

RSA | Security Analytics

Critical Start Threat Analytics Plugin Configuration

Contents

Contents

Threat Analytics Search Plugin for Google Chrome	4
Installing the Search Plugin in Google Chrome	5
Customizing the Plugin.....	7
Performing an Investigation	10
Exporting the Configurations to Another System.....	11
Contact Customer Care	12
Preparing to Contact Customer Care.....	12

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the [thirdpartylicenses.pdf](#) file.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Threat Analytics Search Plugin for Google Chrome

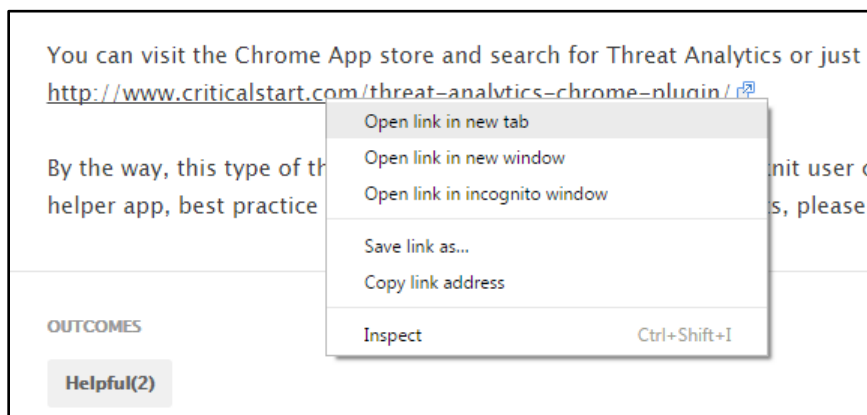
Threat Analytics Search Plugin for Google Chrome is a plugin that has been made by Critical Start and can be used with your Security Analytics deployment or your RSA NetWitness deployment. It is quick and easy to install the plugin and begin using it. The plugin is very flexible and can be fully customized according to the requirements of the analyst. Out of the box the analyst can right click and directly pass IP addresses or Domain names in to several different commonly searched websites. If a user wants to pass other metadata fields such as usernames, ports, email addresses, etc. it is a simple process to add them to the current configuration. Once fully configured, a user can export the configuration and share it with colleagues or other workstations running Google Chrome.

More information about the plugin can be found at the following page:

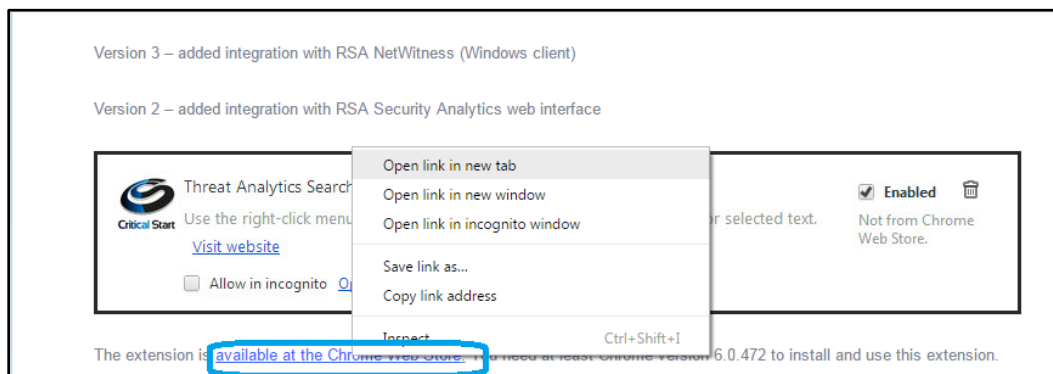
<https://community.rsa.com/thread/34959>

