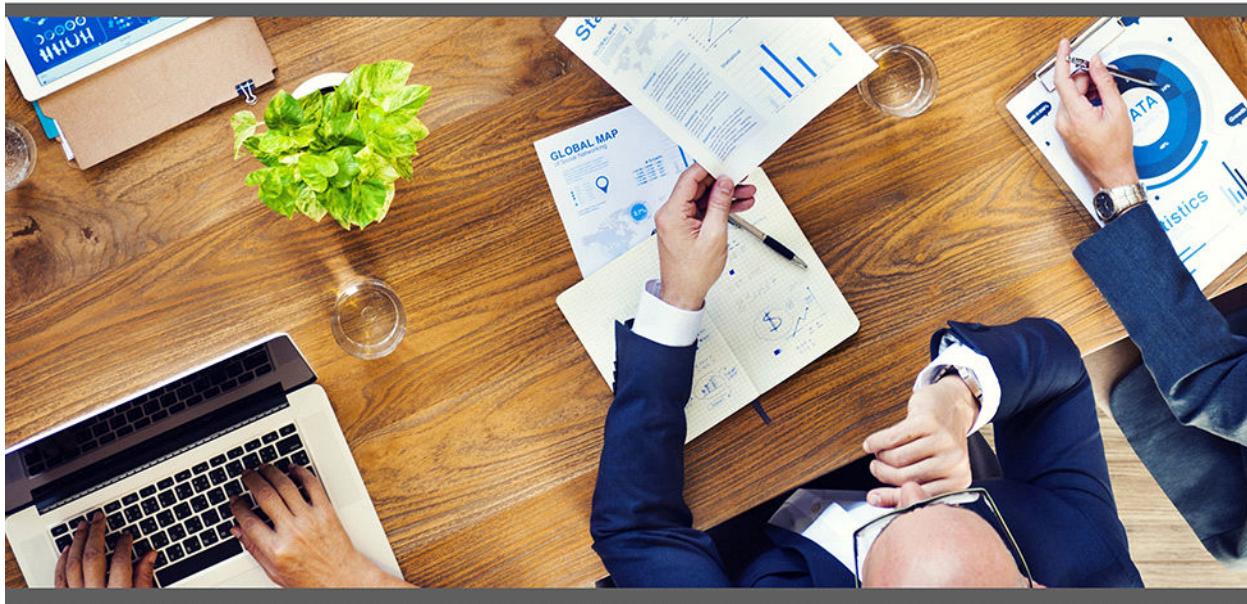




Ignite Technologies
Security and Compliance Solutions



Analytics Guide (DRAFT)

SenSage Standard 2016 (v. 6.1.1)

August 2, 2016

COPYRIGHT INFORMATION

No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic, mechanical, photocopied, recorded, or otherwise, without the prior written consent of Ignite Technologies, Inc.

401 Congress Avenue Suite 2650

Austin, TX 78701

800-248-0027

info@ignitetech.com

Copyright © 2016 Ignite Technologies, Inc.

All Rights Reserved.

Published June 21, 2016

TABLE OF CONTENTS

PREFACE	21
Audience for this Book	21
Analytics Guide Organization	21
Road Map to SenSage AP Documentation	23
Conventions Used in SenSage AP Documentation	25
Contacting Technical Support	26
CHAPTER 1: OVERVIEW OF SENSAge AP ANALYTICS	27
Analytics Workbench	28
IntelliSchema	28
Implementation of IntelliSchema	28
Connector Views	29
Master Views	29
Event-Type Views	29
Reference Tables	29
IntelliSchema Architecture	30
Namespaces in IntelliSchema	32
Event Focus	32
Event Types	32
Analytics Reports	33
Foundation Analytics Reports	33
Compliance Analytics Reports	34
McAfee Analytics Reports	34
Log Adapters	35
Log Adapter Verification	35
Tools for Managing and Using SenSage AP Analytics	35
Creating, Viewing, and Scheduling Reports	35
Exporting and Importing Analytics Components	36
Creating Views and Modifying IntelliSchema	36
CHAPTER 2: CONFIGURING AND EXECUTING THE INSIDER THREAT MODEL DETECTION	37
IT Detection Model and the Analytics Workbench	37
Overview: The Insider Threat Model Detection (IT Model)	37
User Requirements for Configuring the IT Model	38
Access and Privileges	38
Deployment Package and Recommended Database Client	39
Creating Views/Function(s), Schemas, and Database Tables for the IT Model	39
saw_simulated_data schema	39
aa_it_model_internals schema	40
aa_it_model_external_inputs schema	40
aa_it_model_baseline schema	41
Check for Populated Events Data	41
How to Modify Configuration Parameters in Analytics Workbench	41

Component Input Parameter	42
Configuring Changes for the Insider Threat Detection Model	44
IntelliSchema Name Configuration	44
Configuration Summary - IntelliSchema Name	45
Email Name Configuration	45
Configuration Summary - Email Domain	46
Human Resources Table Configuration	46
Configuration Summary - HR Table	47
Time Period Settings	48
Configuration Summary - Time Period Settings	48
External Inputs Schema and Watchlists, Whitelists, and Blacklists	49
Configuration Summary - External Inputs Schema	49
Modifying the Weighting used in the IT Model (for Advanced Users)	49
Configuration Summary: Model = Branch - Exfiltration	50
Configuration Summary: Model = Scores - Email Leaf Nodes	51
Configuration Summary: Model = Scores - Upload Leaf Nodes	51
Configuration Summary: Model = Scores - Login Leaf Nodes	51
Configuration Summary: Model = Scores - HR Leaf Nodes	52
Creating an Insider Threat Detection Dashboard	53
Drilling down to Log Events from Reports	55
Backfilling Data	59
Verifying the Model through a Regression Test	59
Monitoring Network Upload and Email Behavior	61
Upload Blacklist Behavior	61
Upload Whitelist Behavior	61
Email Watchlist	62
Email Whitelist	62
Obtaining Model Feedback with Advanced Analytics Models and Events Report	63
Events Report Associations	64
Executing the Insider Threat Model	66
Configuring and Executing the IT Model in a Hybrid Setup	66
AP Analyzer Configuration	66
Creating Schemas, Tables, Views, and Functions for the IT Model	67

