RSA enVision Content 2.0

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: **www.rsa.com**

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.rsa.com/legal/trademarks_list.pdf**.

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.

Contents

RSA enVision Version 2.0 Event Sources

Content 2.0 features new tables and improvements to the parsing of event data into variables in those new tables.

For rules and reports, note the following:

- For factory reports, as existing event sources are converted to Content 2.0, their device-specific reports are updated to work with the new content. In some cases, class-specific reports have replaced device-specific reports.
- Factory correlated rules have been modified to take advantage of the improved tables, variables and parsing.
- Custom rules, that involve event sources updated to work with Content 2.0, need to be rewritten.
- Custom reports may not produce the same results as previously. For guidance on updating custom reports, see the accompanying table documentation and the *RSA enVision Content Inspection Tool* guide.

For details on a specific event source, see the Configuration topic for the event source.

Content 2.0 Notes

- The Event Source Update makes available several Content 2.0 event source updates. If you select updates to event sources in the interactive Installer window, a second screen asks if the Content 2.0 version of the event sources are to be delivered.
- Once Content 2.0 has been delivered for an event source, you must follow manual steps to roll back to the V1.0 content. For details, see the How to Roll Back ESU topic in the Help. Additionally, you may need to reindex your data.
- For existing event source types converted to Content 2.0, events collected before the conversion must be reindexed using the RSA enVision lsmaint command.

Note: The lsmaint command does not reindex events being collected during the current GMT day, so you must reindex those events on the next GMT day. For details, see the lsmaint command in the enVision Help.

Content 2.0 Event Sources

The following table shows the status of event source conversion to Content 2.0.

Total Content 2.0	225
Remaining	55
Total Devices	281
Percentage Content 2.0	80.4%

Currently, 75.6% of the event source library has been converted to Content 2.0. The following event sources have been updated to use Content 2.0.

Manufacturer	Event Source	Content 2.0 Table
ActivIdentity	4TRESS AAA Server	Access
Airmagnet	Enterprise	Network
Apache	HTTP Server	Web
Apache	Tomcat	Web
Application Security	DBProtect	Database
Arbor Networks	Peakflow SP5	Network
Aruba Networks	Mobility Controller	Network
Astaro	Security Gateway	Firewall
Avocent	IP KVM	Network
Barracuda Networks	Spam Firewall	Malware
Barracuda Networks	Web Application Firewall	Application Firewall
BigFix	BigFix Enterprise Suite	Configuration Man-

Manufacturer	Event Source	Content 2.0 Table
		agement
Blue Coat	ProxySG SGOS	Web
Brocade	FabricOS	Network
Brocade	Fast Iron Switch	Network
CA	Integrated Threat Management	Malware
CA	Siteminder	Malware
CheckPoint	IPSO	Unix
CheckPoint	FW-1	Firewall
Cisco	ACE	Network
Cisco	Adaptive Security Appliance	Firewall
Cisco	CiscoWorks NCM	Configuration Management
Cisco	IPS	Intrusion
Cisco	IronPort C-Series (ESA)	Application Firewall
Cisco	IronPort S-Series (WSA)	Web
Cisco	LAN Management Solution	Configuration Management
Cisco	MARS	Analysis
Cisco	Mobility Services Engine	Network
Cisco	NAC	Access
Cisco	Nexus	Network
Cisco	PIX	Firewall
Cisco	Router / IOS Firewall	Network

Manufacturer	Event Source	Content 2.0 Table
Cisco	Secure ACS Express	Access
Cisco	Secure IDS	Intrusion
Cisco	Security Agent	Intrusion, Malware, DLP
Cisco	Security Manager	Configuration Management
Cisco	UCS Manager	Configuration Management
Cisco	Wireless LAN Controller	Network
Citrix	Access Gateway	Access
Citrix	NetScaler	Application Firewall
Citrix	XenApp v5	Virtualization
CyberArk	Enterprise Password Vault, Inter-Business Vault, and Sensitive Document Vault	Access
CyberGuard	Firewall	Firewall
CyberGuard	Classic Firewall	Firewall
Dell	DRAC	Access
Dell	PowerConnect 5324 Switch	Network
eEye	Blink Endpoint Protection	Intrusion
eEye	REM Security Management Console	Intrusion
eEye	Retina Scanner	Intrusion
EMC	Avamar	Storage
EMC	Celerra	Storage, Windows
EMC	Clariion / VNX	Storage

Manufacturer	Event Source	Content 2.0 Table
EMC	Data Protection Advisor	Analysis
EMC	Documentum	Database
EMC	Ionix UIM	Configuration Management
EMC	Symmetrix	Storage
EMC	Voyence	Access
Enterprise IT	SF-NoEvasion	Mainframe
Enterasys Networks	Dragon	Intrusion
Enterasys Networks	Switch	Network
F5	Big-IP LTM	Network
F5	Big-IP APM	Application Firewall
F5	Big-IP ASM	Application Firewall
F5	Firepass SSL VPN	VPN
FairWarning	Privacy Monitoring	Analysis
Fortinet	FortiGate	Firewall, Web, Vulnerability, Malware, DLP, Intrusion, Messaging
Fortinet	FortiMail	Application Firewall
HP	Open VMS	Midrange
HP	ProCurve Switch	Network
HP	TippingPoint SMS	Intrusion
HP	UX	UNIX

Manufacturer	Event Source	Content 2.0 Table
HyTrust	HyTrust	Configuration Management, Access
IBM	AIX	UNIX
IBM	DB2 UDB	Database
IBM	Guardium SQL Guard	Application Firewall
IBM	ISS SiteProtector	Intrusion
IBM	Lotus Domino	Messaging
IBM	Mainframe IDMS	Mainframe
IBM	Mainframe IMS	Mainframe
IBM	Mainframe RACF	Mainframe
IBM	TAM	Access
IBM	TAM WebSEAL	Access, Web
IBM	TIM	Access
IBM	WebSphere	Application Server
Imperva	SecureSphere	Application Firewall
Infoblox	NIOS	Network
Ipswitch	WhatsUp Gold	Configuration Management
Juniper Networks	Networks Infranet Controller 4500	Access
Juniper Networks	JUNOS	Network
Juniper Networks	NetScreen	Firewall

Manufacturer	Event Source	Content 2.0 Table
Juniper Networks	NetScreen-Security Manager	Firewall, Intrusion, VPN Configuration Management
Juniper Networks	Steel-Belted Radius	Access
Juniper Networks	SSL VPN	VPN
Kaspersky	Total Space Security, Business Space Security, Enterprise Space Security	Malware
Lancope	StealthWatch	Intrusion
Lumension	Endpoint Security	Configuration Management
ManageEngine	Netflow Analyzer	Analysis
Mazu Networks	Mazu Profiler	Intrusion
McAfee	DLP	DLP
McAfee	Email Gateway	Application Firewall
McAfee	Endpoint Encryption	Access
McAfee	Host Intrusion Prevention	Intrusion
McAfee	ePolicy Orchestrator	Configuration Management, Malware
McAfee	Network Access Control	Access
McAfee	Firewall Enterprise	Firewall
McAfee	Network Security Platform (formerly Intrushield)	Intrusion
McAfee	Policy Auditor	Configuration Man-

Manufacturer	Event Source	Content 2.0 Table
		agement
McAfee	Reconnex	DLP
McAfee	VirusScan	Malware
McAfee	Vulnerability Manager (formerly Foundscan)	Vulnerability
McAfee	Web Gateway	Web
McKesson	Horizon Patient Folder	Storage
Microsoft	Audit Collection Services	Windows
Microsoft	DHCP Server	Application Server
Microsoft	Exchange Server	Messaging
Microsoft	Forefront Client	Malware
Microsoft	Forefront TMG / ISA	Firewall, Web
Microsoft	Forefront Unified Access Gateway	VPN
Microsoft	IIS	Web
Microsoft	SCCM	Configuration Management
Microsoft	System Center Operations Manager	Configuration Management
Microsoft	SQL Server	Database
Microsoft	Windows	Windows
Microsoft	Windows Server Update Service	Windows
Motorola	AirDefense Enterprise	Intrusion
MySQL	MySQL Enterprise	Database
NetWitness	NextGen	Network

Manufacturer	Event Source	Content 2.0 Table
Network Appliance	Data ONTAP	Storage
NFR	NIDS	Intrusion
Oracle	Database	Database
Oracle	Database Vault	Access
Oracle	Identity Manager	Access
Oracle	Internet Directory	Access
Oracle	iPlanet Web Server	Web
Oracle	WebLogic	Application Servers
Open Source	NFDump	Network
Open Source	Squid	Web
Palo Alto Networks	Firewall	Firewall
Radware	DefensePro	Intrusion
Rapid7	Nexpose	Vulnerability
Redhat, Novell, Debian	Linux	UNIX
RIM	Blackberry Enterprise Server	Messaging
RSA	Access Manager	Access
RSA	Adaptive Authentication (OnPrem)	Access
RSA	Authentication Manager and UCM	Access
RSA	Certificate Manager	Access
RSA	DLP	DLP

Manufacturer	Event Source	Content 2.0 Table
RSA	FIM	Access
RSA	Key Manager	Access
Safend	Protector	Configuration Management
Safestone	DetectIT	Analysis
Secude	Security Intelligence	Analysis
Sourcefire	SNORT/Defense Center	Intrusion
SonicWALL	Email Security	Application Firewall
SonicWALL	Global Management System	Configuration Management
Sophos	Enterprise Console	Malware
Sun	SunOne LDAP	Access
Sun	Solaris	UNIX
Sun	Solaris Basic Security Model (BSM)	UNIX
Sybase	Adaptive Server Enterprise	Database
Symantec	Critical Systems Protection	Intrusion
Symantec	DLP	DLP
Symantec	Endpoint Protection	Malware
Symantec	Intruder Alert	Intrusion
Tenable	Nessus	Intrusion
Trend Micro	Deep Security	Application Firewall
Trend Micro	IMSS	Application Firewall
Trend Micro	IWSS	Application Firewall

Manufacturer	Event Source	Content 2.0 Table
Trend Micro	OfficeScan and Control Manager	Malware
Trend Micro	OSSEC	Intrusion
Trend Micro	Scanmail	Application Firewall
Tripwire	Enterprise	Configuration Management
Varonis	DatAdvantage	Access
VMware	ESX/ESXi	Virtualization
VMware	vCenter	Virtualization
VMware	vCloud	Configuration Management
VMware	View	Virtualization
VMware	vShield	Firewall
Websense	Web Security	Web

Table Mappings to Content 2.0

Standard content for RSA enVision contains numerous tables. As part of the process of converting to Content 2.0, the number of tables has been reduced, so that the data for each event source class can reside (for the most part) in a single table. There is a many-to-one mapping from the standard tables to the Content 2.0 tables.

Note: Tables marked as **FUTURE** are not yet released.

Standard Table	Content 2.0 Table
Access Control	Access
Access Control Accounting	Access
Access Control Security	Access
Access Control System	Access
Antivirus	Malware
Checkpoint Audit Logs	Firewall
Configuration Management Configuration Changes	Configuration Management
Configuration Management Level	Configuration Management
Configuration Management System	Configuration Management
Configuration Management User Activity	Configuration Management
Database Audit	Database
Database System	Database
Email Accounting	Messaging
FireWall AAA Authentication	Firewall
FireWall Accounting	Firewall
FireWall Blocked URL	Firewall
FireWall Email Security	Firewall

Standard Table	Content 2.0 Table
FireWall Level	Firewall
FireWall Security	Firewall
FireWall System	Firewall
FireWall URL Requests	Firewall
Global	Universal (4.1 only)
Intrusion Detection System	Intrusion
IPS Accounting	Intrusion
IPS Intrusion	Intrusion
IPS Security	Intrusion
IPS System	Intrusion
ISDN	Network
iSeries Audit	Midrange
Mainframe Accounting	Mainframe
Mainframe Security	Mainframe
Mainframe System	Mainframe
Router Accounting	Network
Router FW Bytes	Network
Router FW Security	Network
Router Interface	Network
Router Level	Network
Router Security	Network
Router System	Network

Standard Table	Content 2.0 Table
Storage Accounting	Storage
Storage Activity	Storage
Storage Level	Storage
Storage System	Storage
Switch Authentication	Network
Switch System	Network
Unix Accounting	Unix
Unix Authentication	Unix
Unix Level	Unix
Unix Security	Unix
Unix System	Unix
VPN Accounting	VPN
VPN Level	VPN
VPN Message	VPN
VPN Security	VPN
VPN System	VPN
Web Accounting	Web
Windows Accounting	Windows
Windows Level	Windows

Content 2.0 Tables

The following tables exist for storing Content 2.0 data.

- Access Table
- Analysis Table
- Application Firewall Table
- Application Server Table
- Configuration Management Table
- Database Table
- Data Loss Prevention Table
- Firewall Table
- Intrusion Table
- Mainframe Table
- Malware Table
- Messaging Table
- Midrange Table
- Network Table
- Storage Table
- Universal Table
- Unix Table
- Virtualization Table
- Virtual Private Network Table
- Vulnerability Table
- Web Table
- Windows Table

Note the following information concerning the Content 2.0 tables:

- The Universal table is a superset of all the tables and variables used for parsing data from event source logs. To better understand the usage and organization of the columns in the Universal table, refer to each of the variable categories, Content 2.0 Variables.
- The table descriptions contain both column and variable names.
  - Column names are displayed in the RSA enVision UI. You can use the column names to set filters for the standard reports.
  - Variable names are used by the report definition files. You can use the variable names to construct the XML report definitions for custom reports.
- The column names in the table descriptions are presented in the same order as they are displayed in the RSA enVision UI.

Access

Below is a list of access variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
Date/Time	stamp	RESERVED	
MessageID	msg_id	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the	

Column Name	Variable Name	Description	Indexed
		RSA enVision Enhanced Categorization Tagging guide. Note: Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. Note: Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. Note: Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. Note: Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or time of the occurrence of the event as recorded	Yes

Column Name	Variable Name	Description	Indexed
		by the system that generated it.	
EventTimeString	event_time_string	Date or time of the occurrence of the event as recorded by the system that generated it. **Note:** This field should be used if the format of the raw log data does not conform to RSA configuration specifications for the event source.	Yes
EventLog	event_log	Name of the event log.	
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
EventType	event_type	The event category type as specified by event source generator.	
ConnectionID	connectionid	Connection ID.	
Session	sessionid	Session ID.	
LinkedSessionID	sessionid1	Linked (related) session ID.	
OperationID	operation_id	An alert number or operation number. A common use case would be to reference a vendor event number.	

Column Name	Variable Name	Description	Indexed
		Note: The values should be unique and non-repeating.	
ReferenceID	id	Event or message ID.	Yes
Action	action	The action taken or proposed to be taken. **Note:** For Databases, this is the SQL Query Statement.	Yes
Disposition	disposition	The end state of the action.	Yes
ResultCode	resultcode	Result (error) code. **Note:** This field is numeric.	Yes
Result	result	Result (error) string.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact, relative to other events.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column. **Note:** This column should be used only if the info column is also required.	
SourceAddress	saddr	Source IP address.	Yes
SourceAddressv6	saddr_v6	Source IPv6 address.	Yes

Column Name	Variable Name	Description	Indexed
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	
TranslatedSourceAddress	stransaddr	The translated source address	
SourceMacAddress	smacaddr	Source MAC address.	
DestinationAddress	daddr	Destination address.	Yes
DestinationAddressv6	daddr_v6	Destination IPv6 address.	Yes
DestinationPort	dport	Destination port.	Yes
DestinationHostName	dhost	Destination hostname.	
DestMacAddress	dmacaddr	Destination MAC address.	
Protocol	protocol	IP protocol name.	
NetworkService	network_service	The name of the network service. **Note:** Some services comprise multiple ports.	
Direction	direction	Direction of the network flow (for the systems that capture this).	
TypeOfService	tos	The priority given to a network protocol.	

Column Name	Variable Name	Description	Indexed
DeviceMacAddress	macaddr	Event Source MAC address.	
IPAddress	hostip	Event Source IP address.	Yes
NetworkPort	network_port	Network port. **Note:** This variable should be used to capture protocol port information, but only in the case where there is no inherently implied network communication occurring.	Yes
HostName	hostname	Hostname. **Note:** This hostname should be fully qualified.	Yes
EventComputer	event_computer	The hostname or IP address of the system that originally generated the event. This variable may be used in situations where a log relay is in place and the hostname variable is referring to the relay.	
FQDN	fqdn	Fully qualified domain name.	
OwnerName	owner	The identity name of the owner of an object. For example, file, directory, and policy.	
Administrator	administrator	Administrative user name.	Yes
Username	username	Account name.	Yes

Column Name	Variable Name	Description	Indexed
DomainName	domain	Domain name.	
UserID	uid	The unique user identifier that is associated with the username.	Yes
ClientUserName	c_username	Client user name. For example, a user name on the client (source) referenced in the event, but not the actual event source.	Yes
LogonID	logon_id	Unique identifier for an account.	Yes
Group	group	Group name.	Yes
Duration	duration	Duration of the event in minutes.	
DurationString	duration_string	A text string version of the duration.	
StartTime	starttime	Start time of the event. **Note:** If you use this variable, you must also use **event_time**.	
EndTime	endtime	End time of the event.	
ExpirationTime	expiration_time	A timestamp that explicitly refers to an expiration.	
EffectiveTime	effective_time	The effective time referenced by the individual event. Must be a timestamp format.	

Column Name	Variable Name	Description	Indexed
RecordedTime	recorded_time	The event time as recorded by the system the event is collected from. For example, a multi-tiered application where the management layer of the system records its own timestamp at the time of collection from its child nodes. **Note:** This variable must be in timestamp format.	
TimeZone	timezone	A time zone name or offset value.	
EventUser	event_user	The user that created the event or the user that is the subject of the event. It should not be the user that is the actor in the event.	
EventState	event_state	The current state of the object or item referenced within the event.	
LinkedReferenceID	id1	Linked (related) event/message ID.	
LinkedReferenceID2	id2	Second linked event/message ID. It can be linked to id or id1 but should not be used unless the other two variables are being used.	
AccessListNo	listnum	Access list number.	
PolicyID	policy_id	Policy ID. This is a numeric field.	
PolicyName	policyname	Policy name.	Yes

Column Name	Variable Name	Description	Indexed
PolicyValue	policy_value	The contents of the policy itself. **Note:** This should contain the details of what the policy does.	
PolicyVersion	policy_version	The version identifier for the policy, or configuration, of the device or application.	
RiskNumber	risk_num	Risk value for event logs that produce a risk metric. **Note:** You cannot typically relate risk values produced by separate products.	
Rule	rule	Rule number.	Yes
RuleName	rulename	Rule name. **Note:** This variable is not always populated. Many products only record a rule number and not an associated descriptive rule name.	Yes
RuleGroup	rule_group	The name of a grouping of rules. **Note:** This grouping should relate rule names and/or rule numbers.	
RuleGroupID	rule_groupid	Rule group ID.	

Column Name	Variable Name	Description	Indexed
RuleTemplate	rule_template	A default set of parameters which overlays onto a rule or rule name which effectively constitutes a template.	
AuditObject	audit_object	The name, or identifier, of the object that is subject of the audit event.	
TriggerValue	trigger_val	The conditions that caused an event to be recorded, for example, an exceeded threshold.	
TriggerDesc	trigger_desc	Description of the trigger condition.	
Info	info	Additional event information that could not be captured in a separate column.	
ProtocolDetail	protocol_detail	IP protocol details. **Note:** For protocols that do not contain details such as ports, this variable is the place to capture that information.	
NodeName	node	Node name. A common use case is the node name within a cluster where the cluster name is reflected by the hostname. In configuration management systems, this variable would store the name of the event source being managed.	
VLAN	vlan	VLAN number.	
Version	version	Version of the application or OS that is generating the	

Column Name	Variable Name	Description	Indexed
		event.	
HostID	hostid	Host identifier.	
PortName	portname	Physical or logical port connection, for example, a printer port name.	
Terminal	terminal	Terminal.	
LogonType	logon_type	The type of logon. **Note:** Some systems record a value for the level in which a logon was performed (interactive vs non-interactive).	Yes
Realm	realm	Radius realm, or similar grouping of accounts.	Yes
DistinguishedName	dn	X.500 (LDAP) distinguished name.	
SourceDistinguishedName	src_dn	An X.500 (LDAP) distinguished name that is used in a context that indicates a source.	
DestinationDistinguishedName	dst_dn	An X.500 (LDAP) distinguished name that is used in a context that indicates a destination.	
AuthenticationMethod	authmethod	Authentication mechanism.	
Privilege	privilege	The privilege level or attributes recorded.	Yes

Column Name	Variable Name	Description	Indexed
ServiceAccount	service_account	The name (including domain if applicable) of the account under which a service (referenced in the event) is running.	
UserRole	user_role	The account or group name under which the user's action is being performed.	Yes
UserFullName	user_fullname	The full name of a user. **Note:** This variable is sometimes called Real Name.	Yes
UserAddress	user_address	User e-mail address.	Yes
UserOrganization	user_org	User organization.	Yes
FederatedIdentityProvider	federated_idp	The Federated Identity Provider. **Note:** This item is the server providing the authentication.	
FederatedServiceProvider	federated_sp	The Federated Service Provider. **Note:** This item is the application requesting authentication.	
Category	category	Category name.	Yes
GroupID	groupid	Group ID number related to the group name.	

Column Name	Variable Name	Description	Indexed
GroupObject	group_object	A collection or grouping of entities. **Note:** This variable is not specific to authentication.	
PoolID	pool_id	The identifier of a resource pool. **Note:** This field is typically numeric.	
Agent	agent	Agent that processes a portion of the event.	
Application	application	The name of the application (software).	
Product	product	The name of the product. **Note:** This name can be for either software or hardware.	
Service	service	A software daemon or service. **Note:** This item is a resident version of an application.	
Parameters	param	Parameters passed as part of a command or application.	
ProcessID	process_id	Process ID number.	
Process	process	Process name.	
DataType	data_type	The classification type of the data that is the subject of the event referenced.	

Column Name	Variable Name	Description	Indexed
DatabaseName	db_name	The database name.	
InstanceName	instance	Instance name.	
ObjectType	obj_type	Object type.	
ObjectName	obj_name	Name of the object. **Note:** You must use **obj_type** to describe what type of object this is.	
Directory	directory	Directory name. **Note:** This is a file directory, not LDAP.	
FileName	filename	Document or file name.	Yes
Method	web_method	Web method. For example, POST or GET.	
URL	url	Uniform Resource Locator.	
WebHost	web_host	The hostname used in the web request.	
WebPage	webpage	Web page.	
Referer	web_referer	Request header referral.	

Column Name	Variable Name	Description	Indexed
WebCookie	web_cookie	The cookies passed within a web request.	
ChangeAttribute	change_attribute	The change attribute.	
ChangeOldValue	change_old	The prior value of an attribute or object in a change event.	
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	
Bytes	bytes	Total bytes.	
SentBytes	sbytes	Bytes sent.	
ReceivedBytes	rbytes	Bytes received.	
Counter1	dclass_counter1	Event source class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	
Counter2	dclass_counter2	Event source class counter 2.	
Counter2String	dclass_counter2_string	A descriptive string that provides information about the **Counter2** value.	
Counter3	dclass_counter3	Event source class counter 3.	
Counter3String	dclass_counter3_string	A descriptive string that provides information about the **Counter3** value.	

Column Name	Variable Name	Description	Indexed
Ratio1	dclass_ratio1	Event source class Ratio 1.	
Ratio1String	dclass_ratio1_string	A descriptive string that describes the **Ratio1** value.	
Ratio2	dclass_ratio2	Event source class Ratio 2.	
Ratio2String	dclass_ratio2_string	A descriptive string that describes the **Ratio2** value.	
Ratio3	dclass_ratio3	Event source class Ratio 3.	
Ratio3String	dclass_ratio3_string	A descriptive string that describes the **Ratio3** value.	
City	location_city	City name.	
State/Province	location_state	State or province name.	
Country	location_country	Country name.	
Context	context	Additional information that gives context to the event.	
Message	msg	Raw message.	
ClusterMembers	clustermembers	String variable that holds the information about the nodes that define the cluster.	
OperatingSystem	os	Name of the operating system.	
SerialNumber	serial_number	Serial number associated with a physical asset.	
EncryptionType	encryption_type	Contains one or more of the following encryption	

Column Name	Variable Name	Description	Indexed
		elements (but may include other encryption elements not explicitly listed here): ● Encryption method used to generate the session key. ● Encryption algorithm for the session. ● Hashing algorithm for the session.	
CertificateKeySize	cert_keysize	The size (in bits) of the certificate key referenced in the event.	
Comments	comments	Comment information.	

Analysis

Below is a list of analysis variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
Date/Time	stamp	RESERVED	
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
MessageID	msg_id	RESERVED	Yes
EventTime	event_time	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventTimeString	event_time_string	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes

Column Name	Variable Name	Description	Indexed
		Note: This field should be used if the format does not conform to RSA's configuration specifications for the event source.	
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
EventType	event_type	The event category type as specified by the event source generator. **Note:** This variable can also be used to capture the attack name.	
OperationID	operation_id	An alert number or operation number. A common use case could be referencing a vendor event number. **Note:** The values should be unique and non-repeating.	
ReferenceID	id	Event or message ID.	
Session	sessionid	Session ID.	
Action	action	The action taken, or proposed to be taken.	Yes

Column Name	Variable Name	Description	Indexed
Disposition	disposition	The end state of the action.	Yes
ResultCode	resultcode	Result (error) code. **Note:** This field is numeric.	Yes
Result	result	Result (error) string.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column.	
SourceAddress	saddr	Source IP address.	Yes
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	
SourceMask	smask	Source device network mask.	
SourceInterface	sinterface	Source interface.	
DestinationAddress	daddr	Destination address.	Yes
DestinationPort	dport	Destination port.	Yes

Column Name	Variable Name	Description	Indexed
DestinationHostName	dhost	Destination hostname.	
DestinationMask	dmask	Destination device network mask.	
DestinationInterface	dinterface	Destination interface.	
Protocol	protocol	IP protocol name.	
TypeOfService	tos	The priority given to a network mask.	
IPAddress	hostip	Device IP address. **Note:** This variable should be used if the event does not indicate a communication between two parties.	Yes
NetworkPort	network_port	Network port. **Note:** This variable should be used to capture protocol port information, but only in the case where there is no inherently implied network communication occurring.	Yes
HostName	hostname	Hostname.	Yes
EventComputer	event_computer	The hostname or IP of the system which originally generated the event. **Note:** This variable may be used in situations where a log relay is in place and the hostname variable is referring to	

Column Name	Variable Name	Description	Indexed
		the relay.	
UserName	username	Account name.	Yes
LogonID	logon_id	Unique identifier for an account.	
ClientUserName	c_username	Client Username. For example, a scenario including the user name on the client (source) referenced in the event, but not the actual event source.	Yes
RecordedTime	recorded_time	The event time as recorded by the system the event is collected from. For example, a multi-tiered application where the management layer of the system records its own timestamp at the time of collection from its child nodes. **Note:** This variable must be in timestamp format.	
StartTime	starttime	Start time of the event. **Note:** If this variable is used, **event_time** must also be used.	
EndTime	endtime	End time of the event.	
EventUser	event_user	The user which created the event, or the user who is the subject of the event. However, it should not be the user	

Column Name	Variable Name	Description	Indexed
		that is the actor in the event.	
LinkedSessionID	sessionid1	Linked (related) session ID.	
LinkedReferenceID1	id1	Linked (related) event or message ID.	
LinkedReferenceID2	id2	Second linked event or message ID. **Note:** This variable can either be linked to **id** or **id1**, but should not be used unless the other two variables are in play.	
Rule	rule	Rule number.	
RuleName	rulename	Rule name.	
Info	info	Additional event information that could not be captured in a separate column.	
Context	context	Additional information that gives context to the event.	
NodeName	node	Node name. A common use case is the node name within a cluster where the cluster name is reflected by the Hostname.	
Version	version	Version of the application or OS which is generating the event.	

