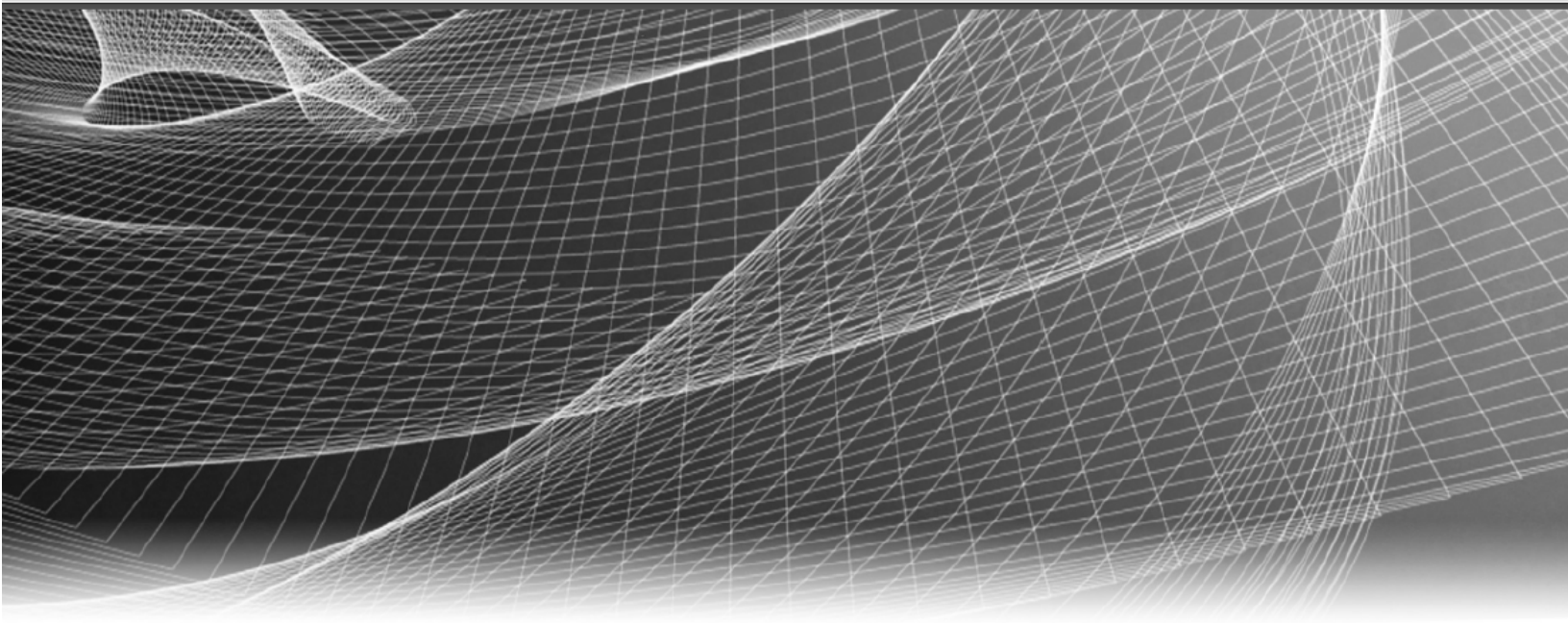


RSA | Security Analytics

Remove Original IR Content Pack

RSA EMC²

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Contents

Removing the Original Incident Response (IR) Pack

The Hunting Pack is designed to allow you to quickly hunt for indicators of compromise or anomalous network activity by dissecting packet traffic within the NetWitness Suite and populating specific meta keys with natural language values for investigation. This package was originally designed by, and distributed through, the RSA Incident Response Team. This content has now been integrated into the officially released content through RSA Live and can be deployed through the product. See https://community.rsa.com/docs/DOC-62341 for more information about the productized Hunting Pack.

RSA recommends that you remove the old IR Content Pack from your system before deploying the new Hunting Pack.

Note: Some of the original IR Content installed Reports and Rules may need modification or complete removal after updating to the new Hunting pack. Any customization to the older IR Content Reports, or Rules, added to the original IR Content installation should be reviewed prior to removal.

Unsupported Keys

The following keys are not supported by RSA:

- http.request
- http.response
- req.uniq
- resp.uniq

If you have rules written around any of these keys, we recommend that you contact RSA support for guidance.

Creation of Metadata

1. Update Reports (or any custom content) to map to the metadata used in the new Hunting Pack.
2. Stop the creation of duplicate meta. Perform one of the following procedures:
   - To disable, but not remove the Lua parsers, see the Disable the IR Pack Lua Parsers procedure.
   - To completely remove the Lua parsers, see the Remove the IR Pack Lua Parsers procedure.
3. Remove Application Rules from all decoders.
4. Remove Feeds.

Consumption of Metadata

After you remove the original content, you should remove meta keys from indexes, meta groups, and profiles. For details, see Meta Keys

1. Remove meta keys from meta groups and profiles.
2. Remove meta keys from concentrator indexes.
3. Remove meta keys from decoders.

Lua Parsers

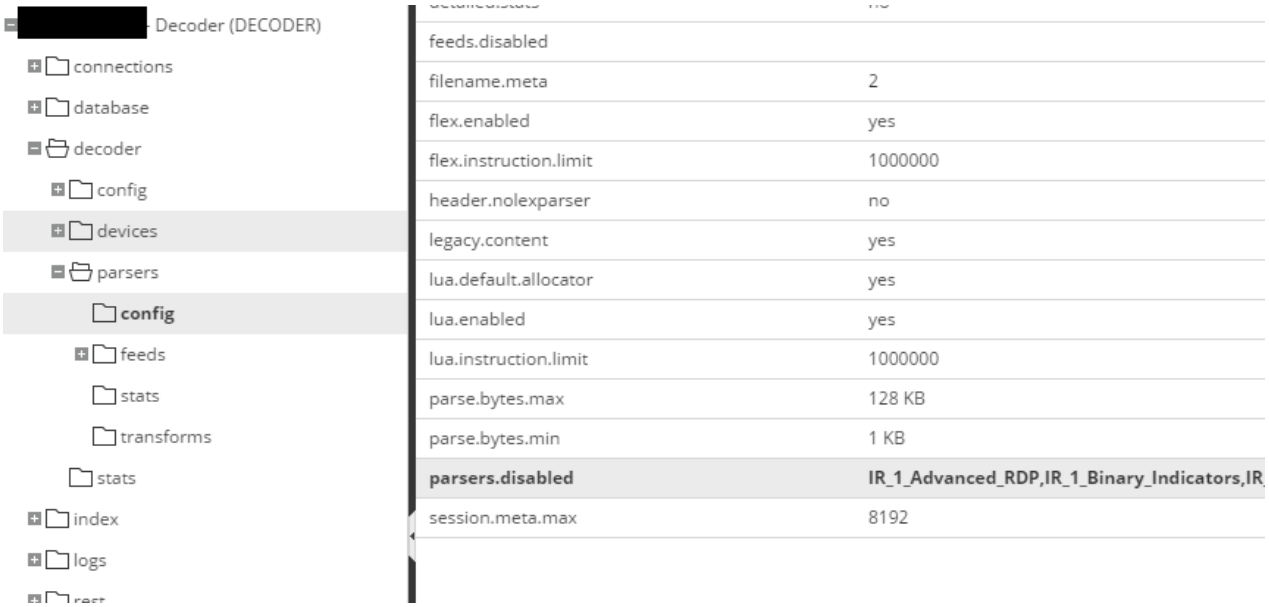
You can disable or remove the IR content Lua parsers.

Note: RSA recommends you remove them.

Disable the IR Pack Lua Parsers

To Disable the IR content pack Lua Parsers:

1. In the Security Analytics menu, select **Administration > Services**, and select a Decoder.
2. Select **Explore**.
3. Expand **decoders > parsers**
4. Click **config**.



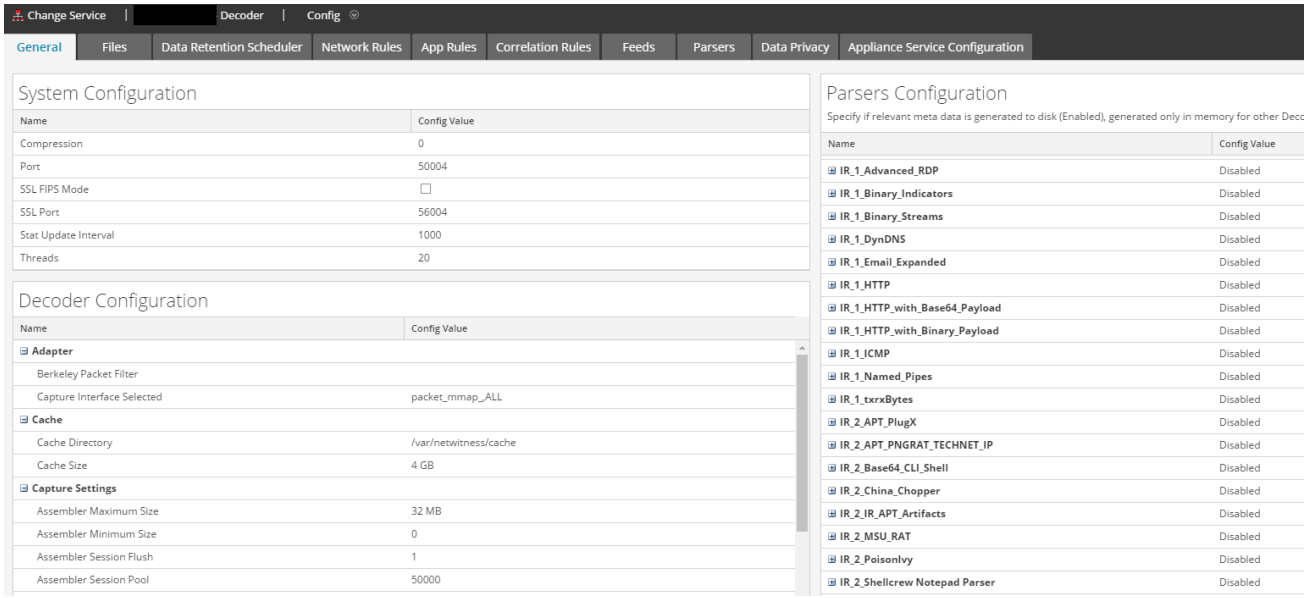
5. For **parsers.disabled**, enter the list of parsers to disable:

```
IR_1_Advanced_RDP,IR_1_Binary_Indicators,IR_1_Binary_Streams,IR_1_DynDNS,IR_1_Email_
Expanded,IR_1_HTTP,IR_1_HTTP_with_Base64_Payload,IR_1_HTTP_with_Binary_Payload,IR_1_
ICMP,IR_1_Named_Pipes,IR_1_txrxBytes,IR_2_IR_APT_Artifacts,IR_2_APT_PlugX,IR_2_APT_PNGRAT_
TECHNET_IP,IR_2_Base64_CLI_Shell,IR_2_China_Chopper,IR_2_MSU_RAT,IR_2_PoisonIvy,IR_2_
Shellcrew Notepad Parser
```

