulk enroll multiple devices without admin rights and manage them through BigFix MCM.
- [Autopilot enrollment with Offline Domain Join service \(on page 28\)](#): MCM Admins can configure to automatically enroll remote or mobile devices by accessing domain resources.
- [SCEP enrolment \(on page 148\)](#): For MCM admins to automatically provision certificates to all the MCM-managed devices and provide access to corporate Wi-Fi, VPN, and secure e-mail through encryption.

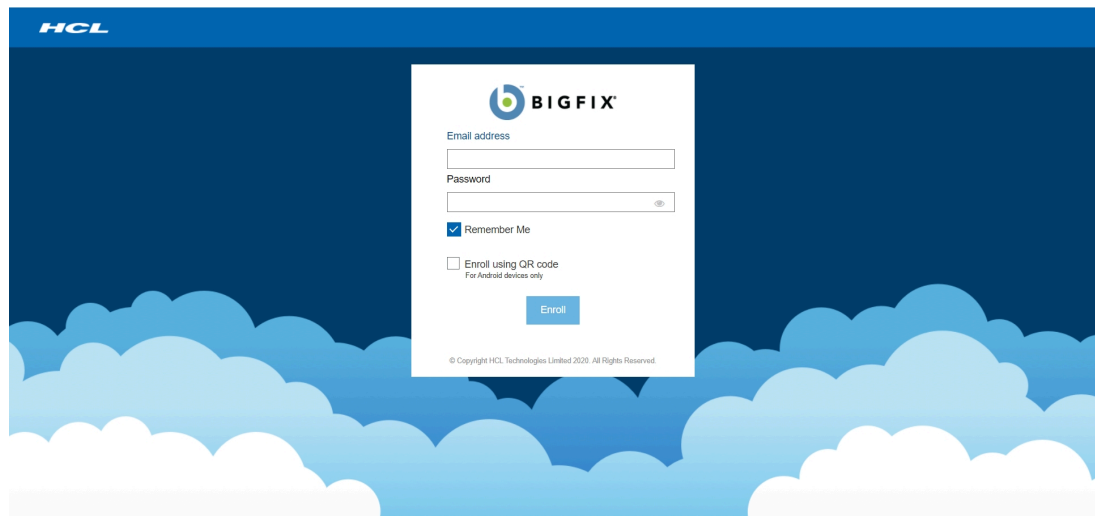
Enrolling through enrollment URL - Windows

Read this section to understand how the users can enroll Windows 10 and Windows 11 devices to MDM when the admin shares the enrollment URL.

- You must know the MDM Server enrollment URL, which the BigFix administrator shares through email or chat. The MDM Server enrollment URL must be the fully qualified domain name of the MDM server (For example, <https://enroll-mdm.bigfix.com>).
- To log in to the enrollment URL, you need an email ID and password associated with a valid Active Directory (AD) credentials (If LDAP Authentication is enabled on the MDM server).
- To enroll a device successfully, the user doing the enrollment on the Windows device must be an administrator of the Windows device.

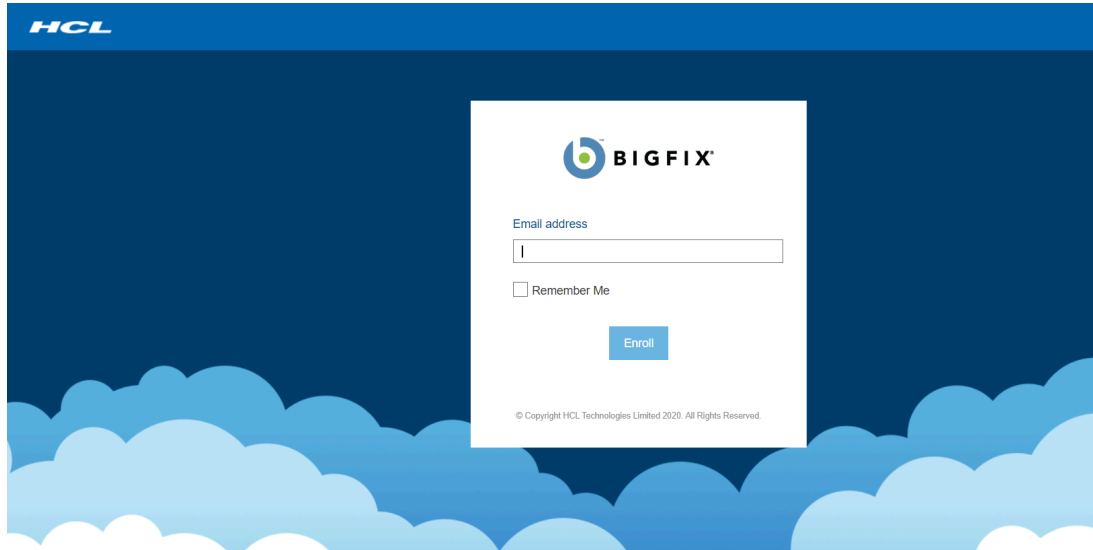
To enroll a Windows device in MDM, complete the following steps:

1. On a Windows device which needs to be enrolled, launch a web browser and go to the MDM server URL.
 - If a `ppkg` package is present on the MDM server and [bulk enroll \(on page 24\)](#) had been configured as TRUE, the following screen appears.



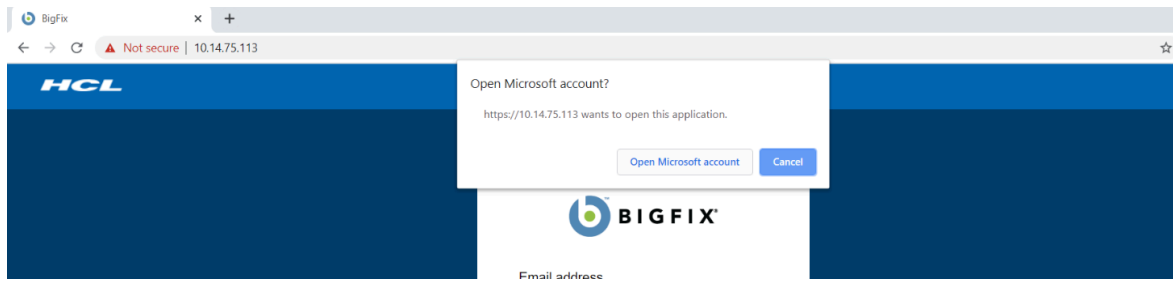
If LDAP Authentication is on, enter an email address and Password that is associated with a valid AD set of credentials and click **Enroll**. If LDAP authentication is off, simply click enroll. A `ppkg` file gets downloaded and the enrollment process begins.

- If the bulk enroll option had been configured as FALSE, the following screen appears.

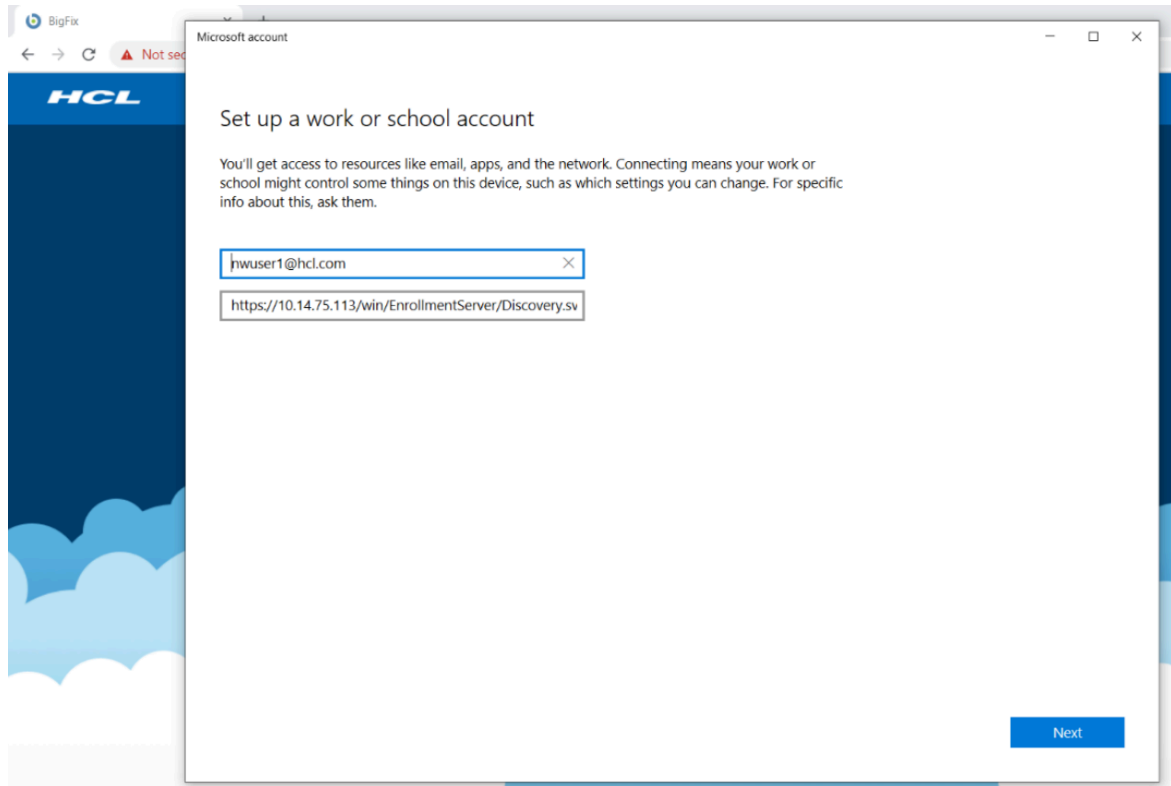


Enter an email address that is associated with a valid AD set of credentials and click **Enroll**. The enrollment process begins.

2. A pop-up window appears requesting you to open the Microsoft account, click **Open Microsoft account**.



3. On the next screen, enter an email address that is associated with a valid AD set of credentials. The MDM enrollment server URL should already be preconfigured and need not be altered.



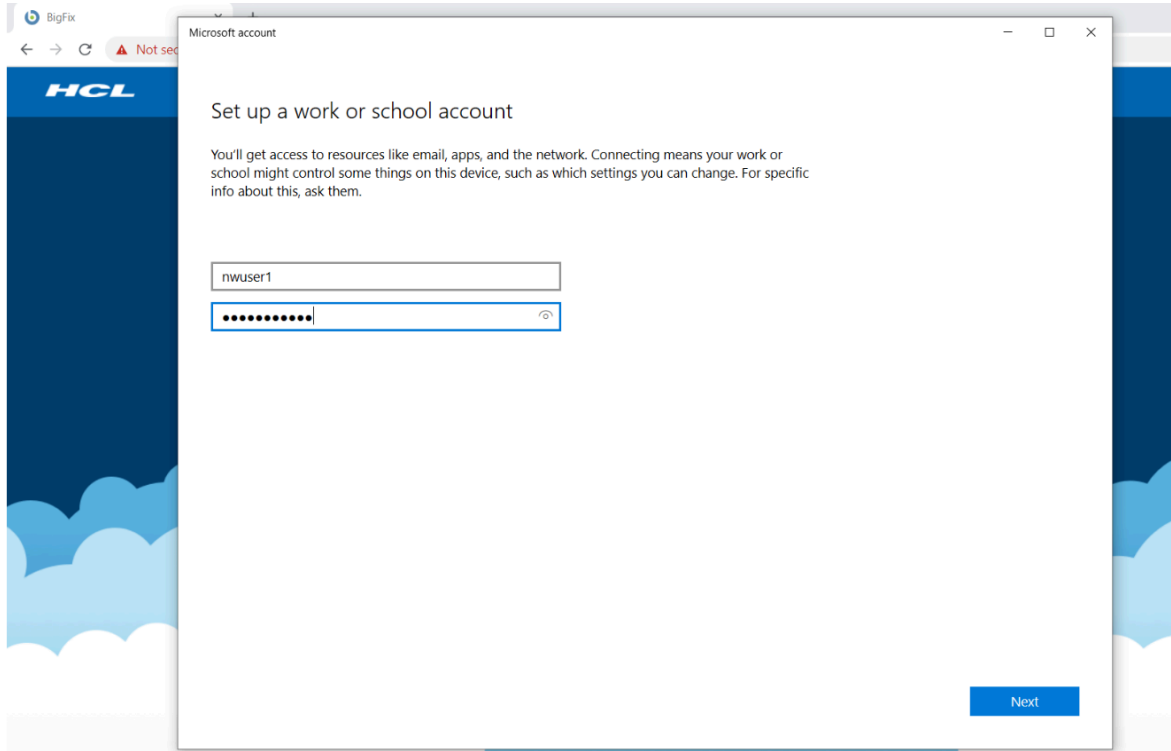
4. Click **Next**.

5. On the next screen, enter the following information:

- User name or email ID – This field is optional and can be empty.
- Password – This field is mandatory.



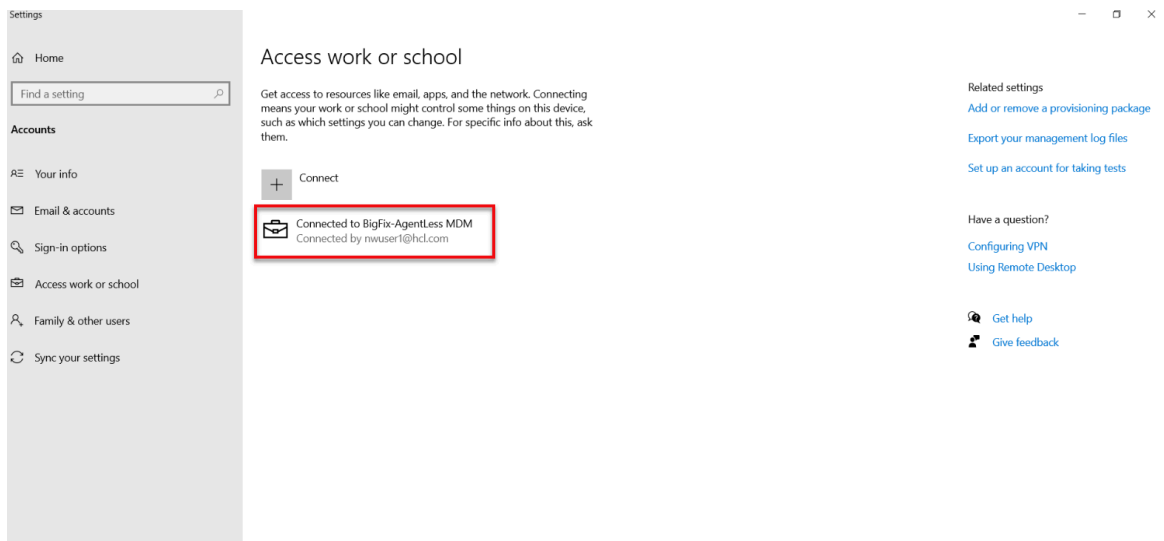
Note: If the LDAP is turned off in MDM environment, enter any value for the device to enroll.



6. Click **Next**.

After successful authentication, the device gets enrolled.

- To verify MDM enrollment status, go to **Settings > Access work or school**. You can view that the device is connected to MDM.



If you have configured ODJ service, the device gets automatically joined to the Active Directory Domain as configured.

Related reference

[Endpoint not disconnected from AD after unenrollment \(on page 158\)](#)

Bulk enrollment - Windows

Bulk enrollment is an efficient way to set up and enroll a huge number of Windows devices to BigFix MCM.

For more information about bulk enrollment of Windows devices, see [Bulk enrollment](#).

The main advantages of bulk enrollment are:

- Large scale enrollment – With this method of enrollment, you can enroll huge numbers of Windows devices efficiently.
- One-time configuration – As an administrator, you just need to configure the Windows provisioning package (.ppkg) once; after that the same configuration can be effortlessly applied to a huge set of devices.



Note: A provisioning package (.ppkg) is a container for a collection of configuration settings. For more information, see [Provisioning packages for Windows](#).

You can also configure default Windows profile that allows users to automatically install BigFix, install custom MSI, and configure a default Windows restrictions policy via Policy Groups.

To learn how to enroll Windows devices in bulk, see [Bulk enrollment - Windows](#).

If you have configured ODJ service, the device gets automatically joined to the Active Directory Domain as configured.

Related reference

[Endpoint not disconnected from AD after unenrollment \(on page 158\)](#)

Autopilot enrollment - Windows

BigFix MCM supports Windows Autopilot enrollment.

What is Windows Autopilot

Windows Autopilot is a collection of technologies that helps set up and pre-configure new or factory reset Windows devices. This solution helps the administrator to enroll and manage devices with little to no infrastructure to manage, with a process that is easy and simple. The only interaction required from the end user is to connect to a network and login with their AD credentials. Everything beyond that is automated. You can also use Windows Autopilot to reset, repurpose, and recover devices.

For more information about Windows Autopilot enrollment, see the Windows official documentation at [Windows Autopilot](#).

How it works

The admin configures the Autopilot settings in Azure Active Directory (Azure AD). The devices configured to be enrolled with Windows Autopilot are automatically enrolled in BigFix MCM on first boot up. Devices can be configured to automatically have a default Windows profile to apply via Policy Groups. The default Windows profile can be configured to automatically install BigFix and other applications of the company's choice, custom MSI, and set a default Windows restrictions policy.

Configuration workflow

The admin needs to sign in to the [Azure portal](#) with an active [Azure AD Premium license](#) and configure MDM server, Autopilot group, deployment profile, devices and assign users to enroll devices through Windows Autopilot. For detailed instructions on how to configure Windows Autopilot settings through Azure AD, see the BigFix Wiki page [Windows Autopilot Configuration Guide](#).

Briefly to configure Autopilot enrollment, complete the following steps:

1. Configure BigFix MCM application in Azure AD.
2. Create Autopilot users and device groups. This enables you to assign devices to a created group and manage the devices by group.
3. Configure default deployment profile. You can configure default deployment profile [through Microsoft Azure AD](#) or through WebUI via Policy Groups. The configured profile is applied by default when a device is enrolled through Autopilot enrollment.
4. Harvest device IDs in a `.csv` file and upload your Configure Autopilot devices and assign users.
5. Configure Windows Autopilot Terms of Service. With this, you can customize the end user agreement screen by adding your company's logo and terms of service.

After the configuration is completed, when the user switches the machine on, connects to the Internet, enters the password for the assigned user, the enrollment process starts.

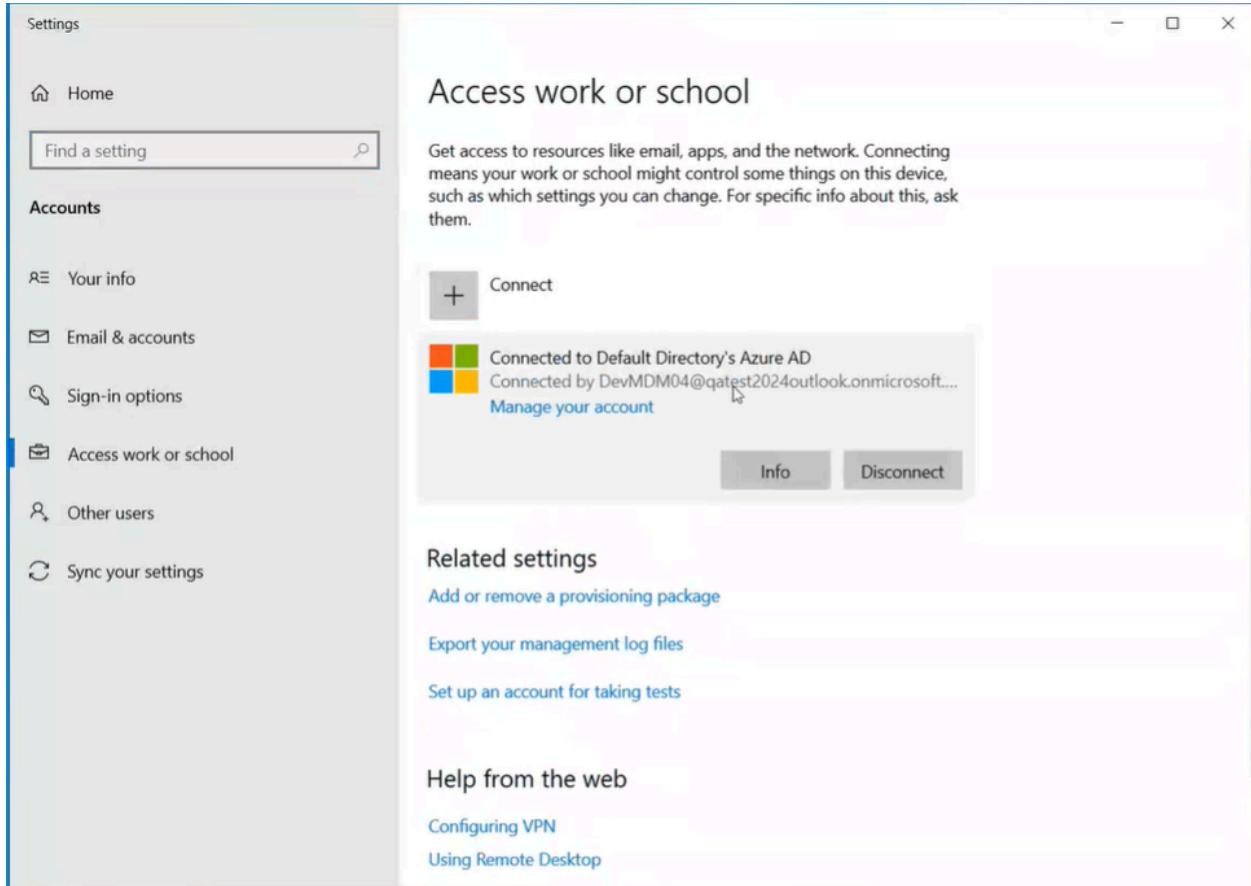
Enrollment process

The Autopilot enrollment process begins on first power up of the device or power up following a factory reset.

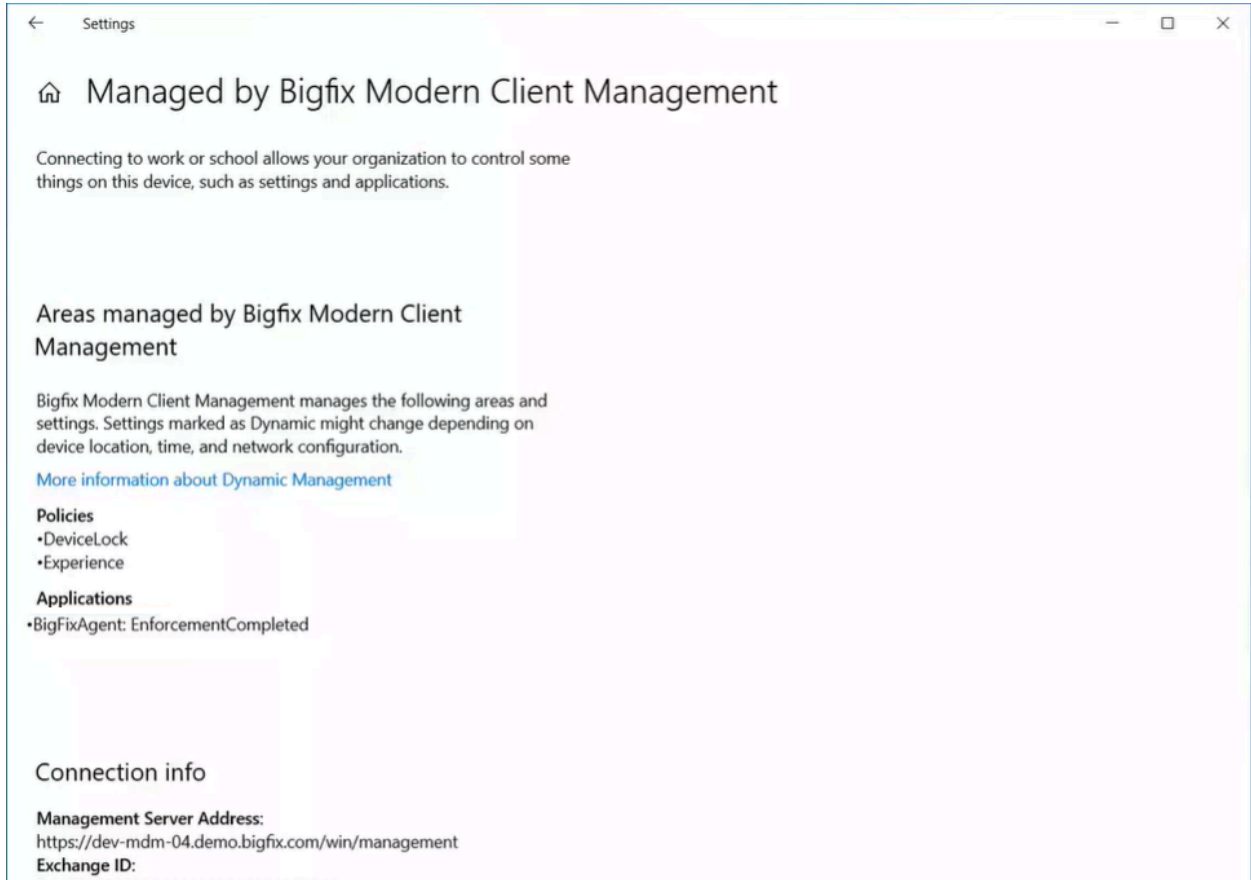
To begin the enrollment process, do the following steps:

1. Open the Windows device that is associated with the MDM server. Connect to internet. Enter the password as set in Azure AD. Update the password.
2. The End User License Agreement page appears. Select the license agreement check box after reading and click **Accept**. Afterwards, the autopilot enrollment process begins.

After the enrollment is completed, go to **Settings > Access work or school** to verify MDM server details.



Click **Info** to verify the policy and application details.



Managing through WebUI

You can manage the enrolled devices through WebUI. In the WebUI device list, you can see the enrollment type is listed as `autopilot_enroll`.

BigFix WebUI - Devices page

4 devices | Reset all filters | View: 20 | 1 of 1 pages

Computer Name	Enrollment Type	Last Report Time	Applicable Patches	Deployments	Device Type	OS	Groups	User Name	IP Address	DN
ZTD	autopilot_enroll	12 minutes ago	0	0	Mobile	Windows 10 E...	MDM Devices,...	<none>		
ZTD-71013634043	autopilot_enroll	an hour ago	0	0	Mobile	Windows 10 E...	MDM Devices,...	<none>		
ZTD-71013634043	autopilot_enroll	2 hours ago	0	0	Mobile	Windows 10 E...	MDM Devices,...	<none>		
ZTD-71013634043	autopilot_enroll	an hour ago	0	0	Mobile	Windows 10 E...	MDM Devices,...	<none>		

In the device document, you can see Enrollment Type as `autopilot_enroll`.

The screenshot displays the BigFix MCM WebUI interface for a device with ID 1618022613. The device is a Windows 10 Enterprise Evaluation (10.0.19042.508) mobile device. The 'Enrollment Type' is 'autopilot_enroll', which is highlighted with a red box. The 'Windows Modern Client Management Analysis' section shows the following details:

Windows Modern Client Management Analysis	
Applications	Microsoft Edge, 84.0.522.69, Microsoft Edge Update, 1.3.133.5
Computer Name	ZTD-71013634043
Deployed Password Policy	False
Deployed Restrictions Policy	False
Enrollment Type	autopilot_enroll
Installed Custom MCM Policies	<Not specified>
Installed Password Policy	<Not specified>
Installed Restrictions Policy	<Not specified>
MAC addresses	00-15-5D-A0-19-02
Operating System	Windows 10 Enterprise Evaluation 10.0.19042.508
Primary Ethernet MAC Address	<Not specified>

To know how to further manage BigFix MCM, see [Manage devices](#)

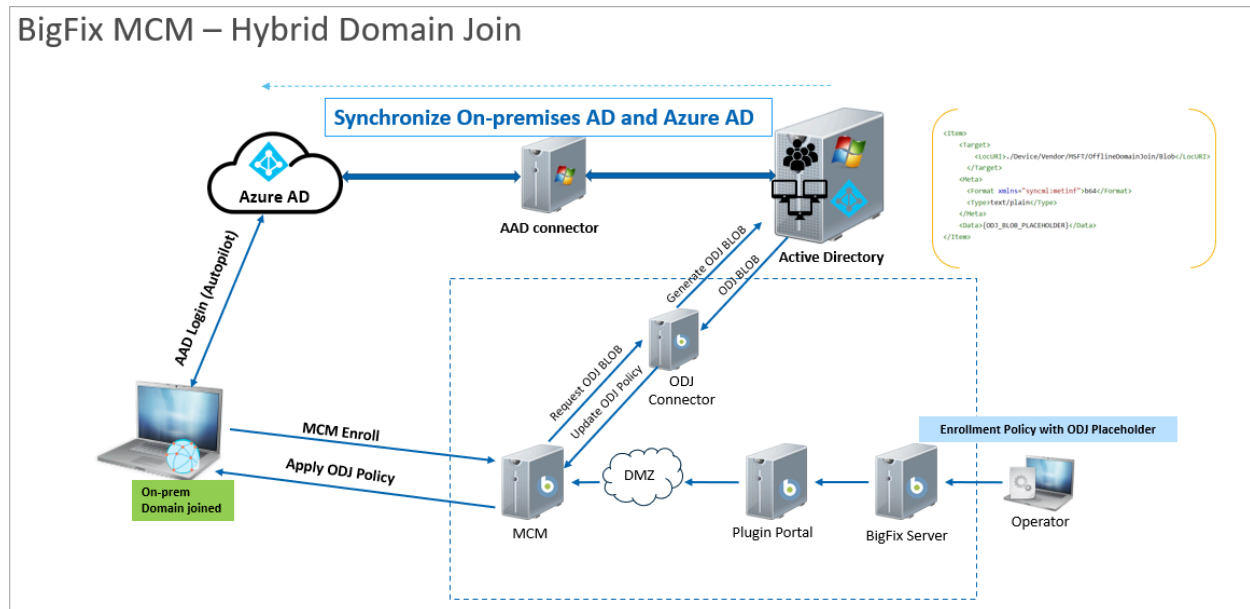
Warning: If you unenroll Autopilot enrolled Windows device, it deletes work or school account and disconnects the AD user from the device. After unenrolling the device, the Admin cannot re-login to the device unless there is a pre-existing local operator account. To learn how to create a custom local operator account, see <https://docs.microsoft.com/en-us/windows/client-management/mdm/accounts-csp>.

Autopilot enrollment with Offline Domain Join service

Read this page to learn the ODJ architecture in MCM and the high-level process flow for enrolling Autopilot enabled Windows devices with ODJ service.

ODJ service is an "Add-on" service and is installed through WebUI after completing the initial MDM server installation. For complete information on installing and configuring ODJ service, refer to [Domain join installation and configuration](#).

Windows Autopilot Hybrid Domain Join Setup Architecture



1. AAD connector establishes a sync between the On premises active directory and the Azure AD.
2. BigFix Operator creates a Domain Join Profile through WebUI to configure it as part of a Windows Policy Group that can be tailored with a specific blob of data that contains everything necessary for a Windows laptop to join to an AD domain, even if there is no direct access to the AD server at the time of enrollment. This profile becomes available in the MCM server.
3. As per the Azure AD autopilot setup, at the time of enrolment, the devices contacts the MCM server for information.
4. MCM server communicates with Azure AD and gets the identification information.
5. The blob in the Domain Join Profile gets updated with the identify information.
6. Plugin Portal contacts On Premises Active Directory and performs DJoin command.
7. The Domain Join Profile is deployed on the enrolling device as per the group policy.

High-level ODJ Autopilot enrollment flow

- Before enrolling, ensure that the windows endpoint is ready for first time use or perform factory reset.
- Sign-in to the windows endpoint device using Azure AD user credentials, synchronized from on-premises AD.
- Wait for the domain join to complete and for the device to automatically restart; it takes several minutes.
- After successful domain join, use on-premises AD credentials to sign-in to the device.
- After successful sign-in:
 - The device joins to the on-premises AD domain, connected to on-premises MDM
 - The Azure work account is automatically provisioned.
 - The device is listed in Azure portal as Hybrid Azure AD joined.

Related reference

[Endpoint not disconnected from AD after unenrollment \(on page 158\)](#)

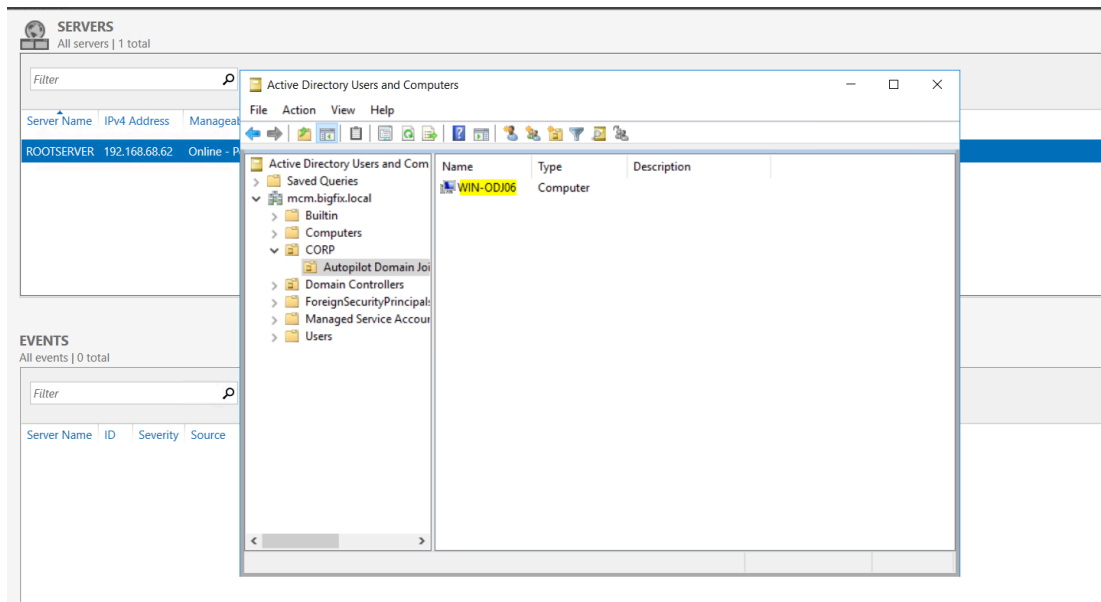
Hybrid AD join verification

After a successful autopilot enrollment with Hybrid Azure AD join, verify the following:

You can ensure if an enrolled Windows endpoint is Hybrid Azure AD joined by verifying the following:

Active Directory

Log in to the Active Directory as an Admin user, navigate to **Active Directory Users and Computers** > **Autopilot Domain Join** and verify if the enrolled computer name is listed under the specified organization unit.



Azure AD

Log in to Azure AD as an Admin user and verify if the **Join Type** of the device is "Hybrid Azure AD joined".

[Home](#) > [HCLSW_AZR_BIGFIXMCM](#) | [Devices](#) > [Devices](#) | [Overview](#) >

All devices (Preview) ...

✓ Enable ⏸ Disable 🗑 Delete ⚙ Manage ⬇ Download devices ↻ Refresh 📄 Columns 📄 Preview features 🗨 Got feedback?

Want to switch back to the legacy devices list experience? [Click here](#) to turn off the preview and refresh your browser. You may need to toggle it on and off once more.

🔍 Search by name or device ID or object ID [Add filter](#)

37 devices found

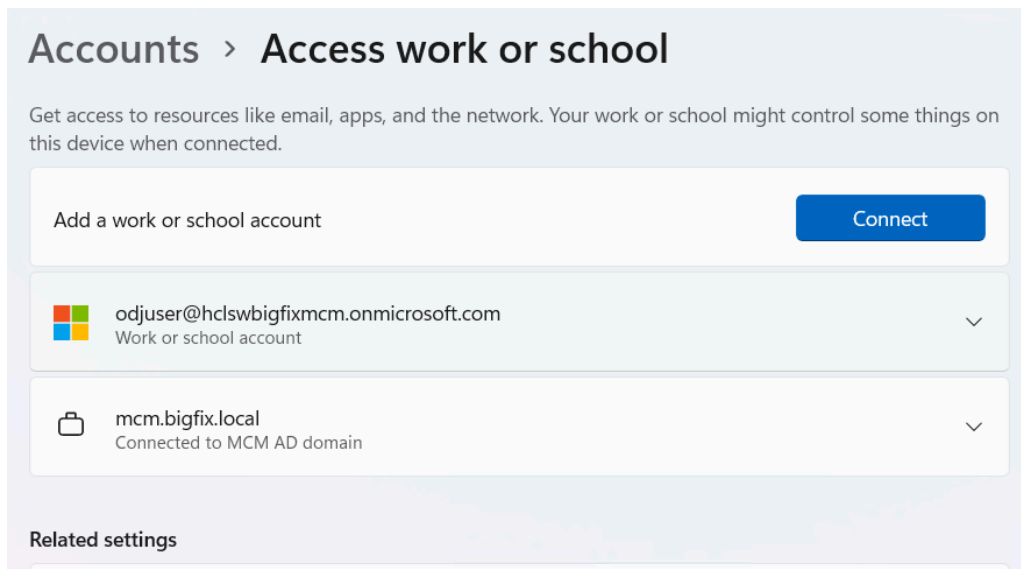
<input type="checkbox"/>	Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant	Registered	Activity
<input type="checkbox"/>	win-odj06	Yes	Windows	10.0.22621.1105	Hybrid Azure AD joined	None	None	N/A	3/2/2023, 1:37 PM	3/2/2023, 1:37 PM
<input type="checkbox"/>	KIOSK-PFZALONC	Yes	Windows	10.0.22621.1265	Azure AD joined	None	Microsoft Intune	Yes	3/2/2023, 2:29 PM	3/2/2023, 12:54 PM

**Note:**

- The domain joined device is synchronized to Azure AD portal only after successful login using on-premises domain credentials.
- Azure AD connect synchronizes the on-premises object with Azure AD in every 30 minutes.
- Therefore, wait for a maximum of 30 minutes for the device to get listed in the Azure AD portal.

Windows endpoint

- Ensure if dual account is provisioned at the endpoint.



Note: If Azure Primary refresh token is not successfully updated, SSO connect is not established, and so, the Azure AD account does not get provisioned. As a workaround, device user can manually sign-in with Azure AD credentials to provision the account by clicking the MDM **Sync** option under the domain account. This action must be performed only after the device is listed as 'Hybrid Azure AD joined' under Azure AD portal.

- Ensure if the On-premises MDM synchronization is successful.

... > **Managed by Bigfix Modern Client Management**

Connecting to work or school allows your organization to control some things on this device, such as settings and applications.

Areas managed by Bigfix Modern Client Management

Bigfix Modern Client Management manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.

[More information about Dynamic Management](#)

Connection info

Management Server Address:
 https://enroll-demo1.hclbigfix.com/win/management
Exchange ID:
 0B8A09124B467D9CB281EC3758F07025

Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.

Last Attempted Sync:
 The sync was successful
 02-03-2023 15:06:33

- Ensure the device registration status reflects "YES" for both **AzureAdJoined** and **DomainJoined**.

```
C:\Users\odjuser>dsregcmd /status

+-----+
| Device State |
+-----+

AzureAdJoined : YES
EnterpriseJoined : NO
DomainJoined : YES
DomainName : MCM
Virtual Desktop : NOT SET
Device Name : win-odj06.mcm.bigfix.local
```


- Under the SSO state section, Device registration status must reflect **AzureAdPrt** as 'YES' .

```

SSO State
-----
AzureAdPrt : YES
AzureAdPrtUpdateTime : 2023-03-02 15:52:01.000 UTC
AzureAdPrtExpiryTime : 2023-03-16 15:52:21.000 UTC
AzureAdPrtAuthority : https://login.microsoftonline.com/f01e1f4a-b635-49c2-9de3-8305b85f8a5c
EnterprisePrt : NO
EnterprisePrtAuthority :
OnPremTgt : NO
CloudTgt : YES
KerberosLevelNames : .windows.net, .windows.net:1433, .windows.net:3342, .azure.net, .azure.net:1433, .azure.net:3342

```

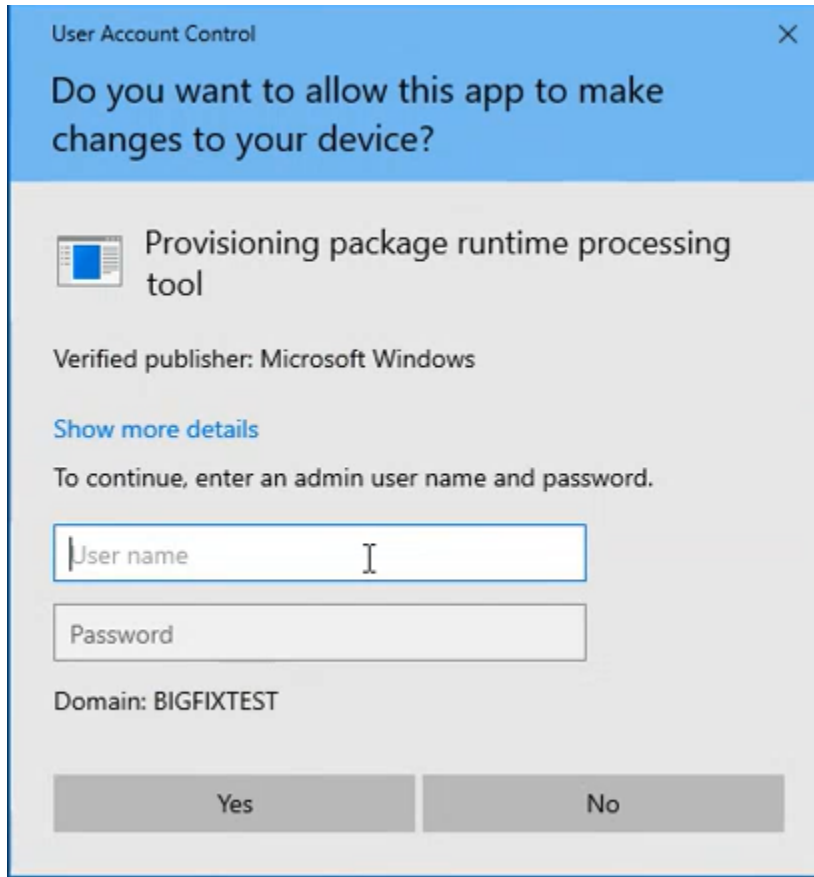
For further reference to verify if a Windows endpoint is dual joined, see <https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-hybrid-join-verify>.

Enrollment by non-admin device users

BigFix MCM facilitates non-admin device users to enroll the domain-joined devices to MDM and manage them.

Following are some of the options to enable non-admin device users to perform enrollment to MDM server and manage the domain-joined devices after the enrollment.

- User-initiated enrollment with one-time admin password: In this method, the non-admin device user logs in via enrollment URL through which a .ppkg is downloaded. The device users need to be provided with one-time admin password to run the .ppkg file to initiate enrolment. After enrollment, the Admin can reset the password.



- [Grant and Revoke admin rights through Domain Controller \(on page 34\)](#): In this method, the domain users are granted with admin rights through Domain Controller, the users get admin rights and perform user-initiated enrollment by downloading .ppkg file, after which the Admin rights can be revoked from the Domain Controller.
- [Automatic enrollment of Hybrid Azure AD joined devices using Group Policy Object \(on page 39\)](#): In this method, a group policy is configured so that the Hybrid AD joined devices get enrolled to MDM server automatically without admin rights.
- [Autopilot non-admin enrollment \(on page 24\)](#): In this method, the only interaction required from the device user is to connect to a network and to verify credentials. Everything beyond that is automated.

