Savvius Insight Tech Notes

Replacing the dashboards and indexes on Insight

Here are the instructions for replacing the dashboards and indexes on Insight (make sure to obtain the most current index.json and dashboards.json files by submitting a request at the Savvius Insight Portal):

1. From the Kibana UI, go to Settings > Objects, and delete the Searches, Visualizations, and Dashboards. Be sure to delete them all, since the select all and delete only deletes a page at a time.
2. Get the index.json and dashboards.json files on the Insight Support Portal under the Downloads link.
3. Copy the index.json and dashboards.json files to /usr/share/savvius/elk/data.
4. Run: python /usr/share /savvius/elk/init.py.
5. From the Kibana UI, go to Settings > Objects, and validate that the new dashboards are there.

ELK: Event map and charts did not populate for VoIP flows

This can happen even if the data is present in ElasticSearch. For a capture to generate events, the Expert must be enabled on that capture. The reason there are no VoIP Flow Events in the ELK dashboards is because VoIP analysis is enabled on a separate capture with Expert disabled. We separate VoIP into its own capture to increase performance in the case where the data rate is high. However, in the case where the data rate is not too high to require this level of separation of analysis into different captures, the separate VoIP capture can be deleted, and instead VoIP analysis can be enabled on the Expert capture. Having VoIP enabled on the Expert capture will cause VoIP Events to be generated and sent to ELK.

VoIP: None of the Quality Scores in the Calls and Media view match Omnipeek

In Omnipeek, the MOS and R Factor scores are calculated on an ongoing basis, as new packets are added to the media flows. So, the scores are always based on all the packets in the media flow. With ELK, the R Factor and MOS scores are recorded for each media flow every one minute. The R Factor and MOS scores displayed in the Kibana VoIP Media dashboard are the average of all the one-minute scores, for whatever time period is selected for display.

VoIP: Filtering by End-Cause type displays only the final interval of the call

This is because the “End Cause Types” graph can only track the last interval in the call, which is where the End Cause is recorded. Below are workflows which will allow you to see the entire call:

To find calls that have a particular End Cause, do the following:

1. Click on the Calls dashboard
2. In the legend of the End Cause Types graph, click on the End Cause type that you are interested in (i.e. “Temporarily Not Available”), then click on the magnifying glass with the “plus” in it, to create a filter with this End Cause.
3. With the End Cause filter in place, the Calls dashboard will display only the calls with the filtered End Cause. However, the because the “End Cause Types” graph can only track the last interval of the call (which is where the End Cause is recorded), the Calls dashboard will now only display the last interval of each of the calls with this filtered End Cause.

If you want to see statistics for the full duration of the call, do the following:

1. Click on one of the calls in the Call List, which will create a filter for the call.
2. Scroll up to the top of the dashboard, so that you can see the applied filters.
3. Leave the CallNumber filter in place, but delete the EndCause filter (place the cursor over the EndCause filter and click on the trash can).
4. The dashboard will then display all the statistics for the full duration of the filtered call..

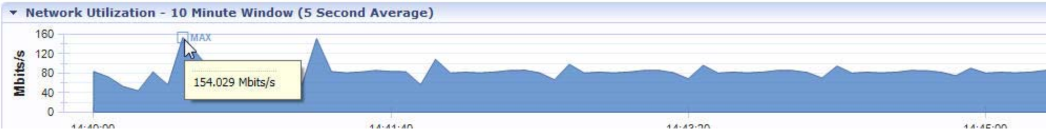
DHCP Warning

Savvius Insight can be configured to obtain an IP address automatically from a DHCP server; however, we strongly recommend the use of a static IP address for Savvius Insight. If DHCP is used, and if the address should change on a new DHCP lease, then the user must look up the new IP address assigned to Savvius Insight from the DHCP server. To help you look up the IP address, the Mac Address of Savvius Insight is displayed if you select DHCP.

Note If DHCP is selected, you will have approximately two minutes to connect Savvius Insight to your network in order for the DHCP server to assign an IP address. Please make sure Savvius Insight is connected to your network within the two minute time period from the time you click **Apply**.

Define an NTP server

If the date and time are not correct on the Savvius Insight unit, the unit will not show up as a source in the Kibana dashboards, and data will not be received. Make sure you have an NTP server defined in the Savvius Insight unit that is on the same network as the Savvius Insight hardware.