6. Click **Enter**

   You receive a message that the configuration was successful.

You can verify the parsers are disabled by navigating to **Administration > Services > Decoder > Config > General**.



Remove the IR Pack Lua Parsers

Remove the old IR pack Lua parsers from your Decoders:

1. In the Security Analytics menu, select **Administration > Services**, and select a Decoder.
2. In the Actions column, select **View > Config**.
3. Select the **Parsers** tab.
4. Search for parsers that have names beginning with `IR_`, and select only these parsers.
5. Click — to remove the selected parsers.

Parser Name	Metadata Category	Metadata Generated
IR_1_Advanced_RDP.lua	language rdp.info	Extracts keyboard layout Extracts key
IR_1_Binary_Indicators	ir.general	Binary Indicator

Parser Name	Metadata Category	Metadata Generated
IR_1_Binary_Streams	req.binary res.binary ir.general	Determines binary data in the request stream Determines binary data in the response stream Binary_Handshake
IR_1_DynDNS.lua	risk.info	dynamic dns host, dynamic dns server
IR_1_Email_Expanded.lua	emailfrom emailto emailxmailer emailfromdomain language	Extracts From: address Extracts To: address Extracts X-Mailer: Extracts domain from From: field Extracts Language Encoding
IR_1_HTTP.lua	http.request http.response req.uniq res.uniq agent.ext ir.general action	Extracts HTTP Request Headers Extracts HTTP Response Headers Extracts unique values from HTTP Request Headers Extracts unique values from HTTP Response Headers Extracts User-Agent: field Explicit_Proxy_Request put_method
IR_1_HTTP_with_base64.lua	ir.general	http_with_possible_base64
IR_1_HTTP_with_binary.lua	ir.general	HTTP_with_binaryPayload
IR_1_ICMP.lua	action error ir.general	ICMP Types and Codes into action and error. Large frames are alerted into ir.general.
IR_1_Named_Pipes.lua	named.pipe	Extracts Named PIPE from SMB/RPC traffic
IR_1_txrxByptes	txbytes rxbytes bytes.ratio	Payload Transmit Bytes Payload Receive Bytes Payload Transmit Receive Ratio

Parser Name	Metadata Category	Metadata Generated
IR_2_APT_Artificats	ir.alert	apt_possible_prefetch_deletion apt_possible_registry_deletion apt_possible_wmic_cleareventlog apt_possible_regedit apt_possible_invokemimikatz
IR_2_apt_PlugX	ir.alert	apt_PlugX apt_PlugX_possible
IR_2_APT_PNGRAT_TECHNET_IP	ir.alert alias.ip	APT_PNGRAT_@MICR0S0FT_IP IP Address
IR_2_B64_Shell	ir.alert	Possible_B64_Shell
IR_2_China_Chopper	ir.alert	ASPX_China_Chopper PHP_China_Chopper CFM_China_Chopper
IR_2_MSU	ir.alert crypto	apt_MSU_RAT XOR key
IR_2_Poison_Ivy	ir.alert ir.general	Possible_Poison_Ivy_Handshake Possible_Poison_Ivy_Beacon
IR_2_sc_notepad	ir.alert	sc_notepad request/response seen - c2 live sc_notepad initial beacon

Application Rules

Remove the old IR pack application rules from your Decoders:

1. In the Security Analytics menu, select **Administration > Services**, and select a Decoder.
2. In the **Actions** column, select **View > Config**.
3. Select the **App Rules** tab.
4. In the **Filter** field, enter three hash tags: `###` This returns the list of Application Rules that are part of the original IR pack.
5. Select the rules that begin with the `###` string.
6. Click — to remove the selected rules.

Additionally, the application rules listed in the table below should be removed from your Decoders. Use the steps provided above to search for and remove the additional application rules from your Decoders before you install the new Hunting Pack.

Rule Name	Meta Key	Rule
!advertising	ir.general	threat.category != 'advertising'"
!top20dst	ir.general	ir.general != 'top20dst'"
apt_ActiveMonk_UA	ir.alert	client begins \"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Maxthon; TERA\" ||client begins \"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Maxthon; XSL\""
apt_Deep_Panda_C2	ir.alert	(directory = 'Catelog' && action = 'put' && filename = 'login.cgi') || (directory = 'Photos' && action = 'get' && filename = 'Query.cgi') || (directory = 'forum' && action = 'put' && filename = 'login.cgi')"
apt_Foxy_RAT	ir.alert	action = 'put' && filename = '404error.asp'"
apt_Lurid_RAT	ir.alert	service = 80 && action = 'put' && client !exists && directory = 'cgi-bin','/Sjwpc/odw3ux'"
apt_MiniASP	ir.alert	query begins 'device_t='"
apt_NetTravler_RAT	ir.alert	filename = 'nettraveler.asp'"
apt_NFlog_RAT	ir.alert	directory = 'Nflog' || client = 'www'"
apt_PhotoASP_RAT	ir.alert	client = 'Mozilla/4.0' && filename = 'PHOTO.ASP' && http.request != 'referer'"
apt_PNG_Rat	ir.alert	client = 'Windows+NT+5.1'"
apt_Sykipot_RAT	ir.alert	client= 'HTTP-GET'"

Rule Name	Meta Key	Rule
apt_WebC2_CS	ir.alert	client = 'Win32' && query begins 'ID=','INDEX='"
apt_ZipToken_UA_POST	ir.alert	client = 'HttpBrowser/1.0' && action = 'put'"
bad_org_susp_other	ir.general	ir.general = 'suspicious_other' && ir.general = 'watchlist_org.dst'"
bad_ssl	ir.general	alias.host = 'localhost' && service = 443 && direction = 'outbound'"
bytes.ratio_high_tx	ir.general	medium=1 && bytes.ratio = 75-u"
bytes.ratio_low_tx	ir.general	medium=1 && bytes.ratio = l-25"
bytes.ratio_med_tx	ir.general	medium=1 && bytes.ratio = 25-75"
bytes.ratio_tx_only	ir.general	rxbytes !exists && medium=1 && bytes.ratio = 100-u"
common_domains	ir.general	alias.host ends 'gvt1.com'"
common_src	ir.general	org.src='exacttarget','constant contact','responsys','sitewire marketspace solutions','isdnet','e-dialog','linkedin corporation','qwest communications', 'silverpop systems','psinet','postini','cheetahmail','amazon.com','eloqua corporation','spark marketing llc','ibm-mgt','facebook','omeda communications','easystreet online services'"
Crimeware_Black_Hole_Exploit_Kit	ir.alert	filename = 'web7.dat'"
Crimeware_Zeus	ir.alert	service = 80 && action = 'put' && action != 'get' && filename = 'timestamps.php','gameover.php','gameover2.php','gameover3.php','gate.php' && http.request != 'referer'"
Crimeware_Zeus_Knownbad	ir.alert	service = 80 && query contains 'index.php?r=gate&id='"
direct to ip http request	risk.suspicious	ir.general = 'http_direct_to_ip'"
direct_to_ip_one_char_php	ir.general	ir.general = 'http_direct_to_ip' && ir.general = 'one_char_php_filename' && query exists"
dynamic_dns_query	ir.general	service = 53 && risk.info = 'dynamic dns host','dynamic dns server'"
Elderwood_XMailer_Artifact	ir.alert	emailxmailer contains '10.40.1836'"
email_fwd	ir.general	ir.general = 'inbound_email' && subject begins 'fwd'"
email_re	ir.general	ir.general = 'inbound_email' && subject begins 're'"

