DIMETRA™

TRACES Administrator Guide

APRIL 2022

MN004596A01-F

Intellectual Property and Regulatory Notices

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

License Rights

The purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

European Union (EU) and United Kingdom (UK) Waste of Electrical and Electronic Equipment (WEEE) Directive

The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheelie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheelie bin label means that customers and end-users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU and UK countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

CMM Labeling and Disclosure Table

The People's Republic of China requires that our products comply with China Management Methods (CMM) environmental regulations. (China Management Methods refers to the Regulation Management Methods for Controlling Pollution by Electronic Information Products.) Two items are used to demonstrate compliance; the Label and the Disclosure Table.

The label is placed in a customer visible position on the product. The first of the following examples means that the product contains no hazardous substances; the second means that the product contains hazardous substances, and has an Environmental Friendly Use Period (EFUP) of fifty years.

The Environmental Friendly Use Period (EFUP) is the period (in years) during which the Toxic and Hazardous Substances (T&HS) contained in the Electronic Information Product (EIP) will not leak or mutate causing environmental pollution, or bodily injury from the use of the EIP.

The Disclosure Table, printed in simplified Chinese, is included with each customer order. An example of a Disclosure Table (in Chinese) follows:

Disclosure table

部件名称	有毒有害物质或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件	×	○	×	×	○	○
电路模块	×	○	×	×	○	○
电缆及电缆组件	×	○	×	×	○	○
塑料和聚合物部件	○	○	○	○	○	×

本表格依据 SJ/T 11364 的规定编制。
O：表示该有毒有害物质在该部件所有均质材料中的含量均在 GB/T 26572 标准规定的限量要求以下。
X：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 GB/T 26572 标准规定的限量要求。

Service Information

EMEA Technical Support Operations (TSO)

The EMEA Technical Support Operations (TSO) provides a remote Technical Support Service to help customers resolve technical issues and quickly restore networks and systems. This team of highly skilled professionals is available to customers with current service agreements in place that include the Technical Support Service. The TSO technical experts may be accessed through the Service Desk either electronically or by using the listed telephone numbers. If you are unsure whether your current service agreement entitles you to benefit from this service, or if you would like more information about the Technical Support Service, contact your local customer support or account manager for further information.

Contact Details

Technical Requests: techsupport.emea@motorolasolutions.com

Repair Support: repair.emea@motorolasolutions.com

Contact Us: https://www.motorolasolutions.com/en_xu/support.html

Parts Identification and Ordering

If you need help in identifying non-referenced spare parts, direct a request to the Customer Care Organization of a local area Motorola Solutions representative. Orders for replacement parts, kits, and assemblies should be placed directly at the local distribution organization of Motorola Solutions or through the Extranet site Motorola Online at https://emeaonline.motorolasolutions.com.

Your Input

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Document History

Version	Description	Date
MN004596A01-A	Initial version of the *TRACES Administrator Guide*.	December 2017
MN004596A01-B	Updated/added the following sections: • Installing the TRACES Server on page 21 • Collecting Logs from the TRACES Application on page 42 • New procedure: Configuring External API Service on page 33. • New procedure: Using Externally Generated SSL Certificates with External API Services on page 34. • New procedure: Replacing SSL Certificates on page 34. • LDAP-related changes. • New procedure: Backing Up TRACESData Folder on page 40 • New procedure: Restoring TRACESData Folder on page 40 • Configuring Web Container on page 33 • Configuring External API Service on page 33	August 2019
MN004596A01-C	Updates: • Installing the TRACES Server on page 21 • Installing and Configuring Microsoft ADSI Edit (Optional) on page 22 • TRACES Web Mapping Client Requirements on page 20 • Installing the TRACES Server on page 21 • Installing and Configuring Microsoft ADSI Edit (Optional) on page 22 • Adding Web Client Users on page 32 • Configuring Web Container on page 33 New sections: • Map Server on page 44 • Installing the Map Server on page 45 • Data Export Formats on page 47 • Source of Data: DMR on page 47	April 2020

Version	Description	Date
	• DMR: CSV Format on page 47 • DMR: JSON Format on page 48 • Source of Data: Scout on page 49 • Scout: CSV Format on page 49 • Scout: JSON Format on page 50	
MN004596A01-D	TRACES 2.6 updates: • Configuring DMR Collector on page 28 • Obtaining the License File on page 24 • Licensed Features on page 53 • Configuring UMR Service Enabler on page 30 • Configuring UMR Collector on page 30 • Installing and Configuring Microsoft ADSI Edit (Optional) on page 22	November 2020
MN004596A01-E	TRACES 2.7 updates: • TRACES Certificate Management on page 36 • Importing the Customer Private Certificate into the TRACES Keystore on page 36 • Using Externally Generated SSL Certificates with External API Services on page 34 • Replacing SSL Certificates on page 34 • Importing Public Certificates into the TRACES Truststore on page 37 • Generating Self-Signed Certificates in the TRACES Keystore on page 38 • Map Server on page 44 • Installing Base Maps from .tpk File on page 46	June 2021
MN004596A01-F	TRACES 2.8 updates: • Installing a Base Map on page 44 • Uninstalling a Base Map on page 45	April 2022

Contents

List of Figures

List of Tables

List of Procedures

About TRACES Administrator Guide

What is Covered in this Manual?

This document includes the following sections:

- A brief overview of TRACES, which comprises a basic functionality overview, a summary of software applications, and hardware/platform requirements
- An installation and configuration guide for the software applications that are part of TRACES
- A backup and restore chapter for backing up and restoring the TRACES data and storage
- A troubleshooting section that provides solutions to common issues.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system.

For information, go to http://www.learning.motorolasolutions.com to view the current course offerings and technology paths.

Related Information

In addition to this manual, the following documents are available for the TRACES System:

- *TRACES User Guide*

Icon Conventions

The documentation set is designed to give the reader more visual clues. The following graphic icons are used throughout the documentation set.

DANGER: The signal word DANGER with the associated safety icon implies information that, if disregarded, will result in death or serious injury.

WARNING: The signal word WARNING with the associated safety icon implies information that, if disregarded, could result in death or serious injury, or serious product damage.

CAUTION: The signal word CAUTION with the associated safety icon implies information that, if disregarded, may result in minor or moderate injury, or serious product damage.

CAUTION: The signal word CAUTION may be used without the safety icon to state potential damage or injury that is not related to the product.

IMPORTANT: IMPORTANT statements contain information that is crucial to the discussion at hand, but is not CAUTION or WARNING. There is no warning level associated with the IMPORTANT statement.

NOTE: NOTICE contains information more important than the surrounding text, such as exceptions or preconditions. They also refer the reader elsewhere for additional information, remind the reader how to complete an action (when it is not part of the current procedure, for instance), or tell the reader where something is on the screen. There is no warning level associated with a notice.

Style Conventions

The following style conventions are used:

Convention	Description
Bold	This typeface is used for names of, for instance, windows, buttons, and labels when these names appear on the screen (example: the **Alarms Browser** window). When it is clear that we are referring to, for instance, a button, the name is used alone (example: Click **OK**).
`Monospacing font`	This typeface is used for words to be typed in exactly as they are shown in the text (example: In the **Username** field, type `Admin`).
	This typeface is used for messages, prompts, and other text displayed on the computer screen (example: `A new trap destination has been added`).
<Monospacing font in bold Italic>	This typeface is used with angle brackets as placeholders for a specific member of the group that the words represent (example: ***<router number>***). **NOTE:** In sequences to be typed in, the angle brackets are omitted to avoid confusion whether to include the angle brackets in the text to be typed.
CAPITAL LETTERS	This typeface is used for keyboard keys (example: Press Y, and then press ENTER).
Italic	This typeface is used for citations. A citation usually is the name of a document or a phrase from another document (example: *DIMETRA System Overview*).
→	An → (arrow pointing right) is used for indicating the menu or tab structure in instructions on how to select a certain menu item (example: **File→Save**) or a certain sub-tab.

Acronyms

The following acronyms are used in this manual:

BTS
Base Transceiver System

CPU
Central Processing Unit

DMR
Downlink Measurement Report

DSR
Dynamic System Resilience

iTM
Integrated Terminal Management

ISSI
Individual Short Subscriber Identity

LAC
Location Area Code

MS
Mobile Station

MSBR
Multi Site Base Radio

NM
Network Management

OS
Operating System

PC
Personal Computer

POS
Performance, Optimisation, and Security

RAM
Random Access Memory

RF
Radio Frequency

RSSI
Received Signal Strength Indication

SATA
Serial ATA

SC
Site Controller

SQL
Structured Query Language

TETRA
Terrestrial Trunked Radio

TRACES
Terrestrial RF Automated Coverage Evaluation Solution

UCS
User Configuration Server

UMR
Uplink Measurement Report

UNS
Unified Network Services

USB
Universal Serial Bus

VLAN
Virtual Local Area Network

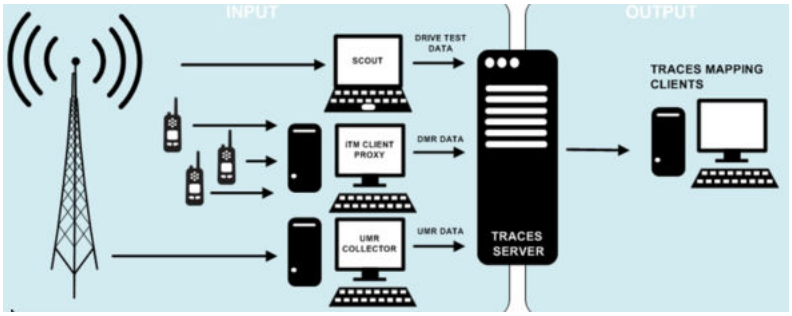
Chapter 1

TRACES Overview

The service comprises the TRACES mapping database server and at least one TRACES mapping client.