Installing the Search Plugin in Google Chrome

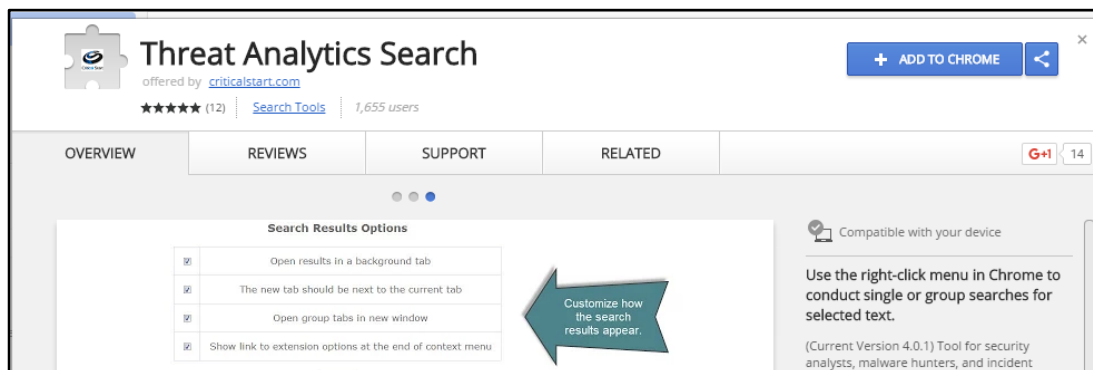
To install the plugin please visit <https://community.rsa.com/thread/34959> and open the link presented in the page shown below. You may also directly access the link here: <https://www.criticalstart.com/threat-analytics-chrome-plugin/>



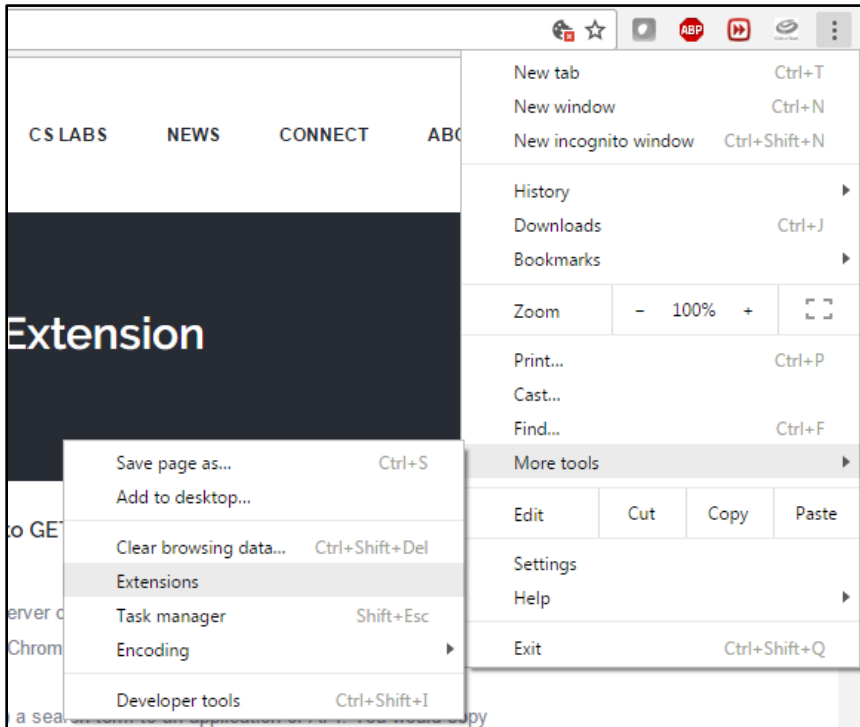
In the following page right click on the “available at the Chrome Web Store” link and open it in a new tab:



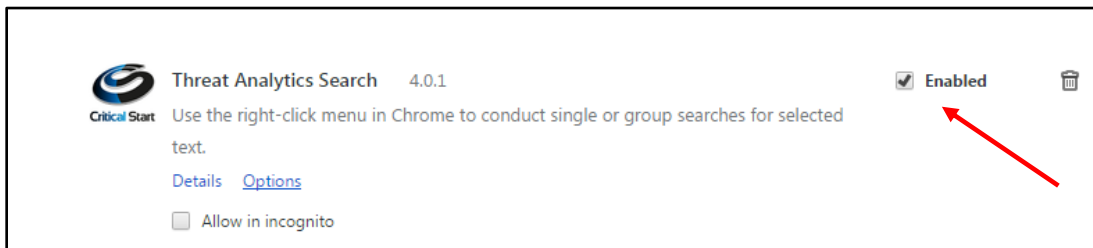
Add the extension to Google Chrome. Click Add to Chrome.



After the extension is added, go to More Tools -> Extensions in Google Chrome.



Find the Threat Analytics Search plugin in the extensions page and enable it if it is not already enabled.



Customizing the Plugin

Clicking on “Options” in the previous screenshot will load the following page:

For more information visit <http://www.criticalstart.com/threat-analytics-chrome-plugin/>


Display name	Link
<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Add POST value	<input type="text"/>
<input type="checkbox"/> Add Proxy URL	<input type="text"/>

Manage Context Menu Items

Display label	P	Link	Enabled?	Delete	From Download	IP Lookup	Domain	Hash
<input type="text" value="Google"/>		http://www.google.com/search?q=TESTSEARCH	<input checked="" type="checkbox"/>	<input type="button" value="X"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="D - WhoIS DN"/>		http://who.is/whois/TESTSEARCH	<input checked="" type="checkbox"/>	<input type="button" value="X"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="D - VirusTotal"/>		https://www.virustotal.com/en/domain/%s/inform	<input checked="" type="checkbox"/>	<input type="button" value="X"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="D - McAfee TI"/>		http://www.mcafee.com/threat-intelligence/doma	<input checked="" type="checkbox"/>	<input type="button" value="X"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="D - Builtwith"/>		https://builtwith.com/TESTSEARCH	<input checked="" type="checkbox"/>	<input type="button" value="X"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="D - TotalHash"/>		http://totalhash.com/search/dnsrr:TESTSEARCH	<input checked="" type="checkbox"/>	<input type="button" value="X"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="D - Builtwith"/>		https://builtwith.com/TESTSEARCH	<input checked="" type="checkbox"/>	<input type="button" value="X"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The above screenshot shows the default configuration for the plugin.

To configure the plugin for RSA Security Analytics or RSA NetWitness, click on the link called Security Analytics at the top right of the page. Clicking on this link will take you to the following page.

 **Critical Start**

[Search Providers](#) | [Options](#) | [Feedback](#) | [About](#)

[Security Analytics](#) | [NetWitness](#) | [Carbon Black](#)

Security Analytics Configuration

Paste example link from Security Analytics Investigation to autofill settings.	<input type="text"/>
Enable RSA Security Analytics Settings	<input type="checkbox"/>
Enable debug popup window	<input type="checkbox"/>
HTTPS (SSL) Enabled	<input checked="" type="checkbox"/>
Switch Focus to New Tab	<input checked="" type="checkbox"/>
Security Analytics Host (IP Address/Hostname)	<input type="text" value="192.168.1.10"/>
Port Number (leave blank if port 80 and HTTP or port 443 and HTTPS)	<input type="text"/>
DeviceID	<input type="text" value="2"/>

Configure the plugin by editing the fields highlighted in the screenshot below or by copying and pasting an investigation link from RSA NetWitness into the first field in the configuration menu. An example link that a user would paste into the first field is: <https://<ip address or hostname>/investigation/18/navigate/values>

In the link above, 18 is the device ID.

