Oracle® Adaptive Access Manager
IP Location Data Import Guide
10*g* (10.1.4.3.0)

December 2007

Oracle Adaptive Access Manager IP Location Data Import Guide, 10g (10.1.4.3.0)

Contents

About This Document

This document describes a utility for importing the IP location data into the Oracle Adaptive Access Manager database. This data is used by the risk policies framework to determine the risk of fraud associated with a given IP address.

This document is divided into three major sections. The first section, “How to run the load utility,” documents the details necessary to run the import utility. System Behavior defines the expected inputs and outputs of the system. Design Specification gives a technical description of how the utility works behind the scenes.

How to Run the Load Utility

Setting Up IP Location Loader Properties

1. Rename bharosa_location.properties.sample to bharosa_location.properties.
2. Update bharosa_location.properties file to set appropriate values for the following properties.

Please note that the properties marked as “Advanced” are not to be changed in general.

IP Loader Properties	Description
location.data.provider	quova or ip2location or maxmind
location.data.file	only if quova location data is to be loaded; else leave this property unset/blank
location.data.ref.file	only if quova location data is to be loaded; else leave this property unset/blank
location.data.anonymizer.file	only if anonymizer data is to be loaded; else leave this property unset/blank
location.data.location.file	only if maxmind location data is to be loaded; else leave this property unset/blank
location.data.blocks.file	only if maxmind location data is to be loaded; else leave this property unset/blank
location.data.country.code.file	only if maxmind location data is to be loaded; else leave this property unset/blank
location.data.sub.country.code.file	only if maxmind location data is to be loaded; else leave this property unset/blank
location.loader.database.pool.size	number of threads to use to update the database
location.loader.dbqueue.maxsize	Advanced: maximum number of location records to be kept in queue for database threads
location.loader.cache.location.maxcount	Advanced: maximum number of location records to be kept in cache, while updating existing location data
location.loader.cache.split.maxcount	Advanced: maximum number of location split records to be kept in cache, while updating existing location data

IP Loader Properties	Description
location.loader.cache.anonymizer.maxcount	Advanced: maximum number of anonymizer records to be kept in cache, while updating existing location data
location.loader.database.commit.batch.size	Maximum number of location records to batch before issuing a database commit
location.loader.database.commit.batch.seconds	Maximum time to hold an uncommitted batch
location.loader.cache.isp.maxcount	Maximum number of ISP records to be kept in cache

Setting Up Database Properties - TopLink

Follow the instructions in this section when using TopLink.

Database Configuration Fields

Update conf/sessions.xml file to set the following database configuration fields.

Configuration Fields	Description
<platform-class>	TopLink database platform class
<driver-class>	The name of the JDBC Driver class
<connection-url>	The database URL
<user-name>	The database username
<password>	The password should be TopLink encrypted password
<max-connections>, <min-connections> in <write-connection-pool>	The <max-connections>, <min-connections> in <write-connection-pool>must be set to at least 1 higher than the value of property "location.loader.database.pool.size" (in bharosa_location.properties)

Encrypt Password Command

To encrypt a given password, use the following command:

```
java –classpath “vcrypt.jar;toplink.jar”
com.bharosa.vcrypt.utility.cmdline.BharosaCmdLine -toplink-password-
encrypt mydbpassword
```

Setting Up Log Properties

Update conf/log4j.xml file to set the log file name

Setting Up for SQL Server Database

To load data to Microsoft SQL Server database, sqljdbc.jar should be copied to a third party directory. This file can be downloaded for free from Microsoft at http://www.microsoft.com/downloads/details.aspx?FamilyID=6d483869-816a-44cb-9787-a866235efc7c&DisplayLang=en.

Setting Up for Loading MaxMind IP data

Before running the IP location loader, Blocks.csv file from MaxMind needs to be preprocessed with the following commands:

```
$ mv Blocks.csv Blocks-original.csv
$ sed -e 's/\"//g' Blocks-original.csv | sort -n -t, -k1,1 -o Blocks.csv
```

Loading Location and/or Anonymizer Data

Note: a single script is provided to load location data from any provider (Quova, IP2Location, MaxMind). The earlier versions separate scripts were used for each provider.