Column Name	Variable Name	Description	Indexed
PortName	portname	Physical or logical port connection, but does not include a network port. For example, a printer port name.	
Terminal	terminal	Terminal.	
UserFullName	user_fullname	The full name of a user. **Note:** This is sometimes called Real Name.	
UserFirstName	user_fname	The first name of the user.	
UserMiddleName	user_mname	The middle name of the user.	
UserLastName	user_lname	The last name of the user.	
UserDepartment	user_dept	User's Department.	
UserProfile	profile	User's profile name.	
PatientID	patient_id	Patient Identifier.	
PatientFullName	patient_fullname	Patient's Full name.	
PatientFirstName	patient_fname	Patient's First name.	
PatientMiddleName	patient_mname	Patient's Middle name.	

Column Name	Variable Name	Description	Indexed
PatientLastName	patient_lname	Patient's Last name.	
Category	category	Category name.	Yes
GroupObject	group_object	A collection/grouping of entities.	
Application	application	The name of the application (software).	
Service	service	A software daemon, or service (a resident version of an application).	
Parameters	param	Parameters passed as part of a command or application, etc.	
Process	process	Process name.	
ObjectName	obj_name	Name of the object. **Note:** If this variable is used, **obj_type** should be used to describe what type of object this is.	
ObjectType	obj_type	Object type.	
Directory	directory	Directory name. This is a file directory, not LDAP.	
DocumentNumber	doc_number	Document or file number.	
ChangeOldValue	change_old	The old value of an attribute or object in a change event.	

Column Name	Variable Name	Description	Indexed
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	
Bytes	bytes	Total bytes.	
EventCounter	event_counter	Number of times the event has repeated, or the total number of events aggregated.	
Entry	entry	Numeric ID for each statement in audit table.	
TableName	tbl_name	Table name.	
IndexID	index	Index ID of the object affected.	
InstanceName	instance	Instance name.	
Library	library	Library. **Note:** This variable should be only used if the event source is collecting and analyzing events from Mainframe systems.	
JobName	jobname	Job name. **Note:** This variable should be only used if the event source is collecting and analyzing events from Mainframe systems.	
JobNumber	jobnum	Job number.	

Column Name	Variable Name	Description	Indexed
		Note: This variable should be only used if the event source is collecting and analyzing events from Mainframe systems.	
ObjectValue	obj_value	Object value. **Note:** This variable should be only used if the event source is collecting and analyzing events from Mainframe systems.	
Message	msg	Raw message.	

Application Firewall

Below is a list of application firewall variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
Date/Time	stamp	RESERVED	
MessageID	msg_id	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	

Column Name	Variable Name	Description	Indexed
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
EventType	event_type	The event category type as specified by the event source generator.	

Column Name	Variable Name	Description	Indexed
EventState	event_state	The current state of the object or item referenced within the event.	
EventTime	event_time	Date or Time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventTimeString	event_time_string	Date or Time of the occurrence of the event as recorded by the system that generated the event. **Note:** This variable should be used if the date format does not conform to RSA's configuration specifications for the device.	Yes
TimeZone	timezone	A time zone name or offset value.	
Duration	duration	Duration of the event in minutes.	
DurationString	duration_string	A text string version of the duration.	
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
EventLog	event_log	Name of the event log.	
OperationID	operation_id	An alert number or operation number. A common use case would be to reference a vendor event number. **Note:** The values should be unique and non-repeating.	

Column Name	Variable Name	Description	Indexed
SessionID	sessionid	Session ID.	
LinkedSessionID	sessionid1	Linked (related) session ID	
ReferenceID	id	Event or Message ID.	Yes
LinkedReferenceID	id1	Linked (Related) Event or Message ID.	
LinkedReferenceID2	id2	Second Linked Event or Message ID. **Note:** This can be linked to either **id** or **id1**, but should not be used unless the other two variables are being used.	
EventCounter	event_counter	Number of times the event has repeated OR The total number of events aggregated.	
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
HostID	hostid	Host identifier.	
IPAddress	hostip	Device IP address.	Yes
NetworkPort	network_port	Network port. This variable should be used to capture protocol port information but only in the case where there is NO inherently implied network communication occurring.	

Column Name	Variable Name	Description	Indexed
HostName	hostname	Hostname.	Yes
FQDN	fqdn	Fully qualified domain name.	Yes
Interface	interface	Device interface name.	
NetworkServiceName	network_service	The name of the network service.	
SourceAddress	saddr	Source IP address.	Yes
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	
SourceMacAddress	smacaddr	Source MAC address.	
DestinationAddress	daddr	Destination address.	Yes
DestinationPort	dport	Destination port.	Yes
DestinationHostName	dhost	Destination hostname.	
DestinationDomain	ddomain	Destination domain.	
DestMacAddress	dmacaddr	Destination MAC address.	
TranslatedSourceAddress	stransaddr	Translated source address.	
TranslatedSourcePort	stransport	Translated source port.	

Column Name	Variable Name	Description	Indexed
TranslatedDestinationAddress	dtransaddr	Translated destination address.	
TranslatedDestinationPort	dtransport	Translated destination port.	
Country	location_country	Country name.	
Version	version	Version of the application or OS which is generating the event.	
ContentVersion	content_version	A version which indicates the release level of a signature or database content.	
ComponentVersion	component_version	A version which reflects the version level of a sub-component of a product.	
Protocol	protocol	IP protocol name.	
ProtocolDetail	protocol_detail	IP protocol details. **Note:** For protocols that do not contain details such as ports, this is the place to capture that information.	
Gateway	gateway	Gateway to be used when dealing with routing information.	
Bytes	bytes	Total bytes.	
ReceivedBytes	rbytes	Bytes received.	

Column Name	Variable Name	Description	Indexed
SentBytes	sbytes	Bytes sent.	
CompressedReceivedBytes	comp_rbytes	Compressed bytes received.	
CompressedSentBytes	comp_sbytes	Compressed bytes sent.	
Counter1	dclass_counter1	Device class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	
Counter2	dclass_counter2	Device class counter 2.	
Counter2String	dclass_counter2_string	A descriptive string that provides information about the **Counter2** value.	
Ratio1	dclass_ratio1	Device class Ratio 1.	
Ratio1String	dclass_ratio1_string	A descriptive string that describes the **Ratio1** value.	
Ratio2	dclass_ratio2	Device class Ratio 2.	
Ratio2_String	dclass_ratio2_string	A descriptive string that describes the **Ratio2** value.	
InstanceName	instance	Instance name.	
DNSOpcode	dns_opcode	DNS Opcode value.	
DNSARecord	dns_a_record	DNS A record value.	

Column Name	Variable Name	Description	Indexed
DNSCNameRecord	dns_cname_record	DNS CName record.	
DNSPTRRecord	dns_ptr_record	DNS PTR record.	
SenderAddress	from	Messaging source address. **Note:** This is not limited to e-mail. It can also include instant messaging and other messaging concepts.	
RecipientAddress	to	Messaging destination address. **Note:** This is not limited to e-mail. It can also include instant messaging and other messaging concepts.	
Subject	subject	Messaging subject.	
MessageBody	message_body	The contents of the message body.	
IMChatroomID	im_croomid	Chat room identifier.	
IMChatroomType	im_croomtype	Chat room type.	
IMMembers	im_members	List of the chat participants.	
IMClient	im_client	IM client information.	
IMUsername	im_username	IM user name.	

Column Name	Variable Name	Description	Indexed
IMUserID	im_userid	IM user ID.	
IMBuddyname	im_buddyname	IM buddy name.	
IMBuddyID	im_buddyid	IM buddy ID.	
StartTime	starttime	Start time of the event.	
EndTime	endtime	End time of the event.	
TriggerValue	trigger_val	The conditions which caused an event to be recorded For example, an exceeded threshold.	
TriggerDesc	trigger_desc	Description of the trigger condition.	
URL	url	Uniform Resource Locator.	
WebPage	webpage	Web page.	
WebQuery	web_query	Query portion of the URL.	
Method	web_method	Web method For example, POST or GET.	
WebCookie	web_cookie	The cookies passed within a web request.	
Referer	web_referer	Request header referral.	

Column Name	Variable Name	Description	Indexed
WebHost	web_host	The hostname used in the web request.	
WebDomain	web_domain	The web domain	
Content	content_type	content encoding type.	
UserAgent	user_agent	User agent identifier. **Note:** This variable should only be used in reference to the browser identification string.	
ChangeOldValue	change_old	The prior value of an attribute or object in a change event.	
ChangeNew	change_new	The new value of an attribute or object in a change event.	
CertificateSubject	cert_subject	The subject name of a certificate.	
CertificateUserName	cert_username	Certificate user name.	
SourceSSLVersion	s_sslver	Source (Client) SSL Version.	
SourceCipher	s_cipher	Source (Client) Cipher.	
Group	group	Group name.	Yes
GroupObject	group_object	A collection or grouping of entities.	
HardwareID	hardware_id	A unique identifier for a device or system (not a MAC	

Column Name	Variable Name	Description	Indexed
		address).	
Category	category	Category name.	
Filter	filter	Filter category name.	
PolicyName	policyname	Policy name.	
ThreatName	threat_name	Name of the threat, exploit, vulnerability, or malware.	
ReputationNumber	reputation_num	A reputation score that is generally used by IP address and e-mail filters to accept or deny traffic or data through the device.	
Rule	rule	Rule number.	
RuleName	rulename	Rule Name . **Note:** This variable is not always populated. Many products only record a rule number and not an associated descriptive rule name.	
RuleGroup	rule_group	The name of a grouping of rules. **Note:** This grouping should relate rule names and/or rule numbers.	
Agent	agent	Agent that processes a portion of the event, and is effectively handed off to.	

Column Name	Variable Name	Description	Indexed
ProcessID	process_id	Process ID number.	
Process	process	Process name.	
Administrator	administrator	Administrative user name.	
UserName	username	Account name.	Yes
DomainName	domain	The domain name	
ClientSID	c_sid	The client security ID	
ClientUserName	c_username	Client user name. Example scenarios include user name on the client (source) referenced in the event but not the actual event source.	
LogonID	logon_id	Unique identifier for an account.	
LogonType	logon_type	The type of logon. Some systems record a value for the level to which a logon was performed. For example, interactive vs non-interactive.	
UserAddress	user_address	User e-mail address, but not in the context of a communication between two parties.	
DatabaseName	db_name	Database name.	
Terminal	terminal	The terminal	

Column Name	Variable Name	Description	Indexed
Application	application	The name of the application (software).	
Service	service	A software daemon or service. This is also a resident version of an application.	
Product	product	The name of the product (software or hardware).	
FileName	filename	Document or File name.	
FilenameSize	filename_size	Size of the Document or File name.	
Disposition	disposition	The end state of the action.	Yes
Result	result	Result (Error) String.	Yes
ResultCode	resultcode	Result (Error) Code. **Note:** This field is numeric.	Yes
SignatureID	sigid	Signature ID.	
SignatureName	signame	Signature name/string/hex value.	
VirusName	virusname	The name of the virus.	
ObjectName	obj_name	Name of the object. **Note:** If this variable is used, then **obj_type** should be used to describe what type of object this is.	

Column Name	Variable Name	Description	Indexed
ObjectType	obj_type	Object type.	
Direction	direction	Direction of the network flow.	
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column.	
Info	info	Additional event information that could not be captured in a separate column.	
Context	context	Additional information that gives context to the event.	
Department1	iassoc1	RESERVED	
Department2	iassoc2	RESERVED	
Department3	iassoc3	RESERVED	
Category1	eassoc1	RESERVED	
Category2	eassoc2	RESERVED	
Category3	eassoc3	RESERVED	
VID	vid	RESERVED	
Action	action	The action taken or proposed to be taken.	Yes
Message	msg	Raw message.	

Application Server

Below is a list of application server variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
Date/Time	stamp	RESERVED	
MessageID	msg_id	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	Yes

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	Yes
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	Yes
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	Yes

Column Name	Variable Name	Description	Indexed
EventTime	event_time	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventSource	event_source	Source of the event. This is not a hostname.	
ReferenceID	id	The event message ID	
OperationID	operation_id	An alert number or operation number. A common use case is referencing a vendor event number. The values should be unique and non-repeating typically.	
Action	action	The action taken or proposed to be taken. **Note:** For databases, this is the SQL Query Statement.	Yes
EventState	event_state	The current state of the object or item referenced within the event.	
Disposition	disposition	The end state of the action.	Yes
Result	result	Result (Error) string.	Yes
ResultCode	resultcode	Result (Error) code. **Note:** This field is numeric.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes

Column Name	Variable Name	Description	Indexed
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column. **Note:** This column should be used only if the **info** column is also required.	
SourceAddress	saddr	The source IP address	
SourcePort	sport	Source port	
SourceHostName	shost	The source host name	
SourceMacAddress	smacaddr	The source MAC address.	
Protocol	protocol	IP protocol name.	
IPAddress	hostip	Device IP address.	Yes
HostName	hostname	Hostname. Preferably fully qualified.	Yes
NetworkPort	network_port	Network port. **Note:** This variable should be used to capture protocol port information, but only in the case where there is no inherently implied network communication occurring.	Yes
UserName	username	The account name	

Column Name	Variable Name	Description	Indexed
DomainName	domain	Domain name	
LogonID	logon_id	Unique identifier for an account	
ClientSID	c_sid	Client security ID	
ClientUserName	c_username	The client username. Example scenarios include username on the client (source) referenced in the event, but not the actual event source.	
ClientDomain	c_domain	Client domain	
ClientLogonID	c_logon_id	Client logon ID	
Interface	interface	Event Source interface name.	
Version	version	Version of the application or OS which is generating the event.	
Info	info	Additional event information that could not be captured in a separate column.	
LogonType	logon_type	The type of logon. **Note:** Some systems record a value for the level in which a logon was performed.	
AuthenticationMethod	authmethod	Authentication mechanism	

Column Name	Variable Name	Description	Indexed
Privilege	privilege	The privilege level/attributes recorded	
UserRole	user_role	The account or group name under which the user's action is being performed.	
GroupObject	group_object	A collection or grouping of entities. **Note:** This is not specific to authentication.	
Agent	agent	Agent that processes a portion of the event and is effectively handed off to.	
Product	product	The name of the product. **Note:** This variable can be software or hardware.	
Application	application	The name of the application (software)	
Process	process	Process name	
ParentProcessID	parent_pid	Parent process ID number	
ParentProcess	parent_process	Parent process name	
Directory	directory	Directory name (file directory, not LDAP).	
FileName	filename	Document or file name.	

Column Name	Variable Name	Description	Indexed
ChangeOldValue	change_old	The prior value of an attribute/object in a change event	
ChangeNewValue	change_new	The new value of an attribute/object in a change event	
OperatingSystem	os	Name of the operating system.	
Message	msg	Raw message.	

Configuration Management

Below is a list of configuration management variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
Date/Time	stamp	RESERVED	
MessageID	msg_id	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
Level	level	The RSA enVision event priority level.	
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity.	

Column Name	Variable Name	Description	Indexed
		Note: For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventTimeString	event_time_string	Date or Time of the occurrence of the event as recorded by the system that generated the event. **Note:** This field should be used if the format does not conform to RSA's configuration specifications for the event source.	Yes
EventLog	event_log	Name of the event log.	
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
EventType	event_type	The event category type as specified by event source generator.	
EventState	event_state	The current start of the object or item referenced within the event.	
OperationID	operation_id	An alert number or operation number. Common use case, referencing a vendor event number.	

Column Name	Variable Name	Description	Indexed
		Note: The values should be unique and non-repeating.	
ReferenceID	id	Event or Message ID.	Yes
Action	action	The action taken or proposed to be taken. **Note:** For databases, this is the SQL Query Statement.	Yes
Disposition	disposition	The end state of the action.	Yes
ResultCode	resultcode	Result (Error) code. This field is numeric.	Yes
Result	result	Result (Error) string.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured into a separate column. **Note:** This column should be used only if the **info** column is also required.	
SourceAddress	saddr	Source IP address.	Yes
SourceAddressv6	saddr_v6	Source IPv6 address.	Yes

Column Name	Variable Name	Description	Indexed
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	
SourceMacAddress	smacaddr	Source MAC address.	
DestinationAddress	daddr	Destination address.	Yes
DestinationAddressv6	daddr_v6	Destination IPv6 address.	Yes
DestinationPort	dport	Destination port.	Yes
DestinationHostName	dhost	Destination hostname.	
Protocol	protocol	IP protocol name.	
NetworkService	network_service	The name of the network service. **Note:** Some services comprise multiple ports.	
DeviceMacAddress	macaddr	Device MAC address.	
IPAddress	hostip	Device IP address.	Yes
NetworkPort	network_port	Network port. **Note:** This variable should be used to capture protocol port information, but only in the case where there is no	Yes

Column Name	Variable Name	Description	Indexed
		inherently implied network communication occurring.	
HostName	hostname	Hostname. Preferably fully qualified.	Yes
FQDN	fqdn	Fully qualified domain name.	Yes
DomainID	domain_id	Name of the domain only, Pre Windows 2000 (NetBIOS).	
DomainName	domain	Domain name.	
IPMask	mask	Device network mask.	
Interface	interface	Device interface name.	
EventComputer	event_computer	The Hostname or IP of the system which originally generated the event. This variable may be used in situations where a log relay is in place and the Hostname variable is referring to the relay.	
Administrator	administrator	Administrative user name.	
Username	username	Account name.	Yes
LogonID	logon_id	Unique identifier for an account.	
ClientUserName	c_username	Client User name, for example, a user name on the client (source) referenced in the event, but not the actual event source.	Yes

Column Name	Variable Name	Description	Indexed
UserID	uid	The unique user identifier that is associated with the user name.	
Group	group	Group name.	Yes
GroupID	groupid	Group ID number related to **group**.	
Duration	duration	Duration of the event in minutes.	
DurationString	duration_string	A text string version of the duration. For example, 02:40.	
StartTime	starttime	Start time of the event. **Note:** If you use this variable, you MUST also use **event_time**.	
EndTime	endtime	End time of the event.	
ExpirationTime	expiration_time	A timestamp that explicitly refers to an expiration.	
EffectiveTime	effective_time	The effective time referenced by the individual event. **Note:** This must be in a timestamp format.	
RecordedTime	recorded_time	The event time as recorded by the system the event is collected from. The usage scenario is a multi-tier application where the management layer of the system records it's own timestamp at the time of collection from its	

Column Name	Variable Name	Description	Indexed
		child nodes. This must be in timestamp format.	
EventUser	event_user	The user that created the event or the user that is the subject of the event. It should not be the user that is the actor in the event.	
ConnectionID	connectionid	Connection ID.	
PolicyID	policy_id	Policy ID. **Note:** Typically numeric field. Could be hex or decimal.	
PolicyName	policyname	Policy Name.	
PolicyTemplate	policy_template	The policy template that accompanies the policy.	
PolicyWaiver	policy_waiver	An exception to the policy in effect. **Note:** This could be the detailed explanation of the waiver or simply a category that the waiver belonged to.	
Risk	risk	Risk value. This is not a numeric value.	
Rule	rule	Rule number.	
RuleUID	rule_uid	Unique Identifier for a rule. Some products also leverage a unique identifier for rules in addition to a rule number.	
RuleName	rulename	Rule name.	

Column Name	Variable Name	Description	Indexed
		Note: This is not always populated. Many products only record a rule number, and not an associated descriptive rule name.	
RuleGroup	rule_group	The name of a grouping of rules. **Note:** This grouping should relate rule names and rule numbers.	
RuleTemplate	rule_template	A default set of parameters which are overlayed onto a rule or rule name which effectively constitutes a template.	
WorkspaceDescription	workspace_desc	A collection of policies (possibly including rules as well) which are organized together into a workspace.	
ExpectedValue	expected_val	The value the system was expecting to see (from the perspective of the device generating the log).	
ObservedValue	observed_val	The value the system actually observed (or received, found etc). **Note:** This variable should be used in conjunction with **expected_val**.	
Info	info	Additional event information that could not be captured into a separate column.	

Column Name	Variable Name	Description	Indexed
Context	context	Additional information that gives context to the event.	
NodeName	node	Node name. A common use case is the node name within a cluster where the cluster name is reflected by the Hostname. **Note:** In configuration management systems, this would store the name of the device being managed.	Yes
VirtualName	vsys	Virtual system name.	
VirtualTemplate	vsys_template	Virtual system template.	
VLAN	vlan	VLAN number.	
SSID	ssid	Wireless SSID name.	
WiFiChannel	wifi_channel	The channel ID used by a wireless access point.	
AccessPoint	access_point	Access point name.	
Version	version	Version of the application or OS which is generating the event.	
HostID	hostid	Host identifier.	
PortName	portname	Physical or logical port connection. For example, a printer port name.	

Column Name	Variable Name	Description	Indexed
		Note: This does NOT include a network port.	
Device	device	Device associated with the node. For example, a physical disk, a printer, or a fan.	Yes
Terminal	terminal	Terminal.	
DistinguishedName	dn	X.500 (LDAP) distinguished name.	
AuthenticationMethod	authmethod	Authentication mechanism.	
UserRole	user_role	The account or group name which the user's action is being performed under.	
UserOrganization	user_org	User organization.	
Profile	profile	User's profile name.	
Category	category	Category name.	Yes
Filter	filter	Filter category name.	
GroupObject	group_object	A collection or grouping of entities. **Note:** This is not specific to authentication.	
PoolID	pool_id	The identifier of a resource pool.	

Column Name	Variable Name	Description	Indexed
		Note: This is typically a numeric field.	
PoolName	pool_name	The name of a resource pool.	
Agent	agent	Agent that processes a portion of the event and is effectively handed off to.	
Product	product	The name of the product, software or hardware.	
Application	application	The name of the software application.	
Service	service	A software daemon or service.	
ProcessID	process_id	Process ID number.	
Data	data	Data field. The data_type variable is used to describe the type of data being represented in this field.	
DataType	data_type	The classification type of the data that is the subject of the event referenced.	
ObjectType	obj_type	Object type.	Yes
ObjectName	obj_name	Name of the object. **Note:** You MUST use **obj_type** to describe what type of object this is.	Yes

Column Name	Variable Name	Description	Indexed
Directory	directory	Directory name (file directory, not LDAP).	
FileName	filename	Document or file name.	Yes
SenderAddress	from	Messaging source address. Not limited to e-mail, also includes Instant Messaging and other messaging concepts.	
RecipientAddress	to	Messaging destination address. Not limited to e-mail, also includes Instant Messaging and other messaging concepts.	
CC	cc	The CC field usually associated with an e-mail	
Subject	subject	Messaging subject.	
URL	url	Uniform Resource Locator.	
WebPage	webpage	The web page.	
VirusName	virusname	The name of the virus.	
ChangeAttribute	change_attribute	Change attribute.	
ChangeOldValue	change_old	The prior value of an attribute or object in a change event.	Yes
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	Yes

Column Name	Variable Name	Description	Indexed
LDAPAttribute	ldap_attribute	LDAP attribute string name.	
Counter1	dclass_counter1	Device class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	
Counter2	dclass_counter2	Device class counter 2.	
Counter2String	dclass_counter2_string	A descriptive string that provides information about the **Counter2** value.	
Counter3	dclass_counter3	Device class counter 3.	
Counter3String	dclass_counter3_string	A descriptive string that provides information about the **Counter3** value.	
InstanceName	instance	Instance name.	
OperatingSystem	os	Name of the operating system.	
Benchmark	benchmark	The regulatory requirement or best practices standard to which the event is being referred to.	
Message	msg	Raw message.	
LocationDescription	location_desc	A description of the location relevant for the event being logged.	
PortWorldWideName	pwwn	Port World Wide Name.	

Column Name	Variable Name	Description	Indexed
		A World Wide Name uniquely identifying a port on a Host Bus Adapter.	
NodeWorldWideName	nwwn	Node World Wide Name. A World Wide Name uniquely identifying a Host Bus Adapter, shared by all ports on that Host Bus Adapter.	
Scheme	scheme	The encryption scheme used.	

Database

Below is a list of database variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
Date/Time	stamp	RESERVED	
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
MessageID	msg_id	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	Yes

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	Yes
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	Yes
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	Yes

Column Name	Variable Name	Description	Indexed
EventTime	event_time	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventTimeString	event_time_string	Date or time of the occurrence of the event as recorded by the system that generated it. This field should be used if the format does not conform to RSA configuration specifications for the device.	
EventLog	event_log	Name of the event log.	
EventSource	event_source	Source name of the event. This variable is not a hostname.	
VendorEventCategory	vendor_event_cat	Category of the event. **Note:** This variable is a vendor-supplied data field, and is not generated from enVision.	
EventType	event_type	The event category type as specified by the event source generator.	
Session	sessionid	Session ID.	
OperationID	operation_id	An alert number or operation number, for example, referencing a vendor event number. **Note:** These values should be unique and non-repeating.	
ReferenceID	id	Event or message ID.	Yes

Column Name	Variable Name	Description	Indexed
Action	action	The action taken or proposed to be taken. **Note:** This variable is also the query referenced in the event.	Yes
Result	result	Result (error) string.	Yes
ResultCode	resultcode	Result (error) code. **Note:** This field is numeric.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured into a separate column.	
SourceAddress	saddr	Source IP address.	
SourcePort	sport	Source port.	
SourceHostName	shost	Source host name.	
DestinationAddress	daddr	Destination address.	
DestinationHostName	dhost	Destination host name.	