Rule Name	Meta Key	Rule
exe_filetype	ir.general	filetype = 'x86_pe','x64_pe' || filetype begins 'windows'"
exe_under_10k	ir.general	size=l-10000 && ir.general = 'exe_filetype'"
exe_under_5K	ir.general	size=l-5000 && ir.general = 'exe_filetype'"
exe_under_75K	ir.general	size=l-75000 && ir.general = 'exe_filetype'"
exe-ext_but_!exe-file-type	ir.general	extension = 'exe' && ir.general != 'exe_filetype'"
exe-filetype_but_!exe-ext	ir.general	extension exists && extension != 'exe' && ir.general = 'exe_filetype'"
express_x-mailer	ir.general	service=25 && client contains 'express'"
external_dst	ir.general	ir.general != 'rfc1918_dst' && netname.dst !exists"
external_src	ir.general	ir.general != 'rfc1918_src' && netname.src !exists"
filter_netwitness		rule="(tcp.dstport = 50001-50008,50101-50108,56001-56008 || tcp.srcport = 50001-50008,50101-50108,56001-56008) && (netname.src = 'netwitness' || netname.dst = 'netwitness')
first_carve	ir.general	direction = 'outbound' && ir.general != 'zero_payload' && ir.general != 'single_sided_tcp' && ir.general != 'single_sided_udp'"
first_carve_!advertising	ir.general	ir.general='first_carve' && ir.general = '!advertising'"
first_carve_!dns	ir.general	ir.general='first_carve' && service!=53"
first_carve_!top20dst	ir.general	ir.general='first_carve' && ir.general = '!top20dst'"
first_carve_!top20d-st_!advertising	ir.general	ir.general='first_carve_!top20dst' && ir.general = '!advertising'"
four_http_headers	ir.general	http.request exists && http.request count l-4 && service = 80 && ir.general != 'three_http_headers' && ir.general != 'two_http_headers'"
four_or_less_headers	ir.general	http.request exists && http.request count l-4 && service = 80"
high_tx_outbound	ir.general	medium=1 && txbytes=4000000-u && risk.info='outbound_traffic'"
http direct to ip request	risk.info	ir.general = 'http_direct_to_ip'"
http_access_to_dyndns_site	ir.general	service = 80 && risk.info = 'dynamic dns host','dynamic dns server'"
http_connect	ir.general	service=80 && (action = 'connect' && action != 'get','head','options','delete','trace','put','patch')"

Rule Name	Meta Key	Rule
http_direct_to_ip	ir.general	service = 80 && risk.info='http direct to ip request'"
http_get_no_post	ir.general	service=80 && action = 'get' && action != 'put','post'"
http_no_ua	ir.general	service = 80 && agent.ext !exists"
http_post_and_get	ir.general	service=80 && action = 'put','post' && action = 'get'"
http_post_no_get	ir.general	service=80 && action = 'put','post' && action != 'get'"
http_query_with_base64	ir.general	service = 80 && action = 'GET','POST' && query contains '==' && ir.general != 'top20dst'"
http_response_filename	ir.general	res.uniq contains 'filename'"
http_response_filename_attachment	ir.general	res.uniq contains 'filename' && res.uniq contains 'attachment'"
http_response_filename_bin	ir.alert	ir.general = 'http_response_filename_inline','http_response_filename_attachment' && attachment ends 'bin'"
http_response_filename_exe	ir.alert	ir.general = 'http_response_filename_inline','http_response_filename_attachment' && ir.general = 'exe_filetype'"
http_response_filename_inline	ir.general	res.uniq contains 'filename' && res.uniq contains 'inline'"
http_tunnel_rat	ir.alert	query contains '[not%20httptunnel]'"
icmp_large_session	ir.general	size=1000-u && ip.proto = 1 && risk.info = 'outbound_traffic'"
icmp_tunnel	ir.general	service != 0 && ip.proto = 1 && risk.info = 'outbound_traffic'"
ie_short_ua	ir.general	ir.general begins 'short_ie'"
inbound	direction	ir.general = 'external_src' && ir.general = 'internal_dst'"
inbound_email	ir.general	service=25 && direction = 'inbound'"
inbound_traffic	ir.general	org.src exists && ir.general != 'zero_payload' && ir.general != 'single_sided_tcp' && ir.general != 'single_sided_udp'"
interesting_email	ir.general	ir.general = 'inbound_email' && ir.general = 'mail_!common_src' && ir.general != 'email_re' && ir.-general != 'email_fwd'"
internal_dst	ir.general	ir.general = 'rfc1918_dst' || netname.dst exists"
internal_src	ir.general	ir.general = 'rfc1918_src' || netname.src exists"

Rule Name	Meta Key	Rule
invalid_alias.host	ir.general	risk.suspicious='hostname invalid'"
java_1.3	ir.general	agent.ext contains 'java' && agent.ext contains '1.3'"
java_1.4	ir.general	agent.ext contains 'java' && agent.ext contains '1.4'"
java_1.5	ir.general	agent.ext contains 'java' && agent.ext contains '1.5'"
java_1.6	ir.general	agent.ext contains 'java' && agent.ext contains '1.6'"
java_1.7	ir.general	agent.ext contains 'java' && agent.ext contains '1.7'"
java_1.8	ir.general	agent.ext contains 'java' && agent.ext contains '1.8'"
java_exe	ir.alert	ir.general='first_carve' && agent.ext contains 'java' && ir.general = 'exe_filetype'"
java_pdf	ir.alert	ir.general contains 'java' && filetype = 'pdf'"
Known_Bad_File_Name	ir.alert	filename = 'appletLow.-jar','appletHigh.jar','DOITYOUR02.html','DOITYOUR01.txt','logo1229.swf','Func1.class','Tmpschdeul.c-lass'"
Known_Bad_Self_Signed_Cert_MyCom-panyLtd	ir.alert	ssl.ca=\"MyCompany Ltd.\" && ssl.subject=\"MyCompany Ltd.\" || ssl.subject=\"MyCompany Ltd.\""
Known_Bad_UA_Cre-dentialLeak_rule	ir.alert	client = \"HardCore Software For : Public\" "
Known_Bad_UA_IE6Beta_rule	ir.alert	client contains 'MSIE 6.0b'"
Known_Bad_UA_UPSPhishing_rule	ir.alert	client = 'Our_Agent' "
large_dns_service	ir.general	service = 53 && size=100000-u && risk.info = 'outbound_traffic'"
large_session_dns_port	ir.general	tcp.dstport = 53 && size=100000-u && risk.info = 'outbound_traffic'"
local_suffix rule	ir.general	alias.host ends '<customer's domain suffixes>'
long_connection	ir.general	lifetime = 30-u"
long_http_query	ir.general	service = 80 && query length 256-u && query count l-1"
long_ua	ir.general	agent.ext length 56-u"
long_ua2	ir.general	agent.ext length 75-u"

Rule Name	Meta Key	Rule
mail_!common_src	ir.general	service = 25 && ir.general != 'common_src'"
malware_sinkhole	ir.alert	http.response contains 'sinkhole'"
malware_sinkhole	ir.alert	server contains 'sinkhole'"
max_length_ua	ir.general	agent.ext length 256-u"
med_tx_outbound	ir.general	medium=1 && txbytes=1024000-u && txbytes =l-4000000 && risk.info='outbound_traffic'"
mid_ua	ir.general	agent.ext exists && ir.general = 'long_ua' && ir.general != 'long_ua2'"
mozilla_3	ir.general	agent.ext begins 'mozilla/3.0'"
mozilla_4	ir.general	agent.ext begins 'mozilla/4.0'"
mozilla_5	ir.general	agent.ext begins 'mozilla/5.0'"
netbox_Server	ir.general	server begins 'Netbox'"
netwitness	netname.src	ip.src = <customer_netwitness_ip_list>
netwitness	netname.dst	ip.dst = <customer_netwitness_ip_list>
odd_alias.host	ir.general	ir.general != 'invalid_alias.host' && ir.general != 'odd_domain_filter' && alias.host regex '([bcdfghjklmnpqrstvwxyz][bcdfghjklmnpqrstvwxyz][bcdfghjklmnpqrstvwxyz][bcdfghjklmnpqrstvwxyz]){2,}'
odd_domain_filter	ir.general	alias.host ends '.telemetryverification.net','.crwdcntrl.net','.cloudfront.net','.gstatic.com','.disqus.com', '.112.2o7.net','.sophosxl.com','.lognormal.net'
one_char_php_filename	ir.general	filename length 5 && extension='php'"
one_two_filename_ java_class	ir.general	filename length 7-8 && extension='class'"
outbound	direction	ir.general = 'internal_src' && ir.general = 'external_dst'"
outbound_dns	ir.general	service = 53 && risk.info = 'outbound_traffic'"
outbound_syslog	ir.general	udp.dstport = 514 && risk.info = 'outbound_traffic'"
outbound_traffic	risk.info	ir.general = 'internal_src' && ir.general = 'external_dst'"
possible_cybercrime	ir.alert	query contains 'index.php?r=gate&id='"
possible_exploitkit_indic- ator	ir.general	ir.general='first_carve' && ir.general = 'java_1.5','java_1.6','java_1.7','java_1.8' && ir.general = 'http_ get_no_post'"
possible_malware_ua	ir.alert	ir.general = 'first_carve' && agent.ext begins 'user-agent: '"