The TRACES server is a repository database for the captured TETRA RF survey data, network uplink data, and terminal downlink data. The Radio Frequency (RF) survey data exported from the Motorola Solutions Scout application is automatically uploaded to the server after a test drive or test walk. The network Uplink Measurement Reports (UMRs) are automatically uploaded to the database after being measured by the base stations and sent to the UMR collector. The terminal Downlink Measurement Reports (DMRs) are captured by the terminals whenever they experience a network service interruption, and are retrieved by Integrated Terminal Management (iTM) whenever the radio is docked. This data is automatically uploaded to the database. The RF coverage predictions can be imported into TRACES to facilitate comparisons between the predicted and actual coverage.

Figure 1: TRACES System Overview



1.1 TRACES Components

TRACES comprises a number of TRACES Server applications, as well as the TRACES Web Mapping Client.

TRACES includes the following components:

Database Uploader
Automatically uploads the Radio Frequency (RF) data to the database.

UMR Collector
Collects the Uplink Measurement Report (UMR) data from the Base Transceiver System (BTS).

UMR Service Enabler
Part of the UMR Collector, which enables the UMR collection in the BTS.

MS Log Converter
Exports the Downlink Measurement Reports (DMRs) from Integrated Terminal Management (iTM), preparing them to be uploaded to the database.

Log Exporter
Exports files from the Scout application, preparing them to be uploaded to the database. For more information on Scout, see the *TRACES User Guide*.

Web Container
Hosts the TRACES Web application.

1.2
TRACES Hardware and OS Requirements

For TRACES server and applications to operate properly, the hardware and operating system must meet a number of predefined requirements.

1.2.1
TRACES Server Requirements

The hardware requirements for the TRACES Server are estimated for the maximum number of Radio Frequency (RF) sites.

Table 1: TRACES Server Hardware Requirements

System Size	CPU	Memory	Hard Disk (one-year storage)
Small (up to 20 RF sites)	4 cores	8 GB RAM	50 GB SSD
Medium (up to 150 RF sites)	4 cores	16 GB RAM	350 GB SSD
Large (up to 1,000 RF sites)	8 cores	32 GB RAM	2.7 TB SSD

TRACES Server Software Requirements

The software requirements are as follows:

- The required Operating System (OS) for the TRACES software is Windows Server 2016 (recommended) or Windows Server 2012 R2.

  NOTE: It is recommended to use a standard OS image instead of a Motorola image.

- The TRACES Server hard disk must be an SSD disk.

  NOTE: It is recommended for the hardware architecture to allow for extending memory to at least twice the size of the SSD.

- If deploying the TRACES Server in a virtualized environment, the SSD should not be shared with other Virtual Machines (VMs).
- Firewalls must be disabled for the TRACES service to function properly. If not disabled, the firewall must be specifically configured to allow port `8081`.
- The User Account Control feature in Windows must be set to **Never Notify**.
- The TRACES Server must be run on an account with administrator privileges.
- Two partitions must be configured. It is recommended that the Operating System (OS) is installed on the `C:/` drive, leaving the `D:/` drive for data storage.

1.2.2
TRACES Web Mapping Client Requirements

The TRACES Web Mapping Client is hosted on the TRACES Server.

Table 2: Web Mapping Client Hardware and Software Requirements

Browser	GPU	Memory	Additional requirements
Google Chrome version 76 or newer.	Modern graphics card	2 GB RAM	Connectivity to the TRACES Server

1.2.3
Additional Software Requirements

For the TRACES Server to operate, a number of software requirements must be fulfilled.

Table 3: Additional Software Requirements

UMR (Uplink Measurement Report) Data	DMR (Downlink Measurement Report) Data	Scout Data	Digital Geocoded Maps	RF Site List – minimum data required
BTS (Base Transceiver Station) Software version R6.1 Q209 or newer	iTM (Integrated Terminal Management) Release 4.0 or newer	Scout 10.0 or newer	Electronic geo-referenced maps of the coverage area in `MapInfo *.TAB` format	LAC (Location Area Code)
				Site name (identifier)
				Longitude
`DIMETRA-IP NM VLAN` network connectivity	Radio Terminal Software release MR 5.10 or newer			Latitude
				Zone ID
				Site ID

Chapter 2

TRACES Installation and Configuration

2.1 TRACES Server Installation

This section contains installation and configuration procedures for the TRACES Server and its components.

2.1.1 Installing the TRACES Server

The DIMETRA version of the application comprises the UMR (Uplink Measurement Report) Collector, MS Log Converter, Database Uploader, and the TRACES service.

Prerequisites:

- If TRACES version older than 2.3 is already installed, uninstall it and remove all configuration and log files.
- Obtain the `TRACESServerSetup64.exe` installation file.

Procedure:

1 Perform one of the following actions:

If…	Then…
If you want to install a new version of TRACES,	Proceed to step 2 .
If you want to install TRACES for the first time,	**a** In the installation `iso` file, browse to the **activedirectory** folder. **b** Right-click **installService.bat** and click the **Run as administrator** option. **c** After the installation finishes, press ENTER.

2 Open the `TRACESServerSetup64.exe` installation file.

The installation wizard appears.

3 Accept the license terms by clicking **I Agree** and, in the **Release notes** dialog box, click **Next**.

NOTE: If you want to install External API, select the **Server for DIMETRA with External API** option. See Configuring Web Container on page 33 .

4 In the **Choose Components** screen, from the drop-down menu, select **TRACES Server for Dimetra**. Click **Next**.

5 In the **Choose Install Location** screen, click **Browse** to select the destination folder. Click **Next**.

6 In the **Choose TRACES Data Location** screen, click **Browse** toS select the data directory. Click **Next**.

7 In the **Configuration of Elasticsearch performance in TRACES - select system size** window, select the system size and click **Next** .

The default system size provided by the installation is based on the disk size. Do not change it.

8 In **Choose Profile Name**, fill in the customer name and the path to the `KML` file.

If not specified, the customer name defaults to `TRACES`
The `KML` file can be specified later during the **Uploader** component configuration.

9 In the **TRACES Version Type Information** screen, confirm the selection of the “TRACES Server for DIMETRA” option by clicking **Install**.

10 At the end of the installation process, in the dialog box that prompts you to start the server, click **Yes**.

NOTE: If an external TRACES application pop-up window appears with a request for a license key, ignore it.

11 In the **Installation Complete** screen, click **Close**.

2.1.2
Installing and Configuring Microsoft ADSI Edit (Optional)

The Microsoft ADSI Edit tool allows you to verify that the TRACES Active Directory LDS service is running.

Procedure:

1 In the installation `.iso` file, browse to the **adsi** folder.

2 Right-click **installService.bat** and click the **Run as administrator** option.

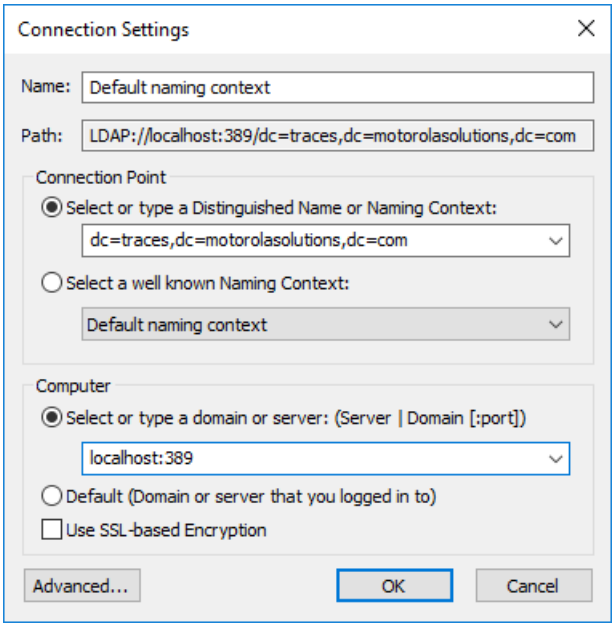
3 When the installation finishes, press ENTER.

4 In the **Start** menu, enter: `Adsi Edit`

5 In the **Service Manager ADSI Edit** tool, right-click **ADSI Edit** and click **Connect To**.

6 In the **Connection Settings** window, configure the settings as shown in Figure 2: Connection Settings Window on page 23.

Figure 2: Connection Settings Window



2.1.3
Launching TRACES Server UI

The TRACES Server User Interface (UI) provides access to configuration settings for the TRACES Server components.