CHAPTER 3: SAMPLE MODELS FOR WORKING WITH ANALYTICS WORKBENCH 69

Listing of Sample Models	69
Using Data Tables in Sample Models	72
Implementing Data Tables in Sample Models	74
Importing Sample Data Table Models	75
Setting up the Database	75
Sample Data Tables Description	76
Data Table Components	76
Sample Data Table Models Description	77
DT Scheduler: Failed Logins Count - All Metrics	77
DT Scheduler: Daily Bytes Uploaded - All Metrics	77
Data Table Programmable Fields	77
Data Table Outputs	79
Scheduling a Data Table	80
Sample Data Table Dashboard and Reports	81
Reports	81
Dashboard	82
Expected Results of Data Table Samples	82

Creating a New Data Table Using the Samples Provided	83
CHAPTER 4: SAMPLE MODEL DESCRIPTION: NOTIFICATION WHEN A THRESHOLD IS EXCEEDED IN A REPORT	85
Dataflow Description	85
How to Use the Notification Model	86
CHAPTER 5: INTELLISchema VIEWS REFERENCE	93
About IntelliSchema Views	93
IntelliSchema Event Type Reference	93
Account Addition and Deletion	95
Account Addition and Deletion: Windows	97
Administrative Account Activity	98
Administrative Account Activity: Linux/unix	99
Administrative Account Activity: Windows	100
Alert Event	101
Application Event	102
Arcsight CEF Forwarder Event	103
Audit Event	109
Database DDL (Data Definition Language)	111
Database DML (Data Manipulation Language)	111
IDS/IPS Event	113
Investigation Event	114
Loss of Audit Messages	117
Loss of Audit Messages: Windows	118
Mail Event	119
Malware Event	120
Network Device Connection	121
Network Device Connection: Router	122
Network Device Connection: Firewall	123
Parsed Data	124
Password Changes and Resets	127
Password Changes and Resets: Windows	128
Privileged Commands	129
Privileged Commands: BSM	130
Privileged Commands: Linux/Unix	131
Privileged Commands: Windows	132
Remote Access Event	133
Security Objects	134
Security Objects: Windows	135
System Startup and Shutdown	136
Startup and Shutdown: Windows	137
Startup and Shutdown: BSM	138
Unparsed Data	139
User Logins	141
User Logins: Router	143
User Logins: Windows	144
User Logins: Windows Non-domain Controller	145
User Logins: Windows	146

User Logins: Linux/Unix	147
Vulnerability Event	148
webProxy Event	149
Wireless Event	149
Connector Views and IntelliSchema Views	150
Reference Tables	164
Adding New Event Sources to IntelliSchema	165
Overview	165
Related Information	165
Source Analysis	166
Adding a New Event Source	166
IntelliSchema Naming Conventions	167
CHAPTER 6: ANALYTICS REPORTS LISTING	169
Compliance Analytics Reports	169
Foundation Reports	170
Systems Analytics Reports	173
McAfee Analytics Reports	175
BlueCoat Reports	178
HawkEye G Reports	178
PanOS Reports	182
SAP Reports	182
Miscellaneous Reports	182
CHAPTER 7: COMPLIANCE ANALYTICS REPORTS	185
Administrative Activity Monitoring Reports	185
Privileged Account Access Details	185
Privileged Account Access Summary	186
Administrative Account Activity	187
Administrative Account Activity Top 100 Summary	188
Privileged Command Summary	189
User-Level Reports	190
User Login Details	190
User Login Summary	192
Logins Outside Business Hours	193
Logins Outside Business Hours Summary	194
General Compliance Reports	196
System Startup and Shutdown	196
Security Objects Accessed	198
Security Objects Deleted	199
Network Device Monitoring Reports	200
Router Denied Connections Details	201
Router Authentication Failure Details	202
Firewall Monitoring Reports	203
Firewall Denied Connections Details	204
Firewall Denied Connections Summary	205
Firewall Accepted Connections Details	206
Firewall Accepted Connections Summary	207
Firewall All Connections Details - new	208

