SAP NetWeaver Mobile Administration & Monitoring Overview

Applies to:

SAP NetWeaver Mobile 7.10 SP03 onwards.

For more information, visit the Mobile homepage.

Summary

The aim of this guide is to help the organizations using SAP NetWeaver Mobile 7.10 to know the job description of a “Mobile Administrator” and describe the various monitoring and administrating tools available in the NetWeaver Mobile Administration and Monitoring portal.

Author: Rahul Saxena

Company: SAP LABS, INDIA

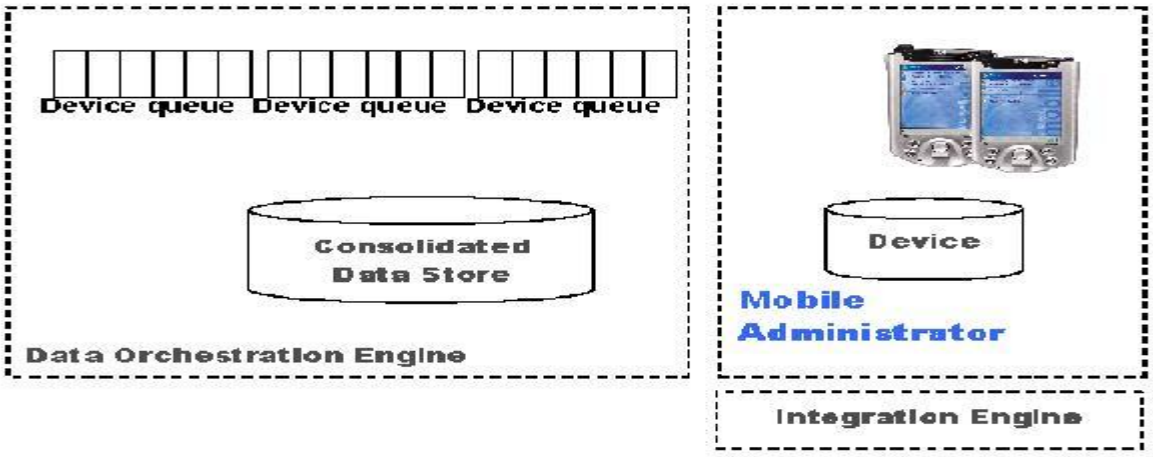
Created on: 10 December 2009

Author Bio

Rahul Saxena has been working on the SAP NetWeaver Mobile 7.1 product for past 3 years.

Table of Contents

Need for Mobile Administrator



- A typical system landscape consists of DQP (Development / Quality/ Production systems) model. The Admin and monitoring infrastructure is available in DOE (Data Orchestration Engine). Ideally a Mobile Administrator wants to keep track of daily activities that are happening in the system; normally Production systems are the ones Mobile Administrator will be more concerned about. The NWMA (NetWeaver Mobile Administration and monitoring portal) provides with him with the tools with which he can achieve the same.
- The tools can provide him the status of the System based on the configurations that have been set, he can monitor the sessions of individual devices, and he can view the message details. Apart from all these there is a separate Device administration section which will be discussed later.
- Using these tools Mobile Administrator can monitor the entire flow of data from backend to DOE and DOE to client and back. There are also tools to provide statistics which can be used to establish a trend of the general system behaviour for the business scenario in which DOE issued. Also, it could help out in determining if there is some deviation from the expected or the standard behaviour.

The NWMA will be of high value to the customer since it catches all relevant status information from any part of the system and all errors occurring anywhere and reports them to a central monitoring UI. Thus, for the Mobile administrator the NWMA ensures one central place of entry from where the whole system can be monitored,

Objective of Mobile Administrator

The primary objective of a Mobile administrator is to ensure smooth functionality of a complex system such as the NetWeaver Mobile by monitoring its status, by using the NWMA.

- A Mobile administrator has to be in a position to quickly recognize whether the system is working fine or not. In case of errors he has to be able to localize the place where the errors occurred and the NWMA shall provide him with the guidance on how to resolve these issues.
- The main focus of a Mobile administrator should be that he should make the end user experience as smooth as possible, because for an end user the Mobile Administrator is the single point of contact.
- In case of some issue, the Mobile Administrator should be able to use the tools and ascertain whether the issue is a user handling issue, a problem with the modeling, or it is a bug. In either case he should be able to find the cause of it and rectify the problem on his own using the tools that are available to him or he should be able to delegate the problem to his development team or report the issue to SAP support team.

