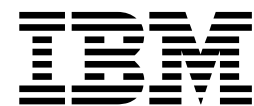




CNA 9.3. Administrator Guide



CNA 9.3. Administrator Guide

Note

Before using this information and the product it supports, read the information in "Notices" on page 19.

Edition Notice

This edition applies to Version 9 Release 3 of Customer & Network Analytics (product number 5725-R30 & 5725-Q80) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview 1

Intended Audience	1
Glossary	1
Hotkey Features	1

Chapter 2. Introduction 3

Scope	3
Version	3
Disclaimer	3
Prerequisites	3

Chapter 3. User Management and Security Options 5

General User Groups and Role model	5
Functional Roles	6
Data Roles	6
User Account Management	7
User Account GUI	7
User Time Zones	8
Users Import - Import Accounts...	8
User Groups Management	9
System Defined Groups	10
Security Options	10
User Account Security Options	10

HTTPS Requirements	11
SMTP Requirements	12
Password recovery	12

Chapter 4. Traceability for Audit 13

Chapter 5. Customer & Network Analytics Alarms Integration 15

System alarms	15
User-defined Alarms	15
SNMP requirements	15

Chapter 6. Troubleshooting 17

Unprovisioned Cells and Device	17
Recovery scenarios	17
Items to Check before Contacting Administrator	17

Notices 19

Accessibility Statement 23

About this document 25

Chapter 1. Overview

Intended Audience

Customer & Network Analytics Administrator Users.

Future Customer & Network Analytics users preparing pre-requisites.

Glossary

Table 1. Glossary of terms.

Acronyms and abbreviations that are used in this document are as described.

Acronym	Description
GUI	Graphical User Interface
CEM	Customer Experience Management
GPRS	General Packet Radio Service
UMTS	Universal Mobile Telecommunications System
Gn	GPRS Node. IP Based interface between SGSN and other SGSNs and (internal) GGSNs.
ISP	Internet Service Provider
LTE S1U - S11	Long-Term Evolution - IP-based Interfaces between MME, SGW, and PGW.
S10	IP-based interfaces between MME.

Hotkey Features

Table 2. Summary Hotkeys

Navigation	Hotkey
Module > HOME	Ctrl + 1
Module > DSM	Ctrl + 2
Module > AM	Ctrl + 3
Module > NA	Ctrl + 4

Table 3. Managing Workspaces Hotkeys

Navigation	Hotkey
Workspace > New workspace	Ctrl + T
Workspace > Close current workspace	Ctrl + W
Workspace > Cycle through opened workspaces	Ctrl + PageUp
Workspace > Cycle through opened workspaces	Ctrl + PageDown
Workspace > lock/unlock	Ctrl + L
Workspace > Rename	Ctrl + R

Table 3. Managing Workspaces Hotkeys (continued)

Navigation	Hotkey
Workspace > Open workspace settings context menu	Ctrl + Alt + W
Workspace > Refresh	Ctrl + Alt + F5
Workspace > Open workspace	Ctrl + O
Workspace > Save as	Shift + Ctrl + S

Table 4. Managing Reports Hotkeys

Navigation	Hotkeys
Report > New report	Ctrl + N
Report > Cycle through reports	Ctrl + TAB
Report > Open report settings context menu	Alt + R
Report > Remove	Del

Table 5. Managing Alarms Hotkeys

Navigation	Hotkeys
AM > View Profile	Ctrl + Alt + V: Navigate the list of data records using Arrow Keys
AM > Open Profiles Dialog ("Manage profiles...")	Ctrl + M
AM > Details	Ctrl + D

Table 6. Network Analyzer Hotkeys

Navigation	Hotkeys
NA > View Data Record	Ctrl + D Navigate the list of data records via Arrow Key.
NA > Copy Record to Clipboard	Ctrl + C Navigate the list of data records via Arrow Key.
NA > CFA Search results > "i" parameters icon	Ctrl + I
NA > CFA Search results > Back to Parameters button	Ctrl + backspace
NA > CFA> scroll Up/Down	PageUp & PageDown

Table 7. Managing Settings Hotkeys

Navigation	Hotkeys
App settings > Change Account Settings	Ctrl + Shift + A
App settings > Account Management	Ctrl + Shift + M
App settings > Groups Management	Ctrl + Shift + G
App settings > Login and Logout Policies	Ctrl + Shift + P
App settings > Security Widget	Ctrl + Shift + E

Chapter 2. Introduction

This document is intended to provide a guide to administrator-users of the *Customer & Network Analytics (CNA)* applications. The guide provides a reference to the correct use of the application's Graphic User Interface (GUI) administrator functions and system options.