Column Name	Variable Name	Description	Indexed
DestinationPort	dport	Destination port.	
IPAddress	hostip	Device IP address. **Note:** This variable should be used if the event does not indicate a communication between two parties.	Yes
NetworkPort	network_port	Network port. **Note:** This variable should be used to capture protocol port information, but only in the case where there is no inherently implied network communication occurring.	Yes
HostName	hostname	Hostname.	Yes
EventComputer	event_computer	The hostname or IP address of the system which originally generated the event. This variable may be used in situations where a log relay is in place and the Hostname variable is referring to the relay.	
OwnerName	owner	The identity name of the owner of an object, for example, a file, directory, or policy.	
Administrator	administrator	Administrative user name.	
UserName	username	Account name.	Yes

Column Name	Variable Name	Description	Indexed
DomainName	domain	Domain name.	
LogonID	logon_id	Unique identifier for an account.	
ClientUserName	c_username	Client user name, for example, a user name on the client (source) referenced in the event, but not the actual event source.	Yes
Group	group	Group name. Use for a group of users only.	
Duration	duration	Duration of the event in minutes.	
StartTime	starttime	Start time of the event. **Note:** If this variable is used, **event_time** must also be also used.	
EndTime	endtime	End time of the event.	
ProcessingTime	processing_time	The time spent processing the request in ms or seconds.	
TimeZone	timezone	A time zone name or offset value. For example, -0400, +0600, EDT and GMT+0700.	
EventUser	event_user	The user that created the event or the user that is the subject of the event. This should not be the user that is the actor in the event.	
EventState	event_state	The current state of the object or item referenced within	

Column Name	Variable Name	Description	Indexed
		the event.	
ConnectionID	connectionid	Connection ID.	
LinkedSession	sessionid1	Linked (related) session ID.	
LinkedReferenceID	id1	Linked (Related) Event/Message ID	
PolicyName	policyname	Policy name.	
Risk	risk	Policy name. **Note:** This value is not numeric.	
RiskNumber	risk_num	Risk value. **Note:** This value is numeric.	
RuleName	rulename	Rule name.	
Info	info	Additional event information.	
Context	context	Additional information that gives context to the event.	
NodeName	node	Node name.	
Version	version	Version of the application or OS that is generating the event.	

Column Name	Variable Name	Description	Indexed
Terminal	terminal	Terminal.	
Accesses	accesses	Actual privileges used in accessing an object.	
AuthenticationMethod	authmethod	Authentication mechanism.	
Privilege	privilege	The privilege level or attributes used.	
ServiceAccount	service_account	The name (including domain if applicable) of the account under which a service (referenced in the event) is running.	
GroupObject	group_object	A collection or grouping of entities. For example, an interface group.	
Product	product	The name of the product (software or hardware).	
Application	application	The name of the application (software).	
Service	service	A software daemon or service, a resident version of an application.	
ProcessID	process_id	Process ID number.	
Process	process	Process name.	
ObjectName	obj_name	Object name.	

Column Name	Variable Name	Description	Indexed
ObjectType	obj_type	Object type.	
FileName	filename	Document or file name.	
Sensor	sensor	Sensor name.	
SignatureName	signame	Signature name, string, or hex value.	
CVEReference	cve	CVE reference.	
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	
Counter1	dclass_counter1	Device class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	
Statement	statement	Numeric ID for each statement run.	Yes
Entry	entry	Numeric ID for each statement in the audit table.	Yes
TransactionID	trans_id	SQL transaction ID.	
TableName	tbl_name	Table name.	Yes
DatabaseName	db_name	Database name.	Yes
IndexID	index	Index ID of the of the index on the object affected.	Yes

Column Name	Variable Name	Description	Indexed
InstanceName	instance	Database instance name.	Yes
Dead	dead	User logged off as DEAD.	
DatabaseProcessID	db_pid	Process ID for the database server where this ID is not the main process ID that is shown within a single event.	
PRead	pread	Number of physical reads.	
Lread	lread	Number of logical reads.	
LWrite	lwrite	Number of logical writes.	
Permissions	permissions	Database permissions.	
BinaryData	binary	Binary data dependent.	
OperatingSystem	os	Name of the operating system.	
CPU	cpu	Central Processing Unit time used in the execution of the event being recorded.	
Message	msg	Raw message.	

Data Loss Prevention

Below is a list of Data Loss Prevention variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
Date/Time	stamp	RESERVED	
MessageID	msg_id	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. Check enVision online help for a list of current themes. **Note:** Only for enhanced categorization tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. Check enVision online help for a list of current subjects. **Note:** Only for enhanced categorization tagging.	

Column Name	Variable Name	Description	Indexed
ECActivity	ec_activity	A normalized set of actions that describes the event. Check the RSA enVision online help for a list of current activities. **Note:** Only for enhanced categorization tagging.	
ECOutcome	ec_outcome	A normalized result set. Check the RSA enVision online help for a list of current outcomes. **Note:** Only for enhanced categorization tagging.	
EventCounter	event_counter	Number of times the event has repeated, or the total number of events aggregated.	
EventState	event_state	The current state of the object or item referenced within the event. **Note:** States such as **successful** and **failed** are not suitable for this variable as they imply the end state.	
OperationID	operation_id	An alert number or operation number. For example, referencing a vendor event number.	
ReferenceID	id	Event or message ID.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes

Column Name	Variable Name	Description	Indexed
Result	result	Result (Error) code. **Note:** This field is numeric.	Yes
VirtualName	vsys	Virtual system name.	
HostName	hostname	Hostname. **Note:** Preferably, this variable should be fully qualified.	Yes
IPAddress	hostip	Event source IP address.	Yes
IPAddressv6	hostip_v6	Event source IPv6 Address.	Yes
DeviceMacAddress	macaddr	Event source MAC address.	
SourceAddress	saddr	Source IP address.	Yes
SourceAddressv6	saddr_v6	Source IPv6 Address.	Yes
SourceHostName	shost	Source hostname.	
SourcePort	sport	Source port.	Yes
SourceInterface	sinterface	Source interface.	
DestinationAddress	daddr	Destination address.	Yes
DestinationAddressv6	daddr_v6	Destination IPv6 Address.	Yes

Column Name	Variable Name	Description	Indexed
DestinationHostName	dhost	Destination hostname.	
DestinationPort	dport	Destination port.	Yes
DestinationInterface	dinterface	Destination interface.	
ProtocolDetail	protocol_detail	IP protocol details. **Note:** For protocols that do not contain details such as ports, this variable is the place to capture that information.	
SessionID	sessionid	Session ID.	
Rule	rule	Rule number.	
RuleName	rulename	Rule name. **Note:** This field is not always populated. Many products only record a rule number, and not an associated descriptive rule name.	
PolicyID	policy_id	Policy ID. **Note:** This variable is typically a numeric field that could be in hex or decimal.	
PolicyName	policyname	Policy name.	

Column Name	Variable Name	Description	Indexed
Risk	risk_num	Risk value that is not a numeric value.	
Bytes	bytes	Total bytes.	
DataType	data_type	The classification type of the data that is the subject of the event referenced.	
Agent	agent	The agent that processes a portion of the event and is effectively handed off to.	
Application	application	The name of the application (software).	
ClientUserName	c_username	Client user name, for example, a user name on the client (source) referenced in the event, but not the actual event source.	
Product	product	The name of the product (software or hardware).	
Process	process	Process name.	
ObjectName	obj_name	Name of the object.	
ObjectType	obj_type	Object type.	
Directory	directory	Directory name (file directory, not LDAP).	
FileName	filename	Document or file name.	
EventSource	event_source	Source of the event.	

Column Name	Variable Name	Description	Indexed
		Note: This variable is not a hostname.	
LogonID	logon_id	Unique identifier for an account.	
AuthenticationMethod	authmethod	The method for authentication.	
NetworkServiceName	network_service	The name of the network service. **Note:** Some services comprise multiple ports.	
OwnerName	owner	The name of the owner of an object. **Note:** Object examples include: file, directory, or policy.	
OwnerID	owner_id	The unique ID associated with the **Owner Name**. **Note:** This value is typically numeric.	
RecipientAddress	to	Messaging destination address. **Note:** This variable is not limited to e-mail and can also include Instant Messaging and other messaging concepts.	
SenderAddress	from	Messaging source address. **Note:** This is not limited to e-mail; also includes Instant	

Column Name	Variable Name	Description	Indexed
		Messaging and other messaging concepts.	
URL	url	Uniform Resource Locator.	
UserAddress	user_address	User e-mail address, but not in the context of a communication between two parties.	
UserDepartment	user_dept	User's department.	
UserName	username	Account name.	Yes
UserOrganization	user_org	User organization.	
Group	group	Group name. **Note:** For Cisco VPNs, this variable is the **tunnel-group** parameter.	Yes
GroupID	groupid	Group ID number (related to the group name).	
Category	category	Category name.	
Version	version	Version of the application or Operating System that is generating the event.	
Info	info	Additional event information that could not be captured in a separate column.	

Column Name	Variable Name	Description	Indexed
Context	context	Additional information that gives context to the event.	
Counter1	dclass_counter1	Device class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	
Ratio1	dclass_ratio1	Device class Ratio 1.	
Ratio1String	dclass_ratio1_string	A descriptive string that describes the **Ratio1** value.	
Department1	iassoc1	RESERVED	
Department2	iassoc2	RESERVED	
Department3	iassoc3	RESERVED	
Category1	eassoc1	RESERVED	
Category2	eassoc2	RESERVED	
Category3	eassoc3	RESERVED	
EventTime	event_time	Date or time of the event, as recorded by the system that generated the event.	Yes
EventTimeString	event_time_string	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes

Column Name	Variable Name	Description	Indexed
		Note: This field should be used if the format does not conform to configuration specifications for the event source provided by RSA.	
Duration	duration	Duration of the event in minutes.	
DurationString	duration_string	A text string version of the duration.	
EffectiveTime	effective_time	The effective time referenced by the individual event. **Note:** This variable must be in a timestamp format.	
RecordedTime	recorded_time	The event time as recorded by the system from which the event is collected. The usage scenario is a multi-tier application.	
EventCategory	ecategory	RESERVED	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column. **Note:** This column should be used only if the info column is also required.	
EventType	event_type	The event category type as specified by the event source generator.	
ForensicInfo	forensic_info	Unstructured forensic event information that is captured	

Column Name	Variable Name	Description	Indexed
		during the referenced event.	
VID	vid	RESERVED	
Action	action	The action taken, or proposed to be taken. **Note:** For databases, this variable is the **SQL Query** statement.	Yes
Accesses	accesses	Actual privileges used in accessing an object, for example, Read or Write.	
HardwareID	hardware_id	A unique identifier for an event source or system. **Note:** This is not a MAC address.	
Message	msg	Raw message.	

Firewall

Below is a list of firewall variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
Date/Time	stamp	RESERVED	
MessageID	msg_id	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the	

Column Name	Variable Name	Description	Indexed
		RSA enVision Enhanced Categorization Tagging guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
EventType	event_type	The event category type as specified by event source generator.	
EventTime	event_time	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes

Column Name	Variable Name	Description	Indexed
EventTimeString	event_time_string	Date or time of the occurrence of the event as recorded by the system that generated the event. **Note:** This field should be used if the format does not conform to RSA configuration specifications for the event source.	Yes
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
StartTime	starttime	Start time of the event.	
EndTime	endtime	End time of the event.	
TimeZone	timezone	A time zone name or offset value. For example, -0400, +0600, EDT and GMT+0700.	
Duration	duration	Duration of the event in minutes.	
DurationString	duration_string	A text string version of the duration, for example, 02:40.	
EventComputer	event_computer	The hostname or IP of the system that originally generated the event. **Note:** This variable may be used in situations where a log relay is in place and the hostname variable is referring to the relay, for example, a Check Point firewall and a Check Point Smart Center.	

Column Name	Variable Name	Description	Indexed
VirtualName	vsys	Virtual system name.	
HostName	hostname	Hostname. Preferably fully qualified.	Yes
DistinguishedName	dn	X.500 (LDAP) Distinguished Name.	
NetworkPort	network_port	The network port. **Note:** This variable should be used to capture protocol port information, but only in the case where there is no inherently implied network communication occurring.	Yes
DomainName	domain	Domain name.	
OperationID	operation_id	An alert number or operation number. Common use case: referencing a vendor event number. The values should be unique and non-repeating typically.	
Action	action	The action taken. **Note:** For Databases this variable is the SQL Query Statement.	Yes
Disposition	disposition	The end state of the action.	Yes
AccessListNo	listnum	Access list number.	
Direction	direction	Direction of the network flow (for the systems that cap-	Yes

Column Name	Variable Name	Description	Indexed
		ture this).	
Interface	interface	Event source interface name.	Yes
NetworkServiceName	network_service	The name of the network service. **Note:** Some services comprise multiple ports.	Yes
Protocol	protocol	IP protocol name.	Yes
CertificateSubject	cert_subject	The subject name of a certificate.	
ProtocolDetail	protocol_detail	IP protocol details. **Note:** For protocols that do not contain details such as ports, this is the variable to capture that information.	
SourceAddress	saddr	Source IP address.	Yes
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	Yes
SourceMacAddress	smacaddr	Source MAC address.	Yes
SourceInterface	sinterface	Source interface.	Yes
SourceZone	src_zone	Source zone.	Yes

Column Name	Variable Name	Description	Indexed
DestinationAddress	daddr	Destination address.	Yes
DestinationPort	dport	Destination port.	Yes
DestinationHostName	dhost	Destination hostname.	Yes
DestinationDomain	ddomain	Destination domain.	
DestinationMacAddress	dmacaddr	Destination MAC address.	Yes
DestinationInterface	dinterface	Destination interface.	Yes
DestZone	dst_zone	Destination zone.	Yes
TranslatedSourceAddress	stransaddr	Translated source address.	
TranslatedSourcePort	stransport	Translated source port.	
TranslatedDestinationAddress	dtransaddr	Translated destination address.	
TranslatedDestinationPort	dtransport	Translated destination port.	
DeviceMacAddress	macaddr	Event Source MAC address.	
IP Address	hostip	Event Source IP address.	Yes
HostID	hostid	Host identifier.	

Column Name	Variable Name	Description	Indexed
IP Mask	mask	Event Source network mask.	
Zone	zone	To be used when referring to a zone that does not have a concept of direction.	
ICMPCode	icmpcode	The "code" value for an ICMP packet.	
ICMPType	icmptype	The "type" value for an ICMP packet.	
SourceLocation	location_src	The location of the source, such as a country or another identifier of the actual location.	
DestinationLocation	location_dst	The location of the destination, such as a country or another identifier of the actual location.	
LocationDescription	location_desc	A description of the location relevant for the event being logged.	
Result	result	Result (Error) String.	Yes
ResultCode	resultcode	Result (Error) Code. **Note:** This field is numeric.	Yes
Bytes	bytes	Total bytes.	
ReceivedBytes	rbytes	Bytes received.	
SentBytes	sbytes	Bytes sent.	

Column Name	Variable Name	Description	Indexed
Packets	packets	Number of times the event has repeated or the total number of events aggregated.	
SessionID	sessionid	Session identifier.	
ConnectionID	connectionid	Connection ID.	
EventState	event_state	The current state of the object or item referenced within the event.	
PolicyID	policy_id	Policy ID, for example, hex or decimal. **Note:** This variable is typically a numeric field.	Yes
PolicyName	policyname	Policy Name.	Yes
Rule	rule	Rule number.	Yes
RuleName	rulename	Rule Name. **Note:** This variable is not always used, even if a rule is in use. Many products only record a rule number and not an associated descriptive rule name.	Yes
RuleUID	rule_uid	Unique identifier for a rule. **Note:** Some products also leverage a unique identifier for rules in addition to a rule number.	

Column Name	Variable Name	Description	Indexed
RuleGroup	rule_group	The name of a group of rules. **Note:** This grouping should relate rule names or rule numbers.	
RuleTemplate	rule_template	A default set of parameters which are overlayed onto a rule (or rule name) which effectively constitutes a template.	
RiskNumber	risk_num	Risk value. **Note:** This value is numeric.	
ThreatValue	threat_val	A threat rating that is a measure of the threat level.	
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
Application	applications	The name of the application (software).	
Product	product	The name of the product (software or hardware).	
Service	service	A resident version of an application.	
NodeName	node	Node name. A common use case is the node name within a cluster where the cluster name is reflected by the Hostname.	
Version	version	Version of the application or OS that is generating the	

Column Name	Variable Name	Description	Indexed
		event.	
ContentVersion	content_version	A version that indicates the release level of a signature or database content.	
SerialNumber	serial_number	Serial number associated with a physical asset.	
AuthenticationMethod	authmethod	Authentication mechanism.	
Agent	agent	Agent that processes a portion of the event and is effectively handed off to.	
LogonID	logon_id	Unique identifier for an account.	
LogonType	logon_type	The type of logon. Some systems record a value for the level in which a logon was performed, for example, interactive versus non-interactive.	
Administrator	administrator	Administrative user name.	
UserName	username	Account name.	Yes
UserAddress	user_address	User e-mail address, but not in the context of a communication between two parties.	
UserProfile	profile	User's profile name.	
ClientUserName	c_username	Client User name.	Yes

Column Name	Variable Name	Description	Indexed
		For example, the user name on the client (source) referenced in the event but not the actual event source.	
ObjectName	obj_name	Name of the object. **Note:** If this variable is used, **obj_type** should be used to describe what type of object this is.	
ObjectType	obj_type	Object type.	
ChangeAttribute	change_attribute	Changed attribute.	
ChangeOldValue	change_old	The prior value of an attribute or object in a change event.	
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	
Directory	directory	Directory name (file directory, not LDAP).	
DocumentNumber	doc_number	Document or file number.	
FileName	filename	Document name or filename.	
FilenameSize	filename_size	Size of the document or filename in bytes.	
SenderAddress	from	Messaging source address (not limited to e-mail, also includes Instant Messaging and other messaging concepts).	
RecipientAddress	to	Messaging destination address (not limited to e-mail, also includes Instant Messaging and other messaging	

Column Name	Variable Name	Description	Indexed
		concepts).	
Subject	subject	Messaging subject.	
TranslatedSenderAddress	trans_from	Translated messaging source address (not limited to e-mail, also includes Instant Messaging and other messaging concepts).	
TranslatedRecipientAddress	trans_to	Translated messaging destination address (not limited to e-mail, also includes Instant Messaging and other messaging concepts).	
URL	url	Uniform Resource Locator.	
WebPage	webpage	Web page.	
WebRoot	web_root	The root URL path.	
WebQuery	web_query	Query portion of the URL.	
Method	web_method	Web method. For example, POST or GET.	
WebHost	web_host	The hostname used in the web request.	
WebRefererHost	web_ref_host	Web referrer's hostname.	
Content	content_type	Content encoding type.	

Column Name	Variable Name	Description	Indexed
UserAgent	user_agent	User agent identifier. **Note:** This variable should only be used in reference to the browser identification string.	
Category	category	Category name.	Yes
Filter	filter	Filter category name.	Yes
FilterCategoryNumber	fcatnum	Filter category number.	
Group	group	Group name.	Yes
GroupID	groupid	Group ID number related to the group name.	
GroupObject	group_object	A collection or grouping of entities.	
EncryptionType	encryption_type	Contains one or more of the following encryption elements (but may include other encryption elements not explicitly listed here): • Encryption method used to generate the session key. • Encryption algorithm for the session. • Hashing algorithm for the session.	
PeerGateway	peer	Encryption peer's IP Address.	
PeerIdentity	peer_id	Encryption peer’s identity. For example, “subnet: 0.0.0.0 (mask=0.0.0.0) and host:	

Column Name	Variable Name	Description	Indexed
		a.b.c.d".	
IKE	ike	The IKE negotiation phase, for example, "Main Mode completion."	
Scheme	scheme	The encryption scheme used.	
IKECookieP1	ike_cookie1	The ID of the negotiation — sent for ISAKMP Phase One.	
IKECookieP2	ike_cookie2	The ID of the negotiation — sent for ISAKMP Phase Two.	
SourceSPI	src_spi	Source Security Parameter Index.	
DestinationSPI	dst_spi	Destination Security Parameter Index.	
ProcessID	process_id	Process ID number.	
Process	process	Process name.	
Counter1	dclass_counter1	Device class specific counter. **Note:** This variable is a storage field for a counter data type object that might be specific to the class of device.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	

Column Name	Variable Name	Description	Indexed
Counter2	dclass_counter2	Device class counter 2.	
Counter2String	dclass_counter2_string	A descriptive string that provides information about the **Counter2** value.	
InstanceName	instance	Instance name.	
TableName	tbl_name	Table name.	
Context	context	Additional information that provides contextual data for the event.	
SignatureID	sigid	IDS or IPS Int Signature ID.	
SignatureName	signame	The signature name, string, or Hex value.	
Department1	iassoc1	RESERVED	
Department2	iassoc2	RESERVED	
Department3	iassoc3	RESERVED	
Category1	eassoc1	RESERVED	
Category2	eassoc2	RESERVED	
Category3	eassoc3	RESERVED	
VID	vid	RESERVED	

Column Name	Variable Name	Description	Indexed
Inbound/Outbound	inout	Direction of the traffic flow.	Yes
Level	level	enVision event priority level.	
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
Type	ntype	Legacy field for event category information. **Note:** This variable will be removed in a future release.	
Information	info	Additional event information that could not be captured into a separate column.	
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column.	
IMClient	im_client	IM client information.	
IMUserID	im_userid	IM user ID.	
IMBuddyID	im_buddyid	IM buddy ID.	
OperatingSystem	os	Name of the OS.	
HardwareID	hardware_id	A unique identifier for a device or system.	

Column Name	Variable Name	Description	Indexed
		Note: This is not a MAC address.	
WiFiChannel	wifi_channel	The channel ID used by a Wireless Access Point.	
BSSID	bssid	Identity used to identify a BSS for an area. **Note:** In a wireless infrastructure, this variable is the MAC address of the AP. In an ad-hoc network, this variable is probably randomly generated.	
Message	msg	Raw event message.	

Intrusion

Below is a list of intrusion variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
Date/Time	stamp	RESERVED	
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
MessageID	msg_id	RESERVED	Yes
VID		RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity.	

Column Name	Variable Name	Description	Indexed
		Note: For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date and time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventLog	event_log	Name of the event log.	
EventTimeString	event_time_string	Date/Time of the occurrence of the event as recorded by the system that generated the event. **Note:** This field should be used if the format does not conform to RSA configuration specifications for the device.	Yes
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
EventType	event_type	The event category type as specified by event source generator. This variable can also be used to capture the attack name.	
Session	sessionid	Session ID.	
VendorEventCategory	vendor_event_cat	Category of the event. **Note:** This variable is a vendor-supplied data field and not generated from enVision. This variable should be	

Column Name	Variable Name	Description	Indexed
		used in situations where the vendor has adopted their own **event_category** taxonomy.	
OperationID	operation_id	An alert number or operation number. A common use case is referencing a vendor event number. The values should be unique and non-repeating.	
ReferenceID	id	Event or message ID.	Yes
LinkedReferenceID	id1	Linked event or message ID.	
Action	action	The action taken or proposed to be taken.	Yes
Disposition	disposition	The end state of the action.	Yes
ResultCode	resultcode	Result (Error) code. **Note:** This field is numeric.	Yes
Result	result	Results (Error) string.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured into a separate column.	
SourceAddress	saddr	Source IP address.	Yes

Column Name	Variable Name	Description	Indexed
SourceAddressv6	saddr_v6	Source IPv6 Address.	Yes
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	
SourceMacAddress	smacaddr	Source MAC address.	
TranslatedSourceAddress	stransaddr	Translated source address.	
TranslatedSourcePort	stransport	Translated source port.	
SourceZone	src_zone	Source zone.	
SourceInterface	sinterface	Source interface.	
SourcePayload	src_payload	Source payload.	
DestinationAddress	daddr	Destination address.	Yes
DestinationAddressv6	daddr_v6	Destination IPv6 Address.	Yes
DestinationPort	dport	Destination port.	Yes
DestinationHostName	dhost	Destination hostname.	
TranslatedDestinationAddress	dtransaddr	Translated destination address.	

Column Name	Variable Name	Description	Indexed
TranslatedDestinationPort	dtransport	Translated destination port.	
DestinationZone	dst_zone	Destination zone.	
DestinationInterface	dinterface	Destination interface.	
DestinationPayload	dst_payload	Destination Payload.	
Protocol	protocol	IP protocol name.	Yes
NetworkServiceName	network_service	The name of the network service, for example: FTP, SQL, and RPC	Yes
Direction	direction	Direction of the network flow.	Yes
DeviceMacAddress	macaddr	Device MAC address.	
IPAddress	hostip	Device IP address. **Note:** This variable should be used if the event does not indicate a communication between two parties.	Yes
IPAddressv6	hostip_v6	Device IPv6 Address. **Note:** This variable should be used if the event does not indicate a communication between two parties.	Yes
NetworkPort	network_port	Network port. This variable should be used to capture protocol port	Yes

Column Name	Variable Name	Description	Indexed
		information but only in the case where there is no inherently implied network communication occurring.	
HostName	hostname	Hostname.	Yes
FQDN	fqdn	Fully qualified domain name.	
EventComputer	event_computer	The hostname or IP of the system which originally generated the event. This variable may be used in situations where a log relay is in place and the hostname variable is referring to the relay.	
IPMask	mask	Device network mask.	
Interface	interface	Device interface name.	
Zone	zone	To be used when referring to a zone that does not have a concept of direction.	
Administrator	administrator	Administrative user name.	
UserName	username	Account name.	Yes
UserRole	user_role	The account or group name that the user's action is being performed under.	
DomainName	domain	Domain name.	
ClientUserName	c_username	Client user name, for example, a user name on the client (source) referenced in the event but not the actual event	Yes

Column Name	Variable Name	Description	Indexed
		source.	
Group	group	Group name. **Note:** This variable should be used only for a group of users.	Yes
Duration	duration	Duration of the event in minutes.	
StartTime	starttime	Start time of the event. **Note:** If you use this variable, you must also use **event_time**.	
EndTime	endtime	End time of the event.	
TimeZone	timezone	A time zone name or offset value.	
EventState	event_state	The current state of the object or item referenced within the event.	
PolicyID	policy_id	Policy ID. **Note:** This field is numeric.	
PolicyName	policyname	Policy Name.	Yes
Risk	risk	Policy Name.	Yes

Column Name	Variable Name	Description	Indexed
		Note: This is not a numeric value.	
RiskNumber	risk_num	Risk value. **Note:** This is a numeric value.	Yes
ThreatName	threat_name	Name of the threat, exploit, vulnerability or malware.	
ThreatValue	threat_val	A threat rating that is a measure of the threat level.	
Rule	rule	Rule number.	Yes
RuleName	rulename	Rule name.	Yes
RuleGroup	rule_group	The name of a grouping of rules. **Note:** This grouping should relate rule names or rule numbers.	Yes
RuleTemplate	rule_template	A default set of parameters that are overlaid onto a rule (or rule name), which effectively constitutes a template.	
TriggerValue	trigger_val	The conditions that caused an event to be recorded, for example, a value that exceeded a threshold.	
TriggerDesc	trigger_desc	Description of the trigger condition.	