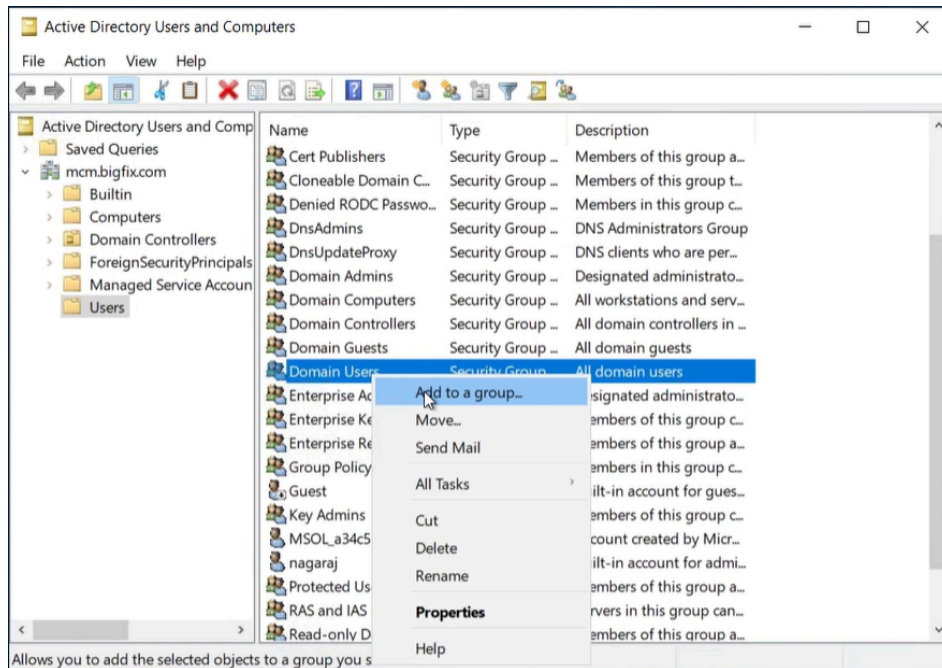
Grant and Revoke admin rights through Domain Controller

Admin can provide one-time admin access to multiple domain-joined devices from the Domain controller. With the admin rights, devices can be enrolled over-the-air via `.ppkg` file. Once the devices are enrolled, domain Admin can revoke the device user's admin access and trigger a [restart](#) for all the devices from MDM.

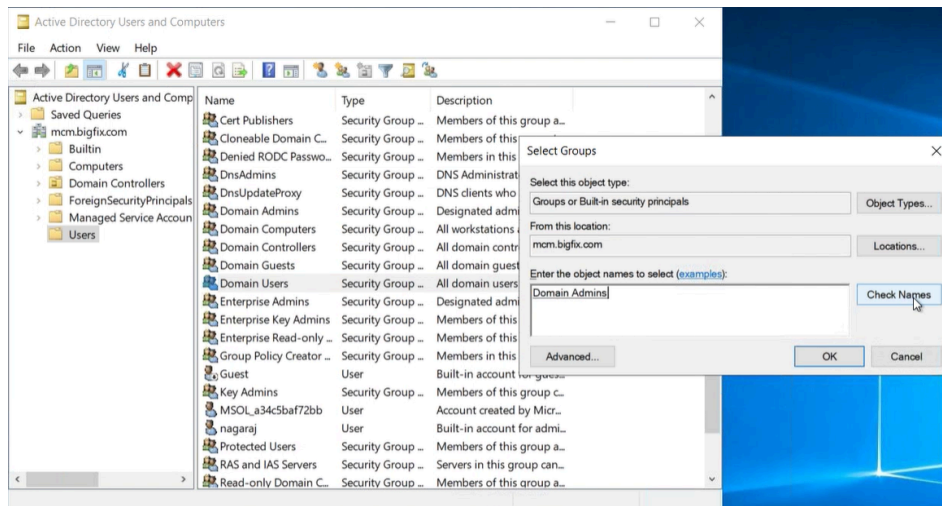
A. Grant Admin rights to the device users from Domain Controller

1. Log in to Domain controller as a Domain Administrator.
2. From the start menu go to **Windows Administrative Tools > Active Directory Users and Computers**.
3. To grant Admin permissions to non-admin users:

- a. Navigate to **Users**, select **Domain Users**, right click and select **Add to a group...**

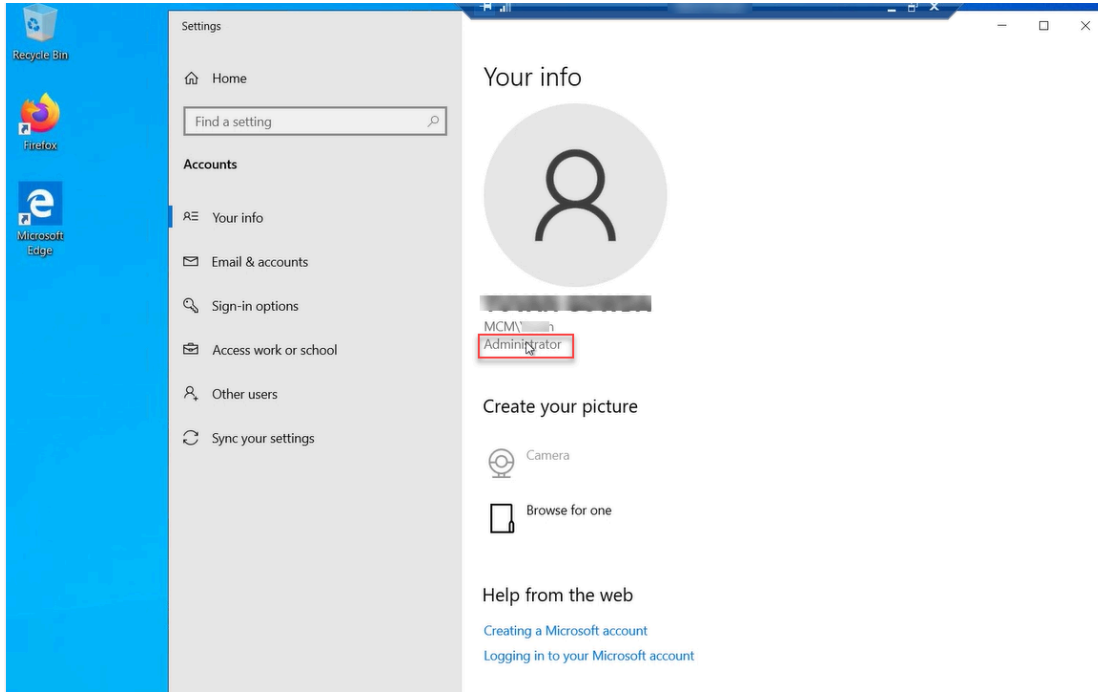


- b. In the Select Groups popup, in the **Enter the object names to select** text box, enter **Domain Admins**.



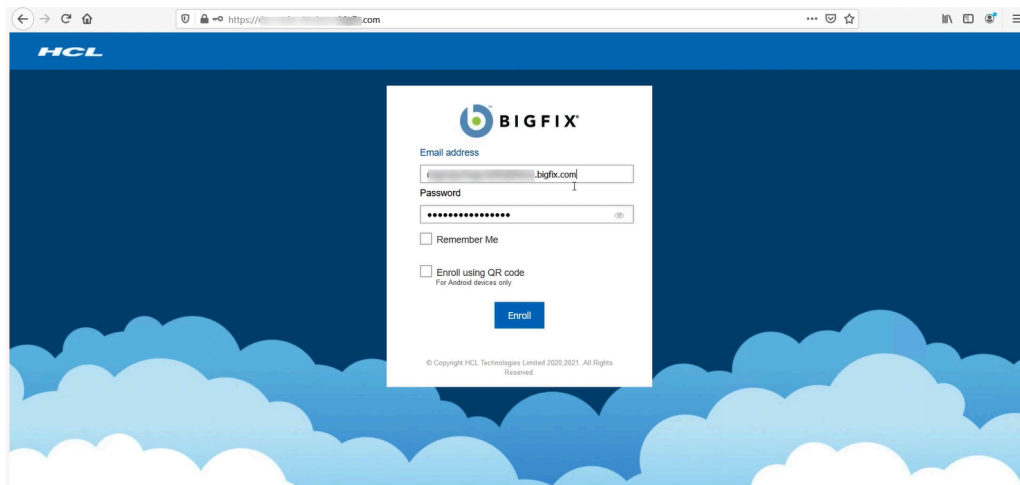
- c. Click **Check Names** to verify and click **OK**.

Now, all the users under Domain Users group get Admin rights. For the changes to take effect, [restart](#) the user's device. From the user's device, you can verify if the user got Admin right by navigating to **Access Work or School > Your Info**.

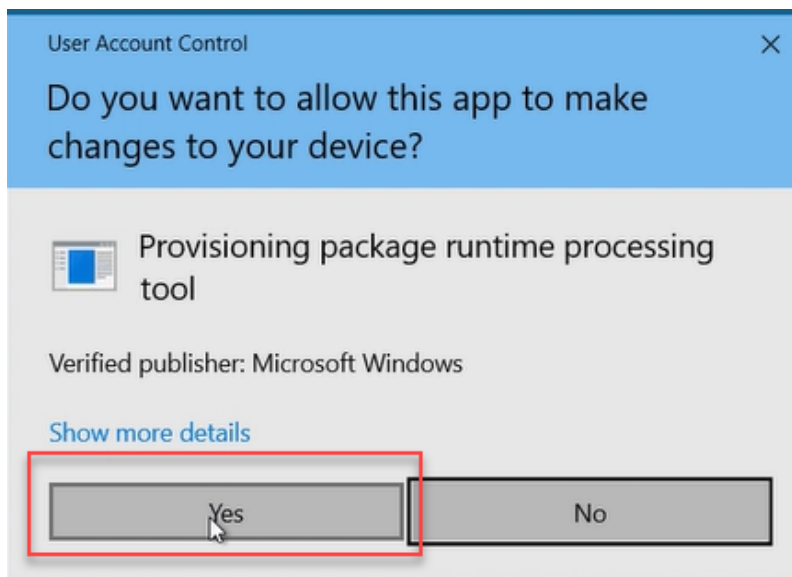
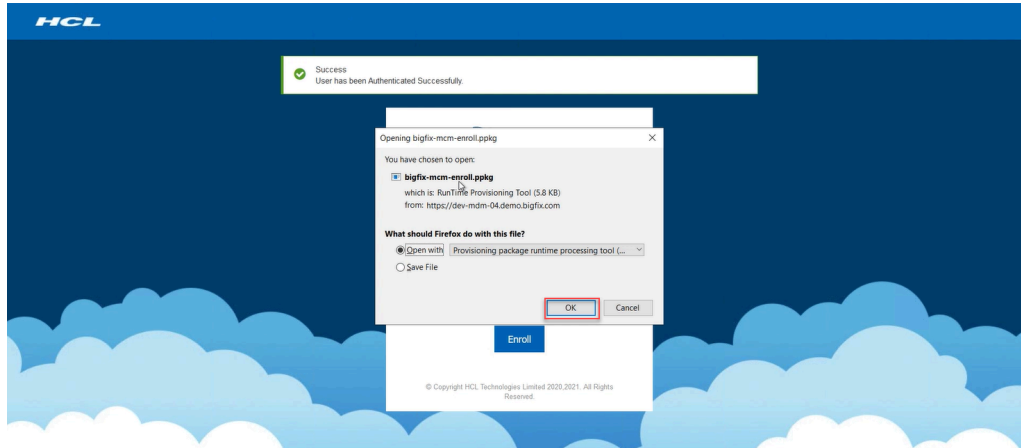


B. Perform user-initiated enrollment

1. Open Firefox or any other supported browser, and in the address bar, enter enrollment URL. For example, *https://mdmserver.demo.com*.
2. Enter valid AD credentials to authenticate.



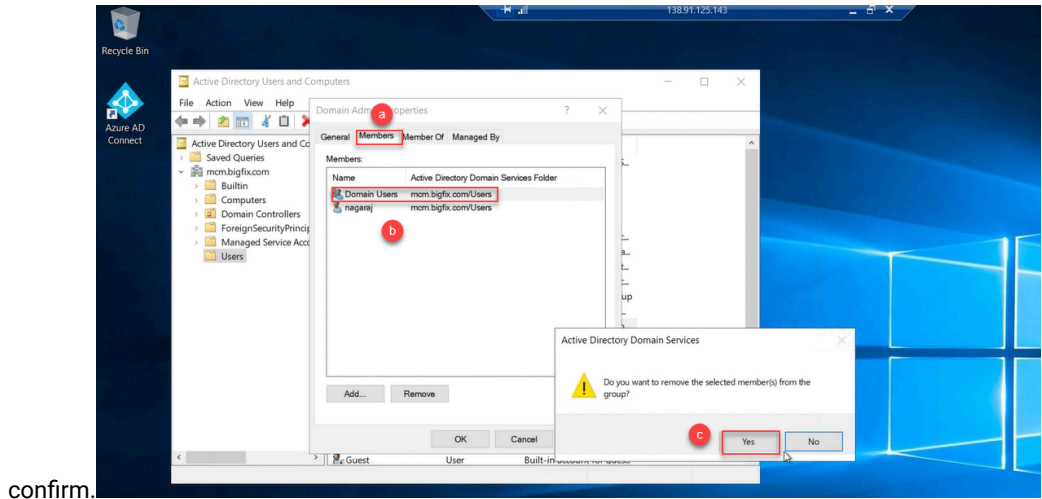
3. Once the authentication is successful, the user can download .ppkg file by clicking **OK > Yes > Yes**, add it in the subsequent screens.



C. Revoke Admin rights of the user from the Domain Controller

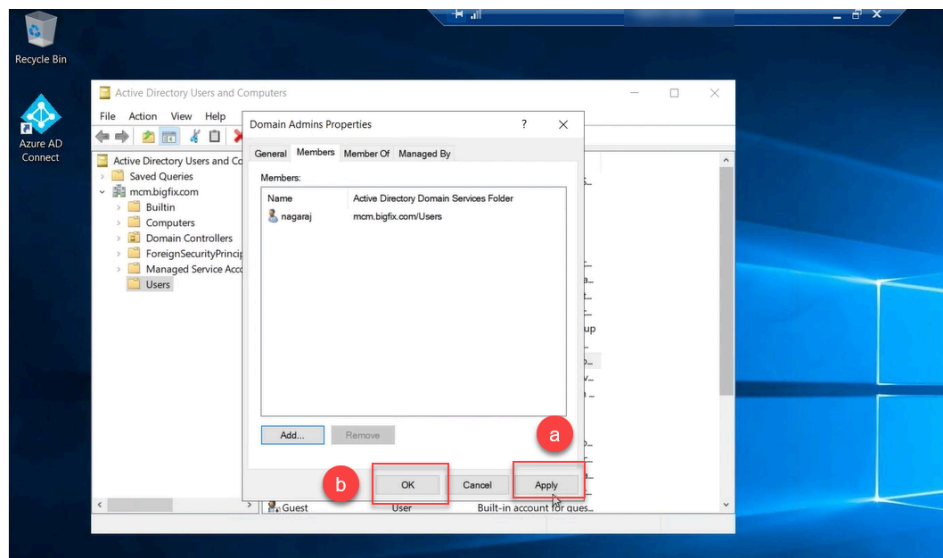
1. Log in to Domain controller as a Domain Administrator
2. From the start menu go to **Windows Administrative Tools > Active Directory Users and Computers**.
3. To revoke Admin permissions from the domain user:

- a. Navigate to **Users**, double click **Domain Admins**.
- b. Go to **Members** tab, select **Domain Users**, click **Remove**, and click **Yes** to



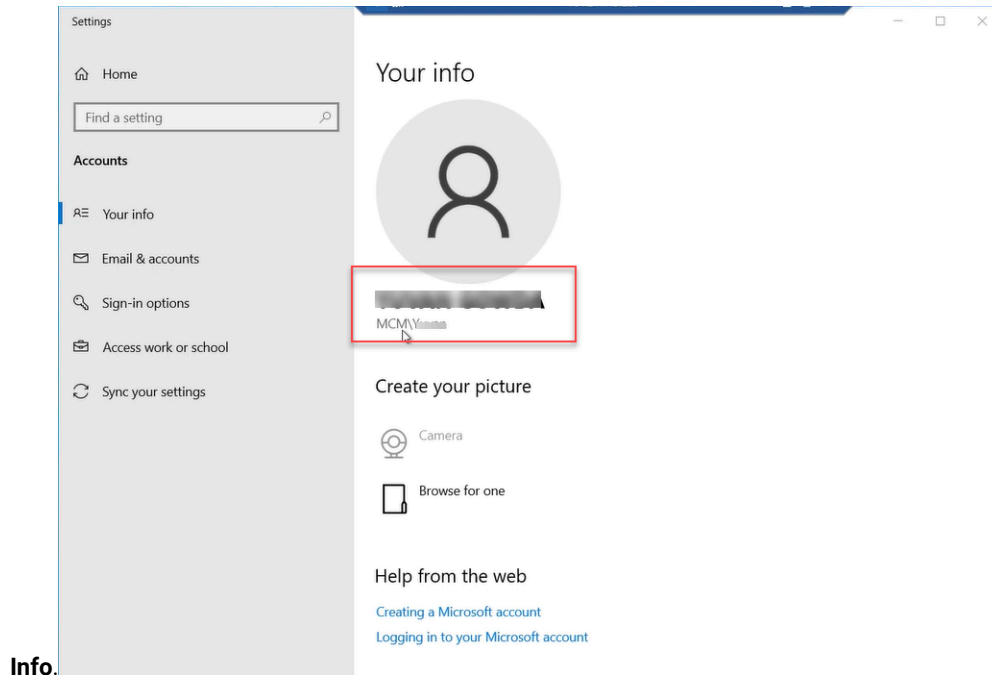
confirm.

- c. Click **Apply** > **OK**.



Now, Admin rights are revoked from all the users under Domain Users group. For the changes to take effect, **restart** the user's device from MDM. From the user's device, you

can verify if the user got Admin right by navigating to **Access Work or School > Your**



Info.

Now, the user can manage the device through MDM without Admin rights. Work or school account will still be present, for non-admin user. However, only Admin can unenroll the device from MDM.

Automatic enrollment of Hybrid Azure AD joined devices using Group Policy Object

You can configure to automatically mass-enroll a large number of Hybrid Azure AD joined corporate devices into BigFix MCM without any user intervention or Admin user credentials. The enrollment into MDM is triggered by a group policy created on the local Active Directory.

What is Hybrid Azure AD join

Hybrid Azure AD joined device means that it is visible in both your on-premises AD and in Azure AD. After adding the devices to Domain Controller (On-premises AD), when you integrate On-premises AD with Azure AD, the devices become Hybrid Azure AD joined devices. Azure AD joined devices automatically get enrolled to BigFix MCM, when Azure AD is configured. This way, you can apply group policies to multiple devices and enroll to BigFix MCM with non-admin user credentials. For more information, see <https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid>

How to configure

To configure, complete the following steps:

1. Integrate On-premises AD with Azure AD.



Note: You can integrate through the Azure AD Connect, after which all the objects are synchronized to Azure AD from on-premises AD.

2. Define group policies in the domain controller.
3. Assign a group policy to Hybrid AD joined devices.

Once the Hybrid AD joined device is assigned to a group policy, the device automatically gets enrolled to BigFix MCM service.

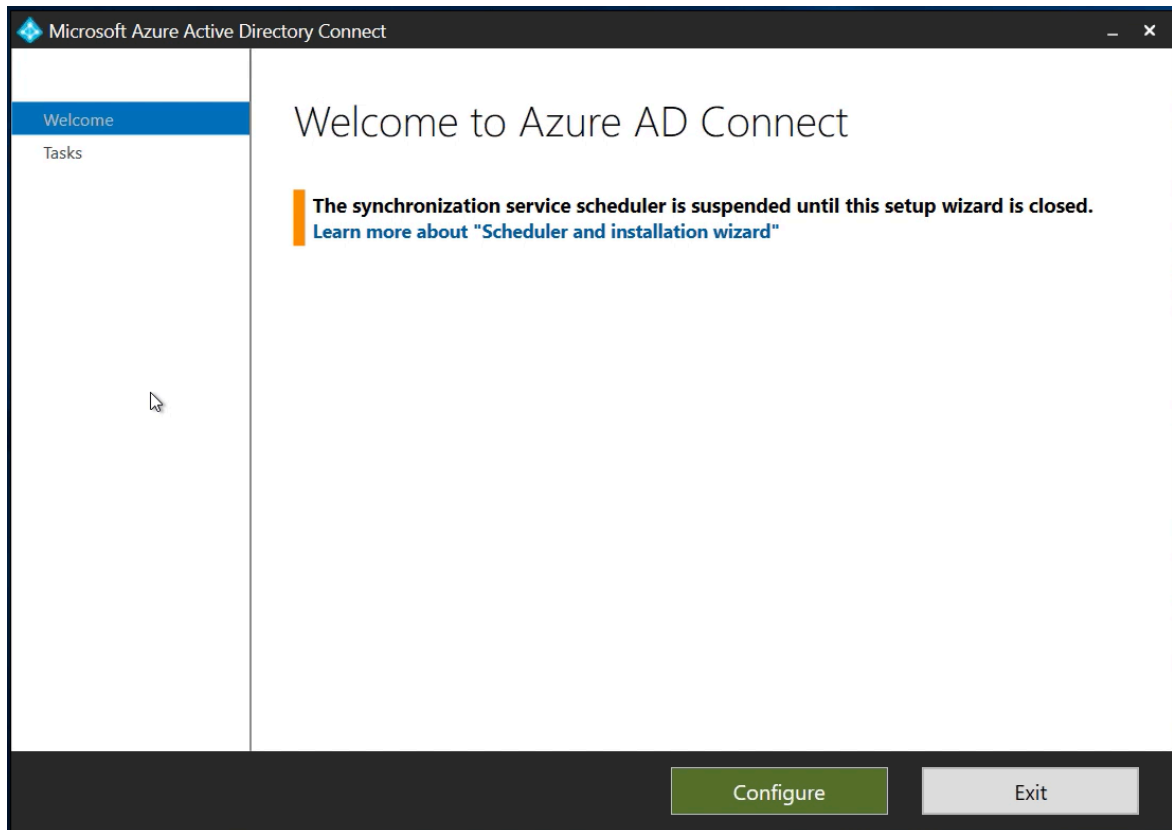
Requirements

- [Domain controller](#) or On-premises AD with users and devices configured
- Azure AD with BigFix MCM application configured
- Administrator privileges on both on-premises and Azure AD

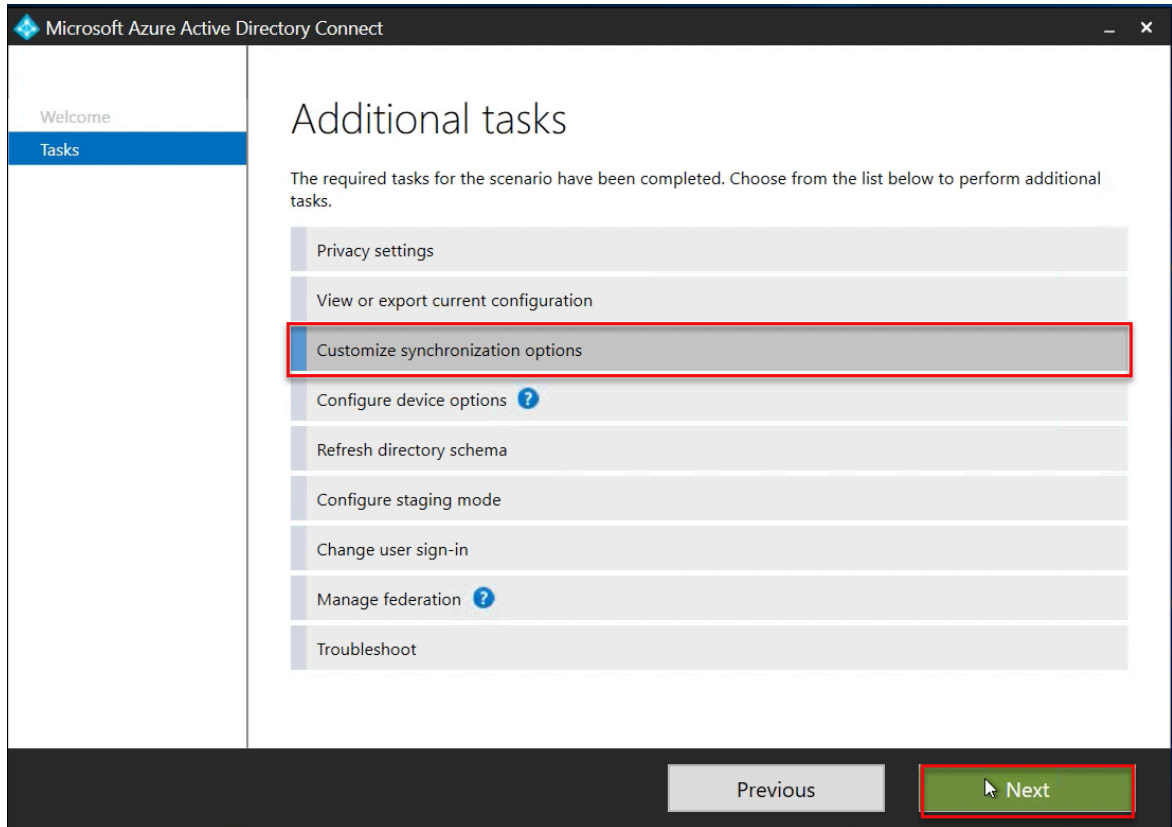
Procedure

Integrate On-premises AD with Azure AD

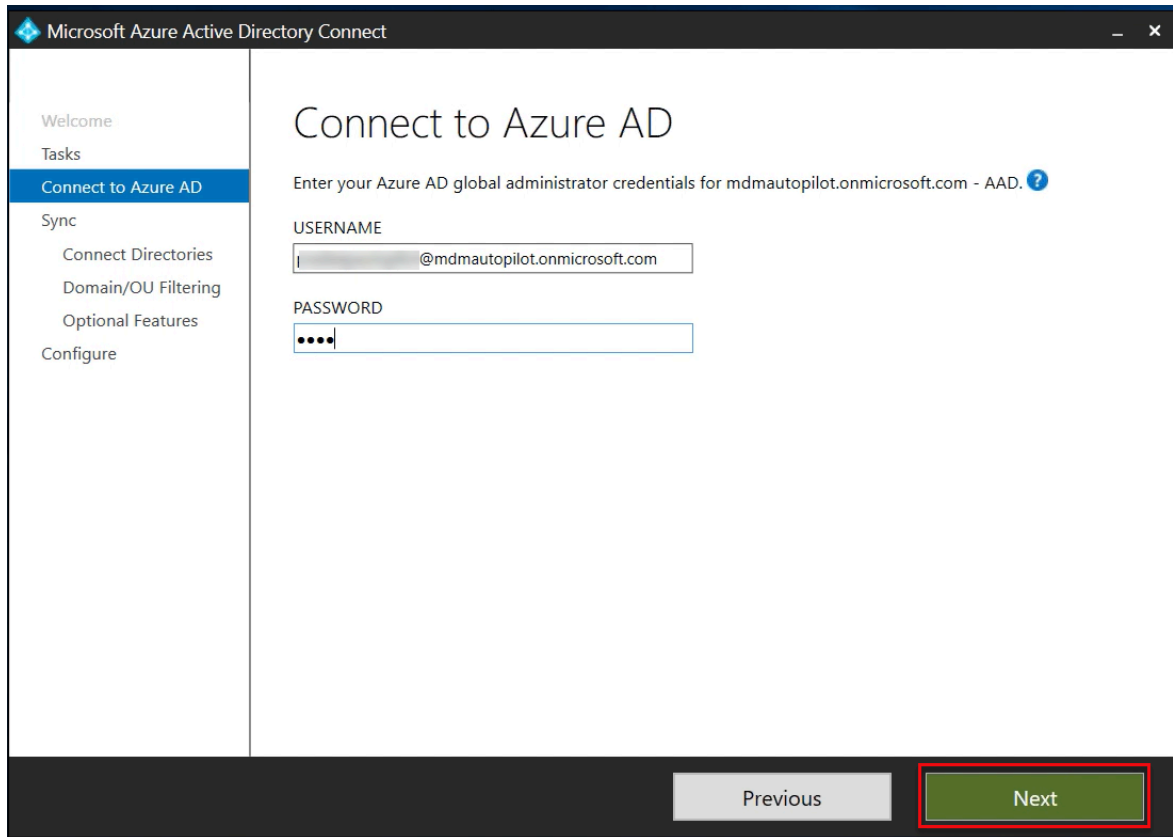
1. [Download Azure AD Connect](#), open Azure AD Connect, and click **Configure**.



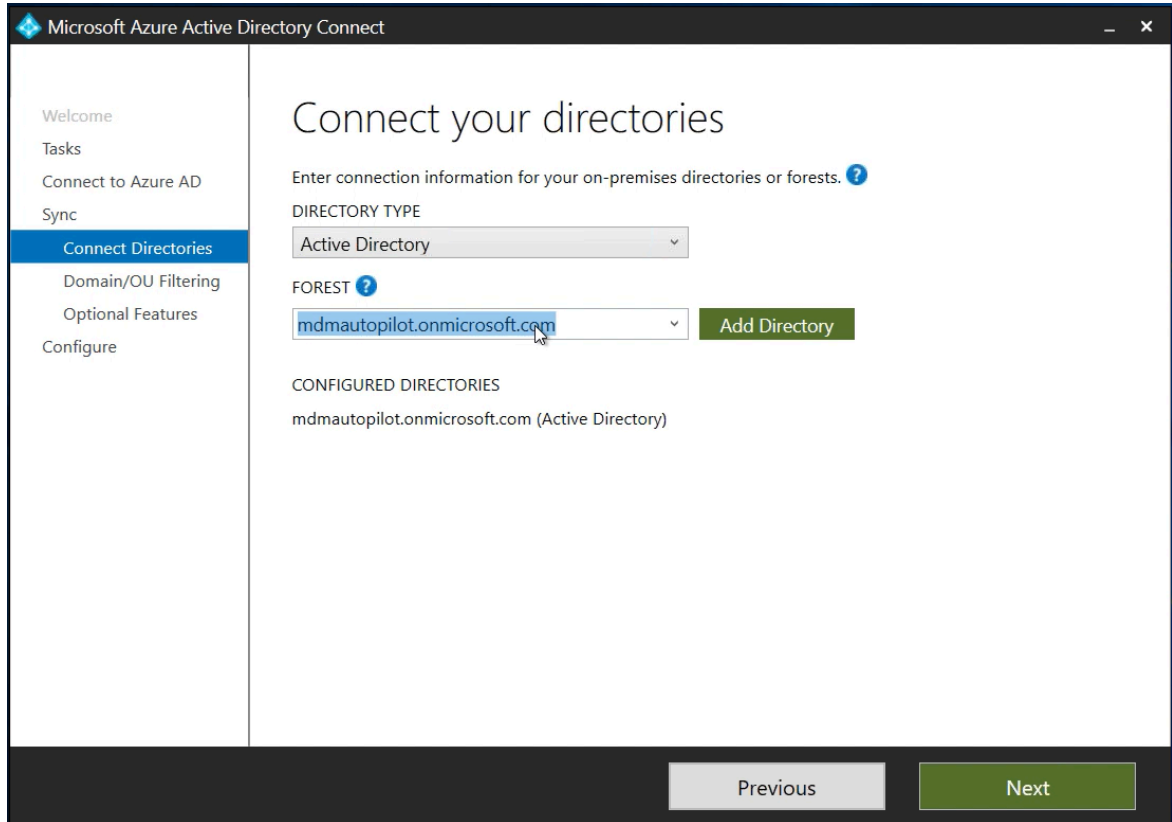
2. Select **Customize synchronization options** and click **Next**.



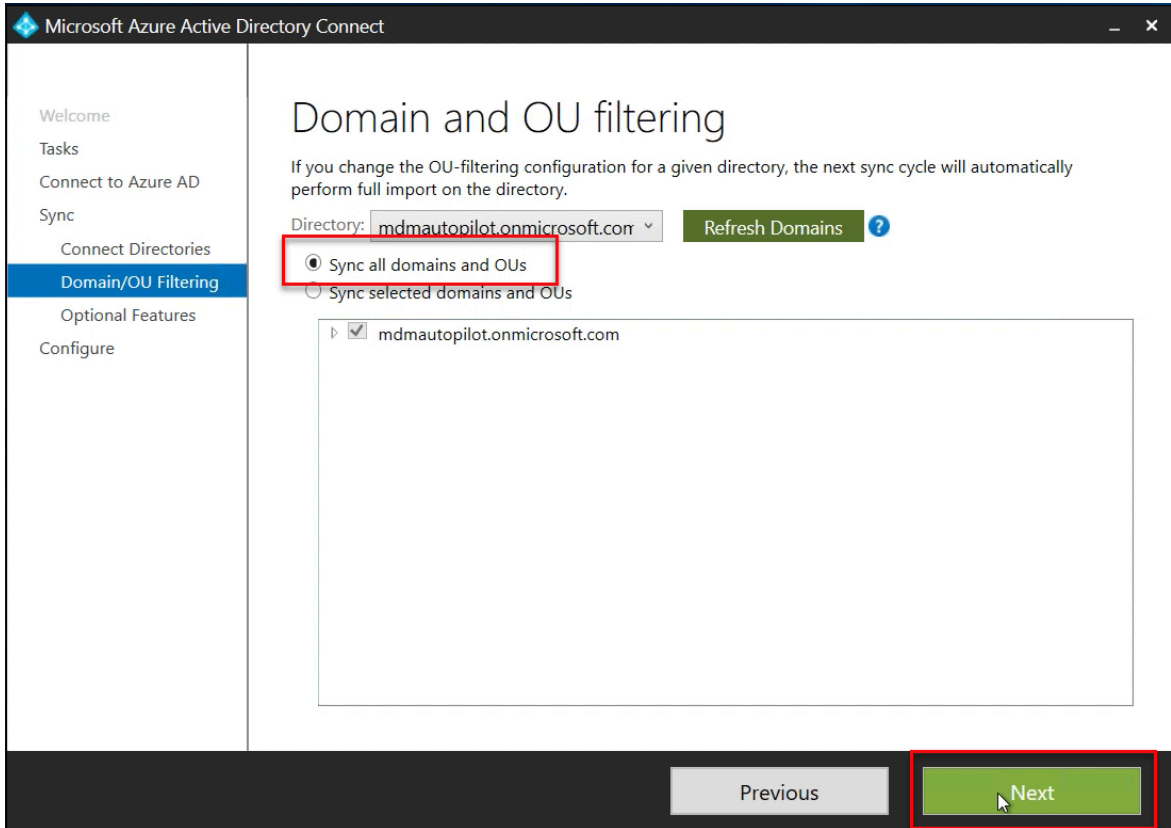
3. Enter Azure AD Global Administrator credentials and click **Next**. The credentials are verified and connected to Azure AD.



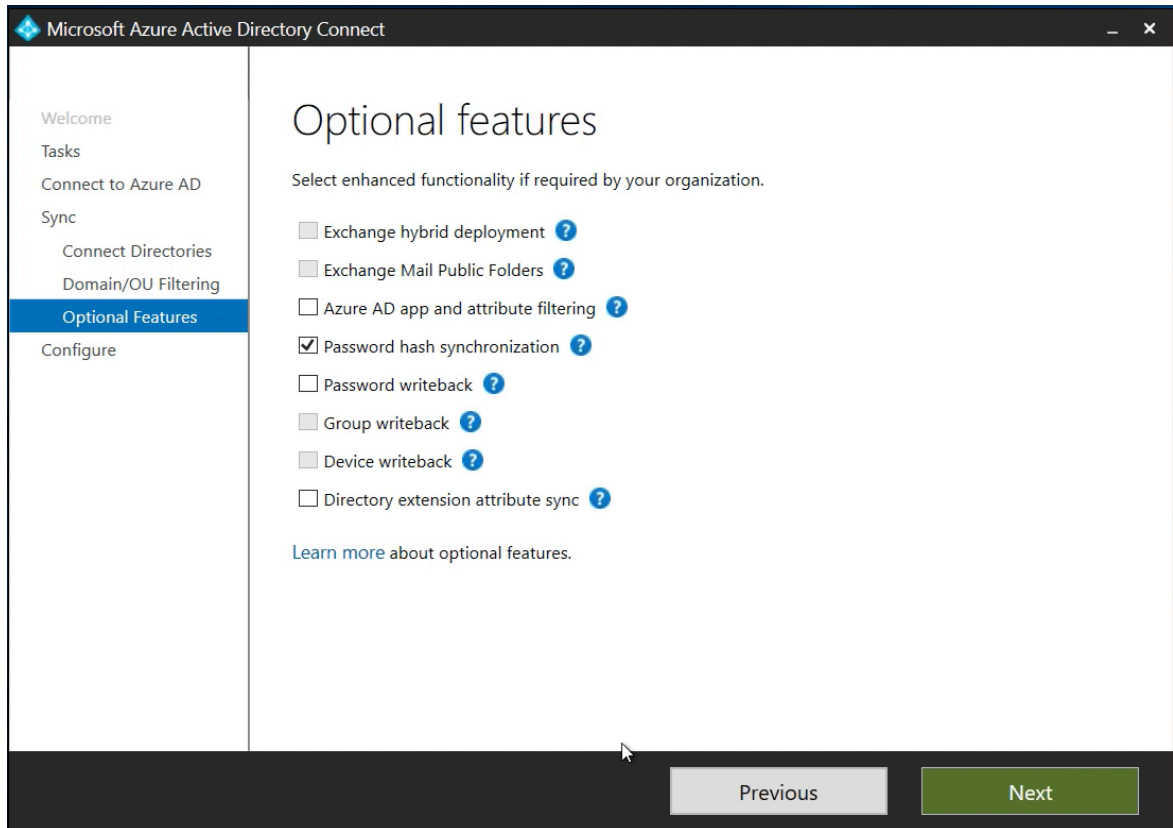
4. After the Azure AD is connected, enter Enterprise Admin credentials to connect to on-premises AD. When the Connect your directories screen appears, enter connection information of the on-premises directories and click **Add Directory**.



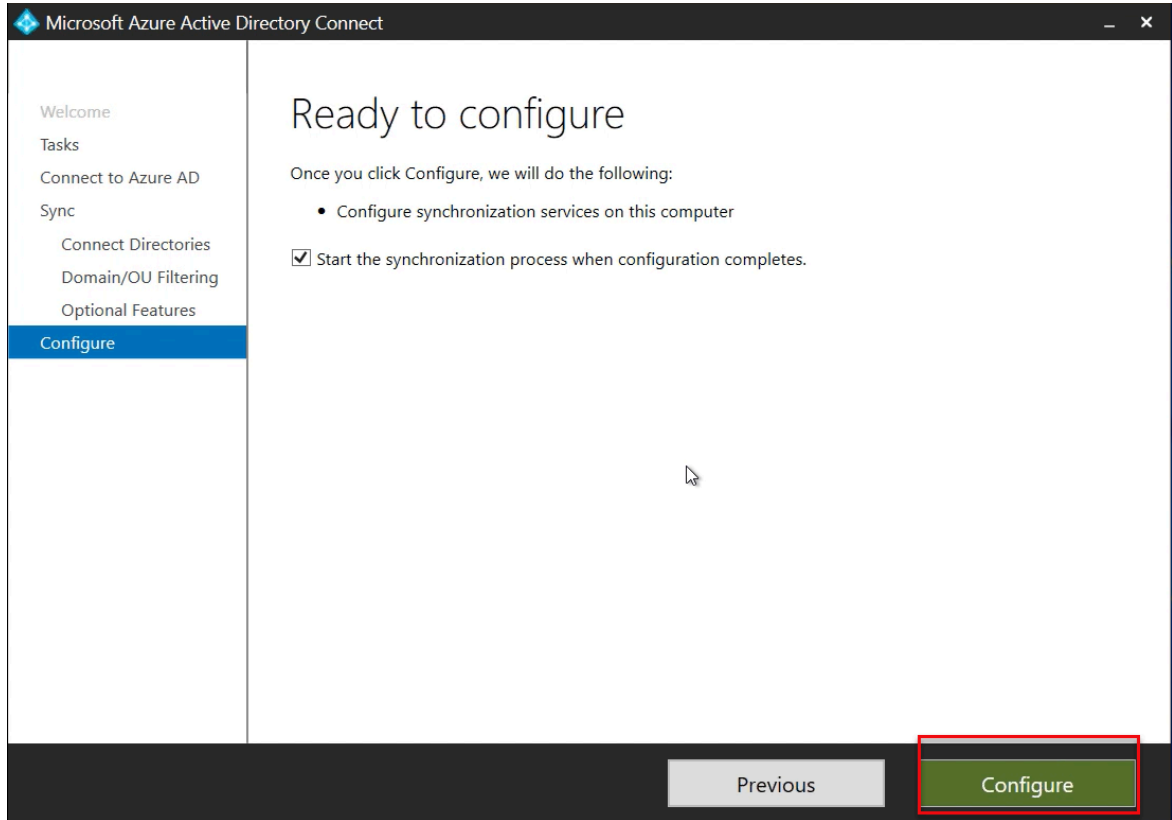
5. After the directory is listed under CONFIGURED DIRECTORIES, click **Next**.
6. On the next screen, select **Sync all domains and OUs** options and click **Next**.



7. In the next screen, ensure the required optional features are selected and click **Next**.



8. On the next screen, click **Configure**.



Once the synchronization is completed, all the users, devices in the on-premises AD appears in Azure AD as well.

After integration

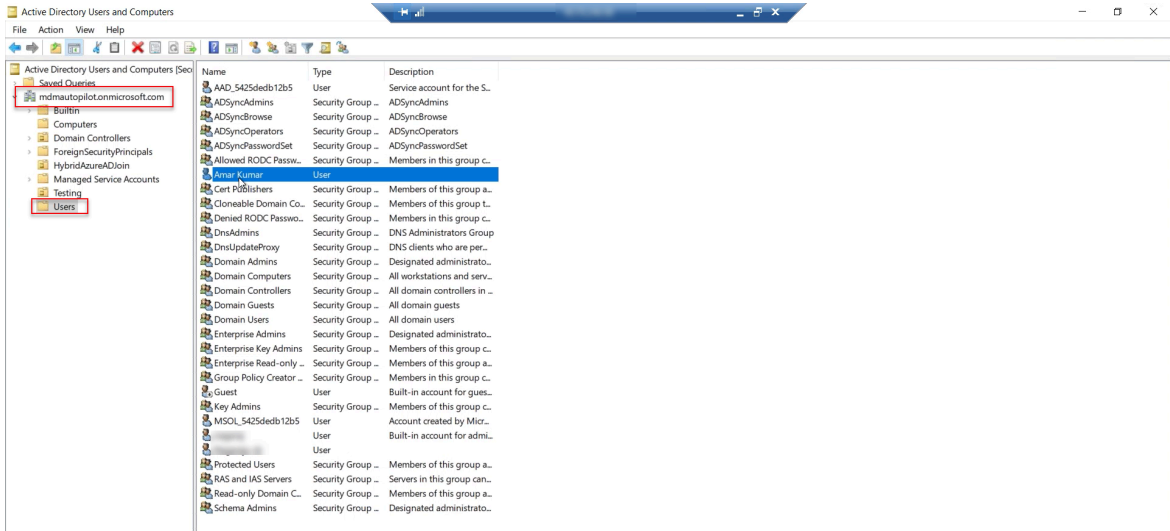
All the users, computers are synchronized. You can see "Yes" under Directory synced column in Azure AD.