After completing the setup detailed above, run the following command to load the location and/or anonymizer data into the Oracle Adaptive Access Manager database.

From bash shell, execute `loadIPLocationData.sh`

From Windows command prompt, execute `loadIPLocationData.cmd`

System Behavior

The IP location loader utility reads the information from the IP location data files (from Quova or IP2Location) to populate the IP location tables in the Oracle Adaptive Access Manager system. The first time the utility is run against a new database, it will insert a new row into the vcrypt_ip_location_map for each record in the data file. It will also create a new record in vcrypt_country for each unique country name in the data file, a new record in vcrypt_state for each unique combination of country name and state name in the data file, and a new record in vcrypt_city for each unique combination of country name, state name, and city name in the data file.

When the IP location loader utility is run with a new data file against an already populated database, it will skip records in the datafile who have matching, identical records in the vcrypt_ip_location_map table. It will create a new row in the vcrypt_ip_location_map for each record in the data file whose FROM_IP_ADDR does not already appear in the database. It will update the rows in the vcrypt_ip_location_map whose FROM_IP_ADDR matches the record in the data file, but has different data in other columns. The utility will also create new countries, states, and cities that do not already exist in the database.

Quova File Layout

The Quova data file is a pipe-delimited ('|') file, with 29 fields on each line, and one record per line. The information in these tables comes from Quova's GeoPoint Data Glossary. In the following table, IP represents the vcrypt_ip_location_map table, CO represents the vcrypt_country table, ST represents the vcrypt_state table, and CI represents the vcrypt_city table.

The file layout is as follows:

Quova Field	OAAM Field	Description
Start IP	IP.from_ip_addr	The beginning of the IP range, also used as an alternate primary key on the vcrypt_ip_location_map table.
End IP	IP.to_ip_addr	The end of the IP range.
CIDR	*(not used)*	
Continent	*(not used)*	
Country	CO.country_name	The country name.
Country ISO2	*(not used)*	
Region	*(not used)*	
State	ST.state_name	The state name.
City	CI.city_name	The city name.
Postal code	*(not used)*	
Time zone	*(not used)*	
Latitude	CI.latitude	The latitude of the IP address. Positive numbers represent North, and negative numbers represent South.
Longitude	CI.longitude	The latitude of the IP address. Positive numbers represent East, and negative numbers represent West.
Phone number prefix	*(not used)*	
AOL Flag	mapped to IP.isp_id	Tells whether or not the IP address is an AOL IP address.
DMA	*(not used)*	
MSA	*(not used)*	
PMSA	*(not used)*	
Country CF	IP.country_cf	The confidence factor (1-99) that the correct country has been identified.
State CF	IP.state_cf	The confidence factor (1-99) that the correct state has been identified.
City CF	IP.city_cf	The confidence factor (1-99) that the correct city has been identified.
Connection type	mapped to IP.connection_type	Describes the data connection between the device or LAN and the internet. See the Connection Type

Quova Field	OAAM Field	Description
		mapping, below.
IP routing type	mapped to IP.routing_type	Tells how the user is routed to the internet. See the IP Routing Type mapping, below.
Line speed	mapped to IP.connection_speed	Describes the connection speed. This is dependent upon connection type. See the Connection Speed mapping, below.
ASN	IP.asn	Globally unique number assigned to a network or group of networks that is managed by a single entity.
Carrier	IP.carrier	The name of the entity that manages the ASN entry.
Second Level Domain	mapped to IP.sec_level_domain	The second level domain of the URL, e.g. Oracle in www.oracle.com. This is mapped through the Quova reference file.
Top Level Domain	mapped to IP.top_level_domain	The top level domain of the URL, e.g. com in www.oracle.com. This is mapped through the Quova reference file.
Registering Organization	*(not used)*	

