

FactotumNOW IAS Reporting

Manual

Version 3.41

©2006 Neu Telekommunikationstechnik, André Neu

Country	Input Bytes in MB	Output Bytes in MB	Sessions from in Minutes
Canada	15306	8371	11562
United States	13111	3776	1992
Japan	289	2307	291
United Kingdom	272	703	85
Belgium	148	936	41
Canada	62	596	30
France	60	1073	30
Netherlands	14	88	25
Germany	12	45	22
France	29	519	13
Italy	8	64	6
Hong Kong	11	36	5
Italy	8	45	5
Germany	11	50	4
Korea Republic of	6	48	2
Australia	5	64	1
Macau	2	22	1

End User License Agreement (EULA)

NEU TELEKOMMUNIKATIONSTECHNIK Company (NEU TELEKOMMUNIKATIONSTECHNIK) hereby gives you a non-exclusive license to use the software FactotumNOW IAS Reporting (the Software).

For evaluation, the license is granted, and is time-limited.

To obtain a fully functional and not time-limited release, you have to pay a license fee by following instructions prompted by the program.

You may:

- use the Software on any single computer;
- use the Software on a second computer so long as the primary user of each copy is the same person and more than one copy is not simultaneously used;
- copy the Software for archival purposes, provided any copy contains all of the original Software's proprietary notices.

You may not:

- permit other individuals to use the Software except under the terms listed above;
- modify, translate, reverse engineer, decompile, disassemble (except to the extent applicable laws specifically prohibit such restriction),
- create derivative works based on the Software;
- copy the Software (except as specified above);
- rent, lease, transfer or otherwise transfer rights to the Software;
- remove any proprietary notices or labels on the Software.

TERMINATION.

The license will terminate automatically if you fail to comply with the limitations described above. On termination, you must destroy all copies of the Software and Documentation.

Disclaimer of Warranty

The Software is provided on an AS IS basis, without warranty of any kind, including without limitation the warranties of merchantability, fitness for a particular purpose and non-infringement.

The entire risk as to the quality and performance of the Software is borne by you.

Should the Software prove defective, you and not NEU TELEKOMMUNIKATIONSTECHNIK assume the entire cost of any service and repair.

NEU TELEKOMMUNIKATIONSTECHNIK IS NOT RESPONSIBLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES.

Title, ownership rights and intellectual property rights in and to the Software shall remain in NEU TELEKOMMUNIKATIONSTECHNIK. The Software is protected by international copyright treaties.

Trademark Notices

Intel® and Itanium® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

® Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Linux® is a U.S. registered trademark of Linus Torvalds.

MS-DOS®, Microsoft®, and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SuSE® is a registered trademark of SuSE Linux AG.

GFI Network Server Monitor is copyright of GFI SOFTWARE Ltd. 2000-2005 GFI SOFTWARE Ltd.

GFI Network Security Scanner is copyright of GFI SOFTWARE Ltd. 2000-2005 GFI SOFTWARE Ltd.

LANguard is copyright of GFI SOFTWARE Ltd. 2000-2005 GFI SOFTWARE Ltd.

Microsoft, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

This product includes GeoLite data created by MaxMind, available from <http://www.maxmind.com/>.

Table of Contents

End User License Agreement (EULA).....	2
Disclaimer of Warranty	2
Trademark Notices.....	3
I Introduction.....	5
II Installation.....	6
III IAS Reports.....	8
i Import the GEO Lite Country Database.....	8
ii Generate reports.....	9

I Introduction

A brief summary of the functions this software covers:

- IAS Log import
 - Native IAS format
 - IAS database format
 - Automated from several IAS servers into a single PostgreSQL database
- IAS Log analysis:
 - Resolution of inbound VPN IP addresses to countries
 - Determination of accounts that have been accessed from the same source IP within a single day
 - Display of rejected VPN login attempts
 - By user
 - By server
 - By day
 - By IP
 - Display of traffic and session durations by user account
 - Display of transfer volume by country
 - Display of currently connected users
- This product includes GeoLite data created by MaxMind®, available from <http://www.maxmind.com/>

II Installation

Installation is quite simple, depending on your experience, you should be able to run through it within only a few minutes although there are several steps involved:

1. Enable logging on your IAS/RAS/VPN server. To do this, follow these steps:
 1. This task is actually more work than the VPN setup itself. You do this from within the "Routing and Remote Access" console (Start - Programs- Administrative Tools - Routing and Remote Access) in the branch "Remote Access Logging". By default, it will say "Local File". That is rather misleading since logging is not enabled by default, it is just "ready". To enable logging, double-click on "Local File" and check the top two boxes ("Log accounting requests" and "Log authentication requests"). The periodic status should not be necessary.
 2. Now, with this in place, you will be collecting a log file called "IASLOG.LOG" into the directory "c:\windows\system32\logfiles" (for XP/2003) and "c:\winnt\system32\logfiles" (for 2000). Verify that you are collecting such a file before you continue because you need the log file before you can run reports.
2. For the first installation of **FactotumNOW IAS Reporting** on your network:
 3. Install the product onto your IAS server.
 4. The first installation should take place onto the IAS server that will also be running your PostgreSQL reporting database.
 5. After installation, open the configuration tool from the desktop link: "FactotumNOW Configure IAS Import Engine".
 6. You should leave all settings on the first tab page ("General") at their defaults except for the database password. As a password, you should assign something other than the default ("postgres") is the default password. The username should remain "postgres".
 7. Change to the "Log Sources" tab.
 8. This will determine you do not yet have PostgreSQL on that system and offer you to install it.
 9. Pick a directory (best is to create a new one) for the PostgreSQL database files. Make sure it is on a drive that has sufficient space to hold your log data.
 10. Let the PostgreSQL installation run through. The configuration tool will also create the database structure and tables for you.
 11. Once this is all done, change to the "Log Sources" tab. In the "Log Sources" tab, click on "Browse" to browse to the directory where your IASLOG.LOG is (normally this is "c:\windows\system32\logfiles" for Windows 2003/XP and "c:\winnt\system32\logfiles" for Windows 2000). Click on "Add".
 12. Click on "OK".
 13. Let the configuration tool start the import service for you.

14. For every other installation of **FactotumNOW IAS Reporting** on your network:
 15. Install the product onto your IAS servers.
 16. After installation, open the configuration tool from the desktop link: “FactotumNOW Configure IAS Import Engine”.
 17. As a “Database Server Name” specify the name of the system you performed the first installation on. Also, modify the “Database Password” to reflect the password you initially assigned. The username should remain “postgres”.
 18. Change to the “Log Sources” tab from the “General” tab.
 19. This will connect your installation to the PostgreSQL server you installed on the first system.
 20. In the “Log Sources” tab, click on “Browse” to browse to the directory where your IASLOG.LOG is (normally this is “c:\windows\system32\logfiles” for Windows 2003/XP and “c:\winnt\system32\logfiles” for Windows 2000). Click on “Add”.
 21. Click on “OK”.
 22. Let the configuration tool start the import service for you.
23. You can now launch the reporting by clicking on “**FactotumNOW IAS Reporting**” on your desktop.

III Generate IAS Reports

i Import the GEO Lite Country Database

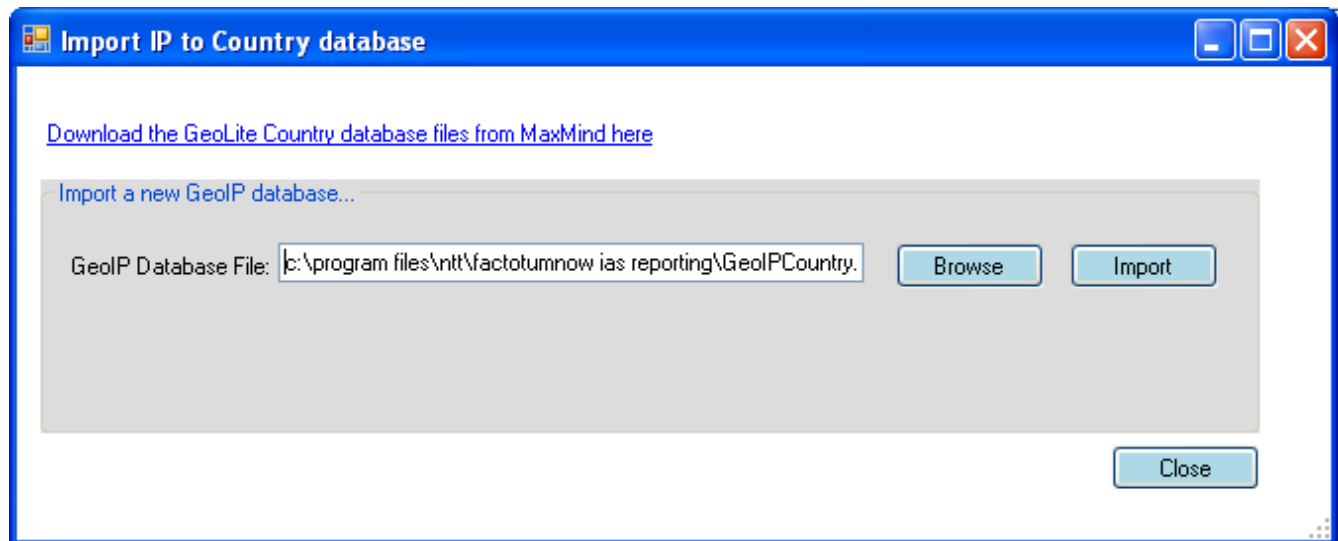
Before you run your IAS reports, we recommend you import the GEO Lite Country database into the repository. A copy of the database is included in your installation files and is placed into the program directory during installation (normally, this is: “<c:\program files\ntt\factotumnow ias reporting>”). You can also download the newest version of the database from this page:

http://www.maxmind.com/app/geoip_country

Currently, the actual database itself is available under this link:

<http://www.maxmind.com/download/geoip/database/GeoIPCountryCSV.zip>

If you have to select the file manually, make sure you download the CSV format. Download the file to your computer and extract the CSV file contained in the ZIP archive. Then, in **FactotumNOW IAS Reporting**, in the main window click on “Import IP to Country database”. This will display a dialog like below:

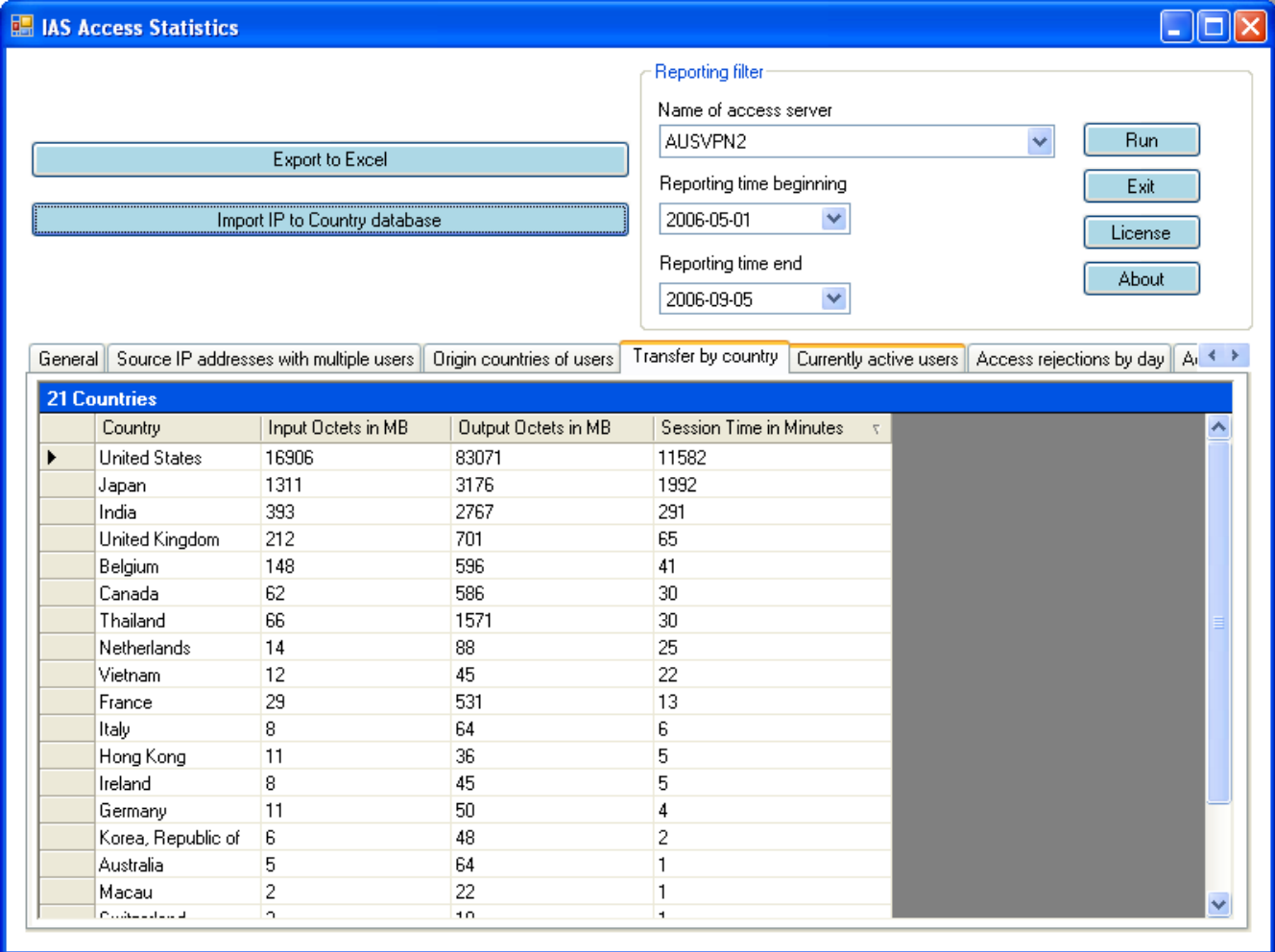


Click on “Browse” to point the program to the location of the file “GeoIPCountry.CSV”, then click on “Import”. You only need to do this once, even when you are importing from several IAS servers. The actual import may take a few minutes since this is a fairly large database. When the import is complete, click on “Close” to return the main window.

ii Generate reports

To generate a report, you will need to supply the following information:

- “Name of access server”: Pick the name of the IAS access server from the dropdown field. The dropdown will display all servers that you have imported data for. You can also view the combined data from all IAS servers by choosing “All”.
- “Reporting time beginning” and “Reporting time end“: Specify the time window that this report should be based on. Keep in mind that you can not report on stats that have not been imported into the database, so you can only go back as far as your IAS logfiles reached.
- Click on “Run” when you have made your choices. Report generation for a site that has a large amount of traffic can take a few minutes depending on the choices you have made.
- After you have completed the report, you will see a screen like the below:



The screenshot shows the 'IAS Access Statistics' application window. It features a 'Reporting filter' section with the following controls:

- Name of access server: AUSVPN2
- Reporting time beginning: 2006-05-01
- Reporting time end: 2006-09-05
- Buttons: Run, Exit, License, About

Below the filter are two buttons: 'Export to Excel' and 'Import IP to Country database'. At the bottom, there are several tabs: 'General', 'Source IP addresses with multiple users', 'Origin countries of users', 'Transfer by country', 'Currently active users', and 'Access rejections by day'. The 'Transfer by country' tab is selected, displaying a table with 21 countries.