Column Name	Variable Name	Description	Indexed
Info	Info	Additional event information.	
Context	context	Additional information that gives context to the event.	
ICMPType	icmptype	The "type" value for an ICMP packet.	
ICMPCode	icmpcode	The "code" value for an ICMP packet.	
ParentNodeName	parent_node	Parent node name.	
NodeName	node	Node name.	
VirtualName	vsys	Virtual system name.	
VLAN	vlan	VLAN number.	
WiFiChannel	wifi_channel	The channel ID used by a Wireless Access Point.	
SSID	ssid	Wireless SSID name.	
AccessPoint	access_point	Access point name.	
Version	version	Version of the application or OS that is generating the event.	
HostID	hostid	Host identifier.	
DistinguishedName	dn	X.500 (LDAP) distinguished name.	
Accesses	accesses	Actual privileges used in accessing an object.	

Column Name	Variable Name	Description	Indexed
Category	category	Category name.	Yes
FilterCategoryNumber	fcatnum	Filter category number.	
GroupObject	group_object	A collection or grouping of entities. For example, an interface group.	
Agent	agent	Agent that processes a portion of the event and is effectively handed off to.	
Product	product	The name of the product (software or hardware).	
Application	application	The name of the application (software).	
Service	service	A software daemon or service (a resident version of an application).	
Parameters	param	Parameters passed as part of a command or application.	
Process	process	Process name.	
ObjectName	obj_name	Object name.	
ObjectType	obj_type	Object type.	
DocumentNumber	doc_number	Document or file number.	
FileName	filename	Document or filename.	

Column Name	Variable Name	Description	Indexed
SenderAddress	from	Messaging source address (not limited to e-mail, also includes Instant Messaging and other messaging concepts).	
RecipientAddress	to	Messaging destination address (not limited to e-mail, also includes Instant Messaging and other messaging concepts).	
TranslatedSenderAddress	trans_from	Translated messaging source address (not limited to e-mail, also includes Instant Messaging and other messaging concepts).	
TranslatedRecipientAddress	trans_to	Translated messaging destination address (not limited to e-mail, also includes Instant Messaging and other messaging concepts).	
URL	url	Uniform Resource Locator.	
WebPage	webpage	Web page.	
WebHost	web_host	The hostname used in the web request.	
WebRoot	web_root	The root URL path.	
Circuit	circuit	Circuit name.	
Sensor	sensor	Sensor name.	Yes
SignatureID	sigid	Signature ID.	Yes
SignatureIDString	sigid_string	A string object of the **sigid** variable.	Yes

Column Name	Variable Name	Description	Indexed
SignatureID1	sigid1	A signature ID which, combined with **SignatureID**, represents a unique attack.	Yes
SignatureName	signame	Signature name, string, or hex value.	Yes
SignatureType	sigtype	Signature type.	Yes
VirusName	virusname	The name of the virus.	Yes
ChangeOldValue	change_old	The prior value of an attribute or object in a change event.	
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	
Bytes	bytes	Total bytes.	
ReceivedBytes	rbytes	Bytes received.	
SentBytes	sbytes	Bytes sent.	
Packets	packets	Total packets.	
EventCounter	event_counter	Number of times the event has repeated, or the total number of events aggregated.	
Counter1	dclass_counter1	Device class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	

Column Name	Variable Name	Description	Indexed
Counter2	dclass_counter2	Device class counter 2.	
Counter2String	dclass_counter2_string	A descriptive string that provides information about the **Counter2** value.	
Counter3	dclass_counter3	Device class counter 3.	
Counter3String	dclass_counter3_string	A descriptive string that provides information about the **Counter3** value.	
Ratio1	dclass_ratio1	Device class Ratio 1	
Ratio1String	dclass_ratio1_string	A descriptive string that describes the Ratio1 value.	
InstanceName	instance	Instance name.	
LocationDescription	location_desc	A description of the location relevant for the event being logged.	
Country	location_country	Country name.	
OperatingSystem	os	Name of the OS.	
SerialNumber	serial_number	Serial number associated with a physical asset.	
HardwareID	hardware_id	A unique identifier for a device or system. **Note:** This variable is not a MAC address.	
PeerGateway	peer	Encryption peer's IP Address	

Column Name	Variable Name	Description	Indexed
PeerIdentity	peer_id	Encryption peer's identity	
IKE	ike	The IKE negotiation phase.	
IKECookieP1	ike_cookie1	The ID of the negotiation — sent for ISAKMP Phase One.	
IKECookieP2	ike_cookie2	The ID of the negotiation — sent for ISAKMP Phase Two.	
EncryptionType	encryption_type	Contains one or more of the following encryption elements (but may include other encryption elements not explicitly listed here): Encryption method used to generate the session key, Encryption algorithm for the session, Hashing Algorithm for the session	
SourceSPI	src_spi	Source security parameter index.	
DestinationSPI	dst_spi	Destination security parameter index.	
Inbound/Outbound	inout	Direction of the traffic flow.	Yes
Level	level	RSA enVision event priority level.	
Comments	comments	Comment information.	
Message	msg	Raw message.	
Department1	iassoc1	RESERVED	
Department2	iassoc2	RESERVED	

Column Name	Variable Name	Description	Indexed
Department3	iassoc3	RESERVED	
Category1	eassoc1	RESERVED	
Category2	eassoc2	RESERVED	
Category3	eassoc3	RESERVED	

Mainframe

Below is a list of mainframe variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
Date/Time	stamp	RESERVED	
MessageID	msg_id	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject,	

Column Name	Variable Name	Description	Indexed
		ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventType	event_type	The event category type as specified by event source generator.	
ReferenceID	id	Event or message ID.	
OperationID	operation_id	An alert number or operation number. A common use case would be to reference a vendor event number. **Note:** The values should be unique and non-repeating.	
Action	action	The action taken or proposed to be taken. **Note:** For Databases, this is the SQL Query Statement.	Yes
Disposition	disposition	The end state of the action.	Yes
Result	result	Result (error) string.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact, relative to other events.	Yes

Column Name	Variable Name	Description	Indexed
SourceAddress	saddr	Source IP address.	
SourcePort	sport	Source port.	
DestinationAddress	daddr	Destination IP address.	
DestinationPort	dport	Destination port.	
IPAddress	hostip	Event source IP address.	Yes
HostName	hostname	Hostname. Preferably fully qualified.	Yes
Username	username	Account name.	Yes
UserID	uid	The unique user identifier that is associated with the user name.	
Group	group	Group name.	Yes
Info	info	Additional event information that could not be captured into a separate column.	
Version	version	Version of the application or OS which is generating the event.	
HostID	hostid	The host identifier.	
Terminal	terminal	Terminal.	

Column Name	Variable Name	Description	Indexed
Privilege	privilege	The privilege level or attributes recorded.	
Category	category	Category name.	Yes
Application	application	The name of the application (software).	
Process	process	Process name.	
InstanceName	instance	Instance name.	
DiskVolume	diskvolume	A unique name assigned to logical units (volumes) within a physical disk.	
Resource	resource	Name of the Mainframe resource that is being accessed or used.	Yes
ResourceClass	resource_class	Class to which the Mainframe resource belongs to.	Yes
Message	msg	Raw message.	

Malware

Below is a list of malware variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
Date/Time	stamp	RESERVED	
MessageID	msg_id	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the	

Column Name	Variable Name	Description	Indexed
		RSA enVision Enhanced Categorization Tagging guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventTimeString	event_time_string	Date or time of the occurrence of the event as recorded by the system that generated the event. **Note:** This field should be used if the format does not conform to RSA's configuration specifications for the event source.	Yes
EventSource	event_source	Source of the event.	Yes
VendorEventCategory	vendor_event_cat	Category of the event. This is a vendor supplied data field and not generated from RSA enVision.	
EventType	event_type	The event category type as specified by the event source generator.	
OperationID	operation_id	An alert number or operation number. A common use case is when referencing a vendor event number. **Note:** These values should be unique and non-repeating.	
ReferenceID	id	Event or message ID.	Yes

Column Name	Variable Name	Description	Indexed
Action	action	The action taken or proposed to be taken.	Yes
Disposition	disposition	The end state of the action.	Yes
Result	result	Result (error) string.	Yes
ResultCode	resultcode	Result (error) code. **Note:** This field is numeric.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column.	
SourceAddress	saddr	Source IP address.	Yes
SourceAddressv6	saddr_v6	Source IPv6 address.	Yes
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	
SourceDomain	sdomain	The source domain.	
SourceMacAddress	smacaddr	Source MAC address	

Column Name	Variable Name	Description	Indexed
SourceInterface	sinterface	Source interface.	
DestinationAddress	daddr	Destination address.	Yes
DestinationAddressv6	daddr_v6	Destination IPv6 Address.	Yes
DestinationPort	dport	Destination port.	Yes
DestinationHostName	dhost	Destination hostname.	
DestinationDomain	ddomain	Destination domain	
DestinationZone	dst_zone	Destination zone	
DestinationInterface	dinterface	Destination interface.	
DestMacAddress	dmacaddr	Destination MAC address	
DestinationMask	dmask	Destination device network mask	
Protocol	protocol	IP protocol name.	
NetworkServiceName	network_service	The name of the network service, for example, FTP, SQL, RPC.	
Direction	direction	Direction of the network flow.	
DeviceMacAddress	macaddr	Device MAC address.	
IPAddress	hostip	Device IP address, only in the case where there is no	Yes

Column Name	Variable Name	Description	Indexed
		inherently implied network communication occurring.	
IPAddressv6	hostip_v6	Device IPv6 Address.	Yes
HostName	hostname	Hostname. Preferably fully qualified.	Yes
FQDN	fqdn	Fully Qualified Domain Name.	Yes
Zone	zone	To be used when refering to a zone that dose not have a concept of direction	
UserName	username	Account name.	Yes
DomainName	domain	Domain name.	
ClientUserName	c_username	Client Username, not the actual event source.	Yes
Group	group	Group name. **Note:** This variable should only be used for a group of users.	Yes
DurationString	duration_string	A text string version of the duration. For example, 02:40.	
StartTime	starttime	Start time of the event.	

Column Name	Variable Name	Description	Indexed
EndTime	endtime	End time of the event.	
RecordedTime	recorded_time	The event time as recorded by the system the event is collected from.	
EventUser	event_user	The user who created the event, or the user who is the subject of the event.	
EventState	event_state	The current state of the object or item referenced within the event.	
PolicyID	policy_ID	Policy ID.	Yes
PolicyName	policyname	Policy name.	Yes
Risk	risk	Risk metric.	
RiskNumber	risk_num	Risk value for event logs that produce a risk metric.	
ThreatName	threat_name	Name of the threat, vulnerability, or malware.	
ThreatValue	threat_val	A threat rating that is a measure of the threat level	
Rule	rule	Rule number.	Yes
RuleName	rulename	Rule name.	Yes
RuleGroup	rule_group	The name of a grouping of rules. **Note:** This grouping should relate rule names or rule	

Column Name	Variable Name	Description	Indexed
		numbers.	
RuleTemplate	rule_template	A default set of parameters that is overlaid onto a rule, or rule name, which effectively constitutes a template.	
Info	info	Additional event information that could not be captured into a separate column.	
Context	context	Additional information that gives context to the event.	
Version	version	Version of the application or OS that is generating the event.	
ContentVersion	content_version	A version that indicates the release level of a signature.	
ComponentVersion	component_version	A version that reflects the version level of a sub-component of a product like a scan engine version.	
HostID	hostid	Host identifier.	
Accesses	accesses	Actual privileges used in accessing an object.	
UserAddress	user_address	User e-mail address, but not in the context of a communication between two parties.	
Category	category	Category Name.	Yes
GroupObject	group_object	A collection or grouping of entities.	

Column Name	Variable Name	Description	Indexed
HardwareID	hardware_id	A unique identifier for a device or system. **Note:** This variable is not a MAC address.	
OperatingSystem	os	Name of the operating system on the event source.	
Agent	agent	Agent that processes a portion of the event and is effectively handed off to.	
Product	product	The name of the product (software or hardware).	
Application	application	The name of the application (software).	
Service	service	A software daemon or service, a resident version of an application.	
Parameters	param	Parameters passed as part of a command or application.	
Process	process	Process name.	
ParentProcess	parent_process	The parent process name.	
ObjectName	obj_name	Object name.	
ObjectType	obj_type	Object type.	
DiskVolume	disk_volume	A unique name assigned to logical units (volumes) within a physical disk.	

Column Name	Variable Name	Description	Indexed
Directory	directory	Directory name.	
FileName	filename	Document or file name.	Yes
FileNameSize	filename_size	Size of the document or file name.	
SenderAddress	from	Messaging source address.	Yes
RecipientAddress	to	Messaging destination address.	Yes
Subject	subject	Messaging subject.	
URL	url	Uniform Resource Locator.	
Method	web_method	Web method (Example: POST, GET)	
Referer	web_referer	Request header referral	
SignatureID	sigid	The signature ID	
SignatureIDString	sigid_string	A string object of the **sigid** variable.	
SignatureID1	sigid1	A signature ID which combined with **SignatureID** represents a unique attack	
SignatureName	signame	Signature name, string, or hex value.	Yes
VirusName	virusname	The name of the virus.	Yes

Column Name	Variable Name	Description	Indexed
ChangeAttribute	change_attribute	Changed attribute.	
ChangeOldValue	change_old	The prior value of an attribute or object in a change event.	
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	
CheckSum	checksum	A fixed size value computed from a block of data primarily for integrity check purposes.	
Bytes	bytes	Total bytes.	
ReceivedBytes	rbytes	Bytes received	
SentBytes	sbytes	Bytes sent	
EventCounter	event_counter	Number of times the event has repeated, or the total number of events aggregated.	
Counter1	dclass_counter1	Number of viruses.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value, for example, "Number of Viruses" or "Virus count."	
Counter2	dclass_counter2	Number of infected computers.	
Counter2	dclass_counter2_string	A descriptive string that provides information about the **Counter2** value, for example, "Number of infected computers."	

Column Name	Variable Name	Description	Indexed
Counter3	dclass_counter3	Device class counter 3.	
Counter3String	dclass_counter3_string	A descriptive string that provides information about the **Counter3** value.	
LocationDescription	location_desc	A description of the location relevant for the event being logged.	
Message	msg	Raw message.	
EncryptionType	encryption_type	Contains one or more of the following encryption elements: ● Encryption method used to generate the session key. ● Encryption algorithm for the session. ● Hashing algorithm for the session.	

Messaging

Below is a list of messaging variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
Date/Time	stamp	RESERVED	
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
MessageID	msg_id	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the	

Column Name	Variable Name	Description	Indexed
		RSA enVision Enhanced Categorization Tagging guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or Time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventTimeString	event_time_string	This value always equals the **event_time**. **Note:** The primary usage for this variable is situations where customers have legacy data already captured in an alternate date format that does not conform to RSA configuration specifications for the event source.	Yes
EventLog	event_log	Name of the event log.	
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
EventType	event_type	The event category type as specified by the event source generator.	
EventState	event_state	The current state of the object or item referenced within the event, for example, Pending or In Progress.	
RecordedTime	recorded_time	The event time as recorded by the system from which the event is collected. For example, a multi-tiered application where the management layer of the system records its own	

Column Name	Variable Name	Description	Indexed
		timestamp at the time of collection from its child nodes. **Note:** This variable must be in timestamp format.	
Duration	duration	Duration of the event in minutes.	
DurationString	duration_string	A text string version of the duration.	
EventComputer	event_computer	The hostname or IP of the system that originally generated the event, for example, a Check Point firewall or a Check Point Smart Center. **Note:** This variable may be used in situations where a log relay is in place and the **hostname** variable is referring to the relay.	
ReferenceID	id	Event or Message ID.	Yes
Action	action	The action taken or proposed to be taken. **Note:** For Databases, this is the SQL Query Statement.	Yes
Disposition	disposition	The end state of the action.	Yes
ResultCode	resultcode	Result (error) code. This field is numeric.	Yes
Result	result	Result (Error) string.	Yes

Column Name	Variable Name	Description	Indexed
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column. **Note:** This column should be used only if the info column is also required.	
Context	context	Additional information that gives context to the event.	
SourceAddress	saddr	Source IP address.	Yes
SourceAddressv6	saddr_v6	Source IPv6 address.	Yes
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	
SourceInterface	sinterface	Source interface.	
DestinationAddress	daddr	Destination address.	Yes
DestinationPort	dport	Destination port.	Yes
DestinationHostName	dhost	Destination hostname.	
DestinationInterface	dinterface	Destination interface.	

Column Name	Variable Name	Description	Indexed
Protocol	protocol	IP protocol name.	
NetworkServiceName	network_service	The name of the network service. **Note:** Some services use multiple ports.	
IPAddress	hostip	Event source IP address. This variable should be used if the event does not indicate a communication between two parties.	Yes
HostName	hostname	Hostname.	Yes
UserName	username	Account name.	Yes
Group	group	Group name. This variable should only be used for a group of users.	Yes
DomainName	domain	Domain name.	
EventUser	event_user	The user who created the event, or the user who is the subject of the event. However, this variable should not be the user that is the actor in the event.	
OperationID	operation_id	An alert number or operation number. **Note:** These values should be unique and non-repeating.	

Column Name	Variable Name	Description	Indexed
LinkedReferenceID	id1	Linked (Related) Event or Message ID.	
LinkedReferenceID2	id2	Second Linked Event or Message ID. **Note:** This variable can be linked to either **id** or **id1**, but should not be used unless the other two variables are being used.	
Info	info	Additional event information that could not be captured in a separate column.	
Category	category	Category name.	Yes
Filter	filter	Filter category name.	
DistinguishedName	dn	Distinguished name.	
SourceDistinguishedName	src_dn	Source distinguished name.	
DestinationDistinguishedName	dst_dn	Destination distinguished name.	
GroupObject	group_object	A collection or grouping of entities, for example, an interface group.	
HardwareID	hardware_id	A unique identifier for an event source or system. **Note:** This is not a MAC address.	
Agent	agent	Agent that processes a portion of the event and is effec-	

Column Name	Variable Name	Description	Indexed
		tively handed off to.	
Product	product	The name of the product. **Note:** This can be either software or hardware.	
Application	application	The name of the software application.	
Service	service	A software daemon or service.	
Param	param	Parameters passed as part of a command or application.	
ProcessID	process_id	Process ID number.	
Process	process	Process name.	
ObjectName	obj_name	Object name.	
ObjectType	obj_type	Object type.	
Directory	directory	Directory name (file directory, not LDAP)	
FileName	filename	Document or file name.	
MailBox	mail_id	Mailbox name or ID.	
SenderAddress	from	Messaging source address.	Yes

Column Name	Variable Name	Description	Indexed
		Note: This is not limited to e-mail. It can also include instant messaging and other messaging concepts.	
RecipientAddress	to	Messaging destination address. **Note:** This variable is not limited to e-mail, and can also include instant messaging and other messaging concepts.	Yes
CC	cc	The Carbon Copy field usually associated with an e-mail.	
BCC	bcc	The Blind Carbon Copy field usually associated with an e-mail.	
UserAddress	user_address	User e-mail address, but not in the context of a communication between two parties.	Yes
Subject	subject	Messaging subject.	
MessageBody	message_body	The contents of the message body.	
PhoneNumber	phone_number	A telephone number.	Yes
VirusName	virusname	The name of the virus	
Direction	direction	Direction of the network flow for the systems that capture this.	Yes

Column Name	Variable Name	Description	Indexed
Bytes	bytes	Total bytes.	
Counter1	dclass_counter1	Event source class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the Counter1 value.	
Counter2	dclass_counter2	Event source class counter 2.	
Counter2String	dclass_counter2_string	A descriptive string that provides information about the Counter2 value.	
Counter3	dclass_counter3	Event source class counter 3.	
Counter3String	dclass_counter3_string	A descriptive string that provides information about the Counter3 value.	
DatabaseName	db_name	Database name.	
Message	msg	Raw Message.	

Midrange

Below is a list of midrange variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
Date/Time	stamp	RESERVED	
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
MessageID	msg_id	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the	

Column Name	Variable Name	Description	Indexed
		RSA enVision Enhanced Categorization Tagging guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes
Action	action	The action taken, or proposed to be taken.	Yes
Result	result	Result (error) string.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column.	
NetworkPort	network_port	Network port. **Note:** This variable should be used to capture protocol port information, but only in the case where there is no inherently implied network communication occurring.	Yes
HostName	hostname	Hostname.	Yes
FQDN	fqdn	Fully Qualified Domain Name.	
OwnerName	owner	The identity name of the owner of an object.	
ClientUserName	c_username	Client user name, for example, a user name on the client (source) referenced in the event, but not the actual event source.	Yes

Column Name	Variable Name	Description	Indexed
UserName	username	Account name.	Yes
UserID	uid	The unique user identifier that is associated with the user name.	
Group	group	Group name. Use for a group of users only.	
GroupID	groupid	Group ID number (related to the group name).	
NodeName	node	Node name.	
RemoteHostID	r_hostid	Host Identifier for a remote system.	
Terminal	terminal	Terminal.	
Accesses	accesses	Actual privileges used in accessing an object.	
Privilege	privilege	The privilege level or attributes recorded.	
Application	application	The name of the application (software).	
ProcessIDValue	process_id_val	Process ID value. **Note:** This variable is not an integer field.	
Process	process	Process name.	
ObjectName	obj_name	Object name.	

Column Name	Variable Name	Description	Indexed
ObjectType	obj_type	Object type.	
FileName	filename	Document or file name.	
Directory	directory	File directory name.	
Info	info	Additional event information.	
Message	msg	Raw message.	

Network

Below is a list of network variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
Date/Time	stamp	RESERVED	
DeviceClassName	DeviceClassName	RESERVED	Yes
MessageID	msg_id	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	

Column Name	Variable Name	Description	Indexed
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
EventType	event_type	The event category type as specified by event source generator.	

Column Name	Variable Name	Description	Indexed
EventState	event_state	The current state of the object or item referenced within the event.	
EventComputer	event_computer	The hostname or IP of the system which originally generated the event.	
EventTime	event_time	Date or Time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventTimeString	event_time_string	Date or Time of the occurrence of the event as recorded by the system that generated the event. **Note:** This variable should be used if the date format does not conform to RSA's configuration specifications for the event source.	Yes
StartTime	starttime	Start time of the event.	
EndTime	endtime	End time of the event.	
TimeZone	timezone	A time zone name or offset value, for example, -0400, +0600, EDT and GMT +0700.	
SourceAddress	saddr	Source IP address.	Yes
SourceAddressv6	saddr_v6	Source IPv6 Address	Yes
SourcePort	sport	Source Port.	Yes

Column Name	Variable Name	Description	Indexed
SourceHostName	shost	Source hostname.	
SourceMacAddress	smacaddr	Source MAC address.	Yes
SourceInterface	sinterface	Source interface.	Yes
SourceZone	src_zone	Source zone.	
DestinationAddress	daddr	Destination address.	Yes
DestinationPort	dport	Destination port.	Yes
DestinationHostName	dhost	Destination hostname.	
TranslatedDestinationAddress	dtransaddr	Translated destination address.	
TranslatedDestinationPort	dtransport	Translated destination port.	
DestMacAddress	dmacaddr	Destination MAC address.	Yes
DestinationInterface	dinterface	Destination interface.	Yes
DestinationZone	dst_zone	Destination zone.	
DestinationDomain	ddomain	Destination domain.	
Direction	direction	Direction of the network flow.	
Longitude	longitude	The north-south location.	

Column Name	Variable Name	Description	Indexed
Latitude	latitude	The east-west location.	
LocationDescription	location_desc	A description of the location relevant for the event being logged.	
Distance	distance	Distance from a location reference mark or from the device expressed in meters.	
ReferenceMark	location_mark	A reference location. **Note:** This variable can be used in conjunction with **distance** to provide a more accurate location.	
Floor	location_floor	Floor number.	
VirtualName	vsys	Virtual system name.	
NodeName	node	Node name.	
ParentNodeName	parent_node	Parent Node Name. **Note:** This variable must be related to the **node** variable.	
HostName	hostname	Hostname.	Yes
FQDN	fqdn	Fully Qualified Domain Name.	Yes
IPAddress	hostip	Device IP address.	Yes

Column Name	Variable Name	Description	Indexed
Network Port	network_port	Network port. This variable should be used to capture protocol information but only in the case where there is no inheritly implied network communication occurring.	Yes
IPMask	mask	Device network mask.	Yes
DeviceMacAddress	macaddr	Device MAC address.	Yes
Interface	interface	Device interface name.	Yes
Zone	zone	To be used when referring to a zone that does not have a concept of direction.	
VLAN	vlan	VLAN number.	Yes
WLAN	wlan	WLAN number.	Yes
SSID	ssid	Wireless SSID name.	Yes
BSSID	bssid	Identity used to identify a BSS for an area. **Note:** In a wireless infrastructure, this variable is the MAC address of the AP. In an ad hoc network, this variable is probably randomly generated.	Yes
WiFiChannel	wifi_channel	The channel ID used by a Wireless Access Point.	
AccessPoint	access_point	Access point name.	
Version	version	Version of the application or OS which is generating the	

Column Name	Variable Name	Description	Indexed
		event.	
PortName	portname	Physical or logical port connection, but does not include a network port for example, a printer port name.	
Device	device	Device associated with the node, for example, a physical disk, a printer, or a fan.	
Terminal	terminal	Terminal.	
NetworkServiceName	network_service	The name of the network service.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column.	
UserRole	user_role	The account or group name that the user's action is being performed under.	
UserDepartment	user_dept	User's department.	
Session	sessionid	Session ID.	
ConnectionID	connectionid	Connection ID.	
TriggerValue	trigger_val	The conditions that caused an event to be recorded.	
Method	web_method	Web method. For example, POST or GET.	

Column Name	Variable Name	Description	Indexed
URL	url	Uniform Resource Locator.	
WebPage	webpage	Web page.	
WebQuery	web_query	Query portion of the URL.	
ResultCode	code	Result (Error) Code. **Note:** This field is numeric.	
InOut	inout	Directionality of the traffic flow.	Yes
Result	result	Result (Error) String.	Yes
LogonID	logon_id	Unique identifier for an account.	
EventUser	event_user	The user which created the event or the user which is the subject of the event. However, it should not be the user that is the actor in the event.	
Administrator	administrator	Administrative user name.	Yes
UserName	username	Account name.	Yes
UserID	uid	The unique user identifier that is associated with the user name.	
ClientUserName	c_username	Client user name, for example, a scenario could include a user name on the client (source), referenced in the event, but not the actual event source.	Yes

Column Name	Variable Name	Description	Indexed
LogonType	logon_type	The type of logon. Some systems record a value for the level to which a logon was performed, for example, interactive vs non-interactive.	
Privilege	privilege	The privilege level or attributes recorded.	
AuthenticationMethod	authmethod	Authentication mechanism.	
DistinguishedName	dn	X.500 (LDAP) distinguished name.	
SentBytes	sbytes	Bytes sent.	
ReceivedBytes	rbytes	Bytes received.	
Bytes	bytes	Total bytes.	
Packets	packets	Total packets.	
Counter1	number	Device class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	
Counter2	dclass_counter2	Device class counter 2.	
Counter2String	dclass_counter2_string	A descriptive string that provides information about the **Counter2** value.	