Note: this document does **not** cover the detailed underlying processes that are involved, or the hardware upon which the application runs.

Scope

The scope of this document is IBM Now Factory's Customer & Network Analytics product. It is focused on the application layer and is not intended as a description of the data collection and mediation layers.

The main areas that are covered by this Administrator's Guide are:

- User Management and Security options
- Traceability options
- Alarms Integration
- Troubleshooting

For information on Reference Data Provisioning that is required for the Customer & Network Analytics solution, refer the Analytics Accelerator Framework (AAF) Provisioning Guide.

Version

This guide applies to Customer & Network Analytics 9.3.

Disclaimer

No part of this publication can be reproduced, stored in a retrieval system, or transmitted in any form or by any means, including photocopying, electronic, mechanical, recording, or otherwise, without the prior written permission of the copyright holder.

This document contains proprietary information of IBM Now Factory. The contents are confidential and any disclosure to persons other than the officers, employees, agents, or subcontractors of the owner or licensee of this document, without the prior written consent of IBM Now Factory is strictly prohibited.

Prerequisites

The Customer & Network Analytics (CNA) application suite is certified to run on Chrome 55 or later with Macromedia Flash plugin 24.0 or later.

Chapter 3. User Management and Security Options

Access to the Customer & Network Analytics GUI is secured by authenticated users and associated roles. The roles available to any user can be defined in a flexible way through the mappings from the user's groups in order to give enough granular flexibility to the network operator. A key requirement is the protection of individual subscribers' data.

Multiple options are available to enforce different levels of security as befits the operator's standard and regulation.

This section details the administrative user options management GUI and security options available to the Customer & Network Analytics Administrator.

General User Groups and Role model



Figure 1. A set of Predefined Customer & Network Analytics Functional Roles are provided:

- Alarm Normal Role
- User Management and Security Administrator Role
- Standard Data Service Manager Role
- Power Data Service Manager Role
- Customer Manager Role
- Power Network Analyzer Role

These roles define the set of functional features, which an individual user can access.

Data Access Roles define the access to Customer-level data:

- A data role for Individual Customer Data is required to send any request on an individual Customer (MSISDN / IMSI / CSID) and to view any affected Customer ID (MSISDN / IMSI / CSID) in the affected Customers List.
- A data role for Customer Group Data is required to send any request on any Customer Group (Customer Segment Group / Customer Corporate Group).

Customer & Network Analytics Users are assigned to groups, and each group has a set of roles. Customer & Network Analytics ships with a set of Default Groups. New groups can be created and edited at any time by any Customer & Network Analytics user with User Management and Security Administrator Role.

A dedicated special security functional role Customer Manager Role is available, which enables access to un-anonymised customer identifiers and typing in MSISDN in the **Customer Manager** for individual customer reports.

Functional Roles

Each pre-defined Functional Role specifies exact access to individual functions (actions). The available functional roles are as follows:

- **USER_ADMIN_ROLE:** Full access to all User Management and Groups Security Configuration for the Mobile Moments Framework.
- **DSM_NORMAL_ROLE:** Standard access to Data Service Manager. This role allows functional access to all the actions required to create reports: opening the Dimension Panel, selecting and searching the Selection panel, options to drill-down, opening and saving own Workspaces and Dashboard, as well as viewing affected anonymized customer list.
- **DSM_POWER_ROLE:** Advanced access to Data Service Manager. This role allows functional access to all the previous actions plus creating and editing functions, including: creating a user-defined application for reporting, creating, and editing Customer Segment Groups.
- **SI_NORMAL_ROLE:** Standard access to Network call Flow Analyzer - Call Flows and Sessions (Historical Search) features and all associated menu options.
- **SI_POWER_ROLE:** Full access to Network Analyzer - Call Flows and Sessions features (Historical Search and Live Trace) and all associated menu options.
- **ALARM_NORMAL_ROLE:** Standard access to Alarms Manager: alarms that are generated by metrics thresholds: view open alarms and change alarms state (close, reopen, acknowledge).
- **ALARM_POWER_ROLE:** Full Access to Alarms Manager. This role allows the functional access to all the previous actions plus creating and editing alarm definitions.
- **CM_SUPER_ROLE :** Full Access to Customer Manager. This role allows typing in an MSISDN and viewing all related information to this MSISDN. Customer Data Role is also required. Cloning reports to the Data Service Manager workspace is only enabled if the user also has **DSM_NORMAL_ROLE** or **DSM_POWER_ROLE**.
- **CM_LIMITED_ROLE:** Standard Access to the Customer Manager. This role allows typing in an MSISDN and viewing all related information to this MSISDN. The user will not be able to use the Analyze option on charts, drill down to customer lists, or remove the subscriber filters.
- **CALLFLOWS_POWER_ROLE:** Full access to Network Call Flow Analyzer.
- **CALLFLOWS_NORMAL_ROLE:** Standard access to Network Call Flow Analyzer.
- **SESSIONS_POWER_ROLE:** Full access to Network Session Analyzer.
- **SESSIONS_NORMAL_ROLE:** Standard access to Network Session Analyzer.

Note: Functional Roles: **SI_NORMAL_ROLE**, **SI_POWER_ROLE**, **CALLFLOWS_POWER_ROLE**, **CALLFLOWS_NORMAL_ROLE**, **SESSIONS_POWER_ROLE** and **SESSIONS_NORMAL_ROLE** are deprecated in release CNA 9.3.

Data Roles

Each pre-defined Data Role specifies exact access to specific types of data. The available data roles are as follows:

- **CUSTOMER_SENSITIVE_ROLE:** this data role is required for users to view any individual customer's sensitive data: customers' identifiers (MSISDN / IMSI /CSID) in affected customers list and type in the ID to launch searches in the **Customer Manager** and view reports in the **Data Service manager** on individual customers.

- **CUSTOMER_DIMENSION_GROUP_ROLE:** this data role is required for users to view any customers group's sensitive data: view reports in the Data Service manager on any customers group.
- **GN_INTERFACE_ROLE:** this data role is required for viewing any report on the GPRS-UMTS dataset.
- **LTE_S1U_S11_INTERFACE_ROLE:** this data role is required for viewing any report on the 4G LTE dataset.
- ***INTERFACENAME*_INTERFACE_ROLE:** For every interface in the system, there is a specific role to determine access to any report on that interfaces dataset.

User Account Management

Users with the Administrator role might view the currently configured list of users, create and de-activate user accounts, manually unlock users account as well as create and edit groups and their assigned roles.

The current user is flagged with a green **Online** icon.

User Account GUI

The GUI to manage Customer & Network Analytics users can be accessed via the *Settings* icon - **Account Management**.

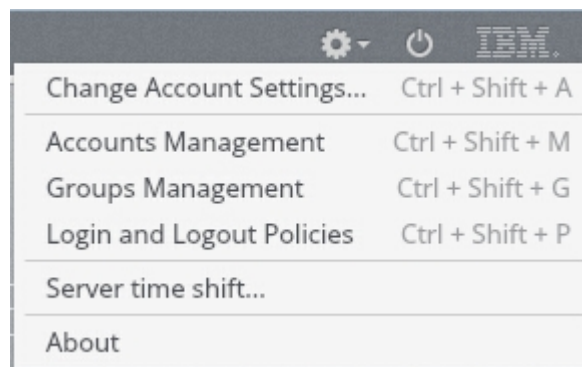


Figure 2. Settings Menu

Online	Account name▲	First name	Last name	Mobile number	Email address	Groups	Lock	Status	Last login time	IP address
	audituser							Active		
	superuser					Admin, CM Standard User		Active	24.08.12 09:46	127.0.0.1

Figure 3. User Management Main Screen

Users' details can be edited by double-clicking any user's line or the right-click contextual menu.