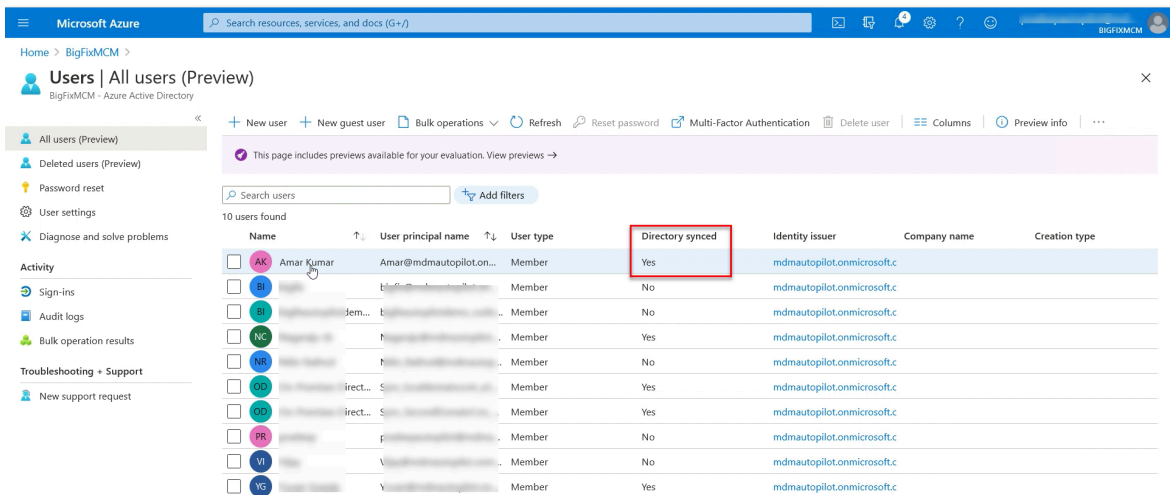
Note: The screenshots were captured at the time of creating this document. For latest UI, refer to the official documentation at <https://docs.microsoft.com/en-us/mem/autopilot/> as the Azure UI gets updated with Microsoft releases.

- Users synchronized

On-premises AD

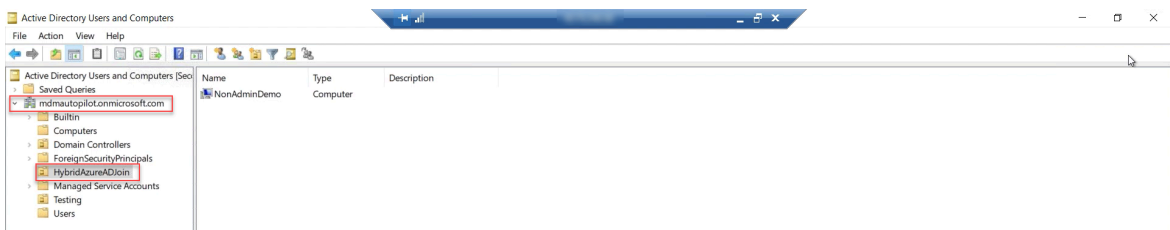


Azure AD

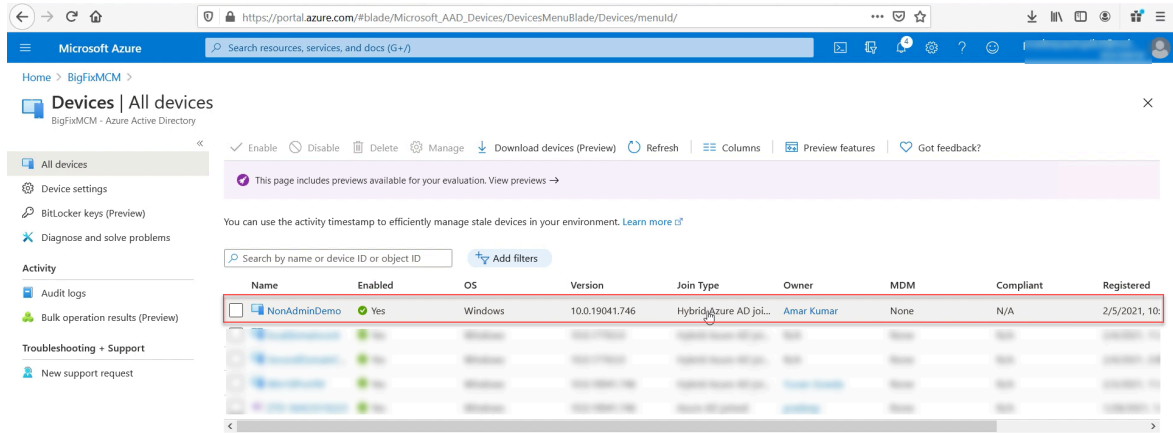


- Devices Synchronized and become Hybrid AD joined devices

On-premises AD

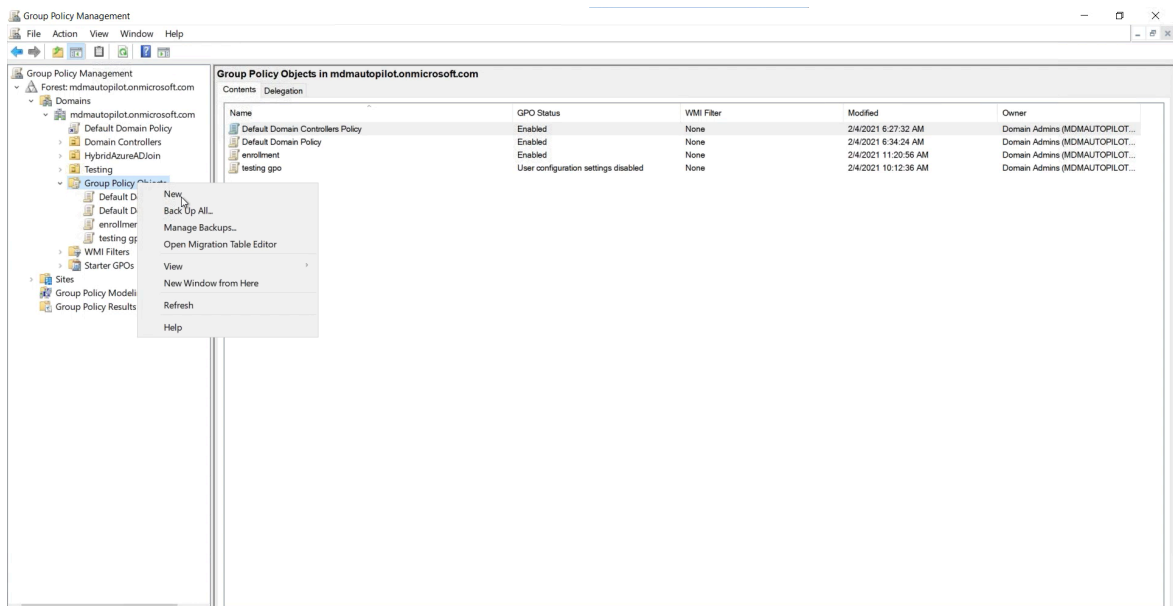


Azure AD



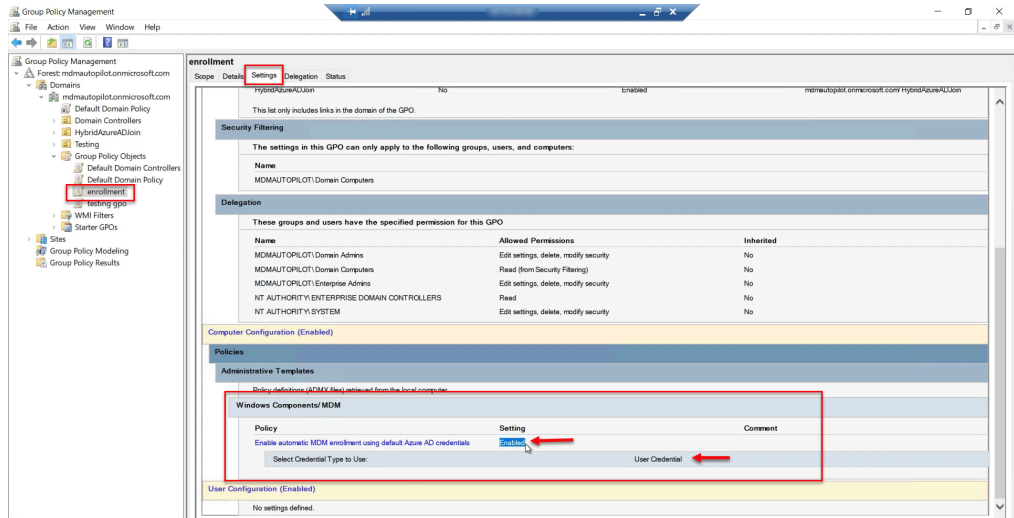
Define group policies in the domain controller

1. From Group Policy Management screen, under **Domains**, select your domain, click **Group Policy Objects**, right click, and from the context menu select **New**.



2. In the **NEW GPO** pop-up, enter the group policy name and click **OK**. The created policy is listed under Group Policy Objects.

- a. To enable non-admin user to enroll to BigFix MCM, select the created group policy, click **Settings**. Under **Computer Configuration > Policies > Administrative Templates > Windows Components/MDM**, do the following:
 - i. Enable the setting **“Enable automatic MDM enrollment using default Azure AD credentials”**
 - ii. For **Select Credential Type to Use**, select *User Credential*

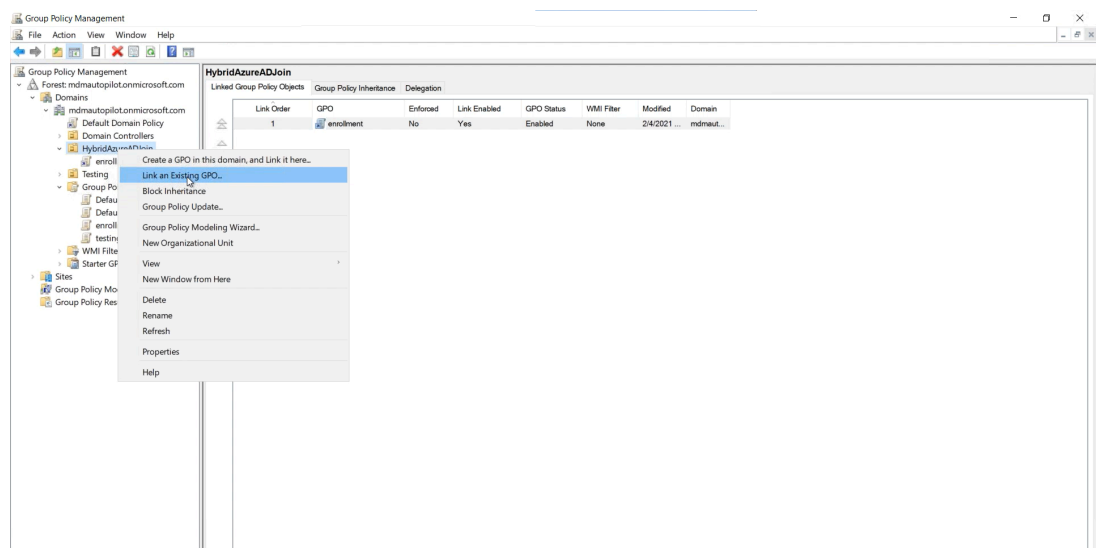


Now, the group policy is created and defined to enable non-admin user to enroll.

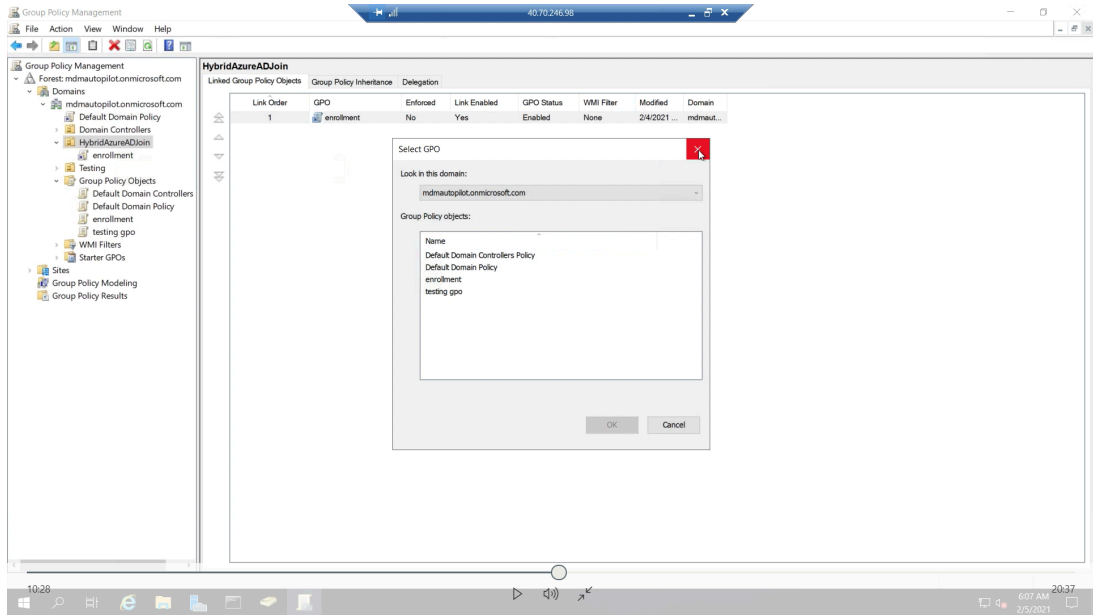
Next step: Associate the defined policy to devices

Assign the group policy (that enables non-admin device user to enroll) to Hybrid AD joined devices

1. Assign the group to the organization
 - a. Under **Group Policy Management**, select **Domains**, select (the organization), right click, and select **Link an Existing GPO**.



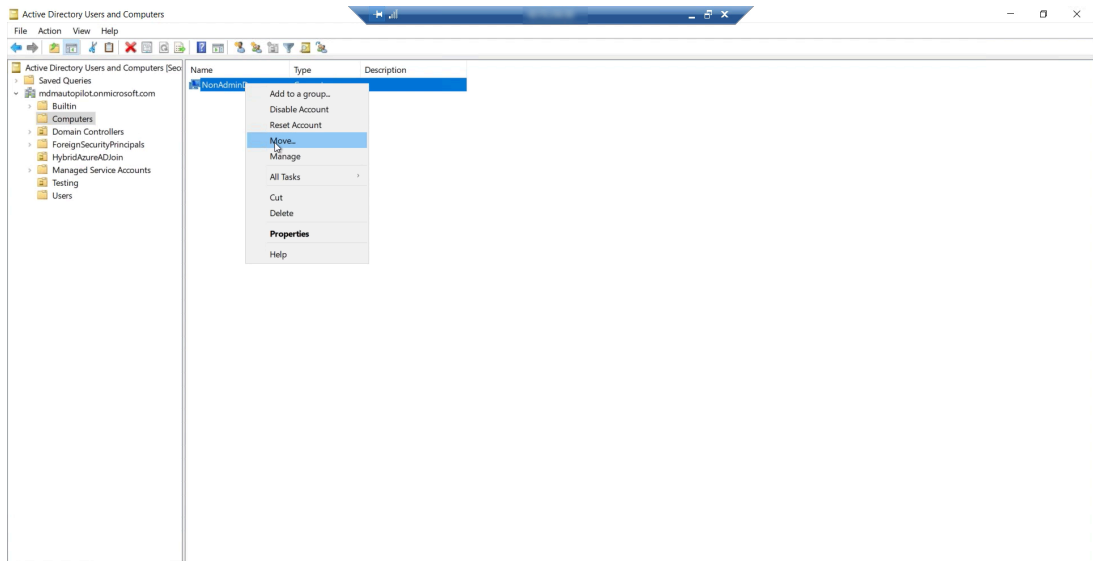
b. In the **Select GPO** pop-up, select the desired **Group Policy object** and click **OK**.



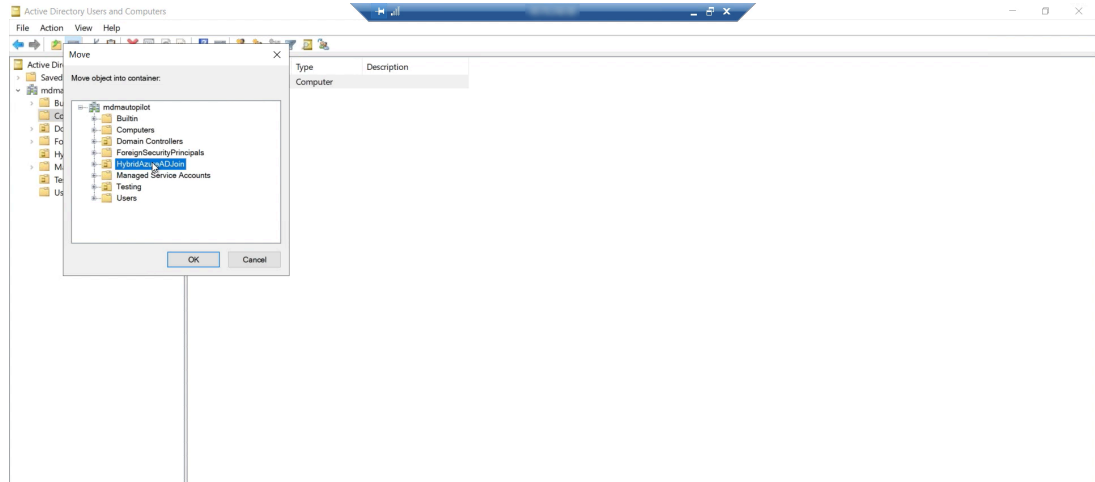
2. Assign the device to Organization

a. To move the Computers to the organization, From Azure Directory Users and Computers, navigate to Computers.

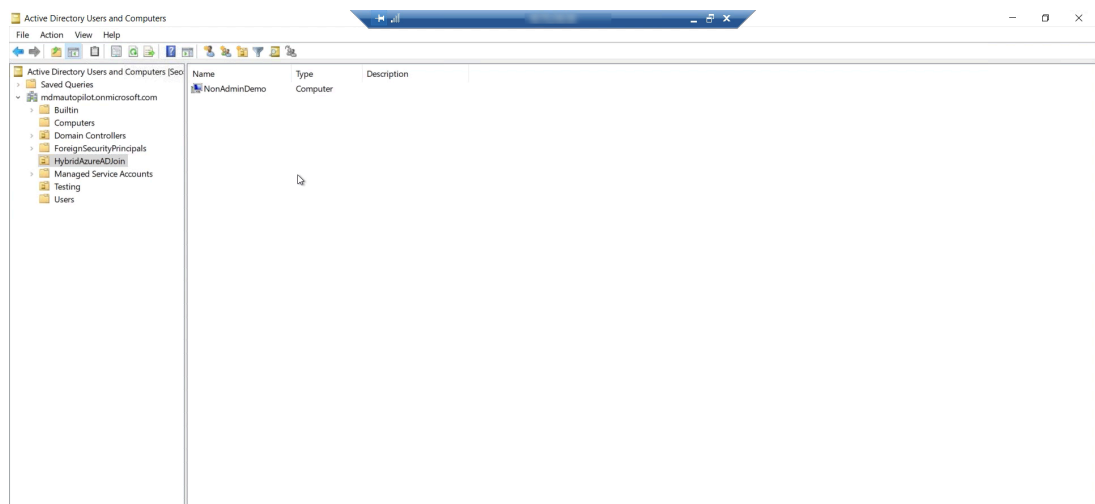
b. Select the device, right click, and click **Move**.



c. From the Move pop-up, select the organization and click **OK**.

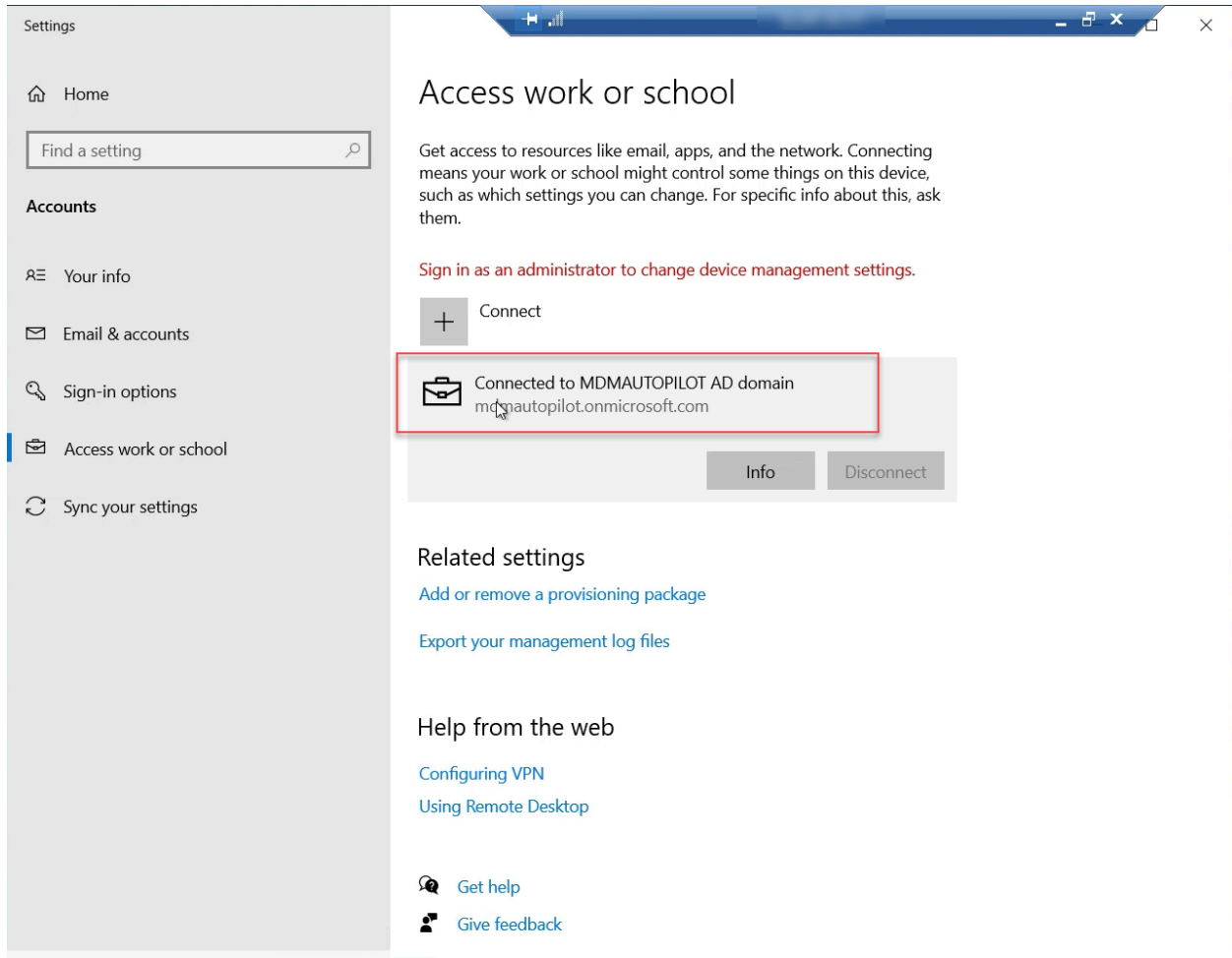


Now, the computer is moved to the selected organization. Now, this device is eligible for automatic enrollment.



Enrollment process

When a Hybrid AD joined device is restarted, it is automatically enrolled to BigFix MCM.



To verify Azure AD and on-prem AD and other details, from the enrolled device, in the command prompt, run the command `dsregcmd /status`. You can view all the required details.

```

Command Prompt
C:\Users\Amar>dsregcmd /status

-----+
| Device State |
-----+

AzureAdJoined : YES
EnterpriseJoined : NO
DomainJoined : YES
DomainName : MDMAUTOPILOT
Device Name : NonAdminDemo.mdmautopilot.onmicrosoft.com

-----+
| Device Details |
-----+

DeviceId : (REDACTED) 4d
Thumbprint : 02 (REDACTED) 0783ACC
DeviceCertificateValidity : [ 2021-02-05 04:14:42.000 UTC -- 2031-02-05 04:44:42.000 UTC ]
KeyContainerId : f802115-6-0151-4b3-8760-11700115078
KeyProvider : Microsoft Software Key Storage Provider
TpmProtected : NO
DeviceAuthStatus : SUCCESS

-----+
| Tenant Details |
-----+

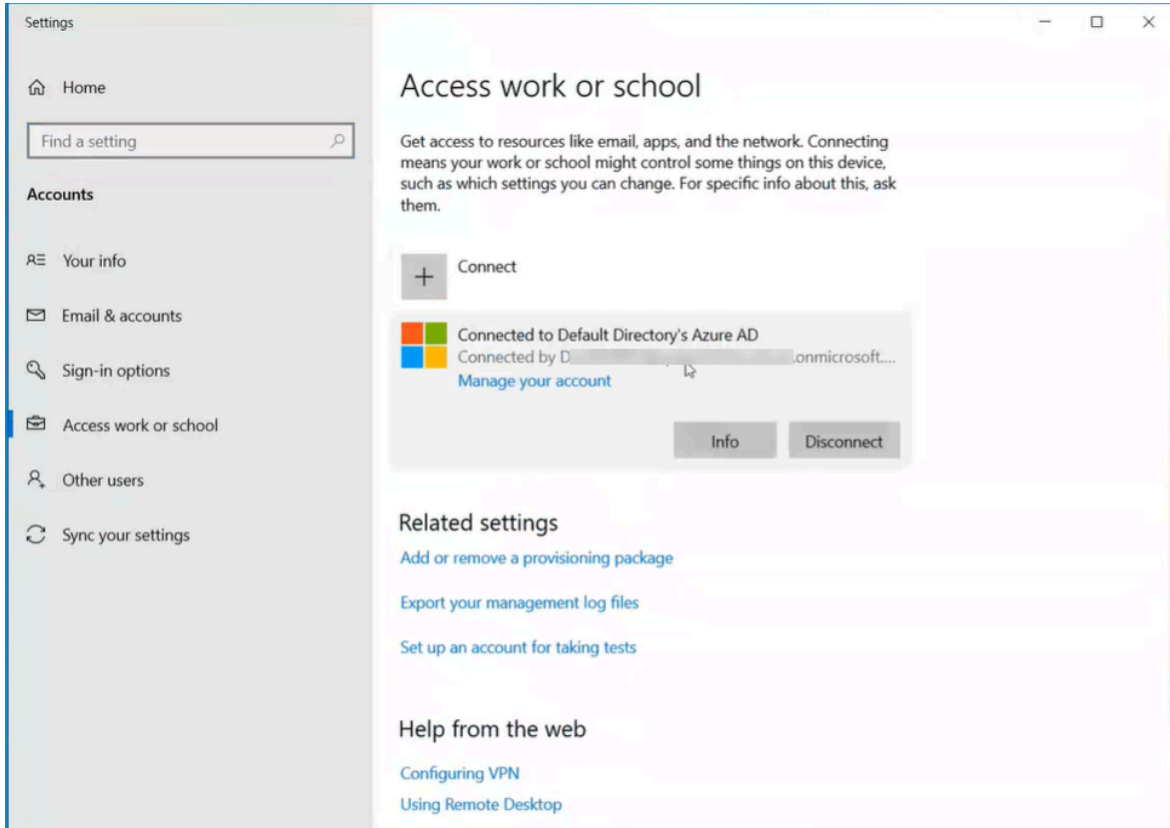
TenantName : BigFixMCM

```

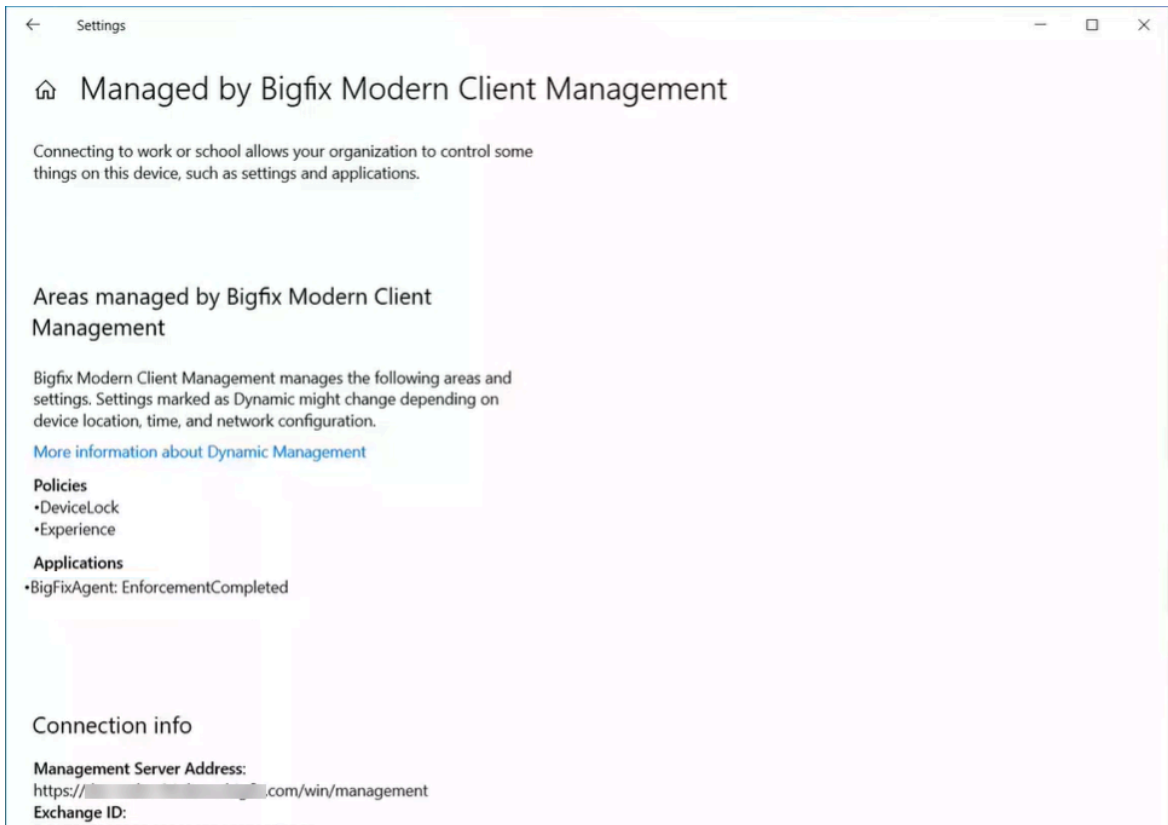
To begin the enrollment process, do the following steps:

1. Open the Windows device that is associated with the MDM server. Connect to the Internet. Enter the password as set in Azure AD. Update the password.
2. The End User License Agreement page appears. Select the license agreement check box after reading and click **Accept**. The autopilot enrollment process begins.

After the enrollment is completed, go to **Settings > Access work or school** to verify MDM server details.



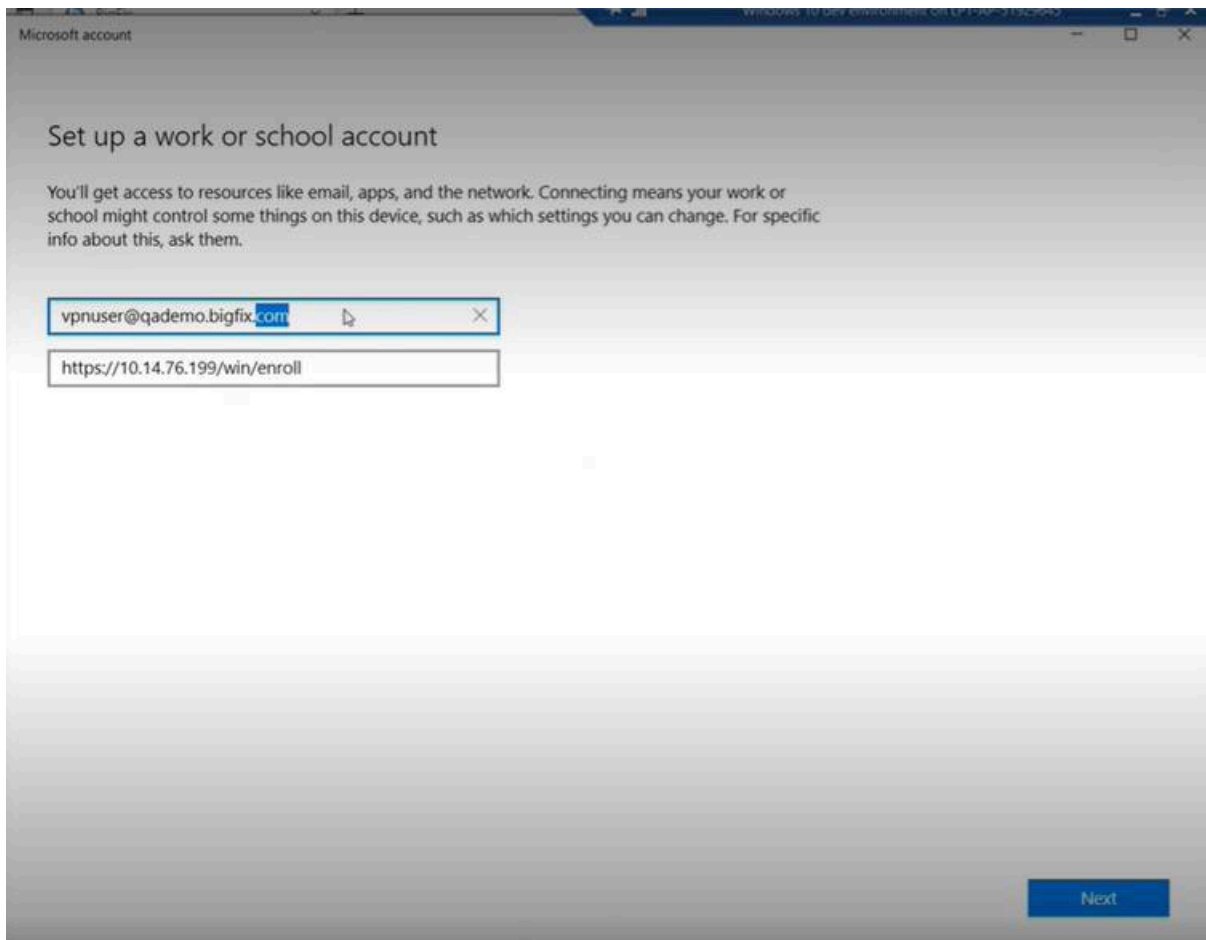
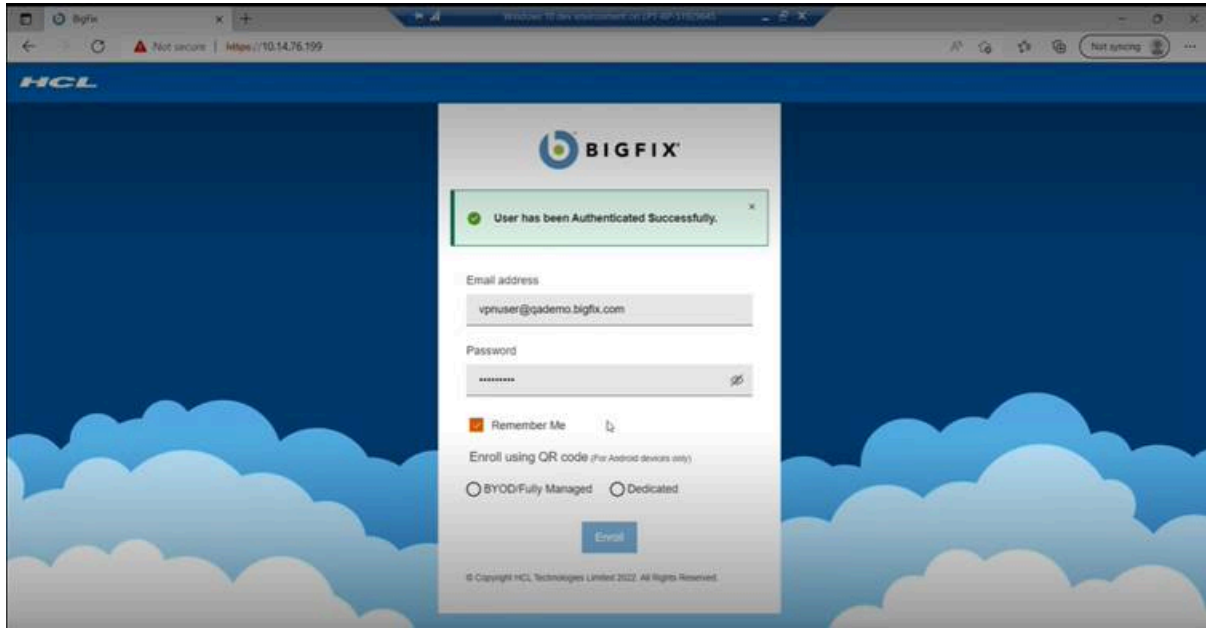
Click **Info** to verify the policy and application details.

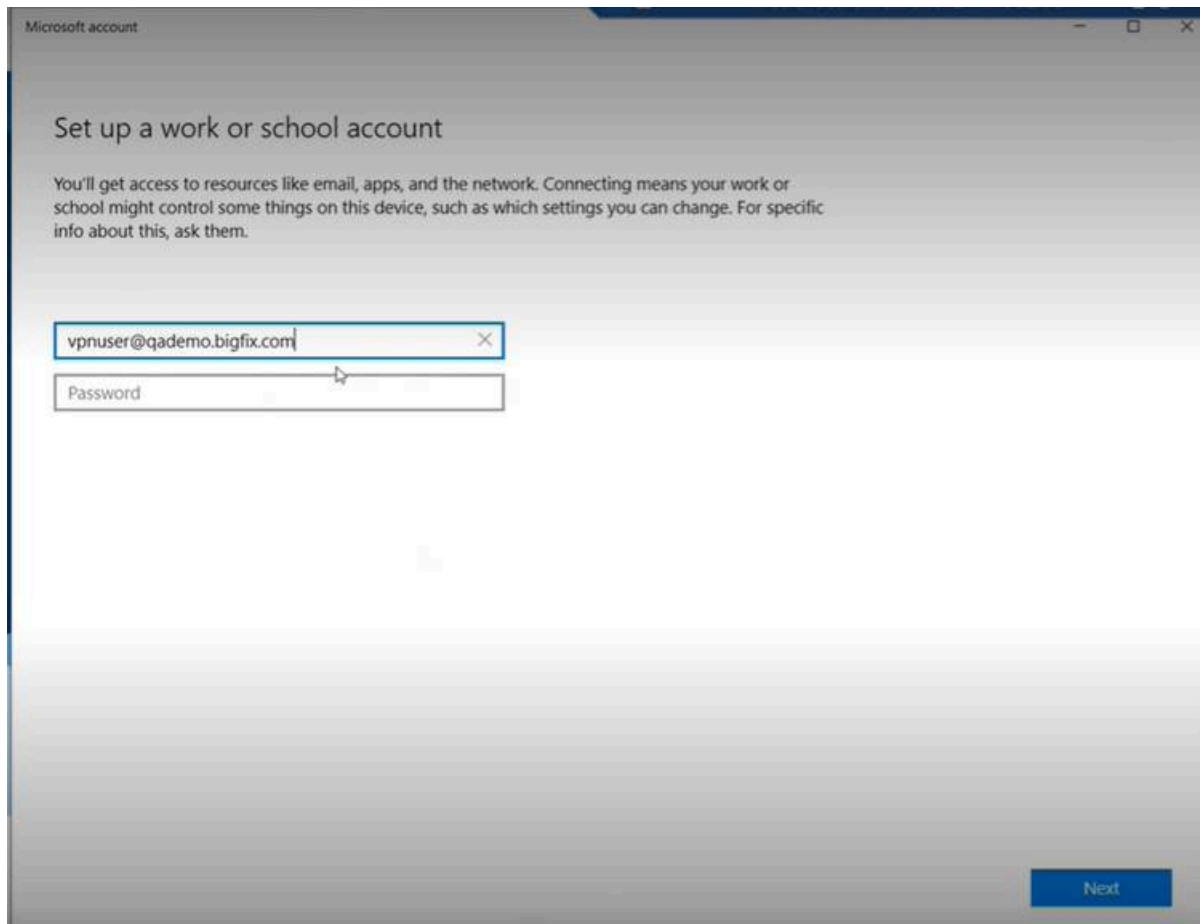


SCEP enrollment

BigFix MCM supports certificate management and certificate-based authentication through Simple Certificate Enrollment Protocol (SCEP). SCEP is the fastest and most secure way to provision certificates to all your MCM-managed devices. With SCEP, IT Admins can automate issuing certificates to the endpoints to provide access to corporate Wi-Fi, VPN, and secure e-mail through encryption.

1. Deploy a Policy Group with default SCEP policy on to the MDM server.
2. Enroll a Windows device





Result

- Enrolment is successful. It invokes the SCEP certificate.
- User can see the certificate in `certmgr.msc`
- The certificate name is created using the logged in user name.
 - Login to the enrolled device, run the "`certmgr.msc`" cmd, and navigate to the `Personal > Certificates`.
 - You can see that the certificate is created with the logged in user name.

Related information

[SCEP Certificate-based authentication \(on page 148\)](#)

Simple Certificate Enrollment Protocol (SCEP) configuration

Enrolling Apple devices

You can get Apple devices enrolled in BigFix MCM in the following ways.

- [Over the Air Enrollment \(on page 58\)](#): Users can enroll their Apple devices through an enrollment URL.
- [User Enrollment \(BYOD\) \(on page 60\)](#): Device users can enroll their personally owned iOS or iPadOS devices with BigFix Mobile, so that the IT admin can manage the devices.
- **Apple Automated Device Enrollment**: Administrators can configure and automate enrollment of out-of-the-box Apple devices that an organization purchases through Apple or authorized resellers to provide to employees.

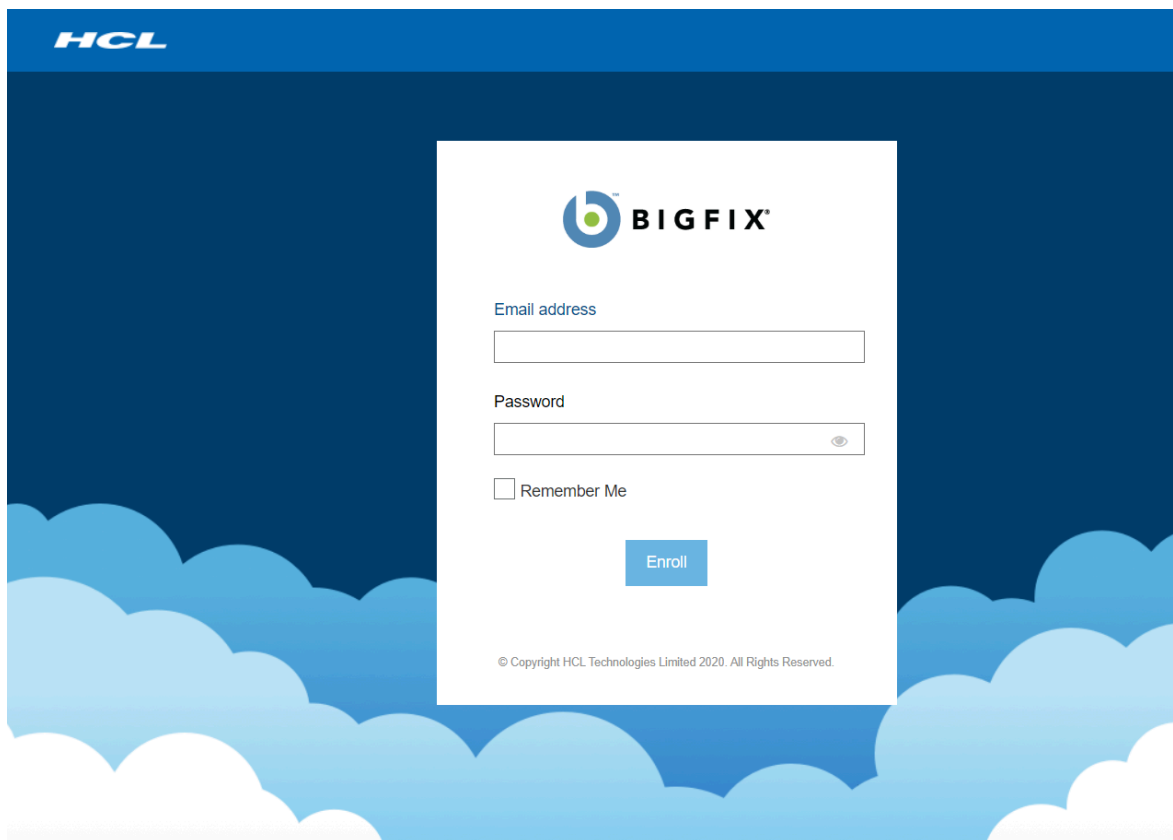
Enrolling through enrollment URL - Apple

Read this section to understand how the users can enroll Apple devices to MDM when the admin shares the enrollment URL.