Column Name	Variable Name	Description	Indexed
Counter3	dclass_counter3	Device class counter 3.	
Counter3String	dclass_counter3_string	A descriptive string that provides information about the **Counter3** value.	
ServerTime	time	Server time.	
SenderAddress	from	Messaging source address.	
CallingFrom	calling_from	The telephone number from which a call is coming.	
RecipientAddress	to	Messaging destination address.	
CallingTo	calling_to	The telephone number being called.	
DomainName	domain	Domain name.	
FilterCategoryNumber	fcatnum	Filter category number.	
Group	group	Group name.	Yes
GroupObject	group_object	A collection or grouping of entities.	
PoolName	pool_name	The name of a resource pool.	
Process	process	Process name.	
ProcessID	process_id	Process ID number.	

Column Name	Variable Name	Description	Indexed
ChildProcessID	child_pid	Child process ID number.	
OperationID	operation_id	An alert number or operation number.	
Parameters	param	Parameters passed as part of a command or application.	
ReferenceID	id	Event or message ID.	Yes
LinkedReferenceID	id1	Linked or related event or message ID.	
Info	info	Additional event information.	
EventSource	event_source	Source of the event.	Yes
EventLog	event_log	The name of the event log	
ObjectName	obj_name	Object name.	
ObjectType	obj_type	Object type.	
FileName	filename	Document or Filename.	
ContentType	content_type	Content encoding type.	
Application	application	The name of the application (software).	
Type	ntype	Legacy field for event category information. **Note:** This variable will be removed in a future release.	

Column Name	Variable Name	Description	Indexed
Protocol	protocol	IP protocol name.	Yes
ICMPType	icmptype	The **type** value for an ICMP packet	
ICMPCode	icmpcode	The **code** value for an ICMP packet	
ProtocolDetail	protocol_detail	IP protocol details. **Note:** This variable is for protocols that do not contain details such as ports.	
Gateway	gateway	Gateway to use with routing information.	
AccessListNo	list_name	Access list number.	
Directory	directory	Directory name.	
UserOrganization	user_org	User organization.	
Referrer	web_referer	Request header referral.	
PolicyName	policyname	Policy name.	
RuleName	rulename	Rule name.	
RuleTemplate	rule_template	A default set of parameters which are overlaid onto a rule (or rule name), which effectively constitutes a template.	
Duration	duration	Duration of the event in minutes.	

Column Name	Variable Name	Description	Indexed
Service	service	A software daemon or service.	
EncryptionType	encryption_type	Contains one or more of the following encryption elements: • Encryption method used to generate the session key. • Encryption algorithm for the session. • Hashing Algorithm for the session.	
Category	sigcat	Category name.	
Filter	filter	Filter category name.	
UserAddress	user_address	User e-mail address.	
Context	context	Additional information that gives context to the event.	
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
OwnerName	owner	The identity of the owner of an object.	
Disposition	disposition	The end state of the action.	Yes
Action	action	The action taken or proposed to be taken.	Yes
ChangeOldValue	change_old	The prior value of an attribute or object in a change event.	

Column Name	Variable Name	Description	Indexed
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	
Product	product	The name of the product (software or hardware).	
SerialNumber	serial_number	Serial number associated with a physical asset.	
DatabaseName	db_name	Database name.	
CertificateHostname	cert_hostname	The Hostname value of a certificate.	
SourceSSLVersion	s_sslver	Source (Client) SSL version.	
SourceCipher	s_cipher	Source (Client) cipher.	
DestinationSSLVersion	d_sslver	Destination (Server) SSL version.	
DestinationCipher	d_cipher	Destination (Server) cipher.	
Department1	iassoc1	RESERVED	
Department2	iassoc2	RESERVED	
Department3	iassoc3	RESERVED	
Category1	eassoc1	RESERVED	
Category2	eassoc2	RESERVED	
Category3	eassoc3	RESERVED	

Column Name	Variable Name	Description	Indexed
VID	vid	RESERVED	
Message	msg	Raw event message.	

Storage

Below is a list of storage variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
Date/Time	stamp	RESERVED	
MessageID	msg_id	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the	

Column Name	Variable Name	Description	Indexed
		RSA enVision Enhanced Categorization Tagging guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or Time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventLog	event_log	Name of the event log.	
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
EventType	event_type	The event category type as specified by the event source generator.	
OperationID	operation_id	An alert number or operation number. Common use case: referencing a vendor event number. **Note:** The values should be unique and non-repeating typically.	
ReferenceID	id	Event/Message ID.	Yes
Action	action	The action taken or proposed to be taken. **Note:** For databases this variable is the SQL Query Statement.	Yes
Disposition	disposition	The end state of the action.	Yes

Column Name	Variable Name	Description	Indexed
ResultCode	resultcode	Result (error) code. **Note:** This field is numeric.	Yes
Result	result	Result (error) string.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured into a separate column. **Note:** This column should be used only if the info column is also required.	
SourceAddress	saddr	Source IP address.	Yes
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	
SourceZone	src_zone	Source zone.	
DestinationAddress	daddr	Destination address.	Yes
DestinationPort	dport	Destination port.	Yes

Column Name	Variable Name	Description	Indexed
DestinationHostName	dhost	Destination hostname.	
DestinationZone	dst_zone	Destination zone.	
Protocol	protocol	IP protocol name.	
Gateway	gateway	The gateway to be used when handling routing information.	
NetworkServiceName	network_service	Name of the network service, for example ftp, SQL, or RPC.	
IPAddress	hostip	Device IP address. It should be used if the event does not indicate a communication between two parties.	Yes
NetworkPort	network_port	This variable should be used to capture protocol port information but only where there is no inherited implied network	Yes
HostName	hostname	Hostname. Preferably fully qualified.	Yes
FQDN	fqdn	The fully qualified domain name	
Interface	interface	Event source interface name.	
EventComputer	event_computer	The hostname or IP of the system which originally generated the event.	

Column Name	Variable Name	Description	Indexed
		Note: This variable may be used in situations where a log relay is in place, and the **hostname** variable is referring to the relay.	
SID	sid	Security ID. **Note:** This variable is a unique concept to Windows accounts and should not be used otherwise.	
Username	username	Account name.	Yes
DomainName	domain	Domain name.	
LogonID	logon_id	Unique identifier for an account.	
SessionID	sessionid	Session ID.	
ClientSID	c_sid	Client SID.	
ClientUserName	c_username	Client user name, for example, a username on the client, referenced in the event, but not the actual event source.	Yes
ClientDomain	c_domain	Client domain.	
LinkedSessionID	sessionid1	Linked (related) session ID.	
Group	group	Group name.	Yes

Column Name	Variable Name	Description	Indexed
Duration	duration	Duration of the event in minutes.	
RecordedTime	recorded_time	The event time as recorded by the system from which the event is collected. A usage scenario is a multi-tier application where the management layer of the system records its own timestamp at the time of collection from its child nodes. **Note:** This variable must be in timestamp format.	
EventUser	event_user	The user who created the event, or the user who is the subject of the event. However, it should not be the user that is the actor in the event.	
EventState	event_state	The current state of the object/item referenced within the event.	
LinkedReferenceID	id1	Linked (related) event or message ID.	
LinkedReferenceID2	id2	Second linked event or message ID. **Note:** This variable can be linked to either **id** or **id1**, but should not be used unless the other two variables are in use.	
ConnectionID	connectionid	Connection ID.	
PolicyID	policy_id	Policy ID. This is a numeric field.	

Column Name	Variable Name	Description	Indexed
PolicyValue	policy_value	The contents of the policy itself. **Note:** This variable should contain the details of what the policy does.	
RuleName	rulename	Rule Name. **Note:** This variable is not always populated. Many products only record a rule number, and not an associated descriptive rule name.	Yes
RuleGroup	rule_group	The name of a grouping of rules. This grouping should relate rulenames and/or rule numbers.	
WorkspaceDescription	workspace_desc	A collection of policies, possibly including rules as well, which are organized together into a "workspace."	
AuditRecord	audit_record	The audit record number.	
AuditClass	audit_class	The class name of the functional audit area.	
AuditObject	audit_object	The name or identifier of the object that is subject of the audit event.	
TriggerValue	trigger_val	The conditions which caused an event to be recorded. For example, a value that exceeded a threshold.	
Info	info	Additional event information that could not be captured	

Column Name	Variable Name	Description	Indexed
		into a separate column.	
NodeName	node	The node name	
VirtualName	vsys	Virtual system name.	
Version	version	Version of the application or OS that is generating the event.	
ContentVersion	content_version	A version which indicates the release level of a signature, database content, or a document.	
RemoteHostID	r_hostid	Host Identifier for a remote system. **Note:** This variable is to be used in the context of an event that also has a **hostid**.	
HostID	hostid	Host identifier.	
PortName	portname	Physical or logical port connection. **Note:** This variable does not include a network port, for example, a printer port name.	
Device	device	Device associated with the node, for example: a physical disk, a printer, or a fan.	
RemoteDomainName	remote_domain	Remote domain name.	

Column Name	Variable Name	Description	Indexed
RemoteDomainID	remote_domain_id	Remote domain ID.	
UserRole	user_role	The account or group name under which a user action is being performed.	
Accesses	accesses	Actual privileges used in accessing an object, for example, Read or Write.	
Privilege	privilege	The privilege lever or attributes recorded.	
PatientID	patient_id	Patient identifier.	
Category	category	Category name.	Yes
GroupObject	group_object	A collection or grouping of entities. For example, an interface group.	
GroupID	groupid	Group ID Number (related to the group name).	
Agent	agent	The agent that processes a portion of the event and is effectively handed off to.	
Product	product	The name of the product (software or hardware).	
Application	application	The name of the application (software).	
Service	service	A software daemon or service (A resident version of an application).	

Column Name	Variable Name	Description	Indexed
Parameters	param	Parameters passed as part of a command or application.	
Process	process	Process name.	
ProcessID	process_id	Process ID number.	
DataType	data_type	The classification type of the data that is the subject of the event referenced, for example, a SSN or Credit Card.	
ObjectServer	obj_server	Object server.	
ObjectType	obj_type	Object type.	
ObjectName	obj_name	Name of the object. **Note:** You must use obj_type to describe what type of object this is.	
Directory	directory	Directory name (file directory, not LDAP).	
FileName	filename	Document or file name.	
URL	url	Uniform Resource Locator.	
WebPage	webpage	Web page.	
ChangeAttribute	change_attribute	Changed attribute.	
ChangeOldValue	change_old	The prior value of an attribute or object in a change event.	

Column Name	Variable Name	Description	Indexed
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	
Bytes	bytes	Total bytes.	
SentBytes	sbytes	Bytes sent.	
ReceivedBytes	rbytes	Bytes received.	
Counter1	dclass_counter1	Device class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the Counter1 value.	
Message	msg	Raw message.	
PortWorldWideName	pwwn	Port World Wide Name. A WWN uniquely identifying a port on a Host Bus Adapter.	
NodeWorldWideName	nwwn	Node World Wide Name. A WWN uniquely identifying a Host Bus Adapter, shared by all ports on that Host Bus Adapter.	
DiskVolume	disk_volume	A unique name assigned to logical units (volumes) within a physical disk.	
LUN	lun	Logical Unit Number.	

Column Name	Variable Name	Description	Indexed
Department1	iassoc1	RESERVED	
Department2	iassoc2	RESERVED	
Department3	iassoc3	RESERVED	
Category1	eassoc1	RESERVED	
Category2	eassoc2	RESERVED	
Category3	eassoc3	RESERVED	

Universal

Below is a list of the variables in the universal table and brief descriptions of the meaning of each variable.

Note: The Universal table is available for selection in RSA enVision versions 3.7 and 4.0. However, this table is not populated with data for enVision versions earlier than 4.1.

The Universal table is a superset of all the variables used for parsing data from event source logs. To better understand the usage and organization of the columns in the Universal table, refer to each of the variable categories, **Content 2.0 Variables**.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
Date/Time	stamp	RESERVED	
DeviceAddress	paddr	RESERVED	
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	
DeviceClassName	deviceclassname	RESERVED	
EventCategory	ecategory	RESERVED	
EventCategoryName	eventcatname	RESERVED	

Column Name	Variable Name	Description	Indexed
Level	level	RSA enVision event priority level.	
MessageID	msg_id	RESERVED	
enVisionDomain		RESERVED	
enVisionSite		RESERVED	
enVisionNode		RESERVED	
VID		RESERVED	
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	

Column Name	Variable Name	Description	Indexed
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or time of the occurrence of the event as recorded by the system that generated the event.	
EventTimeString	event_time_string	Date or time of the occurrence of the event as recorded by the system that generated the event. **Note:** This field should be used if the format does not conform to RSA configuration specifications for the event source.	

Column Name	Variable Name	Description	Indexed
EventLog	event_log	Name of the event log.	
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	
VendorEventCategory	vendor_event_cat	Category of the event. **Note:** This variable is a vendor supplied data field and is not generated from RSA enVision.	
EventType	event_type	The event category type as specified by event source generator.	
Session	sessionid	Session ID.	
OperationID	operation_id	An alert number or operation number. A common use case would be to reference a vendor event number. **Note:** The values should be unique and non-repeating.	
ReferenceID	id	Event or message ID.	
Action	action	The action taken or proposed to be taken. **Note:** For databases, this variable is the SQL Query Statement.	

Column Name	Variable Name	Description	Indexed
Disposition	disposition	The end state of the action.	
ResultCode	resultcode	Result (error) code. **Note:** This field is numeric.	
Result	result	Result (error) string.	
Severity	severity	A value that is assigned to an event that indicates the level of impact, relative to other events.	
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column. **Note:** This column should only be used if the info column is also required.	
SourceAddress	saddr	Source IP address.	
SourceAddressv6	saddr_v6	Source IPv6 address.	
SourcePort	sport	Source port.	
SourceHostName	shost	Source hostname.	
SourceDomain	sdomain	The source domain	

Column Name	Variable Name	Description	Indexed
TranslatedSourceAddress	stransaddr	Translated source address.	
TranslatedSourcePort	stransport	Translated source port.	
SourceZone	src_zone	Source zone.	
SourceMacAddress	smacaddr	Source MAC address.	
SourceMask	smask	Source device network mask.	
SourceInterface	sinterface	Source interface.	
SourcePayload	src_payload	Source payload.	
DestinationAddress	daddr	Destination address.	
DestinationAddressv6	daddr_v6	Destination IPv6 address.	
DestinationPort	dport	Destination port.	
DestinationHostName	dhost	Destination hostname.	
DestinationDomain	ddomain	Destination domain.	
TranslatedDestinationAddress	dtransaddr	Translated destination address.	
TranslatedDestinationPort	dtransport	Translated destination port.	
DestinationZone	dst_zone	Destination zone.	

Column Name	Variable Name	Description	Indexed
DestMacAddress	dmacaddr	Destination MAC address.	
DestinationMask	dmask	Destination device network mask.	
DestinationInterface	dinterface	Destination interface.	
DestinationPayload	dst_payload	Destination payload.	
Protocol	protocol	IP protocol name.	
Gateway	gateway	Gateway to use when dealing with routing information.	
NetworkServiceName	network_service	The name of the network service, for example, ftp, SQL, or RPC.	
Direction	direction	Direction of the network flow.	
TypeOfService	tos	The priority given to a network protocol.	
DeviceMacAddress	macaddr	Event source MAC address.	
IPAddress	hostip	Event source IP address. Use if the event does not indicate a communication between two parties.	
IPAddressv6	hostip_v6	Event source IPv6 address. Use if the event does not indicate a communication between two parties.	
NetworkPort	network_port	Network port.	

Column Name	Variable Name	Description	Indexed
		Note: This variable should be used to capture protocol port information, but only in the case where there is no inherently implied network communication occurring.	
HostName	hostname	Hostname.	
FQDN	fqdn	Fully qualified domain name.	
EventComputer	event_computer	The hostname or IP of the system that originally generated the event. This variable may be used in situations where a log relay is in place and the hostname variable is referring to the relay.	
IPMask	mask	Device network mask.	
Interface	interface	Device interface name.	
Zone	zone	To be used when referring to a zone that does not have a concept of direction.	
OwnerName	owner	The identity name of the owner of an object, for example, file, directory, and policy.	
Administrator	administrator	Administrative user name.	
SID	sid	The security ID	
UserName	username	Account name.	

Column Name	Variable Name	Description	Indexed
DomainID	domain_id	Pre Windows 2000 (NetBIOS) name of the domain ONLY.	
DomainName	domain	Domain name.	
LogonID	logon_id	Unique identifier for an account.	
ClientSID	c_sid	The client security ID	
ClientUserName	c_username	Client user name. For example, a user name on the client (source) referenced in the event, but not the actual event source.	
ClientDomain	c_domain	Client domain.	
ClientLogonID	c_logon_id	Client logon ID.	
UserID	uid	The unique user identifier that is associated with the user name.	
Group	group	Group name. Use for a group of users only.	
GroupID	groupid	Group ID number related to the group name.	
Duration	duration	Duration of the event in minutes.	
DurationString	duration_string	A text string version of the duration.	

Column Name	Variable Name	Description	Indexed
StartTime	starttime	Start time of the event. **Note:** If you use this variable, you must also use **event_time**.	
EndTime	endtime	End time of the event.	
EventQueueTime	event_queue_time	Time that the event was queued.	
ExpirationTime	expiration_time	A timestamp that explicitly refers to an expiration.	
EffectiveTime	effective_time	A timestamp that explicitly refers to an expiration.	
RecordedTime	recorded_time	The event time as recorded by the system the event is collected from. For example, a multi-tiered application where the management layer of the system records its own timestamp at the time of collection from its child nodes. **Note:** This variable must be in timestamp format.	
TimeZone	timezone	A time zone name or offset value.	
EventUser	event_user	The user that created the event or the user that is the subject of the event. However, it should not be the user that is the actor in the event.	
EventState	event_state	The current state of the object or item referenced within the event.	

Column Name	Variable Name	Description	Indexed
ConnectionID	connectionid	Connection ID.	
LinkedSessionID	sessionid1	Linked (related) session ID.	
LinkedReferenceID	id1	Linked (related) event/message ID.	
LinkedReferenceID2	id2	Second linked event/message ID. It can be linked to id or id1 but should not be used unless the other two variables are being used.	
AccessListNo	listnum	Access list number.	
PolicyID	policy_id	Policy ID (numeric field).	
PolicyName	policyname	Policy name.	
PolicyValue	policy_value	The contents of the policy itself. **Note:** This should contain the details of what the policy does.	
PolicyVersion	policy_version	The version identifier for the policy, or configuration, of the device or application.	
Risk	risk	Risk value that is not a numeric value.	
RiskNumber	risk_num	Risk value for event logs that produce a risk metric.	

Column Name	Variable Name	Description	Indexed
		Note: You cannot typically relate risk values produced by separate products.	
Rule	rule	Rule number.	
RuleUID	rule_uid	Unique Identifier for a rule. Some products also leverage a unique identifier for rules in addition to a rule number.	
RuleName	rulename	Rule name. **Note:** This variable is not always populated. Many products only record a rule number and not an associated descriptive rule name.	
RuleGroup	rule_group	The name of a grouping of rules. **Note:** This grouping should relate rule names and/or rule numbers.	
RuleGroupID	rule_groupid	Rule group ID.	
RuleTemplate	rule_template	A default set of parameters that are overlapped onto a rule (or rulename) that effectively constitutes a template.	
AuditClass	audit_class	The class name of the functional audit area.	
AuditObject	audit_object	The name, or identifier, of the object that is subject of the audit event.	

Column Name	Variable Name	Description	Indexed
ExpectedValue	expected_val	The value that the system was expecting to see (from the perspective of the device generating the log).	
ObservedValue	observed_val	The value that the system actually observed (or received, found etc). This variable should be used in conjunction with expected_val.	
TriggerValue	trigger_val	The conditions that caused an event to be recorded., for example, an exceeded threshold.	
TriggerDesc	trigger_desc	Description of the trigger condition.	
SubjectContext	s_context	This variable is used in an audit context where the subject is the object being identified.	
TargetContext	t_context	This variable is used in an audit context where the Target is the object being identified.	
Info	info	Additional event information that could not be captured in a separate column.	
Context	context	Additional information that gives context to the event.	
ICMPType	icmptype	The type value for an ICMP packet.	
ICMPCode	icmpcode	The code value for an ICMP packet.	
ProtocolDetail	protocol_detail	IP protocol details.	

Column Name	Variable Name	Description	Indexed
		Note: For protocols that do not contain details such as ports, this is the place to capture that information.	
ParentNodeName	parent_node	Parent node name.	
NodeName	node	Node name. A common use case is the node name within a cluster where the cluster name is reflected by the hostname. In configuration management systems, this would store the name of the event source being managed.	
VirtualName	vsys	Virtual system name.	
VLAN	vlan	VLAN number.	
WLAN	wlan	WLAN number.	
SSID	ssid	Wireless SSID name.	
BSSID	bssid	Identity used to identify a BSS for an area. In a wireless infrastructure this will be the MAC address of the AP. In an ad hoc network this is probably randomly generated.	
WiFiChannel	wifi_channel	The channel ID used by a wireless access point.	
AccessPoint	access_point	Access point name.	
VMTarget	vm_target	VMWare target.	

Column Name	Variable Name	Description	Indexed
		Note: This variable can only be used for VMWare.	
Version	version	Version of the application or OS that is generating the event.	
ContentVersion	content_version	A version that indicates the release level of a signature or database content. Common uses are antivirus signatures or IDS signatures.	
ComponentVersion	component_version	A version that reflects the version level of a sub-component of a product.	
HostID	hostid	Host identifier.	
RemoteHostID	r_hostid	Host identifier for a remote system. To be used in the context of an event that also has a host ID.	
PortName	portname	Physical or logical port connection but does not include a network port, for example, a printer port name.	
Device	device	Device associated with the node, for example, a physical disk, a printer, or a fan.	
Terminal	terminal	Terminal.	
LogonType	logon_type	The type of logon. **Note:** Some systems record a value for the level in which	

Column Name	Variable Name	Description	Indexed
		a logon was performed (interactive vs non-interactive).	
Realm	realm	Radius realm, or similar grouping of accounts.	
DistinguishedName	dn	X.500 (LDAP) distinguished name.	
SourceDistinguishedName	sdn	An X.500 (LDAP) distinguished name that's used in a context which indicates a source.	
DestinationDistinguishedName	ddn	An X.500 (LDAP) distinguished name that's used in a context which indicates a destination.	
Accesses	accesses	Actual priviliges used in accessing an object.	
AuthenticationMethod	authmethod	Authentication mechanism.	
Privilege	privilege	The privilege level or attributes recorded.	
ServiceAccount	service_account	The name (including domain if applicable) of the account a service (referenced in the event) is running under.	
UserRole	user_role	The account or group name under which a user action is being performed.	
UserFullName	user_fullname	The full name of a user. **Note:** This variable is sometimes called Real Name.	

Column Name	Variable Name	Description	Indexed
UserFirstName	user_fname	The first name of the user.	
UserMiddleName	user_mname	The middle name of the user.	
UserLastName	user_lname	The last name of the user.	
UserAddress	user_address	User e-mail address, but not in the context of communication between two parties.	
UserOrganization	user_org	User organization.	
UserDepartment	user_dept	The department of the user.	
UserProfile	profile	The profile name of the user.	
FederatedIdentityProvider	federated_idp	The Federated Identity Provider. **Note:** This variable is the server providing the authentication.	
FederatedServiceProvider	federated_sp	The Federated Service Provider. **Note:** This variable is the application requesting authentication.	
PatientID	patient_id	Patient identifier.	
PatientFullName	patient_fullname	Full name of the patient.	

Column Name	Variable Name	Description	Indexed
PatientFirstName	patient_fname	First name of the patient.	
PatientMiddleName	patient_mname	Middle name of the patient.	
PatientLastName	patient_lname	Last name of the patient.	
Category	category	Category name.	
Filter	filter	Filter category name.	
FilterCategoryNumber	fcatnum	Filter category number.	
FilterResult	fresult	Filter result.	
GroupObject	group_object	A collection or grouping of entities. **Note:** This variable is not specific to authentication.	
PoolID	pool_id	The identifier of a resource pool. **Note:** This variable is typically a numeric field.	
PoolName	pool_name	The name of a resource pool.	
HardwareID	hardware_id	A unique identifier for a device or system (not a MAC address).	
Agent	agent	Agent that processes a portion of the event, and is effectively handed off to.	

Column Name	Variable Name	Description	Indexed
Product	product	The name of the product. **Note:** This variable can represent either software or hardware.	
Application	application	The name of the application (software).	
Service	service	A software daemon or service. **Note:** This variable is a resident version of an application.	
Parameters	param	Parameters passed as part of a command or application.	
ProcessID	process_id	Process ID number.	
ProcessIDValue	process_id_val	Process ID value (Non integer field).	
Process	process	Process name.	
ParentProcessID	parent_pid	Parent Process ID number.	
ParentProcess	parent_process	The parent process name	
ChildProcessID	child_pid	Child process ID number.	
ChildProcess	child_process	Child process name.	

Column Name	Variable Name	Description	Indexed
Data	data	Data field. The data_type variable is used to describe the type of data being represented in this field.	
DataType	data_type	The classification type of the data that is the subject of the event referenced.	
Object Server	obj_server	Object server.	
ObjectName	obj_name	Name of the object. **Note:** You must use **obj_type** to describe what type of object this variable is.	
ObjectType	obj_type	Object type.	
Inode	inode	An inode stores basic information about a regular file, directory, or other file system object.	
Directory	directory	Directory name. **Note:** This variable represents a file directory, not LDAP.	
DocumentNumber	doc_number	Document or file number.	
FileName	filename	Document or filename.	
FileNameSize	filename_size	Size of the document or file.	
PhoneNumber	phone_number	A telephone number.	

Column Name	Variable Name	Description	Indexed
CallingFrom	calling_from	The telephone number from which a call is coming.	
CallingTo	calling_to	The telephone number being called.	
MailBox	mail_id	Mailbox name or ID.	
SenderAddress	from	Messaging source address (Not limited to e-mail, also includes Instant Messaging and other messaging concepts).	
RecipientAddress	to	Messaging destination address (Not limited to e-mail, also includes Instant Messaging and other messaging concepts).	
CC	cc	The CC field usually associated with an e-mail.	
BCC	bcc	The BCC field usually associated with an e-mail.	
Subject	subject	Messaging subject.	
MessageBody	message_body	The contents of the message body.	
TranslatedSenderAddress	trans_from	Translated messaging source address (not limited to e-mail, also includes instant messaging and other messaging concepts).	
TranslatedRecipientAddress	trans_to	Translated messaging destination address (not limited to e-mail, also includes instant messaging and other messaging concepts).	

Column Name	Variable Name	Description	Indexed
Method	web_method	Web method, for example, POST or GET.	
URL	url	Uniform Resource Locator.	
WebHost	web_host	The hostname used in the web request.	
WebDomain	web_domain	Web domain.	
WebRoot	web_root	The root URL path.	
WebPage	webpage	Web page.	
WebQuery	web_query	Query portion of the URL.	
Referer	web_referer	Request header referral.	
WebRefererHost	web_ref_host	Web referrer hostname.	
WebRefererDomain	web_ref_domain	Web referrer domain.	
WebRefererRoot	web_ref_root	Web referrer root URL path.	
WebRefererPage	web_ref_page	Web referrer page.	
WebRefererQuery	web_ref_query	Web referrer query portion of the URL.	
WebCookie	web_cookie	The cookies passed within a web request.	
UserAgent	user_agent	User agent identifier. This variable should probably only be used in reference to the browser identification string.	