A new user can be created by clicking the **New Account...** Link. The creation of a user requires the following input fields.

- **Username**
- **Password**
- **Groups**

At least one group must be associated to any user.

- **First Name**
- **Last Name**

- Email address

Live Status

Online	Account	First name	Last name	Mobile number	Email address	Groups	Lock Status	Last login	IP address
	Admin						Active		
	supervisor					Admin, CM Standard User	Active	24.08.12 09:46	172.0.0.1

Figure 4. Live User Status

In the **accounts management** screen, there are **Live Status details** on system users. The following information is available:

- **Online Indicator:** Yellow / Green signal to show a currently offline / online user.
- **Last Login Time:** The time at which the online user logged in.
- **IP Address:** The IP address of the user's computer.

User Time Zones

In CNA, the time shown in the GUI is the local time on the user's desktop.

Daily KPIs are calculated midnight to midnight based on the local time on the CEM Servers.

Users Import - Import Accounts...

A number of users can be imported as Batch from a CSV file. Start with clicking the **Import Accounts...** Link in the navigation bar of the **Account Management** section.

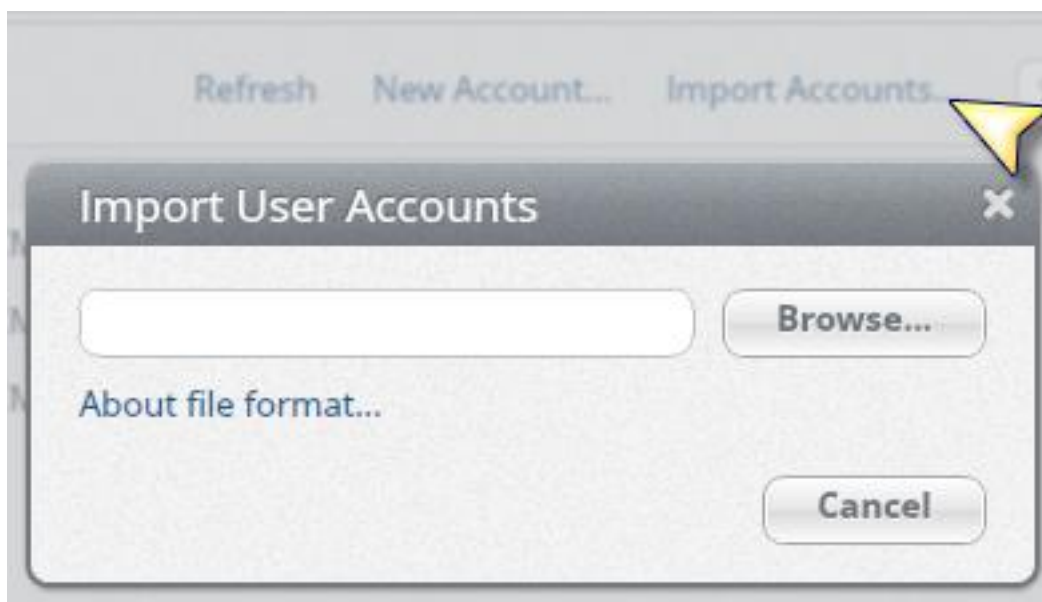



Figure 5. Batch Users Import dialogue

The file format is described in the **About File Format...** Link:

Each created user receives an email to log in the system and needs to set their password when they log in before the password expiry.