Rule Name	Meta Key	Rule
possible_malware_ua	ir.alert	client contains 'GTB0.0; '"
Possible_Poison_Ivy	ir.alert	service = 0 && tcp.dstport = 443,79,80,81,7000 && payload = 256 && lifetime = 0 && rpayload !exists "
possible_redkit	ir.alert	ir.general = 'first_carve' && filename = 'hmod.html','332.jar','887.jar','987.pdf'"
possible_zeroaccess_ p2p_botnet	ir.alert	service=0 && (tcp.dstport=16464,16471 || udp.dstport=16464,16465,16470,16471) && ir.general = 'rfc1918_src'"
post_no_get_no_refer	ir.general	ir.general = 'http_post_no_get' && http.request != 'referer'"
post_no_get_no_refer_ directtoip	ir.general	ir.general = 'http_post_no_get' && ir.general='http_direct_to_ip' && http.request != 'referer'"
potential_beacon	ir.general	service = 0 && ir.general = 'watchlist_ports' && size=l-1200 && packets=4-u && risk.info = 'outbound_ traffic'"
psexec_remote_exe- cution	ir.general	service = 139 && filename = 'psexesvc.exe'"
rfc1918_dst	ir.general	ip.dst = 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16"
rfc1918_src	ir.general	ip.src = 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16"
session_size_0-5k	ir.general	streams=2 && size=l-5120"
session_size_10-50k	ir.general	streams=2 && size=l-51200 && size = 10240-u"
session_size_100-250k	ir.general	streams=2 && size=l-256000 && size=102400-u"
session_size_5-10k	ir.general	streams=2 && size=l-10240 && size=5120-u"
session_size_50-100k	ir.general	streams=2 && size=l-102400 && size=51200-u"
short_filename	ir.general	ir.general='first_carve_!dns' && filename length 5-7 && extension length 3"
short_ie_10	ir.general	ir.general != 'long_ua' && agent.ext contains 'ie 10'"
short_ie_11	ir.general	ir.general != 'long_ua' && agent.ext contains 'ie 11'"
short_ie_3	ir.general	ir.general != 'long_ua' && agent.ext contains 'ie 3'"
short_ie_4	ir.general	ir.general != 'long_ua' && agent.ext contains 'ie 4'"
short_ie_5	ir.general	ir.general != 'long_ua' && agent.ext contains 'ie 5'"
short_ie_6	ir.general	ir.general != 'long_ua' && agent.ext contains 'ie 6'"
short_ie_7	ir.general	ir.general != 'long_ua' && agent.ext contains 'ie 7'"

Rule Name	Meta Key	Rule
short_ie_8	ir.general	ir.general != 'long_ua' && agent.ext contains 'ie 8'"
short_ie_9	ir.general	ir.general != 'long_ua' && agent.ext contains 'ie 9'"
short_ua	ir.general	agent.ext exists && ir.general != 'long_ua'"
single_sided_tcp	ir.general	ip.proto = 6 && streams = 1 && payload = 0 && service = 0"
single_sided_udp	ir.general	ip.proto = 17 && streams = 1"
six_or_less_headers	ir.general	http.request exists && http.request count l-6 && service = 80"
small_java_class	ir.general	size=l-10000 && filetype='java_class','java class'"
small_java_jar	ir.general	size=l-10000 && filetype='java_jar','java jar'"
smb_at_command	ir.alert	named.pipe contains 'atsvc'"
subject_phish	ir.general	ir.general = 'interesting_email' && subject contains 'update','important','notice','attention','please','vpn'"
suspicious_4headers	ir.general	ir.general='first_carve' && ir.general='http_post_no_get' && ir.general='four_or_less_headers' && agent.ext != 'shockwave flash'
suspicious_6headers	ir.general	ir.general='first_carve' && ir.general='http_post_no_get' && ir.general !='four_or_less_headers' && ir.general='six_or_less_headers' && agent.ext != 'shockwave flash'
Suspicious_Connect	ir.general	ir.general = 'HTTP_CONNECT' && ir.general ends '_http_headers' && http.request != 'User-Agent' && ssl.ca !exists && ssl.subject !exists
suspicious_other	ir.general	ir.general = 'first_carve' && service = 0 && ir.general = 'long_connection' && tcp.dstport exists && risk.info = 'flags_syn' && ir.general != 'top20dst'
suspicious_tcp_beaconing	ir.general	(ip.proto=6 && streams = 1 && risk.info = 'flags_syn' && risk.info != 'flags_ack' && risk.info != 'flags_psh' && risk.info != 'flags_fin' && risk.info != 'flags_rst' && ir.general != 'rfc1918_dst') || (ip.proto = 6 && streams = 2 && risk.info = 'flags_syn' && risk.info = 'flags_rst' && risk.info != 'flags_psh' && risk.info != 'flags_fin' && ir.general != 'rfc1918_dst' && payload = 0)
suspicious_traffic_over_53	ir.general	risk.info = 'outbound_traffic' && (service = 80 || service = 443) && tcp.dstport = 53
suspiciously_named_domains	ir.general	alias.host contains 'google','yahoo','microsoft','trendmicro','facebook','twitter','adobe','solaris','cisco','symantec','amazon' && ir.general != 'well_known_domains','local_suffix' && alias.host count l-1
three_http_headers	ir.general	http.request exists && http.request count l-3 && service = 80 && ir.general != 'two_http_headers'"
tld_is_com_org_net	ir.general	tld = 'com','org','net'"
tld_is_not_com_org_net	ir.general	tld exists && ir.general != 'tld_is_com_org_net'"

Rule Name	Meta Key	Rule
top20dst	ir.general	org.dst='akamai technologies','google','microsoft corp','rcn corporation','server central network', 'amazon.com','microsoft hosting','level 3 communications','yahoo!','limelight networks', 'edgecast networks','facebook','global crossing','altavista company','mcafee','apple', 'america online','adobe systems','dropbox','cotendo'
top20src	ir.general	service=25 && org.src='exacttarget','constant contact','responsys','sitewire marketspace solutions', 'isdnet','e-dialog','linkedin corporation','qwest communications','silverpop systems','psinet','postini', 'cheetahmail','amazon.com','eloqua corporation','spark marketing llc','ibm-mgt','facebook', 'omeda communications','easystreet online services'
Trojan/Napolar	ir.alert	http.request = 'Agtid'"
two_http_headers	ir.general	http.request exists && http.request count l-2 && service = 80"
ua_begins_mozilla	ir.general	agent.ext begins 'mozilla/'"
ua_non_standard_mozilla	ir.general	ir.general = 'ua_begins_mozilla' && ir.general != 'mozilla_3' && ir.general != 'mozilla_4' && ir.general != 'mozilla_5'"
ua_not_good_mozilla	ir.general	agent.ext exists && ir.general != 'ua_begins_mozilla'"
watchlist_file_extension	ir.general	extension = 'exe','cgi','php','bin','rar','zip','pdf','txt','js','jar','bat'"
watchlist_file_fingerprint	ir.general	filetype = 'windows_executable','windows_dll','java_jar','zip','pdf','rar','java_class'"
watchlist_org.dst	ir.general	org.dst contains 'hurricane','linode','ovh','rackspace'"
watchlist_ports	ir.general	tcp.dstport = 21,22,23,25,53,80,110,137,138,139,143,443,445"
web_susp_act	ir.general	agent.ext contains ';)',';)'"
web_susp_act	ir.general	ir.general = 'short_filename' && ir.general = 'http_post_no_get' && extension = 'php','asp','aspx','cgi','pl'"
web_susp_act	ir.general	ir.general='http_post_no_get' && ir.general ends 'http_headers' && agent.ext != 'shockwave flash'"
web_susp_act	ir.general	http.request != 'content-length' && ir.general = 'http_post_no_get'"
web_susp_act	ir.general	http.request = 'content-length' && ir.general = 'http_get_no_post'"
web_susp_act	ir.general	http.request exists && http.request != 'user-agent'"
web_susp_act	ir.general	ir.general = 'http_post_no_get' && ir.general ends 'short_ua'"
web_susp_act_alias.host	ir.general	service = 80 && ir.general = 'web_susp_act' && ir.general='http_direct_to_ip'"
web_susp_act_direct_to_ip	ir.general	service = 80 && ir.general = 'web_susp_act' && ir.general='http_direct_to_ip'"

Rule Name	Meta Key	Rule
web_susp_act_no_cookie	ir.general	ir.general ='http_post_no_get' && http.response EXISTS && http.response != 'cookie' && http.response != 'set-cookie'"
webshell_indicator	ir.general	action = 'head' && extension = 'zip','rar','exe','dll','jsp','php','vbs','bat','asp','aspx' && direction = 'inbound'"
webshell_indicator	ir.general	action = 'put_method' && direction = 'inbound'"
webshell_indicator	ir.general	ir.general = 'http_post_no_get' && extension = 'php','jsp','class','java','cfm','cgi','dll','pl','asp','aspx' && direction = 'inbound'"
webshell_indicator	ir.general	query contains '\\+\\%','\\%70\\%68\\%70\\%' && ir.general = 'http_post_no_get' && direction = 'inbound'"
webshell_indicator	ir.general	query contains 'c\\:\\\\','d\\:\\\\','e\\:\\\\','f\\:\\\\','g\\:\\\\','h\\:\\\\' && ir.general = 'http_post_no_get' && direction = 'inbound'"
webshell_indicator	ir.general	query contains 'command\\=' && direction = 'inbound'"
webshell_indicator	ir.general	query contains 'dallow_url_fopen','ddisable_functions','dallow_url_include' && direction = 'inbound'"
webshell_indicator	ir.general	query contains 'tar-getHost','targetPort','downfile','uplMonitor','servicePort','getData','cmd=','GetFile','Command'"
webshell_indicator	ir.general	query contains '.exe' && direction = 'inbound'"
webshell_indicator_http_error	ir.general	ir.general = 'webshell_indicator' && error exists"
webshell_indicator_no_http_error	ir.general	ir.general = 'webshell_indicator' && error !exists"
well_known_domains	ir.general	alias.host count l-1 && alias.host = 'apple.com','adobe.com','adobe.co.uk','solaris.com','cisco.com', 'cisco.co.uk','symantec.com','amazon.com','amazon.cn','amazon.fr','amazon.com.br','amazon.de', 'amazon.se','amazon.es','amazon.it','amazon.co.jp','amazon.co.uk','symantecliveupdate.com', 'amazonaws.com','googlesyndication.com','google-analytics.com','googleadservices.com', 'googleusercontent.com','facebook.net','images-amazon.com','doubleclick.net','akadns.net'
well_known_domains	ir.general	alias.host count l-1 && alias.host = 'google.com','google.com.sg','google.co.uk','google.com.ar', 'googleapis.com','googleads.com','google.be','google.ch','google.com.hk','google.fr','google.ru', 'google.es','googlemail.com','googlemail.co.uk','yahoo.com','yahoo.com.us','yahoo.co.uk', 'yahoodns.net','yahoo.net','yahoo.co.jp','yahoo-email.com','microsoft.com','microsoft.co.uk', 'trendmicro.com','facebook.com','twitter.com','twitter.co.uk'
well_known_domains	ir.general	alias.host count l-1 && alias.host ends '.apple.com','.adobe.com','.adobe.co.uk','.solaris.com','.cisco.com','.cisco.co.uk','.symantec.com', '.amazon.com','.amazon.cn','.amazon.fr','.amazon.com.br','.amazon.de','.amazon.se','.amazon.es', '.amazon.it','.amazon.co.jp','.amazon.co.uk','.symantecliveupdate.com','.amazonaws.com', '.googlesyndication.com','.google-analytics.com','.googleadservices.com','.googleusercontent.com', '.facebook.net','.images-amazon.com','.doubleclick.net','.akadns.net'