Routing Types Mapping

Routing Type	OAAM ID	Description
fixed	1	User IP is at the same location as the user.
anonymizer	2	User IP is located within a network block that has tested positive for anonymizer activity.
aol	3	User is a member of the AOL service; The user country can be identified in most cases; any regional info more granular than country is not possible.
aol pop	4	
aol dialup	5	
aol proxy	6	
pop	7	User is dialing into a regional ISP and is likely to be near the IP location; the user could be dialing across geographical boundaries.
superpop	8	User is dialing into a multi-state or multi-national ISP and is not likely to be near the IP location; the user could be dialing across geographical boundaries.
satellite	9	A user connecting to the Internet through a consumer satellite or a user connecting to the Internet with a backbone satellite provider where no information about the terrestrial connection is available.
cache proxy	10	User is proxied through either an internet accelerator or content distribution service.

Routing Type	OAAM ID	Description
international proxy	11	A proxy that contains traffic from multiple countries.
regional proxy	12	A proxy (not anonymizer) that contains traffic from multiple states within a single country.
mobile gateway	13	A gateway to connect mobile devices to the public internet. For example, WAP is a gateway used by mobile phone providers.
none	14	Routing method is not known or is not identifiable in the above descriptions.
unknown	99	

Connection Types Mapping

Connection Type	OAAM ID	Description
ocx	1	This represents OC-3 circuits, OC-48 circuits, etc. which are used primarily by large backbone carriers.
tx	2	This includes T-3 circuits and T-1 circuits still used by many small and medium companies.
satellite	3	This represents high-speed or broadband links between a consumer and a geosynchronous or lowearth orbiting satellite.
framerelay	4	Frame relay circuits may range from low to highspeed and are used as a backup or alternative to T-1. Most often they are high-speed links, so GeoPoint classifieds them as such.
dsl	5	Digital Subscriber Line broadband circuits, which include aDSL, iDSL, sDSL, etc. In general ranges in speed from 256k to 20MB per second.
cable	6	Cable Modem broadband circuits, offered by cable TV companies. Speeds range from 128k to 36MB per second, and vary with the load placed on a given cable modem switch.
isdn	7	Integrated Services Digital Network high-speed copper-wire technology, support 128K per second speed, with ISDN modems and switches offering 1MB per second and greater speed. Offered by some major telcos.
dialup	8	This category represents the consumer dialup modem space, which operates at 56k per second. Providers include Earthlink, AOL and Netzero.
fixed wireless	9	Represents fixed wireless connections where the location of the receiver is fixed. Category includes WDSL providers such as Sprint Broadband Direct, as well as emerging WiMax providers.
mobile wireless	10	Represents cellular network providers such as Cingular, Sprint and Verizon Wireless who employ CDMA,

Connection Type	OAAM ID	Description
		EDGE, EV-DO technologies. Speeds vary from 19.2k per second to 3MB per second.
consumer satellite	11	
unknown high	12	GeoPoint was unable to obtain any connection type or the connection type is not identifiable in the above descriptions.
unknown medium	13	
unknown low	14	
unknown	99	

Connection Speed Mapping

Connection Speed	OAAM ID	Description
high	1	OCX, TX, and Framerelay.
medium	2	Satellite, DSL, Cable, Fixed Wireless, and ISDN.
low	3	Dialup and Mobile Wireless.
unknown	99	Quova was unable to obtain any line speed information.

OAAM Tables

This section contains the tables used by the ETL process

Anonymizer

The following tables and sequences are used for uploading the Anonymizer data. Please make sure the ETL process has sufficient privileges to read and update these tables.