Column Name	Variable Name	Description	Indexed
		Other use cases could be considered on a one by one basis.	
Content	content_type	Content encoding type.	
Hierarchy	h_code	Hierarchy.	
Circuit	curcuit	Circuit name.	
Sensor	sensor	Sensor name.	
SignatureID	sigid	Signature ID.	
SignatureIDString	sigid_string	A string object of the sigid variable.	
SignatureID1	sigid1	A signature ID which, combined with SignatureID, represents a unique attack.	
SignatureName	signame	Signature Name/String/Hex value.	
SignatureType	sigtype	Signature type.	
CVEReference	cve	CVE reference.	
VirusName	virusname	The name of the virus.	
ChangeAttribute	change_attribute	Changed attribute.	

Column Name	Variable Name	Description	Indexed
ChangeOldValue	change_old	The prior value of an attribute or object in a change event.	
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	
LDAPAttribute	ldap_attribute	LDAP attribute string name.	
CheckSum	checksum	A fixed size value computed from a block of data primarily for integrity check purposes.	
Bytes	bytes	Total bytes.	
ReceivedBytes	rbytes	Bytes received.	
SentBytes	sbytes	Bytes sent.	
Packets	packets	Total packets.	
EventCounter	event_counter	Number of times that the event has repeated or the total number of events aggregated.	
Counter1	dclass_counter1	Device class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	
Counter2	dclass_counter2	Device class counter 2.	
Counter2String	dclass_counter2_string	A descriptive string that provides information about the **Counter2** value.	

Column Name	Variable Name	Description	Indexed
Counter3	dclass_counter3	Device class counter 3.	
Counter3String	dclass_counter3_string	A descriptive string that provides information about the **Counter3** value.	
Ratio1	dclass_ratio1	Device class Ratio 1.	
Ratio1String	dclass_ratio1_string	A descriptive string that describes the **Ratio1** value.	
Ratio2	dclass_ratio2	Device class Ratio 2.	
Ratio2String	dclass_ratio2_string	A descriptive string that describes the **Ratio2** value.	
Ratio3	dclass_ratio3	Device class Ratio 3.	
Ratio3String	dclass_ratio3_string	A descriptive string that describes the **Ratio3** value.	
Statement	statement	Numeric ID for each statement run	
Entry	entry	Numeric ID for each statement in audit table.	
TransactionID	trans_id	SQL transaction ID.	
TableName	tbl_name	Table name.	
DatabaseName	db_name	Database name.	
IndexID	index	Index ID of the of the index on the object affected.	

Column Name	Variable Name	Description	Indexed
InstanceName	instance	Instance name.	
Dead	dead	User logged off as DEAD.	
DatabaseProcessID	db_pid	Process ID for the database server where this ID is not the main process ID that is shown within a single event.	
Lread	lread	Number of logical reads.	
LWrite	lwrite	Number of logical writes.	
PRead	pread	Number of physical reads.	
Permissions	permissions	Database permissions.	
BinaryData	binary	Binary data dependent.	
ProcessingTime	processing_time	The time spent processing the request. This variable can be in milliseconds or seconds.	
SourceLocation	location_src	The location of the source, such as a country or another identifier of the actual location.	
DestinationLocation	location_dst	The location of the destination, such as a country or another identifier of the actual location.	
LocationDescription	location_desc	A description of the location relevant for the event being logged.	

Column Name	Variable Name	Description	Indexed
City	location_city	City name.	
State/Province	location_state	State or province name.	
Country	location_country	Country name.	
ClusterMembers	clustermembers	String variable that holds the information about the nodes which define the cluster.	
OperatingSystem	os	Name of the operating system.	
CPU	cpu	CPU time used in the execution of the event being recorded.	
SerialNumber	serial_number	Serial number associated with a physical asset.	
LUN	lun	Logical unit number.	
DiskVolume	disk_volume	A unique name assigned to logical units (volumes) within a physical disk.	
NodeWorldWideName	nwwn	A WWN uniquely identifying an HBA, shared by all Ports on that HBA.	
PortWorldWideName	pwwn	A WWN uniquely identifying a port on an HBA.	
PeerGateway	peer	Encryption peer IP address.	

Column Name	Variable Name	Description	Indexed
PeerIdentity	peer_id	Encryption peer identity.	
IKE	ike	The IKE negotiation phase.	
IKECookieP1	ike_cookie1	The ID of the negotiation — sent for ISAKMP Phase One.	
IKECookieP2	ike_cookie2	The ID of the negotiation — sent for ISAKMP Phase Two.	
Scheme	scheme	The encryption scheme used.	
EncryptionType	encryption_type	Contains one or more of the following encryption elements (but may include other encryption elements not explicitly listed here): • Encryption method used to generate the session key. • Encryption algorithm for the session. • Hashing algorithm for the session.	
CertificateSubject	cert_subject	The subject name of a certificate.	
CertificateHostname	cert_hostname	The hostname value of a certificate.	
CertificateHostnameCategory	cert_hostname_cat	The hostname category value of a certificate.	
CertificateStatus	cert_status	Certificate validation status.	
CertificateError	cert_error	Certificate error.	

Column Name	Variable Name	Description	Indexed
CertificateKeySize	cert_keysize	The size (in bits) of the certificate key referenced in the event.	
SourceSSLVersion	s_sslver	Source (client) SSL version.	
SourceCipher	s_cipher	Source (client) cipher.	
SourceCipherSize	s_ciphersize	Source (client) cipher size.	
SourceSPI	src_spi	Source security parameter index.	
DestinationSSLVersion	d_sslver	Destination (server) SSL version.	
DestinationCipher	d_cipher	Destination (server) cipher.	
DestinationCipherSize	d_ciphersize	Destination (server) cipher size.	
DestinationSPI	dst_spi	Destination security parameter index.	
Resource	resource	Name of the MainFrame resource that is being accessed or used. **Note:** This variable should only be used for Mainframe devices.	
ResourceClass	resource_class	Class to which the MainFrame resource belongs to. **Note:** This variable should only be used for Mainframe	

Column Name	Variable Name	Description	Indexed
		devices.	
Library	library	Library. **Note:** This variable should only be used if the event source is collecting and analyzing events from Mainframe systems.	
JobName	jobname	Job Name. **Note:** This variable should only be used if the event source is collecting and analyzing events from Mainframe systems.	
JobNumber	jobnum	Job Number. **Note:** This variable should only be used if the event source is collecting and analyzing events from Mainframe systems.	
ObjectValue	obj_value	Object value. **Note:** This variable should only be used if the event source is collecting and analyzing events from Mainframe systems.	
Comments	comments	Comment information.	

Column Name	Variable Name	Description	Indexed
VulnerabilityReferences	vuln_ref	Vulnerability references.	
Message	msg	Raw message.	

Unix

Below is a list of Unix variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
Date/Time	stamp	RESERVED	
MessageID	msg_id	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the	

Column Name	Variable Name	Description	Indexed
		RSA enVision Enhanced Categorization Tagging guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventTimeString	event_time_string	This values always equals **event_time**. **Note:** The primary usage for this variable is situations where customers have legacy data already captured in an alternate date format that does not conform to RSA configuration specifications for the event source.	Yes
TimeZone	timezone	A time zone name or offset value, for example -0400, +0600, EDT and GMT+0700.	
EventType	event_type	The event category type as specified by the event source generator.	
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
SessionID	sessionid	Session ID.	
ReferenceID	id	Event or message ID.	Yes
Action	action	The action taken or proposed to be taken. **Note:** For databases, this is the SQL Query statement.	Yes

Column Name	Variable Name	Description	Indexed
Disposition	disposition	The end state of the action.	Yes
ResultCode	resultcode	Result (error) code. **Note:** This field is numeric.	Yes
Result	result	Result (error) string.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column. **Note:** This column should only be used if the **info** column is also required.	
SourceAddress	saddr	Source IP address.	Yes
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	
SourceMask	smask	Source device network mask.	
SourceInterface	sinterface	Source interface.	

Column Name	Variable Name	Description	Indexed
TranslatedSourceAddress	stransaddr	Translated source address.	
TranslatedSourcePort	stransport	Translated source port.	
SourceMacAddress	smacaddr	Source MAC address.	
DestinationAddress	daddr	Destination address.	Yes
DestinationPort	dport	Destination port.	Yes
DestinationHostName	dhost	Destination hostname.	
DestinationMask	dmask	Destination device network mask.	
DestinationInterface	dinterface	Destination interface.	
TranslatedDestinationAddress	dtransaddr	Translated destination address.	
TranslatedDestinationPort	dtransport	Translated destination port.	
DestMacAddress	dmacaddr	Destination MAC address.	
Protocol	protocol	IP protocol name.	
Gateway	gateway	Use to deal with routing information.	
NetworkServiceName	network_service	The name of the network service. **Note:** Some services comprise multiple ports.	

Column Name	Variable Name	Description	Indexed
DeviceMacAddress	macaddr	Device MAC address.	
Interface	interface	Device interface name.	
IPAddress	hostip	Device IP address.	Yes
HostName	hostname	Hostname, preferably fully qualified.	Yes
FQDN	fqdn	Fully qualified domain name.	Yes
Zone	zone	Use to refer to a zone that does not have a concept of direction.	
EventComputer	event_computer	The hostname or IP of the system which originally generated the event. **Note:** This variable may be used in situations where a log relay is in place and the **hostname** variable is referring to the relay. An example scenario could be a Check Point firewall and a Check Point Smart Center.	
NetworkPort	network_port	Network port. **Note:** This variable should be used to capture protocol port information, but only in the case where there is no inherently implied network communication occurring.	
Administrator	administrator	Administrative user name.	Yes

Column Name	Variable Name	Description	Indexed
UserName	username	Account name.	Yes
DomainName	domain	Domain name.	
ClientUserName	c_username	Client user name. Example scenarios include user name on the client (source) referenced in the event, but not the actual event source.	Yes
Uid	uid	The unique user identifier that is associated with the user name.	Yes
LinkedReferenceID	id1	Linked (related) event or message ID.	
Group	group	Group Name. **Note:** For Cisco VPNs, this variable is the **tunnel-group** parameter.	Yes
GroupID	groupid	Group ID number (related to the group name).	Yes
GroupObject	group_object	A collection or grouping of entities. **Note:** This variable is not specific to authentication.	
Duration	duration	Duration of the event in minutes.	
DurationString	duration_string	A text string version of the duration.	

Column Name	Variable Name	Description	Indexed
Info	info	Additional event information that could not be captured in a separate column.	
Context	context	Additional information that gives context to the event.	
EventState	event_state	The current state of the object or item referenced within the event.	
PolicyName	policyname	Policy name.	
Rule	rule	Rule number.	
TriggerValue	trigger_val	The conditions that caused an event to be recorded.	
TriggerDesc	trigger_desc	Description of the trigger condition.	
SubjectContext	s_context	Use this variable in an audit context where the subject is the object being identified.	
TargetContext	t_context	Use this variable in an audit context where the target is the object being identified.	
NodeName	node	Node name. A common use case is the node name within a cluster where the cluster name is reflected by the hostname.	
Version	version	Version of the application or OS that is generating the event.	

Column Name	Variable Name	Description	Indexed
ComponentVersion	component_version	A version that reflects the version level of a sub-component of a product.	
PortName	portname	Physical or logical port connection, but does not include a network port, for example, a printer port name.	
Device	device	Device associated with the node, for example, a physical disk, a printer, or a fan.	
Terminal	terminal	User terminal.	
Realm	realm	Radius realm or similar grouping of accounts.	
DistinguishedName	dn	X.500 (LDAP) distinguished name.	
AuthenticationMethod	authmethod	Authentication mechanism.	
Privilege	privilege	The privilege level or attributes that are recorded.	
UserRole	user_role	The account or group name under which a user action is being performed.	
UserFullName	user_fullname	The full name of a user. **Note:** This is variable sometimes called **Real Name**.	
UserAddress	user_address	User e-mail address, but not in the context of a communication between two parties.	

Column Name	Variable Name	Description	Indexed
UserProfile	profile	User's profile name.	
Category	category	Category name.	
Agent	agent	Agent that processes a portion of the event and is effectively handed off to.	Yes
Product	product	The name of the product, software or hardware.	
Application	application	The name of the application.	
Service	service	A software daemon or service.	Yes
Parameters	param	Parameters passed as part of a command or application.	
ProcessID	process_id	Process ID number.	
Process	process	Process name.	Yes
ParentProcessID	parent_pid	Parent process ID number.	
ChildProcessID	child_pid	Child process ID number.	
ChildProcess	child_process	Child process name.	
ObjectName	obj_name	Object name.	
ObjectType	obj_type	Object type.	

Column Name	Variable Name	Description	Indexed
Inode	inode	An inode stores basic information about a regular file, directory, or other file system object.	
Directory	directory	Directory name (file directory, not LDAP).	Yes
FileName	filename	Document or filename.	Yes
FileNameSize	filename_size	Size of the document or filename.	
MailBox	mail_id	Mailbox name or ID.	
SenderAddress	from	Messaging source address. **Note:** This is not limited to e-mail; can also include Instant Messaging and other messaging concepts.	
RecipientAddress	to	Messaging destination address. **Note:** This variable is not limited to e-mail and can also include Instant Messaging and other messaging concepts.	
Subject	subject	Messaging subject.	
Method	web_method	Web method, for example, POST or GET.	
URL	url	Uniform Resource Locator	
WebPage	webpage	Web page.	

Column Name	Variable Name	Description	Indexed
UserAgent	user_agent	User agent identifier. **Note:** This variable should only be used in reference to the browser identification string. Other use cases could be considered on a case by case basis.	
ChangeAttribute	change_attribute	Changed attribute.	
ChangeOldValue	change_old	The prior value of an attribute or object in a change event.	
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	
Bytes	bytes	Total bytes.	
ReceivedBytes	rbytes	Bytes received.	
SentBytes	sbytes	Bytes sent.	
Packets	packets	Total packets.	
Counter1	dclass_counter1	Device class Counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	
Ratio1	dclass_ratio1	Device class Ratio 1.	
Ratio1String	d_class_ratio1_string	A descriptive string that describes the **Ratio1** value.	

Column Name	Variable Name	Description	Indexed
InstanceName	instance	Instance name.	
LocationDescription	location_desc	A description of the location relevant for the event being logged.	
LUN	lun	Logical unit number.	
CertificateHostname	cert_hostname	The hostname value of a certificate.	
Message	msg	Raw message.	

Virtualization

Below is a list of virtualization variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
Date/Time	stamp	RESERVED	
MessageID	msg_id	RESERVED	Yes
EventTime	event_time	Date or Time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
EventQueueTime	event_queue_time	Time that the event was queued.	
DurationString	duration_string	A text string version of the duration.	
StartTime	starttime	Start time of the event.	

Column Name	Variable Name	Description	Indexed
		Note: If you are using this variable, you must also use **event_time**.	
EndTime	endtime	End time of the event.	
SourceAddress	saddr	Source IP address.	Yes
SourcePort	sport	Source port	
SourceHostName	shost	Source hostname.	
DestinationAddress	daddr	The destination IP address	
DestinationHostName	dhost	The destination host name	
IPAddress	hostip	Device IP address.	Yes
HostName	hostname	Hostname. Preferably fully qualified.	Yes
EventType	event_type	The event category type as specified by event source generator.	
OperationID	operation_id	An alert number or operation number. A common use case would be to reference a vendor event number. **Note:** The values should be unique and non-repeating.	
SessionID	sessionid	Session ID.	

Column Name	Variable Name	Description	Indexed
ReferenceID	id	Event or Message ID.	Yes
Action	action	The action taken, or proposed to be taken. **Note:** For databases, this variable is the SQL Query statement.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
PolicyName	policyname	Policy name.	
Application	application	The name of the application (software).	
Product	product	The name of the product (software or hardware).	
Result	result	Result (Error) string.	Yes
ResultCode	resultcode	Result (Error) code. This is a numeric field.	
Administrator	administrator	Administrative user name.	
UserID	userid	The unique user identifier that is associated with the user name.	
UserName	username	Account name.	Yes
UserRole	user_role	The account or group name under which a user action is being performed.	

Column Name	Variable Name	Description	Indexed
LogonID	logon_id	Unique identifier for an account	
ClientUserName	c_username	Client user name. Example scenarios include user name on the client (source) referenced in the event, but not the actual event source.	Yes
Privilege	privilege	The privilege level or attributes recorded.	
Group	group	Group name. **Note:** For Cisco VPNs this variable is the **tunnel-group** parameter.	Yes
GroupObject	group_object	A collection or grouping of entities. **Note:** This variable is not specific to authentication.	
HardwareID	hardware_id	A unique identifier for a device or system. **Note:** This variable is not a MAC address.	
Agent	agent	Agent that processes a portion of the event and is effectively handed off to.	
Service	service	A software daemon or service (a resident version of an application)	

Column Name	Variable Name	Description	Indexed
DomainName	domain	Domain name.	
GroupID	groupid	Group ID number related to the group name.	
PoolID	pool_id	The identifier of a resource pool. **Note:** This field is typically numeric.	
PoolName	pool_name	The name of a resource pool.	
VirtualName	vsys	Virtual system name.	Yes
VMTarget	vm_target	VMWare Target. **Note: Important:** This variable is for VMware only.	Yes
LUN	lun	Logical Unit Number.	
Version	version	The version of the application or OS which is generating the event.	
ObjectName	obj_name	Name of the object. **Note:** You must use **obj_type** to describe what type of object this variable is.	
ObjectType	obj_type	Object type.	

Column Name	Variable Name	Description	Indexed
Directory	directory	Directory name (file directory, not LDAP).	
URL	url	Uniform Resource Locator.	
ChangeAttribute	change_attribute	The changed attribute	
ChangeOldValue	change_old	The prior value of an attribute or object in a change event.	
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured into a separate column. **Note:** This column should be used only if the info column is also required.	
Info	info	Additional event information	
Department1		RESERVED	
Department2		RESERVED	
Department3		RESERVED	
Category1		RESERVED	
Category2		RESERVED	

Column Name	Variable Name	Description	Indexed
Category3		RESERVED	
EventCategoryName	eventcatname	RESERVED	Yes
VID		RESERVED	
Counter1	dclass_counter1	Device class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	
Message	msg	Raw message.	

Virtual Private Network

Below is a list of Virtual Private Network (VPN) variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
Date/Time	stamp	RESERVED	
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
MessageID	msg_id	RESERVED	Yes
Level	level	RSA enVision event priority level.	
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity.	

Column Name	Variable Name	Description	Indexed
		Note: For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the	

Column Name	Variable Name	Description	Indexed
		RSA enVision Enhanced Categorization Tagging guide. **Note:** Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventTimeString	event_time_string	Date or time of the occurrence of the event as recorded by the system that generated the event. **Note:** This field should be used if the format does not conform to RSA configuration specifications for the event source.	Yes
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
Session	sessionid	Session ID.	
ReferenceID	id	Event or message ID.	Yes
Action	action	The action taken, or proposed to be taken.	Yes
Disposition	disposition	The end state of the action.	Yes
Result	result	Result (Error) string.	Yes

Column Name	Variable Name	Description	Indexed
ResultCode	resultcode	Result (Error) Code. **Note:** This field is numeric.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column.	
SourceAddress	saddr	Source IP address.	Yes
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	
TranslatedSourceAddress	stransaddr	Translated source address.	
TranslatedSourcePort	stransport	Translated source port.	
SourceMacAddress	smacaddr	Source MAC address.	
DestinationAddress	daddr	Destination address.	Yes
DestinationPort	dport	Destination port.	Yes
DestinationHostName	dhost	Destination hostname.	
TranslatedDestinationAddress	dtransaddr	Translated destination address.	

Column Name	Variable Name	Description	Indexed
TranslatedDestinationPort	dtransport	Translated destination port.	
DestMacAddress	dmacaddr	Destination MAC address.	
Protocol	protocol	IP protocol name.	
NetworkServiceName	network_service	The name of the network service. **Note:** Some event sources comprise multiple ports.	
IPAddress	hostip	Device IP address. **Note:** This variable should be used if the event does not indicate a communication between two parties.	Yes
HostName	hostname	Hostname.	Yes
FQDN	fqdn	Fully Qualified Domain Name	
NetworkPort	network_port	Network port. **Note:** This variable should be used to capture protocol port information, but only in the case where there is no inherently implied network communication occurring.	Yes
IPMask	mask	Device network mask.	
Interface	interface	Device interface name.	

Column Name	Variable Name	Description	Indexed
Administrator	administrator	Administrative user name.	
UserName	username	Account name.	Yes
DomainName	domain	Domain name.	
ClientUserName	c_username	Client user name, for example, a user name on the client (source) referenced in the event, but not the actual event source.	Yes
UserID	uid	The unique user identifier that is associated with the user name.	
Group	group	Group Name. **Note:** This variable should only be used for a group of users.	Yes
GroupID	groupid	Group ID number related to the group name.	Yes
Duration	duration	Duration of the event in minutes.	
DurationString	duration_string	A text string version of the duration. For example, 02:40.	
StartTime	starttime	Start time of the event. If this variable is used, then event_time must be also	

Column Name	Variable Name	Description	Indexed
		used	
TimeZone	timezone	A time zone name or offset value, for example, -0400, +0600, EDT and GMT+0700.	
PolicyName	policyname	Policy name.	
Rule	rule	Rule number.	
RuleName	rulename	Rule name. **Note:** This variable is not always populated. Many products only record a rule number and not an associated descriptive rule name.	
LinkedReferenceID	id1	Linked (related) event or message ID.	
TriggerValue	trigger_val	The conditions which caused an event to be recorded. For example, a value that exceeded a threshold.	
Info	info	Additional event information.	
HostID	hostid	Host identifier.	
Realm	realm	Radius realm or similar grouping of accounts.	Yes
DistinguishedName	dn	An X.500 (LDAP) distinguished name.	
SourceDistinguishedName	src_dn	An X.500 (LDAP) distinguished name that, when used within a specific context, indicates a source.	

Column Name	Variable Name	Description	Indexed
DestinationDistinguishedName	dst_dn	An X.500 (LDAP) distinguished name that, when used within a specific context, indicates a destination.	
AuthenticationMethod	authmethod	Authentication mechanism.	
UserRole	user_role	The account or group name which the user's action is being performed under.	
UserFullName	user_fullname	The full name of a user (sometimes called "Real Name")	
Category	category	Category name.	Yes
GroupObject	group_object	A collection or grouping of entities. For example, an interface group.	
PoolName	pool_name	The name of a resource pool.	
Agent	agent	Agent that processes a portion of the event and is effectively handed off to.	
Service	service	A software daemon or service.	
Application	application	The name of the application.	
ProcessID	process_id	Process ID number.	
Process	process	Process name.	

Column Name	Variable Name	Description	Indexed
ObjectName	obj_name	Object name.	
ObjectType	obj_type	Object type.	
Directory	directory	Directory name. This is a file directory, not LDAP.	
FileName	filename	Document or file name.	
Subject	subject	The messaging subject.	
RecipientAddress	to	Messaging destination address. This is not limited to e-mail, and can also includes Instant Messaging and other messaging concepts.	
Method	web_method	Web method. For example, POST or GET.	
URL	url	Uniform Resource Locator.	
WebCookie	web_cookie	The cookies passed within a web request.	
UserAgent	user_agent	User agent identifier. This should only be used in reference to the browser identification string. Any other use cases could be considered on a one by one basis.	
WebPage	webpage	Web page.	

Column Name	Variable Name	Description	Indexed
ChangeAttribute	change_attribute	Changed attribute.	
ChangedOldValue	change_old	The prior value of an attribute or object in a change event.	
ChangedNewValue	change_new	The new value of an attribute or object in a change event.	
Bytes	bytes	Total bytes.	
ReceivedBytes	rbytes	Bytes received.	
SentBytes	sbytes	Bytes sent.	
Counter1	dclass_counter1	Device class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	
Counter2	dclass_counter2	Device class counter 2.	
Counter2String	dclass_counter2_string	A descriptive string that provides information about the **Counter2** value.	
InstanceName	instance	Instance name.	
PeerGateway	peer	Encryption peer's IP Address.	
IKE	ike	The IKE negotiation phase.	Yes

Column Name	Variable Name	Description	Indexed
CertificateSubject	cert_subject	The subject name of a certificate.	
Scheme	scheme	The encryption scheme used.	Yes
SourceSPI	src_spi	Source Security Parameter Index.	
DestinationSPI	dst_spi	Destination Security Parameter Index.	
Message	msg	Raw message.	Yes

Vulnerability

Below is a list of vulnerability variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
Date/Time	stamp	RESERVED	
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
MessageID	msg_id	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject,	

Column Name	Variable Name	Description	Indexed
		ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or Time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventTimeString	event_time_string	Date or Time of the occurrence of the event as recorded by the system that generated the event. **Note:** This field should be used if the format does not conform to RSA's configuration specifications for the event source.	Yes
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
EventType	event_type	The event category type as specified by the event source generator.	
ReferenceID	id	Event or message ID.	
Action	action	The action taken or proposed to be taken.	Yes
Disposition	disposition	The end state of the action.	Yes
Result	result	Result (Error) string.	Yes
Severity	severity	A value that is assigned to an event that indicates the	Yes

Column Name	Variable Name	Description	Indexed
		level of impact relative to other events.	
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured into a separate column.	
SourceAddress	saddr	Source IP address.	
SourceHostName	shost	Source hostname.	
SourcePort	sport	The source port.	
SourceInterface	sinterface	The source interface.	
SourceMacAddress	smacaddr	The source MAC address.	
Protocol	protocol	IP protocol name.	
DeviceMacAddress	macaddr	Device MAC address.	
IPAddress	hostip	Device IP address, only in the case where there is no inherently implied network communication concurring.	Yes
NetworkPort	network_port	Network port. **Note:** This variable should be used to capture protocol port information but only in the case where there is no inherently implied network communication occurring.	Yes

Column Name	Variable Name	Description	Indexed
HostName	hostname	Hostname.	Yes
FQDN	fqdn	Fully qualified domain name.	
UserName	username	Account name.	Yes
StartTime	starttime	Start time of the event. **Note:** If this variable is used, **event_time** must also be used.	Yes
EndTime	endtime	End time of the event.	Yes
TimeZone	timezone	A time zone name or offset value, for example -0400, +0600, EDT and GMT+0700.	
Risk	risk	Risk value that is not a numeric value.	Yes
RiskNumber	risk_num	Risk value for event logs that produce a risk metric.	Yes
ThreatName	threat_name	This is the name of the threat, exploit, vulnerability or malware.	
Rule	rule	Rule number.	Yes
RuleName	rulename	Rule name.	Yes
RuleGroup	rule_group	The name of a grouping of rules. This grouping should relate rule names and rule numbers.	