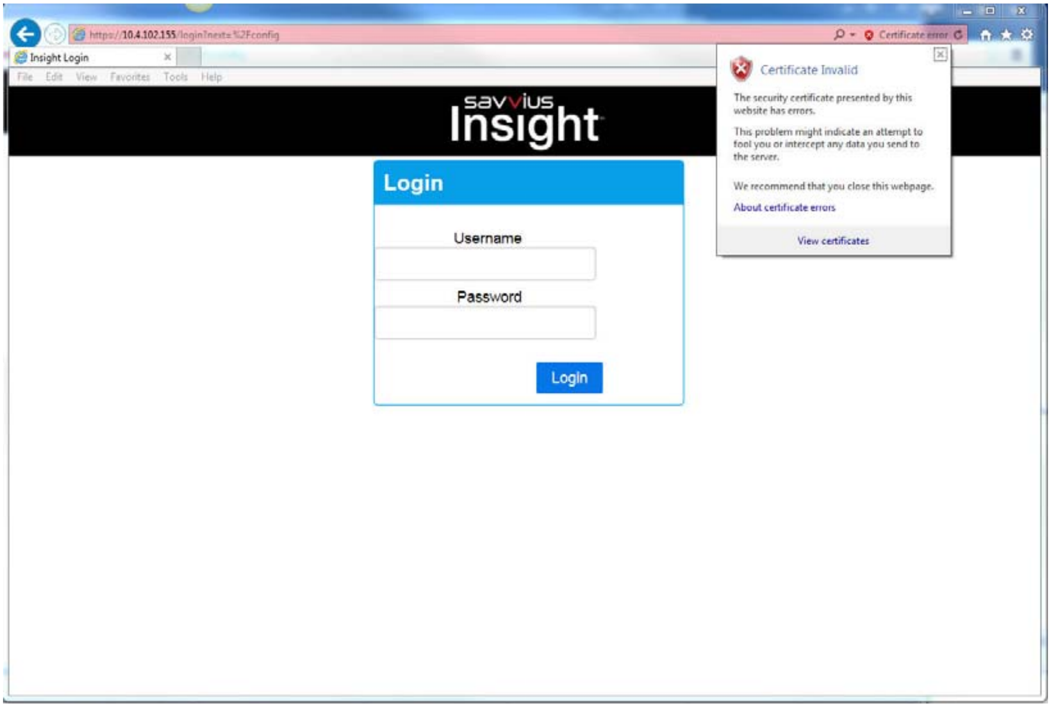
Enable web browser support for TLS 1.1

In order to use your web browser to configure your Savvius Insight, the browser must have support for TLS 1.1 or later enabled. This must be enabled for I.E. versions less than 11, FireFox less than 27, Chrome less than 22 and Safari OS X 10.9. For I.E., go to Options → Advanced, scroll down to the security section and enable the "Use TLS 1.1" option.

Certificate Error

When connecting to the home page of your Savvius Insight unit, you may encounter a certificate error as shown below. This happens because the Insight certificate is self-signed. Please just continue to the home page.

Internet Explorer:

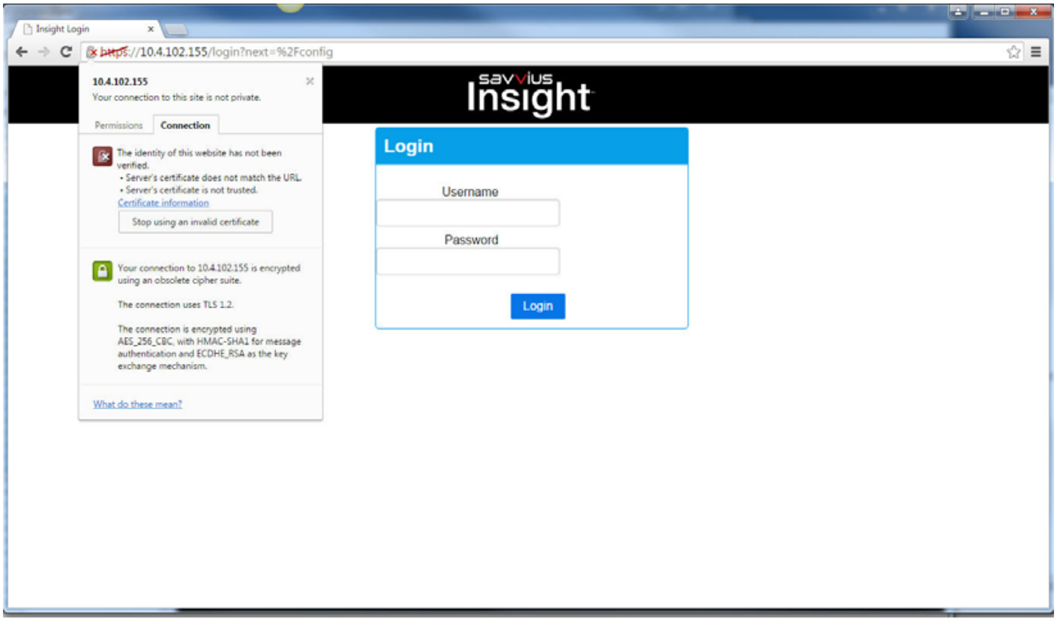


The security certificate presented by this website has errors.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

Chrome:



10.4.102.155

Your connection to this site is not private.

The identity of this website has not been verified.

- Server's certificate does not match the URL.
- Server's certificate is not trusted.

Certificate information

Stop using an invalid certificate

Your connection to 10.4.102.155 is encrypted using an obsolete cipher suite.

The connection uses TLS 1.2.

The connection is encrypted using AES_256_CBC, with HMAC-SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism.

What do these mean?

False spikes may be seen in very high traffic situations

False spikes may be seen in very high traffic situations. This can be caused when the system gets overloaded, and the timestamps on the packets are later than they actually arrived, creating false spikes in the network utilization graph.

Slow response when using current version of FireFox (47.01) to browse to Insight MGMT IP address

Other browsers (Chrome, IE) seem to work fine.

Insight/Kibana reports a Max Utilization of 157Mbps on a 100Mbps network

This happens when there is so much processing taking place that packets left in the buffer not previously processed show up in the next graph interval creating the >100Mb value.

Latest version of Firefox gets Unresponsive script error when viewing last hour or more on Insight

The solution is to click the Continue button and also check the “Do not show this again” box. This is not seen in Chrome or IE.

Dashboard Country by Bytes don't match with OP/ Forensics search

The engine and logstash use different databases for their GeoIP lookups and the engine's database is newer than the one logstash uses so it is very likely that the engine country statistics will be slightly different from the ones displayed in Kibana.

In order to get the Deduplicate Packets Discard stat to show up in Kibana

You must enable the option in the Reporting Capture - “Analysis” capture.

Address Types graph shows “Bytes” instead of “Counts”

Total Events tool tip shows: “Sum of Bytes” instead of “Sum of Counts”

Attempts to display six or more days in Flows dashboard always fails

You must keep searches to 5 days or less.