Rule Name	Meta Key	Rule
well_known_domains	ir.general	alias.host count l-1 && alias.host ends '.google.com','.google.com.sg','.google.co.uk','.google.com.ar','.googleapis.com','.googleads.com', '.google.be','.google.ch','.google.com.hk','.google.fr','.google.ru','.google.es','.googlemail.com', '.googlemail.co.uk','.yahoo.com','.yahoo.com.us','.yahoo.co.uk','.yahoodns.net','.yahoo.net', '.yahoo.co.jp','.yahoo-email.com','.microsoft.com','.microsoft.co.uk','.trendmicro.com', '.facebook.com','.twitter.com','.twitter.co.uk'
wget_direct_to_ip	ir.general	client begins 'wget' && alias.host !exists"
xor_exe	ir.alert	risk.warning='xor encoded executable'"
Xtreme_RAT	ir.alert	filename = '1234567890.functions'"
zero_payload	ir.general	streams = 2 && payload = 0 && service != 443,22"

Feeds

Remove the feeds supplied in the IR content pack. All actively supported feeds should be downloaded through Live, and can be searched by Resource Type of **RSA Feed**.

To remove the old IR pack feeds from your Decoders:

1. In the Security Analytics menu, select **Administration > Services**, and select a Decoder.
2. In the **Actions** column, select **View > Config**.
3. Select the **Feeds** tab.
4. Search for feeds that have names beginning with `IR_`, and select only these feeds.
5. Click — to remove the selected feeds.

Original IR feeds to remove
ir_1_advertising_domains
ir_2_possible_malware_ua

Meta Keys

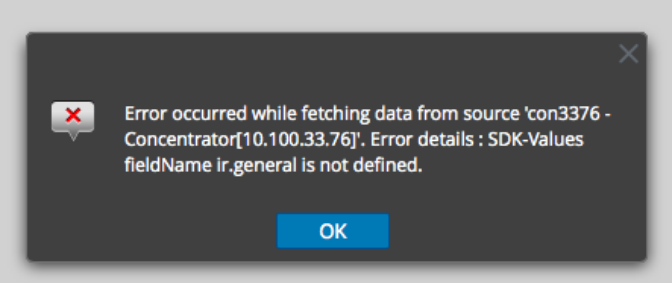
The meta keys that are populated as a result of the IR content pack deployment are listed below. Remove these entries where they exist from the following configuration files:

- index-broker-custom.xml
- index-concentrator-custom.xml
- index-decoder-custom.xml

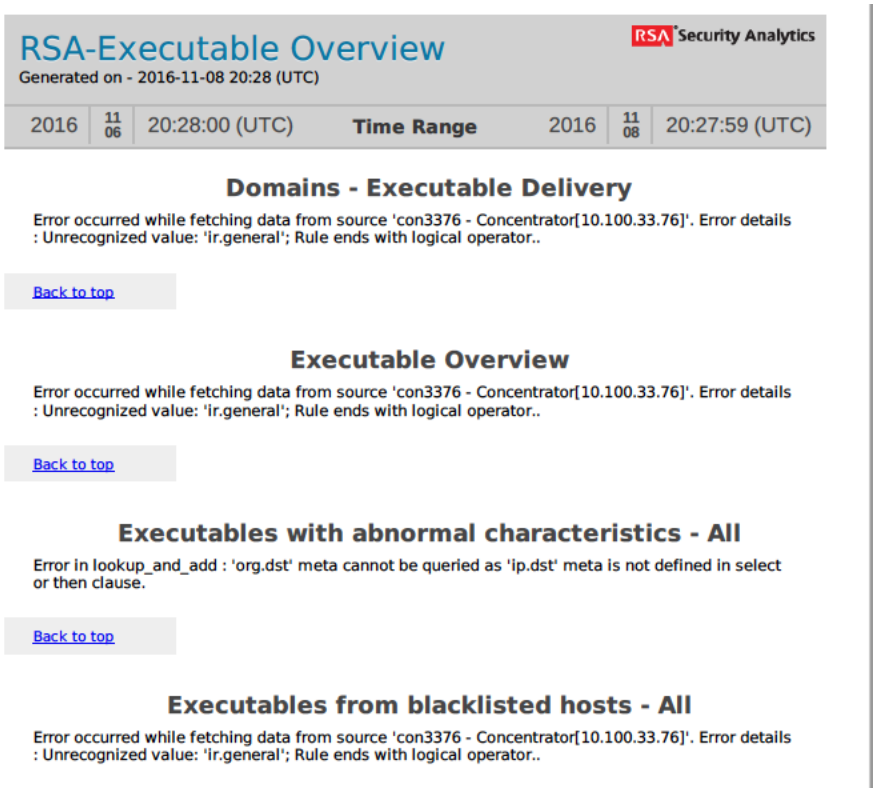
Consequences of Removing Meta Keys

Caution: Historical reports that use meta related to the original IR Content pack will not run if the meta keys listed in the IR Meta Keys section are removed.

If you run a rule that used meta from the IR Content pack, you receive an error similar to the following:



If you run a report that used meta from the IR Content pack, you receive an error similar to the following:



Procedure for Removing Meta Keys

To remove the old IR pack meta keys from your Brokers/Concentrators/Decoders:

1. In the Security Analytics menu, select **Administration > Services**.
2. You will need to do this for your Brokers, Concentrators, and Decoders:
   a. Select the appropriate service (Broker, Concentrator or Decoder).
   b. In the **Actions** column, select **View > Config**.
   c. Select the **Files** tab.
   d. Select the appropriate index file to match the service:
      - `index-broker-custom.xml`
      - `index-concentrator-custom.xml`, or
      - `index-decoder-custom.xml`
   e. Find the meta keys (as listed in the following table), and delete them from the file.

f. Click **Apply** to save your changes.

g. Restart the service to immediately apply the changes, or wait for the next index save.

> **Note:** An index save occurs through either a scheduled task that runs at some interval, usually between 6 to 24 hours, or by the number of sessions received since the last save. See the **Index Saves** section in the **Core DB: Optimization Techniques** topic (https://community.rsa.com/docs/DOC-41597) for more information on this topic).

h. If you have meta groups that use the old keys, proceed to section Update IR Meta Groups to Remove the Old Keys.

i. If you do not have meta groups that use the old keys, and want to immediately remove the deleted keys from use in the UI, restart the **jettysrv**. To restart the jettysrv, SSH in to the Security Analytics Server, and run the following command:

```
restart jettysrv
```

