ZENworks 2020 Update 3 Troubleshooting Mobile Device Management

November 2021

This section provide solutions to the problems you might encounter while using the Mobile Management feature.

Log Locations

If any of the ZENworks operations fail, then you can check the following logs for additional details:

- **loader-messages.log:** logs messages related to background tasks performed by ZENloader services, which can be accessed from the following locations:
  - On a Windows Server: `%ZENWORKS_HOME%\logs\loader-messages.log`
  - On Linux Server: `/var/opt/novell/log/zenworks/loader-messages.log`

- **services-messages.log:** logs issues related to tasks performed by the ZENworks Server, which can be accessed from the following locations:
  - On a Windows Server: `%ZENWORKS_HOME%\logs\services-messages.log`
  - On Linux Server: `/var/opt/novell/log/zenworks/services-messages.log`
- **zcc.log:** logs issues related to ZENworks Control Centre User Interface related failures while configuring or creating components such as push notifications, bundles, policies, user sources or an MDM server. These logs can be accessed from the following locations:
  - On a Windows Server:

    `%ZENSERVER_HOME%/logs/admin-mgmt` and `%ZENSERVER_HOME%/logs/client-mgmt`
  - On Linux Server: `/var/opt/microfocus/log/zenworks/admin-mgmt` and `/var/opt/microfocus/log/zenworks/client-mgmt`

  NOTE: References to `%ZENWORKS_HOME%` indicates the following default path that can be changed during installation: `C: \Program Files\Novell\ZENworks.`
- **zapp.log:** logs issues related to the ZENworks Agent App installed on Android devices. For logs within a Work Profile, the administrator needs to approve a file manager app using which the file can be viewed in the device.
- **eup-casa.log:** logs issues related to zenworks-eup login. The logs can be accessed from the following locations:
  - On a Windows Server: `%ZENWORKS_HOME%\logs`
  - On Linux Server: `/var/opt/novell/log/zenworks/`

The following table lists some of the possible troubleshooting scenarios along with details of related log files that might help you resolve the issues:

Scenario	Logs
Apple Volume Purchase Program	
Unable to create a VPP subscription.	zcc.log, services-messages.log
VPP Subscription has failed to replicate bundles based on apps approved in Apple VPP.	loader-messages.log
VPP Bundle distribution has failed on the device	services-messages.log
ActiveSync Server	
ActiveSync server creation fails in the ZCC wizard.	zcc.log
Failed to establish a connection with the ActiveSync server.	services-messages.log
Android Enterprise	
Unable to create an Android Enterprise Subscription	zcc.log, services-messages.log
The subscription has failed to replicate bundles based on apps approved in the managed Google Play Store.	loader-messages.log
Work profile enrollment has failed	services-messages.log, zapp.log (on the personal side of the device)
Work managed enrollment has failed	services-messages.log

Scenario	Logs
Apple Device Enrollment Program	
Unable to assign the DEP server role to an MDM Server.	zcc.log, services-messages.log
DEP device enrollment fails	services-messages.log
Intune App Management	
Microsoft Graph API configuration fails	zcc.log, services-messages.log
Failed to create an Intune App Protection policy	zcc.log, services-messages.log
iOS Bundles	
Failed to create an iOS bundle	zcc.log, services-messages.log
Failed to distribute an iOS bundle	zcc.log, services-messages.log
Push Notifications	
APNs certificate import has failed	zcc.log, services-messages.log
Mobile Security and Control Policies	
Device control policy settings are not applied on the device	zcc.log, services-messages.log. For an Android device, check zapp.log on the device.

Intune App Management

Microsoft Graph API Configuration fails

Explanation: Microsoft Graph API configuration in ZENworks fails.

Possible Cause: Some of the reasons for failure are:

- ZENworks Server using which Microsoft Graph API is configured does not have outbound connectivity to contact the Azure portal.
- Pop-up blocker is not disabled on the browser using which Microsoft Graph API is configured. Disable the pop-up blocker and try again.

iOS Intune App Protection Policy creation fails in ZENworks.

Explanation: iOS Intune App Protection policy creation fails in ZENworks.

Possible Cause: Some of the reasons for failure are:

- ZENworks Server using which Microsoft Graph API is configured does not have outbound connectivity to contact the Azure portal.