Job of Mobile Administrator

An Administrator should be able to:

- Perform Daily monitoring - Central access to all monitoring functionality (System status or System Health)
- Alert-driven error handling - Receives active support through system via logs/traces collected by agents on the device.
- Able to report an error to SAP support and supplies all relevant information.
- Perform House-keeping - Mobile specific data archiving which is independent from the Backend application to reduce data volume on the device (e.g. sales orders) and Data base house-keeping on the device (e.g. index reorganization) and on the server.
- Able to triggers reports on average sync time/volume, number of users with defined etc.
- Receives patch or upgrade from SAP and applies it to all affected landscape components. After successful test, incremental roll-out to all affected users.
- Able to handle Model Changes and assignment of data to devices changes.

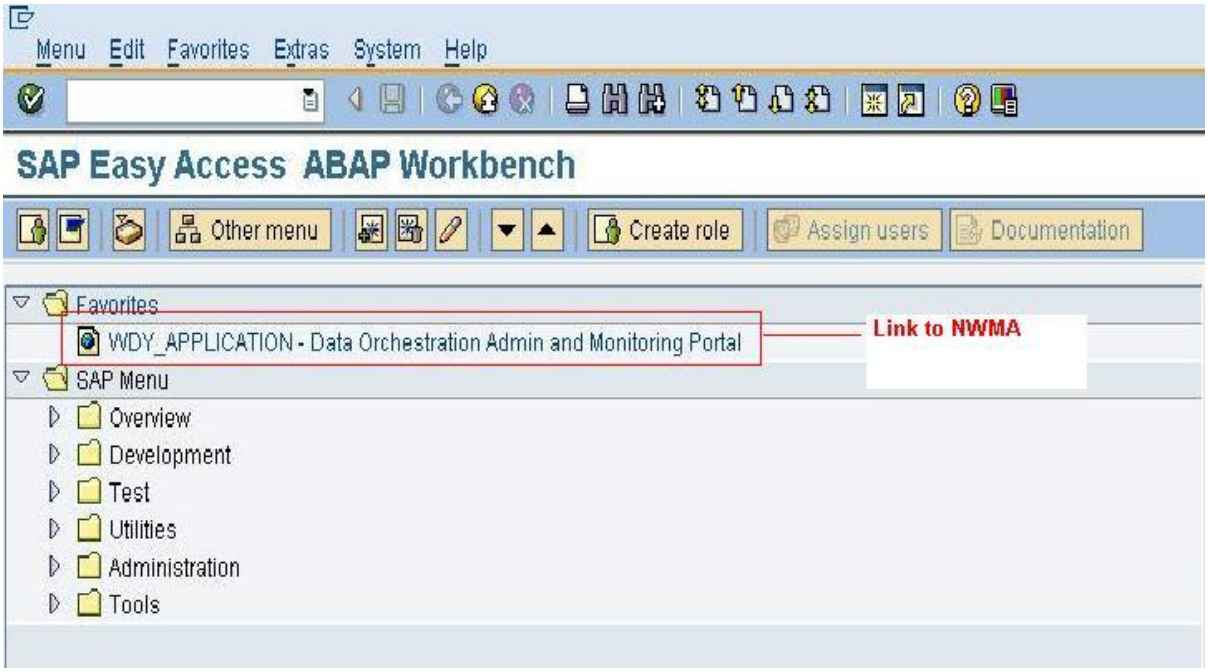
Who can be Mobile Administrator

This is a very often asked question when a DOE system is being set up. However, the answer to this question is fairly straight forward. The skill set of a person assigned SAP NetWeaver Mobile administrator job should look like this:

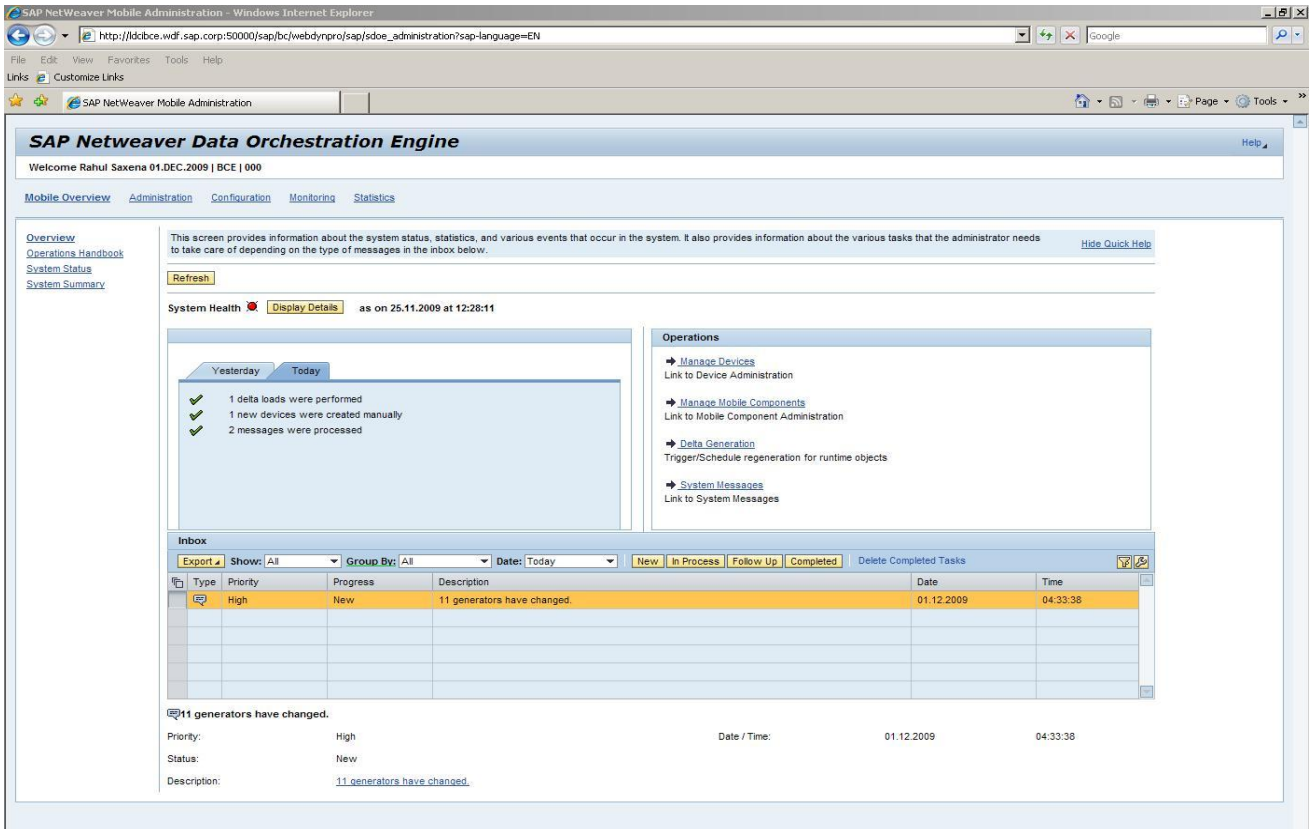
- Business Use Case knowledge
- Basic knowledge of DOE
- Knowledge of SAP System

NetWeaver Mobile Administration and Monitoring tool (NWMA)

The link to NWMA can be found under user menu on logging into the DOE server.



On clicking the link NWMA tool should open in the web browser.



Some of the important links are discussed below.

Administration

It groups together and provides the starting point for performing various administrative related tasks. This view would precisely provide links to navigate to:

Device Management

- Device Administration
- Device Profile Administration
- Channel Administration

Device Administration

The purpose of this View is to provide user interface for performing basic Device related tasks.

- Administrator can do search, advance search for devices.
- Administrator can display details of one device at a time – such as all the single and multi-valued attributes, the mobile component details, the DM SWCV's associated to the device etc. He can modify these values also
- Administrator can change the attribute values for a device.
- Administrator can see monitoring information for a device. Example: pending extracts; DO's pending in the outbound queue; DO's waiting for data completeness etc.
- Administrator can perform various operations for one or a set of devices. Example: device reassignment, trigger extract, backup and recovery etc. Out of these Creating setup packages, Device Reassignment, Assigning DMSWCV and Reprocessing of Queue blocker messages can be done for multiple devices at once.