IR Meta Keys

> **Note:** While the following keys should be removed from all 3 index files, the complete text for a key may vary between the 3 index files. Just make sure to remove the complete entry for each of these keys.

```
<!-- IR Keys -->
<key description="IR Alert" format="Text" level="IndexValues" name="ir.alert"
valueMax="10000" />
<key description="IR General" format="Text" level="IndexValues" name="ir.general"
valueMax="10000" />
<!-- IR Feed based Keys -->
<key description="IR Feed" format="Text" level="IndexValues" name="ir.feed"
valueMax="100000" />
<key description="IR MD5" format="Text" level="IndexNone" name="ir.md5" />
<key description="IR Description" format="Text" level="IndexKeys" name="ir.desc" />
<!-- Feeds -->
<!-- Netname -->
<key description="Source NetName" format="Text" level="IndexValues" name="netname.src"
valueMax="1000" defaultAction="Closed"/>
<key description="Destination NetName" format="Text" level="IndexValues" name="netname.dst"
valueMax="1000" defaultAction="Closed"/>
<!-- Parsers -->
<!-- email.url.host (from NW Live) -->
<key description="Email URL Host" format="Text" level="IndexValues" name="email.url.host"
defaultAction="Closed" valueMax="500000"/>
```

```
<!-- email_expanded_parser -->

<key description="Email Mail From" level="IndexValues" name="mailfrom" format="Text"
valueMax="500000" defaultAction="Closed"/>

<key description="Email RCPT To" level="IndexValues" name="rcptto" format="Text"
valueMax="500000" defaultAction="Closed"/>

<key description="Email From" level="IndexValues" name="emailfrom" format="Text"
valueMax="500000" defaultAction="Closed"/>

<key description="Email To" level="IndexValues" name="emailto" format="Text"
valueMax="500000" defaultAction="Closed"/>

<key description="Email X-Mailer" level="IndexKeys" name="emailxmailer" format="Text"
defaultAction="Closed"/>

<key description="Email Mail from Domain" level="IndexValues" name="mailfromdomain"
format="Text" valueMax="500000" defaultAction="Closed"/>

<key description="Email RCPT TO Domain" level="IndexKeys" name="rcpttodomain" format="Text"
defaultAction="Closed"/>

<key description="Email From Display Name" level="IndexKeys" name="fromname" format="Text"
defaultAction="Closed"/>

<!-- full_useragent -->

<key description="User-Agent Extended" format="Text" level="IndexValues" name="agent.ext"
defaultAction="Closed" valueMax="500000" />

<!-- HTTP_headers -->

<key description="HTTP Request Header" format="Text" level="IndexValues" name="http.request"
defaultAction="Closed" valueMax="5000" />

<key description="HTTP Response Header" format="Text" level="IndexValues"
name="http.response" defaultAction="Closed" valueMax="5000" />

<key description="Unique HTTP Request Header" level="IndexKeys" name="req.uniq"
format="Text" defaultAction="Closed"/>

<key description="Unique HTTP Response Header" level="IndexKeys" name="res.uniq"
format="Text" defaultAction="Closed"/>

<!-- Named_Pipe -->

<key description="Pipe Details" level="IndexValues" name="named.pipe" valueMax="10000"
format="Text" defaultAction="Closed"/>

<!-- Advanced RDP -->

<key description="RDP Info" level="IndexValues" name="rdp.info" valueMax="10000"
format="Text" defaultAction="Closed"/>

<!-- TxRx Bytes Parser -->

<key description="Payload Transmit Bytes" level="IndexNone" name="txbytes" format="UInt32"
defaultAction="Closed"/>

<key description="Payload Receive Bytes" level="IndexNone" name="rxbytes" format="UInt32"
defaultAction="Closed"/>

<key description="Payload Transmit Receive Ratio" level="IndexValues" name="bytes.ratio"
format="UInt8" valueMax="101" defaultAction="Closed"/>
```

Update IR Meta Groups to Remove the Old Keys

1. Find meta groups by selecting **Investigation > Navigate** from the NetWitness Suite menu.
2. From the **Meta** drop-down menu, choose **Manage Meta Groups**.
3. If any groups use the old keys, replace them with the appropriate new key—see the Content Mapping of Meta Keys section for details.
4. To remove the old keys so that they are immediately unavailable from the UI, restart the **jettysrv**.
   a. SSH in to the Security Analytics Server.
   b. Run the following command:

   ```
   restart jettysrv
   ```

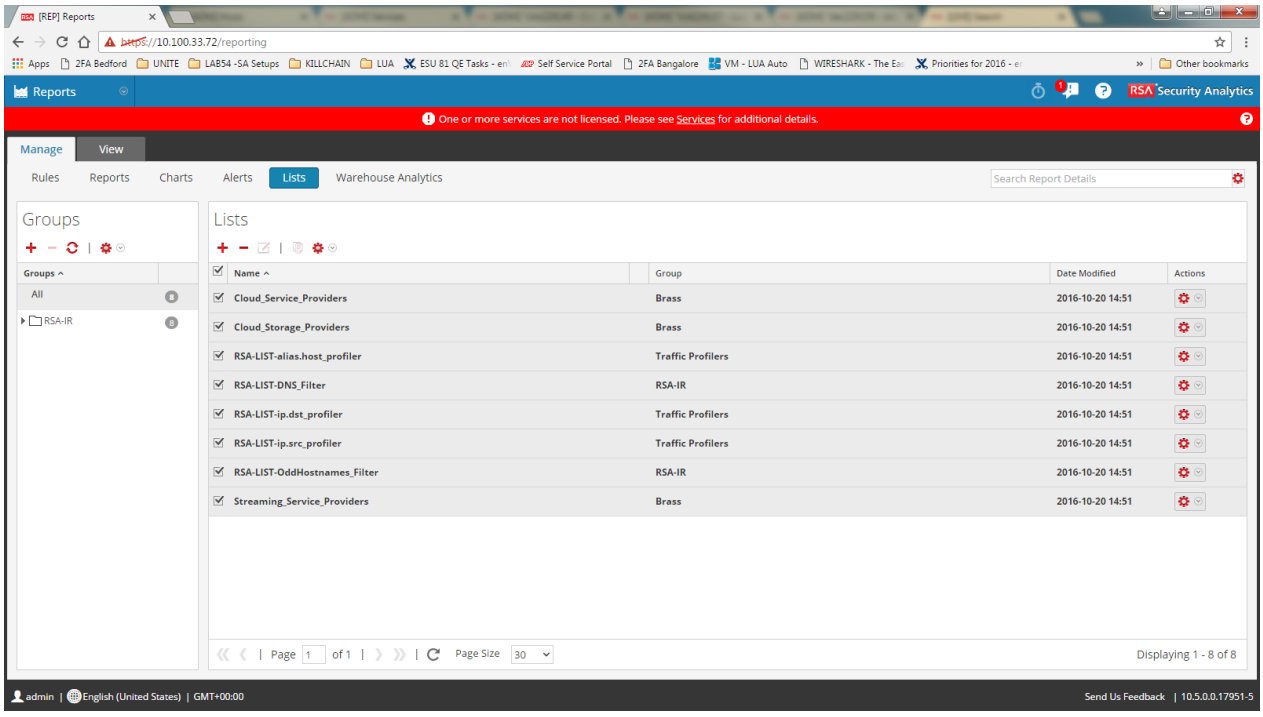
Lists, Rules, and Reports

The reports within the IR Content Pack use meta keys of **ir.general** and **ir.alert**. If you wish to continue using these reports, then use the Content Mapping of Meta Keys table at the end of the document to remap these meta keys and values to the new Hunting Pack. The Hunting Pack will be distributed with two new reports – Hunting Summary and Hunting Details – that use the new metadata, but at a high level.

If you do not wish to continue using the old reports, below are steps to remove them, as well as a full list of items that were provided as part of the IR Content Pack. Remove the Lists, Rules, and then Reports in that order. (There could be dependencies between the three, with reports dependent upon rules, and rules dependent on lists.)

Lists

1. From the Security Analytics menu, select **Reports > Manage**.
2. Select **Lists** from the menu bar.
3. Select the IR content lists as shown here:



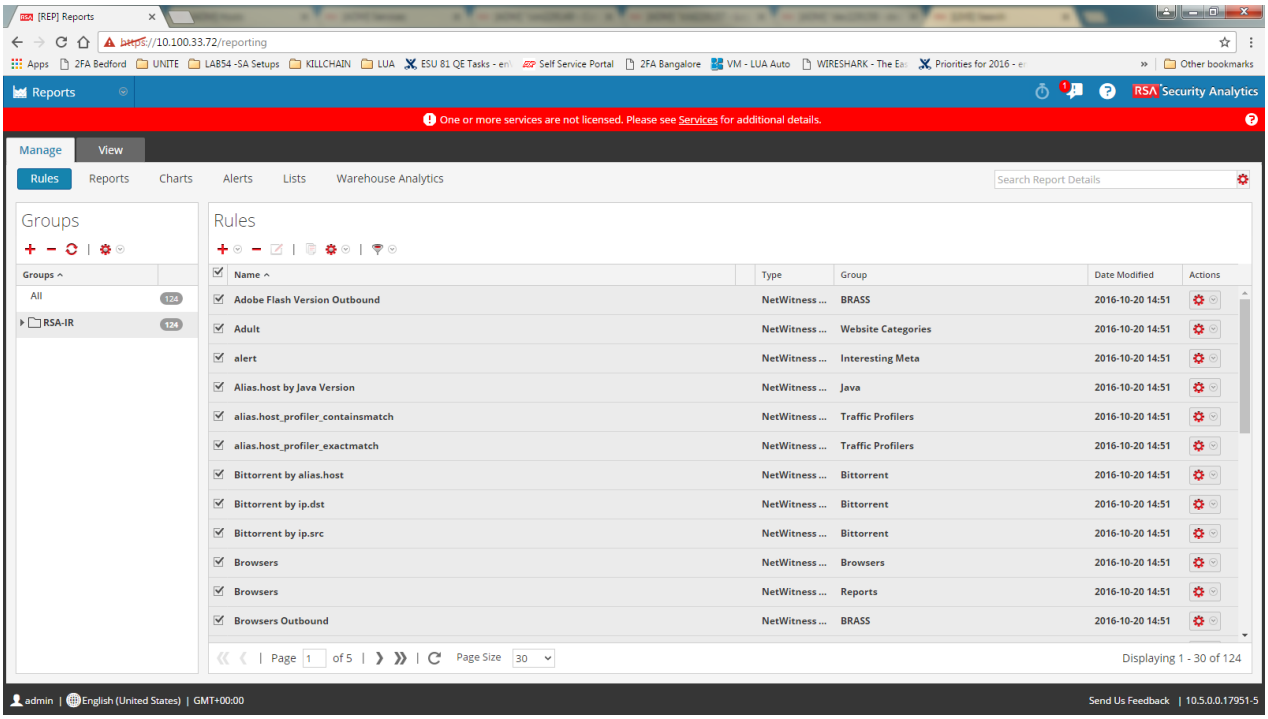
4. Click — to remove the selected lists.