NOTE: The TRACES Server UI displays the status of the service by using the following status images next to the TRACES Server icon:

Yellow exclamation mark ("!")
All components disabled

Red "X"
One or more components disabled

No additional status image
All components enabled

Procedure:

1 Go to **Start→Programs→TRACES Server→TRACES Server UI**.

The TRACES Server UI icon appears in your task bar.

2 Open the TRACES Server menu by right-clicking the **TRACES Server UI** icon.

2.1.4
TRACES Licensing

This section contains procedures for obtaining and applying the TRACES license.

The license file determines, among others, the maximum number of Base Transceiver Stations and Web Clients within the network.

2.1.4.1
Obtaining the License File

You can obtain the license from the Motorola Services team by sending the team a previously saved hardware ID file. For a complete list of licensed features, see Licensed Features on page 53.

Procedure:

1. From your task bar, right-click the **TRACES Server UI** icon and select **License**.
2. Perform one of following actions:
   - If you are obtaining the license for the first time, proceed to step 3.
   - If you are updating the license, in the **License information** window, select **Update License**.
3. In the **License verification** window, click **Save** and save the hardware ID file on the system disk as:
   <CustomerName> **_** ***<ServerName>*** **_** ***<HW_ID>***

   where ***<CustomerName>*** , ***<ServerName>*** , and ***<HW_ID>*** are custom values. The system generates the file name automatically.
4. Exit the **License verification** window by clicking **Cancel**.
5. When the error message appears, click **OK**.

Postrequisites: Send the saved hardware ID file to the Motorola Services team or another designated Motorola contact.

2.1.4.2
Applying the License

After obtaining the license file from the Motorola Services team and saving it on a system disc, you need to apply it in the TRACES Server UI license settings.

Procedure:

1. From the task bar, right-click the **TRACES Server UI** icon and select **License**.
2. Perform one of following actions:
   - If you are applying the license for the first time, proceed to step 3.
   - If you are reapplying the license, in the **License information** window, select **Update License**.
3. In the **License verification** window, select **Import**, navigate to the license file and select **Open**.
4. Verify the license by clicking **OK**.

   A pop-up window with information about services restart appears. When the restart finishes, the information about successful restart of services appears.
5. Close the window by clicking **OK**.

2.1.4.3
License Renewal

The license expires on the date specified in the service contract. If a license renewal is issued, see Applying the License on page 24 for information on how to update the TRACES server license.

2.1.5 TRACES Server Components Configuration

This sections contains configuration procedures for TRACES data-collecting components.

2.1.5.1 Configuring Uploader

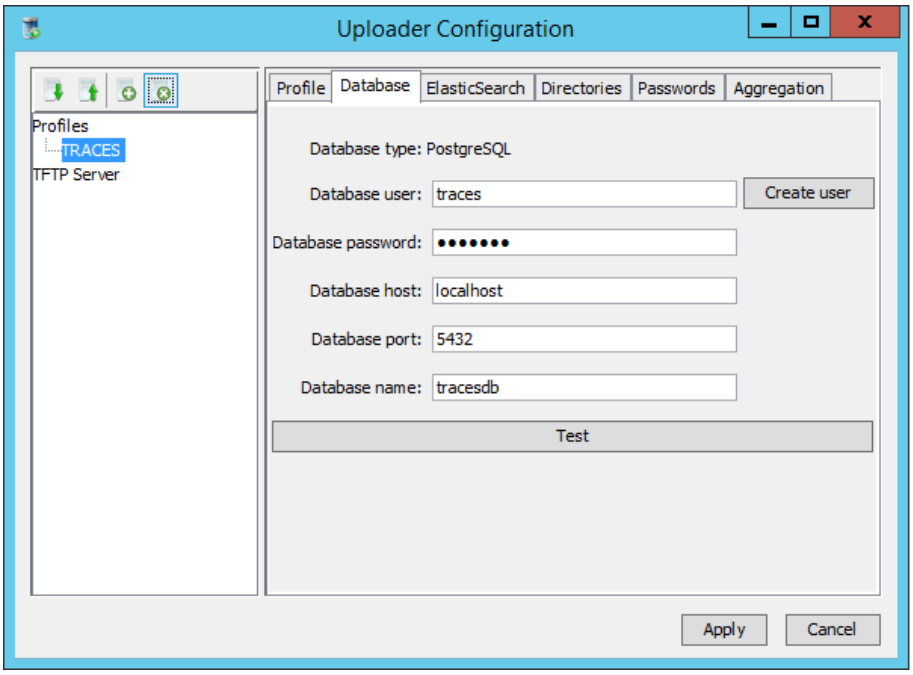
Uploader is used to upload data to the database.

NOTE: After modifying profiles in Uploader, the TRACES service needs to be restarted for the available profiles to reload in WebContainer, where you can match profiles with Web Client Users.

Procedure:

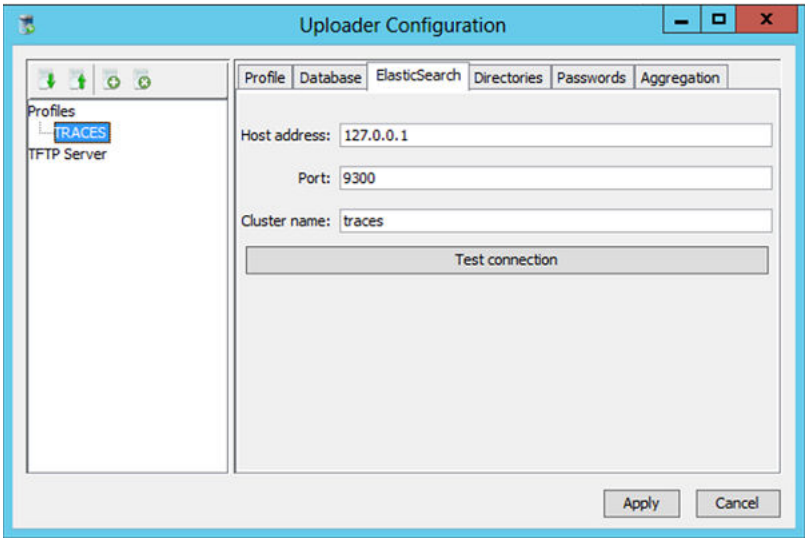
1. Right-click the **TRACES Server UI** icon and from the menu, select **Uploader→Configuration**.
2. In the **Uploader Configuration** window, from **Profiles** in the left pane, select **TRACES**.
3. On the **Profile** tab, perform the following actions:
   a. Ensure that the **Customer name** and **Customer prefix** are set to: `TRACES`
   b. Set the **Data expiration period [days]** according to instructions from the Motorola Services team.
4. On the **Database** tab, leave all settings unchanged and click **Test**.

Figure 3: Uploader Configuration – Database tab



5. Perform one of the following actions:
   - If a dialog box appears stating that the configuration is correct, return to the main **Uploader Configuration** window by clicking **OK**.
   - If a dialog box with errors appears, contact the Motorola Services team to determine the issue with database connectivity.
6. On the **ElasticSearch** tab, leave all settings unchanged and click **Test connection**.

Figure 4: Uploader Configuration – ElasticSearch tab



7 On the **Directories** tab, assign the following directories:

Upload directory
<Drive>*:\TRACESData\Uploader**, where ***<Drive> is the letter assigned to the drive selected during installation

Loaded directory
<Drive>*:\TRACESData\Uploader\Loaded**, where ***<Drive> is the letter assigned to the drive selected during installation

Rejected directory
<Drive>*:\TRACESData\Uploader\Rejected**, where ***<Drive> is the letter assigned to the drive selected during installation.

8 Click **Apply**.

2.1.5.2
Configuring Storage Deployer

The TRACES storage is deployed by using Storage Deployer. A specific storage type is deployed depending on the TRACES version installed for the particular infrastructure (ASTRO or DIMETRA). The storage cannot be migrated between infrastructures.

Procedure:

1 Right-click the **TRACES Server UI** and, from the menu, select **Uploader→Storage Deployer**.

2 In the **Storage Deployer** window, select the **Deploy/Migrate** check box and click **Deploy/Migrate**.

If errors appear during the deployment, contact the Motorola Services team.

3 If the deployment was successful, close the **Storage Deployer** window.

2.1.5.3

Configuring Database Aggregator

Database Aggregator is used to aggregate Uplink Measurement Report (UMR) data, which allows for faster data loading and viewing.

Prerequisites: Ensure you have the border file for your country/region in Google Earth kml format. To ensure the file is supported, contact the Motorola Solutions services team.