Some of the examples where Device Administration can be useful:

- If the device is registered and the end user is not able to see the data, (which was present in the outbound queue) in that case the Administrator can go and see whether the user for that device is maintained in the user tab for that device.
- In case the user is not getting the desired data and while rule modeling receiver attributes are mapped, the Administrator can cross check the Receiver attributes based on whether they are single valued or multi valued from device administration.
- When the subscription is not getting calculated, the Administrator should go and check in Rule Administration whether the rules for the DMSWCV are active or not. If they are not active he should make it active.
- After first sync when the device becomes registered, if the DMSWCV doesn't become operational then the Administrator should check the queue for the device, if there are entries in the queue then the Administrator should check the status once the queue is entirely processed.

Device Profile Administration

From this view the administrator can map one or more Mobile Components to a Device Profile. Also one or more users can be mapped to a Device Profile. The mass maintenance is possible in either ways

- Assigning one or more Device Profiles to one device at a time – this can be done from the device administration view where there is a detail tab for displaying list of Device Profiles assigned to a device.
- Assigning one Device Profile to one or more devices at a time – this can be done from the Device Profiles view.

Channel Administration

The concept of multi channel access allows DOE to send and receive data to any types of receivers who are interested in data exchange with it.

The term receivers, includes:

- Any kind of physical devices like Laptops, PDA's, and Mobile Phones etc.
- Any application running on the devices specified above. E.g. RSS feed readers, portals, Email clients etc.

Additionally, these receivers are not bound by any underlying technology to run on or any specific communication protocol. The message formats to be exchanged by them with DOE are decided by them and the mode of communication, quality of service etc is also determined by them. Thus enabling of the multi channel access brings true openness to DOE.

A channel can be of three types:

1. Outbound Channel: The outbound channels can be used to send out the data distributed to a receiver by DOE.

   Filtering of the messages is possible for a channel based upon the following characteristics:

   - Data Object: It is possible for a channel to define a list of data objects whose messages it does not want to receive (i.e. filter out)
   - Message Type: In a channel defining a filter based on message type to view messages is possible.
   - Task of Message: Filtering of messages is also possible based upon the message task at root node level.

   If more than one filter is provided than priority to the filter is in the following order:

   - Data Object
   - Message Type
   - Message Task

2. Inbound Channel:

   Presently there is only one implementation published, which is owned by DOE and will invoke the standard flows of DOE for inbound messages. The default implementation at the inbound side offers a set of quality of services as mentioned below:

   - In order delivery and guaranteed delivery with asynchronous processing.
   - Guaranteed delivery with asynchronous processing.
   - None with synchronous processing.

   The channel definition will specify which option it wants and default will be "In order delivery and guaranteed delivery with asynchronous processing".

3. Both

   This channel has capabilities of both Inbound and outbound channels.

All the channels can be activated and deactivated. This includes the default channel also. Apart from this attributes of each channel, devices and its filters can also be managed and changed if needed.

Monitoring

It groups together and provides the starting point for viewing various kinds of Monitoring Data. Under the Mobile Monitoring Section, there are links to different types of Monitoring Data that an administrator can view:

- Client Communication Session Monitoring
- Device Logs Monitoring
- Message Monitoring
- Logs and Traces
- Queue Tracking
- Delta Generation Monitoring

Client Communication Session Monitoring

Under this type of Monitoring, Administrator can monitor the Communication Sessions between the Mobile Clients and the Server. Typically the information available will be

- Session Start Date at Server
- Session Start and End Time at Server
- Errors that occurred during a Session

The session status conveys the following information:

1. Green: Session ended successfully
2. Yellow: Session is still active – if this is for a long time then it means that the session has ended without client sending a logout message to the server, or there was a time-out on the client else network connection had a problem.
3. Red: Session ended due to error. Error messages can be viewed by clicking on the link in the session information tab. This would take you to message monitoring for details of the message.

For more info on this topic refer to the Reference 2 in the RELATED TOPICS section in this document.

Device Logs Monitoring

Under this type of Monitoring, Administrator can view the traces and logs that were generated on the Mobile Clients (the physical mobile devices) and were sent to the DOE on periodic basis. So, in this view, Administrator can search for the devices for which he/she wants to view the logs and traces. There is an additional log filter to refine the search for logs once the device is selected.

Message Monitoring

Administrator can search for DO Messages based on various criteria. For example: based on DO type, sender device, the send date of the message, receiver device, status of messages etc.

