ZENworks 2020 Troubleshooting Mobile Device Management

October 2020

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

1 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: `%ZENWORKS_HOME%\logs\zcc.log`
  - On Linux Server: `/var/opt/novell/log/zenworks/zcc.log`

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. This can be found on the device at: `storage/emulated/0/ZENworks/logs`. 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.

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
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	

Scenario	Logs
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.

2 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.

3 Apple DEP

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.

4 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.

5 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.

6 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.

7 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.

8 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.

9 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.

10 Policies

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

11 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.

12 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.

13 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.

14 Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.novell.com/company/legal/.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.