CHAPTER 8: FOUNDATION ANALYTICS REPORTS (WINDOWS) 211

Microsoft Windows Reports	211
Windows Login Activity Details	213
Windows Login Failure Summary	214
Windows Login Success Summary	215
Windows Login Failure Details	216
Windows Remote Login Details	217
Windows Account Addition and Deletion	218
Windows Account Modifications	219
Windows Group Member Addition and Deletion	220
Windows Group Modification Summary	221
Windows Password Changes and Resets	222
Windows User Account Locked and Unlocked by Date	223
Windows User Activity Journal	224
Windows Account Rights Modified	225
Windows User Special Privileges Details	226
Windows Privileged Account Access Details	227
Windows System Startup Summary	228
Windows New Process Started	229
Windows New Process Started Summary	230
Windows Audit Log Cleared Summary	231
Windows Application Events	232
Windows Application Events Summary per Day	233
Windows System Events	234
Windows System Event Summary per Day	235
Windows File Replication Service Events	236
Windows File Replication Service Events Summary per Day	237
Windows Error Events	238
Windows DNS Server Events	239
Windows DNS Server Events Summary per Day	240
Windows Directory Service Events	241
Windows Directory Service Events Summary per Day	242
Windows Major Security Events	243
Windows Loss of Audit Messages	244
Windows Active Directory Object Changes	245
Windows Active Directory Policy Changes	246
Windows Active Directory Users - Deleted or Disabled	247
Windows Active Directory Users - Lockouts and Password Resets	248
Windows Active Directory Users - New or Enabled	249
Windows Security Objects Accessed	250
Windows Security Objects Deleted	251
Windows Security Objects Access Optimized	252

CHAPTER 9: FOUNDATION ANALYTICS REPORTS (UNIX/LINUX) 253

Unix/Linux Reports	253
Unix or Linux Login Details	254
Unix or Linux Failed Login Summary by User	255
Unix or Linux Failed Login Summary by Count	256
Unix or Linux Failed Login Summary by Server	257
Unix or Linux Success Login Summary by User	258
Unix or Linux Success Login Summary by Count	259
Unix or Linux Success Login Summary by Server	260

Unix or Linux SSH and FTP Login Details	261
Unix or Linux Privileged Commands Details	262
Unix or Linux Elevated Access Success (su and sudo) Summary by Count	263
Unix or Linux Elevated Access Success (su and sudo) Summary by Date	264
Unix or Linux Elevated Access Success (su and sudo) Summary by Server	265
Unix or Linux Elevated Access Failed (su and sudo) Detail by Date ..	266
Unix or Linux Elevated Access Failed (su and sudo) Summary by Count	267
Unix or Linux Elevated Access Failed (su and sudo) Summary by Server	268
Unix or Linux Elevated SU Access Failed by Server	269
Unix or Linux Elevated SUDO Access Failed by Date	270
Unix or Linux Elevated SUDO Access Failed by Server	271
 CHAPTER 10: SYSTEMS ANALYTICS REPORTS	273
EDW (SLS) Command Tools Usage Reports	273
EDW (SLS) ATManage Command History	274
EDW (SLS) ATQuery Command History	275
EDW (SLS) Command History	276
EDW (SLS) Command History per User	277
EDW (SLS) Load Command History	278
EDW (SLS) Percent Disk Space Usage	279
EDW (SLS) System Disk Space Usage Alerts	280
EDW (SLS) System Disk Space per Node	281
Collector Activity Monitoring Reports	282
Collector Avg Load Size per Event Source	283
Collector Collection Exceeds x Event per Day -- Exception Report ..	284
Collector Collection Exceeds x GB per Day -- Exception Report ..	285
Collector Daily Load - Trend	286
Collector Daily Load per Event Source	287
Collector Daily Load per loaderEnd Type	288
Collector EPS Statistics	289
Collector Load Volume per Day	290
Collector Table Sizes per Timerange	291
Collector Total Load Volume per Event Source	292
Collector Total Number of Records and Avg Record Size per Source ..	293
Collector Total Number of Records in System	294
Collector Total Records Loaded per Table	295
Collector Total Records Loaded per Table per Day	296
Collector Total Number of Records in System	297
Internal Systems Reports	298
Internal System Failed Login Details	299
Internal System Report Activity Details	300
Internal System Report Activity Summary	301
Internal System Successful Admin Login to System	302
Internal System Successful Login Details	303
Internal System Successful Summary Login to System	304
Internal System User Activity Details	305
Internal System User Activity Summary	306
Internal System User Password Change	307

CHAPTER 11: McAfee Analytics Reports	309
Email and Web Security (EWS)	309
McAfee EWS Virus Email Details	309
McAfee EWS Virus Web Details	310
McAfee EWS Virus Web Summary	311
Database Activity Monitoring	312
McAfee - Detail Last 100 Records	313
McAfee - Detail Top 100 Records	315
McAfee - Investigation Most Active Agent Host	317
McAfee - Investigation Most Active Agent IP	317
McAfee - Investigation Most Active Command Type	318
McAfee - Investigation Most Active Database Name	319
McAfee - Investigation Most Active Database Type	319
McAfee - Investigation Most Active Database Version	320
McAfee - Investigation Most Active Exec User	321
McAfee - Investigation Most Active Module	321
McAfee - Investigation Most Active OS User	322
McAfee - Investigation Most Active Program	323
McAfee - Investigation Most Active Reporter Host	323
McAfee - Investigation Most Active Rule Name	324
McAfee - Investigation Most Active Source Host	325
McAfee - Investigation Most Active Source IP	325
McAfee - Investigation Wizard	326
McAfee - Statistics Command Type Access by Database Type, Name	328
McAfee - Statistics Database Name Access by Database Type	329
McAfee - Statistics Command Type Access by Database Type, Name	330
ePolicy Orchestrator (ePO)	331
McAfee ePO Top Threats	331
McAfee ePO Console Logon Activity	332
McAfee ePO Agents by Server	333
McAfee ePO Console Activity Summary	334
McAfee ePO Agent Communication Detail	335
McAfee ePO Agent Communication Top 100 Summary	336
Network Security Platform (IntruShield)	337
McAfee NSP Possible Successful Exploits (by Target)	338
McAfee NSP Possible Successful Exploits (by Source)	339
McAfee NSP Attacks Details	340
McAfee NSP Attacks Summary	341
McAfee NSP Top 20 Most Common Events	342
McAfee NSP Top 10 Source IP	343
McAfee NSP Top 10 Target IP	344
McAfee NSP Top 10 Directed Attacks	345
Vulnerability Manager (Foundstone)	346
McAfee Foundstone OS & Application Vulnerabilities	346
McAfee Foundstone Top 20 Affected Hosts	348
McAfee Foundstone High Risk Vulnerabilities	349
McAfee Foundstone High Risk Vulnerabilities Top 100 Summary	350
CHAPTER 12: BlueCoat Reports	351
BlueCoat - High Offender List	351
BlueCoat - Individual IP Usage Detail	352