Name	Table/Sequence
V_LONG_VALUE_ELEM_SEQ	Sequence
VCRYPT_LONG_VALUE_ELEMENT	Table
VCRYPT_VALUE_LIST	Table
V_VALUE_LIST_SEQ	Sequence
VCRYPT_CACHE_STATUS	Table
VCRYPT_CACHE_STATUS_SEQ	Sequence

Tables in Location Loading

The IP location loader requires read/write access to the following tables:

- VCRYPT_IP_LOCATION_MAP
- V_IP_LOCATION_MAP_SEQ
- V_IP_LOC_MAP_HIST
- V_IP_LOC_MAP_HIST_SEQ
- V_IP_LOC_MAP_SPLIT
- V_IP_LOC_MAP_SPLIT_SEQ
- V_IP_LOC_MAP_SPLIT_HIST
- V_IP_LOC_MAP_SPLIT_HIST_SEQ
- VCRYPT_COUNTRY
- V_COUNTRY_SEQ
- V_COUNTRY_HIST
- V_COUNTRY_HIST_SEQ
- VCRYPT_STATE
- V_STATE_SEQ
- V_STATE_HIST
- V_STATE_HIST_SEQ
- VCRYPT_CITY
- V_CITY_SEQ
- V_CITY_HIST
- V_CITY_HIST_SEQ
- VCRYPT_ISP
- VCRYPT_ISP_SEQ
- V_ISP_HIST
- V_ISP_HIST_SEQ
- V_LOC_LOOKUP
- V_LOC_LOOKUP_SEQ
- V_LOC_UPD_SESS
- V_LOC_UPD_SESS_SEQ
- V_UPD_LOGS
- V_UPD_LOGS_SEQ
- VCRYPT_LONG_VALUE_ELEMENT
- V_LONG_VALUE_ELEM_SEQ
- VCRYPT_VALUE_LIST

- V_VALUE_LIST_SEQ
- VCRYPT_VALUE_LIST_HIST
- V_VALUE_LIST_HIST_SEQ
- VCRYPT_CACHE_STATUS
- VCRYPT_CACHE_STATUS_SEQ

Troubleshooting

Characters Added During Transfer of Files

During the transfer/ftp of files, characters such as carriage return “\r” are added. To resolve the issue, run dos2unix against the files. When you are running the .sh file, use either dos2unix <filename> or dos2unix . *.* .

“TNS:no appropriate service handler found” error

If you get the following error

```
TNS:no appropriate service handler found
```

it may be that the number of processes in your database is set to a minimal value.

Use the following commands to check the number of process set in the database

```
SQL> show parameter process
SQL> alter system set processes=100 scope=spfile;
```

bharosa_location.properties.sample File

```
### IP location loader specific properties go here

### Specify the data provider: quova or ip2location or maxmind
location.data.provider=quova

### Specify the data file, for both quoval and ip2location
location.data.file=test_08132006.dat.gz

### Specify the reference file for quova
location.data.ref.file=test_08132006.ref.gz

### Specify the anonymizer data file for quova
location.data.anonymizer.file=test_anonymizer.dat.gz

### Specify the location data file, for maxmind
location.data.location.file=test_MaxMindLocation.csv

### Specify the blocks data file, for maxmind
location.data.blocks.file=test_MaxMindBlocks.csv

### Specify the country code data file, for maxmind
location.data.country.code.file=ISO_3166_CountryCode.csv

### Specify the sub country code data file, for maxmind
location.data.sub.country.code.file=FIPS_10_4_SubCountryCode.csv

### Specify the number of database threads
location.loader.database.pool.size=2

### Specify the maximum number of location records to batch before
issuing a database commit
location.loader.database.commit.batch.size=2500

### Specify the maximum time to hold an uncommitted batch
location.loader.database.commit.batch.seconds=30
```

```
### Specify the maximum number of location records to be kept in
queue for database threads

location.loader.dbqueue.maxsize=100000


### Specify the maximum number of location records to be kept in
cache

location.loader.cache.location.maxcount=25000


### Specify the maximum number of location split records to be kept
in cache

location.loader.cache.split.maxcount=25000


### Specify the maximum number of anonymizer records to be kept in
cache

location.loader.cache.anonymizer.maxcount=25000


### Specify the maximum number of ISP records to be kept in cache

location.loader.cache.isp.maxcount=25000
```