- The access token is either invalid or has expired. You need to renew the token, in ZCC, by navigating to **Configuration** > **Management Zone Settings** > **Intune App Management** > **Renew Token**. After renewing the token, you need to start creating the policy again.
- The Microsoft Graph API is either not configured or is deleted from ZENworks. To configure it, navigate to **Configuration** > **Management Zone Settings** > **Intune App Management**. After configuring the account, you need to start creating the policy again.

The creation or modification of iOS App Protection policy succeeds in ZENworks but fails in Azure

Explanation: iOS Intune App Protection Policy is created or modified (such as copying or renaming the policy) successfully in ZENworks but the creation or modification of the same policy fails in the Azure portal.

Possible Cause: Some of the reasons for failure are:

- ZENworks Server is facing some network connectivity issues.
- The access token is either invalid or has expired. You need to renew the token, in ZCC, navigate to **Configuration** > **Management Zone Settings** > **Intune App Management** > **Renew Token**.
- The Microsoft Graph API is either not configured or is deleted from ZENworks. To configure it, navigate to **Configuration** > **Management Zone Settings** > **Intune App Management**.

Action: After resolving the issue, you need to undo the operation in ZCC and retry. For example: If copying of the policy succeeds in ZENworks but not in Azure, you need to resolve the issue, delete the copy of the policy created in ZENworks and then copy the policy again.

The deletion of iOS App Protection policy succeeds in ZENworks but fails in Azure

Explanation: iOS Intune App Protection Policy is deleted (such as copying or renaming the policy) successfully in ZENworks but the deletion of the same policy fails in the Azure portal.

Possible Cause: Some of the reasons for failure are:

- ZENworks Server using which is facing some network connectivity issues.
- The access token is either invalid or has expired.
- Microsoft Graph API account was already removed from ZENworks.

Action: Visit the Azure portal to manually delete the iOS Intune App Protection Policy.

Token renewal fails if the process is initiated from another ZENworks Server

Explanation: When there are multiple Primary Servers in the zone and the redirect (callback) URL of a particular ZENworks server is specified in the Microsoft portal while configuring Microsoft Graph API, then token renewal fails if the process is initiated using a different ZENworks server and not the server whose callback URL is specified in the Microsoft App Registration portal.

Action: Modify the redirect URL in the Microsoft App Registration portal to the redirect URL of the ZENworks server using which you want to renew the token.

Apple DEP

DEP Server creation fails if certain mandatory information is missing in the uploaded token

Explanation: While uploading a token, if certain mandatory information such as the Server GUID or the Virtual MDM Server name is missing in the token, then the DEP server creation fails. This might occur if the Device Manager role is not added to your Apple account.

Action: Ensure that you add the Device Manager role to your Apple account and re-generate the token in the DEP portal. If this role is already linked to your account, then contact the customer support team.

DEP enrollment fails if the user initially skips applying the MDM Profile on the device

Explanation: While enrolling a device through Apple DEP, if the user initially skips DEP enrollment (if **Allow user to skip applying the MDM profile on the device** is enabled in the assigned DEP profile) and returns to the previous page to allow DEP enrollment, then the enrollment fails.

Action: To enroll the device, reset the device to its factory settings.

DEP enrollment does not proceed further after specifying assigned user credentials

Explanation: During DEP enrollment, if the device is assigned to a specific user and the user specifies their login credentials, DEP enrollment might not proceed to the next screen.

Action: Ensure that the user credentials entered are correct.

DEP enrollment fails while re-enrolling a retired device

Explanation: A device that was retired by another user is now being re-enrolled via Apple DEP. However, DEP enrollment fails after the new user enters his/her credentials.

Action: Ensure that you delete the device object of the retired device in ZCC, before you proceed with re-enrollment.

MDM Servers

While configuring access controls to secure an MDM Server, Administration access is denied for all

Explanation: While configuring access controls to secure an MDM Server, Administration access is denied for all and ZCC remains inaccessible except from the server in which the access was allowed or denied.

Action: Change the configuration by accessing ZCC from the MDM Server in which the access was denied. You can access ZCC in the following ways:

- Enter the Server IP.
- Enter https://localhost (applicable for IPv4 addresses only)
- Enter the loopback address.