Security Analytics Configuration	
Paste example link from Security Analytics Investigation to autofill settings.	<input type="text"/>
Enable RSA Security Analytics Settings	<input checked="" type="checkbox"/>
Enable debug popup window	<input type="checkbox"/>
HTTPS (SSL) Enabled	<input checked="" type="checkbox"/>
Switch Focus to New Tab	<input checked="" type="checkbox"/>
Security Analytics Host (IP Address/Hostname)	<input type="text" value="10.25.52.160"/>
Port Number (leave blank if port 80 and HTTP or port 443 and HTTPS)	<input type="text" value="44105"/>
DeviceID	<input type="text" value="4"/>
Search Range 1 in Hour(s)	<input type="text" value="1"/>
Search Range 2 in Hour(s)	<input type="text" value="24"/>
Search Range 3 in Hour(s)	<input type="text" value="48"/>
Search Range 4 in Hour(s)	<input type="text" value="72"/>

1. RSA Security Analytics and/or RSA NetWitness settings need to be enabled to use the plugin.
2. Change the Security Analytics Host (IP Address/Hostname) to the IP address of the SA Server or the hostname of the SA Server.
3. Change the port number if the Security Analytics UI uses a different port than the default port of 443. Most users will use the default: 443.
4. The device ID needs to be updated to match the user's Security Analytics environment. It will be different for every RSA Security Analytics or RSA NetWitness installation. Typically a user will use the device ID of their top level broker. It can also be updated to use the device ID of a Concentrator, if a user does not have a broker in their environment. This is typically seen in single site, small deployments.
5. Search ranges can be customized for the user's needs. The values entered represent the number of hours which the analyst wants to use for performing an investigation.

Scroll down towards the bottom of the page and there will be more options to customize specific search criteria. A user can add additional queries using the example template below. Any meta key from RSA NetWitness or RSA Security Analytics can be added here.

Add More Query Options

To add a new query, replace the search term with "TESTSEARCH" in your query and copy the query to the 'Query' field below.

Display name	Security Analytics Pivot (Query)
Destination User	<code>user.dst="TESTSEARCH"</code>

