

# TECHNICAL NOTE

## CHANGING THE GEOGRAPHIC VIEW

OCTOBER 2009

This technical note provides information on changing Geographic Views to display network traffic grouped by country. Geographic information is displayed on various STRM interfaces, including Network Surveillance, Offenses, Events, and Flows.

On the STRM Network Surveillance interface, for example, you can pivot the data to view traffic from a different perspective. One of the views is Geographic Views, which displays traffic by geographic regions.

By default, the Geographic View displays network traffic grouped by continent. You can change the geographic view default to display network traffic grouped by country.



**Caution:** *An environment with high flow volume and many network objects has a high demand on processing and storage on the Flow Processor and Console. If you are experiencing high flow volumes, changing the Geographic View to display network traffic grouped by country will further increase the load and may cause flows to drop. To save on processing power, you can set the Geographic View to Virtual using the Admin interface. For more information about virtual views, see the Managing Views chapter of the STRM Administration Guide. For advice on determining whether your system can accommodate the extra load, please contact Customer Support.*

---

### Changing Geographic Views

To change the Geographic View to display network traffic by country:

- Step 1** Log in to STRM as root.
- Step 2** Change the geographic reference in each of the following directories:
  - `/store/configservices/staging/globalconfig`
  - `/store/configservices/deployed/globalconfig`
  - `/opt/qradar/conf`

To change the geographic reference:

- a Access the directory.

b Enter the following command:

```
ln -fs geographic.classify.country.conf geographic.classify.conf
```

```
ln -fs geographic.country.conf geographic.conf
```

c Repeat **a** and **b** for all directories.

**Step 3** Repeat this procedure on the following systems:

- Consoles (STRM 2500 and STRM 5000)
- STRM 2500 FP and STRM 2500 EP/FP combo
- Software installations on any system running a Classification Engine



**Warning:** *If you do not repeat this procedure on all systems listed above, improperly categorized flows will not appear in the Geographic View and some sentries will cease to function. For example, if your Console displays Geographic Views by continent and your STRM 2500 FP appliance references Geographic View by city, the Console will not display the flow in the Geographic View.*

**Step 4** Deploy the changes.

a Access the STRM user interface.

b Click the **Admin** tab.

The Admin interface appears.

c Click **Deploy Changes**.

**Step 5** After the deploy has finished, enter the following command:

```
service tomcat restart
```

Now your Geographic View in the Network Surveillance tab displays network traffic by country.

**Copyright Notice**

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Published: 2009-10-12