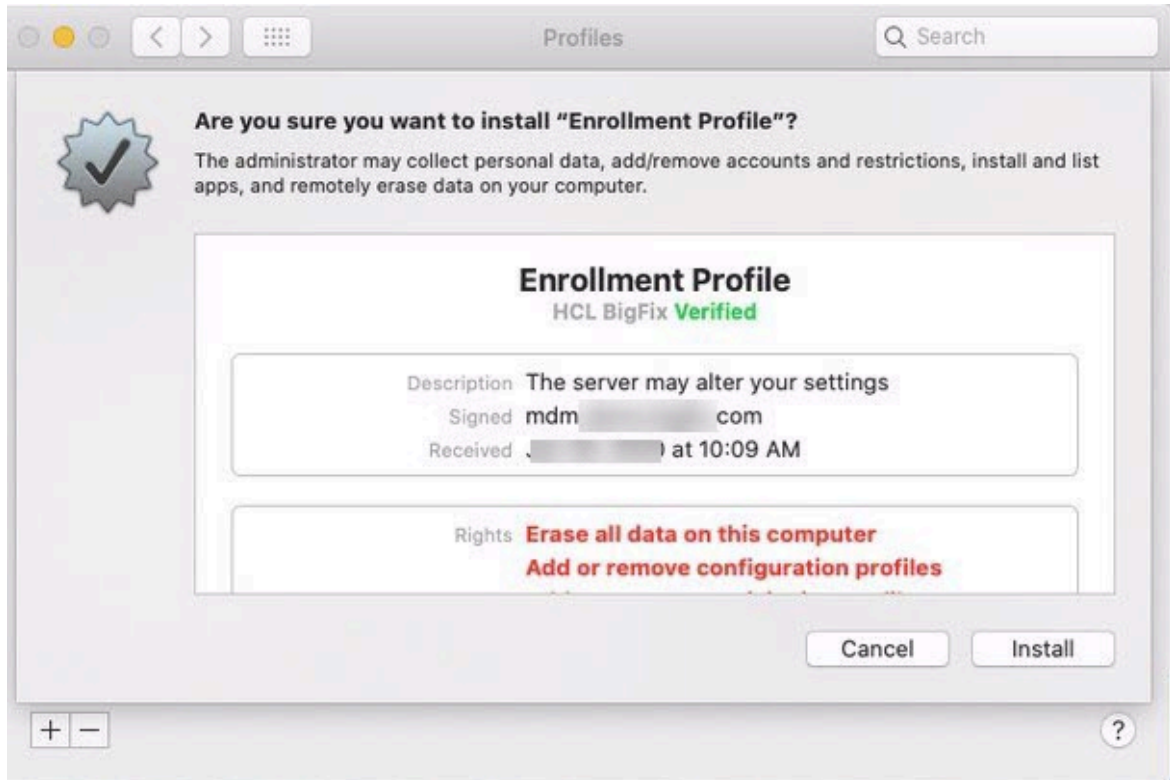
Users must visit the enrollment URL that is shared by BigFix administrator (via email or chat). This enrollment URL is the FQDN of the MDM Server (For example, <https://enroll-mdm.bigfix.com>). After authenticating in this enrollment portal, users must install the enrollment profile on their devices as an administrator.

To enroll the Apple device in MDM, follow these steps:

1. On the Apple devices, launch a web browser and navigate to the MDM Server URL.



2. Enter a valid email address and password associated with the Active Directory deployment configured when the MDM Server was set up.
3. Click **Enroll** to download the Mac enrollment profile.
4. OSX opens this Enrollment Profile and shows users the information about the MDM deployment they are about to enroll in. If things look okay, click **Install** to enroll the device in MDM.



Apple Automated Device Enrollment

MCM supports the Apple Automated Device Enrollment Program (DEP) – an online service to automate the enrollment and configuration of Apple devices.

Through Apple Automated Device Enrollment, you can enroll a large number of Apple devices effortlessly without user intervention. On the Apple Business Manager portal, BigFix administrators can preconfigure which devices can be assigned to which MDM Servers, so that as part of initial device setup, devices can automatically enroll in BigFix MCM.

For more information on Apple Automated Device Enrollment such as how to qualify for the program and links for Apple Business Manager and Apple School Manager, see [Apple's support site](#).

All Apple devices, as part of initial configuration, reach out to Apple Business Manager to see if they have been preassigned to a specific MDM Server to get enrolled. If Apple Business Manager finds configuration for a device that maps to a specific profile, it sends that profile to the device. The device processes the enrollment info, make the required settings, and then reaches out to the defined MDM Server within the profile to do an MDM enrollment. If there

is no specific device to Apple Automated Device Enrollment profile mapping, a device gets the Automated Device Enrollment profile assigned to the MDM Server that is marked as an auto-assigner.

Configuration

For instructions on configuring ABM or BigFix MCM server for Automated Device Enrollment, see the BigFix Wiki page [Apple Business Manager Quick Start Guide for DEP](#)



Note: All the Automated Device Enrollment profile configuration files (`.cert`, `.key`, `.enc`, and `.p7M`) are stored in the `/var/opt/BESUEM/certs` directory on the MDM server.

Enrollment

Once all these configurations are done, when a user powers up the Apple device for the initial OS setup and connects to Internet, Apple server receives a notification, recognizes the Automated Device Enrollment profile account, and redirects the device to the appropriate MDM server. The Setup Assistant on Mac devices takes the users through the activation process.

After the devices are enrolled, you can manage MDM devices through WebUI.

Apple BYOD enrollments

Allows device users to enroll their personally owned iOS or iPadOS devices with BigFix MCM so that the IT admin can manage the devices. Apple BYOD user enrollment separates work and personal data on the device, allowing employees to use their own device for work without compromising their privacy. With User Enrollment, the organization can manage work-related apps and data, but the user retains control over their personal apps and data.



Note: This option is available for devices running iOS 13 or later.

- User enrolled devices get personal and company profile. The company does not have access to the personal profile and hence cannot wipe, lock, or impose any control over the personal use of the device.
- Users can review the IT management capabilities of personally owned iOS and iPadOS devices before enrolling their device. Users can remove the MDM profile as the device is in unsupervised state.
- Users can securely access institutional resources such as email, contacts, calendars, Wi-Fi, and VPN, while keeping their personal data secure. Users maintain a personal Apple ID for their personal data and use a Managed Apple ID for institutional data.
- IT can only remove institutional data from the device, ensuring protection of the user's personal data, such as photos and documents. Since users must interactively complete enrollment, User Approved MDM status is achieved and grants administrators additional device management privileges.

Prerequisites

The user must have a managed Apple ID or Federated AD credentials through the associated business manager account.

WebUI

- In case of BYOD enrollments, on the Devices List page, the Enrollment Type column displays "BYOD". Users can filter devices by enrollment type.
- The Primary User column displays the Managed Apple ID that is used to enroll an Apple BYOD user.

Applicable actions for BYOD

- Lock (iOS only)
- Remove Policy
- Push VPP Apps and Books
- Unenroll

Applicable policies for BYOD

- Passcode policy
- Certificates policy

Managed Apple ID

A Managed Apple ID is an Apple ID that is created and managed by an organization or institution for its employees, students, or other members. It facilitates organizations to deploy and manage Apple devices, apps, and services.

Managed Apple IDs are created using Apple Business Manager or Apple School Manager. Managed Apple ID and associated password is used to enroll Apple devices to BigFix MCM and BigFix Mobile and can be used to access Apple services such as iCloud, the App Store, and Apple Music.

Managed Apple IDs allow organizations to maintain control over the devices and data used by their employees or students. This helps to ensure that data is secure and that devices are used in compliance with organizational policies.

Managed Apple IDs enable organizations to distribute apps and content to users, configure device settings, and manage software updates remotely.

For Apple user enrollments, the user must have a Managed Apple ID and Federated AD credentials through the associated Apple Business Manager account.

How to create a Managed Apple ID

To create a Managed Apple ID, you need to access either Apple Business Manager for a business or Apple School Manager for an educational organization.

Apple Business Manager

Here are the steps to create a Managed Apple ID using Apple Business Manager:

1. Go to the Apple Business Manager website and sign in with your administrator account.
2. Click on "Accounts" in the sidebar and select "People."
3. Click on the "+" button in the upper right corner and choose "Create New User."
4. Enter the user's first name, last name, and email address.
5. Select the role you want to assign to the user (e.g., manager, staff, student).
6. Choose whether you want to create a new Managed Apple ID for the user or assign an existing one.
7. If creating a new Managed Apple ID, choose a username and password for the user.
8. Optionally, you can add additional information such as phone number and address.
9. Click "Create" to create the Managed Apple ID and send an invitation to the user.

Apple School Manager

Here are the steps to create a Managed Apple ID using Apple School Manager:

1. Go to the Apple School Manager website and sign in with your administrator account.
2. Click on "Accounts" in the sidebar and select "Students" or "Staff."
3. Click on the "+" button in the upper right corner and choose "Add New User."
4. Enter the user's first name, last name, and email address.
5. Select the role you want to assign to the user (e.g., teacher, student).
6. Choose whether you want to create a new Managed Apple ID for the user or assign an existing one.
7. If creating a new Managed Apple ID, choose a username and password for the user.
8. Optionally, you can add additional information such as phone number and address.
9. Click "Add" to create the Managed Apple ID and send an invitation to the user.

Once the users accept the invitation and set up their Managed Apple ID, they can use it to access Apple services and enroll in BigFix MCM and BigFix Mobile.

Enrolling BYOD Apple devices (User enrollment)

Read this section to understand how the users can enroll BYOD Apple devices to MDM when the admin shares the enrollment URL.

- Ensure you have the Managed Apple ID
- Ensure you have the AD credentials which is the associated business manager account

Users must visit the enrollment URL that is shared by BigFix administrator (via email or chat). This enrollment URL is the FQDN of the MDM Server (For example, <https://enroll-mdm.bigfix.com>).

To enroll the Apple device in MDM, follow these steps:

1. On the Apple device, launch a web browser and navigate to the MDM Server URL.

2. Enter a valid email address and password associated with the Active Directory deployment configured when the MDM Server was set up.
3. Select ownership type of the device as **Personally Owned** to enroll your BYOD device.



Note:

- Click the information button to read the information as to what an IT admin can and cannot do on a personally owned device.
- The option "Institutionally Owned" is the default option. When selected, it takes you through the [device enrollment flow](#) to enroll the company-owned device.

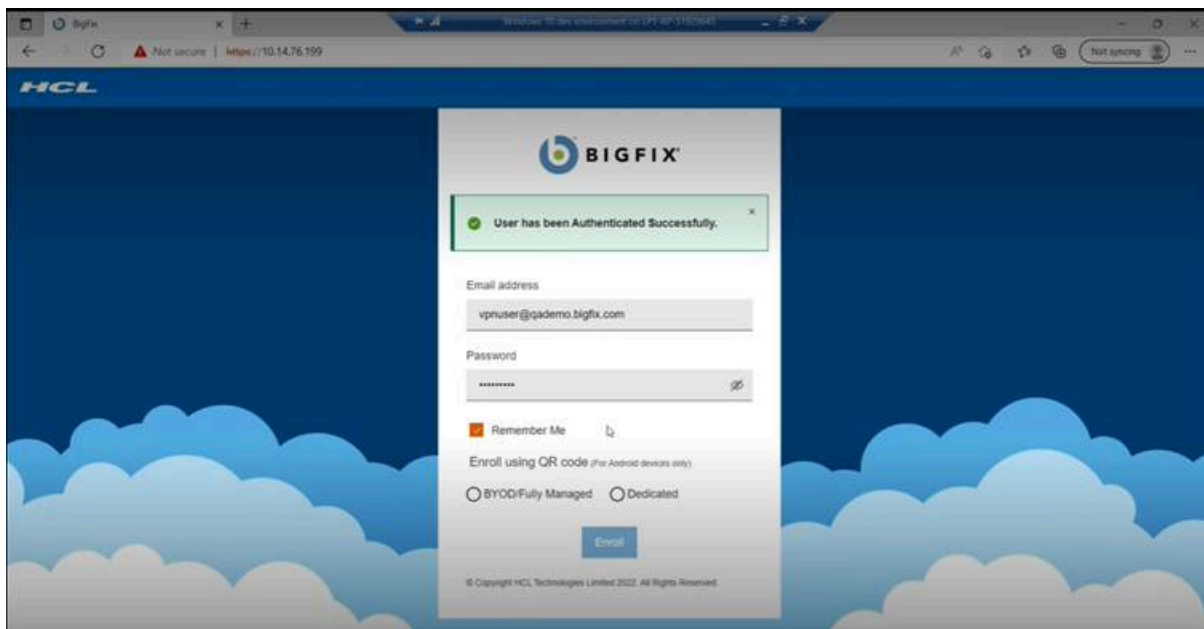
4. The text box to enter Managed Apple ID appears. Enter your managed Apple ID to install MDM profile.
5. Click **Enroll** to download the Apple enrollment profile.
6. OSX opens this Enrollment Profile and shows users the information about the MDM deployment they are about to enroll in. If things look okay, click **Install** to enroll the device in MDM.

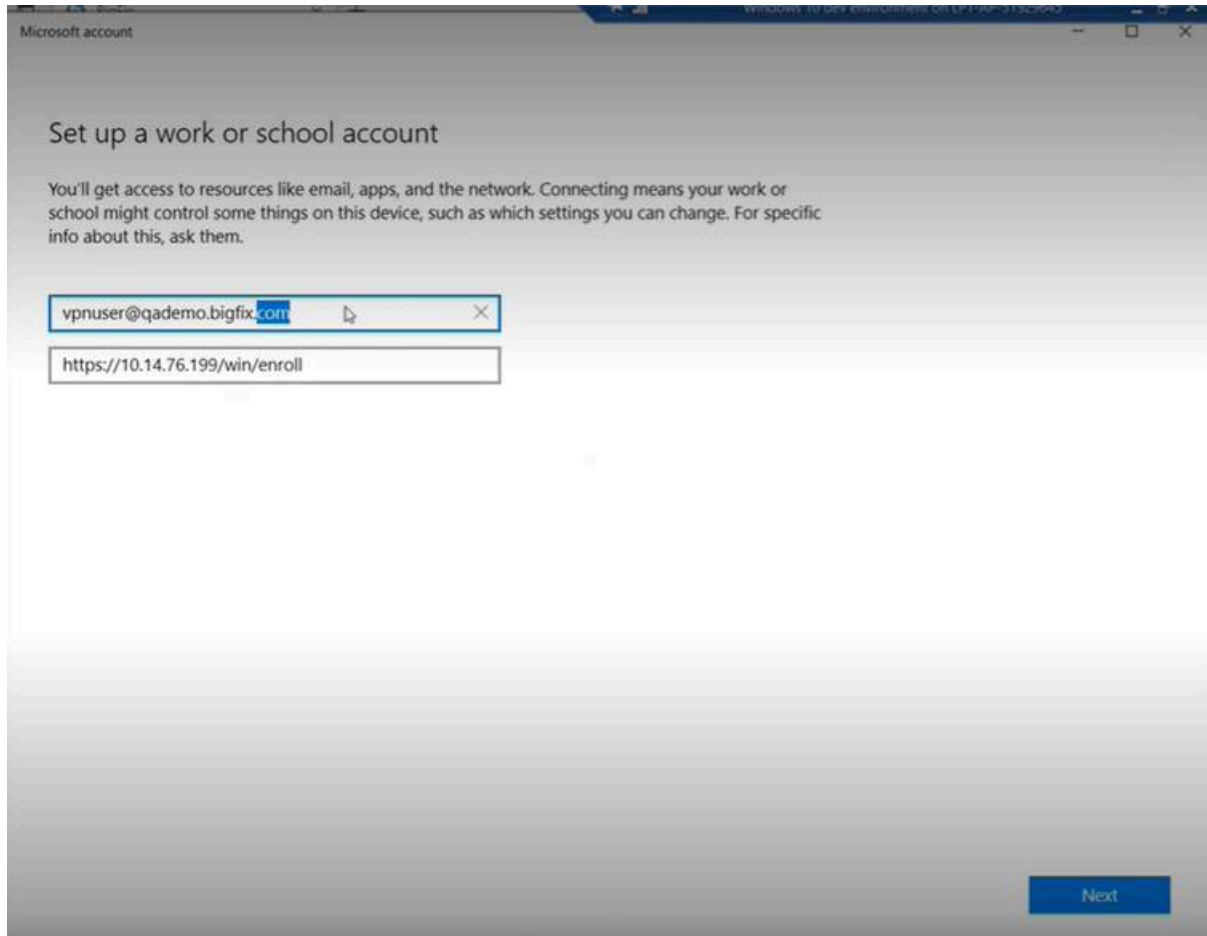
The MDM profile gets installed. User sees a personal profile and a company profile. The organization does not have access to the personal profile and hence cannot wipe, lock, or impose any control over the personal use of the device. The organization can manage only the company profile section.

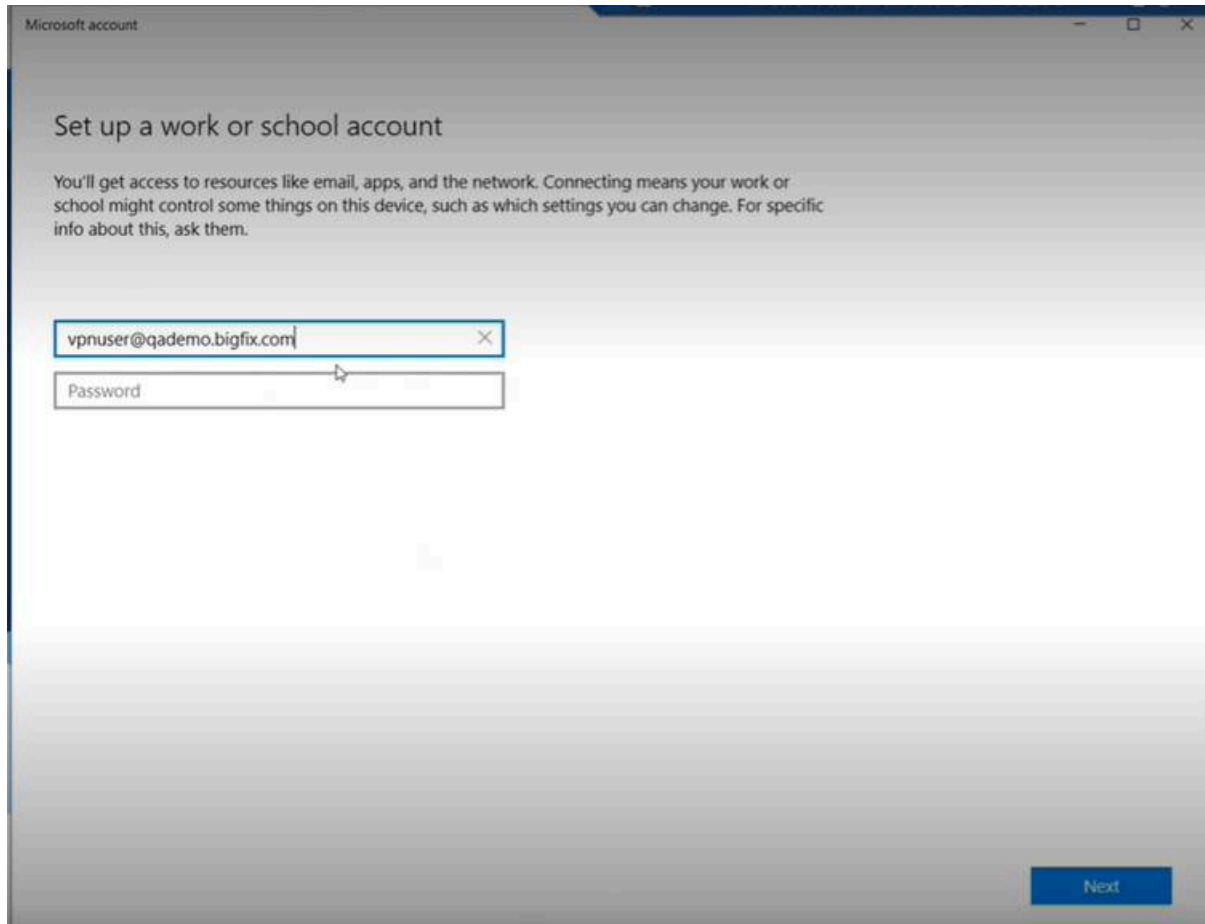
SCEP enrollment

BigFix MCM supports certificate management and certificate-based authentication through Simple Certificate Enrollment Protocol (SCEP). SCEP is the fastest and most secure way to provision certificates to all your MCM-managed devices. With SCEP, IT Admins can automate issuing certificates to the endpoints to provide access to corporate Wi-Fi, VPN, and secure e-mail through encryption.

1. Deploy a Policy Group with default SCEP policy on to the MDM server.
2. Enroll a Windows device







Result

- Enrolment is successful. It invokes the SCEP certificate.
- User can see the certificate in `certmgr.msc`
- The certificate name is created using the logged in user name.
 - Login to the enrolled device, run the "`certmgr.msc`" cmd, and navigate to the `Personal > Certificates`.
 - You can see that the certificate is created with the logged in user name.

Related information

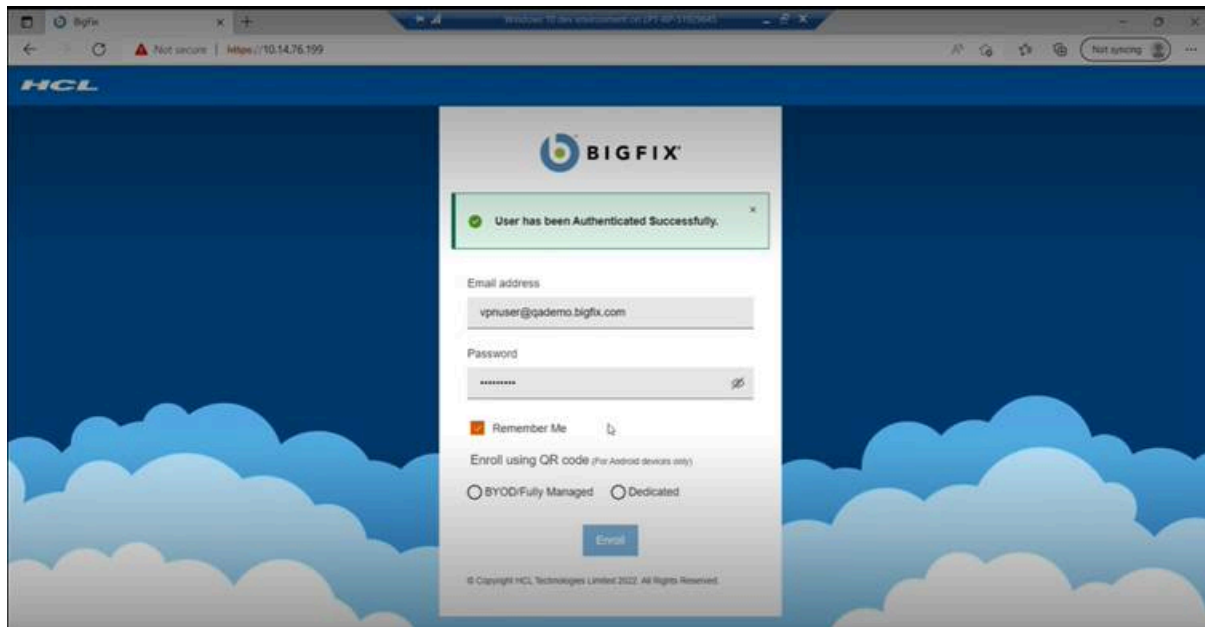
[SCEP Certificate-based authentication \(on page 148\)](#)

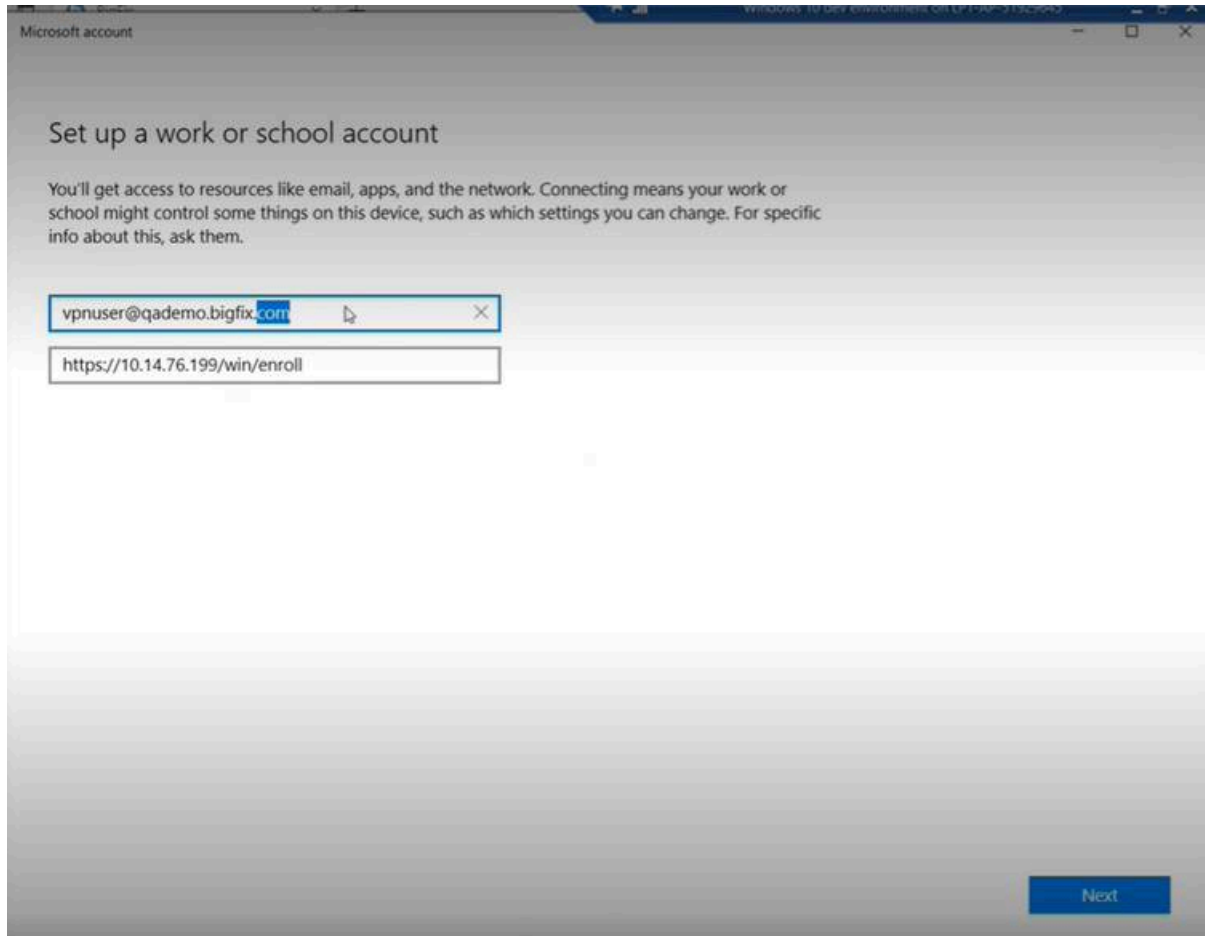
Simple Certificate Enrollment Protocol (SCEP) configuration

Enrollment flow

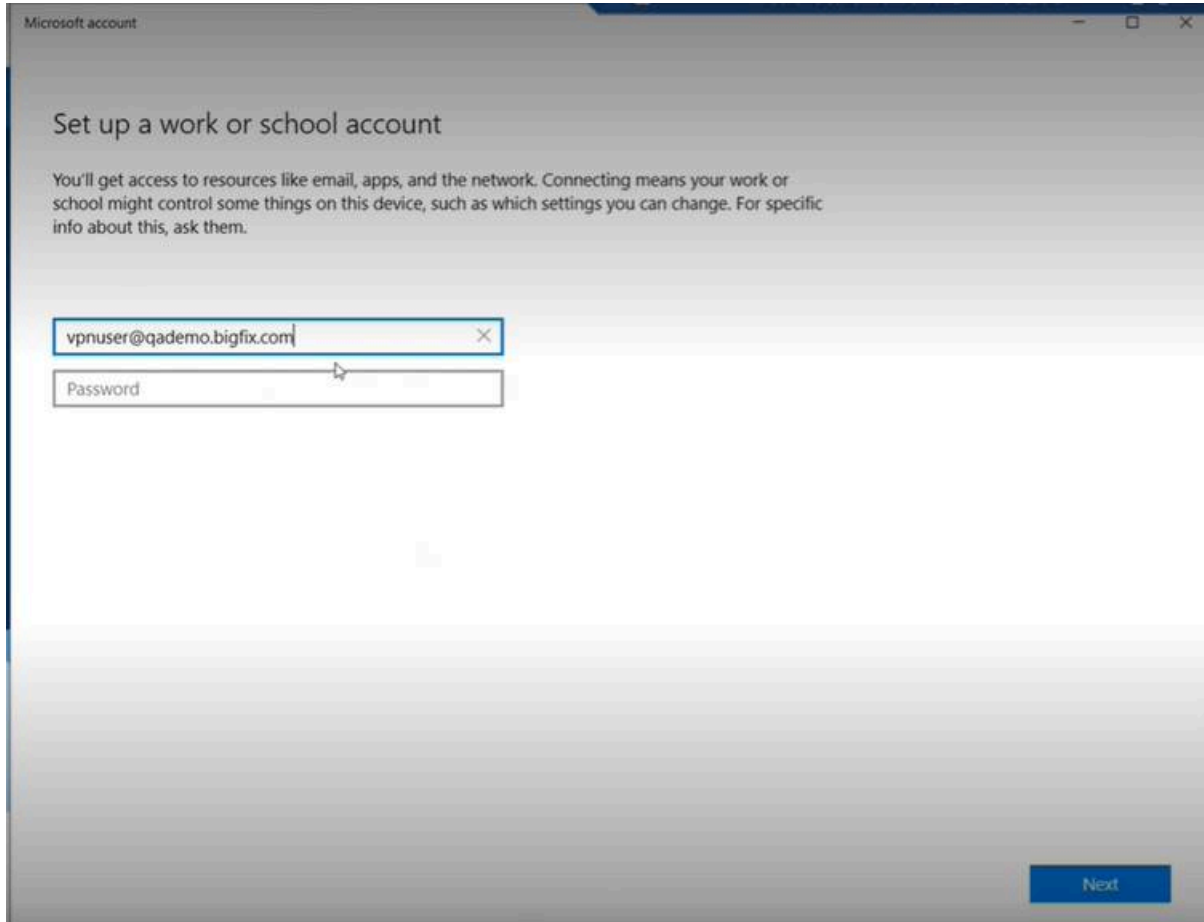
BigFix MCM supports certificate management and certificate-based authentication through Simple Certificate Enrollment Protocol (SCEP). SCEP is the fastest and most secure way to provision certificates to all your MCM-managed devices. With SCEP, IT Admins can automate issuing certificates to the endpoints to provide access to corporate Wi-Fi, VPN, and secure e-mail through encryption.

1. Deploy the SCEP Group policy on to the MDM server.
2. Enroll a device using OTA enrolment method
3. Login to MDM server and navigate to respective MDM service log path i.e Windows/Apple
4. Check the logs whether any errors found during the enrolment.





NEXT > NEXT



Result

- No enrollment errors in the MDM logs.
- Enrolment is successful. It invokes the SCEP certificate.
- User is able to see the certificate in `certmgr.msc`
- The certificate name is created using subject name that is mentioned in the SCEP profile.
 - Login to the enrolled device, run the "`certmgr.msc`" cmd in run box, and navigate to the **Personal > Certificates**
 - Check the certificate that is created with the subject name that is issued.

Full Disk Encryption

With BigFix MCM, you can centrally manage the native full-disk encryption technologies from Windows (BitLocker) and macOS (FileVault2) to secure data at rest.

Full disk encryption

Full disk encryption (FDE) is a technology which protects information at the hardware level by automatically converting it into unreadable code that cannot be deciphered easily by unauthorized people. It is used to prevent unauthorized access to data storage. Without the proper authentication key, even if the hard drive is removed and placed in another machine, the data remains inaccessible.

Benefits of FDE

BigFix MCM provides a hybrid FDE solution through which you can:

- Enforce data encryption through an MDM policy
- Enable or disable data encryption
- Query encryption status of the endpoints
- Get a report of compliant vs. non-compliant endpoints
- Secure and manage encryption keys (key escrow)



Note:

- FDE involves user interaction to continue with setup, enter password at start up to start encryption process, or to start OS after the forced restart.
- On macOS, encrypting secondary drives or enforcement of encryption of removable drives is not supported.

Supported Operating Systems

BigFix MCM supports the native FDE technologies from the following operating systems:

- [Windows \(on page 71\)](#)
- [MacOS \(on page 72\)](#)

Prerequisites

- Enrollment to BigFix MCM.
- Versions of Operating Systems that are supported by BigFix MCM (Windows, macOS).
- If BES server is installed on a RHEL 8 machine, you must register the RHEL instance on RHN for the yum command to run by default. Then run the following yum command:

```
yum install libns1
```

- [BES server plugin service \(on page 72\)](#)



Note: The system requirements and the limitations specific to Windows BitLocker and macOS FileVault2 are applicable as appropriate for BigFix MCM FDE feature as well.

How to configure FDE

1. [Set up the BES Server Plugin Service \(Fixlet 708 in BES Support\) \(on page 72\)](#)
2. [Recovery Key Escrow Configuration \(on page 73\)](#)

Regenerate Encryption Recovery Key

The certificate and private key used to escrow recovery keys can be regenerated if needed. Caution must be taken when doing this, as any in-progress encryption actions cannot be decrypted and escrowed. You must wait until there are no open actions and devices have had time to report recovery keys, and the escrow plugin has had time to process them.

To retrieve escrowed recovery keys, operator or support person must log in directly to the Vault server interface (if you have set up vault, you can use the bigfix-read access token) The credentials used to login to the Vault server are set at the time of installing Vault. These credentials are different from the BigFix credentials. The 'bigfix' secret engine contains the recovery keys. Recovery keys are stored in folders based on the last digit of the BigFix computer ID. Once you are inside a folder, you can search using the computer ID, computer name or user. The name of the entry in Vault has these values as of the time the recovery key was escrowed.

If you suspect an encryption recovery key has been compromised, or if you want to rotate recovery keys as part of your organizations best practices, recovery keys can be regenerated through WebUI, see [Regenerate Encryption Recovery Key](#)

Related reference

[Generating Encryption Recovery Key Escrow fails \(on page 160\)](#)

Windows BitLocker

BitLocker is the Windows encryption technology that protects your data from unauthorized access by encrypting your drive.

BigFix MCM provides a hybrid full-disk encryption solution for Windows devices, which uses MDM policies for enforcement of the encryption settings, while using the BigFix agent and the manage-bde CLI to perform encryption actions. This allows for greater control as well as the ability to do more unattended setup and configuration.

<https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/manage-bde>

Prerequisites

- Trusted Protection Module (TPM) on Windows

- The endpoint must be correlated; must be enrolled in BigFix MCM and must have BigFix agent installed.

For a complete information about system requirement, see <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview#system-requirements>

Configuration options

- Fixed/removable drives require encryption
- Encryption methods
- Custom recovery message
- Basic TPM Readiness checks/status reporting (Check if the device can be encrypted)
- Gathering encryption status/data through the BigFix agent.
- Reporting is done through agent analysis with relevance using WMI calls

BigFix MCM enables BitLocker using the TPM to encrypt the system drive using AES-256. At this time, only the system drive can be encrypted, but policy setting that fixed and removable drives must be encrypted can be set, and the end user can enable BitLocker using appropriate methods to be compliant.

MacOS FileVault

For information about macOS FileVault, see <https://developer.apple.com/documentation/devicemanagement/fdefilevault>



Note: Enabling full disk encryption on macOS devices disables auto-login. For more information, read Apple official documentation at <https://support.apple.com/en-us/HT201476> and <https://support.apple.com/en-us/HT204837>.

Set up the BES Server Plugin Service (Fixlet 708 in BES Support)

To enable the Full Disk Encryption feature, you must install the BES Server plug-in in BigFix. To install the BES Server plug-in, run the installation Fixlet and target the BigFix server.

Before enabling FDE feature, complete the following prerequisite steps as necessary:

1. Ensure that the **BES Server Plugin Service** is installed on the BigFix server and is configured correctly.



Note: The user must be a Master Operator to install the `mdm-fde-plugin`.

2. After you install the **BES Server Plugin Service** on the server, enable encryption of the credentials for the BigFix REST API by running the `Configure REST API credentials for BES Server Plugin Service` task from **Fixlets and Tasks** node of the **All Content** domain.

- a. Click the Configure REST API credentials for BES Server Plugin Service Task. The user interface from which you must start the encryption enablement Task is displayed.
- b. Enter the user name and password for the master operator user that you created. This creates an encrypted password.
- c. Click **Take Action** and specify the server where you are installing the mdm-fde-plugin, which is the BigFix server.



Note: The Configure REST API credentials for BES Server Plugin Service Task remains relevant after you run it. You can check the action history to confirm that it runs successfully.

Recovery Key Escrow Configuration

Key escrow is a method of storing important cryptographic keys. By using key escrow, organizations can ensure that in the case of crisis, such as security breach, lost or forgotten keys, natural disaster, or otherwise, their critical keys are safe and can be recovered.

Recovery Key Escrow Configuration involves the following steps:

1. Certificate creation – You must create a certificate and key pair for encrypting the recovery key through WebUI MDM app. This certificate is used in Windows actions and in macOS escrow payload. The key is placed in BES Server Plugin folder for decrypting.
2. [Set up Vault \(on page 73\)](#) – You must specify an existing Vault server (URL, access keys), or you can also deploy Vault with self-signed certificates. You can access the Vault directory to get the unseal keys and access keys that were generated, and configure Vault settings in WebUI.
3. Escrow server plugin setup – Set up the Escrow server plugin through WebUI by configuring with details of the key and Vault details, so that the private key is stored in the 'Applications' directory of the BES server.

Troubleshooting

Manual device task to escrow recovery key – If recovery key is missing or out of date, you can retrieve it through Regenerate Encryption Recovery Key.

Set up Vault

Vault is the open source secret engine that BigFix uses to secure, store and tightly control access to tokens, passwords, certificates, encryption keys for protecting secrets and other sensitive data using a UI, CLI, or #HTTP#API.

For more information about Vault, see <https://www.vaultproject.io/> by HashiCorp.

- Users can set up their own Vault instance and provide details and appropriate access keys to store recovery keys and obtain information about the recovery key.

A secret engine named 'bigfix' of type KV version 2 must be created. A user with write permission must be created with the userpass auth method. An ACL policy of:

```
path "bigfix/data/*" {
  capabilities = ["create", "update",]
}

path "bigfix/metadata/*" {
  capabilities = ["list", "read"]
}
```

or

- Deploy Vault on a specified system and set up with default security configuration, by running the Fixlet from BESUEM site to install Vault server. This automates the setup of the Vault with default security settings (specified unseal key, automatically unsealing, self-signed certificate or specified). On Linux, Vault is deployed as a docker container, and on Windows Vault is deployed as an application and a scheduled task launches upon system start up. Unseal and access keys are logged, and users must save those keys somewhere,

configure them in the WebUI for plugin configuration, key escrow status retrieval. Users can provide SSL certificate or user-facing host name. More information can be found in the Fixlet description.

The screenshot shows the BigFix Console interface. On the left is a navigation tree with 'Fixlets and Tasks (31)' selected. The main pane displays a table of Fixlets and Tasks. The task 'Install Vault Server on RHEL' is highlighted with a red box. Below the table, the task details are shown, including a note about prerequisites and instructions for entering Vault key settings and TLS certificates.

ID	Name	Source	Severity	Site	Applicable Com...	Open Action Co...	Category
701	BigFix MDM Server - Deploy staged TLS Certificates	BESUEM Dev	Normal	BESUEM Dev	0 / 12	0	Certificate
702	BigFix MDM Server - Stage External TrustedCA TLS Certificates	BESUEM Dev	Normal	BESUEM Dev	1 / 12	0	Certificate
4004	Add BigFix MacOS MDM Server (Version 1.0.1)	<Unspecified>	<Unspecified>	BESUEM Dev	0 / 12	0	Upgrade
4005	Add BigFix Windows MDM Server (Version 1.0.1)	<Unspecified>	<Unspecified>	BESUEM Dev	0 / 12	0	Upgrade
4006	Install BigFix Apple MDM Server (Version 1.1.0)	<Unspecified>	<Unspecified>	BESUEM Dev	0 / 12	0	Upgrade
4007	Install BigFix Windows MDM Server (Version 1.1.0)	<Unspecified>	<Unspecified>	BESUEM Dev	0 / 12	0	Upgrade
4008	Updated BigFix MDM Server Components (Version 1.0.1) Now Available!	<Unspecified>	Critical	BESUEM Dev	0 / 12	0	Upgrade
4009	Add BigFix Apple MDM Server (Version 1.1.0)	<Unspecified>	<Unspecified>	BESUEM Dev	0 / 12	0	Upgrade
4010	Add BigFix Windows MDM Server (Version 1.1.0)	<Unspecified>	<Unspecified>	BESUEM Dev	0 / 12	0	Upgrade
4011	Updated BigFix MDM Server Components (Version 1.1.0) Now Available!	<Unspecified>	Critical	BESUEM Dev	0 / 12	0	Upgrade
4502	Install BigFix Plugin for Apple MDM (Version 1.1.0)	<Unspecified>	<Unspecified>	BESUEM Dev	0 / 12	0	Upgrade
4503	Install BigFix Plugin for Windows MDM (Version 1.1.0)	<Unspecified>	<Unspecified>	BESUEM Dev	0 / 12	0	Upgrade
4504	Updated BigFix Plugins for MDM (Version 1.0.1) Now Available!	<Unspecified>	Critical	BESUEM Dev	0 / 12	0	Upgrade
4505	Updated BigFix Plugins for MDM (Version 1.1.0) Now Available!	<Unspecified>	Critical	BESUEM Dev	0 / 12	0	Upgrade
4506	Install Vault Server on RHEL	BESUEM Dev	Normal	BESUEM Dev	0 / 12	0	Setup

Task: Install Vault Server on RHEL

Note: Prerequisites on the OS include openssl, docker, docker-compose, and unzip

This fixlet will install and setup a simple installation of Vault. It will install as a docker container located at "/var/opt/vault". Unseal keys and access tokens will be located at "/var/opt/vault/volumes/secrets"

Enter the following Vault Key Settings:

Key Shares:

Key Threshold:

TLS Certificate can be specified here, or a hostname can be specified for self-signed certificate generation.