BlueCoat - Top 10 Domains Visited	353
BlueCoat - Top Domains Visited by UserId	354
BlueCoat - Top Download Users	355
BlueCoat - Top Sending Users	356
BlueCoat - Top Users with Most Site Visits	357
CHAPTER 13: HAWKEYE G ANALYTICS REPORTS	359
Actions Monitoring Reports	359
Actions: File List Details	360
Actions: File List Investigation	361
Actions: File List Summary	362
Actions: Kill Process Details	363
Actions: Kill Process Investigation	364
Actions: Kill Process Summary	365
Actions: Network Connection List Details	366
Actions: Network Connections List Investigation	367
Actions: Network Connections List Summary	368
Actions: Process List Details	369
Actions: Process List Investigation	370
Actions: Process List Summary	371
Actions: Quarantine File Details	372
Actions: Quarantine File Investigation	373
Actions: Quarantine File Summary	375
Actions: Registry List Details	376
Actions: Registry List Investigation	378
Actions: Registry List Summary	379
Actions: Undo Quarantine File Details	380
Actions: Undo Quarantine File Investigation	381
Actions: Undo Quarantine File Summary	382
All Events Monitoring Reports	383
All Events Details	383
All Events Investigation	385
All Events Summary by Event Type	387
Device ThreatSync Monitoring Reports	388
Device ThreatSync Score Changes Details	389
Device ThreatSync Score Changes Investigation	390
Device ThreatSync Score Changes Summary by Host	391
Heuristics Monitoring Activity	392
Heuristics: File Details	393
Heuristics: File Investigation	394
Heuristics: File Top 100 Summary	395
Heuristics: Process Details	396
Example	396
Heuristics: Process Investigation	397
Heuristics: Process Summary	398
Heuristics: Registry Details	399
Example	399
Heuristics: Registry Investigation	400
Example	400
Heuristics: Registry Summary	401
Event Indicator Activity Monitoring reports	402
Indicator: DNS Inject Details	403

Indicator: DNS Inject Investigation	405
Example	406
Indicator: DNS Inject Summary	407
Indicator: IP Redirect Details	408
Example	409
Indicator: IP Redirect Investigation	410
Example	411
Indicator: IP Redirect Summary	412
Indicator: URL Match Details	413
Example	413
Indicator: URL Match Investigation	414
Example	414
Indicator: URL Match Top 100 Summary	415
Example	415
MIS Potential Monitoring reports	416
Malware Identification Service (MIS) Potential: File Details	417
Example	417
Malware Identification Service (MIS) Potential: File Investigation	418
Example	418
Malware Identification Service (MIS) Potential: File Summary	419
Example	419
Malware Identification Service (MIS) Potential: Process Details	420
Example	420
Malware Identification Service (MIS) Potential: Process Investigation	421
Example	421
Malware Identification Service (MIS) Potential: Process Summary	422
Example	422
Malware Identification Service (MIS) Potential: Registry Details	423
Example	423
Malware Identification Service (MIS) Potential: Registry Investigation	424
Example	424
Malware Identification Service (MIS) Potential: Registry Summary	425
Example	425
Threat Match Monitoring Reports	426
Threat Match: File Details	427
Example	427
Threat Match: File Investigation	428
Example	428
Threat Match: File Top 100 Summary	429
Example	429
Threat Match: Process Details	430
Example	430
Threat Match: Process Investigation	431
Example	431
Threat Match: Process Top 100 Summary	432
Example	432
Threat Match: Registry Details	433
Example	433
Threat Match: Registry Investigation	434
Example	434
Threat Match: Registry Top 100 Summary	435
Example	435
CHAPTER 14: PANOS REPORTS	437
Panos - IP Based Data Query	437

Panos - Threats Blocked Per Hour: total and by IAP	438
Panos - Top 100 Source-Destination IP Pairs by Session Count	439
CHAPTER 15: SAP REPORTS	441
SAP Security Audit - Program Summary	441
SAP Security Audit - Terminal Summary	442
SAP Security Audit - Top 10 Records	443
SAP Security Audit - User Summary	444
CHAPTER 16: MISCELLANEOUS REPORTS	445
Investigation Report	446
Microsoft Exchange - Audit Trail Integrity Events	447
CHAPTER 17: LOG ADAPTERS LISTING	449
Apache	449
Catbird	449
Checkpoint	449
Cisco	449
Hewlett-Packard	449
Microsoft Windows	449
McAfee	450
Oracle	450
Unix/Linux	450
VMware	450
Miscellaneous	450
CHAPTER 18: APACHE_ACCESS_SYSLOGNG	453
Summary Information	453
Setting up apache_access_syslogng Log Adapter	453
Source System Setup	454
Error Log Example	455
SenSage Collector Configuration	456
Sample Configuration Files	456
Collector Configuration (config.xml)	456
Syslog- ng Configuration Entries (syslog-ng.conf)	457
Troubleshooting	457
CHAPTER 19: APACHE_ERROR_SYSLOGNG	459
Summary Information	459
Setting up apache_error_syslogng Log Adapter	459
Source System Setup	460
Example for error log	461
SenSage Collector Configuration	462
Sample Configuration Files	462
Collector Configuration (config.xml)	462
Syslog- ng Configuration Entries (syslog-ng.conf)	463
Troubleshooting	463