User Groups Management

The GUI to manage CNA user groups can be accessed via the *Settings* icon 

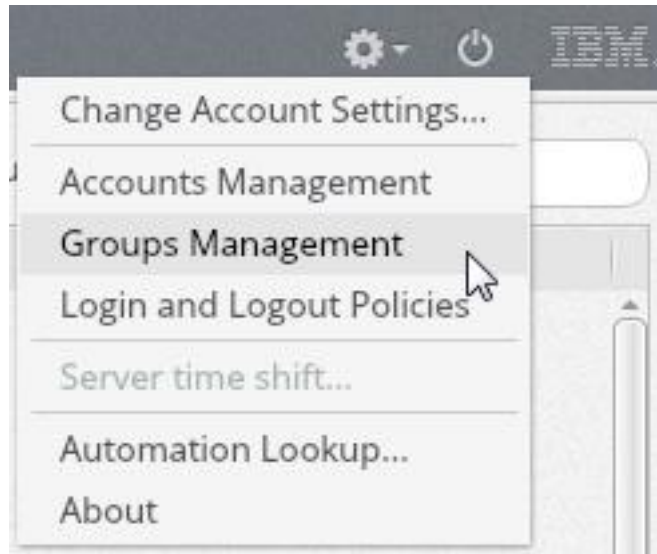


Figure 6. Groups Management

A new custom group can be created and edited in order to assign a number or roles (at least 1) to any group and thus control users' access to functional and data items.

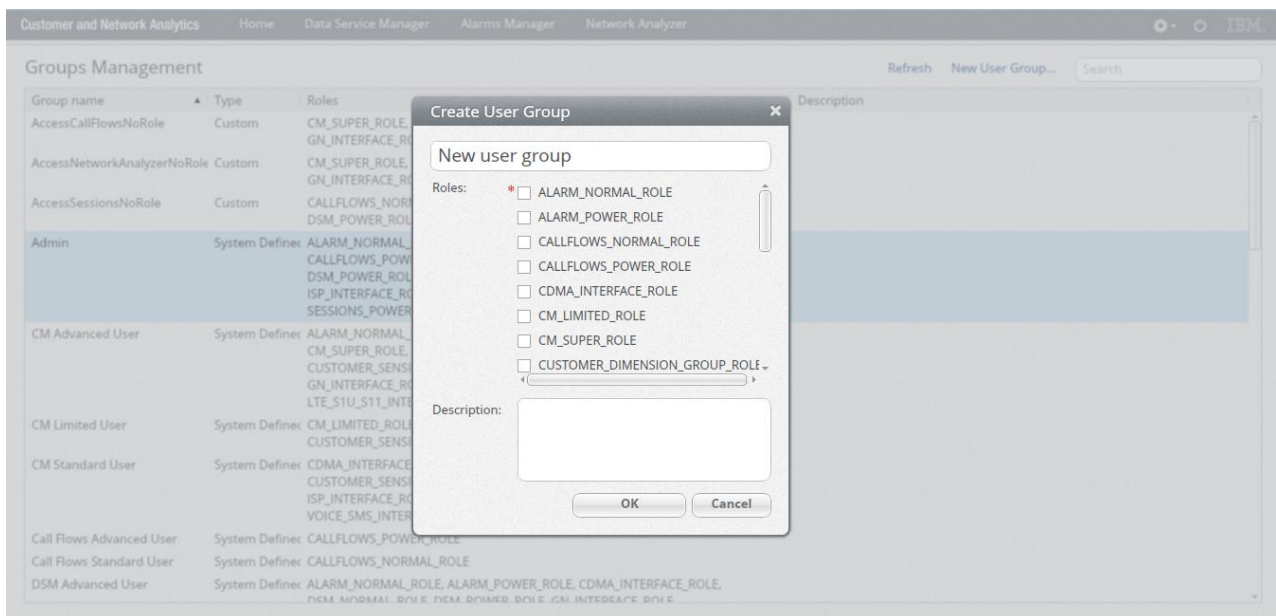


Figure 7. User Group Edit dialogue

System Defined Groups

The following system defined groups are available when Customer Network Analytics is installed. Refer to section “Functional Roles” on page 6 for a description of each functional role that is associated with a group.

Note: Functional Roles SI_NORMAL_ROLE and SI_POWER_ROLE are deprecated in release CNA 9.3.