Column Name	Variable Name	Description	Indexed
Info	info	Additional event information.	
Context	context	Additional information that gives context to the event.	
Version	version	The version of the application or OS which is generating the event.	
ContentVersion	content_version	A version which indicated the release level of a signature or database content. For example, Antivirus signatures, and IDS signatures.	
ComponentVersion	component_version	A version which reflects the version level of a sub-component of a product.	
HostID	hostid	Host Identifier.	
Category	category	Category name.	Yes
GroupObject	group_object	A collection/grouping of entities.	
Agent	agent	Agent that processes a portion of the event and is effectively handed off to.	
Application	application	The name of the application (software).	
Service	service	A software daemon or service. A resident version of an application.	
ProcessID	process_id	Process ID number.	

Column Name	Variable Name	Description	Indexed
Directory	directory	The directory name (file directory, not LDAP).	
FileName	filename	The file name or document name.	
ObjectName	obj_name	Name of the object. **Note:** If this variable is used then **obj_type** should also be used to describe what type of object this variable represents.	
ObjectType	obj_type	Object type.	
URL	url	Uniform Resource Locator.	
SignatureName	signame	Signature Name,String, or Hex value.	Yes
Counter1	dclass_counter1	Device class counter 1.	
Counter1String	dclass_counter1_string	A descriptive string that provides information about the Counter1 value.	
InstanceName	instance	Instance name.	
HardwareID	hardware_id	A unique identifier for a device or system. **Note:** This variable is not a MAC address.	
LocationDescription	location_desc	A description of the location relevant for the event being	

Column Name	Variable Name	Description	Indexed
		logged.	
OperatingSystem	os	Name of the operating system.	
VulnerabilityReference	vuln_ref	Vulnerability references.	
Message	msg	Raw message.	

Web

Below is a list of web variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
Date/Time	stamp	RESERVED	
MessageID	msg_id	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject,	

Column Name	Variable Name	Description	Indexed
		ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventTimeString	event_time_string	Date or time of the occurrence of the event as recorded by the system that generated the event. **Note:** This field should be used if the format does not confine to configuration specifications for the device provided by RSA.	Yes
EventSource	event_source	Source of the event. **Note:** This variable is not a hostname.	Yes
EventType	event_type	The event category type as specified by event source generator.	
SessionID	sessionid	Session ID.	
OperationID	operation_id	An alert number or operation number. Common use case: referencing a vendor event number. The values should be unique and non-repeating typically.	
ReferenceID	id	Event or message ID.	Yes

Column Name	Variable Name	Description	Indexed
Action	action	The action taken or proposed to be taken. **Note:** For databases, this variable is the SQL Query Statement.	Yes
Disposition	disposition	The end state of the action.	Yes
ResultCode	resultcode	Result (Error) Code in numeric format.	Yes
Result	result	Result (Error) String.	Yes
Severity	severity	A value that is assigned to an event that indicates the level of impact relative to other events.	Yes
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured into a separate column. **Note:** This column should be used only if the info column is also required.	
SourceAddress	saddr	Source IP address.	Yes
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	
SourceInterface	sinterface	Source interface.	

Column Name	Variable Name	Description	Indexed
DestinationAddress	daddr	Destination address.	Yes
DestinationPort	dport	Destination port.	Yes
DestinationHostName	dhost	Destination hostname.	
TranslatedDestinationAddress	dtransaddr	Translated destination address.	
DestinationInterface	dinterface	Destination interface.	
Protocol	protocol	IP protocol name.	Yes
NetworkServiceName	network_service	The name of the network service. **Note:** Some services comprise multiple ports.	Yes
Direction	direction	Direction of the network flow for the systems that capture this.	
HostName	hostname	Hostname. Preferably fully qualified.	Yes
NetworkPort	network_port	Network port. **Note:** This variable should be used to capture protocol port information but only in the case where there is no inherently implied network communication occurring.	Yes
Username	username	Account name.	Yes

Column Name	Variable Name	Description	Indexed
DomainName	domain	Domain name.	
Group	Group	Group Name. **Note:** For VPNs, this variable is the tunnel-group parameter.	Yes
GroupObject	group_object	A collection or grouping of entities. For example, an interface group.	
Duration	duration	Duration of the event in minutes.	
DurationString	duration_string	A text string version of the duration.	
StartTime	starttime	Start time of the event. If this variable is used, then event_time must be also used.	
TimeZone	timezone	A time zone name or offset value. For example, -0400, +0600, EDT and GMT+0700.	
EventState	event_state	The current state of the object/item referenced within the event.	
PolicyID	policy_id	Policy ID. **Note:** This field is numeric.	

Column Name	Variable Name	Description	Indexed
PolicyName	policyname	Policy Name.	Yes
RiskNumber	risk_num	Risk value for event logs that produce a risk metric. **Note:** You typically cannot relate risk values produced by separate products.	
ReputationNumber	reputation_num	A reputation score that is generally used by IP or e-mail filters to accept or deny traffic or data through the device.	
RuleName	rulename	Rule name.	Yes
RuleGroup	rule_group	The name of a grouping of rules. **Note:** This grouping should relate rule names or rule numbers.	Yes
Information	info	Additional event information that could not be captured into a separate column.	
TriggerValue	trigger_val	The conditions that caused an event to be recorded, for example, a value that exceeded a threshold.	
TriggerDesc	trigger_desc	Description of the trigger condition.	
DistinguishedName	dn	X.500 (LDAP) Distinguished Name.	
SourceDistinguishedName	src_dn	An X.500 (LDAP) Distinguished name that used in a con-	

Column Name	Variable Name	Description	Indexed
		text that indicates a source.	
DestinationDistinguishedName	dst_dn	An X.500 (LDAP) Distinguished name that used in a context that indicates a destination.	
AuthenticationMethod	authmethod	Authentication mechanism.	
Category	category	Category Name.	Yes
Filter	filter	Filter Category Name.	Yes
FilterCategoryNumber	fcatnum	Filter Category Number.	Yes
FilterResult	fresult	Filter Result.	
Agent	agent	Agent that processes a portion of the event and is effectively handed off to.	
Application	application	The name of the application (software).	
Service	service	A software daemon or service (a resident version of an application).	
ProcessID	process_id	Process ID number.	
InstanceName	instance	Instance name.	
ObjectType	obj_type	Object type.	
ObjectName	obj_name	Name of the object.	

Column Name	Variable Name	Description	Indexed
		Note: You must use **obj_type** to describe what type of object this variable represents.	
Directory	directory	Directory name. This is a file directory, not LDAP.	
FileName	filename	Document or file name.	
Method	web_method	Web method.	
URL	url	Uniform Resource Locator.	Yes
WebHost	web_host	The hostname used in the web request.	Yes
WebDomain	web_domain	Web Domain.	Yes
WebRoot	web_root	The root URL path.	Yes
WebPage	webpage	Web page.	Yes
WebQuery	web_query	Query portion of the URL.	
Referrer	web_referer	Request header referral.	
WebRefererHost	web_ref_host	Web referrer hostname.	
WebRefererDomain	web_ref_domain	Web referrer domain.	

Column Name	Variable Name	Description	Indexed
WebRefererRoot	web_ref_root	Web referrer root URL path.	
WebRefererPage	web_ref_page	Web referrer page.	
WebRefererQuery	web_ref_query	Web referrer query portion of the URL.	
WebCookie	web_cookie	The cookies passed within a web request.	
UserAgent	user_agent	User agent identifier. **Note:** This variable should probably only be used in reference to the browser identification string (other use cases could be considered on a one by one basis).	
Content	content_type	Content encoding type.	Yes
Hierarchy	h_code	Hierarchy.	
VirusName	virusname	The name of the virus.	
SentBytes	sbytes	Bytes sent.	
ReceivedBytes	rbytes	Bytes received.	
Bytes	bytes	Total bytes.	
Content	content_type	Content encoding type.	
HardwareID	hardware_id	A unique identifier for a device or system.	

Column Name	Variable Name	Description	Indexed
		Note: This variable is not a MAC address.	
Comments	comments	Comment information.	
Message	msg	Raw Message.	
OperatingSystem	os	Name of the Operating System on the event source.	
ProcessingTime	processing_time	The time spent processing the request. Can be in milliseconds or seconds.	
CertificateSubject	cert_subject	The subject name of a certificate.	
CertificateHostname	cert_hostname	The hostname value of a certificate.	
CertificateHostnameCategory	cert_hostname_cat	The hostname category value of a certificate.	
CertificateStatus	cert_status	Certificate validation status.	
CertificateError	cert_error	Certificate error.	
SourceSSLVersion	s_sslver	Source (Client) SSL Version.	
SourceCipher	s_cipher	Source (Client) Cipher.	
SourceCipherSize	s_ciphersize	Source (Client) Cipher Size.	

Column Name	Variable Name	Description	Indexed
DestinationSSLVersion	d_sslver	Destination (Server) SSL Version.	
DestinationCipher	d_cipher	Destination (Server) Cipher.	
DestinationCipherSize	d_ciphersize	Destination (Server) Cipher Size.	
Department1	iassoc1	RESERVED	
Department2	iassoc2	RESERVED	
Department3	iassoc3	RESERVED	
Category1	eassoc1	RESERVED	
Category2	eassoc2	RESERVED	
Category3	eassoc3	RESERVED	

Windows

Below is a list of Windows variables and brief descriptions of the meaning of each variable.

Note: A RESERVED field denotes content that is populated by the core RSA enVision system. All other fields are populated by the event source XML definition files.

Column Name	Variable Name	Description	Indexed
Date/Time	stamp	RESERVED	
DeviceAddress	paddr	RESERVED	Yes
DeviceHostName	devicehostname	RESERVED	
DeviceTypeName	devicetypename	RESERVED	Yes
DeviceClassName	deviceclassname	RESERVED	Yes
EventCategory	ecategory	RESERVED	Yes
EventCategoryName	eventcatname	RESERVED	Yes
MessageID	msg_id	RESERVED	Yes
ECTheme	ec_theme	The underlying theme for the event based partially on the subject and activity. **Note:** For details on the ECTheme, ECSubject,	

Column Name	Variable Name	Description	Indexed
		ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECSubject	ec_subject	The subject of the activity described in the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECActivity	ec_activity	A normalized set of actions that describe the event. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide. **Note:** Only for Enhanced Categorization Tagging.	
ECOutcome	ec_outcome	A normalized result set. **Note:** For details on the ECTheme, ECSubject, ECActivity, and ECOutcome columns, see the *RSA enVision Enhanced Categorization Tagging* guide.	

Column Name	Variable Name	Description	Indexed
		Note: Only for Enhanced Categorization Tagging.	
EventTime	event_time	Date or Time of the occurrence of the event as recorded by the system that generated the event.	Yes
EventLog	event_log	Name of the event log.	
EventSource	event_source	Source of the event, for example: Security, Microsoft-Windows-Security-Auditing, MSI Installer,and so on.	Yes
EventType	event_type	Event type. For Windows, this information is in the header, not the body of the message, for example, Success Audit.	
OperationID	operation_id	An alert number or operation number.	
ReferenceID	id	Event or message ID.	Yes
Action	action	The action taken or proposed to be taken.	Yes
Disposition	disposition	The end state of the action.	Yes
ResultCode	resultcode	Result (error) code. **Note:** This field is numeric.	Yes
Result	result	Result (error) string.	Yes

Column Name	Variable Name	Description	Indexed
EventDescription	event_description	A detailed description of the event that typically includes additional specific details that would not be captured in a separate column.	
SourceAddress	saddr	Source IP address.	Yes
SourcePort	sport	Source port.	Yes
SourceHostName	shost	Source hostname.	
TranslatedSourceAddress	stransaddr	Translated source address.	
SourceMacAddress	smacaddr	Source MAC address.	
SourceInterface	sinterface	Source interface.	
DestinationAddress	daddr	Destination IP address.	Yes
DestinatioPort	dport	Destination port.	Yes
DestinationHostName	dhost	Destination hostname.	
TranslatedDestinationAddress	dtransaddr	Translated destination address.	
DestMacAddress	dmacaddr	Destination MAC address.	
DestinationInterface	dinterface	Destination interface.	
Protocol	protocol	IP protocol name.	

Column Name	Variable Name	Description	Indexed
Direction	direction	Direction of the network flow.	
NetworkPort	network_port	Network port. **Note:** This variable should be used to capture protocol port information, but only in the case where there is no inherently implied network communication occurring.	Yes
HostName	hostname	Hostname. Preferably fully qualified.	Yes
Interface	interface	Device interface name.	
Zone	zone	To be used when referring to a zone that does not have a concept of direction.	
EventComputer	event_computer	The hostname or IP of the system that originally generated the event.	
SID	sid	Security ID.	
UserName	username	Account name of the primary,subject, or caller user.	Yes
DomainID	domain_id	Pre Windows 2000 (NetBIOS) name of the domain only.	
DomainName	domain	Domain name of the primary, subject, or caller user.	Yes
SessionID	sessionid	Session ID.	
ClientSID	c_sid	Client or Target security ID.	

Column Name	Variable Name	Description	Indexed
ClientUserName	c_username	Account name of the client or target user.	Yes
ClientDomain	c_domain	Domain name of the client or target user.	Yes
LinkedSessionID	sessionid1	Linked (Related) session ID.	
Group	group	Group name.	Yes
GroupID	groupid	Group ID number.	
ExpirationTime	expiration_time	A timestamp that explicitly refers to an expiration.	
Duration	duration	Duration of the event in minutes.	
EventUser	event_user	The user who created the event. For Windows events, this individual is the user mentioned in the header, not in the message body.	
LinkedReferenceID	id1	Linked (Related) event or message ID. **Note:** This variable should be used if an event references another event ID.	
LinkedReferenceID2	id2	Second linked event message ID. **Note:** This variable can be linked to **id** or **id1**, but should not be used unless the other two variables are used.	
PolicyID	policy_id	Policy ID.	

Column Name	Variable Name	Description	Indexed
		Note: This field is numeric.	
PolicyName	policyname	Policy name.	
PolicyValue	policy_value	The contents of the policy itself. **Note:** This should contain the details of what the policy does.	
Rule	rule	Rule number.	
RuleName	rulename	Rule name.	
AuditClass	audit_class	The class name of the functional audit area.	
ExpectedValue	expected_val	The value that the system was expecting to see.	
ObservedValue	observed_val	The value that the system actually observed.	
TriggerValue	trigger_val	The conditions that caused an event to be recorded, for example, a value that exceeded a threshold.	
Information	info	Additional event information that could not be captured into a separate column.	
SSID	ssid	Wireless SSID name.	
Version	version	Version of the application or OS that is generating the	

Column Name	Variable Name	Description	Indexed
		event.	
HostID	hostid	Host identifier.	
RemoteHostID	r_hostid	Host identifier for a remote system. **Note:** This variable is to be used in the context of an event that also has a **hostid**.	
PortName	portname	Physical or logical port connection, but does not include a network port, for example, a printer port name.	
Device	device	Device associated with the node, for example, a physical disk, a printer, or a fan.	
LogonType	logon_type	The type of logon.	Yes
Realm	realm	Radius realm or similar grouping of accounts.	Yes
RemoteDomainName	remote_domain	Remote domain name.	
RemoteDomainID	remote_domain_id	Remote domain ID.	
DistinguishedName	dn	X.500 (LDAP) distinguished name.	
Accesses	accesses	Actual priviliges used in accessing an object.	Yes
AuthenticationMethod	authmethod	Authentication mechanism.	

Column Name	Variable Name	Description	Indexed
Privilege	privilege	The privileges level or attributes recorded.	Yes
ServiceAccount	service_account	The name (including domain if applicable) of the account a service (referenced in the event) is running under.	
UserFullName	user_fullname	The full name of a user. **Note:** This variable is sometimes called Real Name.	Yes
UserProfile	profile	User's profile name.	
Category	category	Category name.	Yes
Filter	filter	Filter category name.	
Agent	agent	Agent that processes a portion of the event, and is effectively handed off to.	
Application	application	The name of the application (software).	
Service	service	A software daemon or service (a resident version of an application).	
Parameters	param	Parameters passed as part of a command or application.	
Process	process	Process name.	Yes
ProcessID	process_id	Process ID number.	

Column Name	Variable Name	Description	Indexed
ParentProcess	parent_process	Parent process name.	
ParentProcessID	parent_pid	Parent process ID number.	
ObjectServer	obj_server	Object server.	
ObjectType	obj_type	Object type.	Yes
ObjectName	obj_name	Object name.	Yes
Directory	directory	File directory name, not LDAP.	
DocumentNumber	doc_number	Document or file number.	
FileName	filename	Document filename.	Yes
URL	url	Uniform Resource Locator.	
ChangeAttribute	change_attribute	Changed attribute.	
ChangeOldValue	change_old	The prior value of an attribute or object in a change event.	
ChangeNewValue	change_new	The new value of an attribute or object in a change event.	
LDAPAttribute	ldap_attribute	LDAP attribute string name.	
Bytes	bytes	Total bytes.	
Counter1	dclass_counter1	Device class counter 1.	

Column Name	Variable Name	Description	Indexed
Counter1String	dclass_counter1_string	A descriptive string that provides information about the **Counter1** value.	
LocationDescription	location_desc	A description of the location relevant for the event being logged.	
PeerGateway	peer	Encryption peer IP address.	
PeerIdentity	peer_id	Encryption peer identity.	
IKE	ike	The IKE negotiation phase.	
Scheme	scheme	The encryption scheme used.	
EncryptionType	encryption_type	Encryption method used to generate the session key.	
CertificateIssuer	cert_issuer	Certificate issuer.	
SourceCertAuth	s_certauth	Source certificate authority.	
DestinationCertAuth	d_certauth	Destination certificate authority.	
Message	msg	Raw message.	

Content 2.0 Variables

For Content 2.0, RSA enVision uses a well-defined set of variables, separated into categories. The individual variables for each category are described in the following topics.

- Auth / Auth Variables
- Category and Group Variables
- Chat Variables
- Counters Variables
- Database Variables
- Encryption Variables
- Event Variables
- Health Care Variables
- Mainframe Legacy Variables
- Network Variables
- Node Variables
- Physical Variables
- Regulations and Compliance Variables
- Resources Variables
- Storage Variables
- Time Variables

Authentication and Authorization Variables

Below is a list of authentication and authorization variables and brief descriptions of the meaning of each variable.

Variable Name	Column Name	Description	Data Sample
accesses	Accesses	Actual privileges used in accessing an object, such as Read, or Write.	
administrator	Administrator	Administrative user name	
authmethod	AuthenticationMethod	Authentication mechanism.	
c_domain	ClientDomain	Client domain.	
c_logon_id	ClientLogonID	Client logon ID	
c_sid	ClientSID		
c_username	ClientUserName	Client Username. Example scenarios include username on the client (source) referenced in the event but not the actual event source.	
creator	ObjectCreator	The identity of the creator (Logon ID, DN, etc.) of an object (examples: file, directory, policy).	
dn	DistinguishedName	X.500 (LDAP) Distinguished Name	CN=Rabbit,

Variable Name	Column Name	Description	Data Sample
			Roger, OU=CORP1, DC=EMC, DC=COM
domain	DomainName	Domain name	CORP1
domain_id	DomainID	Pre Windows 2000 (NetBIOS) name of the domain ONLY	CORP1\
dst_dn	DestinationDistinguishedName	An X.500 (LDAP) Distinguished name that used in a context that indicates a source / destination	
federated_idp	FederatedIdentityProvider	The federated Identity Provider. This is the server providing the authentication.	
federated_sp	FederatedServiceProvider	Federated Service Provider. This is the application requesting authentication.	
logon_id	LogonID	Unique identifier for an account.	
logon_type	LogonType	The type of logon. Some systems record a value for the level to which a logon was performed (ie interactive vs non-interactive).	
owner	OwnerName	The identity name of the owner of an object (examples: file, directory, policy).	

Variable Name	Column Name	Description	Data Sample
owner_id	OwnerID	The unique ID associated with the Owner Name. Typically a numeric value.	
privilege	Privilege	The privilege level/attributes recorded	
profile	UserProfile	User's profile name	
realm	Realm	Radius realm or similar grouping of accounts	
remote_ domain	RemoteDomainName		
remote_ domain_id	RemoteDomainID		
service_ account	Service Account	The name (including domain if applicable) of the account a service (referenced in the event) is running under.	localhost\SYSTEM
sid	SID	Security ID (Unique concept to Windows accounts). Not to be used otherwise.	
src_dn	SourceDistinguishedName	An X.500 (LDAP) Distinguished name that used in a context that indicates a source / destination	

Variable Name	Column Name	Description	Data Sample
uid	UserID	The unique user identifier that is associated with the username.	500
user_address	UserAddress	User e-mail address, but not in the context of a communication between two parties.	
user_dept	UserDepartment	User's Department	
user_fname	UserFirstName	The first name of the user	
user_fullname	UserFullName	The full name of a user (sometimes called Real Name)	John Doe
user_lname	UserLastName	The last name of the user	
user_mname	UserMiddleName	The middle name of the user	
user_org	UserOrganization	User organization	
user_role	UserRole	The account or group name which the user's action is being performed under.	
username	UserName	Account name	

Category and Group Variables

Below is a list of category and group variables and brief descriptions of the meaning of each variable. These variables store information from the event that indicates a group or category.

Variable Name	Column Name	Description	Data Sample
category	Category	Category Name	
fcatnum	FilterCategoryNumber	Filter Category Number	
filter	Filter	Filter Category Name	
fresult	FilterResult	Filter Result	
group	Group	Group Name For Cisco VPNs this is the tunnel-group parameter	wheel
group_object	GroupObject	A collection/grouping of entities. This is not specific to authentication.	
groupid	GroupID	Group ID Number (related to the group name)	0 500
pool_id	PoolID	The identifier (typically numeric field) of a resource pool.	
pool_name	PoolName	The name of a resource pool	

Chat Variables

Below is a list of chat variables and brief descriptions of the meaning of each variable. These variables store data for instant messaging or other chat related services.

Variable Name	Column Name	Description	Data Sample
im_buddyid	IMBuddyID	IM buddy ID	
im_buddyname	IMBuddyname	IM buddy name	
im_client	IMClient	IM client information	
im_croomid	IMChatroomID	Chat room identifier	
im_croomtype	IMChatroomType	Chat room type	public invite_only voice
im_members	IMMembers	List of the chat participants	
im_userid	IMUserID	IM user ID	
im_username	IMUsername	IM user name	

Counters Variables

Below is a list of variables for counters and brief descriptions of the meaning of each variable. These variables store information for counters.

Variable Name	Column Name	Description	Data Sample
bytes	Bytes	Total bytes	1976308
dclass_counter1 dclass_counter2 dclass_counter3	Counter1 Counter2 Counter3	Device class counters. Each device class possesses its own counters specific to its environment. For example, e-mail systems might log the number of recipients of a message. That counter would not have any relevance to the number of pages printed as logged by a print system.	
dclass_counter1_string dclass_counter2_string dclass_counter3_string	Counter1String, Counter2String, Counter3String	A descriptive string that provides information about the the corresponding Counter value.	
dclass_ratio1 dclass_ratio2 dclass_ratio3	Ratio1	Device class Ratio 1, 2 and 3	
dclass_ratio1_string	Ratio1String	A descriptive string that describes the Ratio1, 2,	

Variable Name	Column Name	Description	Data Sample
dclass_ratio2_string dlcass_ratio3_string		and 3 values	
event_counter	EventCounter	Number of times the event has repeated, or the total number of events aggregated.	
packets	Packets	Total packets	1320
rbytes	ReceivedBytes	Bytes received	184502
sbytes	SentBytes	Bytes sent	171806

Database Variables

Below is a list of database variables and brief descriptions of the meaning of each variable.

Variable Name	Column Name	Description
binary	BinaryData	binary data dependent
db_name	DatabaseName	Database Name
db_pid	DatabaseProcessID	Process ID for the database server where this is not the main process ID that is shown within a single event.
dead	Dead	User logged off as DEAD
entry	Entry	Numeric ID for each statement in audit table
index	IndexID	Index ID of the of the index on the object affected
instance	InstanceName	Database instance name
lread	Lread	Number of logical reads
lwrite	LWrite	number of logical writes
permissions	Permissions	database permissions
pread	PRead	number of physical reads

Variable Name	Column Name	Description
statement	Statement	Numeric ID for each statement run
tbl_name	TableName	Table Name
trans_id	TransactionID	SQL Transaction ID

Encryption Variables

Below is a list of encryption variables and brief descriptions of the meaning of each variable.

Variable Name	Column Name	Description	Data Sample
cert_error	CertificateError		
cert_hostname	CertificateHostname	The hostname value of a certificate	www.rsa.com *.yahoo.com
cert_host-name_cat	CertificateCategory	The hostname category value of a certificate	
cert_issuer	CertificateIssuer		
cert_keysize	CertificateKeySize	The size (in bits) of the certificate key referenced in the event.	1024 2048
cert_status	CertificateStatus	Certificate validation status	
cert_subject	CertificateSubject	The subject name of a certificate	
d_certauth	DestinationCertAuth	Destination Certificate Authority	
d_cipher	DestinationCipher	Destination (Server) Cipher	DES-CBC3-SHA
d_ciphersize	DestinationCipherSize	Destination (Server) Cipher Size	256

Variable Name	Column Name	Description	Data Sample
			512
d_sslver	DestinationSSLVersion	Destination (Server) SSL Version	TLSv1
dst_spi	DestinationSPI	Destination Security Parameter Index	
encryption_ type	EncryptionType	Contains one or more of the following encryption elements (But may include other encryption elements not explicitly listed here): • Encryption method used to generate the session key • Encryption algorithm for the session • Hashing Algorithm for the session	
ike	IKE	The IKE negotiation phase.	Main Mode completion
ike_cookie1	IKECookieP1	"The ID of the negotiation — sent for ISAKMP Phase One"	
ike_cookie2	IKECookieP2	"The ID of the negotiation — sent for ISAKMP Phase Two"	
peer	PeerGateway	Encryption peer's IP Address	
peer_id	PeerIdentity	Encryption peer’s identity	subnet: 0.0.0.0 (mask= 0.0.0.0) host: a.b.c.d.

Variable Name	Column Name	Description	Data Sample
s_certauth	SourceCertAuth	Source Certificate Authority	
s_cipher	SourceCipher	Source (Client) Cipher	DES-CBC3-SHA
s_ciphersize	SourceCipherSize	Source (Client) Cipher Size	256 512
s_sslver	SourceSSLVersion	Source (Client) SSL Version	TLSv1
scheme	Scheme	The encryption scheme used. A value of PLAIN indicates no encryption scheme is used.	IKE SSL PLAIN
src_spi	SourceSPI	Source Security Parameter Index	

Event Variables

These variables convey information about the event itself, including details such as the source or additional details that could not be captured into a specific variable column.