If you are still unable to access ZCC, then delete the configuration file `access-filters.json` from the directory available at `%ZENWORKS_HOME%/share/tomcat/conf`. Restart the MDM server. Administration access will be allowed for all. You need to navigate back to ZCC and re-configure the access controls.

After configuring access controls to secure an MDM Server, an IP address of a device that is denied access is still able to contact the ZENworks Server

Explanation: While securing an MDM Server, a specific IP address of a device is denied access to the server. However, this device is still able to contact the MDM Server.

Action: Enable the Tomcat valve logging to check the logs. For more information, see Tomcat Valve Logging.

Also, check whether the device is communicating with the ZENworks Server using a proxy server. If so, you need to deny access to the IP address of the proxy server, if other devices are not using this proxy server.

Mobile devices are unable to contact the ZENworks Server

Explanation: Mobile devices are unable to communicate with the MDM Server.

Action: Verify that the Primary Server, to which the device is enrolled, still has the MDM Server Role. Since mobile devices contact the MDM Server to which they are enrolled and if mobile devices are enrolled to a server that you have chosen to remove from the zone, then you will have to re-enroll these mobile devices to the zone using another MDM Server. Before re-enrollment, ensure that you delete the corresponding device objects in ZCC. However, if you are upgrading or replacing the MDM Server with another server, then the enrolled devices will automatically reconcile with the replaced server.

NOTE: Also, if you delete all the MDM Servers in the zone, then the Push Notifications configuration (APNs and GCM) will be automatically deleted.

APNs keystore fails to replicate on a newly added MDM Server in the zone

Explanation: When a new MDM Server is added in the zone, the APNs keystore is replicated on this server by retrieving the keystore from one of the existing MDM Servers.This will ensure that the newly added MDM Server also has the capability to communicate with the APNs server. However, if the existing MDM Server is not connected to the network, the APNs keystore fails to replicate on the new MDM Server.

Action: When you add a new MDM Server to the zone, ensure that all the MDM Servers are online. After you ensure that the existing MDM Servers are online, remove the MDM role from the newly added MDM Server and re-assign it to the same server.

Push Notifications

APNs certificate import fails

Explanation: While configuring the Apple Push Notification service in ZENworks, APNs certificate import fails.

Action: Check the ZCC.log or the service-messages.log of the MDM Servers. If the failure is due some issue with the APNs Keystore, try restarting the server and then import the certificate. If `CertificateNotYetValidException` is displayed as the reason for failure, then this indicates that the MDM Server time is ahead of the certificate creation time. You need to wait for a while and then try importing the certificate.

Push notifications to enrolled devices will not work as expected, if the APNs certificate has expired and a new certificate is imported

Explanation: When the existing APNs certificate has expired and you create a new certificate in the Apple Push Certificates portal and import it to ZENworks, then the push notifications to mobile devices, which were enrolled using the earlier certificate, will not work as expected.

Action: Re-enroll the devices. As a best practice, if the APNs certificate has expired, it is recommended that you **Renew** the certificate in the Apple Push Certificates portal instead of creating a new certificate. For details, see Enabling Push Notifications.

While migrating from Google Cloud Messaging (GCM) to Firebase Cloud Messaging (FCM), an error is displayed if the Project Number does not match with that of the existing GCM project

Explanation: While migrating from GCM to FCM, the following error message is displayed on uploading the .JSON file: “The Project Number included in this .JSON file does not match with the Project Number specified in the existing GCM project. Ensure that the .JSON file includes the correct Project Number”.

Action: While migrating the GCM project to FCM, use the same login credentials that was used to create the GCM project.

If you are unable to obtain these credentials, then execute the `zman sgd` command to remove the existing GCM values from the ZENworks database. Restart the ZENworks services and then proceed to upload the .JSON file to configure the new FCM project.

ActiveSync

If a device enrolled as an ActiveSync Only device is fully wiped and deleted, then re-enrollment of the same device fails

Explanation: If a device that is enrolled as an ActiveSync Only device is fully wiped and deleted using the **Unenroll** quick task, then you will be unable to re-enroll the same device to the ZENworks Management Zone.