CHAPTER 20: CATBIRD_VSECURITY_SYSLOGNG	465
Summary Information	465
Setting up the catbird_vsecurity_syslogng	465
Source System syslog Setup	466
SenSage AP Collector syslog-ng Setup	466
CHAPTER 21: CHECKPOINT_OPSEC_LEA	467
Summary Information	467
Setting up the checkpoint_opsec_lea Log Adapter	468
Source System syslog Setup	468
SenSage AP System Setup	468
SenSage AP Collector Setup	469
Custom Alerts Setup	470
CHAPTER 22: CISCO_ACS_SYSLOGNG	471
Summary Information	471
Setting up cisco_acs_syslogng Log Adapter	471
Source System Setup	472
SenSage AP Collector Configuration	472
Configuration Files Samples	473
Collector Configuration (config.xml)	473
Syslog-ng Configuration Entries (syslog-ng.conf)	473
CHAPTER 23: CISCO_ASA_SYSLOGNG	475
Summary Information	475
Setting up cisco_asa_syslogng Log Adapter	476
Source System Setup	476
SenSage AP Collector Configuration	476
Configuration Files Samples	477
Collector Configuration (config.xml)	477
Syslog-ng Configuration Entries (syslog-ng.conf)	478
CHAPTER 24: CISCO_IOS_SYSLOGNG	479
Summary Information	479
Setting up the cisco_ios_syslogng Log Adapter	479
Source System Setup	480
SenSage AP Collector syslog-ng Setup	480
CHAPTER 25: CISCO_IPS_ALERT_ERROR	483
Summary Information	483
Setting up cisco_ips_alert_error Log Adapter	483
Source System Setup	484
SenSage AP Collector Configuration	485
Sample Configuration Files	486
Collector Configuration (config.xml)	486
Cisco_IPS_Alert_Error.Retriever.Conf Entries	486

CHAPTER 26: CISCO_IRONPORT_EMAIL_SECURITY_APPLIANCES	487
Summary Information	487
Setting up cisco_ironport_Email_Security_Appliances Log Adapter	488
Source System Setup	488
SenSage AP Collector Configuration	489
Configuration Files Samples	489
Collector Configuration (config.xml)	489
CHAPTER 27: CISCO_NETFLOW_RECEIVER	491
Summary Information	491
Setting up the cisco_netflow_reciever Log Adapter	491
Source System Setup	492
SenSage AP Collector Setup	492
CHAPTER 28: CISCO_PIX_SYSLOGNG	495
Summary Information	495
Setting up the cisco_pix_syslogng Log Adapter	495
Source System Setup	496
HawkEye Collector Configuration	496
Sample Configuration Files	497
Collector Configuration (config.xml)	497
Syslog- <i>ng</i> Configuration Entries (syslog-<i>ng</i>.conf)	497
CHAPTER 29: F5_ASM_CEF_SYSLOGNG	499
Summary Information	499
Setting up f5_asm_cef_syslogng Log Adapter	499
Source System Setup	500
Logging Web Application Data	500
Response Logging Content Headers	500
Creating Logging Profiles	501
Configuring the Storage Filter	502
Setting Event Severity Levels for Security Policy Violations	503
SenSage AP Collector Configuration	504
CHAPTER 30: HEXIS_HAWKEYE_G_CEF_SYSLOGNG	505
Summary Information	505
Setting up hexis_hawkeye_g_cef_syslogng Log Adapter	505
Source System Setup	506
SenSage AP Collector Configuration	507
Samples of Configuration Files	507
Collector Configuration (Config.xml)	508
Syslog- <i>ng</i> Configuration Entries (syslog-<i>ng</i>.conf)	508
CHAPTER 31: HP_NONSTOP_EMS_CINSET_NSET	511
Summary Information	511
Setting up the hp_nonStop_ems_cinset_nset Log Adapter	511
Steps to Implement CINSET	512

Step 1: Install Log Adapters and Modify config.xml	512
Step 2: Creating SSH Keying Relationship	513
Step 3: Actions Needed in the NonStop Environment	513
Step 4: Getting Things Ready to Run	514
Step 5: Preliminary Testing	515
Trouble Shooting Guide	515
CHAPTER 32: HP_PROCURVE_T3T4_SYSLOGNG	517
Summary Information	517
CHAPTER 33: HP_PROCURVE_TMSZ_SYSLOGNG	519
Summary Information	519
CHAPTER 34: IBM_DB2_RDBMS	521
Summary Information	521
Setting up the ibm_db2_rdbms Log Adapter	521
Source System Setup	522
SenSage AP Collector Setup	524
Sample Configuration Files	525
Collector Configuration (config.xml)	525
CHAPTER 31: JUNIPER_NETSCREENFW_SYSLOGNG	529
Summary Information	529
Setting up the juniper_netscreenFw_syslogng Log Adapter	529
Source System Setup	530
SenSage AP Collector syslog-ng Setup	531
CHAPTER 32: McAFFEE_EPO_AUDIT_RDBMS	533
System Information	533
Setting up the mcafee_epo_audit_rdbms Log Adapter	533
Configuring the RDBMS Retriever	534
Reloading Data	535
Sample sources.conf file	535
Sample freetds.conf file	536
CHAPTER 33: McAFFEE_EPO_EVENT_RDBMS	537
System Information	537
Setting up the mcafee_epo_event_rdbms Log Adapter	537
Configuring the RDBMS Retriever	538
Reloading Data	539
Sample sources.conf file	539
Sample freetds.conf file	540
CHAPTER 34: McAFFEE_FOUNDSTONE_RDBMS	541
System Information	541
Setting up the mcafee_foundstone_rdbms Log Adapter	541