These are the IR content pack Lists:

- Cloud_Service_Providers
- Cloud_Storage_Providers
- RSA-LIST-alias.host_profiler
- RSA-LIST-DNS_Filter
- RSA-LIST-ip.dst_profiler
- RSA-LIST-ip.src_profiler
- RSA-LIST-OddHostnames_Filter
- Streaming_Service_Providers

Rules

1. From the Security Analytics menu, select **Reports > Manage**.
2. Select **Rules** from the menu bar.
3. Select the IR content rules as shown here:



4. Click — to remove the selected rules.

These are the IR content pack Rules:

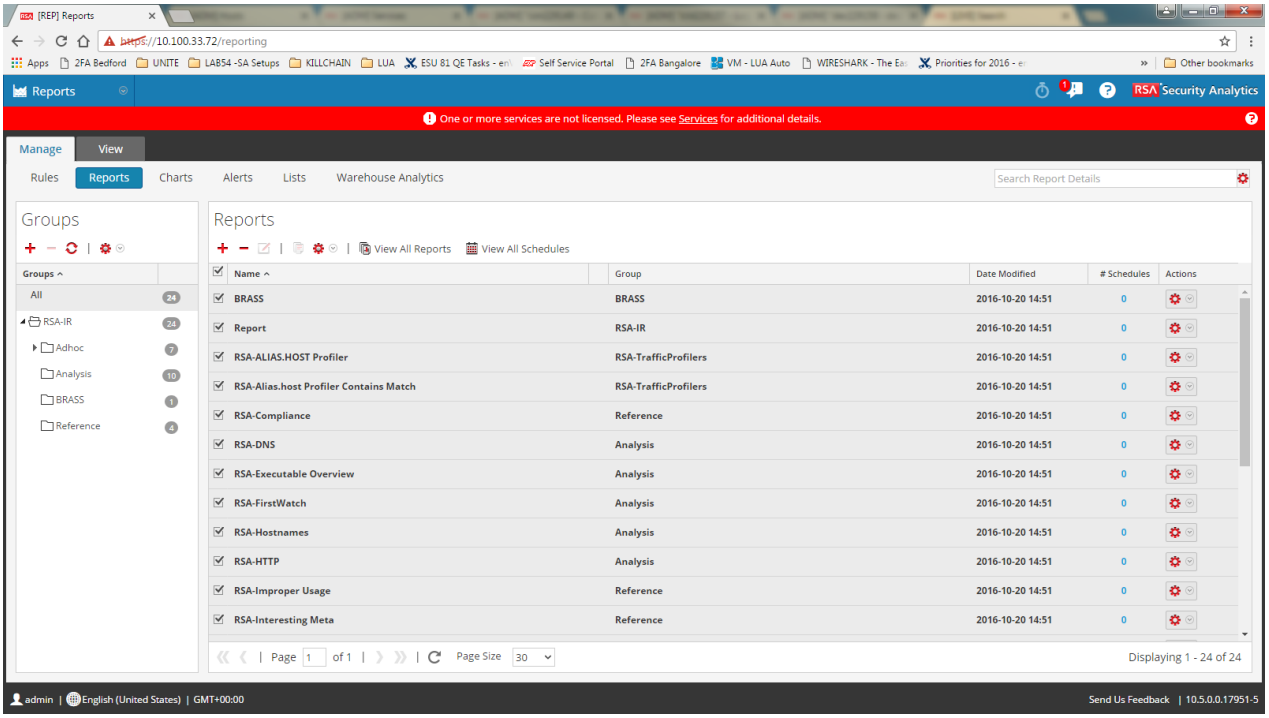
IR content pack Rules	
Adobe Flash Version Outbound	Adult
alert	Alias.host by Java Version
alias.host_profiler_containsmatch	alias.host_profiler_exactmatch
Bittorrent by alias.host	Bittorrent by ip.dst
Bittorrent by ip.src	Browsers
Browsers Outbound	Browsers_1
Compressed_File_Upload	Default Accounts
Default Accounts(1)	Default Passwords
Default Passwords(1)	Destination Country Outbound
DNS Large Number of Authority Records to Loopback IP	DNS Large Number of Authority Records to Loopback IP - Top 15
DNS Large Number of Authority Records without Answer	DNS Large Number of Authority Records without Answer - Top 15
Domains - Executable Delivery	Dynamic DNS by alias.host
Dynamic DNS HTTP by alias.host	Embedded Java Filenames
Executable Overview	Executables from blacklisted hosts - All
Executables with abnormal characteristics - All	ExploitKit Indicator
External DNS Reflection	First Watch - DNS
First Watch - HTTP	First Watch - Non- HTTP_DNS_OTHER
First Watch - OTHER	Ip.dst by Java Version Direct to IP
ip.dst_profiler	ip.src
ip.src_profiler	ip.src_to_alias.host_profiler_containsmatch
ip.src_to_alias.host_profiler_exactmatch	ip.src_to_ip.dst_profiler
ir.alert	ir.general
ir_ona_2013_domain	ir_watchlist_domain_oct2013
Java	Java Outbund
Loopback Traffic Top 50 Talkers	Mobile OS Outbound

IR content pack Rules	
MS Excel Version Outbound	MS Outlook Version Outbound
MS Word Version Outbound	odd_alias.host - DNS
odd_alias.host - HTTP	odd_alias.host - Non-HTTP_DNS
Operating Systems	Operating Systems - Mobile Devices
OS Outbound	Outbound Services over non-standard port by tcp.dstport & alias.host
Outbound Services over non-standard port by tcp.dstport & ip.dst direct to IP	Outbound Services over non-standard port by tcp.dstport & ip.src
Pastebin Overview	Peer to Peer
Plaintext Passwords - Sorted	Plaintext Passwords - Sorted(1)
Risk Info	Risk Suspicious
Risk Warning	Security Tools
Self-Signed-Certs	Services over non-standard port
short_ie_10	short_ie_3
short_ie_4	short_ie_5
short_ie_6	short_ie_7
short_ie_8	short_ie_9
Small Java Class	Small Java Jar
Small_EXE	Src Country Inbound
Streaming Services	Suspicious Domains - DNS
Suspicious Domains - HTTP	Suspicious Domains - Non-HTTP_DNS
suspicious_4headers	suspicious_4headers - Direct to IP
suspicious_6headers	suspicious_6headers - Direct to IP
Suspicious_HTTP	Suspicious_Other_Connections
Suspicious_TCP_Beaconing	Threat Category
Threat Description	Threat Source
Top Cloud Hosting Providers	Top Cloud Storage Providers

IR content pack Rules	
Top Outbound ip.src by Session Count	Top Outbound agent.ext by Session Count
Top Outbound agent.ext by Session Size	Top Outbound alias.host by Session Count
Top Outbound alias.host by Session Size	Top Outbound country.dst by Session Count
Top Outbound country.dst by Session Size	Top Outbound ip.dst by Session Count
Top Outbound ip.dst by Session Size	Top Outbound ip.src by Session Size
Top Outbound org.dst by Session Count	Top Outbound org.dst by Session Size
Top Outbound service by Session Count	Top Outbound service by Session Size
Top Outbound Website Categories by Session Count	Top Outbound Website Categories by Session Size
TOR Exit Node	UA_does_not_begin_Mozilla (Non-Java)
UA_does_not_begin_Mozilla (Non-Java) - Detail	UDP_Overview
Unidentified User Agents Outbound	Watchlist TLD (Get_No_Post)
Watchlist TLD (Post_No_Get)	Windows OS versions Outbound

Reports

1. From the Security Analytics menu, select **Reports > Manage**.
2. Select **Reports** from the menu bar.
3. Select the IR content reports as shown here:



4. Click — to remove the selected reports.

IR content pack Reports	
BRASS	Report
RSA-ALIAS.HOST Profiler	RSA-Alias.host Profiler Contains Match
RSA-Compliance	RSA-DNS
RSA-Executable Overview	RSA-FirstWatch
RSA-Hostnames	RSA-HTTP
RSA-Improper Usage	RSA-Interesting Meta
RSA-IP.DST Profiler	RSA-IP.SRC Profiler
RSA-IP.SRC to ALIAS.HOST Profiler Contains Match	RSA-IP.SRC to ALIAS.HOST Profiler Exact Match
RSA-IP.SRC to IP.DST Profiler	RSA-IR Watchlist
RSA-Java	RSA-Network Activity
RSA-Non-Standard Ports	RSA-Other
RSA-UserAgents	Source Address

Content Mapping of Meta Keys

If you have content built on top of the old IR content pack, it should be rewritten to map to the new meta keys and values.

Unsupported Keys

The following keys are not supported by RSA:

- http.request
- http.response
- req.uniq
- resp.uniq

If you have rules written around any of these keys, we recommend that you contact RSA support for guidance.

Mapping Table

The following table describes these mappings.