Procedure:

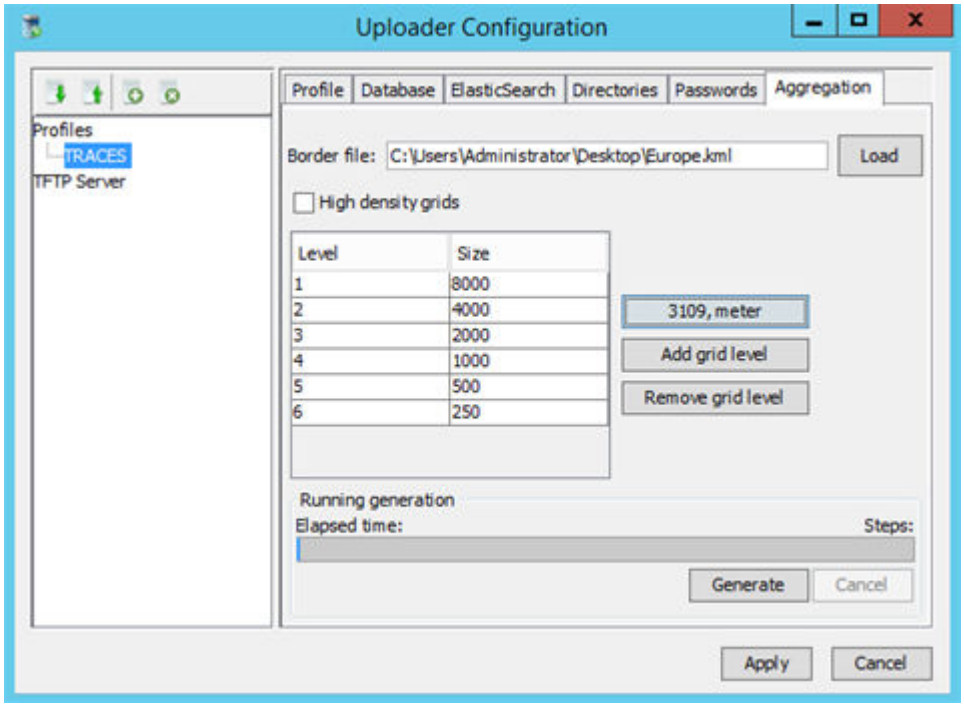
1 Right-click the **TRACES Server UI** and, from the menu, select **Uploader→Configuration** .

2 From the profile list on the left, select **TRACES**.

3 In the **Aggregation** tab, click **Refresh data**.

The Uploader aggregation settings window appears.

Figure 5: Uploader Tab – Aggregation Settings



4 Select the border file for your region/country by clicking **Load** .

5 Optional: Enable additional options for large area systems with large amounts of data by selecting **High density grids**.

NOTE: This option is dedicated to the UMR data source only. Selecting the **High density grids** check box before **Select SRID** creates additional two grid levels: 50 m and 25 m. To determine which option must be selected, contact the Motorola Services team.

6 Assign a set of uniform grid levels by clicking **Add grid level**.

The default set of grid levels to use is 8000, 4000, 2000, 1000, 500, and 250.

The following constraints are imposed on grid levels:

- The grid levels must be ordered from largest to smallest in size.

- The levels of smaller sizes must fit within those of bigger sizes, so groups of levels, such as: 10000, 1000, 100, or: 10000, 5000, 500 are acceptable, while groups of levels such as: 1000, 600, 40, 30, are not.
- The sizes of grids cannot be larger than the border file itself.

7 Select your region/country by clicking **Select SRID**.

8 Confirm your aggregation settings by clicking **Generate**.

The progress bar informs you of the operation status.

NOTE: When grid generation is finished, a pop-up info window appears. Do not click the **Apply** or **Cancel** buttons during grid generation. If you click one of those buttons during generation, perform Applying Buttons Clicked During Grid Generation on page 43.

9 In the status message, click **OK**.

10 Save the configuration by clicking **Apply**.

2.1.5.4 Configuring DMR Collector

Downlink Measurement Reports (DMRs) are captured by the Motorola TETRA terminals through Integrated Terminal Management (iTM), whenever they encounter a service interruption from the TETRA network. iTM Collector, or DMR Collector, converts the DMRs and Mobile Station logs (MS logs) to be uploaded to the database.

Prerequisites: Ensure the iTM server is present in the system and the iTM client is installed on the TRACES server.

NOTE: For details on iTM installation, version, policies, IP address and passwords, see the *Integrated Terminal Management 7.4 Administrator's Guide* manual.

Procedure:

1 Right-click the **TRACES Server UI** icon and, from the menu, select **DMR Collector→Configuration**.

The **iTM Collector** window appears.

2 In the **Main Configuration** tab, perform the following actions:

a Select the **iTM data collecting enabled** check box.

b Select the **Export to the Uploader enabled** check box.

c For **Customer prefix**, assign a customer prefix.

The default customer prefix is TRACES.

d For **Directory**, assign the TRACES uploader directory (***<Drive>***`:\TRACESData\Uploader`,

where ***<Drive>*** is the letter assigned to the drive selected during the installation). The default directory is `D:\TRACESData\Uploader`.

3 From the left pane of the window, select **iTM Pooler**.

4 In the **iTM Pooler** tab, perform the following actions:

a For the iTM version, select the check box assigned to the version installed.

NOTE: For details on iTM, see the *Integrated Terminal Management 7.4 Administrator's Guide* manual.

b For **User**, enter: `superuser`

This is the name of the user used to export the DMRs/MS logs from iTM.

c For **Password**, enter the iTM user password.

d For **IP and port of iTM Server**, enter the iTM Server IP address.

e Optional: For iTM version 6 SPU2 or later, in the field next to the IP address, enter the iTM port.

f Select the path to the **iTM Client Directory** by clicking **Browse**.

The default iTM Client Directory is `C:\Program Files\Motorola\iTMClient`

g Ensure that the **Pooling Period** is set to 15 minutes.

h Ensure that the **Historical Days** number is set to 7.

i In the **iTM Policy** field, click **Add** and select the policy created in iTM to export the DMRs/MS logs.

The default is MS Log Collection.

j Confirm the settings by clicking **Apply**.

2.1.5.5
Configuring Log Exporter

Log Exporter is used to add a header to the Scout files uploaded to the database.

Procedure:

1. Right-click the **TRACES Server UI** icon and, from the menu, select **Log Exporter→Configuration**.
2. In the **Log Exporter Configuration** window, add a new profile by clicking **+**.
3. Assign a **Customer Prefix**.

   The customer prefix should be identical to the one entered for the Uploader. See Configuring Uploader on page 25. The default customer prefix is “TRACES”.
4. Enter the **Source Directory**.

   The filepath should be identical to the Upload directory. The default source directory is as follows: ***<Drive>***`:\TRACESData\LogExporter\`***<Customer_Prefix>***, where ***<Drive>*** is the letter assigned to the drive selected during the installation, and ***<Customer_Prefix>*** is the previously entered prefix.
5. Enter the **Destination Directory**.

   The default destination directory is as follows: ***<Drive>***`:\TRACESData\Uploader`, where ***<Drive>*** is the letter assigned to the drive selected during the installation.
6. Confirm the settings by clicking **Apply**.

2.1.5.6

Configuring UMR Service Enabler

By configuring the UMR Service Enabler, you can enable the Base Transceiver System (BTS) to collect Uplink Measurement Reports (UMRs).

Uplink Measurement Reports are generated by the DIMETRA BTS when a terminal sends a GPS position update to the infrastructure.

NOTE: This procedure does **not** apply to Dimetra Express systems.

Prerequisites: Ensure that you are connected to the Dimetra-IP ZNM-VLAN network.

Procedure:

1. Right-click the **TRACES Server UI** icon and from the menu, select **UMR Collector→UMR Service Enabler**.
2. Add the IP address of your UCS (User Configuration Server) by selecting **Add UCS**.
3. Configure the following service parameters:
   a. For **BTS User Name**, enter the user name required to log on to the BTS.
   b. For **BTS Password**, enter the user password.
   c. Enable UMR collection by setting the **TETRA Services** to **Enabled**.
   d. For **Source SSI**, perform one of the following actions:
      - If you want to include the source SSI (Short Subscriber Identity) in the UMR data packets (the default option), select **Revealed**.
      - If you want to exclude the source SSI from the UMR data packets, select **Hidden**.
   e. For **Target SSI Range**, determine the range of target identities to be included in the UMR collection by entering values from “0” to “16777215”.
   f. For **Collector Server IP**, select the IP address of the TRACES server on which the UMR Collector is running.
   g. For **Port**, enter the UDP (User Datagram Protocol) port number required for communication with the UMR Collector.

      The number must be identical to the one entered during the UMR Collector configuration. See Configuring UMR Collector on page 30.
4. Under the **List of IP addresses** section, view BTS IP addresses from the UCS by clicking **Discovery**.
5. When all required BTS IP addresses are listed, click **Run**.

   The application communicates with each BTS through Telnet to enable the UMR collection.
6. In the window displaying the results of the operation, click **OK**.
7. Confirm the settings by clicking **Save configuration**.
8. Close the application window.

2.1.5.7

Configuring UMR Collector

The Uplink Measurement Report (UMR) Collector collects the UMRs sent by the Base Transceiver System (BTS) and prepares them for upload to the database.

Prerequisites: In the `TRACESData` folder, create a `UMROutput` subfolder.

Procedure:

1. Right-click the **TRACES Server UI** icon and, from the menu, select **UMR Collector→Configuration**.
2. In the **Collecting** tab, enter the output files prefix.

   The prefix should be identical to the one entered during the Uploader configuration. See Configuring Uploader on page 25. The default prefix is set to “TRACES”.
3. For **Output directory**, select **Browse** and navigate to the `UMROutput` folder, where raw UMR files are temporarily stored.