Variable Name	Column Name	Description	Data Sample
action	Action	The action taken or proposed to be taken. For databases, this is the SQL query statement.	
audit_class	AuditClass	The class name of the functional audit area	
audit_object	AuditObject	The name or identifier of the object that is subject of the audit event.	
audit_record	AuditRecord	The audit record number.	
comments	Comments	Comment information	
connectionid	ConnectionID	Connection ID	
context	Context	Additional information that gives context to the event.	
disposition	Disposition	The end state of the action	
event_description	EventDescription	A detailed description of the event that typically includes additional specific details that would not be captured into a separate column. This column should be used only if the info column is also required.	

Variable Name	Column Name	Description	Data Sample
event_log	EventLog	Name of the event log	
event_source	EventSource	Source of the event, not to be confused with a host name.	
event_state	EventState	The current state of the object/item referenced within the event. This variable is only used to describe an on-going event. Events that have ended contain a value for the **disposition** variable.	Pending In Progress Stalled
event_type	EventType	The event category type as specified by event source generator.	
event_user	EventUser	The user which created the event or the user which is the subject of the event. However, it should not be the user that is the actor in the event.	
expected_val	ExpectedValue	The value the system was expecting to see (from the perspective of the device generating the log).	
id	ReferenceID	Event/Message ID	
id1	LinkedReferenceID	Linked (Related) Event/Message ID	
id2	LinkedReferenceID2	2nd Linked Event/Message ID. Can be either linked to id or id1 value but should not be used unless the	

Variable Name	Column Name	Description	Data Sample
		other two variables are in play.	
info	Info	Additional event information that could not be captured into a separate column	
listnum	AccessListNo		
msg	Message	Raw Message	
nat_rule	Rule2	Network address translation rule number. Note that the column name here is Rule2. The Rule2 column has a many to one relationship (many variables to one column.	
obj_server	ObjectServer		
observed_val	ObservedValue	The value the system actually observed (or received, found, etc.). This variable is used in conjunction with the **expected_val** variable.	
operation_id	OperationID	An alert number or operation number. Common use case: referencing a vendor event number. The values are typically unique.	
policy_id	PolicyID	Policy ID. Usually a numeric field, either hexadecimal or decimal.	
policy_template	PolicyTemplate	The policy template that accompanies the policy	

Variable Name	Column Name	Description	Data Sample
policy_value	PolicyValue	The contents of the policy itself. This should contain the details of what the policy does.	
policy_version	PolicyVersion	The version identifier for the policy or configuration of the device or application.	
policy_waiver	PolicyWaiver	An exception to the policy in effect. This could be the detailed explanation of the waiver or simply a category that the waiver belonged to.	Exception Exemption Suppression
policyname	PolicyName	Policy Name	
result	Result	Result (Error) String.	
resultcode	ResultCode	Result (Error) Code. Numeric field.	
risk	Risk	Risk value that is not a numeric value.	
risk_num	RiskNumber	Risk value (for event logs that produce a risk metric. Note that you typically cannot relate risk values produced by separate products).	
rule	Rule	Rule number	
rule_group	RuleGroup	The name of a grouping of rules. This grouping should relate rule names and/or rule numbers.	
rule_template	RuleTemplate	A default set of parameters which are overlaid onto a	

Variable Name	Column Name	Description	Data Sample
		rule (or rule name) which effectively constitutes a template.	
rule_uid	RuleUID	Unique Identifier for a rule. Some products (check-point, juniper) also leverage a unique identifier for rules in addition to a rule number.	
rulename	RuleName	Rule Name (Not always populated. Many products only record a rule number and not an associated descriptive rule name.)	
s_context	SubjectContext	This variable is to be used in an audit context where the subject is the object being identified	
sessionid	Session	Session ID	
sessionid1	LinkedSessionID	Linked (Related) Session ID	
severity	Severity	A value that is assigned to an event that indicates the level of impact relative to other events.	
t_context	TargetContext	This variable is to be used in an audit context where the Target is the object being identified	
trigger_desc	TriggerDesc	Description of the trigger condition	
trigger_val	TriggerValue	The conditions which caused an event to be recorded, such as a threshold being exceeded.	

Variable Name	Column Name	Description	Data Sample
vendor_event_cat	VendorEventCategory	Category of the event. This is a vendor supplied data field and not generated from enVision.	
workspace_desc	WorkspaceDescription	A collection of policies (possibly including rules as well) which are organized together into a "workspace."	

Health Care Variables

Below is a list of health care variables and brief descriptions of the meaning of each variable. These variables represent data specifically related to the health care field.

Variable Name	Column Name	Description
patient_fname	PatientFirstName	Patient's First Name
patient_fullname	PatientFullName	Patient's Full Name
patient_id	PatientID	Patient Identifier
patient_lname	PatientLastName	Patient's Last Name
patient_mname	PatientMiddleName	Patient's Middle Name

Mainframe Legacy Variables

Below is a list of variables that are used for mainframe event sources and legacy integrations.

Variable Name	Column Name	Description	Data Sample
bypass	Bypass		
volser	VolSer		
jobname	JobName		
resource	Resource	Name of the MainFrame resource that is being accessed or used	Sample Resource names: ISP.SIS-PPENU, SYS1.PARMLIB, LVL0.PARMLIB
resourcename	Resource		
resource_critical	ResourceCritical	The Mainframe applies tags to identify if a resource is critical or not	Yes/No/MAYBE
cmd	Command		
divname	DivisionName		
facilityname	FacilityName		

Variable Name	Column Name	Description	Data Sample
acid	AcidName		
library	Library		
resource_class	ResourceClass	Class to which the MainFrame resource belongs to	DATA SET, FACILITY, TSOP-ROC, ACCT-NUM
name1	ComputerName/FolderDocumentName		
name2	HeaderJobName		
reqacc1	RequestAccess1		
reqacc2	RequestAccess2		
reqacc3	RequestAccess3		
usermode	UserMode		
user_privileged	UserPrivileged	The Mainframe applies a tags to indentify if a user is priviledged or not	Yes/No/
object_privileged	ObjectPrivileged	The Mainframe applies a tags to indentify if an Object is priviledged or not	Yes/No/MAYBE
jobnum	JobNumber		
obj_name	SignalNumber/JobNumber		

Variable Name	Column Name	Description	Data Sample
allowacc1	AllowAccess1		
allowacc2	AllowAccess2		
allowacc3	AllowAccess3		
obj_value	ObjectValue		
zonename	ZoneName		
time	ServerTime		
password	PasswordNone/PasswordStored		
filesystem	SystemName		
password_ expire	PasswordExpired		
audit	Audit		
type1	Key_Operation/JobSubType/TypeRecord		
password_ chg	PasswordChanged		
sessiontype	SessionType		

Network Variables

Below is a list of network variables and brief descriptions of the meaning of each variable.. These variables represent a flow of communication from a source to a destination.

Variable Name	Column Name	Description	Data Sample
daddr	DestinationAddress	Destination address	128.222.180.23
daddr_v6	DestinationAddressv6	Destination IPv6 Address	
ddomain	DestinationDomain	Destination domain	company.com
dhost	DestinationHostName	Destination host name	server.company.com
dinterface	DestinationInterface	Destination interface	hme1
direction	Direction	Direction of the network flow (for the systems that capture this)	outbound
dmacaddr	DestMacAddress	Destination MAC address	00:00:0C:00:70:DF
dmask	DestinationMask	Destionation Device network mask	255.255.255.0, /24, /23
dport	DestinationPort	Destination port	80
dst_zone	DestinationZone	Destination zone	Trust
dtransaddr	TranslatedDestAddress	Translated destination address	10.1.9.200

Variable Name	Column Name	Description	Data Sample
dtransport	TranslatedDestPort	Translated destination port	8080
gateway	Gateway	Gateway to be used when dealing with routing information	192.168.1.1
network_service	NetworkServiceName	The name of the network service. Some services comprise multiple ports.	ftp SQL RPC
protocol	Protocol	IP protocol name	tcp udp icmp
protocol_detail	ProtocolDetail	IP protocol details. For protocols that don't contain details such as ports, this is the place to capture that information	
saddr	SourceAddress	Source IP address	72.5.124.61
saddr_v6	SourceAddressv6	Source IPv6 Address	
sdomain	SourceDomain	Source domain	example.com
shost	SourceHostName	Source host name	hostname.example.com
sinterface	SourceInterface	Source interface	hme0

Variable Name	Column Name	Description	Data Sample
smacaddr	SourceMacAddress	Source MAC address	08:00:20:00:70:DF
smask	SourceMask	Sourec Device network mask	255.255.255.0, /24, /23
sport	SourcePort	Source port	4196
src_zone	SourceZone	Source zone	Untrust
stransaddr	TranslatedSourceAddress	Translated source address	10.1.9.2
stransport	TranslatedSourcePort	Translated source port	31337
zone	Zone	Zone Variable to be used when directionality is not implied	Untrust

Device Class Specific Variables

The following variables are used with event sources that fall into the Firewall class. Some devices log these specific options. Although not critical for daily operations they could be useful in investigations into operational issues or other network issues.

Variable Name	Column Name	Description	Data Sample
icmpcode	ICMPCode	The "code" value for an ICMP packet.	0 1 2 3 4
icmptype	ICMPType	The "type" value for an ICMP packet.	0 8 11

Node Variables

Below is a list of node variables and brief descriptions of the meaning of each variable. Unlike Network variables, node variables do not represent a communication between two parties.

Variable Name	Column Name	Description	Data Sample
access_point	AccessPoint	Access Point Name	linksys, emc_wifi
bssid	BSSID	Identity used to identify a BSS for an area. In a wireless infrastructure this will be the MAC address of the AP. In an ad hoc network this is probably randomly generated.	
cluster_ members	ClusterMembers	String variable that holds the information about the nodes (plural) which define the cluster	'EAC-PLY-CL1 [EAC-PLY-CL1-IC01, 10.114.164.36] [EAC-PLY-CL1-IC02, 10.114.164.38] [EAC-PLY-CL1-IC03, 10.114.164.39]'
component_ version	ComponentVersion	A version which reflects the version level of a sub-component of a product. For example, in Anti-virus, this could indicate the version of the scanner engine itself as opposed to using **version** for the product version.	

Variable Name	Column Name	Description	Data Sample
content_version	ContentVersion	A version which indicates the release level of a signature or database content. Common uses: Antivirus signatures, IDS Signatures	
cpu	CPU	CPU time used in the execution of the event being recorded.	
device	Device	Device associated with the node (Examples: a physical disk, a printer, a fan).	HP LaserJet 4 /dev/c0t0d0
event_computer	EventComputer	The hostname/IP of the system which originally generated the event. This variable may be used in situations where a log relay is in place and the hostname variable is referring to the relay. An example scenario could be a Check Point firewall and a Check Point Smart Center.	fwnode
fqdn	FQDN	Fully Qualified domain name (ONLY!)	
hardware_id	HardwareID	A unique identifier for a device or system (NOT a Mac address)	
hostid	HostID	Host Identifier	
hostip	IPAddress	Device IP address	10.1.9.1
hostip_v6	IPv6Address	Device IPv6 Address	

Variable Name	Column Name	Description	Data Sample
hostname	HostName	Host name. Preferably fully qualified.	hostname.example.com
interface	Interface	Device interface name	hme0
macaddr	DeviceMacAddress	Device MAC address	00:00:0C:00:7C:1F
mask	IPMask	Device network mask	255.255.255.0
network_port	NetworkPort	Network port. This variable should be used to capture protocol port information but only in the case where there is **no** inherently implied network communication occurring. An example is when a network service is started. The service will open a listener on a port but the event itself does not imply that a network communication has occurred.	
node	NodeName	"Node name. Common use case is the node name within a cluster where the cluster name is reflected by the host name. In configuration mgmt systems, this would store the name of the device being managed.	nodea.example.com EAC-PLY-CL1-IC02
os	OperatingSystem	Name of the OS on the device	
parent_node	ParentNode	Parent Node Name. Must be related to node variable.	

Variable Name	Column Name	Description	Data Sample
portname	PortName	Physical or logical port connection but does NOT include a network port. (Example: Printer port name).	IP_128.222.180.50
r_hostid	RemoteHostID	Host Identifier for a remote system. To be used in the context of an event that also has a hostid.	
serial_number	SerialNumber	Serial number associated with a physical asset.	
ssid	SSID	Wireless SSID name	
terminal	Terminal		
version	Version	Version of the application or OS which is generating the event.	
vlan	VLAN	VLAN number	50
vsys	VirtualName	Virtual system name	
wifi_channel	WiFiChannel	The channel ID used by a Wireless Access Point	1,2.3,….9,10,11
wlan	WLAN	WLAN number	2

Physical Variables

Below is a list of physical variables and brief descriptions of the meaning of each variable. These variables represent geographic or relative location information for a physical location.

Variable Name	Column Name	Description	Data Sample
distance	Distance	Distance from a location reference mark or from the device expressed in meters.	1.3
latitude	Latitude	The east-west location.	-71.208605
location_bldg	Building	Building name and/or number	200
location_campus	Campus	Campus name	Westwood
location_city	City	City name	Westwood
location_country	Country	Country name	USA
location_desc	LocationDescription	A description of the location relevant for the event being logged.	200 Brook Dr., Suite 200
location_floor	Floor	Floor number	2
location_mark	ReferenceMark	A reference location. Can be used in conjunction with distance to provide a more accurate location.	Fire extinguisher

Variable Name	Column Name	Description	Data Sample
location_state	State/Province	State or province name	MA
longitude	Longitude	The north-south location.	42.239565

Regulations and Compliance Variables

Below is a list of compliance variables and brief descriptions of the meaning of each variable.

Variable Name	Column Name	Description	Data Sample
benchmark	Benchmark	The regulatory requirement or best practices standard to which the event is being referred.	ISO 27001 SOX PCI

Resources Variables

Below is a list of resources variables and brief descriptions of the meaning of each variable. These variables are used across blended devices (that is, devices that cross multiple device classes) where the reporting device overlaps into several device classes.

Variable Name	Column Name	Description	Data Sample
agent	Agent	Agent that processes a portion of the event and is effectively handed off to. Typically, this is a separate process from the main process that generated the event log.	mail dequeuer
application	Application	The name of the application (software)	
bcc	BlindCarbonCopy	The BCC field usually associated with an e-mail	
calling_from	CallingFrom	The telephone number being called from	888-555-1234
calling_to	CallingTo	The telephone number being called	888-555-1234
cc	CarbonCopy	The CC field usually associated with an e-mail	
change_attribute	ChangeAttribute	Change attribute will identify the name of the item whose value changed from old to new	
change_new	ChangeNewValue	The new value of an attribute/object in a change event	

Variable Name	Column Name	Description	Data Sample
change_old	ChangeOldValue	The prior value of an attribute/object in a change event	
checksum	CheckSum	A fixed size value computed from a block of data primarily for integrity check purposes	158205555
child_pid	ChildProcessID	Child Process ID Number	
child_process	ChildProcess	Child Process Name	
circuit	Circuit		
content_type	Content	content encoding type	
data	Data	Data Field. Must use **data_type** to describe the type of data being represented in this field.	
data_type	DataType	The classification type of the data that is the subject of the event referenced	SSN Credit Card Trade Secret Proprietary Info"
directory	Directory	Directory name (file directory, not LDAP)	
dns_a_record	DNSARecord	DNS A record value	209.73.187.189 66.196.87.126,69.147.121.161
dns_cname_record	DNSCNameRecord	DNS CName record	alias.data.toolbar.yahoo.com toolbar.a00.yahoodns.net

Variable Name	Column Name	Description	Data Sample
dns_opcode	DNSOpcode	DNS Opcode value	query
dns_ptr_record	DNSPTRRecord	DNS PTR record	
doc_number	DocumentNumber	Document/File number	
filename	FileName	Document/File name	
filename_size	FileNameSize	Size of the Document/File name	
forensic_info	ForensicInfo	Unstructured forensic event information that is captured during the referenced event.	
from	SenderAddress	Messaging source address (Not limited to e-mail, also includes Instant Messaging and other messaging concepts).	
h_code	Hierarchy		DIRECT
ldap_attribute	LDAPAttribute	LDAP Attribute String Name	
mail_id	MailBox	Mailbox Name / ID	
mailing_list	MailingList	The name of a group Mailing List	
message_ body	MessageBody	The contents of the message body.	

Variable Name	Column Name	Description	Data Sample
obj_name	ObjectName	Name of the object (Note: you MUST use obj_type to describe what type of object this is)	
obj_type	ObjectType	Object Type	
octets	Octets	The series of Octets captured in a network event	
param	Parameters	Parameters passed as part of a command or application, etc.	
parent_pid	ParentProcessID	Parent Process ID number	
parent_process	ParentProcess	Parent Process Name	
phone_number	PhoneNumber	A telephone number	
process	Process	Process name	
process_id	ProcessID	Process ID number	
process_id_val	ProcessIDValue	Process ID Value (non-integer types)	
product	Product	The name of the product (software or hardware)	
reputation_num	ReputationNumber	A reputation score that is generally used by IP, e-mail filters, and so on, to accept or deny traffic and data through the device.	

Variable Name	Column Name	Description	Data Sample
sensor	Sensor		
service	Service	A software daemon or service (A resident version of an application)	
sigid	SignatureID	IDS/IPS Int Signature ID	
sigid_string	SignatureIDString	A string object of the sigid variable. The value for this variable is always the same as **sigid**.	
sigid2	SubSignatureID		
signame	SignatureName	IDS/IPS Signature Name/String/Hex value	
subject	Subject	Messaging subject	
threat_name	ThreatName	This is the name of the threat, exploit, vulnerability or malware. **Note: Note: virusname** is copied into threat_ name.	
threat_val	ThreatValue	A Threat rating that is a measure of the threat level.	
to	RecipientAddress	Messaging destination address (Not limited to e-mail, also includes Instant Messaging and other messaging concepts).	

Variable Name	Column Name	Description	Data Sample
tos	TypeOfService	The priority given to a network protocol	
trans_from	TranslatedSenderAddress	Translated messaging source address (Not limited to e-mail, also includes Instant Messaging and other messaging concepts). Some devices perform address translation on the sender and recipients in a message.	
trans_to	TranslatedRecipientAddress	Translated messaging destination address (Not limited to e-mail, also includes Instant Messaging and other messaging concepts). Some devices perform address translation on the sender and recipients in a message.	
url	URL	URL - Uniform Resource Locator	
user_agent	UserAgent	User agent identifier, this should probably only be used in reference to the browser identification string (other use cases could be considered on a one by one basis)	
virusname	VirusName	The name of the virus. **Note: Note:** For newer event sources, **threat_ name** is used.	
vm_target	VMTarget	VMware Target	

Variable Name	Column Name	Description	Data Sample
web_cookie	WebCookie	The cookies passed within a web request	
web_domain	WebDomain	The domain used in the web request	
web_extension	WebExtension	The extension of the page that was requested	DOC XML HTM ASP JSP
web_host	WebHost	The hostname used in the web request.	www.sun.com
web_method	Method	Web method	POST GET
web_query	WebQuery	Query portion of the URL	
web_ref_ domain	WebRefererDomain	Web referrer's domain.	example.com
web_ref_host	WebRefererHost	Web referrer's hostname	www.example.com
web_ref_page	WebRefererPage	Web referrer's page	index.asp index.html
web_ref_query	WebRefererQuery	Web referrer's query portion of the URL	

Variable Name	Column Name	Description	Data Sample
web_ref_root	WebRefererRoot	Web referrer's root URL path	/pathname/blah/
web_referer	Referrer	Request header referral	
web_root	WebRoot	The root URL path	/pathname/blah/
webpage	WebPage	Web page	index.asp index.html

Storage Variables

Below is a list of storage variables and brief descriptions of the meaning of each variable.

Variable Name	Column Name	Description
disk_volume	DiskVolume	A unique name assigned to logical units (volumes) within a physical disk
inode	inode	An inode stores basic information about a regular file, directory, or other file system object.
lun	LUN	Logical Unit Number
nwwn	NodeWorldWideName	A World Wide Name uniquely identifying a Host Bus Adapter (HBA), shared by all Ports on that HBA.
pwwn	PortWorldWideName	A World Wide Name uniquely identifying a port on an HBA.

Time Variables

Below is a list of time variables and brief descriptions of the meaning of each variable. These variables represent exact timestamps as well as relative time.

Variable Name	Column Name	Description	Data Sample
duration	Duration	Duration of the event in minutes	160
duration_string	DurationString	A text string version of the duration	0:02:40
effective_time	EffectiveTime	The effective time referenced by the individual event. Must be a timestamp format.	
endtime	EndTime	End time of the event	
event_queue_time	EventQueueTime	Time that the event was queued.	
event_time	EventTime	Date/Time of the occurrence of the event as recorded by the system which generated it.	
event_time_string	EventTimeString	This values ALWAYS will equal the event_time. The primary usage for this variable is situations where customers have legacy data already captured in an alternate date format that does not conform to RSA's config specifications for the device.	
expiration_time	ExpirationTime	A timestamp that explicitly refers to an expiration.	
processing_time	ProcessingTime	The time spent processing the request (can be in ms or seconds)	

Variable Name	Column Name	Description	Data Sample
recorded_time	RecordedTime	The event time as recorded by the system the event is collected from. The usage scenario is a multi-tier application where the management layer of the system records it's own timestamp at the time of collection from its child nodes. Must be in timestamp format.	
starttime	StartTime	Start time of the event	
timezone	TimeZone	A time zone name or offset value	-0400 +0600 EDT GMT+0700

Updating Custom Reports

When you update an event source from standard content to Content 2.0, you may need to update your custom reports. For details on the scope of the work that you will need to do, see the *RSA enVision Content Inspection Tool* document. The Content Inspection tool detects and describes the changes you must make to your reports upon application of an Event Source Update.

Custom reports and dashboard reports are likely to need changes because the name of the table has probably changed, as well as some variables. In many cases, RSA has condensed the number of tables that store data.

This topic contains the following sections:

Determine Where Data is Stored

The first step is to determine where RSA enVision is storing the message data for the Content 2.0 version of the event source.

To view where parsed data is stored:

1. In enVision, navigate to **Overview** > **System Configuration** > **Messages** > **Manage Messages to Parse**.
2. Select the Content 2.0 event source in which you are interested.
3. Click the table name, or **All Messages**, to see the detailed table and variable information for the messages for the event source.

Use this information to determine where the information for messages is being stored. You can then use this information to edit your custom reports.

For example, here is some of the information for the McAfee Firewall Enterprise (formerly Sidewinder) event source.

Table	ID	Message
Firewall	t_acl_change	<@msg:*PARMVAL($MSG)><@fld61:*PARMVAL(process_id)>pid=<process_id>, ruid=<ruid>,euid=<euid>,pgid=<pgid>,logid=<logon_id>,cmd=<process>,domain=<domain>,edomain=<edomain>,acl_admin=<username>,acl_op=<acl_op>,acl_table=<acl_table>,acl_data=<info>
Firewall	t_aclallow	<@msg:*PARMVAL($MSG)><@fld61:*PARMVAL(process_id)>pid=<process_id>,

Table	ID	Message
		ruid=<ruid>,euid=<euid>,pgid=<pgid>,logid=<logon_id>,cmd=<process>,domain=<domain>,edomain=<edomaub>,hostname=<hostname>,event=<event_type>,srcip=<saddr>,srcport=<sport>,srcburb=<srcburb>,dstip=<daddr>,dstport=<dport>,dstburb=<dstburb>,protocol=<protocol>,service_name=<network_service>,agent_type=<agent>,user_name=<username>,auth_method=<authmethod>,rule_name=<rule>,acl_id=<policyname>,cache_hit=<cache_hit>,acl_position=<acl_pos>,reason=<result>
Firewall	t_acldeny	<@msg:*PARMVAL($MSG)><@fld61:*PARMVAL(process_id)>pid=<process_id>,ruid=<ruid>,euid=<euid>,pgid=<pgid>,logid=<logon_id>,cmd=<process>,domain=<domain>,edomain=<edomaub>,srcip=<saddr>,srcburb=<srcburb>,dstip=<daddr>,dstburb=<dstburb>,protocol=<protocol>,service_name=<network_service>,agent_type=<agent>,user_name=<username>,auth_method=<authmethod>,acl_id=<policyname>,cache_hit=<cache_hit>,acl_position=<acl_pos>,hostname=<hostname>,attackip=<stransaddr>,attackburb=<sburb>
Firewall	t_alert	<@result:*RMQ(result)><@msg:*PARMVAL($MSG)><@fld61:*PARMVAL(process_id)>pid=<process_id>,ruid=<ruid>,euid=<euid>,pgid=<pgid>,logid=<logon_id>,cmd=<process>,domain=<domain>,edomain=<edomain>,hostname=<hostname>,event=<event_type>,alert_name=<misc_name>,alert_type=<detail>,num_events=<fld1>,start_time=<starttime>,end_time=<endtime>,sacap_filter=<fld4>,alert_actions=<action>,dropped_count=<fld5>,syslog_alert=<level>,reason=<result>
Firewall	t_app_def_change	<@msg:*PARMVAL($MSG)><@fld61:*PARMVAL(process_id)>pid=<process_id>,ruid=<ruid>,euid=<euid>,pgid=<pgid>,logid=<logon_id>,cmd=<process>,domain=<domain>,edomain=<edomaub>,srcip=<saddr>,dstip=<daddr>,netsessid=<netsessid>,reason=<result>,acl_id=<policyname>,service_name=<network_service>,information=<info>

Update a Custom Report

You may need to change the table that your report uses. Make sure the report uses the new table where data is being stored for the Content 2.0 version of the parsing scheme.

Here are some guidelines to follow:

- Check that the fields you are using are correct.
- Check the SQL Where clause for variables that no longer exist, and map them to their new counterparts. For example, **laddr** (Local Address) and **faddr** (Foreign Address) are now **saddr** (Source Address) and **daddr** (Destination Address) respectively.
- Use **Query** to view the fields in a particular table:
    1. Navigate to **Analysis** > **Query** > **Create New Query**.
    2. Select the table where the data for your report is stored.
    3. Select all available fields.
    4. Choose a time frame that you know contains some data, and click **Run**.

The result displays values for each field. Use this information to help you make the necessary changes to your report.

Note: Older data is still stored in the older tables and the new data is stored in the new, Content 2.0 tables.

Rebuild Indexes (Optional)

You can either still use your old reports to get the old data, or you can use the Maintenance Command Line Interface utility (**lsmaint.exe**) to rebuild the indexes. Run this utility from a command prompt on your enVision appliance. Lsmaint.exe is located in **E:\nic\*version-number*\server-name\bin**.

To move data to the new tables, use the **-rebuild** flag. For example, the following command moves the last four months of data:

```
lsmaint -rebuild all -device device-ip-address -time -4m end
```

In the above command, *device-ip-address* is the specific IP address of the event source that sent the message data to RSA enVision.

Important: This command can take a very long time to run on large data sets. For more details on lsmaint.exe, see the **Maintenance Command Line Interface Utility (lsmaint.exe)** topic in the Help.

Note: The lsmaint command does not reindex events being collected during the current GMT day, so you must reindex those events the next GMT day.