Old Meta Key	Meta Key Value	New Meta Key	New Meta Key Value / Details
agent.ext	variable client string	client	For HTTP traffic clients, use service=80 and client exists
bytes.ratio	high	analysis.session	ratio high transmitted
bytes.ratio	medium	analysis.session	ratio medium transmitted
bytes.ratio	low	analysis.session	ratio low transmitted
emailfrom	variable	email.src	An email address indicating the originator of the email message. Disabled by default. Enable this key using the Mail_lua_options file.
emailto	variable	email.dst	An email address indicating the recipient of the email message. Disabled by default. Enable this key using the Mail_lua_options file.
ir.general	rfc1918_src	none	Replaced by Traffic Flow parser
ir.general	suspicious_other	analysis.session	suspicious other
ir.general	bad_org_susp_ other	analysis.session	suspicious other bad org
ir.general	inbound_email	analysis.service	inbound email

Old Meta Key	Meta Key Value	New Meta Key	New Meta Key Value / Details
ir.general	express_x-mailer	None	Replaced by "express x-mailer"
ir.general	interesting_email	analysis.service	interesting email
ir.general	email_fwd	analysis.service	email fwd
ir.general	tld_is_not_com_org_net	analysis.service	tld not com net org
ir.general	subject_phish	analysis.service	subject phish
ir.general	email_re	analysis.service	email re
ir.general	tld_is_com_org_net	none	Was only used to get to "tld_is_not_com_org_net", which was replaced by "tld not com net org"
ir.general	ua_begins_mozilla	none	Was only used to get to "ua_not_good_mozilla", which was replaced by "http nonstandard Mozilla"
ir.general	ua_not_good_mozilla	analysis.service	http not good mozilla
ir.general	ua_non_standard_mozilla	analysis.service	http nonstandard mozilla
ir.general	bad_ssl	analysis.service	bad ssl
ir.general	mozilla_5	none	Was only used to get to "ua_not_good_mozilla", which was replaced by "http nonstandard Mozilla"
ir.general	mozilla_4	none	Was only used to get to "ua_not_good_mozilla", which was replaced by "http nonstandard Mozilla"
ir.general	mozilla_3	none	Was only used to get to "ua_not_good_mozilla", which was replaced by "http nonstandard Mozilla"
ir.general	http_direct_to_ip	analysis.service	http direct to ip request
ir.general	exe_under_75K	analysis.file	exe under 75k
ir.general	exe_under_5K	analysis.file	exe under 5k
ir.general	!top20dst	analysis.session	not top 20 dst
ir.general	short_filename	none	Was only used to get to one of the "web_susp_act" meta: that particular variation was replaced by "http post no get short filename suspicious extension."
ir.general	well_known_domains	none	was only used to get to "suspiciously_named_domains", which was replaced by "suspiciously named domain"
ir.general	odd_alias.host	none	Was only used to get to "odd_alias.host", which was replaced by "hostname consecutive consonants"
ir.general	invalid_alias.host	analysis.service	hostname invalid
ir.general	direct_to_ip_one_char_php	analysis.service	direct to ip one char php
ir.general	one_char_php_filename	None	Was only used to get to "direct_to_ip_one_char_php", which was replaced by "direct to ip one char php"

Old Meta Key	Meta Key Value	New Meta Key	New Meta Key Value / Details
ir.general	potential_beacon	analysis.session	potential beacon
ir.general	outbound_syslog	analysis.session	outbound syslog
ir.general	suspicious_traffic_over_53	analysis.service	suspicious traffic port 53
ir.general	large_session_dns_port	analysis.service	large session dns port
ir.general	large_dns_service	analysis.service	large session dns service
ir.general	icmp_tunnel	analysis.session	icmp tunnel
ir.general	icmp_large_session	analysis.session	icmp large session
ir.general	wget_direct_to_ip	analysis.service	http wget direct to ip
ir.general	suspiciously_named_domains	analysis.service	suspiciously named domain
ir.general	outbound_dns	analysis.service	outbound dns
ir.general	POST_no_GET_no_REFER_DIRECTtoIP	analysis.service	http post no get no referer directtoip
ir.general	Netbox_Server	analysis.service	http netbox server
ir.general	webshell_indicator_no_http_error	analysis.service	http webshell no error
ir.general	webshell_indicator_http_error	analysis.service	http webshell errortld
ir.general	webshell_indicator	analysis.service	http webshell
ir.general	web_susp_act_direct_to_ip	none	This meta key was identical to "web_susp_act_direct_to_ip" app rule.
ir.general	web_susp_act_alias.host	none	Any set of conditions which resulted in "web_susp_act," which was also a direct-to-ip request, resulted in this meta. There is no direct replacement.
ir.general	web_susp_act	none	There were several of these, each was replaced with more specific and descriptive values (for example, "http post no get short filename suspicious extension")
ir.general	top20dst	none	Was only used to get to "!top20dst", which was replaced by "not top 20 dst"
ir.general	odd_domain_filter	none	Was only used to get to "suspiciously_named_domains", which was replaced by "suspiciously named domain"
ir.general	POST_no_GET_No_REFER	analysis.service	http post no get no referer
ir.general	session_size_100-250k	analysis.session	session size 100-250k

Old Meta Key	Meta Key Value	New Meta Key	New Meta Key Value / Details
ir.general	exe_under_10k	analysis.file	exe under 10k
ir.general	session_size_10-50k	analysis.session	session size 10-50k
ir.general	four_or_less_ headers	analysis.service	http four or less headers
ir.general	session_size_50-100k	analysis.session	session size 50-100k
ir.general	four_http_headers	analysis.service	http four headers
ir.general	three_http_headers	analysis.service	http three headers
ir.general	two_http_headers	analysis.service	http two headers
ir.general	http_connect	analysis.service	http connect
ir.general	http_post_and_get	analysis.service	http post and get
ir.general	http_get_no_post	analysis.service	http get no post
ir.general	http_post_no_get	analysis.service	http post no get
ir.general	one_two_ filename_java_ class	analysis.file	one two filename java class
ir.general	small_java_class	analysis.file	small java class
ir.general	six_or_less_ headers	analysis.service	http four or less headers
ir.general	small_java_jar	analysis.file	small java jar
ir.general	java_1.7	analysis.service	http java 1.7
ir.general	java_1.6	analysis.service	http java 1.6
ir.general	java_1.5	analysis.service	http java 1.5
ir.general	java_1.4	analysis.service	http java 1.4
ir.general	java_1.3	analysis.service	http java 1.3
ir.general	exe_filetype	analysis.file	exe filetype
ir.general	zero_payload	analysis.session	zero payload
ir.general	single_sided_udp	analysis.session	single sided udp
ir.general	single_sided_tcp	analysis.session	single sided tcp
ir.general	suspicious_tcp_ beaconing	boc	suspicious tcp beaconing

Old Meta Key	Meta Key Value	New Meta Key	New Meta Key Value / Details
ir.general	inbound_traffic	analysis.session	inbound traffic **Note:** "inbound traffic" is only for inbound traffic that contains a payload. While "inbound" from the traffic flow parser will create meta for all inbound sessions, without consideration of whether or not the session contains payload.
ir.general	java_1.8	analysis.service	http java 1.8
ir.general	suspicious_ 4headers	analysis.service	http suspicious 4 headers
ir.general	suspicious_ 6headers	analysis.service	http suspicious 6 headers
ir.general	Suspicious_ Connect	analysis.service	http suspicious connect
ir.general	session_size_5-10k	analysis.session	session size 5-10k
ir.general	session_size_0-5k	analysis.session	session size 0-5k
ir.general	long_connection	analysis.session	long connection
ir.general	exe-filetype_ but_!exe-ext	analysis.file	exe filetype but not exe extension
ir.general	rfc1918_dst	none	Replaced by Traffic Flow parser
ir.general	exe-ext_but_!exe-filetype	analysis.file	exe extension but not exe filetype
ir.general	watchlist_org.dst	analysis_section	watchlist dst
ir.general	possible_ exploitkit_ indicator	analysis.service	http possible exploitkit
ir.general	ie_short_ua	analysis.service	http short user-agent ie
ir.general	short_ie_11	analysis.service	http short user-agent ie
ir.general	first_carve_!dns	analysis.session	first carve !dns
ir.general	short_ie_10	analysis.service	http short user-agent ie
ir.general	short_ie_8	analysis.service	http short user-agent ie
ir.general	short_ie_7	analysis.service	http short user-agent ie
ir.general	short_ie_6	analysis.service	http short user-agent ie
ir.general	short_ie_5	analysis.service	http short user-agent ie
ir.general	short_ie_4	analysis.service	http short user-agent ie
ir.general	short_ie_3	analysis.service	http short user-agent ie
ir.general	mid_ua	analysis.service	http mid length user-agent
ir.general	short_ua	analysis.service	http short user-agent

Old Meta Key	Meta Key Value	New Meta Key	New Meta Key Value / Details
ir.general	max_length_ua	analysis.service	http max length user-agent
ir.general	long_ua2	none	Replaced by "http long user-agent"
ir.general	long_ua	analysis.service	http long user-agent
ir.general	short_ie_9	analysis.service	http short user-agent ie
ir.general	first_carve	analysis.session	first carve
rdp.info	Value of variable connection types of: [1] = "Modem", [2] = "Low-Speed Broadband", [3] = "Satellite", [4] = "High-Speed Broadband", [5] = "WAN", [6] = "LAN", [7] = "AUTODETECT"	analysis.service	Same as value for **rdp.info**
risk.info	outbound_traffic	direction	outbound
risk.info	long_http_query	analysis.service	http long query
risk.info	watchlist_file_ fingerprint	analysis.service	watchlist file fingerprint
risk.info	watchlist_file_ extension	analysis.service	watchlist file extension
risk.info	http direct to ip request	analysis.service	http direct to ip request
risk.info	watchlist_ports	analysis.session	watchlist port
risk.suspicious	direct to ip http request	analysis.service	http direct to ip request
rxbytes	variable	responsepayload	Represents the number of payload bytes in the request stream.
txbytes	variable	requestpayload	Represents the number of payload bytes in the request stream.