On search of Messages, following information for each message is available to the administrator:

- Message header information - Message ID, DO Name, Message type (bulk or transaction message), Status (Success, Ended with Errors, Validation Error etc.), Sender User, Sender Date, Flow Blue Print (Flow Context currently being processed for the message) etc.
- On selecting a particular message, its detail information is displayed to the user: The Receivers of the message and the Errors (if any) logged by various executed services for this message.
- Also on selecting a message, the administrator can view the complete DO data (message body) in case of transaction message. This information displays the content of each DO Node filled in that DO instance.
- For messages with erroneous state, it will be possible for administrator to re-process the messages. This however, will depend on configurations whether Re-processing of messages with a particular erroneous state is checked or not.
- Also, it will be possible for the administrator to select one or more messages and remove/delete them.

  For more info on this topic refer to the Reference 1 in the RELATED TOPICS section in this document.

Logs and Traces

Logging and Tracing functionality is provided so as to capture information of all the processes that are executed in the DOE. This view provides a generic interface to the user where user can search for any kinds of logs and traces that were logged on by various services at runtime or various operations at runtime.

- Logs and traces collect in-detail information about the services executed in format of a step-by-step execution protocol. Traces will be provided for all services in the DOE.
- The user can search for logs and traces based on Based on Environments

  For example: during device reassignment, the various steps that were logged could have their own set of logs and traces. These logs and Traces could be searched based on Environment “Device Reassignment”. Similarly, if one wants to search logs and traces for a message flow that went through execution of many services, the logs and traces could be searched based on Environment “Flow”.

  Additional examples of environments are “Client Communication”, “Client external logs and traces”, “Extract”, “Rule Evaluation”, “Backend Integration” etc.

- User gets the generic search criteria fields such as status of logs, user, start date, end date, process id’s etc.
- In addition, based on the environment selected, a custom search criteria field set is also provided to the user which is dynamically rendered for an environment. For every environment, the set of fields are customized in a table based on which the search is done.

Queue tracking

Under this type of Monitoring, Administrator will be able to view information related to Inbound and Outbound Queues of a Device on the DOE. Administrator can search for the devices for which he/she wants to view queue information. Once the device search list is obtained, Administrator can select one device at a time and choose to see either the Inbound Queue details or the Outbound Queue Details.

The information available on the Inbound Queue Details is:

- Number of messages that still are not processed OR messages that result into an error state. For example: validation failed for the DO message. These are the messages that have been sent from the Mobile Client Device.
- For each message, information such as the sender of the message, the date it was sent etc. will be displayed.

The information available on the Outbound Queue Details is:

- Number of messages available on the Queue. These are the messages that have to be sent to the Mobile Client Device.
- For each message information such as the status of the message (whether it has been yet read by the Mobile Client or not), the date it was posted onto the queue, user (somebody who would have triggered the extract for this device) will be displayed.

For more info on this topic refer to the Reference 4 in the RELATED TOPICS section in this document.

Configuration

It groups together and provides the starting point for performing all kinds of configurations required in the DOE for proper flow of data between backend – middleware, middleware-mobile clients and vice-versa. Configuration View is divided into 4 different groups:

- DOE Configuration
- Backend Configuration
- Statistics Configuration
- System Status Configuration

DOE and Backend Configuration views, display the details of the already existing parameters and their values. These values can be configured and new values can be added to these. The values and input helps that these parameters take are dynamic and changed based on the type of parameter.

DOE Configuration

- The DOE configuration parameters are separated by performance relevant or not. The options like CDS_READ_PACK_SIZE_FOR_EXT, CLIENT_PACKAGE_SIZE etc next to which the performance relevant checkbox was checked means that these are the parameters which can affect the system performance. Depending upon the system and scenario the administrator can set the parameters to optimize his system performance.
- Some of the parameters like QUEUE_SIZE have a default value assigned to them. The administrator can change this default value according to his system capacity and the scenario being run on it.

Backend Configuration

- Just like the DOE configuration parameters the Backend configuration parameters are performance relevant or not. E.g.: BACKEND_MAX_QUEUES, BACKEND_PACKAGE_SIZE are performance relevant and the values like BACKEND_BGRFC_Q_DESTINATION, AUTH_DWLD_BE_DEST are not.
- One of the commonly used backend configuration parameter is BACKEND_DESTINATION. Administrator can set the Backend destination for the entire SWCV by leaving the Data Object and the adapter name as blank. Else he can set the backend destination at the Data Object or the adapter level itself. NONE specifies that the local system's RFC destination.