Country	Input Octets in MB	Output Octets in MB	Session Time in Minutes
United States	16906	83071	11582
Japan	1311	3176	1992
India	393	2767	291
United Kingdom	212	701	65
Belgium	148	596	41
Canada	62	586	30
Thailand	66	1571	30
Netherlands	14	88	25
Vietnam	12	45	22
France	29	531	13
Italy	8	64	6
Hong Kong	11	36	5
Ireland	8	45	5
Germany	11	50	4
Korea, Republic of	6	48	2
Australia	5	64	1
Macau	2	22	1
Switzerland	2	10	1

The different tabs of the report detail the following information:

- “General”: Total amount of traffic inbound and outbound and total session durations by user accounts.
- “Source IP addresses with multiple users”: If during a single day, the same IP address has logged on to different user accounts, it will be displayed here. This can have a legitimate reason when two users are traveling together and are staying in the same hotel.
- “Origin countries of users”: For every user account, you will see the countries the account has had logins from. If you have a user that travels, you will see a long list of countries.
- “Transfers by country”: If you have users in many countries, you may want to know how much data they are generating. This can be important when making a decision about building a separate infrastructure for them.
- “Currently active users”: This lists the user accounts that are currently logged in according to the logfiles. This may be inaccurate if one of the IAS servers has crashed and corrupted the logfiles.
- “Access rejections by day”: This tab will allow you to identify a high and unusual volume of access rejections.
- “Access rejections by user”: This tab displays the user accounts that have had access rejections. Either somebody is trying to guess their credentials or they are having trouble logging in.
- “Access rejections by server”: If you have decided to report on all servers in a consolidated view, you can see a breakup of access rejections per server.
- “Access rejections by IP”: This tab will allow you to identify the sources of unsuccessful login attempts.

You can run a new report by changing your settings and clicking on “Run” again.

IV Troubleshooting

Should you encounter problems while operating this software, please do not hesitate to contact us either through the support forums on our web site (<http://www.factotumnow.com>) or via email support@factotumnow.com.