Action: In the database, the `TobeDeleted` value for the device object in the `zZENObject` table, should be updated to 1.

Email accounts might not work properly on some mobile devices if an ActiveSync server is added after the devices are enrolled

Explanation: If a device is already enrolled to the ZENworks Management Zone and an ActiveSync server is configured later, then the email accounts on some of these devices might not receive emails.

Action: For Android devices:

- You might be prompted to re-enter your account password. If this does not work, either initiate a Refresh action on the email account configured on the device or initiate a Refresh action from the Settings menu on the device.

For Windows devices:

- Delete and re-create the email account on the device.

NOTE: For iOS devices, the email client might display an error message a couple of times, after which you will start receiving emails on the device.

As a best practice, it is advisable to configure an ActiveSync server before a device is enrolled to the ZENworks Management Zone.

Email accounts cannot be re-configured, if remote wipe is initiated on the ActiveSync Server.

Explanation: If a remote wipe is initiated directly from the ActiveSync Server, then the email account configured on the device will stop receiving emails. However, the device object is retained in ZENworks Control Center. Whenever the user tries to re-create the email account, the data on the device is wiped.

Action: As a best practice, it is advisable to fully wipe and retire the device. Subsequently, you can click **Delete** to remove the device from the zone.

During email account configuration, user authentication to ActiveSync Server fails

Explanation: While configuring an email account on a device using a Mobile Email Policy, the user credentials are obtained from the configured user source and in turn authenticated with the ActiveSync Server. The user is logged in to the email account, if the credentials provided in the user source match with the ones configured in the Activesync Server. However, the user credentials with which the user logs into the ActiveSync Server to retrieve emails might be different from the credentials that he/she uses to login to the LDAP directory, due to which the email account fails to send or receive emails.

Action: Select the ActiveSync Server login attribute in the User Source to ensure that the user credentials considered for authentication are the same. For more information, see Configuring the Attribute for ActiveSync Server Authentication.

Email accounts on some devices might stop functioning and an authentication error is displayed

Explanation: On a few devices, the configured ActiveSync accounts might stop functioning and an **Authentication Error** notification is displayed. In some cases, this notification recurs even if the user has specified the account credentials and in some cases the device does not respond on clicking this notification.

Action: Delete and re-create the email account on the device.

Enrollment

Status of a newly enrolled iOS device is displayed as Pending Enrollment in ZENworks User Portal, until the browser is refreshed

Explanation: The status of a newly enrolled iOS device is displayed as **Pending Enrollment** in the ZENworks User Portal even though the device object has moved from the **Pending Enrollment** folder to **Devices** > **Mobile Devices** folder in ZCC. Tapping the Home icon or the Sync Now icon in the ZENworks User Portal does not update the status of the enrolled device.

Action: Refresh the ZENworks User Portal browser to view the updated status of the device as **Active**.

If the time on an Android device lags behind the time on the ZENworks Server, then device enrollment will be unsuccessful

Explanation: The time on an Android device lags behind the time on the ZENworks Server. During device enrollment, when the user logs into the ZENworks mobile app, the enrollment process does not advance to the next stage.

Action: Ensure that the time on the device and the ZENworks Server is the same and then try re-enrolling the device.

Re-enrollment of a device might fail with a Constraint Violation exception

Explanation: When a device object, which is associated with a device that has unenrolled from the zone, is deleted from ZCC, then re-enrollment of the same device might fail and a Constraint Violation exception is displayed in services-messages.log. Constraint violation exception indicates that the device object from the previous enrollment is not deleted from the database.

Action: After deleting the device object, you need to wait for the loader process to remove the device object details from the database. This process might take around 10 to 15 minutes, after which you can try re-enrolling the device again. If the error persists even after multiple attempts to re-enroll the device, then contact Customer Care.

A retired iOS DEP device does not sync with the ZENworks Server on unretiring it from ZCC

Explanation: Consider a scenario, where the user needs to take an iCloud backup of an iOS device enrolled through Apple Device Enrollment Program (DEP). After taking a backup, the device is retired in ZCC using the **Unenroll Device** quick task. On restoring the backup, the device is unretired in ZCC using the **Unretire Device** action. On unretiring, the device does not automatically sync with the ZENworks server and does not reconcile with the unretired device object in ZCC.