   The default path is: ***<Drive>***`:\TRACESData\UMROutput`, where ***<Drive>*** is the letter assigned to the drive selected during installation.
4. Enter the number of the **UDP Port** for communication with the BTS. For Dimetra Express systems, leave the default number.

   The default number is `49876`.
5. Perform one of the following actions:
   - If your license is for a limited number of BTSs, ensure that the **Enable BTS auto accepting** check box is selected.
   - If your license is for an unlimited number of BTSs, ensure that the **Enable BTS auto accepting** check box is cleared.

   Dimetra Express systems do not support BTS licenses.
6. Optional: Perform the following actions:
   a. Enable the decryption of received UMR data by selecting the **Enable decryption** check box.
   b. If all incoming traffic is encrypted, clear the **Allow unencrypted data** check box.

   One of the decryption keys (Primary Key or Secondary Key) must match the current encryption key.

   For regular Dimetra systems, the encryption key is defined in the UMR Service Enabler.

   NOTE: In large Dimetra systems, a change of the encryption key may take from a few minutes up to a few hours. During this period, some BTS sites are still using the old key, while others switch to the new key. It is important **not** to remove the old key until the key update is completed. Specify the new key as an alternative.

   For Dimetra Express systems, the decryption key must match the configuration in the Express GUI of the Dimetra Express server.
7. Optional: If for security reasons ISSI/GSSI filtering is required, select the **Filtering** tab and perform the following actions:
   a. Load an ISSI/GSSI filtering configuration file by selecting **Import File**.
   b. From the list, according to your preference, select either **Keep filtered data (replace SSI)** or **Discard filtered data**.
   c. Enable the filtering by selecting the **Filtering active** check box.
8. **NOTE:** If you are configuring a Dimetra Express system, skip this step and go to step 9.

   In the **BTS Site Management** tab, configure BTS licensing by performing the following actions:
   a. From the navigation pane, right-click the selected zone or site and authorize the license for the required BTS sites by clicking **Accept**.
   b. Perform this action for each zone or site, until the **Remaining licenses** count in the right-hand section of the window is “0”.

9 In the **Converting** tab, configure the frequency of uploading the UMR data to the database by performing the following actions:

   a Set the **Converting period**.

   The default is one hour.

   b Set the **Converting output directory** to ***<Drive>***`:\TRACESData\Uploader`, where ***<Drive>*** is the letter assigned to the drive selected during installation.

10 If live UMR data is required, select the **Stream Data** tab and perform the following actions:

   a Select the **Direct data streaming enabled** check box.

   b Enter the **Uploader address/IP**.

   The default uploader address/IP is “localhost”.

11 **For Dimetra Express:** On the **Express Configuration** tab, enter the Express Server IP address.

12 Confirm the settings by clicking **Apply**.

2.1.5.8
Adding Web Client Users

Procedure:

1 Right-click the **TRACES Server UI** icon and, from the menu, select **Web Container→Configuration**.

2 On the **USERS** tab, add a new user profile by clicking **Add**.

3 In the dialog box, define a user account for the TRACES Web Application by providing information for the following columns:

Alias
Name of the user account.

Password
Password defined for the particular user account.

Profile
Data profile previously defined in Uploader. See Configuring Uploader on page 25.

Enabled
The status of the check box indicates whether the particular user account is active and can be used to log on to the Web Client.

NOTE: The `traces` user and a list of users with the ***<profile>*** `_extapi Alias,` where ***<profile>*** is an individual name of the user,

may already appear on the **USERS** tab. This occurrence is normal and the existing user data should not be modified.
The **Locked** option is greyed out.

2.1.5.9
Unlocking User Accounts

When a user enters a wrong password three times in a row, the password is blocked and must be unlocked.

Prerequisites: Log on to the TRACES server with the administrator account.

Procedure:

1. Right-click the **TRACES Server UI** icon and from the menu, select **Web container→Configuration** .
2. Open the **Users** tab.
3. Click **Edit**
4. For the user you want to unlock, clear the **Locked** option.

2.1.5.10 Configuring Web Container

Web Container is a module that hosts the TRACES Web application and its configuration is essential for using the Web Client. Web Container can be configured by using TRACES Server UI.

Procedure:

1. Right-click the **TRACES Server UI** icon and, from the menu, select **Web Container→Configuration**.
2. Add user accounts. See Adding Web Client Users on page 32.
3. In the **HTTPS** tab, configure the secure HTTP connection by performing the following actions:
   a. Select the **HTTPS enable** check box.
   b. For **HTTPS port**, enter the HTTPS port number.

      NOTE: The port number must not be used by other applications or TRACES modules. The default is set to "443"

   c. Enter the **Key file path** and **Key password**.

      Keys are in PKCS # 12 format.

   You can access the TRACES Web application through the HTTPS protocol by entering one of the following addresses in the address bar:

   - `https://localhost`
   - `https://localhost: <port_number> /tracesweb/` if the configured ***<port_number>*** is **NOT** 443.

4. If information about the connection being not private appears, click **Advanced→Proceed to localhost (unsafe)**.

2.1.5.11 Configuring External API Service

External API is a service that provides TRACES data, such as processed Uplink Measurement Reports (UMR) and map data, to external applications. The service is configured by using Trust Application mode, which guarantees that the application will have access to TRACES data. To use it, you must generate a digital signature.

NOTE: External API Service installation verification can be performed by right-clicking the TRACES Server UI icon and verifying whether the External API Service appears as an expandable option.

Prerequisites:
Verify that the license for External API is obtained. See TRACES Licensing on page 23.

Verify that External API was selected while installing TRACES. See Installing the TRACES Server on page 21.

Procedure:

1 From the **TRACES Server** folder, open the **adminscripts** folder.

NOTE: The location of the folder is dependent on your custom settings during the installation. The default path is: `C:\Program Files\MotorolaSolutions\TRACESServer\adminscripts`

2 Open Command Prompt.

3 Perform one of the following actions:

If…	Then…
If you want to register a given trusted application,	enter: `trustedApplicationsManager.bat -r` ***<<app_name>>*** where ***<app_name>*** is the name of the application.
If you want to list all registered trusted applications,	enter: `trustedApplicationsManager.bat -l`
If you want to unregister a given trusted application,	enter: `trustedApplicationsManager.bat -u` ***<app_name>*** where ***<app_name>*** is the name of the application.

4 Copy the result, RSA private key and remember the identifier of the trusted application.

5 Use the copied RSA private key in the second party application which implements the TRACES External API.

NOTE: For second party application development: To obtain specification of the TRACES External API, contact the Motorola Solutions support.

2.1.5.11.1
Using Externally Generated SSL Certificates with External API Services

Procedure:

See Importing the Customer Private Certificate into the TRACES Keystore on page 36.

2.1.5.11.2
Replacing SSL Certificates

Process:

1 De-register and re-register the External API client app. See Configuring External API Service on page 33.

2 Install a third-party public certificate. See Importing Public Certificates into the TRACES Truststore on page 37.

2.1.5.12

Password Complexity Requirements

By default, TRACES passwords must meet specific complexity requirements. You have to change the password every 40 days.

- Passwords cannot contain the user account name or parts of the user's full name that exceed two consecutive characters.
- Passwords must be at least six characters long.
- Passwords must contain characters from three of the following categories:
  - English uppercase characters
  - English lowercase characters
  - digits (0 through 9)
  - non-alphabetic characters (!, $, #, %)

2.2

Populating RF Sites

The RF (Radio Frequency) Sites list must be created and populated on the TRACES Server in the form of a comma-separated values file.

Procedure:

1 Create a file in the comma-separated values format (`.csv` file) with the following column names in the field header:

LAC
Location Area Code for the site

Identifier
The name of the site

Longitude, Latitude
Geographical coordinates of the site

Zone
The number of the zone to which the site is connected

Site
The site number configured in the zone

2 When the list is created, add the following line at the beginning of the file:

`# type = RF_SITES; customer =` ***<customer_prefix>;***

where ***<customer_prefix>*** is the same prefix as the one entered during the Uploader configuration. See Configuring Uploader on page 25. The default is: `TRACES`

3 Save the file to the ***<Drive>***`:\TRACESData\Uploader` directory, where ***<Drive>*** is the letter assigned to the drive selected during installation.

4 Wait for approximately two minutes and verify that the file is moved from the ***<Drive>***`:\TRACESData\Uploader` directory to the ***<Drive>***`:\TRACESData\Uploader\Loaded` directory.

2.3 TRACES Web Mapping Client Configuration

The TRACES Web Mapping Client is hosted on the TRACES Server. To access the Web Mapping Client, a proper configuration of Web Container is required. For information on how to configure Web Container, see Configuring Web Container on page 33.

For information on how to access the TRACES Web Client, see the *TRACES User Guide*.

2.4 TRACES Certificate Management

TRACES has two built-in self-signed certificates for the server authentication and the HTTPS server. These certificates are generated automatically during the first TRACES installation. Extra certificates can be installed for use with the External API.