Configuring the RDBMS Retriever	542
Reloading Data	543
Sample sources.conf file	543
Sample freetds.conf file	544
CHAPTER 35: MCAFEE_INTRUSHIELD_RDBMS	545
System Information	545
Setting up the mcafee_intrushield_rdbms Log Adapter	545
Configuring the RDBMS Retriever	546
Reloading Data	547
Sample sources.conf file	547
CHAPTER 36: MCAFEE_INTRUSHIELD_SYSLOGNG	549
System Information	549
Setting up the mcafee_intrushield_syslogng Log Adapter	549
Source System Setup	550
SenSage AP Collector syslog-ng Setup	550
CHAPTER 37: MICROSOFT_DNS_DEBUG_SENSAGERETRIEVERAGENT ..	553
Summary Information	553
Setting up microsoft_dns_debug_sensageRetriever Log Adapter ..	553
Source System Setup	554
SenSage AP Collector Configuration	554
Sample Configuration Files	554
SenSage AP Collector Configuration (config.xml)	555
Syslog- <i>ng</i> Configuration Entries (syslog-<i>ng</i>.conf)	555
CHAPTER 38: MICROSOFT_EXCHANGE_ADMIN_EVENTS_SYSLOGNG ..	557
Summary Information	557
Setting up microsoft_exchange_admin_events_	
syslogng Log Adapter	557
Source System Setup	558
SenSage AP Collector Configuration	558
Sample Configuration Files	558
SenSage AP Collector Configuration (config.xml)	559
Syslogng Configuration Entries (syslog-<i>ng</i>.conf)	559
CHAPTER 39: MICROSOFT_EXCHANGE_MAILBOX_EVENTS_SYSLOGNG ..	561
Summary Information	561
Setting up microsoft_exchange_mailbox_events_	
syslogng Log Adapter	561
Source System Setup	562
SenSage AP Collector Configuration	562
Sample Configuration Files	562
Collector Configuration (config.xml)	563
Syslog- <i>ng</i> Configuration Entries (syslog-<i>ng</i>.conf)	563
CHAPTER 40: MICROSOFT_EXCHANGE_TRACKING_	

SENSAGERETRIEVERAGENT	565
Summary Information	565
Setting up microsoft_exchange_tracking_	
sensageRetrieverAgent Log Adapter	565
Source System Setup	566
Exchange Management Console	566
Exchange Management Shell	567
SenSage AP Collector Setup	567
HawkEye Retriever Setup	567
CHAPTER 41: MICROSOFT_SHAREPOINT_AUDIT_SENSAGERETRIEVERAGENT	571
Summary Information	571
Setting up microsoft_sharepoint_audit_	
sensageRetrieverAgent Log Adapter	571
Source System Setup	572
SenSage AP Collector Setup	572
SenSage AP Retriever Setup	573
CHAPTER 42: MICROSOFT_WINDOWS_NONSECURITYEVENT_SENSAGERETRIEVER	577
Setting up the Microsoft_Windows_NonSecurityEvent_sensageRetriever	578
CHAPTER 43: MICROSOFT_WINDOWS_SECURITYEVENT_SENSAGERETRIEVER	579
System Information	579
Setting up the microsoft_windows_securityEvent_	
sensageRetriever Log Adapter	580
Source System Setup	580
Source System Setup for Windows machines (no Active Directory) ..	581
Source System Setup for Windows machines (Active Directory domain)	584
SenSage AP Collector Configuration	585
CHAPTER 44: MICROSOFT_WINDOWS2008_SECURITYEVENT_SENSAGERETRIEVER	587
System Information	587
Setting up the microsoft_windows2008_securityEvent_	
sensageRetriever Log Adapter	588
Source System Setup	588
Source System Setup for Windows Machines (no Active Directory) ..	589
Source System Setup for Windows Machines (Active Directory Domain)	591
SenSage AP Collector Configuration	593
CHAPTER 45: MICROSOFT_WINDOWS_SECURITYEVENT_SNARE	595
System Information	595
Setting up the microsoft_windows_securityEvent_	
snare Log Adapter	596