Action: After unretiring the device, delete the ZENworks Management profile from the device and try re-enrolling the device using the ZENworks End User Portal. However, this workaround is applicable only for those devices that allow for removal of the ZENworks Management profile.

To ensure that the device automatically syncs with the ZENworks server after restoring the iCloud backup, refer to the following steps:

1. After taking an iCloud backup instead of retiring the device in ZCC, use the reset option on the device.
2. When the device restarts, restore the backed up data in the Apps and Data screen. Ensure that the option to skip this screen (Restore apps and data) is not enabled in the DEP profile.

After restoring from backup, the device will automatically sync with the ZENworks server.

During ActiveSync enrollment of an already enrolled fully-managed Android device, automatic reconciliation to the existing device object fails

Explanation: Consider a scenario, where an Android device is enrolled to ZENworks as a work profile device (fully-managed). To manage emails on the device, a Mobile Email Policy is assigned that uses ZENworks as the proxy server between the configured ActiveSync Server and the device. The user then re-enrolls the device to the zone as an ActiveSync (Email only) device. However, during ActiveSync only enrollment, the device fails to automatically reconcile with the existing device object in ZCC and a duplicate device object is created.

Action: To ensure that a duplicate device object is not created in ZCC during re-enrollment of a device, you can either:

- **Allow the user to manually reconcile the device:** by enabling the setting in the assigned Mobile Enrollment Policy. For more information, see the Mobile Management Reference.
- **Enable direct communication with the configured ActiveSync server:** by selecting the option **Do not use ZENworks Server as Proxy Server** in the assigned Mobile Email Policy. The device can directly send or receive emails from the configured ActiveSync server. For more information, see the Mobile Management Reference.

Quick Tasks

If the time on the ZENworks Server lags behind the actual enrollment time of a mobile device, then any quick task that is sent to this device within this time period is not processed and its status will remain as Initiated

Explanation: When a mobile device is enrolled to the zone and the ZENworks Server time lags behind the enrollment time of this device, then any quick task that is sent during this time period, is not processed and the status of the quick task remains as **Initiated**.

Action: You need to wait until the ZENworks Server time is equal to or exceeds the device enrollment time, before sending a push notification, such as quick tasks, to the device.

Apple Volume Purchase Program

VPP bundle creation fails

Explanation: At times, VPP bundle creation might fail due to the reasons listed below.

Possible Cause: Some of the possible reasons are:

- The Apple Server is busy and not responding.
- Apple is unable to provide the latest app metadata as Apple might have discontinued support for the app.
- Apple has extended VPP support to a new country, which is not supported by ZENworks. Contact the Micro Focus tech support team to include this country in ZENworks.

VPP bundle distribution fails

Explanation: At times VPP bunle distribution might fail due to the reasons listed below.

Possible Cause: Bundle distribution might fail due to the following reasons. Check the bundle **Deployment Status** to identify the reason for failure.

- A VPP bundle is assigned to a device with iOS version prior to 9.0. Apple supports device assignments on iOS versions 9.0 or newer.
- A VPP bundle is assigned to a user and the invite to associate with the Apple VPP is not accepted by the user.
- A VPP bundle is assigned to a user and the Apple ID on the user's device is different from the Apple ID that the user has used to associate with the Apple VPP.
- The app is not compatible with the device.
- Deficit in the number of licenses.
- The Apple VPP subscription is disabled or deleted.
- The VPP token ownership has changed and is being used by another MDM solution.
- Apple is unable to validate the iTunes Store ID of the specific app.
- The app has discontinued in the iTunes Store.

For an Apple School Manager Account, bundle creation for associated apps that are linked to a specific location might fail in ZCC.

Explanation: When VPP purchases, made in Apple School Manager, are linked to a location and a non-location specific server token is uploaded in ZCC, then bundle creation for these apps fails.

Action: To support location based assets, VPP in Apple School Manager uses location tokens. Therefore, the server token that you upload in ZCC should be linked to the same location as that of the purchased apps. To download the server token for a specific location, in the Apple School Manager portal, navigate to **Settings** > **Apps and books** > **My Server Tokens** and click download against the location of the token that you want to download. For more information on Apple School Manager, see the Apple Documentation.For more information on how to upload a server token in ZCC, see Linking ZENworks to the Apple VPP Account.