Enter the following Server TLS certificate and key contents:

Server TLS Certificate content (PEM Format):

Server TLS Key content (PEM Format):

Or enter the following parameters for self-signed certificate generation:

User facing hostname:

Actions

Click [here](#) to install Vault.

The screenshot shows a web browser window with the URL 'https://jmh-mdm.../vault/secrets'. Below the browser, the 'Secrets Engines' section is visible, listing 'bigfix/' and 'cubbyhole/' engines.

Secrets Engines

Enable new engine +

- bigfix/
v2_kv_074d9dac
- cubbyhole/
cubbyhole_96ad4186

Application management

Through BigFix WebUI, IT admins can manage applications of the enrolled devices.

For Windows and macOS, you must prestage applications, including BigFix agent, on the MDM server to distribute them to enrolled devices.

To learn how to prestage an application through WebUI, see [Prestage an Application](#).

To learn how to prestage BigFix agent, see [Prestage macOS BigFix installer](#) and [Prestage Windows BigFix Installer](#).

In a policy group, you must add prestaged applications to deploy them on the enrolled devices.

OS update

MDM administrators can remotely manage software updates such as software patches, minor or major versions. This can help secure or enhance the current operating system.

Windows

<to be updated>

MacOS

MDM administrators can manage software updates remotely on macOS devices through MDM action. For the steps to perform this action, see [OS Update](#).

User management

Manually assign user to device

Chapter 3. BigFix Mobile

BigFix Mobile enables you to enroll and manage devices starting from Android 5.0, iOS, and iPadOS.

This solution enables IT admins to securely and wirelessly configure corporate-owned or employee-owned mobile devices. After enrolling to BigFix Mobile, IT admins can get the visibility of the enrolled mobile devices through WebUI. IT admins can secure, manage and monitor mobile devices that access corporate data. IT admins can also update software and device settings, monitor compliance with organizational policies, and remotely wipe, lock, and reboot the mobile devices.

Device users can enroll their own devices in BigFix Mobile, or IT admins can enroll company-owned devices automatically.



Important: Ensure all the operating system specific analyses are activated through [WebUI Health Check](#) for MCM app to work as expected.

Supported Operating Systems and versions

- Android 5.0 and later
- iOS 14 and later
- iPadOS 14 and later

Android mobile management

BigFix Mobile, the Enterprise Mobility Management (EMM) solution, is integrated with [Android Enterprise](#). With this solution, you can effortlessly enroll and manage Android devices.

BigFix Mobile separates work-related data from personal data. This ensures to protect sensitive information from loss and theft while addressing privacy.

Work profile management

The Work profile solution is intended for managing employee-owned devices, also known as Bring Your Own Devices (BYOD). By creating a Work Profile, IT administrators can create a secure container on the device that separates business dedicated data from personal data. Work related apps and data are stored in a stand-alone part of the device, and organizations have no visibility or access to user's personal data. More info about Work Profile is [here](#).

Full device management

The Full device management solution is most suited for Corporate Owned Business Only (COBO) devices. These devices are intended for professional use only. Full Device Management allows MDM to create a secure mobile workspace that requires extra layers of security.

Organizations can have a complete control over which apps and data are allowed on the enrolled device, and can control various settings like app management, internet filtering, security challenge, OS updates, Wi-Fi connections. Device-wide controls such as a complete device wipe and reset to factory default

settings are also available on fully managed devices. FDM allows MDM to manage device settings and policies that are not available in the [work profile solution set](#).

Dedicated device management

Dedicated devices are company-owned, fully managed devices that are used exclusively for specific work purposes. [Dedicated device management](#) is an extension of [full device management](#). IT admins can further lock down dedicated devices to a single app or a set of apps. This enables to perform specific employee or customer-facing functions such as inventory management, hospitality kiosk services, and digital signage.

- IT admins can enforce extended security policies where the dedicated devices are locked to an allowed set of apps using [kiosk mode \(on page 130\)](#). This allows to run the device in kiosk mode.
- IT admins can restrict device users from accessing apps other than the allowed apps and prevent other actions performed on the device. Kiosk mode prevents users from exiting apps and accessing a device’s home screen.
- For device and data security, safe boot, screen capture, camera, and factory reset features are disabled by default on dedicated Android devices.

Supported features

BigFix Mobile offers the features from Standard Management Set for work profile management, full device management, and dedicated device management.

Supported features	Supported versions ¹		
	Work profile management(Applicable Android version)	Full device management(Applicable Android version)	Dedicated device management(Applicable Android version)
Device provisioning <ul style="list-style-type: none"> • Enrollment through enrollment link 	5.1+	N/A	N/A
<ul style="list-style-type: none"> • Enrollment through QR code 	5.1+ (on page 88)	6.0+ (on page 93)	7.0+ (on page 106)

1. For updated information on the supported versions, refer to Android Enterprise official documentation at <https://developers.google.com/android/work/requirements>

• Zero-touch enrollment (on page 95)	N/A	7.0+ (on page 95)	7.0+ (on page 108)
Device security (on page 117)			
• Device security challenge	5.0+	5.0+	5.0+
• Work security challenge	7.0+	5.0+	5.0+
• Wipe and lock	5.0+	5.0+	5.0+
• Compliance enforcement	5.0+	5.0+	5.0+
• Default security	5.0+	5.0+	6.0+
• Default security policy override (on page 120)	5.0+	5.0+	6.0+
• Security policies for dedi- cated devices	-	-	6.0+
• Verify Apps enforcement (on page 137)	5.0+	5.0+	5.0+
• Hardware security (on page 134)	5.1+	5.1+	5.1+
Account and app management			

• Managed Google Play Accounts enterprise enrollment	N/A	N/A	N/A
• Managed Google Play Account provisioning	5.0+	5.0+	5.0+
• Silent app distribution <i>(on page 124)</i>	N/A	N/A	N/A
• Managed configurations <i>(on page 125)</i>	5.0+	5.0+	5.0+
• Basic store layout <i>(on page 127)</i>	N/A	N/A	N/A
• Private app deployment <i>(on page 127)</i>	-	-	-
• API usage requirements <i>(on page 129)</i>	N/A	N/A	N/A
Device management			
• Runtime permission policy management	6.0+	6.0+	6.0+
• Runtime permission grant state management	6.0+	6.0+	6.0+

<ul style="list-style-type: none"> • Wi-Fi configuration management (on page 140) 	6.0+	6.0+	6.0+
<ul style="list-style-type: none"> • Wi-Fi security management (on page 140) 	N/A	6.0+	6.0+
VPN management (on page 138)	7.0+	7.0+	7.0+
<ul style="list-style-type: none"> • Factory reset protection management 	6.0+	6.0+	6.0+
Device usability			
<ul style="list-style-type: none"> • System update policy (on page 130) 	N/A	6.0+	6.0+
<ul style="list-style-type: none"> • Kiosk mode management (on page 130) 	N/A	N/A	6.0+
<ul style="list-style-type: none"> • Keyguard feature management 	7.0+	N/A	N/A
<ul style="list-style-type: none"> • Cross-profile contact and data management (on page 135) 	7.0+	N/A	N/A

Enroll to Managed Google Play Accounts enterprise

Managed Google Play Accounts enterprise

Learn how enrolling to Managed Google Play Accounts facilitates you to manage your Android devices through BigFix Mobile.

Enroll to Managed Google Play Accounts enterprise is a one-time activity that binds your organization with BigFix Mobile. It allows managed Google Play to manage Android devices enrolled to BigFix Mobile by rolling out policies

and distributing apps. BigFix Mobile assigns a unique service account to your enterprise, and uses this service account to access Google Android Management Service to manage the devices. Through this unique service account, BigFix Mobile tracks the services consumed by your organization.

Once the Managed Google Play Account for an enterprise is created, when devices are provisioned, Managed Google Play Accounts for user are automatically created by default. Apps can be distributed to the enrolled Android devices through Appstore App Policy or [custom policies uploaded](#) through WebUI.

Apps can be managed as follows:

- IT admins can silently provision enterprise user accounts, called managed Google Play accounts. These accounts identify managed users and allow unique, per-user app distribution rules.
- IT admins can use BigFix WebUI to [distribute enterprise applications \(on page 123\)](#) and policies to the enrolled Android devices.
- IT admins can [silently distribute work apps \(on page 124\)](#) on users' Android devices without any user interaction.
- IT admins can [silently set managed configurations \(on page 125\)](#) for any Android app that supports managed configurations.
- Device users can use the managed [Google Play store app \(on page 127\)](#) on their device to install and update work apps.

BigFix Mobile implements Google's APIs at scale, avoiding traffic patterns that could negatively impact customers' ability to manage apps in production environments.

Provisioning Android devices

During device provisioning, a device is enrolled to BigFix Mobile and deployed with the policies from the associated policy group.

You can get Android devices enrolled in BigFix Mobile in the following ways:

- [Provisioning BYOD devices with enrollment URL \(on page 84\)](#): Users can enroll their personally-owned Android devices through the enrollment URL shared by IT admin. This requires LDAP credentials to authenticate.
- [Provisioning BYOD devices using QR code \(on page 88\)](#): Users can enroll their personally-owned Android devices through the QR code shared by IT admin. This does not need any authentication, as the QR code is generated by authenticating through enrollment link.
- [Provisioning fully-managed devices using QR code \(on page 93\)](#): Users can enroll company-owned fully-managed Android devices through QR code shared by IT admin. This does not need any authentication, as the QR code is generated by authenticating through enrollment link.

- [Dedicated Android devices - QR code enrollment \(on page 106\)](#): Users can enroll company-owned dedicated Android devices through QR code shared by IT admin. This does not need any authentication, as the QR code is generated by authenticating through enrollment link.
- [Zero-touch enrollment \(on page 95\)](#): Zero-touch applies to company-owned devices that the users receive directly from the reseller. The devices can be provisioned as fully-managed devices or dedicated devices.



Note: You can only deploy one set of policy through a policy group into Android devices. You cannot directly deploy a policy into Android devices. You must add a policy into a policy group before deploying. If you deploy another policy group onto an Android device, it effectively overrides any previous policies applied.

Before starting the enrollment:

- (Optional) The IT admin must ensure a policy group is created that is assigned to appropriate group and is deployed on the MDM server. All the policies added to a policy group are provisioned on the enrolled Android devices.
 - BYOD Enrollment group - If a policy group is assigned to BYOD Enrollment group and deployed on MCM server, on enrollment (through enrollment URL or QR code) devices get provisioned as devices with policies added in that policy group.
 - Fully Managed QR Enrollment group - If the policy group is assigned to Fully Managed QR Enrollment group and deployed on MCM server, on enrollment (through QR code enrollment or zero-touch provisioning) devices get provisioned with fully-managed or Device Owner policies added in that policy group.
 - Dedicated Device Enrollment group - If the policy group is assigned to this group and deployed on MCM server, on enrollment (through enrollment QR code) company-owned devices get provisioned with Dedicated Device policies added in that policy group.



Important: Ensure to add a policy with [Kiosk mode \(on page 130\)](#) setting to the policy group for dedicated devices. Otherwise, the device works as just a fully-managed device.

- Device users must know the following:
 - The MCM Server enrollment URL, which the BigFix administrator shares through email or chat. The MCM server enrollment URL must be the fully qualified domain name of the MCM server (For example, <https://enroll-mdm.bigfix.com>).
 - The email ID and password associated with a valid Active Directory (AD) credentials. These are the LDAP credentials supplied during Android MCM server installation. If the LDAP was disabled, then the enrollment UI does not prompt for authentication credentials.

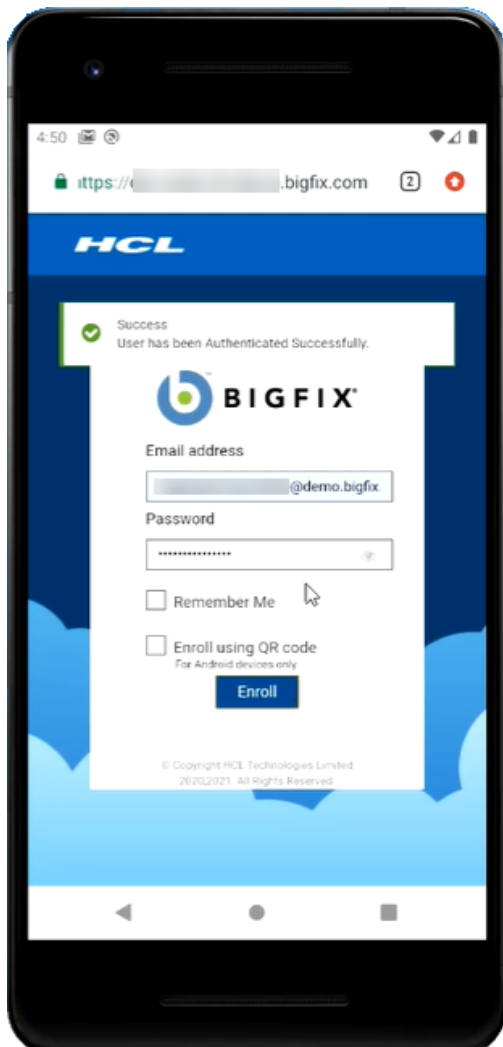
BYOD Android devices - provisioning with the enrollment URL

This page explains provisioning Android devices with the enrollment URL.

Mobile users can enroll their personally-owned Android devices to BigFix Mobile with the enrollment URL. While enrolling, a work profile gets automatically deployed as configured in the associated policy group. After enrolling, the device will have a personal profile and a work profile. Organization can manage the work profile of the enrolled devices through policies in the policy group and through MCM actions. The organization does not have any visibility or control over the personal profile.

To enroll BYOD Android devices to BigFix Mobile and deploy work profile using enrollment link, follow these steps:

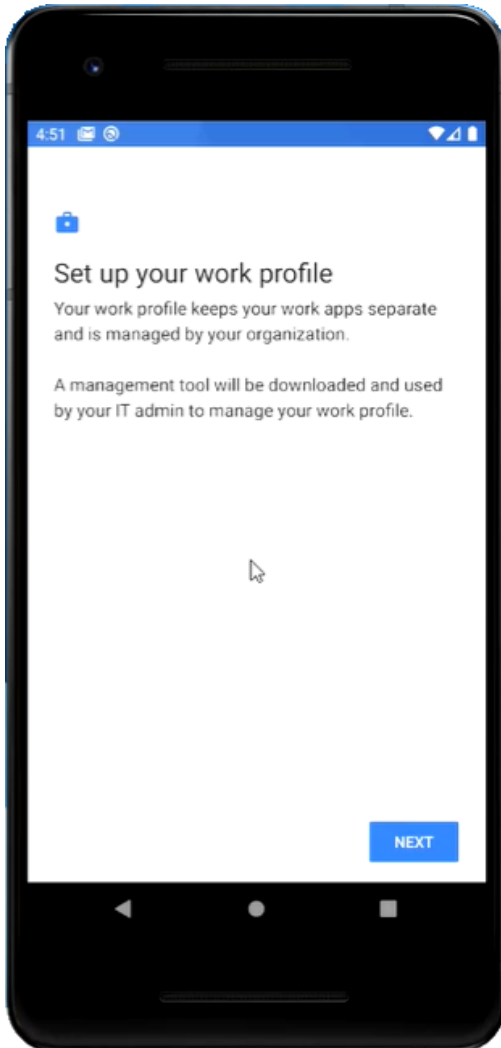
1. On an Android device, open a web browser and enter the MDM server URL (for example www.mdm.bigfix.com/enroll).
2. Enter an email address and password that is associated with a valid AD set of credentials (If LDAP authentication is configured for the MDM server).



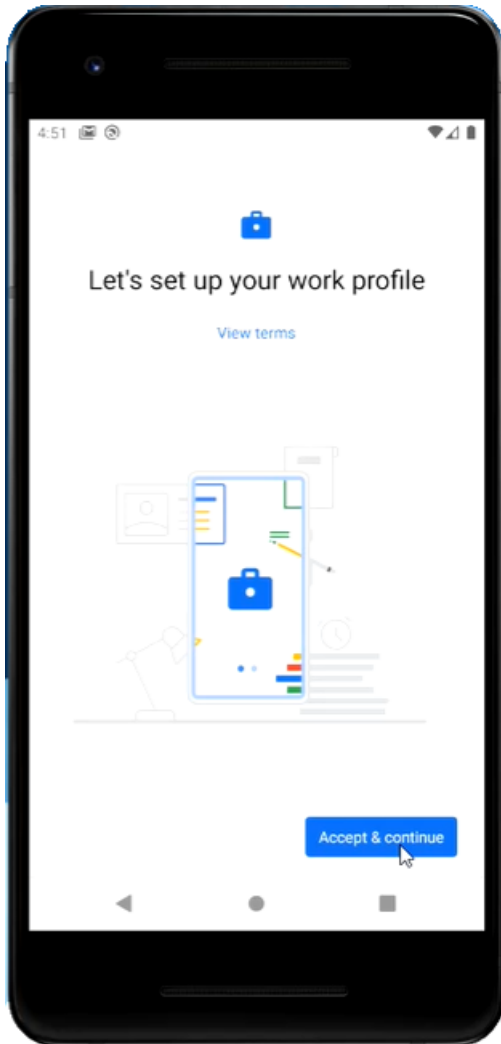
After authenticated successfully, user can see a success message. At this point, the user is redirected to the enrollment URL.

3. Click **Enroll**.

4. In the following screen, click **NEXT**

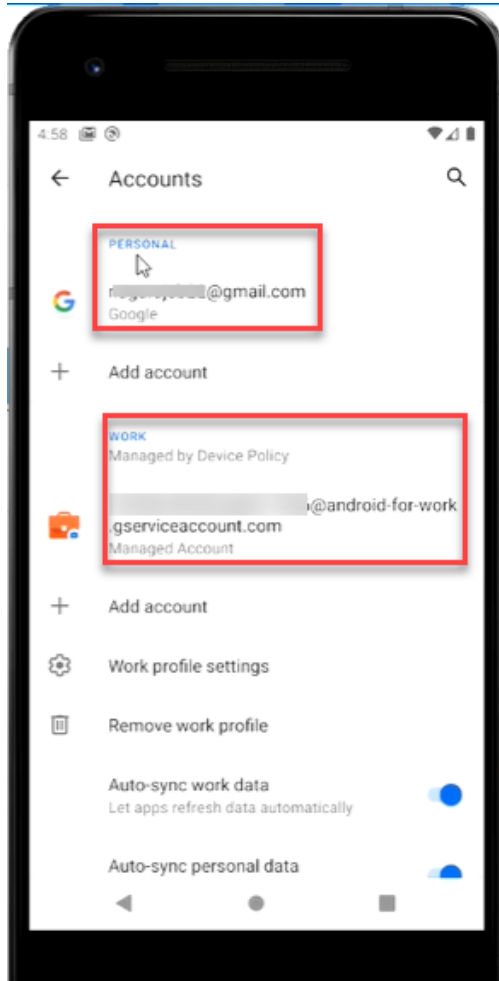


5. In the next screen, to start setting up your work profile, click **Accept & Continue**. Based on the associated policy group, work applications and data are gathered in the device.

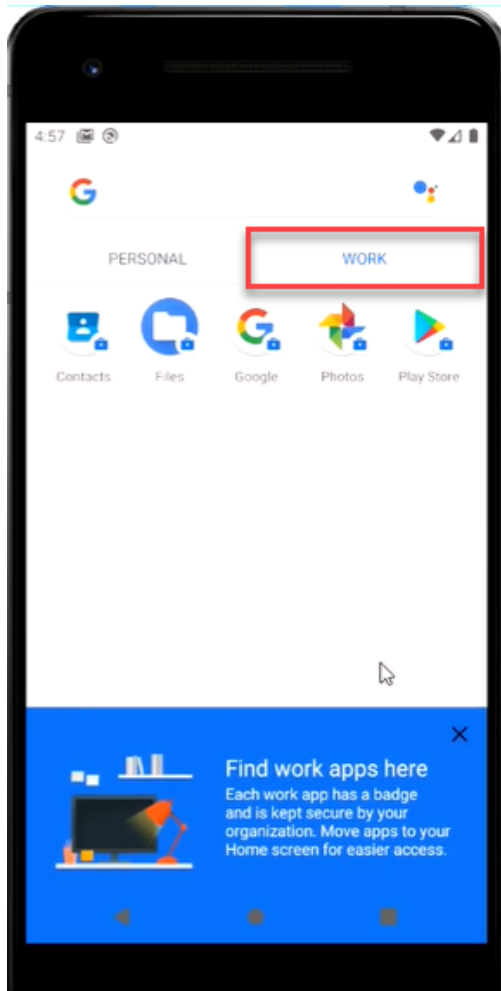


6. Wait for few seconds until the **NEXT** button appears on the screen and then click **NEXT** to continue. Wait for few minutes until the profile gets registered and enrollment is completed.

- After successful installation of MDM on the BYOD devices, navigate to **Personal > Google Accounts**, where you can see two profiles namely Personal and Work.



- Also, you can see two tabs, one for personal and one for work. Under Work profile, you can see only the applications as per the associated policy group.



- In the notification bar, if a policy group was configured to install Appstore apps, you can see “Installing apps from your organization”.
- In the Work profile, if you go to Google Play store, you can see only the apps that are allowed as per the policy, if a policy group was configured to install Appstore apps.

You have successfully enrolled your Android device to BigFix Mobile. The work profile is provisioned based on the policy group deployed onto the device. It might take a few minutes to show up the enrolled device in the WebUI. Once the device is listed under The Device List in WebUI, you can manage the device from here.

BYOD Android devices - QR code enrollment

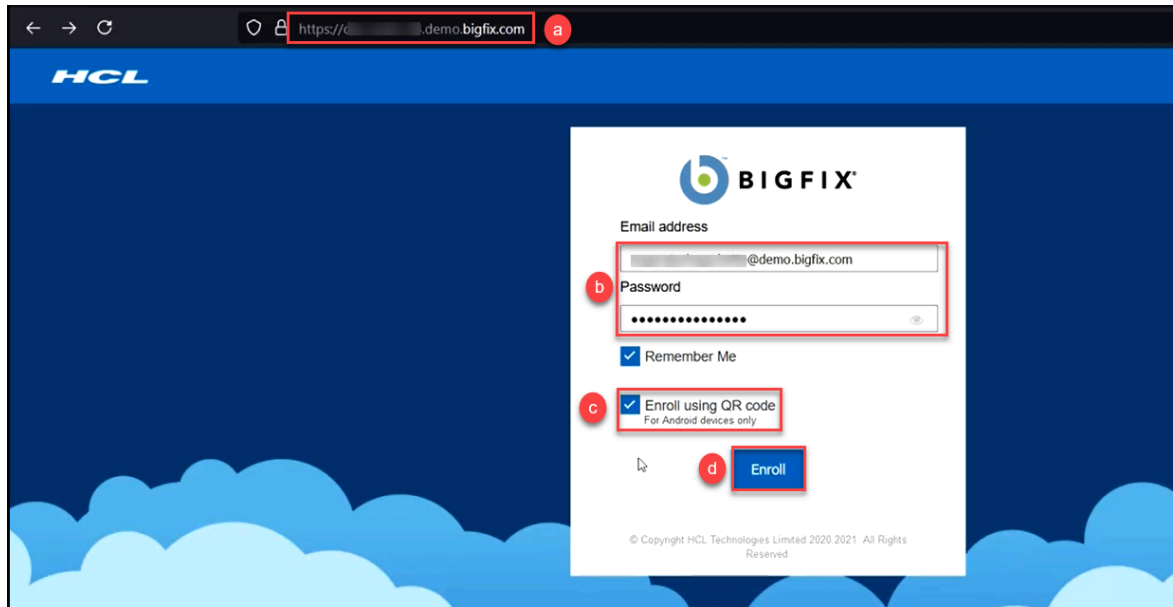
This page explains provisioning BYOD Android devices using a QR code. Mobile users can enroll their personally-owned Android devices to BigFix Mobile with a QR code.

While enrolling, a work profile gets automatically deployed as per the associated policy group. After enrolling, the device will have a personal profile and a work profile. The organization can manage the work profile of the enrolled device through WebUI by applying policies through a policy group and through MDM actions. The organization does not have any visibility or control over the personal profile.

To enroll personally-owned or BYOD Android devices to BigFix Mobile and apply work profile using QR code, follow these steps:

1. Login to the BigFix enrolment URL from another device (other than the Android device that you want to enroll) to generate QR code.

Note: You can generate QR code from a Windows, Apple, or Android device.



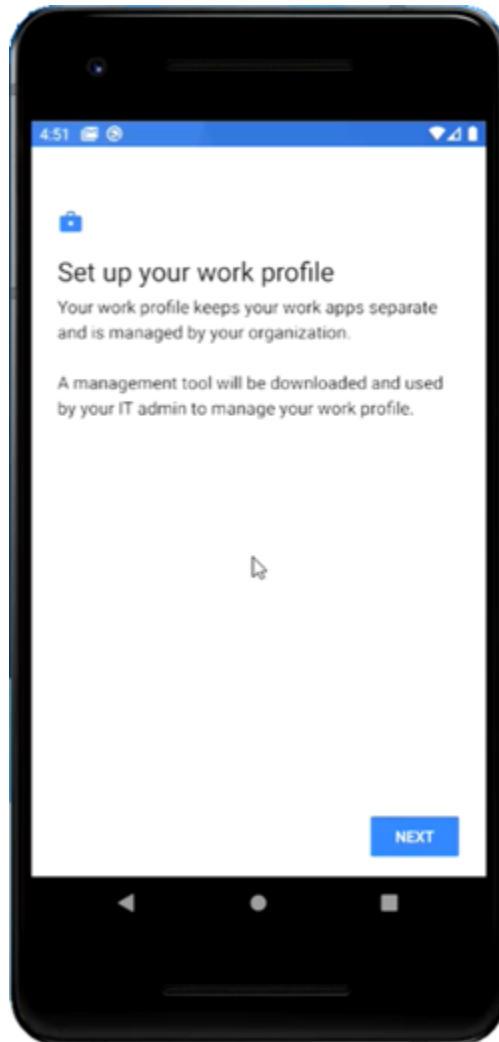
- a. Open the enrollment page where you can see the option to select QR enrollment.
- b. Enter **Email address** and **password** associated with Active Directory.
- c. Select **Enroll using QR code**.
- d. Click **Enroll**.

After successful authentication, you are redirected to the page where QR code is displayed. This QR code is used for enrollment.



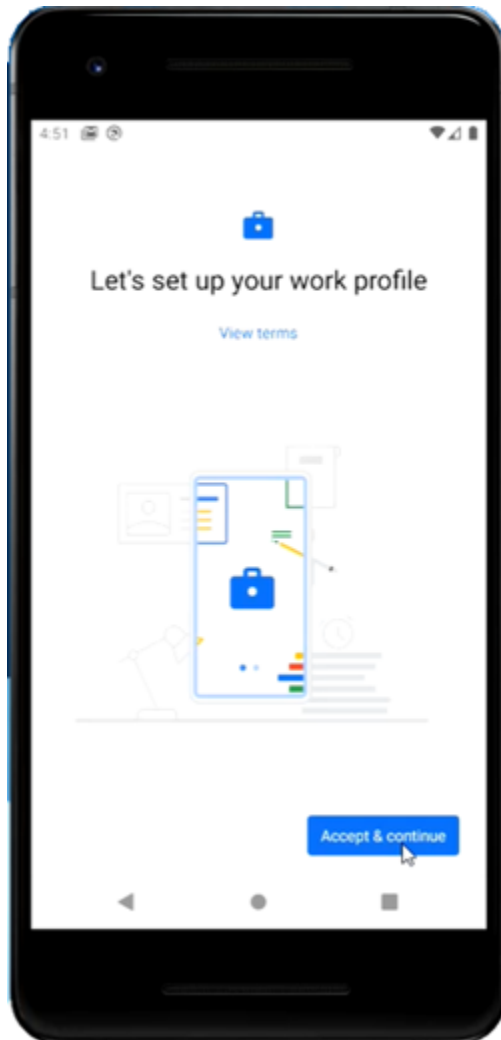
Note: This QR code expires after 15 minutes. If the QR code expires, you cannot enroll your device with that QR code; therefore, you need to regenerate another one.

2. Scan the QR code on the Android device that you want to enroll to complete the enrollment.
 - a. From your Android device navigate to **Settings > Google > Setup and restore > Setup Work profile**.
 - b. Scan the QR code from the device where the QR code is generated or enter the QR code.
 - c. Click **Enroll**. The enrollment process begins.
 - d. In the following screen, click **NEXT**



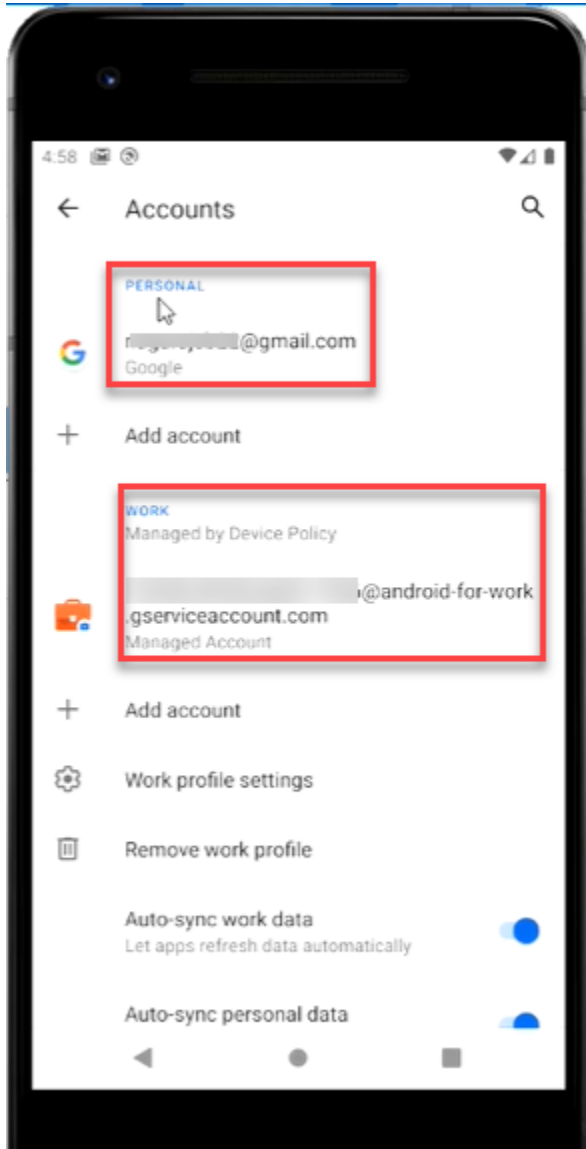
- e. Wait for few seconds until the **NEXT** button appears on the screen and then click **NEXT** to continue. Wait for few minutes until the profile gets registered and enrollment is completed.

- f. In the next screen, to start setting up your work profile, click **Accept & Continue**. Based on the deployed policy group associated with the work profile, work applications and data are deployed to the device.

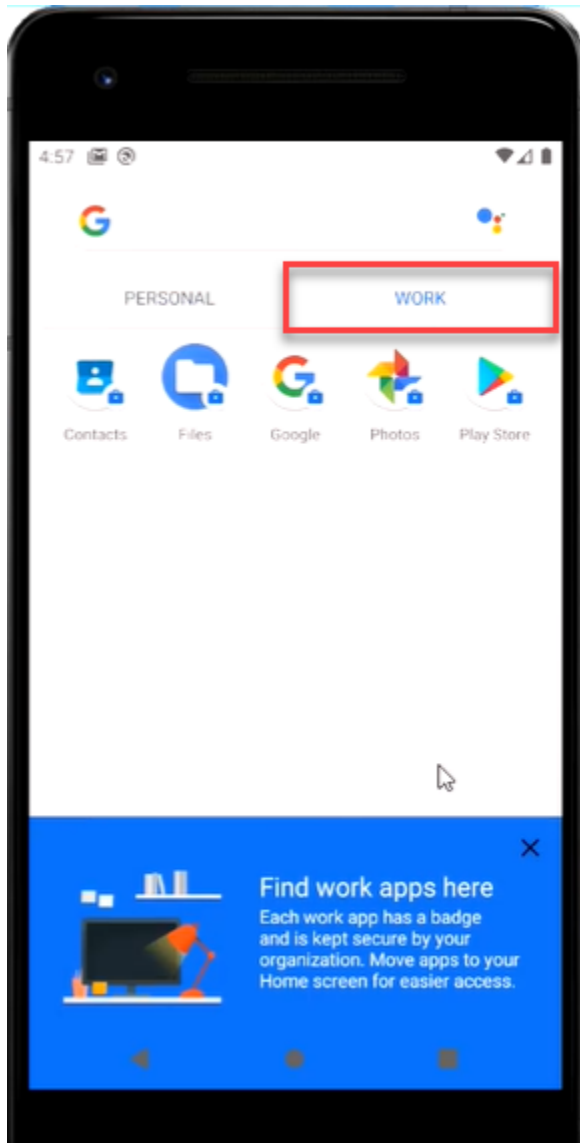


You have successfully enrolled your Android device to the BigFix Mobile and applied work profile. It might take a few minutes for the enrolled device to show up in the WebUI. Once the device is listed under device list in WebUI, you can manage the device from here.

After successfully enrolling the BYOD device to BigFix Mobile, navigate to **Personal > Google Accounts**, you can see two profiles namely Personal and Work.



Also, you can see two tabs, one for personal and one for work. Under Work profile, you can see only the applications as per the applied policy.



- In the notification bar, you can see “Installing apps from your organization” if Appstore apps were part of the policy group that got deployed to the MDM server for BOYD devices.
- In the Work profile, if you go to Google Play store, you can see only the apps that are allowed as per the policy.

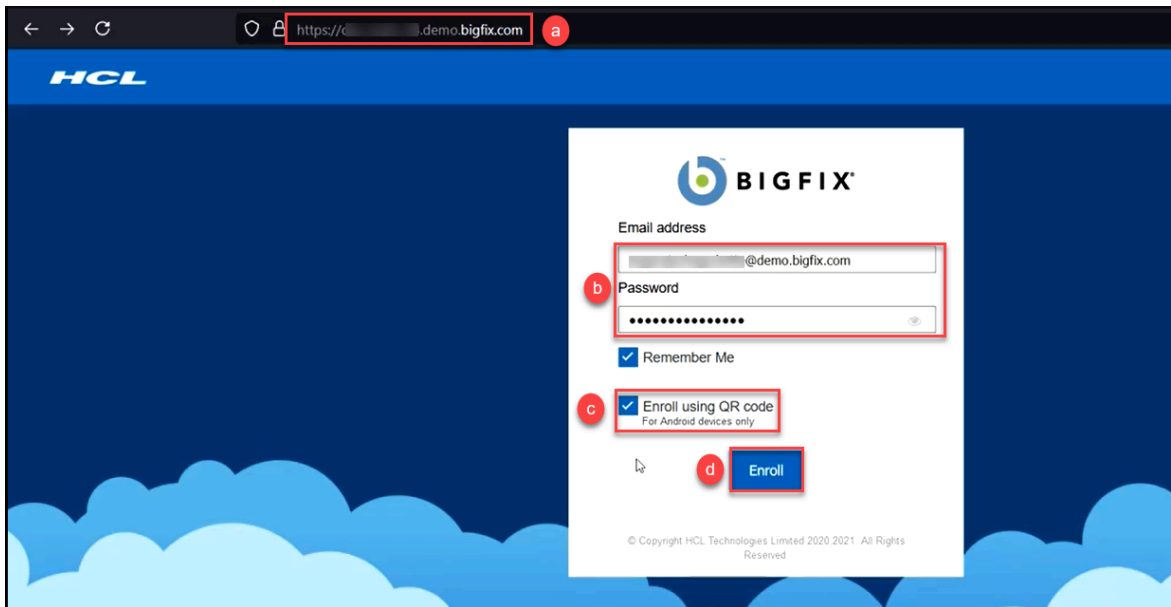
Fully-managed Android devices - QR code enrollment

This page explains provisioning fully-managed Android devices using a QR code.

IT admins can enroll company-owned, factory-reset Android devices to BigFix Mobile with a QR code. While enrolling, a work profile gets automatically deployed via policy groups configured in WebUI. After enrolling, the device gets a work profile. The organization can manage the enrolled devices through policies in the policy group and through MCM actions. To enroll company-owned Android devices to BigFix Mobile and apply fully-managed profile using QR code, follow these steps:

1. Login to the BigFix enrolment URL from another device (other than the Android device that you want to enroll) to generate QR code.

Note: You can generate QR code from a Windows, Apple, or Android device.



- a. Open the enrollment page where you can see the option to select QR enrollment.
- b. Enter **Email address** and **password** associated with Active Directory.
- c. Select **Enroll using QR code**.
- d. Click **Enroll**.

After successful authentication, you are redirected to the page where QR code is displayed. This QR code is used for enrollment.



Note: This QR code expires after 15 minutes. If the QR code expires, you cannot enroll your device with that QR code; therefore, you need to regenerate another one.

2. Scan the QR code on the Android device that you want to enroll and complete the enrollment.
 - a. To open the QR scanner, tap six times on the initial screen of the company-owned, factory-reset Android device.
 - b. Scan the QR code. When prompted, Select Wi-Fi, connect to Internet, and tap **NEXT**.
 - c. On the Set up your device screen, tap **ACCEPT AND CONTINUE**.
 - d. Wait for few seconds until the set up completes. Based on the deployed policy group associated with the fully-managed enrollment, work applications and data are gathered in the device.

You have successfully enrolled your Android device to BigFix Mobile and applied a work profile. It might take a few minutes for the enrolled device to show up in the WebUI. Once the device is listed under device list in WebUI, you can manage the device from here.

To verify, after successfully enrolling the company-owned, fully-managed device to BigFix Mobile, on the enrolled mobile device, navigate to **Settings > Accounts**, device users can see **Managed Account**. Click Managed Account, you can see that it is android for work account.

In WebUI, the device document of the enrolled device shows management mode to be DEVICE_OWNER.

Zero-touch enrollment

BigFix Mobile supports zero-touch enrollment of company-owned Android devices. Android zero-touch enrollment is a deployment method suitable for corporate-owned Android devices. Zero-touch enrollment is a simple, fast, and secure way to configure management settings online. Organizations can get the associated devices shipped with enforced management settings, so that employees can get started immediately on booting up the devices.

The following are the pre-requisites to apply zero-touch provisioning:

- The devices must be company-owned Android devices
- The devices must be running Android 8.0 and above
- The devices must be purchased from a reseller partner
- A zero-touch account must be created by an authorized reseller partner
- Enterprise must be registered to create zero-touch configurations

Supported management modes

- Corporate-Owned Fully-managed devices - Device Owner
- Corporate-Owned Single-Use (COSU) devices - Dedicated Device

Zero-touch enrollment is a streamlined process to provision Android devices for enterprise management. In this method, IT admin preconfigures and provisions the Android devices for enterprise management. Once the configuration is done, when the device user turns on the device for the first time and connects to the Internet, the device checks if it is assigned with an enterprise configuration. If yes, the device initiates the fully-managed or dedicated device provisioning method as per the configuration and downloads the correct device policy controller app. The device automatically gets enrolled to BigFix Mobile and receives pre-configured settings. After successful enrollment, the device is listed in the WebUI device list for further management.



Note: Once the device is enrolled, the user cannot unenroll the device. Only the IT admin can unenroll the device using the WebUI.

To configure and enroll Android devices through zero-touch enrollment method, complete the following steps:

A. Get access to a zero-touch account

1. Associate a Google Account with your corporate email. To get access to the zero-touch portal, the IT admin must associate the corporate email ID with Google account. Refer to [Zero-touch enrollment for IT admins](#) to know more about associating corporate email with G-mail.
2. Once approved by Google, to create a zero-touch account using the corporate Google account, share the mail ID with the reseller. The reseller then provides access to the zero-touch portal (<https://partner.android.com/zerotouch>).

B. Configure through zero-touch portal

Using the zero-touch portal, preconfigure the device.

C. Configure zero-touch method through Admin Configuration

1. Log in to **Admin Configuration** page.
2. Configure zero-touch method.

Method	Description
Manual zero-touch configuration (on page 97) without user authentication	<ul style="list-style-type: none"> ◦ Manually associate the devices and the profile via zero-touch portal. ◦ User is not authenticated on enrolling the device
Manual zero-touch configuration (on page 97) with user authentication	<ul style="list-style-type: none"> ◦ Manually associate the devices and the profile via zero-touch portal ◦ User is authenticated via single-sign on URL while enrolling the device.
Automatic zero-touch configuration (on page 98) without user authentication	<ul style="list-style-type: none"> ◦ Directly associate the zero-touch account to BigFix Mobile ◦ User is not authenticated on enrolling the device
Automatic zero-touch configuration (on page 98) with user authentication	<ul style="list-style-type: none"> ◦ Directly associate the zero-touch account to BigFix Mobile ◦ IT admin can configure a sign-in URL, to authenticate device user to proceed with enrollment. Unauthorized users are restricted to proceed with device enrollment.

3. If you have selected manual configuration, ensure the configurations are applied. In case of automatic configuration, ensure your zero-touch account is linked to BigFix Mobile.
4. Verify the associated enrollment profile, devices, and other enrollment information.

Enroll the device

Zero-touch configuration must be ready.

Once the IT admin completes the zero-touch configuration, device users can enroll Android devices.

To enroll an Android device through zero-touch enrollment, complete the following steps.

1. Turn on the device and perform the basic device settings.
2. Connect to the Internet.
 - The device starts to receive updates and other information.
 - The device displays a message stating that the device will be managed by your organization. It also displays the configured support information and custom message.
3. Proceed with the flow and accept the terms and conditions when prompted. The enrollment process starts and the device gets registered.
4. In case of [user authenticated zero-touch enrollment \(on page 104\)](#), sign-in URL is displayed. Enter valid credentials to proceed with the enrollment process.

On successful completion of the enrollment, you can see the notification about the enrollment. The device is set up with all apps, profile, and other configurations according to the associated enrollment profile.

Manual zero-touch configuration

Read this page to learn how to set up manual zero-touch configuration.

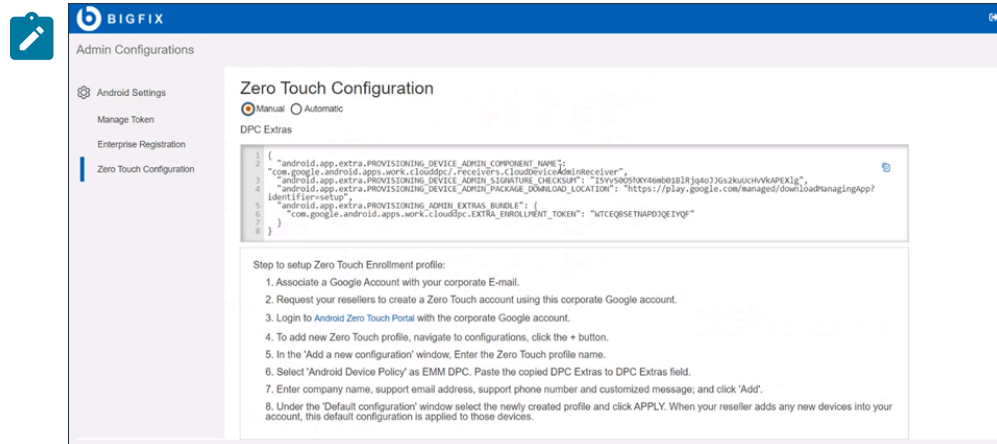
Ensure Enterprise ID is created.