Table 4: TRACES Certificates

Alias	Internal	Server Auth	Common Name	Key	Signature
`traces-services-https`	Y	Y	`Motorola_Solutions_TRACES_Self_SHA256withRSA`	RSA 2048	SHA 256
`traces-webcontainer-https`	Y	N	`Motorola_Solutions_TRACES_Web_SHA256withRSA`	RSA 2048	SHA 256
<ExtAPI app name>	Y	N	`Traces`*	RSA 2048*	SHA 512*

* Applies to certificates generated with the `trustedApplicationsManager.bat` script.

2.4.1 Importing the Customer Private Certificate into the TRACES Keystore

Prerequisites:
Ensure that:

- The Java executable is on your system path. The following is the default location: `C:\Program Files\MotorolaSolutions\TRACESServer\java\bin`
- The certificate is saved in PKCS12 format (with a `.p12` or `.pfx` extension), which can be exported to the keystore.
- The certificate contains a valid Subject Alternative Names (SAN) extension.

Procedure:

1. In Command Prompt, open the `ProgramData TRACESServer` folder and execute the following command:

`keytool -importkeystore -destkeystore keystore.jks -srckeystore` ***<pkcs12 certificate>*** `-srcstoretype PKCS12 -srcalias` ***<srcalias>*** `-destalias` ***<alias>***
where:

<srcalias> can be either set to `1` or, if your certificate has the **friendlyName** attribute set, you can set it to the **friendlyName** attribute value.
<alias> is the certificate alias. For the list of valid certificate aliases, see TRACES Certificate Management on page 36.

2 At the prompt, enter the destination keystore password and the password of your certificate.

3 When prompted to override the existing key, enter: `yes`

4 Change the password of the private key to match the keystore password by executing the following command:

`keytool -keypasswd -keystore keystore.jks -alias` ***<alias>***
where ***<alias>*** is the certificate alias. For the list of valid certificate aliases, see TRACES Certificate Management on page 36.

5 At the prompt, enter your keystore password.

6 Enter the original private key password.

7 Enter the new private key password, and confirm it by re-entering it.

2.4.2
Importing Public Certificates into the TRACES Truststore

Prerequisites:
Ensure that the Java executable is on your system path. The following is the default location:
`C:\Program Files\MotorolaSolutions\TRACESServer\java\bin`

Procedure:

1 Execute the following command:

`keytool -import -storetype JKS -alias` ***<alias>*** `-keystore truststore.ts -file` ***<crt file>***
where ***<alias>*** is the certificate alias. For the list of valid certificate aliases, see TRACES Certificate Management on page 36.

2 At the prompt, enter the truststore password.

3 When prompted to override the existing key, enter: `yes`

2.4.3
Exporting Public Certificates from Private Certificates in the TRACES Keystore

Prerequisites:
Ensure that the Java executable is on your system path. The following is the default location:
`C:\Program Files\MotorolaSolutions\TRACESServer\java\bin`

Procedure:

1 Execute the following command:

`keytool -export -rfc -alias` ***<alias>*** `-keystore keystore.jks -file` ***<crt file>***
where ***<alias>*** is the name under which the private certificate was saved in the keystore.

2 At the prompt, enter your keystore password.

2.4.4
Generating Self-Signed Certificates in the TRACES Keystore

Prerequisites:
Ensure that:

- The Java executable is on your system path. The following is the default location: `C:\Program Files\MotorolaSolutions\TRACESServer\java\bin`
- The value of the **Subject Alternative Names (SAN)** field is: `dns:localhost,dns:`***`<hostname>`***`,dns:`***`<FQDN>`***`,ip:127.0.0.1,ip:`***`<hostIP1>`***`,ip:`***`<hostIPn>`***

  where ***`<FQDN>`*** stands for fully-qualified domain name, and is optional if it is identical to ***`<hostname>`***.
- Verify if the certificate requires the server authentication extension. See TRACES Certificate Management on page 36. If it does, replace ***`<server_auth_extension>`*** with `-ext eku=serverAuth`. Otherwise, remove it.

Procedure:

1 Execute the following command:

```
keytool -genkey -keyalg RSA -validity 9125 -storetype
JKS -alias <alias> -keystore keystore.jks -dname
"C=US, O=Motorola_Solutions_LMR,CN=<common_name>" -ext san="<SAN>"
<server_auth_extension>
```

where ***`<alias>`*** is the certificate alias. For the list of valid certificate aliases, see TRACES Certificate Management on page 36.

2 At the prompt, enter your keystore password.

Chapter 3

TRACES Backup and Restore

Performing a backup of the TRACES data and storage is necessary for protection against potential data loss.

3.1 Data Backup and Restore

This section contains backup and restore procedures for the data collected from Uploader.

NOTE: Data backup and restore procedures must be performed prior to the TRACES upgrade process.

3.1.1 Backing Up Data

Procedure:

1. Navigate to the previously created **Loaded** directory. See Configuring Uploader on page 25.

   The default path is: `D:\TRACESData\Uploader\Loaded`
2. Select and create copies of all files you wish to back up.
3. Move the copy files to a selected secure location outside of the server.

3.1.2 Restoring Data

Procedure:

1. Navigate to the previously created **Uploader** directory. See Configuring Uploader on page 25.

   The default path is: `D:\TRACESData\Uploader`
2. Navigate to the secure location outside of the server that you previously used to back up data files. See Backing Up Data on page 39.
3. From the backup files directory, transfer any files that you wish to restore to the **Uploader** directory.

   The files will be subsequently loaded to the database.

3.1.3 Deleting Data

Procedure:

1. Right-click the **TRACES Server UI** icon and from the menu, select **Uploader→Sessions**.
2. In the **Uploader Sessions List** window, perform the following actions:
   - **a** From the drop-down menu, select the customer profile by clicking **Customers**.
   - **b** From the drop-down menu, select the required file type by clicking **File types**.
   - **c** From the list of files that appears, select the files to be deleted and click **Delete**.

d In the confirmation dialog box that appears, click **Yes**.

e In the dialog box that appears, click **OK**.

3 Close the **Uploader Sessions List** window.

3.2 Preparing the Shared Folder

Shared folder preparation is dependent on individual network configuration.

Procedure:

1 On your backup machine, create a folder accessible for all TRACES Server nodes.

2 Configure the sharing settings of the folder.

3 Ensure that the Elasticsearch service is running on each TRACES Server node with Administrator privileges.

3.3 Storage Backup and Restore

This section contains backup and restore procedures for the database and Elasticsearch.

3.3.1 Backing Up TRACESData Folder

Procedure:

1 Right-click the **TRACES Server UI** icon and, from the menu, select **Exit**.

2 Stop the Elasticsearch services by selecting **Start→Run**, and entering: `services.msc`

a Right-click **TRACESServer** and select **Stop**.

b Right-click **Traces** and select **Stop**.

c Right-click **TRACESDatabase** and select **Stop**.

d Right-click **TRACESElasticSearch** and select **Stop**.

e Right-click **TRACESRabbitMQ** and select **Stop**.

3 Run the command prompt by navigating to **Start→Run**, and enter `cmd`

4 In the command prompt, copy the TRACES data folder by entering the following command:
`robocopy <TRACESData_FOLDER_LOCATION>\TRACESData<SHARED_FOLDER_DIRECTORY>\TRACESData /dcopy:DAT /MIR`

Step example:
`robocopy D:\TRACESData X:\TRACESData /dcopy:DAT /MIR`

WARNING: The /MIR parameter mirrors a complete directory tree and can **delete** files.

3.3.2 Restoring TRACESData Folder

Procedure:

1 Right-click the **TRACES Server UI** icon and, from the menu, select **Exit**.

2 Stop the Elasticsearch services by navigating to **Start→Run**, and entering: `services.msc`

   a Right-click **TRACESServer** and select **Stop**.

   b Right-click **Traces** and select **Stop**.

   c Right-click **TRACESDatabase** and select **Stop**.

   d Right-click **TRACESElasticSearch** and select **Stop**.

   e Right-click **TRACESRabbitMQ** and select **Stop**.

3 Run the command prompt by navigating to **Start→Run**, and enter `cmd`

4 In the command prompt, copy the TRACES data folder by entering the following command:
`robocopy`
<SHARED_FOLDER_DIRECTORY>`\TRACESData`***<TRACESData_FOLDER_LOCATION>***`\TRACES Data /dcopy:DAT /MIR`

   Step example:
`robocopy X:\TRACESData D:\TRACESData /dcopy:DAT /MIR`

   WARNING: The /MIR parameter mirrors a complete directory tree and can **delete** files.

5 Start the Elasticsearch service by navigating to **Start→Run**, and entering: `services.msc`

   a Right-click the **TRACESServer** and select **Start**.

   b Right-click **Traces** and select **Start**.

   c Right-click **TRACESDatabase** and select **Start**.

   d Right-click **TRACESElasticSearch** and select **Start**.

   e Right-click **TRACESRabbitMQ** and select **Start**.

6 Run the TRACES Server by navigating to **Start→TRACES Server→TRACES Server UI**.

Chapter 4

Troubleshooting

This section contains troubleshooting procedures for the most common issues in TRACES.