Purchased license count is not updated, if sync to retrieve latest VPP apps is initiated immediately after purchasing an app

Explanation: If a sync between the ZENworks Server and the Apple Server is initiated immediately after purchasing an app using the Apple VPP account credentials, then the purchased license count might not be updated with these latest app purchases. Subsequently, bundle assignments might fail.

Action: Ensure that you verify the purchased license count for that specific app in the Apple VPP License Summary page, before assigning that app to a device or a user. Wait for the next sync or re-initiate the sync to update the purchased license count.

While uploading or renewing a VPP token, an appropriate error message is displayed and the subscription renders as unusable.

Explanation: If the existing token or the renewed token is managed by another MDM solution, then an appropriate message is displayed and the subscription renders as unusable.

Action: Delete this subscription and create a new subscription. To continue using the same token, you need to claim management of the token.

Policies

EUP session becomes inactive when a Mobile Security or Device Control Policy is applied on iOS devices

Explanation: A Mobile Security Policy or a Mobile Device Control Policy, with modifications to the Safari browser settings, is assigned to an iOS Device. When a device refresh is initiated in the End User Portal (EUP) on a Safari browser, as soon as the policies are effective on the device, the EUP session is logged out.

Action: None. Log in to the EUP session again.

Mobile Security policies might not apply automatically on a few Android devices

Explanation: Mobile Security policies assigned to devices might not apply automatically on a few Android devices.

Action: Initiate a Refresh action on these devices.

Windows mobile devices do not accept alphanumeric or complex characters even if they are enabled in the assigned Mobile Security policy

Explanation: When a Mobile Security policy, which has alphanumeric or complex characters enabled as a part of the Password settings, is assigned to a Windows device, the device keeps prompting for Personal Identification Number (PIN) and does not accept alphanumeric or complex characters.

Action: None. This is a Microsoft limitation.

Simple passwords are accepted by a few Android devices even if the setting is disabled in the assigned Mobile Security policy

Explanation: When a Mobile Security policy, in which the simple password setting is disabled, is assigned to Android devices, a few of the Android devices might still accept a simple password.

Action: None.

Max Grace Period and Max Inactivity Timeout restriction settings might display incorrect values on the device

Explanation: The **display the passcode screen on unlock** (max grace period) and **maximum inactivity timeout** values specified in the mobile security policy that is assigned to an iOS device, might display incorrect values when viewed on the device. However, this does not affect the behavior of the device lock feature as the values specified while defining the mobile security policy in ZENworks Control Center (ZCC) are applied.

Action: None

Mobile Security Policy does not enforce a password on certain work managed Android 8.0 devices

Explanation: When a Mobile Security Policy with password restrictions enabled is assigned to certain Android 8.0 work managed devices, on which no passwords have been set, the policy does not enforce a password on the devices.

Action: You can either apply the latest security patch level applicable for Android 8.0 devices (for details contact your device manufacturer) or update your operating system version to 9.0 or a later version.

Bundles

Variable specified while configuring bundle app parameters, appears as is when the app is pushed to the device

Explanation: Both built-in as well as custom variables can be specified as key value pairs or in the configuration file while configuring specific app parameters. However, these variables appear as is when the application is pushed to the device. This might happen if an incorrect variable is specified.

Action: Ensure that you have provided the correct variable or the specified variable is defined in ZCC.

Android Enterprise

The user is unable to access the managed Google Play Store on the device as the Google user account or its token has expired

Explanation: Occasionally, the accounts or their tokens with which managed Google Play is accessed on the enrolled device, expires due to the following reasons:

- The authentication token that was obtained to add the account to the device has expired.
- The account or enterprise has been deleted.
- Automatic abuse checks are triggered on Google servers.

In such cases, the enrolled user will not be able to access the managed Google Play store on the device and a message stating that the account has expired is logged against the device in ZCC.

Action: If the user is still not able to access the managed Google Play Store, then on accessing the ZENworks Agent App on the device, the user needs to click the refresh icon. Alternatively, you can also refresh the device from the ZENworks server. A new Google user account or token will be automatically created.