A. Configure manual zero-touch enrollment

1. Log in to Android zero-touch portal with the corporate Google account (<https://partner.android.com/zerotouch>).
2. To add new zero-touch profile, navigate to configurations, click the **+** button.
3. In the **Add a new configuration** window, enter the zero-touch profile name, company name, support email address, support phone number, and customized message.
4. Select **Android Device Policy** as EMM DPC.
5. In the **DPC Extras** field, enter the copied DPC Extras values.



Note: The DPC Extras is available at **BigFix MCM > Admin configurations > Zero Touch Configuration**. In **Zero Touch Configuration** panel, select **Manual** and copy the DPC Extra value. If the **DPC Extra** field shows empty, the IT admin must request a token, upload the token file in the **Manage Token** page (by clicking **Manage Token** on the left panel) and register the token to BigFix Mobile. After performing this, the DPC Extra value appears.



6. Under the **Default configuration** window, select the newly created profile and click **Apply**. When your reseller adds any new device into your account, this default configuration is applied to the devices.
7. Click **Add**. The configuration appears in the **Zero Touch Configuration** window.

B. Apply the configuration to the devices

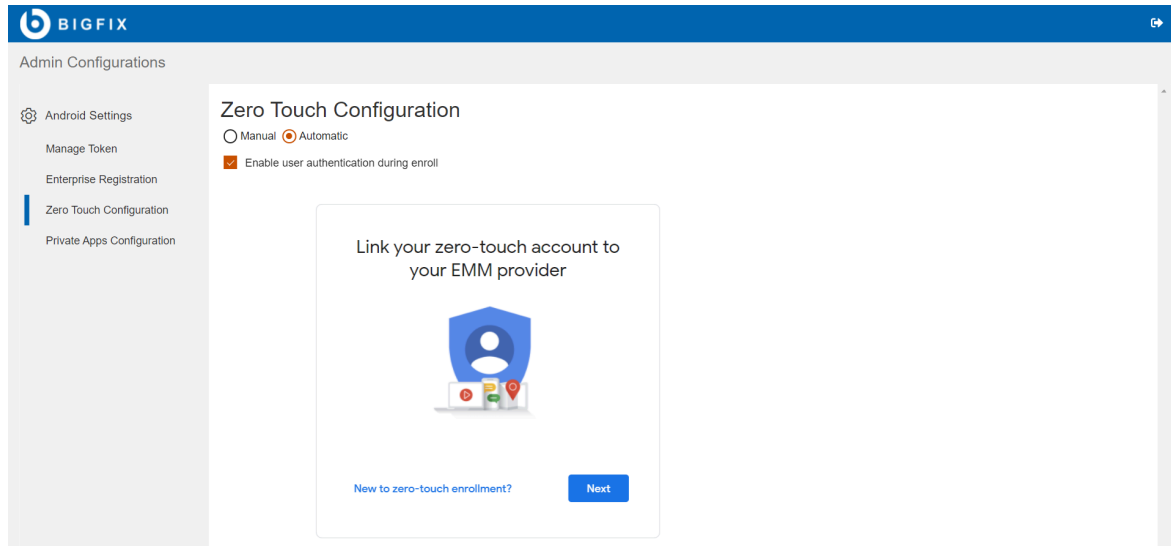
1. In the **Zero Touch Configuration** window, select the configuration and click **Apply**. The configuration becomes default for all upcoming devices.
2. Go to **Devices** and select the device on which you want the configuration needs to be applied.
3. Select the configuration.
4. In the **Update device** dialog box, click **Update**.

Result: The IT Admin can assign the configuration to all future devices or selected devices. Once the device is tuned on, connected to the internet, a the basic set up is completed, a message stating that the device will be managed details appears. Once the user accepts the policy, a work profile in the device is created.

Automatic zero-touch configuration

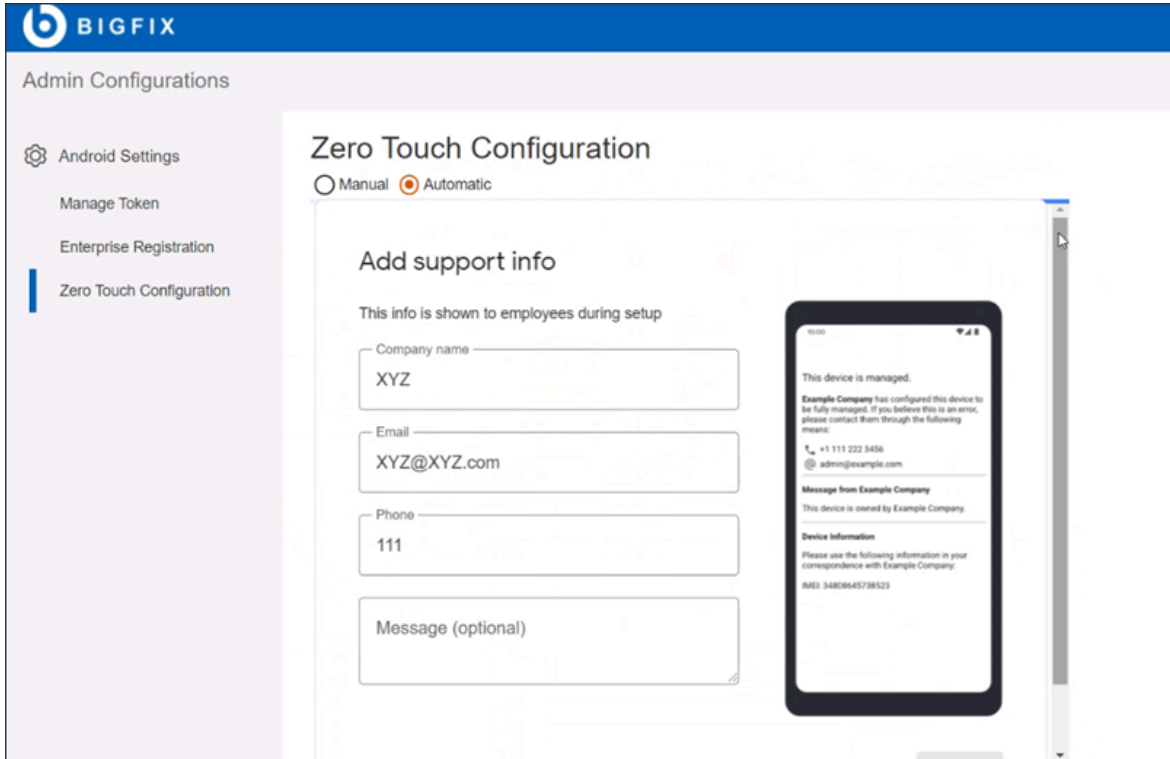
To apply automatic zero-touch configuration, the IT admin must configure the BigFix Mobile directly with the reseller's zero-touch portal.

1. Log in to **Admin Configurations**.
2. From the navigation pane, select **Zero Touch Configuration**. The Zero Touch Configuration page appears.
3. Select **Automatic**.

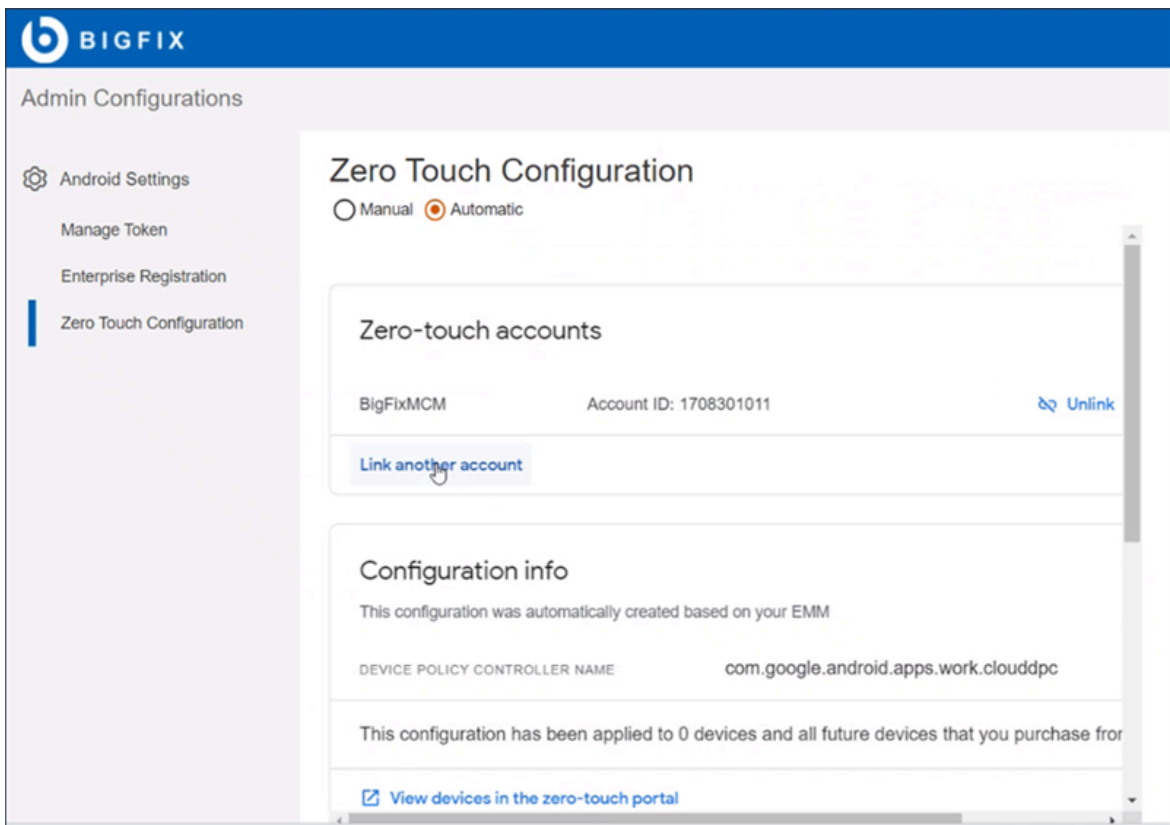


4. Enable user authentication during enroll:

- If this check box is selected, while enrolling the device, the device user is authenticated via sign-in URL with valid LDAP credentials. If the device user enters invalid credentials in the sign-in URL, the user cannot proceed with the enrollment process.
 - If this check box is not selected, the device user can complete enrollment without getting authenticated.
5. Click **Next** and sign in to the Zero Touch portal account. If already signed in to the Zero Touch portal account, then select the account.
 6. Select the listed devices to link with BigFix Mobile.
 7. Click **Link** and click **Next**.
 8. Enter the configuration name, organization name, support email ID, support phone number, and custom message.



9. Click **Save**.



- To unlink the devices, click **Unlink**. Once the account is unlinked, the zero-touch profile is removed.
- To link more accounts, click **Link another account**.

Automatic zero-touch configuration is set up and the selected devices are linked to BigFix Mobile.

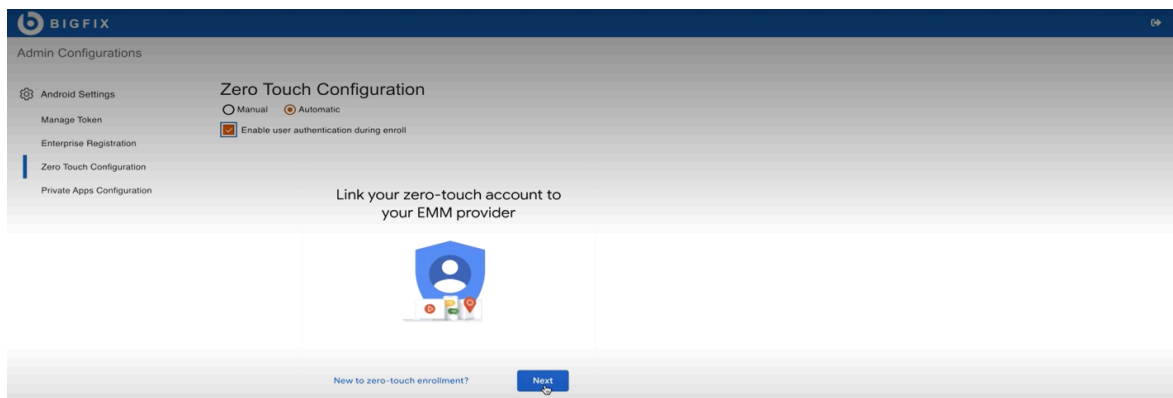
The selected devices are ready for enrollment. Device users can proceed with [enrollment \(on page 97\)](#).

Direct zero-touch configuration

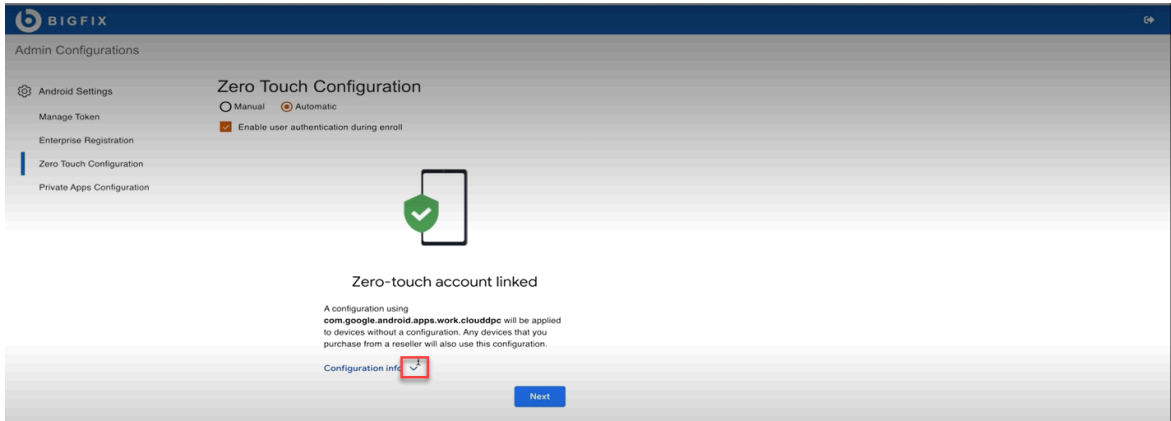
<to be updated>

With direct zero-touch configuration IT admins can log into Admin Configuration and set up zero-touch devices using the [zero-touch iframe](#).

1. Log in to Admin Configuration and select **Zero Touch Configuration**.
2. From the Zero Touch Configuration window, do the following:

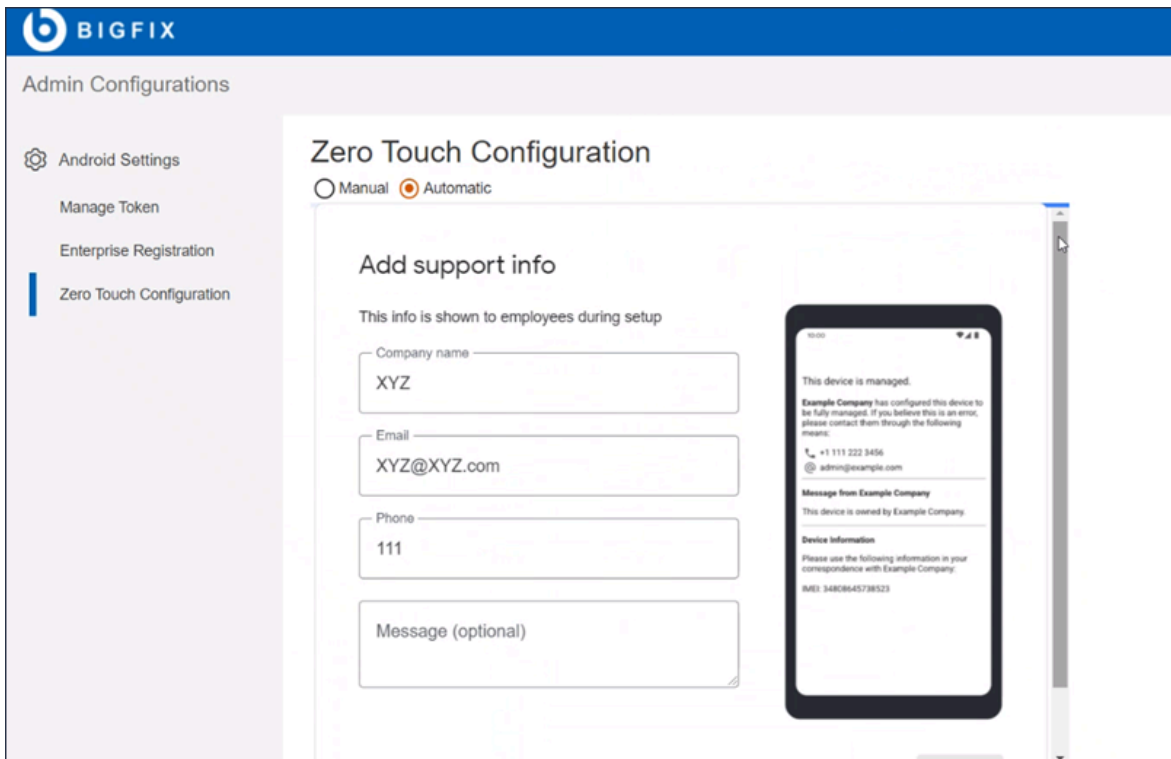


3. Select Manual or Automatic.
4. To authenticate the user during enrollment, select **Enable user authentication during enroll**.
5. Click **Next**.
6. On the next screen, select your zero-touch account. The selected zero-touch account is listed under Choose accounts to link (within Google iFrame). It displays the account ID and the number of associated devices.
7. To link your zero-touch account to BigFix Mobile, select the account and click **Link**. After successfully linking the account, the following screen is displayed. Click **Configuration Info** to verify the configuration details.

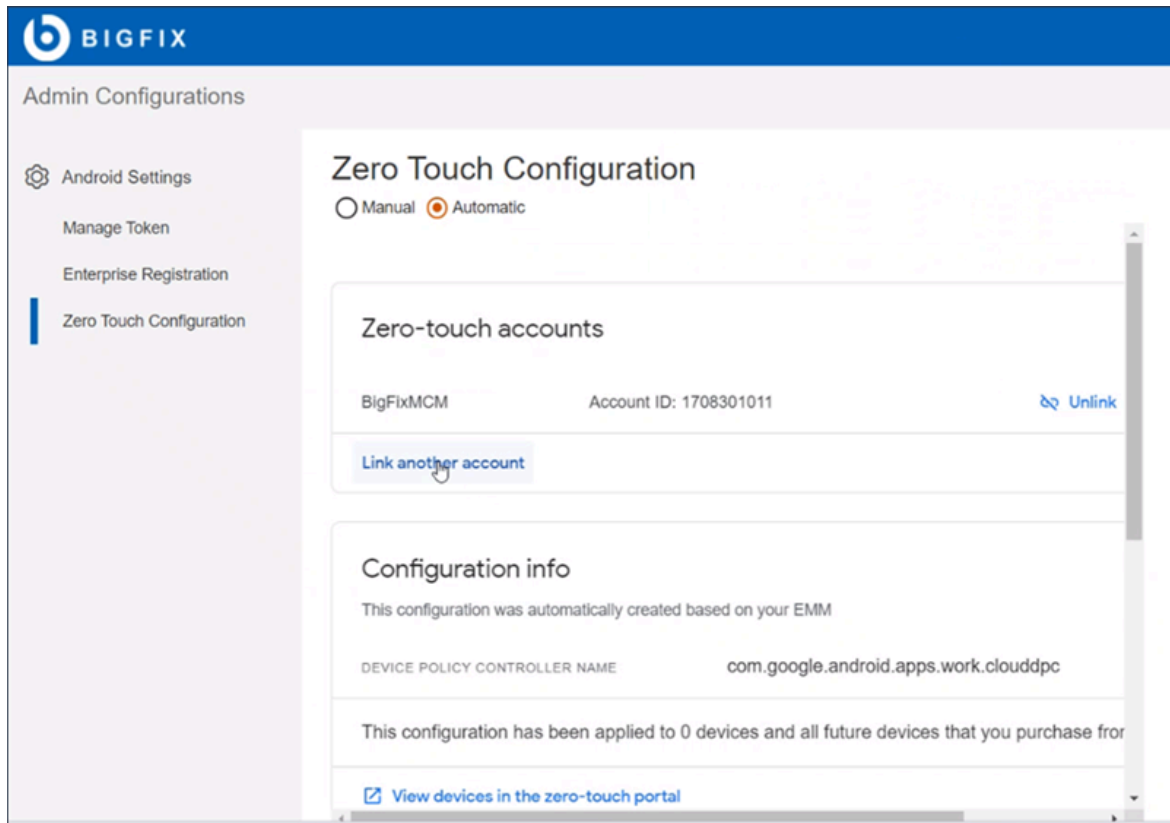


8. Click **Next**.

9. Enter the support information; company name, Email, Phone, and custom message. The information provided here is displayed on the device on enrollment.



10. Click **Save**.



The associated devices are linked to the zero-touch account, mapped to the default enrollment profile, and are ready for advanced zero-touch provisioning.



Note: Click **Unlink** to unlink the devices. Once the account is unlinked, the zero-touch profile is removed. Click **Link another account** to link more accounts.

The users can enroll the associated devices. Once an associated device is tuned on and connected to the internet:

- The user is guided through initial enrollment setup.
- The support information and the custom message are displayed on the device screen while progressing with the enrollment process.
- Google Chrome Terms and Conditions are displayed. Device user needs to accept them to open the Sign-in URL.
- Device user needs to authenticate the sign-in URL with valid credentials and click Enroll.
- Once authenticated successfully, the device user can proceed with the rest of the zero-touch enrollment process.
- After the enrollment process is complete, a work profile in the device is created.

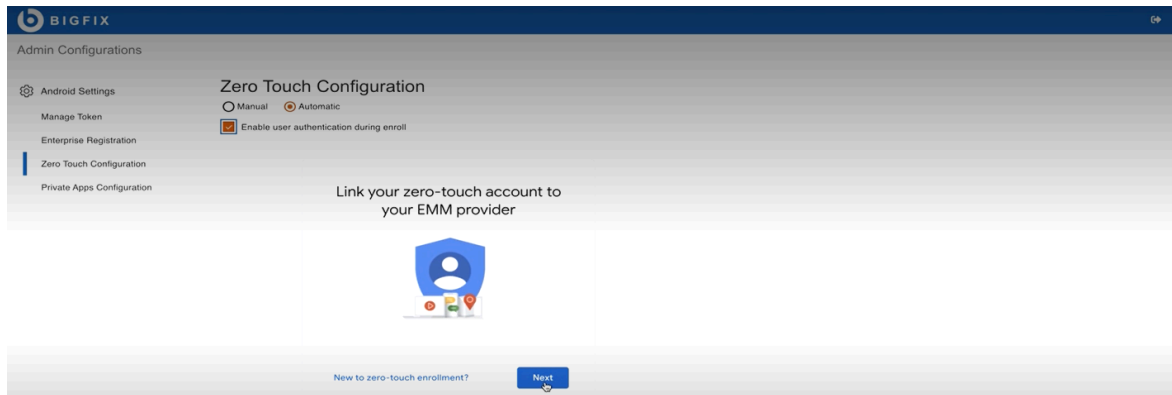
Overall, the enrollment experience is same as the normal zero-touch enrollment except that the user is authenticated via the sign-in URL.

User-authenticated zero-touch enrollment configuration

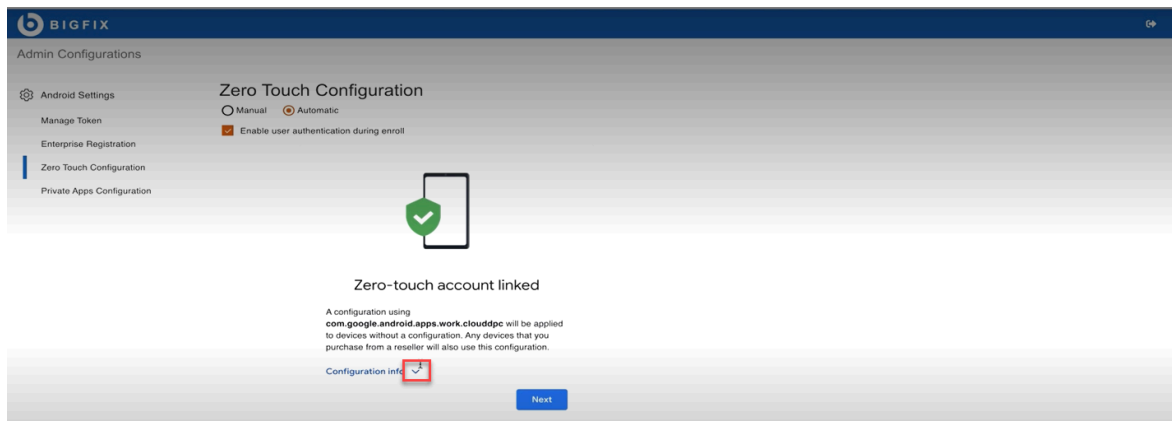
IT admin can configure a [sign-in URL](#), to authenticate device user to proceed with zero-touch enrollment.

Unauthorized users are restricted to proceed with device enrollment. This can be done through Manual or automatic zero-touch enrollment.

1. Log in to Admin Configuration and select **Zero Touch Configuration**.
2. From the Zero Touch Configuration window, do the following:



3. Select **Automatic**.
4. Select **Enable user authentication during enroll**.
5. Click **Next**.
6. On the next screen, select your zero-touch account. The selected zero-touch account is listed under Choose accounts to link (within Google iFrame). It displays the account ID and the number of associated devices.
7. To link your zero-touch account to BigFix Mobile, select the account and click **Link**. After successfully linking the account, the following screen is displayed. Click **Configuration Info** to verify the configuration details.



8. Click **Next**.
9. Enter the support information; company name, Email, Phone, and custom message. The information provided here is displayed on the device on enrollment.

The screenshot shows the 'Zero Touch Configuration' page in the BigFix Admin Configurations interface. The 'Automatic' radio button is selected. The 'Add support info' section contains the following fields:

- Company name: XYZ
- Email: XYZ@XYZ.com
- Phone: 111
- Message (optional):

To the right, a preview of a mobile device screen displays the following information:

10:00

This device is managed.

Example Company has configured this device to be fully managed. If you believe this is an error, please contact them through the following means:

- +1 111 222 3456
- admin@example.com

Message from Example Company

This device is owned by Example Company.

Device Information

Please use the following information in your correspondence with Example Company:

IMEI: 3480845738523

10. Click **Save**.

The screenshot shows the 'Zero Touch Configuration' page in the BigFix Admin Configurations interface. The 'Automatic' radio button is selected. The 'Zero-touch accounts' section displays the following information:

BigFixMCM Account ID: 1708301011 [Unlink](#)

[Link another account](#)

The 'Configuration info' section displays the following information:

This configuration was automatically created based on your EMM

DEVICE POLICY CONTROLLER NAME com.google.android.apps.work.clouddpc

This configuration has been applied to 0 devices and all future devices that you purchase from

[View devices in the zero-touch portal](#)

The associated devices are linked to the zero-touch account, mapped to the default enrollment profile, and are ready for advanced zero-touch provisioning.



Note: Click **Unlink** to unlink the devices. Once the account is unlinked, the zero-touch profile is removed. Click **Link another account** to link more accounts.

The users can enroll the associated devices. Once an associated device is tuned on and connected to the internet:

- The user is guided through initial enrollment setup.
- The [Support information \(on page 104\)](#) and the custom message are displayed on the device screen while progressing with the enrollment process.
- Google Chrome Terms and Conditions are displayed. Device user needs to accept them to open the Sign-in URL.
- Device user needs to authenticate the sign-in URL with valid credentials and click Enroll.
- Once authenticated successfully, the device user can proceed with the rest of the zero-touch enrollment process.
- After the enrollment process is complete, a work profile in the device is created.

Overall, the enrollment experience is same as the normal zero-touch enrollment except that the user is authenticated via the sign-in URL.

Dedicated Android devices - QR code enrollment

Read this page to learn provisioning company-owned Android devices with dedicated device mode using a QR code.

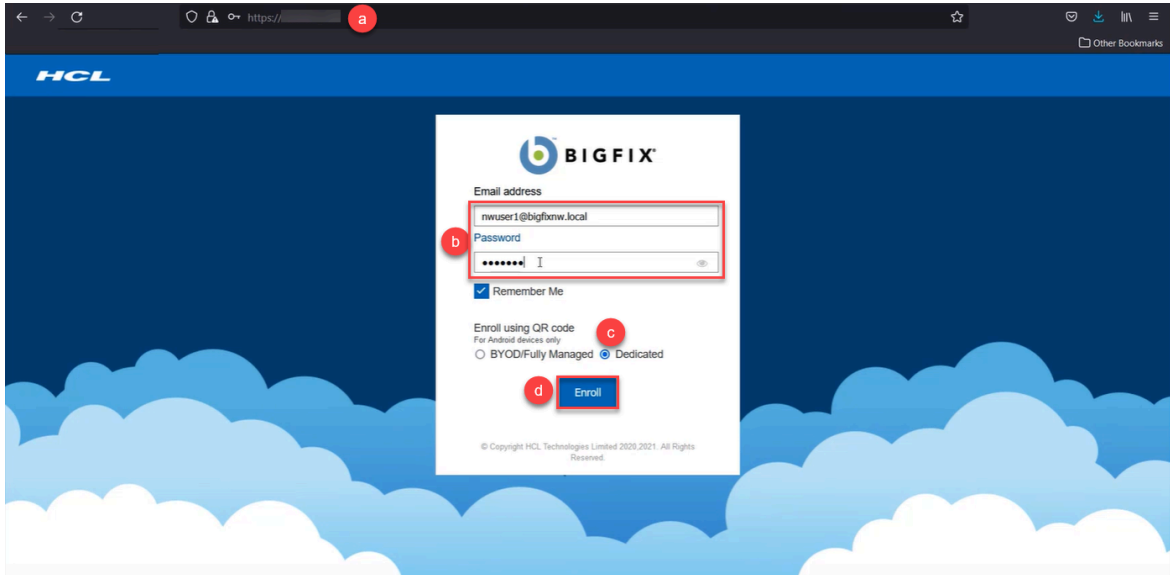
Ensure a Policy Group is created with assigned group as dedicated device and is deployed on to the Android MDM Server for the devices to pick up the dedicated device policy on enrollment.

IT admins can enroll company-owned, factory-reset Android devices to BigFix Mobile with a QR code. While enrolling, a work profile gets automatically deployed through policy groups configured in WebUI. After enrolling, the device gets the work apps and data as per the configured policy. The organization can manage the enrolled devices through policies in the policy group and through MCM actions. To enroll company-owned Android devices to BigFix Mobile and apply dedicated device profile using QR code, follow these steps:

1. Login to the BigFix enrolment URL from another device (other than the Android device that you want to enroll) to generate QR code.



Note: You can generate QR code from a Windows, Apple, or Android device.



- a. Open the enrollment page where you can see the option to select QR enrollment.
- b. Enter **Email address** and **password** associated with Active Directory.
- c. To enroll as a dedicated device, select **Dedicated**.
- d. Click **Enroll**.

After successful authentication, you are redirected to the page where QR code is displayed. This QR code is used for enrollment.



Note: This QR code expires after 15 minutes. If the QR code expires, you cannot enroll your device with that QR code; therefore, you need to regenerate another one.

2. Scan the QR code on the Android device that you want to enroll and complete the enrollment.
 - a. To open the QR scanner, tap six times on the initial screen of the company-owned, factory-reset Android device.
 - b. Scan the QR code. When prompted, Select Wi-Fi, connect to Internet, and tap **NEXT**.
 - c. On the Set up your device screen, tap **ACCEPT AND CONTINUE**.
 - d. Wait for few seconds until the set up completes. Based on the deployed policy group associated with the dedicated device enrollment, work applications and data are gathered in the device.

You have successfully enrolled your Android device to BigFix Mobile as a dedicated device. The device gets apps and policies as per the deployed policy group. It might take a few minutes for the enrolled device to show up in the WebUI. Once the device is listed under device list in WebUI, you can manage the device from here.

To verify, after successfully enrolling the company-owned, dedicated device to BigFix Mobile, on the enrolled mobile device, on the top right corner, tap... and select **Accounts**; device users can see **Managed Account**. Tap Managed Account, you can see that it is android for work account.

In WebUI, the device document of the enrolled device shows the Enrollment Type as DEDICATED_DEVICE.

Dedicated Android devices - Zero-touch enrollment

This page explains provisioning dedicated Android devices through zero-touch enrollment. BigFix Mobile supports zero-touch enrollment of dedicated Android devices. Android zero-touch enrollment offers seamless deployment of dedicated devices.

To apply zero-touch enrollment, the IT admin must have the following:

- An Android device running Android 8.0 and above, purchased from a reseller partner.
- Access to BigFix Mobile.
- A zero-touch account created by an authorized reseller partner.
- Enterprise must be registered to create zero-touch configurations.

Zero-touch applies to devices that are received by the user directly from the reseller. The IT admin, preconfigures and provisions the devices for enterprise management. After receiving the device, when the device user turns it on, connects it to the internet, and follows certain set up instructions, the device automatically gets enrolled to BigFix Mobile and pre-configured settings are applied. The device is listed in WebUI device list for further management. Once the device is enrolled, the user cannot unenroll the device. The IT admin can unenroll the device using the WebUI.

Zero-touch configuration can be applied in two ways; manual and automatic. Enterprise must be registered to create zero-touch configurations. The IT admin must request a token, upload the files (encrypted file in `.enc` format) and then register an enterprise in the enterprise registration portal. This step is mandatory to receive the DPC Extra value during manual configuration and perform other actions during automatic configuration.

Manual zero-touch configuration

To apply manual zero-touch configuration, the IT admin must have access to the reseller's zero-touch portal. To get access to the zero-touch portal, the IT admin must associate the corporate email ID with Google account and once approved by Google, the IT admin needs to share the Google email with the reseller. The reseller then provides access to the zero-touch portal (<https://partner.android.com/zerotouch>). Using the zero-touch portal, the IT admin can preconfigure the device.

Refer to [Zero-touch enrollment for IT admins](#) to know more about associating corporate email with Gmail.

The IT Admin can assign the configuration to all future devices or selected devices.

Steps to configure manual zero-touch enrollment:

1. Associate a Google Account with your corporate email.
2. Request your reseller to create a zero-touch account using the corporate Google account.
3. Log in to Android zero-touch portal with the corporate Google account (<https://partner.android.com/zerotouch>).

4. To add new zero-touch profile, navigate to configurations, click the **+** button.
5. In the **Add a new configuration** window, enter the zero-touch profile name, company name, support email address, support phone number, and customized message.
6. Select **Android Device Policy** as EMM DPC.
7. In the **DPC Extras** field, enter the copied DPC Extras values.



Note: The DPC Extras is available at **BigFix MCM > Admin configurations > Zero Touch Configuration**. In **Zero Touch Configuration** panel, select **Manual** and copy the DPC Extra value. If the **DPC Extra** field shows empty, the IT admin must request a token, upload the token file in the **Manage Token** page (by clicking **Manage Token** on the left panel) and register the token to BigFix Mobile. After performing this, the DPC Extra value appears.

The screenshot shows the BigFix Admin Configurations interface. On the left, there is a navigation menu with options: Android Settings, Manage Token, Enterprise Registration, and Zero Touch Configuration (which is currently selected). The main content area is titled 'Zero Touch Configuration' and has two radio buttons: 'Manual' (selected) and 'Automatic'. Below this is a 'DPC Extras' field containing the following code:

```

1 {
2   "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
3   "com.google.android.apps.work.cloud/pc/.receivers.CloudDeviceAdminReceiver",
4   "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "T5Vv5805hXy46ab01B1Rj4o7JGz2kuUcHvKvAPEXig",
5   "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://play.google.com/managed/download/ManagingApp?
6   identifier=setup",
7   "android.app.extra.PROVISIONING_DEVICE_ADMIN_EXTRAS_BUNDLE": {
8     "com.google.android.apps.work.cloud/pc.EXTRA_ENROLLMENT_TOKEN": "NTCEQBSETHAPD7QEIVQF"
9   }
10 }

```

Below the code is a section titled 'Step to setup Zero Touch Enrollment profile:' with the following steps:

1. Associate a Google Account with your corporate E-mail.
2. Request your resellers to create a Zero Touch account using this corporate Google account.
3. Login to [Android Zero Touch Portal](#) with the corporate Google account.
4. To add new Zero Touch profile, navigate to configurations, click the **+** button.
5. In the 'Add a new configuration' window, Enter the Zero Touch profile name.
6. Select 'Android Device Policy' as EMM DPC. Paste the copied DPC Extras to DPC Extras field.
7. Enter company name, support email address, support phone number and customized message; and click 'Add'.
8. Under the 'Default configuration' window select the newly created profile and click APPLY. When your reseller adds any new devices into your account, this default configuration is applied to those devices.

8. Under the **Default configuration** window, select the newly created profile and click **Apply**. When your reseller adds any new device into your account, this default configuration is applied to the devices.
9. Click **Add**. The configuration appears in the **Zero Touch Configuration** window.

Apply the configuration to the devices:

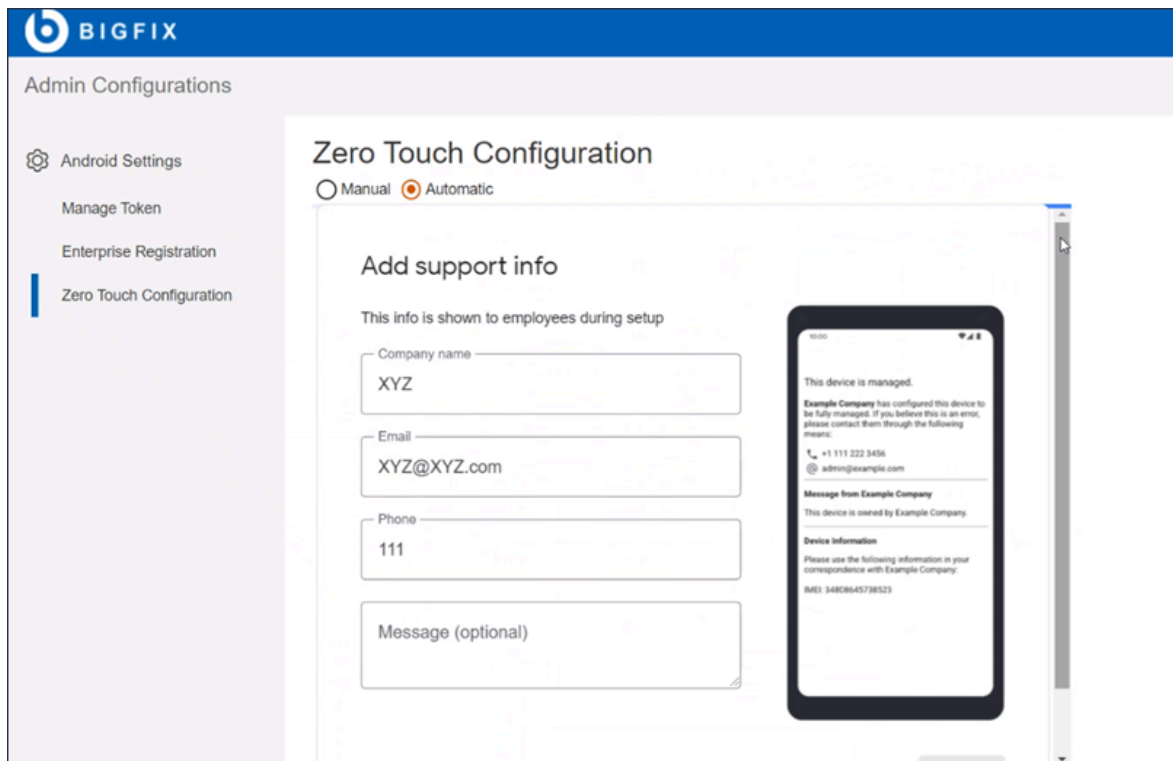
1. In the **Zero Touch Configuration** window, select the configuration and click **Apply**. The configuration becomes default for all upcoming devices.
2. Go to **Devices** and select the device on which you the configuration needs to be applied.
3. Select the configuration.
4. In the **Update device** dialog box, click **Update**.

Result: Once the device is turned on, connected to the Internet, the basic setup is completed, the message "the device will be managed..." appears. Once the user accepts the policy, a work profile in the device is created.

Automatic zero-touch enrollment

To apply automatic zero-touch configuration, the IT admin must configure the BigFix Mobile directly with the reseller's zero-touch portal.

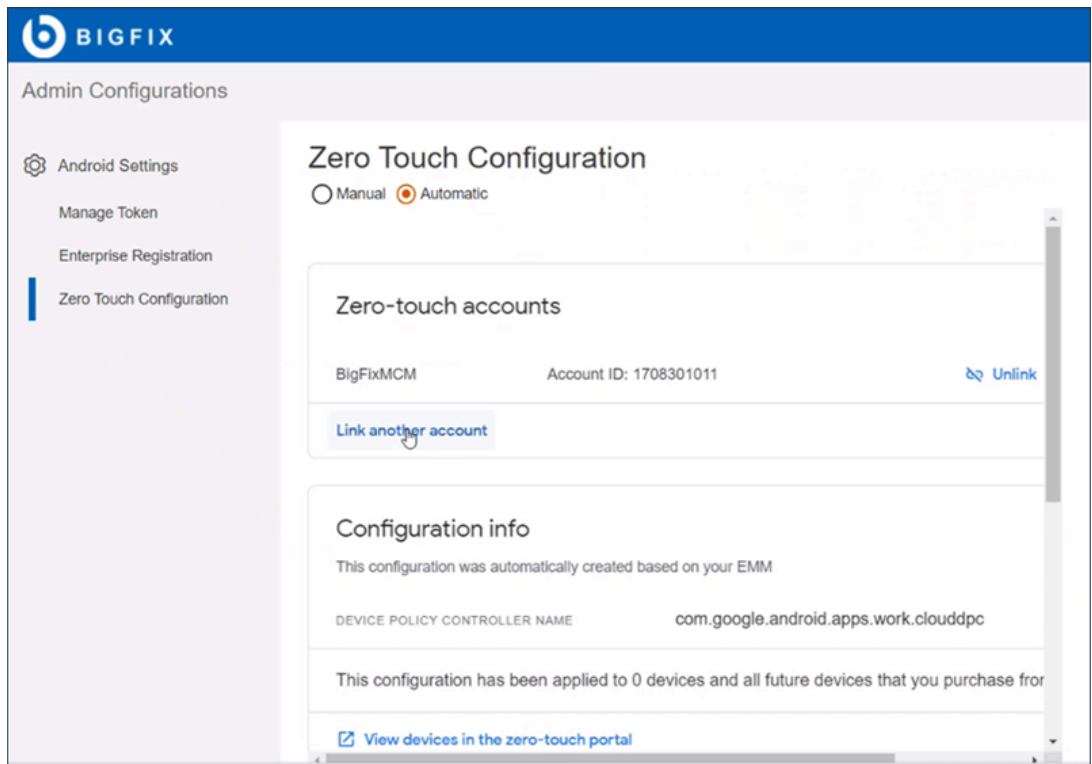
1. Log in to BigFix Mobile and select **Admin Configurations > Zero Touch Configuration**. The **Zero Touch Configuration** window appears.
2. Select **Automatic**.
3. Click **Next** and sign in to the Zero Touch portal account. If already signed in, then select the account.
4. Select the listed devices to link with the BigFix Mobile.
5. Click **Link** and click **Next**.
6. Enter the configuration name, organization name, support email ID, support phone number, and custom message.
7. Click **Save**.



Result: Selected devices are linked to BigFix Mobile. The enrollment process is same as in case of manual zero-touch enrollment.



Note: Click **Unlink** to unlink the devices. Once the account is unlinked, the zero-touch profile is removed. Click **Link another account** to link more accounts.