Source System Setup:	596
Configuring Snare Agent	603
SenSage AP Collector syslog-ng Setup	604
CHAPTER 46: MICROSOFT_WINDOWS2010_APPEVENT_SENSAGERETRIEVER (FOR WINDOWS 7, 8, 10)	607
Setting up the microsoft_windows2010_appEvent_sensageRetriever Log Adapter	607
CHAPTER 47: MICROSOFT_WINDOWS2010_SYSEVENTS_SENSAGERETRIEVER	611
System Information	611
Setting up the microsoft_Windows2010_sysEvent_Log Adapter	611
CHAPTER 48: ORACLE_ADUMP	615
Summary Information	615
Setting up oracle_adump Log Adapter	616
Source System Setup	616
CHAPTER 49: ORACLE_ADUMP_SYSLOGNG	617
Summary Information	617
Setting up oracle_adump_syslogng Log Adapter	618
Source System Setup	618
SenSage AP Collector Configuration	619
Sample Configuration Files	619
Collector Configuration (config.xml)	619
CHAPTER 50: ORACLE_DATABASE_FGA_SENSAGERETRIEVER	621
Setting up the oracle_database_fga sensageRetriever	621
Source System Setup	622
Fine Grained Audit	622
Configuring the Agentless Retriever	623
SenSage AP Collector Setup	623
CHAPTER 51: ORACLE_DATABASE_SYSAUDIT_SENSAGERETRIEVER	625
Summary Information	625
Setting up the oracle_database_sysaudit sensageRetriever	625
Configuring the AgentLess Retriever	626
SenSage AP Collector Setup	626
CHAPTER 52: ORACLE_FGA_XML_BATCH	627
Summary Information	627
Setting up oracle_fga_xml_batch Log Adapter	627
Source System Setup	628
Sys Audit	628
FGA Sys Audit	628

Sample Configuration Files	629
Collector Configuration (config.xml)	629
CHAPTER 53: SAP_AUD_SFTP	631
System Information	631
Setting up the sap_aud_sftp Log Adapter	631
Configure Source System	632
SenSage AP Collector Setup	632
CHAPTER 54: SUN_BSM_SFTP	633
System Information	633
Setting up the sun_bsm_sftp Log Adapter	633
Source System syslog Setup	634
SenSage AP Collector Setup	634
CHAPTER 55: SYMANTEC_ENDPOINT_SYSLOGNG	635
Summary Information	635
Setting up symantec_endpoint_syslogng Log Adapter	635
Source System Setup	636
SenSage AP Collector Configuration	636
Sample Configuration Files	636
Collector Configuration (config.xml)	636
Syslog- <i>ng</i> .Configuration Entries (syslog-<i>ng</i>.conf)	637
CHAPTER 56: SYSLOGNG_CATCHALL_SYSLOGNG	639
System Information	639
Setting up the syslogng_catchall_syslogng Log Adapter	639
Source System syslog Setup	640
Linux	640
HP-UX	640
Sensage AP Collector syslog- <i>ng</i> Setup	641
CHAPTER 57: TIPPING_POINT_SYSLOGNG	643
System Information	643
CHAPTER 58: UNIX_FTPD_SYSLOGNG	645
System Information	645
Setting up the unix_ftpd_syslogng Log Adapter	645
Source System syslog Setup	646
Linux	646
HP-UX	646
SenSage AP Collector syslog- <i>ng</i> Setup	647
CHAPTER 59: UNIX_LOGIN_SYSLOGNG	649
System Information	649
Setting up the unix_login_syslogng Log Adapter	649

Source System syslog Setup	650
Linux	650
HP-UX	650
HawkEye Collector syslog-ng Setup	651
CHAPTER 56: UNIX_SSHD2_SYSLOGNG	653
System Information	653
Setting up the unix_sshd2_syslogng Log Adapter	653
Source System syslog Setup	654
Linux	654
HP-UX	654
SenSage AP Collector syslog-ng Setup	655
CHAPTER 57: UNIX_SU_SYSLOGNG	657
System Information	657
Setting up the unix_su_syslogng Log Adapter	657
Source System syslog Setup	658
Linux	658
HP-UX	658
SenSage AP Collector syslog-ng Setup	659
CHAPTER 58: UNIX_SUDO_SYSLOGNG	661
System Information	661
Setting up the unix_sudo_syslogng Log Adapter	661
Source System syslog Setup	662
Linux	662
HP-UX	662
SenSage AP Collector syslog-ng Setup	663
CHAPTER 59: VMWARE_ESX_500_SYSLOGNG	665
System Information	665
Setting up vmware_esx_500_syslogng Log Adapter	665
Source System Setup	666
SenSage AP Collector Configuration	667
Sample Configuration Files	667
Collector Configuration (config.xml)	667
Syslog -ng Configuration Entries (syslog-ng.conf)	668
APPENDIX A: REPORT LIBRARIES REFERENCE	669
Geo IP Utility	669
domain()	669
Synopsis	669
Arguments	669
Example	669
Return Value	669
get_country_from_domain()	669
Synopsis	670
Arguments	670

Example	670
Return Value	670
IP Conversion Utility	670
hex_to_dotted_quad(IP address in Hexadecimal format)	670
Synopsis	670
Arguments	670
Return Value	670
Example	671
Internal System Audit Library	671
service2Description()	671
Synopsis	671
Arguments	671
Return Value	671
Example	671
Microsoft Windows Library	671
loginType2desc()	672
Synopsis	672
Arguments	672
Return Value	672
Example	672
eventId2desc()	672
Synopsis	672
Arguments	672
Return Value	672
Example	672
rights2desc()	673
Synopsis	673
Arguments	673
Return Value	673
Example	673
k5code2desc()	673
Synopsis	673
Arguments	673
Return Value	673
Example	673
APPENDIX B: SYSLOG-NG SETUP	675
About syslog-ng	675
syslog-ng.conf file	676
destination statement: escaped characters	676
Log Statement: flags(final);	677
Log Statement: Order of Processing and String Matching	677
Setting Up Syslog-NG Log Rotation	677
INDEX	679

Table of Contents

PREFACE

This book, the *Analytics Guide*, describes the 6.1.1 version of SenSage AP software.