NOTE: If you want re-enroll a retired device and if the accounts or their tokens has expired, then on unretiring the device and on accessing the ZENworks agent app on the device, the following error message is displayed and the app is automatically uninstalled from the device.

Your device could not be enrolled to ZENworks. To re-initiate enrollment, enable the ZENworks Agent App in the Google Play Store.

Subsequently, the user can access the Google Play store to re-install the app and the user should re-enroll the device to ZENworks. The device will automatically reconcile with the existing device object in ZCC.

If for any reason, the user is still not able to access the managed Google Play Store, then refer to the server logs to gather more information on this issue.

Device enrollment fails with a message that indicates that the prerequisites required to enroll the device have not been met.

Explanation: When a user enrolls an Android device either in the work profile or the work-managed device mode, then the enrollment fails and an error message `"The prerequisites required to enroll this device in the work profile or work-managed device mode have not been met. Please contact you administrator"` is displayed.

Possible Cause: This error might occur due to one of the following reasons:

- An Android Enterprise Subscription is not created.
- The user is not a part of the user source associated with the Android Enterprise Subscription.
- A Mobile Enrollment policy and an Android Enterprise Enrollment policy are not assigned to the user who is a part of the user source associated with the Android Enterprise Subscription.
- The Android Enterprise Enrollment policy is assigned to a device instead of a user. If a new device is being enrolled to ZENworks, then you need to assign the Android Enterprise Enrollment policy to the users of these devices. Device assignments are supported only for those devices that have already been enrolled using the Device Admin API (the basic mode of enrollment) and need to be re-enrolled to the zone in the work profile or work-managed device mode.

  NOTE: From the ZENworks 2017 Update 4 release onwards, the basic mode of enrollment has been deprecated.

- The device is not Android Enterprise capable.

Action: Identify the exact reason for the error from `service-messages.log` (for server-related log messages) and `zapp.log` (for device-related messages), fix the issue and try enrolling the device again. For more information on the location of these logs, see Log Locations.

Work-managed device enrollment fails

Explanation: Work-managed device enrollment fails.

Possible Cause: Some of the reasons for failure are:

- The Google Play Store on the device is not the latest version and requires an update.
- The Android Enterprise subscription in ZCC is not associated with the user whose device has failed to enroll.
- The Android Enterprise policy is not assigned to the user whose device has failed to enroll.

Unable to access GroupWise emails on enrolled devices using the Gmail app that was remotely configured in ZENworks

Explanation: The GroupWise email account configured in the Gmail app might not be accessible, if the app was remotely configured using the Managed Configuration feature in ZENworks.

Action: Ensure that you specify the email address of the user (or the ${Email} variable) in the username field while remotely configuring the Gmail app in ZENworks. This is a GroupWise limitation.

Unable to associate user context with the Android Enterprise Subscription

Explanation: When you are creating an Android Enterprise Subscription an error occurs while associating a user context.

This might be because of any of the following reasons:

Scenario 1: The selected user context might already be associated with a subscription that is already unenrolled. The data associated with unenrolled subscription will be deleted only after 30 days.

Action: After unenrolling the Android Enterprise Subscription, delete the subscription data. To delete the subscription data run the `zman sca` command.

Scenario 2: Both Parent and child user are associated to the same Android Enterprise Subscription.

Action: Both parent and child user context cannot be associated with the same subscription. Depending on your requirement, you can remove either child or parent user context.

An error Work profile can't be created because you've reached the maximum number of users on your device. Remove at least one user and try again is displayed on certain devices while trying to setup the work profile again.

Explanation: When the work profile setup on a device is initially interrupted and ZENworks tries to setup the work profile again after a device reboot, then the error **Work profile can't be created because you've reached the maximum number of users on your device. Remove at least one user and try again** might be displayed.

Action: Remove the work profile that might have been setup initially by navigating to **Settings** > **Accounts** > **Remove work profile**, reboot the device and retry work profile setup. If the problem persists, remove any additional users from the device and retry work profile setup.

When a device becomes compliant and restrictions are removed, app shortcuts on the home screen might not be restored

Explanation: When an Android device becomes non-compliant, work apps are restricted and app shortcuts in the home screen are hidden. However, when the device becomes compliant, the work apps are enabled but the shortcuts in home screen are not restored.