Table 8. System defined groups

Group Name	Functional Roles
Admin	ALARM_NORMAL_ROLE, ALARM_POWER_ROLE, DSM_NORMAL_ROLE, DSM_POWER_ROLE, SI_NORMAL_ROLE, SI_POWER_ROLE, USER_ADMIN_ROLE
CM Advanced User	ALARM_NORMAL_ROLE, ALARM_POWER_ROLE, CM_SUPER_ROLE, CUSTOMER_DIMESION_GROUP_ROLE, CUSTOMER_SENSITIVE_ROLE, DSM_NORMAL_ROLE, DSM_POWER_ROLE, SI_NORMAL_ROLE, SI_POWER_ROLE
CM Limited User	CM_LIMITED_ROLE, CUSTOMER_DIMESION_GROUP_ROLE, CUSTOMER_SENSITIVE_ROLE
CM Standard User	CM_LIMITED_ROLE, CUSTOMER_DIMESION_GROUP_ROLE, CUSTOMER_SENSITIVE_ROLE
DSM Advanced User	ALARM_NORMAL_ROLE, ALARM_POWER_ROLE, DSM_NORMAL_ROLE, DSM_POWER_ROLE, SMART_VIEW_POWER_ROLE
DSM Standard User	ALARM_NORMAL_ROLE, DSM_NORMAL_ROLE, SMART_VIEW_POWER_ROLE
SI Advanced User	CUSTOMER_SENSITIVE_ROLE, SI_NORMAL_ROLE, SI_POWER_ROLE
SI Standard User	CUSTOMER_SENSITIVE_ROLE, SI_NORMAL_ROLE

Security Options

User Account Security Options

The Customer & Network Analytics Administrator can decide on a number of options to implement the required level of security for this deployment, the possible options and default values are described in the following:

The GUI to manage Customer & Network Analytics Login and Logout can be accessed via the *Settings* icon  - **Login and Logout Policies**.

This option is available to users with **USER_ADMIN_ROLE**. Clicking this option shows the following dialog window:

The user can change the policies using the following settings:

Password Strength

- Minimum password length - a minimum length of the expected password 0 means that a limit of 1 character will be applied. *Default: 8*
- Password contents:

- Uppercase letters: The minimum number of uppercase characters that are required. *Default 1.*
- Lowercase letters: The minimum number of lowercase characters that are required. *Default 1.*
- Digits: The minimum number of numeric digits that are required. *Default 1.*
- Special characters: The minimum number of special characters that are required. *Default 2.*
- Password does not contain password: restricts the use of the password string, user first, last name, or account name in the set password. *Default enabled.*

Password Aging:

- Enforce password history: how long is the password history (that is, when creating a new password, the application prevents the user from reusing old passwords, this setting outlines how far back to check) - 0 means that there is no history, and users are able to reuse passwords at will. *Default: 3.*
- Maximum password age: when a user changes his/her own password - how many days it should last before it expires. 0 means no expiry. Users receive a warning email a number of days before their passwords expire. *Default: 0.*
- Minimum password age: the minimum number of days after which a user can change their password again. *Default: 0.*
- Password expiry warning: indicates for how many days (once per day) the user should be warned of their pending password expiry. *Default: 3*
- *Password Reset after 1st Login*: Number of minutes after which an imported or unlocked user will have to change their password after their 1st login.

Login and Logout

- Maximum failed logins: 0 means that there is no lockout for too many failed logins. Once a user's account is locked, they are unlocked if an administrator sets a new password for them. *Default: 3*
- Account auto-logout period: The time in minutes to wait before logging a user out due to inactivity. *Default 15.*
- Account auto-lockout Period: The time in days to leave an account locked before unlocking an account, which has been auto-locked due to incorrect login attempts. *Default 30.*
- Allow simultaneous logins: allows multiple logins under the same username at the same time. *Default Enabled.*

Permitted IP Addresses: list of IP address from which connection is allowed. Empty for not enforce.

Note: Note, for dashboard with auto-refresh on, auto-logout will not be enforced as new requests are sent automatically.

HTTPS Requirements

The **Customer & Network Analytics** GUI application can be accessed securely via HTTPS if required. By default, the installation is done over HTTP.