Android policy management

A policy represents a group of settings that govern the behavior of a managed device and the apps installed on it.

Policy Groups

Android policies are managed through the Policy Groups created via the WebUI. A policy group contains multiple policies. When you deploy a policy group onto MDM servers, that policy group acts as the default policy for the assigned enrollment groups. Android Policy Groups that are not assigned with any enrollment group can be deployed directly onto the eligible mobile devices.

Custom policy

1. Define policy in a JSON file and [upload this custom policy](#) through WebUI.

For sample codes to create custom policy, see the official Google Android Management API documentation:

- BYOD devices: <https://developers.google.com/android/management/policies/work-profile>
 - Fully Managed devices: <https://developers.google.com/android/management/policies/fully-managed-devices>
 - Dedicated device: <https://developers.google.com/android/management/policies/dedicated-devices>
2. Add the created custom policy to a policy group.
 3. Deploy the policy group to MDM server or directly onto the selected devices.



Important: When you create a policy group through WebUI, you must select the appropriate option under Assign To Group drop-down list.

- **BYOD:** Assigns this policy group to BYOD Android devices. On fresh enrollment, BYOD Android devices receive the policies added in this group automatically. After enrollment, when deployed on selected devices, this policy becomes effective only on BYOD Android devices.
- **Fully Managed:** Assigns this policy group to fully-managed Android devices. On fresh enrollment, company-owned Android devices receive the fully-managed device policies added in this group automatically. After enrollment, when deployed on selected devices, this policy becomes effective only on fully managed Android devices.
- **Dedicated:** Assigns this policy group to dedicated Android devices. On fresh enrollment, company-owned Android devices receive the dedicated device policies added in this group automatically. After enrollment, when deployed on selected devices, this policy becomes effective only on dedicated Android devices.

Android device management

Learn how to configure managed Google Play application runtime permissions and how to push permission rules to the managed Android devices.

Runtime permission policy

With runtime permission policy, IT admins can remotely set permissions to prevent applications from gaining access to data or control over a device.

Runtime permissions policy controls if an app wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other applications. For example, the ability to read the user's contacts, external storage or location are runtime permissions. The device user has to grant these permission for the application. For managed Google Play applications, IT admins can configure and enforce these permissions from WebUI.

IT admins can configure runtime permissions through Appstore App Policy or through custom policy to set the default permissions for the apps within the work profile of an Android device. By modifying the default permissions, the IT admin can set default response to the requests made by work apps.



Note: Runtime permission policy is available for Android 6.0 devices or newer. On older Android versions, the permissions are always granted at installation time.

Features

- IT admins can silently set a default response to runtime permission requests made by work apps. The options to configure permissions are as follows:
 - **Prompt** - prompt the user to grant a permission
 - **Grant** - automatically grant permission
 - **Deny** - automatically deny permission

Example: Microsoft Teams app policy can be configured with the defaultPermissinPolicy as 'Prompt' so that for video meetings, Teams app will always request permission from the device user to use the camera.

- Runtime permission grant: After setting a default runtime permission policy, IT admins can silently set responses for specific permissions for the managed work apps.

Android defines some permissions as dangerous and some as normal. The dangerous permissions may affect the users private information, or can potentially affect the data or the operation of other applications. For example, Android classifies the ability to read the user's contacts as a dangerous permission. Some other examples of dangerous permissions are [accessing camera](#), [calendar](#), [location](#), [phone](#), [storage](#).

Configuring global runtime permission

To quickly configure permissions globally to all the managed apps included in an application policy, refer to Appstore App Policy.

1. Set up Apple App Store (iOS and iPadOS) and Google Play Store (Android) Associations to list the app in the app catalog and include in an app policy.
2. Create an Appstore App Policy.
3. Add the created app policy to a policy group.
4. Deploy the policy group to MDM server or directly onto the selected devices.

Configuring per-app runtime permission

If you want to configure runtime permissions for individual applications rather than defining them globally for all the managed applications, you can do so through a custom policy. Based on these settings, IT admins can define if the run time permission can be granted, prompted, or denied.

To configure per-app runtime permissions, complete the following steps:

1. Define the custom [application policy](#) to set runtime permissions at app level.

The permission grant is managed by the configuration:

```
{  
  "permission": string,  
  "policy": enum (PermissionPolicy)  
}
```

For more details on the permissions listed, see the official Android documentation at <https://developer.android.com/reference/android/Manifest.permission>. Configure Prompt, Grant, or Deny for individual permissions.

2. Upload the custom policy **JSON** file.
3. Add the uploaded custom app policy to a policy group.
4. Deploy the policy group to MDM server or directly onto the selected devices.

Device trust

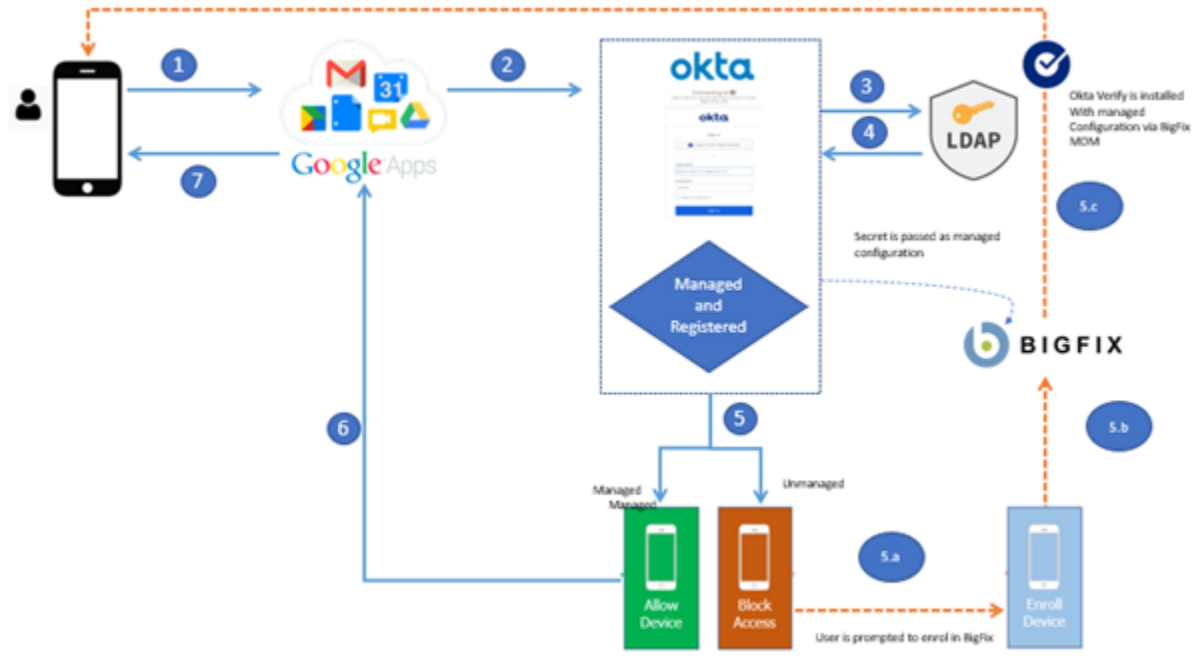
The Device Trust feature from BigFix Mobile prevents unmanaged devices from accessing enterprise services. It provides an extra layer of security to your organization's application access and protects against potential threats from compromised devices. This ensures that your end users are accessing applications from a device that you know is trusted.

With Device Trust feature, administrators can enforce device-level security policies for accessing sensitive applications. This feature uses device attributes, such as operating system, security software, and network information, to assess the trustworthiness of a device before allowing access to protected resources.

BigFix Mobile supports and integrates Okta to establish device trust for iOS and Android mobile devices. For more information on Okta Device Trust, refer to the official documentation at [Okta Device Trust solutions | Okta](#)

Application access flow

When a user tries to access a corporate app, BigFix Mobile verifies, with Okta, that if the device is enrolled and managed. If yes, it allows access to the corporate app. If the device is not enrolled, it is recognized as an untrusted device and prompts the user to enroll to BigFix Mobile before accessing the corporate app.



Supported devices

- Android devices running Android 5.1 (Lollipop) or higher

Supported Apps

- Any Android SAML or WS-Fed cloud app

Port requirements

<TBU>

Prerequisites

- Custom domain app
- Okta LDAP integration
- Configure Okta for BigFix Mobile

Android device trust custom policy

Understand the prerequisites to use BigFix Mobile Device Trust feature, find some examples of managed app configurations, and find an example of device trust custom policy in this topic.


- Android Enterprise management
- Android devices running Android 5.1 (Lollipop) or higher

- Okta Verify app must be added to the device at enrollment time with managed configuration
- Managed app configuration: All the apps that are supported for Okta integration must have managedConfiguration settings specified.

Managed app configurations

The managed app configurations allow you to enable functionality that is built into Android Okta Verify.

Use the examples in this table to help you configure your managed app configurations:

Managed app configuration	Key	Value	Value
Pre-populate the org URL enables admins to pre-populate the First, enter your sign-in URL screen with a sign-in URL, so end users do not need to enter it.	<code>domainName</code>	<code><org_sign-in_URL></code>	String
This is available for Android Okta Verify v6.2.0 and later.			
			
Provide a management hint	<code>managementHint</code>	<code><secret_key></code>	String
Enables admins to specify a secret key, which indicates that a device is managed.			
For more information, refer to the Okta official documentation at Managed app configurations for Android devices Okta			

Example Android device trust custom policy

```
"applications": [
  {
    "packageName": "com.okta.android.auth",
    "installType": "FORCE_INSTALLED",
```

```

"disabled": false,
"managedConfiguration": {
  "domainName": "example.okta.com",
  "managementHint": "3zr7Q~vw4C16FS2bH8UfS 1gJ5cL6sj~x_U9PQ"
}
}

```

Android device security

BigFix Mobile provides various device security management features through which you can protect corporate content and devices.

- By default, BigFix Mobile enforces certain security policies on enrolled Android devices based on the device type, without requiring IT admins to set up or customize any settings.
- Through WebUI pages, IT admins can configure security policies.
- IT admins can define security policies through custom policies.
- IT admins can also prevent unauthorized access and sharing of corporate data through MDM actions.

IT admins can enforce corporate data and device security by deploying security policies on the managed Android devices. Device security policy enforcement ensures that all managed devices are compliant as per the organization's policies. If a device is not compliant, all work apps and work data are blocked in the device unless the device becomes compliant.

Default security policy - General

By default, the following security policies are enforced on all the managed Android devices. The restrictions are effective on devices with Android version 5.0 and above.

The default policy deployed on the enrolled Android devices restricts the installation of apps from any untrusted sources even on the personal profile of the device.

Default security policies

- Restrict app installation by default

```
DISALLOW_INSTALL. DISALLOW_INSTALL Default
```

- Restrict untrusted app installation

```
Enums UNTRUSTED_APPS_POLICY_UNSPECIFIED Unspecified
```

- Restrict app installation on entire device

```
ALLOW_INSTALL_IN_PERSONAL_PROFILE_ONLY
```

- For devices with work profiles, allow untrusted app installation in device's personal profile

```
ALLOW_INSTALL_DEVICE_WIDEAllow
```

- Debugging features are blocked by default.

For the additional securities enforced on dedicated devices and to learn how to override , see [Default security policy override \(on page 120\)](#)

Default security policy - dedicated devices

In addition to the general default security settings, BigFix Mobile enforces the following default security policies on all dedicated devices.

- Users cannot escape a locked down dedicated device to allow other actions. No other actions are allowed for a locked down dedicated device.
- Safe boot disabled: Booting into safe mode is turned off.
- Screen capture disabled
- Camera disabled
- Factory reset disabled


The following code snippet shows the code in the default custom JSON policy file that gets deployed onto dedicated devices on enrollment.

```
{
  "safeBootDisabled": true,
  "screenCaptureDisabled": true,
  "factoryResetDisabled": true,
  "cameraDisabled": true,
  "systemUpdate": {
    "type": "WINDOWED",
    "startMinutes": 120,
    "endMinutes": 240
  },
  "kioskCustomLauncherEnabled": true,
  "keyguardDisabled": true,
  "applications": [
    {
      "packageName": "com.microsoft.office.outlook",
      "installType": "FORCE_INSTALLED",
      "defaultPermissionPolicy": "GRANT"
    }
  ]
}
```

Device security options

Apart from the default security settings that are deployed on enrollment of Android devices, IT admins can enforce device security through MDM policies and actions. The following table shows the overview of various security management options.

Security type	Applicable device type	Security scope
Device security	Company-owned devices (fully managed and dedicated Android devices)	At the device level
Work security	Work profile of the BYOD Android device	At work profile level
Wipe and lock	Company-owned devices(fully managed and dedicated Android devices)	At the device level
Compliance enforcement	Applicable to all managed Android devices depending on the policy configurations	At the device level or at work profile level depending on the policy configurations
SafetyNet support		
Verify Apps enforcement	IT admins can turn on Verify Apps on devices. Verify Apps scans apps installed on Android devices for harmful software before and after they're installed, helping to ensure that malicious apps can't compromise corporate data. Verify Apps must be turned on by default via policy (Go to <code>ensureVerifyApps-Enabled</code>).	
Hardware security management		

 **Important:** For Android, only one policy group can be in effect at a time on the devices and on the MDM server. If you want to deploy a custom policy, you must add it to a Policy group. Only the most recently deployed policy group takes effect on targeted devices.

Passcode Policy

Android passcode policies can be managed from the WebUI passcode policy page. IT admin can configure and enforce a password policy to prompt device user to set a PIN/pattern/password of certain type and complexity to unlock the device or to unlock just the work profile.

Device security

To enforce device security, ensure that you select the Android Passcode Policy Scope as **SCOPE_UNSPECIFIED** or **SCOPE_DEVICE**. Once the user provides the password, the device is unlocked and the user can access apps and data in the device.

Work security

Work security policy is enforced only at the work profile level to protect work apps and data in the Android devices. This policy is useful to enforce on a BYOD device to lock only the work data without disturbing the user's personal data.

To enforce work profile security, ensure that you select the Android Passcode Policy Scope as **SCOPE_UNSPECIFIED** or **SCOPE_PROFILE**.

Once the user provides the password, the work profile is unlocked and the user can access the work profile.



Important: You can add only one password policy to a policy group.

Wipe and lock

Through WebUI, IT admins can remotely wipe or lock company-owned Android devices and ensure corporate data security. The Wipe command is used to wipe corporate content from lost or stolen device. The lock command is used to lock lost or stolen device. To learn how to wipe or lock company-owned Android devices through WebUI, see Wipe and lock device.

Compliance enforcement

- Appstore App Policy: Through application policy, IT admins can enforce rules to protect company apps and data. For example,
 - Control sharing of work data between apps
 - Prevent saving of work app data to a personal storage location
- Restrictions Policy: IT admins can enforce restrictions such as accessing a network through WiFi or Bluetooth.
- Custom policies: IT admins can define custom policies in a JSON file, add it to a policy group, and deploy onto the selected devices or onto the MDM server.

Default security policy override

Learn how to override default security policies.



CAUTION: Though it is possible to override the default security policy, it is recommended that IT admins change it only when it is necessary.

IT admin can override security policies through custom policies. To do that:

1. Define the override settings in a custom JSON file and upload it through WebUI. For example:
 - Code to allow users to boot into safe mode

```
{ "advancedSecurityOverrides": { "developerSettings": "DEVELOPER_SETTINGS_ALLOWED" } }
```


- Code to allow downloading untrusted apps in the personal profile.

```
{ "advancedSecurityOverrides": { "untrustedAppsPolicy":  
  "ALLOW_INSTALL_IN_PERSONAL_PROFILE_ONLY" } }
```

2. Add the defined custom policy to a policy group with appropriate **Assign To Group** selected.
3. Deploy the policy group to MDM server or directly onto the selected devices.

Managing passcode in Android devices

Read this section to learn how to enforce passcode policy, set and wipe passcode in an Android device. The device user can set passcode in the Android device when passcode policy is enforced.

Configuring Passcode policy

[Android passcode policy](#) is configured through WebUI. When the configured passcode policy is deployed onto an Android device via a policy group, the configured passcode policy is enforced on the device.

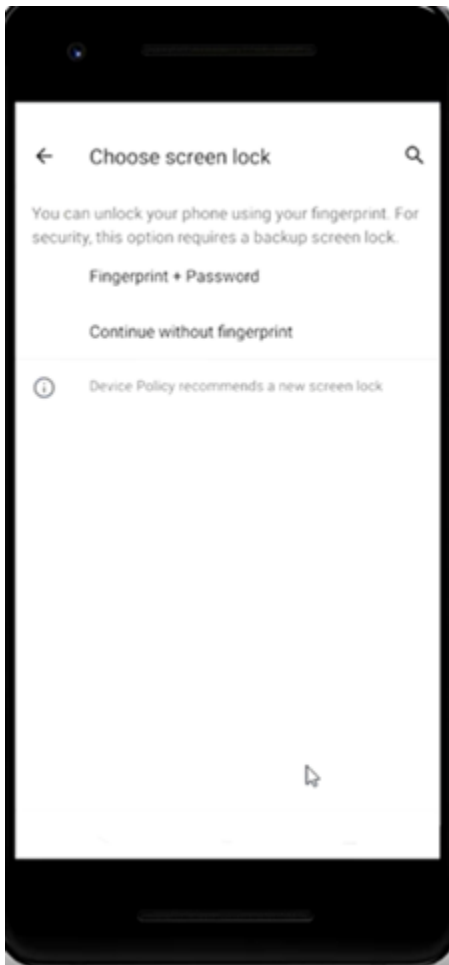
Setting passcode on an Android device

When the configured passcode policy is enforced on the Android device, the device receives a notification, and the user is prompted to set the passcode.

To set the passcode in the Android device, users must complete the following steps:

1. Click the prompt received on the device. The lock screen appears.
2. Click **Set Screen Lock**.
3. From **Choose screen lock**, select **Continue without fingerprints**.
4. Click the **Password** option.
5. In the **Set screen lock** field, enter a passcode as per the set passcode policy.
6. Re-enter the passcode.

7. From **Lock screen**, select the required option. The policy is synced, and the prompt disappears. The user can unlock and access personal and work data by providing the passcode.



Passcode wipe

IT admins can wipe the passcode on a managed Android device by performing an MCM action through WebUI. For more information, see the [Passcode Wipe](#) section in WebUI User Guide.

Android security policies

You can find all the supported Android security policies in this topic.

- Device passcode
- Disable factory reset
- Disable manual unenrollment
- Block installation of non-Google Play applications
- Enforce App verification before App install
- Block installation of non-Google Store Apps
- Disable iCloud/Google Backup

- Disable SD card
- Block USB connection
- Disable Bluetooth
- Disable NFC
- Disable Save as of Microsoft Office documents
- Disable Sharing of Microsoft Office documents
- Block uninstallation of Apps
- Disable Google's location service

- - enforce a passcode
 - lock and wipe a device
 - reset/clear the passcode
 - play an alarm sound
 - track device location

- - separate business data from personal data with secure containers
 - encrypt mobile device storage
 - manage Android system updates

Application management

With the application management capability in BigFix Mobile, you can manage applications on your enrolled mobile devices such as add and assign apps to devices, protect company data in apps, force install work apps which do not require user permission, and do much more.

Before you Begin:

- The organization must enroll to Managed Google Play Accounts enterprise if it uses the non-Google Workspace (formerly non-G-suite) account. For more details, see [Managed Google Play Accounts enterprise \(on page 81\)](#).

About the task:

- You can set Android App configurations through WebUI via Setup Apple App Store Associations and Appstore App Policy.
- You can also manage Android applications through a custom policy uploaded to WebUI.



Important: For Android, only one policy group can be in effect at a time on the devices and on the MDM server. If you want to deploy a custom policy, you must add it to a Policy group. Only the most recently deployed policy group takes effect on targeted devices.

Manage applications through Appstore App Policy

From BigFix WebUI, you can configure application permissions through Appstore App Policy. These permissions are applicable globally for all the apps. To do that:

1. Set up Apple App Store (iOS and iPadOS) and Google Play Store (Android) Associations to list the app in the app catalog and include in an app policy.
2. Create an Appstore App Policy.
3. Add the created app policy to a policy group.
4. Deploy the policy group to MDM server or directly onto the selected devices.

Manage applications through a custom policy

If you want to define configurations for individual applications rather than defining them globally for all the applications, you can do so through a custom policy. Based on these settings, IT admins can define if the app can be automatically installed on applying the policy or made available for the user to install.

To define custom application policy, complete these steps:

1. Define the custom [application policy](#) to set permissions at app level and configure the [installation type](#) in a **JSON** file.
2. [Upload the custom policy JSON](#) file.
3. Add the uploaded custom app policy to a policy group.
4. Deploy the policy group to MDM server or directly onto the selected devices.

Silent app distribution

IT admins can install and manage work applications silently in BigFix Mobile managed Android devices without any user interaction.

If an organization needs to install and manage work applications that are mandatory to the user, IT admins can configure a policy to do so silently without prompting the end user. IT admin can also update or remove an application silently.

Prerequisites

- The android device must be enrolled to BigFix Mobile

The following Application policy settings need to be configured.

- `packageName`: Bundle ID of the Android app that needs to be installed on the Android device. Find the app in [Google Play](#) and click on it to go to the app's page. The app ID is shown in the URL after `?id=`. For example, the URL for outlook is <https://play.google.com/store/apps/details?id=com.microsoft.office.outlook> and the bundle ID is `com.microsoft.office.outlook`.
- `installType`: `FORCE_INSTALLED` or `AVAILABLE`. IT admin can distribute the applications via two methods:

- **AVAILABLE**: To add an app to a device's managed Play store app where the user can install the application
- **FORCE_INSTALLED**: To force install an app to a device remotely without any user intervention

Following is an example of a custom policy (JSON file) to install Excel and Outlook that can be uploaded to WebUI and deployed as part of a policy group:

```

1  {
2  "applications": [
3    {
4      "packageName": "com.microsoft.office.outlook",
5      "installType": "FORCE_INSTALLED"
6    },
7    {
8      "installType": "AVAILABLE",
9      "packageName": "com.microsoft.office.excel"
10   }
11 ]
12 }
```

On Android devices that you have deployed the policy, you can see the notification "Installing apps from your organization" from the Google Play Store. Also, you can see the apps defined in the policy are silently installed.

Install

To install work applications in BigFix Mobile managed Android devices, add Appstore App Policy defined in the WebUI to a policy group. Otherwise, you can upload custom policies that define these work applications to the WebUI and add them to a policy group.

When the policy group has all of the work applications you wish to install properly configured, simply deploy the policy group to an MDM server or to Android devices / device groups.

Managed configurations

IT admins can silently install work applications and apply pre-configurations on BigFix Mobile managed Android devices through custom policies uploaded through WebUI.

Managed configurations are the set of properties of an application that allow the enterprise IT admins to pre-configure and remotely manage that application. These configurations are particularly useful for organization-approved apps deployed to a work profile.

- IT admins can view and silently set managed configurations for any Android app that supports managed configurations.



Note: Not all Android apps support remote configuration. Refer to the software vendor's documentation for the app configuration keys.

- IT admins can set any configuration type (as defined by the Android Enterprise framework) for Google Play store apps.
- IT admins can set wildcards (such as \$username\$ or %emailAddress%) so that a single configuration for an app such as Gmail can be applied to multiple users.

For more information on setting up managed configurations, see the official Android documentation at <https://developer.android.com/work/managed-configurations>

Silently install Android apps and apply managed configurations

Understand the functionality with the following use case.

Use case: Install Microsoft outlook app and configure some of the managed properties like, email address, account name, exchange server name, and domain.

For the key value pairs of the Outlook configurable settings, see <https://docs.microsoft.com/en-us/exchange/clients/outlook-for-ios-and-android/account-setup?view=exchserver-2019#key-value-pairs>:

Sample custom policy JSON for configuring outlook app:

```
{
  "applications": [
    {
      "packageName": "com.microsoft.office.outlook",
      "installType": "FORCE_INSTALLED",
      "disabled": false,
      "managedConfiguration": {
        "com.microsoft.outlook.EmailProfile.EmailAddress": "john.doe@hcl.com",
        "com.microsoft.outlook.EmailProfile.EmailAccountName": "John Doe",
        "com.microsoft.outlook.EmailProfile.ServerHostName": "outlook.office365.com",
        "com.microsoft.outlook.EmailProfile.AccountDomain": "hcl"
      }
    }
  ]
}
```

- Before deploying the policy to device, ensure that Outlook is not installed and configured in work profile.
- After deploying the policy, Outlook gets installed in the targeted Android device. You can verify from Play Store if Outlook is being installed.
- After installation, open the Outlook app, and click Add account.
- You can see that all the managed properties, deployed with policy, are silently set to the application during installation.

Managed configuration template

You can add the managed configurations IFrame to your console and apply settings via `managedConfigurationTemplate` in `ApplicationPolicy`.

The **managed configurations iframe** is an embeddable UI that lets IT admins save, edit, and delete an app's managed configuration settings. You can, for example, display a button (or similar UI element) in an app's details or settings page that opens the IFrame. For more details and the instructions to create a managed configurations IFrame or template, see https://developers.google.com/android/management/managed-configurations-iframe#actions_available_to_it_admins_from_the_iframe.

```
{
  "alwaysOnVpnPackage": {
    "packageName": "com.paloaltonetworks.globalprotect",
    "lockdownEnabled": false
  },
  "applications": [
    {
      "packageName": "com.android.chrome",
      "installType": "FORCE_INSTALLED"
    },
    {
      "packageName": "com.paloaltonetworks.globalprotect",
      "managedConfigurationTemplate": {
        "templateId": "07653241707528085163"
      },
      "installType": "FORCE_INSTALLED"
    }
  ]
}
```

Basic store layout

IT admins can install and update work apps through the managed Google Play Store app. After enrolling an Android device, by default, the managed Google Play Store displays apps approved for a user in a single page. This layout is called basic store layout.

Private app deployment

Private apps are internal apps that are built for your organization and distributed to your enterprise users through Managed Google Play. You can add and manage private apps for Android Enterprise devices via Managed Google Play. This feature is supported on all Android Enterprise deployment scenarios: Device Owner (DO), Profile Owner (PO), and Corporate-Owned Single-Use (COSU).

Ensure you have a signed private apk readily available to upload through the Admin UI.

As an Admin Configuration user, you can:

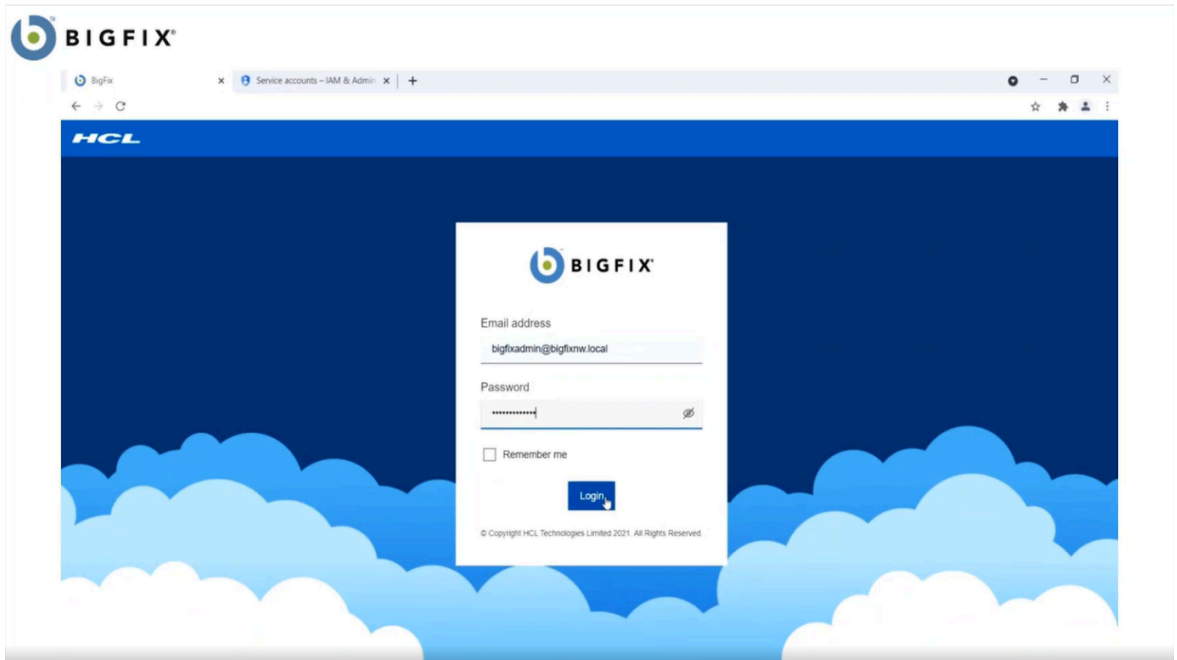
- Update Google-hosted private apps instead of updating through the Google Play Console.
- Upload new versions of apps that are already published privately to the enterprise using the [managed Google Play iFrame](#) or the [Google Play Developer Publishing API](#).

With Managed Google Play's private app publishing iFrame, you can publish private apps directly from Admin UI. .

How to upload a private app

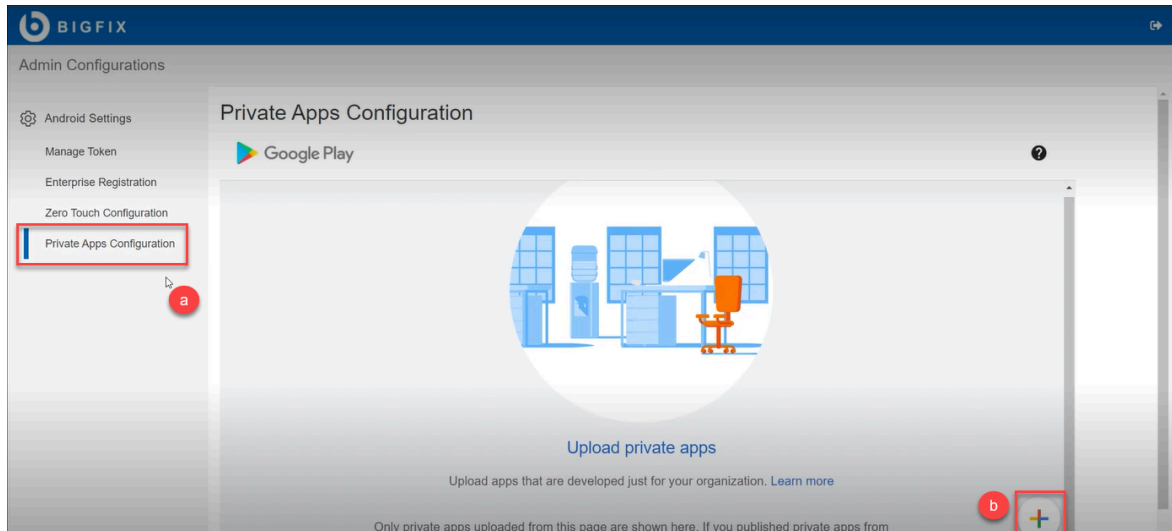
To upload a private app complete the following steps:

1. Go to the Admin UI URL (for example, <https://MDM-demo/config>). This URL represents where you installed MDM and is separate from the WebUI.
2. Enter your organization email ID and password and click



Login.

3. From the BigFix **Admin Configurations** page, navigate to **Private Apps Configuration** and click the **+** button.



4. In the next page, enter the Title of the Private app and click **Upload APK** to navigate and upload the custom apk file.



Note: Ensure the title is unique, as you cannot publish the same app again.

5. When prompted, enter your email address to get notification and click **OK**.
6. Click **Create**.

The private app is published to the Google iFrame. When you publish a private app from Google iFrame,

- Google creates a Play Developer account for your organization.
- Private apps are automatically approved for your organization.
- The apps becomes ready to distribute in less than 10 minutes.
- You can click on the app icon to edit the title or to re-upload the apk file if necessary.
- For advanced editing options such as adding description and screenshots, or unpublishing apps, click **Make advanced edits**.
- Deploy the APK on the MDM server and [distribute the private app through android app policy \(on page 124\)](#)

API usage requirements

BigFix Mobile implements Android Management APIs at scale, avoiding traffic patterns that could negatively impact enterprises' ability to manage apps in production environments.

- BigFix Mobile adheres to the Android Management API usage limits.
 - To not send more than 1000 queries per 100 seconds for each project by default.

- BigFix Mobile distributes traffic from different enterprises throughout the day, rather than consolidating enterprise traffic at specific or similar times.
- BigFix Mobile does not make consistent, incomplete, or deliberately incorrect requests that make no attempt to retrieve or manage actual enterprise data.

System update

An update policy affects the pending system update (if there is one) and any future updates for the device. IT admins can set up and trigger over-the-air (OTA) system updates on Android devices. This feature is applicable for fully-managed and dedicated devices with Android version 6.0 or later.

IT admins can set the following OTA configurations:

- Automatic: Apply OTA system updates when the devices are available.
- Postpone: Postpone OTA system updates on devices for up to 30 days.
- Windowed: Schedule OTA system updates on devices within a daily maintenance window.

You can configure OTA system update through BigFix WebUI [OS Update Policy](#).

To apply the created OS update policy to devices, add the policy to a [Policy Group](#) and deploy the policy group onto the devices.

What is the device user experience when the system update policy is triggered? UI Screens and messages

Is there any error or message that will be displayed to the user or the admin when the system update policy is not applied or failed for some reason?

Will the admin be able to select devices that are not 6.0 to apply system update policy? is there any restriction on selecting the device with appropriate version? if not will the admin sees any messages?

Android Kiosk management

Kiosk mode provides complete control over the device usage and ensures that the devices can be used only for the intended purposes. Android can run tasks in a kiosk mode by configuring the settings through custom policy. . This feature is applicable only for company-owned devices. When Kiosk mode is enabled, a fully-managed device becomes a dedicated device. In a dedicated device, the device user can access only the apps allowed as per the active policy.

Kiosk mode allows the Administrator to disable all the major system UI features, such as notifications, home button, recent apps button, and global actions. WebUI allows Administrator to configure a [policy](#) to allow a single app or multiple apps to be installed and locked on a dedicated device.

For complete information on Kiosk mode, refer to the official Android documentation at https://developers.google.com/android/management/policies/dedicated-devices#kiosk_mode.

Prerequisites

- Device must have Android version 6.0 or later.
- Device must be a dedicated device enrolled as Device Owner in Android Enterprise.

Single app Kiosk mode

Kiosk mode that restricts device access to a single application runs the device on single app kiosk mode. These dedicated devices in kiosk mode run a specialized application with minimal device functionalities. You can set your app as the device's home app so that it is launched automatically when the device starts up or even rebooted.

To enable kiosk mode on a device, configure the following setting in the policy:

```
"kioskCustomLauncherEnabled": true
```

or

Specify a designated kiosk app for the device by setting its `installType` to `KIOSK`. This designated kiosk app launches automatically when the device boots.

```
"applications": [
  {
    "packageName": "com.example.app",
    "installType": "KIOSK",
    "defaultPermissionPolicy": "GRANT"
  }
]
```



Note: You can either configure `"kioskCustomLauncherEnabled": true` or for a preferred application set `"installType": "KIOSK"`. If you configure both together, the Android log shows the error "Kiosk install type cannot be used if kioskCustomLauncherEnabled is true".

Multiple app kiosk mode

You can also install multiple apps pertinent to the organization's requirements and lock down a device on Kiosk mode. However, Kiosk mode limits the device usage to the specified applications by running only those apps the user needs to access.

A device can only have a single designated kiosk app (`installType` set to `KIOSK`). However, if a Kiosk app links to other apps, these additional apps can be added to `applications`. Ensure that the `installType` for any additional apps is not `KIOSK` or `BLOCKED`.

```
"applications": [
  {
    "packageName": "com.example.app",
    "installType": "KIOSK",
    "defaultPermissionPolicy": "GRANT"
  }
]
```

```

},
{
  "packageName": "com.example.app_to_be_linked",
  "installType": "FORCE_INSTALLED",
  "defaultPermissionPolicy": "GRANT"
}
]

```

Temporary network connection for Kiosk mode

It is recommended to add `"networkEscapeHatchEnabled": true` in the enrollment policy. This is because, if a device boots into an app in Kiosk mode, and if there is no suitable network in the enrollment policy, the enrollment does not succeed. To avoid that, IT admins can configure `"networkEscapeHatchEnabled": true` in the enrollment policy for the users to temporarily connect to a network to refresh the device policy with Wi-Fi configuration. After applying the policy with active Wi-Fi configuration, the temporary network is forgotten and the device can continue to boot.

1. Add `"networkEscapeHatchEnabled": true` in the enrollment policy. At the time of booting, if the network connection fails, this setting prompts the user to temporarily connect to an available network to refresh the device policy.
2. After enrolment, for the device to get a permanent network connection, add the Wi-Fi configuration policy with active Wi-Fi name and password.

```

"openNetworkConfiguration": {
  "NetworkConfigurations": [{
    "GUID": "a",
    "Name": "Example A",
    "Type": "WiFi",
    "WiFi": {
      "SSID": "NetworkID",
      "Security": "WEP-PSK",
      "Passphrase": "1234567890"
      "AutoConnect": true
    }
  }]
}

```

3. Restart the Kiosk device and wait for 1 to 2 minutes. A popup appears where the user can select any available network to make a temporary connection. After the connection is established and the device gets the Wi-Fi configuration through the policy, the temporary connection will be forgotten.



Note: The temporary connection is only for fetching the latest policy with active Wi-Fi configuration details. Once the latest policy is fetched the kiosk device will be automatically connected to the network which is specified in the policy. If it does not connect to the Wi-Fi automatically, restart the device.

Device User Experience

- Only apps that are allowed through the policy are accessible. The users can click and navigate through the allowlisted apps and can not leave out of Kiosk mode.
- All other apps and other screens including the homescreen, notifications, and all other screens become inaccessible.
- The allowed app is pinned to the device screen and the device user cannot exit the app screen.
- Device user cannot be unenrolled.

Enabling Kiosk mode

To enable Kiosk mode, perform the following:

1. Create a custom policy to configure an app or set of apps to be installed on Kiosk mode.
 - To enable Kiosk mode, set the `installType` of the desired app as `KIOSK` or set `kioskCustomLauncherEnabled` to `true`.
 - If a device requires users to access one or more apps from the home screen, enable the device's custom launcher by enabling `kioskCustomLauncherEnabled` in the policy.
 - To keep the device unlocked (for public kiosks, for example), enable `keyguardDisabled`
2. Upload the policy through WebUI.
3. Add the created app policy to a policy group targeted for dedicated devices.
4. Deploy the policy group to MDM server or directly onto the selected devices.

Sample JSON code to enable Kiosk mode on a dedicated device:

```
{
  "safeBootDisabled": true,
  "screenCaptureDisabled": true,
  "factoryResetDisabled": true,
  "cameraDisabled": true,
  // Specifies that system updates will be auto-installed during a daily
  // maintenance window between 2am and 4am.
  "systemUpdate": {
    "type": "WINDOWED",
    "startMinutes": 120,
    "endMinutes": 240
  },
}
```

```

"kioskCustomLauncherEnabled": true,
"keyguardDisabled": true,
"networkEscapeHatchEnabled": true,
"applications": [
  {
    "packageName": "com.microsoft.office.outlook",
    "installType": "FORCE_INSTALLED",
    "defaultPermissionPolicy": "GRANT"
  },
]

```

For more sample codes, refer to <https://developers.google.com/android/management/policies/dedicated-devices#kiosk-launcher>

Disabling Kiosk mode

A policy can remotely stop Kiosk mode by removing the app package from the allow list.

Related reference

[Android Kiosk not connected to Internet \(on page 157\)](#)

Android hardware security

The hardware security features from Android helps the Admins to lock hardware elements of a company-owned device to secure company data and prevent data loss.

Applicable device types and management modes

- Company-owned device in fully managed mode
- Company-owned device in dedicated managed mode

Configuring **Restriction policy**

Through WebUI, as a Master Operator, create an Android hardware restriction policy with the following settings:

- **Mount Physical Media Disabled:** To restrict device users from mounting physical external media, set the value to `True`.
- **USB File Transfer Disabled:** To restrict device users from transferring files over USB, set the value to `True`.
- **Outgoing Beam Disabled:** To restrict devices user from sharing company data from the device using NFC beam, set the value to `True`.

Deploying the restriction policy

1. Add the created restriction policy to a policy group.
2. Deploy the policy group to MDM server or directly onto the selected devices.

After applying the policy

- USB file transfer option will not be available.
- When the device user tries to mount the connected physical external storage device, it displays the notification "Action not allowed".
- NFC option is disabled (still shows enabled which is not expected Google team to provide an update and solution for this)

Cross-profile management

With Android crossprofile restriction policy, organizations can protect and control data sharing from the work profile to personal profile in the same device.

- IT admins can configure if the contacts stored in the work profile can be shown in personal profile contact searches and incoming calls.
- IT admins can disable Bluetooth contact sharing of work contacts, for instance hands-free calling in cars or headsets.
- IT admins can [control the ability to copy/paste between the work and personal profiles](#).

Crossprofile restrictions are applicable to devices with personal and work profile; example, BYOD, COPE.



Note: With MCM3.0, users can configure crossprofile restrictions by creating a custom policy and attaching it to a policy group through WebUI.

Sample code for crossprofile restriction policy

The following is the sample code for a custom policy with crossprofile restrictions

```
{
  "showWorkContactsInPersonalProfile": enum (ShowWorkContactsInPersonalProfile),
  "crossProfileCopyPaste": enum (CrossProfileCopyPaste),
  "crossProfileDataSharing": enum (CrossProfileDataSharing)
}
```

Customizable parameters

[showWorkContactsInPersonalProfile](#)

Configures if the contacts stored in the work profile can be shown in personal profile contact searches and incoming calls.

<code>SHOW_WORK_CONTACTS_IN_PERSONAL_PROFILE_UNSPECIFIED</code>	Unspecified. Defaults to <code>SHOW_WORK_CONTACTS_IN_PERSONAL_PROFILE_ALLOWED</code> .
<code>SHOW_WORK_CONTACTS_IN_PERSONAL_PROFILE_DISALLOWED</code>	Prevents work profile contacts from appearing in personal profile contact searches and incoming calls
<code>SHOW_WORK_CONTACTS_IN_PERSONAL_PROFILE_ALLOWED</code>	Default. Allows work profile contacts to appear in personal profile contact searches and incoming calls

crossProfileCopyPaste

Configures if the text copied from one profile (personal or work) can be pasted in the other profile.

<code>CROSS_PROFILE_COPY_PASTE_UNSPECIFIED</code>	Unspecified. Defaults to <code>COPY_FROM_WORK_TO_PERSONAL_DISALLOWED</code>
<code>COPY_FROM_WORK_TO_PERSONAL_DISALLOWED</code>	Default. Prevents users from pasting into the personal profile text copied from the work profile. Text copied from the personal profile can be pasted into the work profile, and text copied from the work profile can be pasted into the work profile.
<code>CROSS_PROFILE_COPY_PASTE_ALLOWED</code>	Text copied in either profile can be pasted in the other profile.

crossProfileDataSharing

Whether data from one profile (personal or work) can be shared with apps in the other profile. Specifically controls simple data sharing via intents. Management of other cross-profile communication channels, such as contact search, copy/paste, or connected work & personal apps, are configured separately.

Enums

<code>CROSS_PROFILE_DATA_SHARING_UNSPECIFIED</code>	Unspecified. Defaults to <code>DATA_SHARING_FROM_WORK_TO_PERSONAL_DISALLOWED</code> .
<code>CROSS_PROFILE_DATA_SHARING_DISALLOWED</code>	Prevents data from being shared from both the personal profile to the work profile and the work profile to the personal profile.
<code>DATA_SHARING_FROM_WORK_TO_PERSONAL_DISALLOWED</code>	Default. Prevents users from sharing data from the work profile to apps in the personal profile. Personal data can be shared with work apps.
<code>CROSS_PROFILE_DATA_SHARING_ALLOWED</code>	Data from either profile can be shared with the other profile.