Action: None

Work profile setup fails on an Android O device that already has work profile

Explanation: While setting up the work profile on an Android O device that already has a work profile set up from another EMM vendor, the work profile setup process might fail to remove the existing profile automatically.

Action: Manually remove the existing work profile before setting up the work profile using ZENworks.

On certain devices, apps fail to install but is made available in managed Google Play store

Explanation: During bundle assignment, the **Allow users to install from the managed Google Play store** remains unchecked for the app to silently install on the device. However, at times, instead of installing the app, it is made available in managed Google Play store.

Action: Install the app from managed Google Play store.

Work profile enrollment fails on certain Android 5.0 devices

Explanation: An Android 5.0 or 5.0.x device fails to enroll in the work profile mode, even if an Android Enrollment Policy is assigned,

Action: None. The device might not be Android enterprise capable.

Certain work apps crash when the user logs in to those specific apps

Explanation: When a user tries to log in to an app within the work profile, the app crashes or does not respond. This might happen if the app requires the user to add another account, which is by default disabled by ZENworks.

Action: Navigate to the **Mobile Device Control Policy** assigned to the user, select Android and enable the **Allow Adding of Account** Setting. This setting will enable users to add accounts within the work profile. However, this setting should be used with caution, as by enabling it users can also add their personal Google accounts and download personal apps within the work profile, which might make it difficult to contain corporate data within the profile workspace.

As a best practice, it is recommended that you pre-configure the app and deploy it using the Managed Configurations feature in ZENworks.

ZENworks Agent App

When the ZENworks Agent app contacts the server to obtain the new certificate after the CA remint activation date, the status of the system update is momentarily displayed as failed

Explanation: The ZENworks app installed on an Android device, which was offline during the period from CA remint initiation to activation, contacts the server only after the certificate activation date, then a message is displayed requesting the user to accept the new certificate. After the user accepts the request, the **Update Assigned** status for this device is momentarily displayed as **Failed** and changes to **Successful** after the next refresh.

Action: None

The ZENworks Agent App shortcut crashes when the app is updated

Explanation: When the latest ZENworks update is applied on the ZENworks Agent app, then on clicking the app shortcut in the home screen, it crashes with the error **App not installed**. However, the updated app is installed correctly.

Action: Remove and add the app shortcut again. You can also open the app from the launcher.

On opening the ZENworks Agent App, an error **Device is no longer enrolled with server. Please reinstall the app and enroll the device again** is displayed.

Explanation: On opening the ZENworks Agent app on a device that is enrolled to ZENworks, the following error is displayed **Device is no longer enrolled with server. please reinstall the app and enroll the device again**.

Action: You need to perform the following:

1. Check whether the device object is present in ZCC or not.
2. If the device object is not present in ZCC, then uninstall and re-install the ZENworks Agent app. Re-enroll the device to ZENworks.
3. If the problem persists, disable Device Administrator for the app, clear the app data and open the ZENworks Agent app again. To clear the app data, perform the following steps:

   NOTE: A Moto E4 Plus device with Android version 7.1.1 was considered to provide the following navigation path, which may vary based on the Android version or the device manufacturer.

   a. Navigate to **Settings** > **Security** > **Device Administrator**. Deselect ZENworks checkbox and follow the prompts to complete deactivating Device Administrator.
   b. Navigate back to the **Settings** menu, click **Apps** > **ZENworks** > **Storage** > **Clear Data**. Follow the prompts to complete clearing the app data.
   c. Open the ZENworks Agent app.

Miscellaneous

Enrolled mobile devices might not work as expected, if a user source is deleted and the same user source is re-configured.

Explanation: If a configured user source is deleted and the same user source is configured again, then you will be unable to manage mobile devices enrolled using the earlier user source.

Action: Re-enroll the devices. As a best practice, ensure that you delete the device objects of these devices that are already present in ZCC and then re-enroll these devices.

Activation lock bypass code cannot be retrieved from an iOS supervised device

Source: ZENworks 2017 Update 2

Explanation: For some iOS supervised devices even if the Activation lock bypass setting is enabled in ZCC, the activation lock bypass code cannot be retrieved from the device.

Action: Reset and re-enroll the device.

Legal Notice