In this case, the network operator provides a Private Key, Private Certificate, and Root Certificate:

- Certificates (server/client) MUST conform to the standard X.509v3
- Certificates MUST have a minimum key length of 2048 bits

- Certificates **MUST** lose their validity on expiry of a maximum period of 24 months

SMTP Requirements

The following configuration information and access must be provided by the network operator in order to enable all the password security requirements, which include sending emails:

- the host where the SMTP service can be found
- the username that is used to access the SMTP service
- the password that is used to access the SMTP service
- Optional: from email address - this value is placed in the "From:" header of system emails to allow people to respond to emails.

Password recovery

If any user has forgotten, he or she can request to reset his or her password. An email is sent to the user's email address with a new temporary password for the user to login (provided SMTP integration is complete).

Chapter 4. Traceability for Audit

Log information will be saved to the **Customer & Network Analytics** log files in the following format:

```
TimeStamp Logging Level | Start time | End time | IP-Address  
| Username | Application ID | Action | Viewed Object Name | Final Status | Custom data
```

For example:

Report request for MSISDN: 353855447442:

```
2012-03-30 09:41:48,087 INFO|2012-30-03 09:41:47,498  
|2012-30-03 09:41:48,018|172.1.2.3|superuser|3000|submitReportRequest  
|MSISDN|Complete  
|{start:Fri Jul 08 00:00:00 IST 2011,metrics:ACTIVITYTRACKER,  
selectedDimension:SUBSCRIBER:353855447442,  
granularity:_MIN_15,interface:GN,end:Sat Jul 09 00:00:00 IST 2011}
```

Report on Customers Group F:

```
2012-03-30 10:14:02,631 INFO|2012-30-03 10:13:59,765  
|2012-30-03 10:14:02,604|172.1.2.3|test4|3000|submitReportRequest  
|USERGROUP|Complete  
|{start:Sat Jul 09 12:50:48 IST 2011,metrics:BYTESDOWN,  
selectedDimension:SUBSCRIBER_GROUP:GOLDENCUSTOMERGROUP,  
granularity:_MIN_15, interface:GN,end:Sat Jul 09 15:50:48 IST 2011}
```

Customers List request on Customers Group M:

```
2012-03-30 10:15:32,580 INFO|2012-30-03 10:15:29,747  
|2012-30-03 10:15:32,551|172.1.2.3|test4|3000|submitReportRequest  
|USERGROUP|Complete|{start:Sat Jul 09 12:52:18 IST 2011,metrics:BYTESDOWN,  
selectedDimension:SUBSCRIBER_GROUP:M,granularity:_MIN_15,interface:GN,  
end:Sat Jul 09 15:52:18 IST 2011}
```

User password change:

```
2012-04-17 16:12:26,405 WARN|2012-17-04 16:12:26,331  
|2012-17-04 16:12:26,380|172.1.2.3|superuser|0|saveAccountSettings  
|account name|success|Password changed successfully
```

User account change:

```
2012-04-17 16:12:26,405 WARN|2012-17-04 16:12:26,331  
|2012-17-04 16:12:26,380|172.1.2.3|superuser|0|saveAccount|account name|success|
```

Password Reset:

```
2012-04-17 16:12:26,405 WARN|2012-17-04 16:12:26,331|2012-17-04 16:12:26,380  
|172.1.2.3|superuser|0|resetPassword|account name|success  
|Complete, please check your email box
```

User Group created or edited:

```
2012-02-27 12:15:34,049 INFO|2012-27-02 12:15:34,027  
|2012-27-02 12:15:34,027|172.1.2.3|superuser|0|saveGroup  
|New Custom Group's name|complete|
```

Login attempts:

```
2013-01-03 00:49:20,446 WARN|2013-03-01 00:49:20,386|2013-03-01 00:49:20,445  
|192.168.221.214|anonymous|0|login|superuser|failed|Wrong username and password
```

```
2013-01-03 00:49:24,044 WARN|2013-03-01 00:49:23,969|2013-03-01 00:49:24,043  
|192.168.221.214|superuser|0|login|superuser|success|
```

Chapter 5. Customer & Network Analytics Alarms Integration

System alarms

Customer & Network Analytics System Alarms can be set up and integrated via SNMP to any monitoring system in order to track possible system hardware, OS or network failures.