Statistics Configuration

- Administrator can choose the statistics he wants to see by checking the check box against to Message statistics, Queue statistics, or Sync statistics. If the checkbox is cleared the statistics will not be calculated for that parameter.
- Configure statistics parameters allow the administrator to determine the duration for which the statistics are available and also the unit in which they are calculated. By default they are calculated in milliseconds.
- Configure Maximum Level Values to Stop Extract for Receivers helps the administrator set the value for which the extract will be stopped for a device. This can be done by setting two parameters.

  1. Maximum threshold for Queue size

     The value should be set for this parameter depending upon what is considered as value which is a very high and can potentially affect the system performance or which is not expected in a normal use case.

  2. Maximum threshold for days not synced

     The extract will be stopped for the devices which have not synced for that many days. For e.g. if the end user is not syncing for say x days then administrator can avoid the outbound queue for the device being filled as the device has not consumed the data which is already present.

System Status Configuration

This is one of the most commonly used tools that are used by the administrator. This tool helps the administrator to configure the system status parameters for:

- Receiving alerts in his inbox
- Receive sms or email if configured to CCMS
- Set threshold values for warning or alert message

The threshold value against the yellow means a warning will be shown to the administrator in admin inbox and the system status will be yellow. The threshold value against red should indicate that if the value of the parameter exceeds this value then the system would be in error state.

Let us consider the following examples:

1. If the administrator wants to be informed about the failure of a backend destination, he needs to set the Number of failed destination as Active (checkbox). If we want to be alerted he ticks the checkbox against Alert and gives a threshold value for yellow and red. Then he needs to add the RFC destination which will be monitored.
2. If the administrator is concerned about the outbound queue sizes of the devices he can set the Device Outbound Queue Size Threshold to active and mention the threshold for which he wants to be informed about. This threshold values corresponds to the number of devices that will exceed the threshold set for Statistics Configuration -> Maximum threshold for Queue size

Statistics

Mobile statistics can be used by the administrator to see the Message and Synchronization data of the system in a report format. This data can also be used by the administrator in case there is deviation in the system from the expected behaviour.

- Message Statistics
- Sync Statistics

Message Statistics

Message statistics give the data regarding the messages that are processed in the DOE. Administrator can get the information regarding the Date, time, and the classification of the messages according to inserts, update, deletes, initial uploads and delta downloads. The administrator can get the report by choosing the aggregation type as daily, weekly or monthly.

Synchronization Statistics

Synchronization details can be viewed as a report from Synchronization statistics. The report can be aggregated based on daily, weekly and monthly duration. These statistics are consolidation of statistics of data got from Client session monitoring.

System Status

If the system status configuration parameters that are active exceed the threshold value system status would become Red and a view details button would appear adjacent to it. On clicking it details will be shown to the user for the same. These parameters if set would be used by the background job which is scheduled for system status calculation and the results of it can be seen in Admin inbox. If the Administrator wants to see the current system status; in that case he can go to the Mobile overview page and click on the System Status button. On the system status view he can click on the calculate system status button to run the background job immediately. Once the job finishes Administrator needs to refresh the page by clicking on the refresh button.

For more info on this topic refer to the Reference 3 in the RELATED TOPICS section in this document.

Mobile Inbox

The Mobile Operations Inbox should be provided as a View under the Mobile Monitoring. The Mobile Operations Inbox provides the administrator the ability to track the various operations that he performed and what was their status.

- Administrator can search for the operations performed by him based on the time period, status, or the type of the group like alerts, notification or information.
- Based on the search criteria the list of Operations is displayed to the administrator with information such as Operation Name, Triggered date/time, Status.

The administrator can typically change the status of the operations by selecting the row of the operation and pressing one of the status button given in the toolbar like New, In Process, Follow up or Completed. The completed tasks can be directly deleted by pressing Delete Completed Tasks button.

Some of the typical scenarios where the Inbox is used are:

- To receive notifications about the devices created through receiver generation Data Object. The administrator can actually go and view the devices created by clicking on the link that is displayed in the table.
- To receive alerts regarding Backend not being configured for Backend adapters.

Related Content

Reference 1 - How to monitor messages in sap netweaver mobile 7.1

Reference 2 - How to monitor communication sessions in sap netweaver mobile 7.1

Reference 3 - How to check sap netweaver mobile 7.1 system status and system summary

Reference 4 - How to track queues in sap netweaver mobile 7.1

For more information, visit the Mobile homepage.

Copyright