4.1 Enabling Base Transceiver System with Multiple Passwords

To enable the TRACES Service for individual sites, a password needs to be configured in the UMR (Uplink Measurement Report) Service Enabler. If more than one password is used in the system, a standalone UMR Service Enabler must be used for each configuration.

Procedure:

1. Create a shortcut file (`.lnk` file) with the following target: `C:\Program Files\MotorolaSolutions\TRACESServer\umrcollector" -Xms128m -Xmx512m -jar BTSEnabler.jar`
2. From **Start**, run: `regedit.exe`
3. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\umr_col`
4. Right-click anywhere in the right pane of the window and select **New→String value**.
5. Save the new string value as `ldata`
6. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\traces_srv`
7. Right-click the existing `ldata` file and select **Modify**.
8. Copy the value from the **Value data** field.
9. Navigate back to `HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\umr_col\ldata`, right-click the **ldata** file and select **Modify**.
10. Paste the copied value into the **Value data** field.
11. Click **OK**.

    You can now run a standalone UMR Service Enabler by clicking the created shortcut.

    NOTE: The BTS (Base Transceiver System) password type must be set to **Engineering access**. The Collector Server IP cannot be "localhost".
    It is recommended that you use the BTS interface to communicate with TRACES Server instead.

4.2 Collecting Logs from the TRACES Application

Procedure:

1. From the **TRACESServer** folder, open the **adminscripts** file.

   NOTE: The location of the folder is dependent on your custom settings during the installation. The default path is `C:\Program Files\MotorolaSolutions\TRACESServer\adminscripts`

2 Run the following script: `bkpLogs`

Log files are saved to `D:\!Bkp\Logs` and are individually accessible in folders named after the current date.

4.3 Applying Buttons Clicked During Grid Generation

NOTE: Grid generation process cannot be interrupted with the **Apply** or **Cancel** buttons. If you click one of the buttons, the Traces Server may freeze or crash, or the drawing grid on Traces Web may cause Internal Server Error.

Procedure:

1 Click **Uploader→Storage Deployer** .
2 In the **Storage Deployer** window, select your storage.
3 Click **Delete Storage** .
4 In the warning pop-up window, click **OK** .
5 In the text field, enter: `delete`
6 Configure the storage deployer. See Configuring Storage Deployer on page 26 .
7 Configure the database aggregator. See Configuring Database Aggregator on page 27 .

4.4 Fixing Grid Generation Failures

Procedure:

1 Click **Uploader→Storage Deployer** .
2 In the **Storage Deployer** window, select your storage.
3 Click **Delete Storage** .
4 In the warning pop-up window, click **OK** .
5 In the text field, enter: `delete`
6 Restart Traces services.
7 Right-click the **TRACES Server UI** and, from the menu, select **Uploader→Configuration** .
8 From the profile list on the left, select the profile that you want to modify.
9 In the **Aggregation** tab, select the border file for your region/country by clicking **Load** .
10 Click **Select SRID** .
11 In the **Select SRID** window, select the coordinate system that uses degrees instead of metric units.
12 Click **OK** .
13 In the **Uploader Configuration** window, select the **High density grid** option.
14 Click **Apply.**

Chapter 5

Map Server

This section provides instructions for installing the Map Server and an offline base map.

5.1 Installing a Base Map

This section provides instructions for installing an offline base map. The Map Server provides maps for the TRACES Server. It also includes a basic world map.

Prerequisites: You can request a custom map from Motorola Solutions ESSC. Specify the area of your interest by using Google Maps and deliver the exact location as a screen capture of a map or a geographical name of the area.

Procedure:

1. From the TRACES Server main menu, select **Map Server**.
2. Perform one of the following actions:

If…	Then…
If you want to use the provided basic world map,	click **Use built-in map**.
If you want to provide a custom map,	perform the following actions: **a** Click **Browse**. **b** Select a `.vhd`, `.tpk`, or `.zip` file.

3. Optional: After providing the `.tpk` or `.zip` file, the map destination option appears. To change it, click **Browse** next to the actual destination path.

   The default path is `C:\ProgramData\MotorolaSolutions\TRACESServer\mapserver`

   NOTE: The destination folder must be on a partition that has enough space for extracting `.zip` or processing `.tpk` file.

4. Click **Install map**.

   Elapsed time is visible at the bottom of the display.

   When the installation is complete, a message appears stating that the map was installed successfully.

5. Press **OK**.

   The file path to the **Current map** updates automatically.

6. Close the window.

5.2 Uninstalling a Base Map

Procedure:

1. From the TRACES Server main menu, select **Map Server**.

   NOTE: You can check the already installed map in the **Current map** section.

2. Click **Uninstall map**.

   When the uninstallation is complete, a message appears stating that the map was installed successfully.

3. Press **OK**.

   The **Current map** file path remains empty.

   NOTE: The map uninstaller does not delete the `.vhd` file. You have to delete the file manually.

4. Close the window.

5.3 Installing the Map Server

The Map Server provides maps for the TRACES Server. It also includes a basic world map.

Prerequisites:
Obtain the Map Server installation media included in the TRACES Server Installation media image.

Optional: You can request a custom map from Motorola Solutions ESSC. Specify the area of your interest by using Google Maps, and deliver the exact location as a screenshot of a map or a geographical name of the area.

Procedure:

1. Browse to the installation `.iso` folder, and open `TRACESMapsServerSetup64-<version_number>.<build_number>.exe`

   For example: `TRACESMapsServerSetup64-2.5.0.2042.exe`
   where `2.5.0` is the version number, and `2042` is the build number.

2. Accept the license terms by clicking **I Agree**.
3. In the **Choose Install Location** screen, select the destination folder by clicking **Browse**. Click **Next**.
4. In **Choose VHD File Location**, perform one of the following actions:
   - If you want to use the provided basic world map, click **Use Basic World Map**.
     You need to wait a moment for the map to decompress. When the decompression is done, the **VHD File Path** field is populated with the path of the `.vhd` file.
   - If you want to provide a custom map, click **Browse** and choose the `.vhd` file.
5. Click **Install**.
6. At the end of the installation process, in the dialog box that prompts to start the server, click **Yes**.
7. In the **Installation Complete** screen, click **Close**.

5.4

Installing Base Maps from .tpk File

Prerequisites:
Install the Map Server. See Installing the Map Server on page 45.

Procedure:

1. Navigate to the Map Server installation directory.

   The default location of the installation directory is: `C:\Program Files\MotorolaSolutions\TRACESMapsServer`
   It may differ based on the settings you selected during the installation.
2. Open Command Prompt.
3. Run the `parseTpk.bat` script by entering the following:

   `parseTpk.bat "<tpk file path>" "<vhd file path>"`
   where:

   <tpk file path> is an argument containing the path to the `.tpk` file.

   <vhd file path> is an **optional** argument indicating where the generated `.vhd` file should be placed.

   The default location of the `.vhd` file is: `C:\ProgramData\MotorolaSolutions\TRACESMapServer\maps`. To view the description of the arguments, you can run the script without any arguments.

   Step example:
   `parseTpk.bat "C:\Users\Motorola\Desktop\file.tpk"`
4. Wait until the script completes.

   When it is successfully parsed, the message `done` is displayed.
5. Open the TRACES Web application.
6. From the left menu bar, access settings.
7. Select **General→Base Map configuration**, and set **TRACES Map Server** to **Source**.

Appendix A

Data Export Formats

For more information on exporting data by using TRACES Web Mapping Client GUI, see the "TRACES Web Mapping Client" section in the *TRACES User Guide*.

A.1 Source of Data: DMR

DMR data can be exported in `CSV` and `JSON` format.

A.1.1 DMR: CSV Format

File name format: `DMR_`***`<from_time>`***`_`***`<to_time>`***`.csv`,
where ***`<from_time>`*** and ***`<to_time>`*** format is `YYYY-MM-ddTHH-mm-ss`

For example: `DMR_2019-11-01T00-00-01_2019-11-01T23-59-59.csv`

Table 5: CSV Format Fields for DMR Data

Field Name	Description	Example
DateTime	Time of sample in format `YYYY-MM-ddTHH:mm:ss UTC`	2019-11-01T18:15:31 UTC
ISSI	Radio identifier. Range: 0 - 16777216	10005
Lac	Location Area Code. Decimal	100
Channel	Channel number. Decimal	100
Ncells	Cells number. Decimal	1
Longitude	GPS Latitude position. Decimal degree value. Range: -180..180 (WGS84)	50.1243
Latitude	GPS Latitude position. Decimal degree value. Range: -90..90 (WGS84)	-10.1212
CellState	Cell state value. Decimal	0
Rssi	Received Signal Strength Indication. Float value in dBm	-79.5

Field Name	Description	Example
LinkFailCause	Code of link fail cause. Integer value. List of codes is available in DMR Link Fail Cause Codes on page 52	48
LinkFailCauseName	Description of link fail cause. Description of codes are available in DMR Link Fail Cause Codes on page 52	Insufficient signal strength

Example:
Example of a CSV file containing DMR data

```
DateTime,ISSI,Lac,Channel,Ncells,Longitude,Latitude,CellState,Rssi,
LinkFailCause,LinkFailCauseName
2019-11-01T18:15:31 UTC,10005,1,1063,1,50.0212,19.8916,0,-79,16,Poor signal
quality
2019-11-01T18:20:53 UTC,1007,3748,3600,1,50.0215,19.9020,0,-111,48,
Insufficient signal strength
```

A.1.2
DMR: JSON Format

File name format: `DMR_<from_time>_<to_time>.json`
where ***<from_time>*** and ***<to_time>*** format is `YYYY-MM-ddTHH-mm-ss`

For example: `DMR_2019-11-01T00-00-01_2019-11-01T23-59-59.json`

The `JSON` file contains the same field names as defined in the `CSV` format, and an additional **metadata** section that includes all applied filters.