Add new query

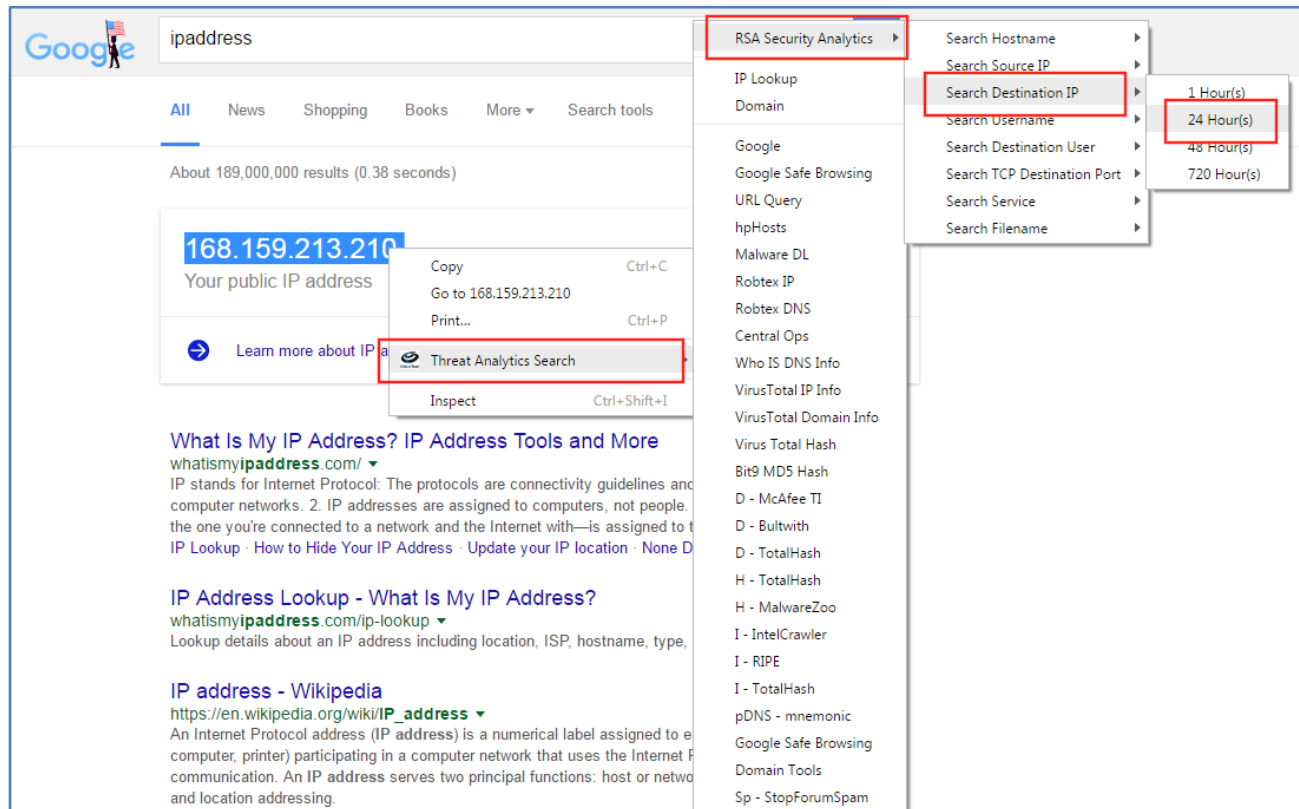
Manage Security Analytics Pivot Queries

	Display label	Query	Enabled	Delete
+	Search Hostname	<code>alias.host="TESTSEARCH"</code>	<input checked="" type="checkbox"/>	X
+	Search Source IP	<code>ip.src=TESTSEARCH</code>	<input checked="" type="checkbox"/>	X
+	Search Destination IP	<code>ip.dst=TESTSEARCH</code>	<input checked="" type="checkbox"/>	X
+	username	<code>username = "TESTSEARCH"</code>	<input checked="" type="checkbox"/>	X

Save

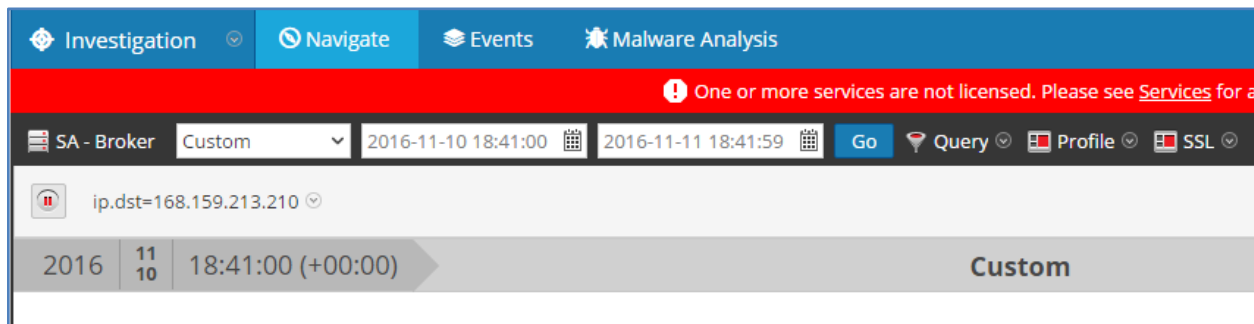
Once the customizations are saved the user is ready to perform investigations.

Performing an Investigation



We can use a quick Google search to test our investigation functionality. The analyst can enter any search string, select the entire string, and right click on it to go the options as shown in the above screenshot. The analyst has the ability to perform searches on a large list of community websites, custom websites added by the user and on and within RSA Security Analytics/RSA NetWitness.

Clicking on the specific time range will take you to the Security Analytics window as shown below:



Exporting the Configurations to Another System

If there is another system where the plugin is installed in the Chrome browser, we can export the settings from a system which is already configured.