Note: Historical Alarms are disabled by default. If it is required to enable them, it can be done by an IBM Now Factory installation engineer.

User-defined Alarms

User-Defined Alarms can be set up by Customer & Network Analytics users as required to monitor the network operator's customers' quality of experience. See the Customer & Network Analytics User Guide [2] for details on how to set up alarm profiles in the Customer & Network Analytics GUI.

SNMP traps are sent when any alarm associated with an alarm profile configured for SNMP notification is opened or closed by the system. Traps are not sent when a Customer & Network Analytics user manually changes the state of an alarm.

Notifications are sent when alarms open and close automatically. Emails will not be sent when alarms are manually closed in the Customer & Network Analytics GUI. If a user has an SNMP integrated system, there is no synchronization between alarm profiles. If a user closes an alarm in the integrated system, it is not closed in Customer & Network Analytics, and vice versa.

SNMP requirements

The following configuration settings are required in order to enable SNMP integration for System Alarms and User-defined Alarms:

- SNMP Trap IP address
- SNMP Trap Port (default 1662)
- Heartbeat frequency: number of seconds between heartbeats.

Chapter 6. Troubleshooting

Unprovisioned Cells and Device

In the **Service Manger** and **Customer Manager**, if any device used on the operator's network is not provisioned yet, the associated traffic metrics are marked as Uncategorized and not available in breakdown by **Devices Groups**.

It is recommended to monitor the level of Uncategorized Device traffic (for example Bytes Total) and review the provisioning if the percentage gets significant.

If any own Network Operator's Cell is not provisioned yet, the associated User Plane Volume metrics (Bytes down, Bytes Up, Bytes total, Packets up...) are not available in breakdown by Cells or Cell Groups. The full volume is available in global report, without breakdown by Cells. It is possible to check the total volume (for example Bytes Total) for the full network (report 1) and broken down by Cell (report 2) and review the Cell provisioning if the difference is significant.

Recovery scenarios

In a temporary data link down between Mediation blades at the Customer & Network Analytics application location and the data collectors at the data sites or downtime on a Mediation box, the Customer & Network Analytics system is set up to recover when the link is back up again or the downtime is over. However, the system will only load historical data back to about 20 min old data, so that the system doesn't get overloaded.

Items to Check before Contacting Administrator

1. *Prerequisites are all filled in.*
2. Network availability.
Check other web sites are available.

Notices

This information was developed for products and services offered in the U.S.A.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy,

modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: <http://www.ibm.com/legal/copytrade.shtml>

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Accessibility Statement

IBM Now Factory is committed to making our technical communications broadly accessible, including to users with disabilities or impairments that occur with aging. For guidance, we look to the accessibility best practices and standards defined by Section 508 of the U.S. Rehabilitation Act and the Web Content Accessibility Guidelines (WCAG 2.0) of the World Wide Web Consortium Web Accessibility Initiative (W3C WAI).

Accessibility Processes

Our processes require new pages to meet a set of accessibility requirements which include:

- Providing aids to navigation for screen reader users such as:
 - WAI-ARIA landmarks for application, banner, navigation, search, complementary, contentinfo, document, form, and region sections of the page
 - an invisible link which allows the users to skip navigation links in order to get quickly to the main content of the page
 - proper markup for identifying the page title (i.e. an <h1> element)
- Providing WAI-ARIA attributes, roles, states, and properties
- Providing text equivalents for images
- Providing null text equivalents on decorative images
- Identifying row and column headers for data tables
- Programmatically associating labels with form fields
- Using valid XHTML 1.0 Transitional markup language
- Supporting browser settings for enlarging text and user style sheets
- Using consistent navigation mechanisms and style of presentation throughout the site
- Keyboard navigation of web pages
- Identifying the primary natural language of each page

We strive to make our Web sites accessible and continuously work on accessibility improvements.

About this document

The content of this document is confidential to IBM. Doc number: SC27457402



Printed in USA