Example:
Example of a JSON file containing DMR data

```
{
    "Metadata":{
        "Version":1.0,
        "From":"2014-01-01T00:00:00",
        "To":"2014-01-02T23:59:00",
        "Source":"DMR",
        "AppliedFilters":{
            "Channel":"[3600]",
            "ISSI":"[1002]",
            "LinkFailCause":"[Uplink failure]",
            "ZoneSite":"[KRK006, KRK011]"
        }
    },
    "Data":[
        {
            "DateTime":"2014-01-01T20:51:29 UTC",
            "ISSI":1002,
            "Lac":3748,
            "Channel":3600,
            "Ncells":1,
            "Longitude":19.90888,
            "Latitude":50.06763,
            "CellState":0,
```

```
            "Rssi":-111,
            "LinkFailCause":33,
            "LinkFailCauseName":"Uplink failure"
        },
        {
            "DateTime":"2014-01-02T06:28:46 UTC",
            "ISSI":1002,
            "Lac":3748,
            "Channel":3600,
            "Ncells":1,
            "Longitude":19.89784,
            "Latitude":50.07687,
            "CellState":0,
            "Rssi":-113,
            "LinkFailCause":33,
            "LinkFailCauseName":"Uplink failure"
        }
    ]
}
```


A.2
Source of Data: Scout

Scout data can be exported in `CSV` and `JSON` format.

A.2.1
Scout: CSV Format

File name format: `SCOUT_`***`<from_time>`***`_`***`<to_time>`***`.csv`
where ***`<from_time>`*** and ***`<to_time>`*** format is `YYYY-MM-ddTHH-mm-ss`

For example: `SCOUT_2019-11-01T00-00-01_2019-11-01T23-59-59.csv`

Table 6: CSV Format Fields for Scout Data

DateTime	Time of sample in format `YYYY-MM-ddTHH:mm:ss UTC`	2019-11-01T18:15:31 UTC
Channel	Channel number. Decimal	100
Longitude	GPS Latitude position. Decimal degree value. Range: -180..180 (WGS84)	50.1243
Latitude	GPS Latitude position. Decimal degree value. Range: -90..90 (WGS84)	-10.1212
Trigram	Site name if available Text	KRK004
Timeslot	The used time slot (1, 2, 3, 4). Decimal	1
Lac	Location Area Code Decimal	100

Rdc	Radio Downlink Counter Decimal	3
Rssi	Received Signal Strength Indication. Float value in dBm	-79.5
Mer	Message Erasure Rate as defined in ETSI document EN 300 392-2. Decimal	1
Cx1	Serving Cell, See C1 value in Scout documentation Decimal	1

Example:
Example of a CSV file containing Scout data

```
DateTime,Channel,Longitude,Latitude,Trigram,Timeslot,Lac,Rdc,Rssi,
Mer,Cx1
2014-01-01T08:10:27 UTC,804,19.8937,50.0221,KRK001,1,3712,432,-69,2,31
2014-01-01T08:10:28 UTC,804,19.8955,50.0139,KRK001,1,3712,432,-47,1,53
```

NOTE: For more information on scout exported data, see the Scout Manual located at http://www.scouthome.de/.

A.2.2
Scout: JSON Format

File name format: `SCOUT_<from_time>_<to_time>.json`
where *<from_time>* and *<to_time>* format is `YYYY-MM-ddTHH-mm-ss`

For example: `SCOUT_2019-11-01T00-00-01_2019-11-01T23-59-59.json`

The `JSON` file contains the same field names as defined in the `CSV` format, and an additional **metadata** section that includes all applied filters.

Example:
Example of a JSON file containing Scout data

```
{
    "Metadata":{
        "Version":1.0,
        "From":"2014-01-01T01:00:00",
        "To":"2014-01-02T23:59:59",
        "Source":"SCOUT",
        "AppliedFilters":{
            "Channel":"[822]",
            "ZoneSite":"[KRK004]",
            "Session":"[Route2]"
        }
    },
    "Data":[
        {
            "DateTime":"2014-01-01T08:33:42 UTC",
            "Channel":822,
            "Longitude":19.9097,
            "Latitude":49.9976,
```

```
            "Trigram":"KRK004",
            "Timeslot":1,
            "Lac":3723,
            "Rdc":432,
            "Rssi":-83,
            "Mer":0,
            "Cx1":17
        },
        {
            "DateTime":"2014-01-01T08:33:43 UTC",
            "Channel":822,
            "Longitude":19.9099,
            "Latitude":49.9976,
            "Trigram":"KRK004",
            "Timeslot":1,
            "Lac":3723,
            "Rdc":432,
            "Rssi":-84,
            "Mer":0,
            "Cx1":16
        }
    ]
}
```

Appendix B

DMR Link Fail Cause Codes

Table 7: DMR Link Fail Cause Codes

Value	Description	Legend Text
16	L1 BAD CRC	Poor signal quality
32	MAXIMUM PATH DELAY EXCEEDED	Max path delay exceeded
33	RADIO UPLINK FAILURE	Uplink failure
35	CIPHER SET RESULT FAILURE	Cipher set result failure
36	JAMMED CHANNEL	Jammed channel
48	NEGATIVE CX	Insufficient signal strength
49	INVALID AIE CELL	Invalid air interface encryption cell
50	FORCED REGISTRATION FAILURE	Forced registration failure
51	L1 MEASUREMENT INDICATION TIMER EXPIRED	Measurement indication timer expired
52	TXI OFF	Transmit inhibit off
53	MCCH MULTIPLE TO FAILED SINGLE	MCCH multiple to failed single
54	MCCH MULTIPLE TO FAILED MULTIPLE	MCCH multiple to failed multiple
55	INVALID CELL DENIED LA	Invalid cell – denied LA
56	SUBSCRIBER CLASS MISMATCH	Subscriber class mismatch

Appendix C

Licensed Features

Table 8: TRACES 2.6 Licensed Features

Group	Feature	Description
TRACES Server	TRACES Server	Basic functionality. **NOTE:** In remote collector systems, both TRACES Server license and the Collector license require this feature.
	License for <N> clients	Limit of web client accounts. Simultaneous logons from multiple computers are not allowed.
UMR Collector	UMR	Enables UMR data collection and visualization on a map.
	License for <N> BTS sites	Limit of supported Dimetra BTS sites. Unlimited option available.
DMR Collector	DMR	Enables DMR data collection and visualization on a map.
RF Survey Data	RF Survey Data	Enables drive-test data import and visualization on a map. **NOTE:** Motorola Scout is the only RF survey tool currently supported.
External API	External API	Provides access to collected data for third-party applications as a REST service.

Table 9: TRACES 2.2 to 2.5 Licensed Features

Group	Feature	Description
TRACES Server	TRACES Server	Basic server functionality.
Traces Web Apps	Traces Web Apps	Basic web functionality.
	DMR	Enables DMR data visualization on a map.
	SCOUT	Enables Motorola Scout RF survey data visualization.
	UMR	Enables UMR data visualization on a map.

Group	Feature	Description
	AIRS	Enables the visualization of data in ASTRO systems.
	License for <N> clients	Limit of web client accounts (1–127).
UMR Collector	UMR Collector	Enables UMR data collection.
	TMV Processing	Enables collection of UMR data in TMV format.
	UMR Service Enabler	Enables UMR data collection.
	License for <N> BTS sites	Limit of supported Dimetra BTS sites.
External API	External API	Provides access to collected data for third-party applications as a REST service.
AIRS Collector	AIRS Collector	Enables the collection of data in ASTRO systems.

Table 10: License Conversion Guide for Pre-2.6 Licenses

TRACES 2.2 – 2.5 features		Feature replacements in TRACES 2.6	
Group	**Feature**	**Group**	**Feature**
TRACES Server	TRACES Server	TRACES Server	TRACES Server
Traces Web Apps	Traces Web Apps	TRACES Server	TRACES Server
Traces Web Apps	DMR	DMR Collector	DMR
Traces Web Apps	SCOUT	RF Survey Data	RF Survey Data
Traces Web Apps	UMR	UMR Collector	UMR
Traces Web Apps	AIRS	n/a	No longer available
Traces Web Apps	License for <N>N clients	TRACES Server	License for <N> clients
UMR Collector	UMR Collector	UMR Collector	UMR
UMR Collector	TMV Processing	UMR Collector	UMR
UMR Collector	UMR Service Enabler	UMR Collector	UMR
UMR Collector	License for <N> BTS sites	UMR Collector	License for <N> BTS sites
External API	External API	External API	External API
AIRS Collector	AIRS Collector	n/a	No longer available