Verify Apps enforcement

Verify Apps enforcement feature enables Google Play Protect to scan all the apps installed on Android device for harmful software before and after they are installed to ensure that malicious apps cannot compromise corporate data. This setting is optional.

- IT admins can enforce Verify Apps by default via custom policy. This restricts the user from disabling Google Play Protect to scan and verify apps on the device.
- IT admins can provide device users an option to turn the setting `Scan apps with Play Protect` on or off.

Google Play Protect

Google Play Protect helps to keep devices safe and secure.

- It runs a safety check on apps from the Google Play Store before device user downloads them.
- It checks the device for potentially harmful apps from other sources.
- It warns about any detected potentially harmful apps found, and removes known harmful apps from the device.
- It warns about detected apps that violate [Unwanted Software Policy](#) by hiding or misrepresenting important information.
- It sends privacy alerts about apps that can get user permissions to access personal information, violating [Developer Policy](#).

Custom policy

To verify apps enforcement, as an IT Admin, you can upload a custom policy through WebUI in `JSON` file format with specific settings, and then deploy this policy on to your Android devices.

- To view or download a custom policy with required verify apps enforcement policy settings, visit BigFix Wiki at [Android Custom Policy Templates](#) and click the desired policy link.
- For the steps to upload and deploy the custom policy, see [Custom policy \(on page 111\)](#).

Configuration parameters

To configure verify apps settings, include `advancedSecurityOverrides` field on a custom policy.

Configuration parameters	Definition
<code>googlePlayProtectVerifyApps</code>	Whether Google Play Protect verification is enforced. Valid values:

Configuration parameters	Definition
	<ul style="list-style-type: none"> • <code>GOOGLE_PLAY_PROTECT_VERIFY_APPS_UNSPECIFIED</code>: Unspecified. Defaults to <code>VERIFY_APPS_ENFORCED</code>. • <code>VERIFY_APPS_ENFORCED</code>: Default. Force-enables app verification. • <code>VERIFY_APPS_USER_CHOICE</code>: Allows the user to choose whether to enable app verification.

Sample JSON Code

```
{
  "advancedSecurityOverrides": {
    "developerSettings": "DEVELOPER_SETTINGS_ALLOWED",
    "untrustedAppsPolicy": "DISALLOW_INSTALL",
    "googlePlayProtectVerifyApps": "VERIFY_APPS_ENFORCED"
  },
  "applications": [
    {
      "packageName": "com.android.chrome",
      "installType": "AVAILABLE"
    }
  ]
}
```

VPN management

Virtual private network (VPN) management feature allows IT admins to ensure that data from certain apps always goes through the specified . IT admins can also apply a setting such that a device is connected to the network only when VPN is connected.

Use these settings to create a VPN connection, choose how the VPN authenticates, select a VPN server type, and more. VPNs give device users a secure remote access to your organization network. Devices use a VPN connection profile to start a connection with the VPN server. Use these settings so users can easily and securely connect to your organizational network.

This feature applies to:

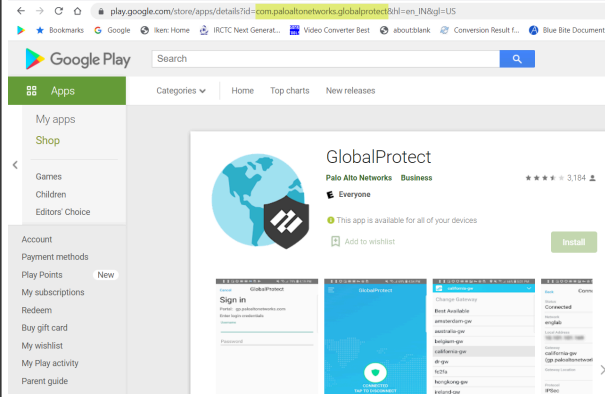
- Android Enterprise personally owned devices with a work profile (BYOD)
- Android Enterprise corporate-owned work profile (COPE)
- Android Enterprise corporate owned fully managed (COBO)
- Android Enterprise corporate owned dedicated devices (COSU)

Allows IT admins to specify an Always On VPN to ensure that the data from specified managed apps will always go through a set-up Virtual Private Network (VPN). **Note:** this feature requires deploying a VPN client that supports both Always On.

- IT admins can [specify an arbitrary VPN package](#) to be set as an Always On VPN.
 - The EMM's console may optionally suggest known VPN packages that support Always On VPN, but can't restrict the VPNs available for Always On configuration to any arbitrary list.
- IT admins can specify the VPN app to be used using "AlwaysOnVpnPackage" property in the Android policy.
- The "lockdownEnabled" property can be set to true to ensure devices are connected to the network only when VPN is connected.
- IT admins can use managed configurations to specify the VPN settings for an app.

Always on VPN Package

Android can start a VPN service when the device boots, and keep it running while the device or work profile is on. This feature is called always-on VPN and is available in Android 7.0 or higher.

Configuration parameters	Definition
packageName	<p>The package name of the VPN app.</p> <p>Example: com.paloaltonetworks.globalprotect</p> <p>You can find it from the Google Play store on the address bar when you click on an app.</p> 
lockdownEnabled	<p>Valid values: true, false</p> <p>When set to <code>true</code>, disallows networking when the VPN is not connected.</p> <p>When set to <code>false</code>, allows networking when the VPN is not connected.</p>

Sample JSON code

```
{
  "alwaysOnVpnPackage": {
    "packageName": "com.paloaltonetworks.globalprotect",
    "lockdownEnabled": false
  },
  "applications": [
    {
      "packageName": "com.paloaltonetworks.globalprotect",
      "installType": "FORCE_INSTALLED"
    },
    {
      "packageName": "com.android.chrome",
      "installType": "FORCE_INSTALLED"
    }
  ]
}
```

Wi-Fi configuration management

IT admins can manage Wi-Fi configurations on MDM-managed Android devices.

- IT admins can silently provision enterprise Wi-Fi configurations on MDM managed Android devices.
- For fully managed devices, IT admins can optionally prevent a device user from manually modifying corporate Wi-Fi settings on their device by setting `wifiConfigsLockdownEnabled` to `true` in the policy.
- For fully managed devices, IT admins can optionally restrict device users from adding or modifying Wi-Fi network (personal and corporate) on the device by setting `wifiConfigDisabled` to `true` in the policy. This limits Wi-Fi connectivity to just those networks provisioned through the policy.

To manage Wi-Fi configurations, as an IT Admin, you can upload a custom policy through WebUI in **JSON** file format with specific Wi-Fi settings, and then deploy this policy to your Android devices.

- To view or download a custom policy with required Wi-Fi settings, visit BigFix Wiki at [Android Custom Policy Templates](#) and under the Wi-Fi Configuration section, click on a desired Wi-Fi policy link.
- For the steps to upload and deploy the custom policy, see [Custom policy \(on page 111\)](#).

Supported management modes and versions

The following table shows different Wi-Fi configuration options and the supported management mode along with the Android version.

Wi-Fi configurations	Work profile	Fully managed	Dedicated
Silently provision enterprise Wi-Fi configurations	6.0+	6.0+	6.0+
Prevent a device user from manually modifying corporate Wi-Fi settings	N/A	6.0+	6.0+
Restrict device users from adding or modifying Wi-Fi network (personal and corporate) on the device	N/A	6.0+	6.0+

Wi-Fi configuration parameters

To configure Wi-Fi settings, include an Open Network Configuration and set the `openNetworkConfiguration` field on a custom policy.



Important: The Android Management API only supports a subset of the Open Network Configuration specification. For more details, see official Android Management API page at <https://developers.google.com/android/management/configure-networks>.

Wi-Fi configuration parameters	Definition
<code>SSID</code>	Service Set Identifier The name of your wireless network, also known as Network ID. Enter the service set identifier, which is the real name of the wireless network that devices connect to.
<code>Security</code>	Wireless Security Protocol. Examples: WEP-PSK, WPA-PSK
<code>Passphrase</code>	Wi-Fi password
<code>Autoconnect</code>	Enables autoconnect on the device. Valid values: true, false
<code>wifiConfigsLockdownEnabled</code>	Valid values: true, false When set to true, locks down (corporate) Wi-Fi configurations set and to prevent users from modifying the set configurations
<code>wifiConfigDisabled</code>	Valid values: true, false When set to true, restricts device users from adding or modifying any Wi-Fi network on the device, limiting Wi-Fi connectivity to just those networks provisioned through the policy.

Sample JSON code

```
"openNetworkConfiguration": {
  "NetworkConfigurations": [{
    "GUID": "a",
    "Name": "Example A",
    "Type": "WiFi",
    "WiFi": {
      "SSID": "NetworkID",
      "Security": "WEP-PSK",
      "Passphrase": "1234567890"
      "AutoConnect": true
    }
  ]
}
```

Result:

Once the policy is applied, the MDM-managed Android device automatically gets connected to the Wi-Fi network as defined in the custom policy without user intervention.

Apple mobile management

With BigFix Mobile, you can seamlessly enroll iOS and iPadOS devices.

Through policies and actions, you can manage the MDM enrolled iOS and iPadOS devices in many ways including but not limited to the following:

- Manage mobile settings and applications remotely.
- Enforce security policies to prevent unauthorized access and sharing of corporate data and devices.
- Remotely wipe corporate content from lost or stolen device and ensure corporate data security.
- Remotely manage apps such as adding and assigning apps to devices, protecting company data in apps, force installing corporate apps.

Certificates

You need to manage Apple mobile devices through MDM.





- Ensure you always have a valid certificate by monitoring the notifications displayed on Modern Client Management dashboard in the WebUI.
- Renew the APNs before expiry.
- Keep the Apple enrollment certificate up to date for continued management of Apple devices without interruption.

Provisioning

The MDM protocol for provisioning iOS and iPadOS is largely the same as macOS. The same Apple MDM server and same Apple MDM PlugIn is used for all three options. The user experience during enrollment is slightly different. For more information on different types of enrollment options, see [Provisioning Apple mobile devices \(on page 144\)](#).

Remote actions

You can perform remote actions like lock, wipe, wipe passcode, restart, shutdown, remove policy, and unenroll on one or more selected MDM managed iOS and iPadOS devices through WebUI. For more details and instructions, see **Deploy MCM actions** section in WebUI User Guide.

Policies

BigFix Mobile enables you to configure profiles for your iOS and iPadOS devices just the way you can configure your macOS devices. You can define Passcode policy, Restrictions Policy, Appstore App Policy, OS Update Policy settings through BigFix WebUI.

You can also create custom configuration policies in `.xml`, `.mobileconfig`, or `syncML` format and upload through WebUI.



Note: When you create custom policies, ensure the settings and the format are valid. For more information on configuring profile payloads and settings, see the official Apple documentation at [Mobile Device Management Settings](#) and [Profile-specific Payload Keys](#).

Managing Applications

With the application management capability in BigFix Mobile, you can manage applications on your enrolled mobile devices such as add and assign apps to devices, protect company data in apps, force install work apps which do not require user permission, and do much more.

You can set Android App configurations through WebUI via Setup Apple App Store Associations and Appstore App Policy.

From BigFix WebUI, you can configure application permissions through Appstore App Policy. These permissions are applicable globally for all the apps. To do that:

1. Set up Apple App Store (iOS and iPadOS) and Google Play Store (Android) Associations
to list the app in the app catalog and include it in an app policy.
2. Create an Appstore App Policy.
3. Add the created app policy to a policy group.
4. Deploy the policy group to MDM server or directly onto the selected devices.

Provisioning Apple mobile devices

You can get Apple mobile devices enrolled to BigFix Mobile in the following ways.

- [Enrolling through enrollment URL - Apple \(on page 58\)](#): Users can enroll their Apple mobile devices (iOS and iPadOS) over-the-air through an enrollment URL.
- **Apple Automated Device Enrollment**: Administrators can configure and automate enrollment of out-of-the-box Apple mobile devices (iOS and iPadOS) that an organization purchases through Apple or authorized resellers to provide to employees. iPhone and iPad DEP enrollment is very similar to Mac DEP enrollment, with minor changes in options and screen flows. DEP profiles allow specification of which setup screens to skip during enrollment.
- [Apple BYOD enrollments \(on page 60\)](#): Device users can enroll their personally owned iOS or iPadOS devices with BigFix Mobile, so that the IT admin can manage the devices.

On enrollment

- Appstore applications can be added to a Policy Group for delivery at the time of enrollment to iOS or iPadOS devices. In such cases, when presented with the DEP enrollment screen to supply an Apple ID, users should have an existing Apple ID to enter.



Note: Do not create a new ID during enrollment as then the Appstore apps cannot be delivered through the Group Policy at time of enrollment.

Post enrollment

- After enrollment, under the Enrollment profile, you can see two new sections – Apps and Restrictions. This is where you can find out which policies, apps and restrictions have been applied through MDM, either at the time of enrollment, or after enrollment.

Screen-locked Devices

- Even if the iPhone or iPad is turned on, the device will not respond to most requests (such as profile delivery, client refresh) unless the device is unlocked. If the screen is locked, the Apple Push notification server will check in and report the status as “NotNow”, meaning it is not able to process the requests.

Known issue

- It is possible to target Apple actions against Apple devices that do not support the action. For example, an MDM shutdown command might target non-supervised Apple devices. In these situations, the action will fail.

Apple mobile policy management

A policy represents a group of settings that govern the behavior of a managed device and the apps installed on it.

Blueprints

A blueprint is a JSON file which contains a list of prestaged applications, app store apps, and profiles to deliver at device enrollment time. Blueprints allow you setup a template of settings, options, apps, and restore data, and then apply those settings on Apple devices. It can be applied not only to devices part of the current session, but also saved for future use without having to be recreated each time deployment is required.

For example, if you have 1,000 iOS devices, you can create a Blueprint with a restore item, an enrollment profile, a default wallpaper, skip all of the activation steps, install 4 apps, and then enable encrypted backups. The Blueprint will provide all of these features to any enrolling device that the Blueprint is applied to.

Policy Groups

In WebUI, Apple Policy Groups that get deployed onto MDM servers transform into Blueprints for Apple devices.

Policy and apps file locations

- If Apple policy groups are deployed to MDM servers, Blueprints are present in the MDM server at `/var/opt/BESUEM/apple/config/blueprints`
- The profiles staged along with Blueprints (policy groups) are present in the MDM server at `/var/opt/BESUEM/apple/config/profiles`
- Prestaged applications that are referenced in Blueprints are present in the MDM server at `/var/opt/BESUEM/packages`

Chapter 4. Apple VPP Apps and Books

Apple VPP stands for Apple Volume Purchase Program. It is a program offered by Apple that allows businesses and educational institutions to purchase, distribute, and manage Apple Store apps and books in bulk for their employees or students. Through this, organizations can distribute Apple Store apps and books directly to managed Apple devices or authorized users, and keep track of what content has been assigned to which user or device.

To participate in the VPP, organizations need to enroll in the program. Once enrolled, they can purchase apps and other content through the Apple Business Manager or Apple School Manager portal.

BigFix MCM and BigFix Mobile are integrated with the Apps and Books (VPP) capabilities in Apple Business Manager to deliver:

- Custom apps
- Apple Appstore apps
- Company licensed Appstore apps



Note: For a user enrollment, the only way to deliver apps to the device through MDM is via the Volume Purchase Program (VPP).

VPP token

A VPP token, also known as a Volume Purchase Program token, is a unique identifier that is used to connect an organization's MDM server to Apple Business Manager or Apple School Manager. The VPP token is required for the MDM Server to communicate with Apple Business Manager for VPP operations to allocate and release licenses when managing VPP app deployment.

The VPP token is used to authenticate the organization's account when purchasing apps and other content through the VPP. When the organization purchases apps or content, the VPP token is used to tie the purchase to the organization's account. This allows the organization to manage and distribute the purchased content to their employees or students.

It is important to keep the VPP token secure, as it provides access to the organization's VPP account and the ability to purchase apps and content in bulk. If the token is lost or compromised, it should be revoked, and a new token should be generated.

A VPP token is required to communicate with Apple Business Manager to exchange information on purchased apps and any custom apps supported by Apple Business Manager. This token must be available in the MDM Server, and used in all communications between MDM server and ABM.

- Both free and for-fee applications can be assigned/delivered in this way
- VPP provides an app delivery mechanism for user-enrolled (BYOD) Apple devices.

How to download VPP token from ABM

To obtain a VPP token, an organization needs to enroll in the Apple Volume Purchase Program (VPP) through either the Apple Business Manager or Apple School Manager portal. Here are the steps to obtain a VPP token:

1. Go to the Apple Business Manager or Apple School Manager portal (depending on whether you are a business or educational institution).
2. Log in using your Apple ID and password.
3. Click on "Settings" in the sidebar.
4. Click on "Apps and Books".
5. Click on "Volume Purchase Program".
6. Click on "Enroll" and follow the prompts to complete the enrollment process.
7. When prompted, create a VPP token. This token will be a unique alphanumeric code that identifies your organization in the VPP program.
8. Download and store the VPP token securely.

You can then upload the VPP token to WebUI. That flow is driven from WebUI through the "Toggle VPP: option under Apple Volume Purchase Program in the MCM Admin menu.

Apple VPP work flow

Following is the work flow to enable VPP functionality and distribute apps to managed Apple devices:

1. Download VPP token.



Note: You need to have an Apple Business Manager account to log in and download the VPP token.

2. Enable Apple Volume Purchase Program functionality through WebUI.
3. Set up Apple Appstore associations.
4. Create an Appstore App Policy.
5. Add the App policy to a Policy Groups and deploy as necessary.

Unassign VPP licenses on unenroll

If a VPP or Custom app has been deployed on an endpoint, when the device is unenrolled from MCM, any licenses that were allocated are automatically freed up by the MDM server for re-use.

Chapter 5. SCEP Certificate-based authentication

BigFix MCM supports certificate-based authentication through Simple Certificate Enrollment Protocol (SCEP). SCEP is the fastest and most secure way to provision certificates to all your MCM-managed devices. With SCEP, IT Admins can automate issuing certificates to the endpoints to provide access to corporate Wi-Fi, VPN, and secure e-mail through encryption.

Advantages of SCEP

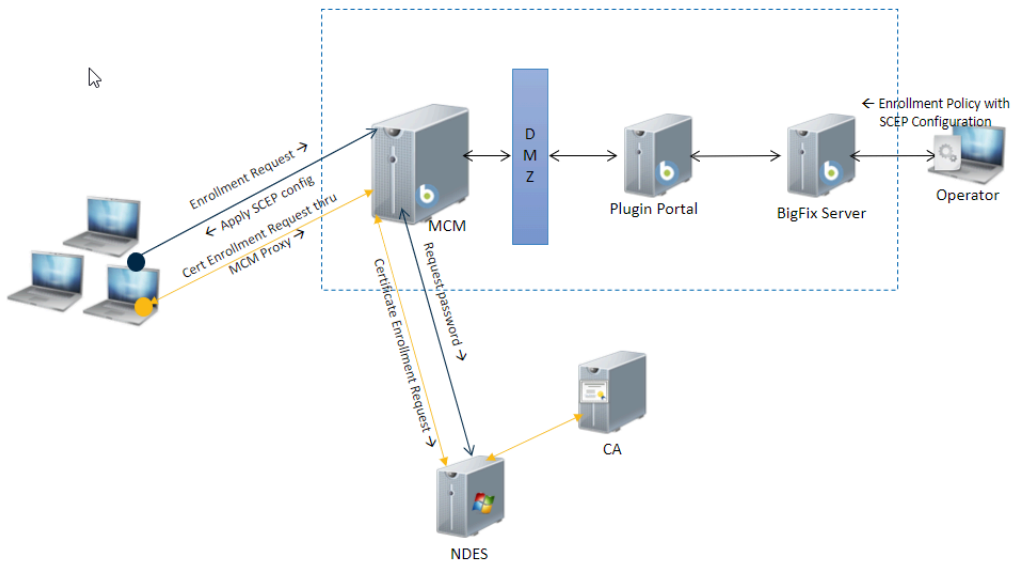
- Facilitates to authenticate users via certificates.
- Ensures secure network communication, where the data is encrypted and authenticated using certificates.
- Simplifies certificate distribution to MCM-enrolled devices.
- Facilitates distributing certificates in huge number of devices.
- Reduces the burden on Network Administrators as the users can request their digital certificate electronically.



Note: SCEP policy is used for distributing client certificates to devices while WebUI certificate policy is used for distributing the CA certificates to devices.

SCEP architecture and communication flow

Certificate Enrollment Workflow



BigFix MCM supports the use of SCEP to authenticate connections to your apps and corporate resources. SCEP uses the Certification Authority (CA) certificate to secure the message exchange for the Certificate Signing Request (CSR). When your infrastructure supports SCEP, you can use *SCEP certificate* policy created through WebUI to deploy the certificates to your devices.

Using this protocol, SCEP servers issue a one-time password (OTP) to the user transmitted out-of-band (OOB). The user generates a key pair and sends the OTP and certificate signing request to the SCEP server, which validates it, signs it, and makes the signed certificate available to the user.

Applicable devices

- Windows 10 and later
- macOS

Supported enrollment methods

- [Autopilot enrollment - Windows \(on page 24\)](#)
- [Bulk enrollment - Windows \(on page 24\)](#)
- [Enrolling through enrollment URL - Windows \(on page 19\)](#)
- [Enrolling through enrollment URL - Apple \(on page 58\)](#)
- [Apple Automated Device Enrollment \(on page 59\)](#)

For information on how to configure the environment to support certificate management and certificate-based authentication through SCEP, see [Simple Certificate Enrollment Protocol \(SCEP\) configuration](#).

For Windows SCEP enrollment flow, see [Windows SCEP enrollment \(on page 55\)](#).

For macOS SCEP enrollment flow, see [macOS SCEP enrollment \(on page 55\)](#).

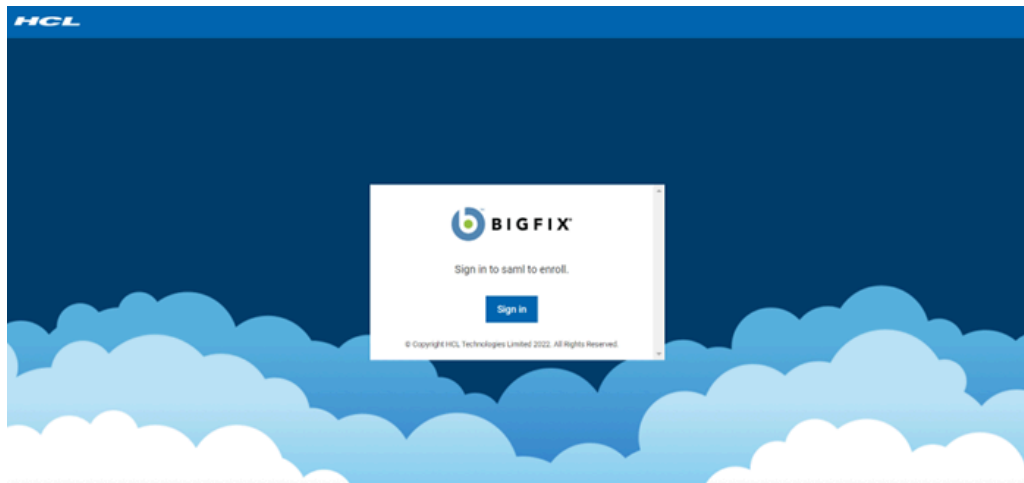
Chapter 6. SAML-authenticated enrolment flow

When you configure SAML as the authentication method, when a user hits the enrollment URL and click Enroll, the user is first authenticated via the identity provider before proceeding with the enrollment process.

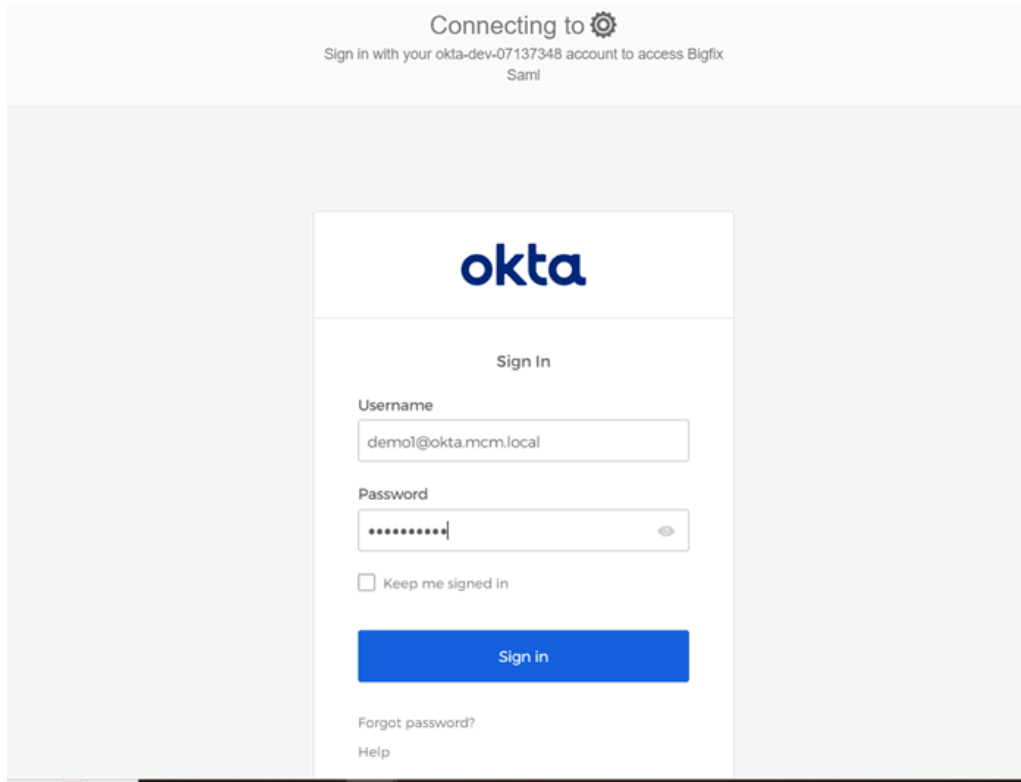
Enrollment flow for a fresh login

When a user visits the enrollment URL for the first time before single sign-on authentication, then initial enrollment flow is as follows:

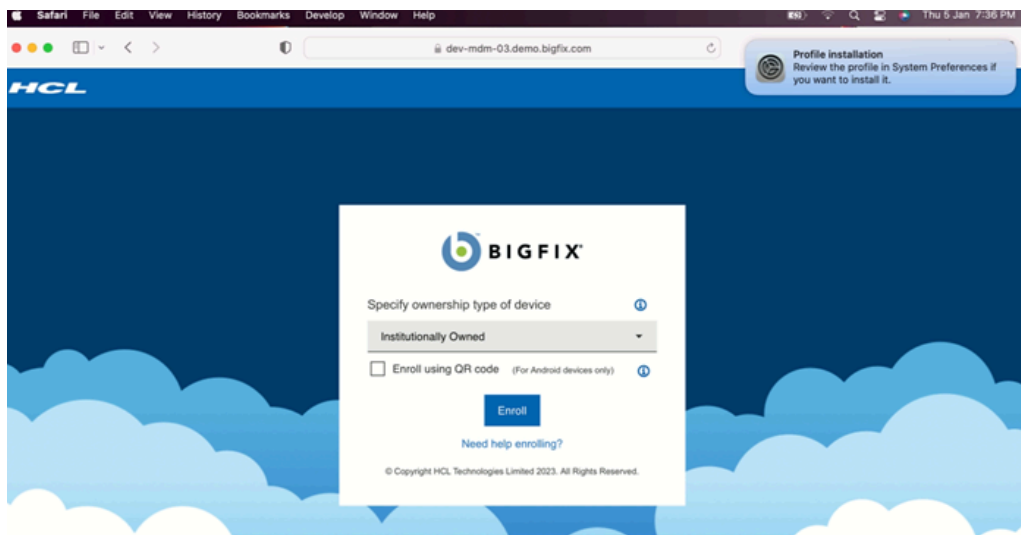
1. On the enrollment page, when the user clicks **Sign in**, the user is redirected to the SAML service for login.



If Okta is configured as the SAML service, user is redirected to Okta Sign in page as follows.



2. With the corporate's identity service credentials to the SAML service, the user is authenticated. After the user logs in to the SAML service, the enrollment page appears:



3. Provide the necessary information and click **Enroll** to begin the MDM enrollment process and access the corporate resources.

Enrollment flow when the session times out

When the logged in session times out for a user, the enrollment flow is same that of a fresh log in.



Note: By default, the session times out after 15 minutes.

Enrollment flow when the user has already authenticated via SAML

When the user has already logged in with SAML authentication, the user can continue to enroll without the need for any further authentication, as SAML is the single sign-on (SSO) authentication that allows the users to log in once and access multiple applications without needing to enter credentials for each application.

Chapter 7. Known limitations

Read this topic to get familiarized with MCM v3.0 known limitations.

Device Ownership attribute limitations for enrolments

In BigFix MCM v3.0, while creating Smart Groups, consider the following recommendations:

- Pre enrollment: Do not use "Device Ownership" as a Device Attribute rule.
- Post enrollment: If you want to use "Device Ownership" as a Device Attribute rule, use the values "Personally Owned" or "Institutionally Owned" (case sensitive) and deploy the policies and Policy Groups directly to a Smart Group.

VPP and Custom App Assume management limitation for BYOD devices

While setting up App association for the apps that need to be delivered to Apple user enrolled devices, do not select the "Assume Management" option. This is because App configuration options on BYOD devices are limited compared to supervised devices. Administrators can only manage settings that don't interfere with the user's personal data. Deploying different application policies with different app management configuration for the same App is not supported in MCM v3.0. Therefore, you can select Assume Management option for delivering apps to supervised devices only.

Chapter 8. Troubleshooting

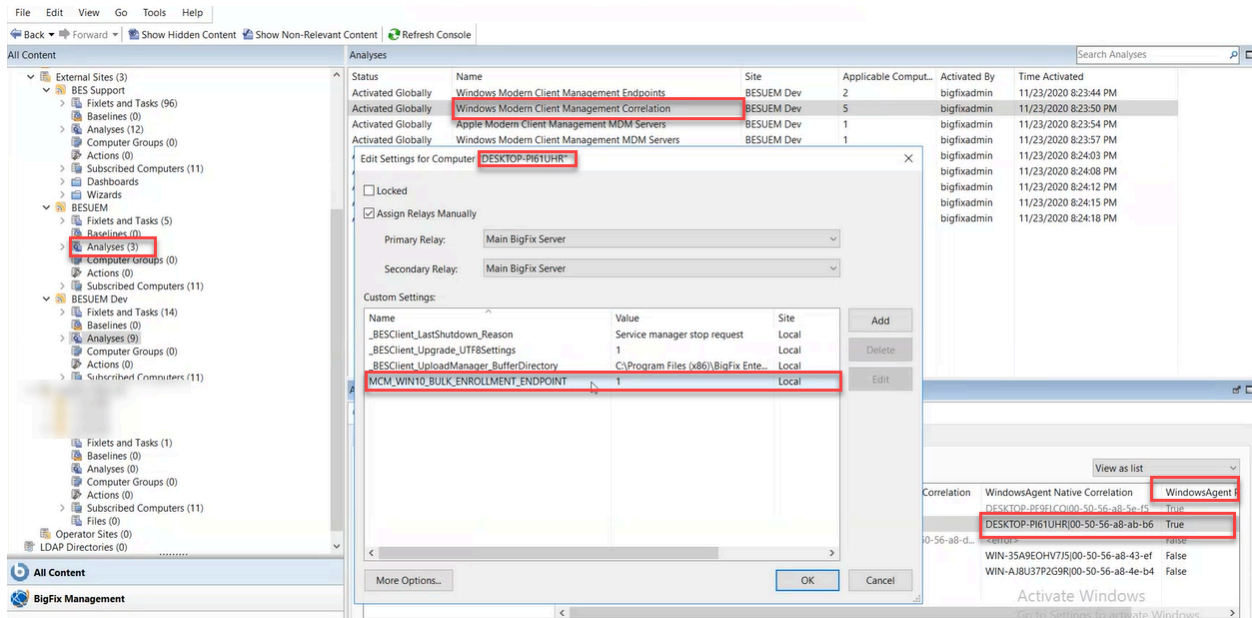
This section is intended to help you solve problems that might occur when installing BigFix MCM and BigFix Mobile.

Verify if PPKG generation point is set for bulk enrollment

To troubleshoot bulk enrollment issues, ensure if the targeted device is designated as the provisioning package generation point.

To do that, in the BigFix Console, go to **BESUEM > Analyses > Windows Modern Client Management Correlation**. For the device you want to verify, check the values of the following parameters.

- The **WindowsAgent PPKG Designation** parameter value becomes True.
- Right click the designated device and select Edit Computer Settings. The client setting **MCM_BULK_ENROLL_ENDPOINT** is set to 1.



Enrollment fails with 401 authentication error

Learn how to resolve the issue when the enrollment fails with 401 authentication error when there is no issue with LDAP.

Problem

Enrollment fails with 401 authentication error. On ping tests, Docker containers could not ping properly. For example, Openresty is not able to reach MDM server.

Cause

DNS resolution issues. Docker containers on MDM server do not resolve DNS network hostnames.

Solution

1. Restart Docker using the service Docker restart command.
2. If the issue persists, if you are not using the DNS, enter the following `extra_hosts` entry manually in the `docker-compose.yml` file at `/var/opt/BESUEM/` and restart the MDM server containers.

```
extra_hosts:
- "<hostname>:<IP>"
```

where `<hostname>:<IP>` is the MDM server hostname and IP Address.



Note:

- You must indent the added entries properly to get the expected result.
 - If the install or upgrade Fixlet is run after the changes in the `.yaml` file, you must add the entries manually again and restart MDM server containers.
3. Login to the `windowismdm` container using `docker exec -it windowismdm sh` and check if the `/etc/hosts` file has the above hostname and IP address entry.
 4. Ping the hostname from within the container to see if it is resolving properly.

The following `docker-compose.yml` screenshot shows the sample `extra-hosts` line added. You must add the `extra-hosts` entries for `windowismdm`, `androidmdm`, and `applemdm` docker containers as applicable for your environment. This allows docker containers to resolve hostnames that are not

```
version: '2'

services:
  openresty:
    container_name: openresty
    image: bigfix/openresty
    restart: always
    extra_hosts:
      - "enroll.bigfix.com:192.168.1.10"
    ports:
      - "443:9443"
      - "9080:9080"
      #server2 instance with /apple location
      - "8443:8443"
    env_file:
      - ${MDM_HOME}/.env
    volumes:
      - certs:/usr/local/openresty/nginx/certs
      - ${MDM_HOME}/openresty/logs:/usr/local/openresty/nginx/logs:z #OPENRESTY_BLOCK
      - ${MDM_HOME}/openresty/termsofuse:/usr/local/openresty/nginx/html/win/termsofuse:z #OPENRESTY_BLOCK
    resolvable.
```

Policy is deployed, but is not effective on the device

This page provides information to troubleshoot the issue if a policy is deployed but is not effective on the device.

Problem

A policy has been deployed successfully through WebUI without error, but the expected policy is not applied to the target device.

Cause

This can be due to various reasons depending on the OS, the policy type such as custom uploaded policy or policy created through WebUI and so on. Some of the reasons are as follows:

- Profile is valid looking but it is missing something or has incorrect values somewhere, so OS says success but does not have the effect expected.
- Profile is valid, but not supported by the version of the OS on the target machine.

For example, in macOS, Restriction policy for screen sharing (where the users cannot enable screen sharing) is supported only in version 10.14.4 and later. See <https://support.apple.com/en-in/guide/mdm/mdmba790e53/1/web/1.0>. To find if the policy is supported on a specific version of the OS, refer the official documentation of the respective OS.

- Device is offline.

Solution

- Ensure you upload policy with appropriate extension for the intended target device.
- Ensure the expected policy is available for the intended target's OS version.
- Ensure the device is online. Deployed policy is applied only when the device becomes online.

Apple profile displayed as unverified

Read this section to troubleshoot if the Apple mobile displays the deployed Apple profile as "Unverified."

Problem

- When an Apple MDM enrollment or MDM policy profile is installed or deployed, the device shows the profile status as "Unverified".
- An Apple profile (Enrollment or Policy Profile) that was verified previously suddenly show as "Unverified" on the device.

Cause

- If you use Digicert certificates, you might encounter this issue when you renew TLS certificate.
- If a TLS certificate is renewed and the Trusted CA has actually replaced/renewed the intermediate certificates (which is not a usual scenario), then it could cause new enrollment and policy profiles to appear as "Unverified" as the signing certificate is signed by an intermediate certificate that is currently unknown to the endpoint.

Solution

- If you have Apple Devices in your MCM deployment, ensure that you run the Update Apple Enrollment Certificate before expiration Fixlet as a policy action. The devices due for their device identity certificate renewal within 45 days are displayed on the main MCM Dashboard in a tile showing Expiring Certificates. With this you can proactively avoid the certificate expiry.
- Re-deploy the Policy in question to a device through WebUI, if you need to correct an Unverified profile".
- If any devices still have "Unverified" enrollment or MDM profiles after these steps complete, contact HCL support for further assistance.

Android Kiosk not connected to Internet

Read this section to troubleshoot Android Kiosk Wi-Fi connection issues.

Problem

Android Kiosk does not get connected to the Internet. Device user is unable to modify the Wi-Fi settings, as it is restricted in Kiosk mode.

Cause

If an Android device boots into an app in Kiosk mode, and if the Wi-Fi network configured in the enrollment policy is not available, the device does not get connected to Wi-Fi network.

Solution

IT admin can configure the enrollment policy to enable the device user to temporarily connect to an available network and refresh Wi-Fi configuration with active settings.



Note: The temporary Wi-Fi connection is only for fetching the latest policy with active Wi-Fi configuration details. Once the latest Wi-Fi configuration policy is applied, the Kiosk device automatically connects to the network as specified in the policy.

To do that, complete the following steps:

1. Ensure the setting `"networkEscapeHatchEnabled": true` is configured in the dedicated device enrollment policy. After booting, if the network connection fails, within 90 seconds, this setting prompts the user to temporarily connect to an available network to refresh the device policy.
2. For the device to get a permanent network connection, add the Wi-Fi configuration policy with active Wi-Fi information.

Sample Wi-Fi configuration policy:

```
"openNetworkConfiguration": {
  "NetworkConfigurations": [{
```

```

"GUID": "a",
"Name": "Example A",
"Type": "WiFi",
"WiFi": {
  "SSID": "NetworkID",
  "Security": "WEP-PSK",
  "Passphrase": "1234567890"
  "AutoConnect": true
}
}
}

```

3. If the device does not connect to the Wi-Fi network automatically, restart the Kiosk device and wait for 1 to 2 minutes. The device gets connected to the Wi-Fi network as defined in the new Wi-Fi configuration policy.

Endpoint not disconnected from AD after unenrollment

Read this page to remove an ODJ-enrolled endpoint from Active Directory (AD) on unenrollment to prevent it from accessing network resources.

Problem

On unenrolling an endpoint from WebUI, if the endpoint was enrolled with ODJ policy, it is disconnected from MDM, but is not removed from AD.

Cause

MCM v3.0 does not support any setting or action that can be invoked to disconnect an unenrolled device from AD.

Solution

Post unenrollment, the AD Admin must manually remove the unenrolled endpoint from AD.

To remove an endpoint from AD, follow these steps:

1. Open Active Directory Users and Computers on a domain controller or a computer with the Active Directory Administration Tools installed.
2. Expand the domain tree and navigate to the container where the computer account is located.



Note: By default, computer accounts are created in the Computers container, but they can also be located in a different OU or container depending on your Active Directory design.

3. Locate the computer account that you want to remove and right-click on it.
4. Select the Delete option from the context menu.

! **Important:** Deleting a computer account in AD does not actually remove the computer from the network or prevent it from accessing network resources. It simply removes the association between the computer and its account in Active Directory, which can cause issues with group policy, security permissions, and other Active Directory-related functions.

- To prevent the deleted endpoint from accessing network resources, remove its DNS record and DHCP lease (if applicable), and disable or remove its network connection.

Health Check MDM Plugin Status is not displayed properly

Read this section to troubleshoot when WebUI Health Check MDM Plugin Status section keeps loading for longer time and does not display the required information.

Problem

In WebUI, the MDM Plugin Status section of the Health Check page keeps loading and does not display the required analyses information.

The screenshot shows the BigFix Modern Client Management interface. The top navigation bar includes 'BIGFIX', 'Devices', 'Apps', 'Deployments', and 'Reports'. The main content area is titled 'Modern Client Management' and has tabs for 'Home', 'Policies', 'Actions', 'Policy Groups', 'Admin', and 'Health Check'. The 'Health Check' tab is active. On the left, there are sections for 'Android MDM Servers' and 'Apple MDM Servers', each with an 'Activate All' toggle. Below these are tables for server details. On the right, the 'MDM Plugin Status' section is highlighted with a red box and is empty. Below it are sections for 'MDM Full Disk Encryption Status', 'Recovery Key Escrow Plugin Status', and 'Vault Escrow Server Status'.

Server Name	Package	Version	URL
beautifulplanet	Yes	1.1.0.166	beautifulplanet.testqa.bes.prod.hclp...
blueplanet	No	1.1.0.166	blueplanet.testqa.bes.prod.hclpnp...

The log shows `Uncaught Error: Unparseable analysis result....`

Cause

If you have duplicate computers in your environment and if your deployment is older than MCM v3.0, you might see this issue. This could be due to some old analysis data.

Solution

To fix this issue, remove the duplicate computers from BES Console. After removing, you can see that the plugin info is displayed appropriately in Health Check dashboard under MDM Plugin Status section.

Generating Encryption Recovery Key Escrow fails

Read this page to troubleshoot Encryption Recovery Key Escrow generation failure when the BigFix Server is installed on RHEL 8.0.

Problem

When BigFix WebUI server is running on RHEL 8.0, if the user tries to generate Encryption Recovery Key Escrow from **MCM > Admin > Recovery Key Escrow > Generate Encryption Recovery Key Escrow**, the action fails.

Cause

This problem occurs only with BigFix deployment on Linux system. WebUI with Node.js v18 does not run on RHEL7. Therefore, it has to be upgraded to RHEL 8. As `libnsl` is not installed on RHEL8 by default, `CryptoUtility` which is downloaded from <http://software.bigfix.com/download/bes/util/CryptoUtility-linux-1.0.0.x64> and saved to `/var/opt/BESServer/Applications/CryptoUtility` fails to run.

Solution

To fix this issue, manually install the `libnsl` by running the following command on the RHEL 8 machine and retry generating Encryption Recovery Key Escrow.

```
yum install libnsl
```

This will successfully run `CryptoUtility` by itself, as well as complete the Generate Escrow Key action from WebUI.



Note: You must register the RHEL instance on RHN for the yum command to run by default.

Chapter 9. Frequently Asked Questions

Read this section for commonly asked questions and their answers to manage the MCM deployments better.

How do I move an existing MCM server environment from one machine to another machine?

If you have already enrolled devices to an MCM server through a specific enrollment URL, and if you want to change the MCM server infrastructure, you must unenroll all the enrolled devices from the original MCM server and re-enroll them to the new MCM server through the new enrollment URL.

Appendix A. Support

For more information about this product, see the following resources:

- [BigFix Support Portal](#)
- [BigFix Developer](#)
- [BigFix Playlist on YouTube](#)
- [BigFix Tech Advisors channel on YouTube](#)
- [BigFix Forum](#)

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).

Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.