To do that one needs to go click on “Options” at the top right of the page. Clicking on “Options” will take the user to the following page:

Configuration File Options

File URL	<input type="text" value="http://www.criticalstart.com/cschromeplugin/criticalstart.txt"/>
Use groups from this download	<input checked="" type="checkbox"/>
Encrypted	<input type="checkbox"/>
Encryption Key	<input type="text"/>
Refresh Automatically	<input type="checkbox"/>
Last Refreshed on	Tue Nov 08 2016 14:43:29 GMT+0530 (India Standard Time)

Export/Import Search Options

```
1 {"RSAConfigEnable":true,"RSAConfigPopup":false,"RSAConfigUseHttps":true,"CBCConfigNewTab":true,"CBCConfigHost":"192.168.1.100",
2 "RSAConfigPort":44105,"RSAConfigDevId":4,"RSAConfigRange1":1,"RSAConfigRange2":24,"RSAConfigRange3":48,"RSACon
3 figRange4":72},"Queries":[[-1,"Search Hostname","alias.host=TESTSEARCH",true],[[-1,"Search Source
4 IP","ip.src=TESTSEARCH",true],[[-1,"Search Destination IP","ip.dst=TESTSEARCH",true],[[-1,"Username","username
5 =\\TESTSEARCH\\",true],[[-1,"Destination User","user.dst=\\TESTSEARCH\\",true]]],"NWI":{"Config":
6 {"NWIConfigEnable":false,"NWIConfigPopup":false,"NWIConfigGMT":false,"NWIConfigHost":"","NWIConfigPort":"","NWIConfigCollection
7 Name":"","NWIConfigRange1":1,"NWIConfigRange2":24,"NWIConfigRange3":48,"NWIConfigRange4":720},"Queries":
8 [[-1,"Search Hostname","alias.host=TESTSEARCH",true],[[-1,"Search Source IP","ip.src=TESTSEARCH",true],[[-1,"Search
9 Destination IP","ip.dst=TESTSEARCH",true]]],"CBC":{"Config":
10 {"CBCConfigEnable":false,"CBCConfigPopup":false,"CBCConfigUseHttps":true,"CBCConfigNewTab":true,"CBCConfigHost":"192.168.1.1
11 0","CBCConfigPort":"","CBCConfigURLVersion":1},"Queries":[[-1,"Search All (Mostly Use This)","q=TESTSEARCH",true],[[-1,"Domain
12 Name (FODN)","cb.q.domain=TESTSEARCH",true],[[-1,"Hostname (Has CB Sensor)","cb.q.hostname=TESTSEARCH",true],[[-1,"Process
13 or EXE","cb.q.process_name=TESTSEARCH",true],[[-1,"MD5 Hash Search","cb.q.md5=TESTSEARCH",true]]]}}
```

Use the above string to transfer your search engine options from one install of Chrome to another effortlessly.
Just copy the string from here to the options page in other install of chrome (or vice-versa) and press 'Save'
Warning: Editing the above string may cause unexpected behaviour!

The entire text that is highlighted can be copied and pasted on another system where the plugin is installed. This will copy all the configurations that have been created.

Contact Customer Care

RSA SecureCare Online:	https://knowledge.rsasecurity.com/ or https://community.rsa.com/community/rsa-customer-support
Phone:	1-800-995-5095, option 3
International Contacts:	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Email:	support@rsa.com
Community:	https://community.rsa.com/community/products/netwitness
Basic Support:	Technical Support for your technical issues is available during your local time, Monday through Friday. 8am to 5pm
Enhanced Support:	Technical Support is available by phone 24 x 7 x 365 days of the year for Severity 1 and Severity 2 issues only.

Preparing to Contact Customer Care

When you contact Customer Care, you should be at your computer. Be prepared to give the following information:

1. The version number of the RSA NetWitness product or application you are using.
2. The type of hardware you are using.