It provides instructions on how to configure the Log Adapters provided with your SenSage AP software. Each Log Adapter's configuration is discussed in a separate chapter titled with the name of the Log Adapter. Configuration steps include SenSage AP setup steps, source system setup steps, and `syslog-ng` configurations (where needed).

This Preface contains the following sections:

- “Audience for this Book”, next
- “Analytics Guide Organization”, on page 21
- “Road Map to SenSage AP Documentation”, on page 23
- “Conventions Used in SenSage AP Documentation”, on page 25
- “Contacting Technical Support”, on page 26

AUDIENCE FOR THIS BOOK

This book is intended for:

- system administrators, partners, and professional service personnel who configure log collection for a SenSage AP deployment. (Knowledge of the source system(s), `syslog-ng`, and the enterprise's network environment is required.)
- business analysts who view or write reports

ANALYTICS GUIDE ORGANIZATION

This book contains the following chapters:

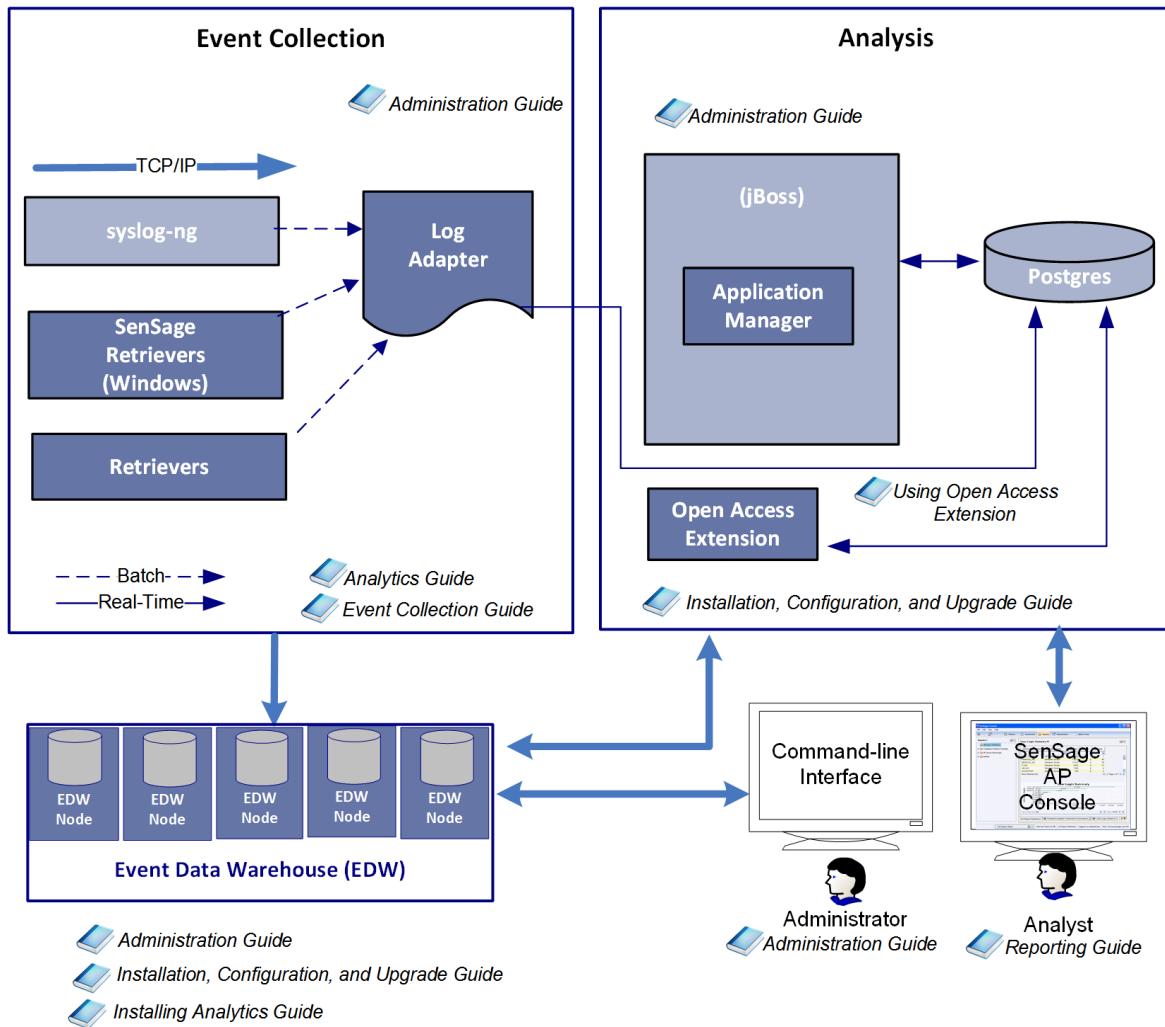
- [Chapter 1: Overview of SenSage AP Analytics](#)—Describes SenSage AP Analytics and IntelliSchema
- [Chapter 2: Configuring and Executing the Insider Threat Model Detection](#)—Provides required configuration for the IT Detection Model, which uses log events and human resources information to compute a daily insider threat risk score.
- [Chapter 3: Sample Models for Working with Analytics Workbench](#)—Provides a list of sample models included in your system for working with Analytics Workbench.
- [Chapter 4: Sample Model Description: Notification when a Threshold is Exceeded in a Report](#)—Provides a sample model description to include a notification when a given threshold is exceeded in a report.
- [Chapter 5: IntelliSchema Views Reference](#)—Provides reference on the IntelliSchema views on which SenSage AP Analytics reports run
- [Chapter 6: Analytics Reports Listing](#)—Provide brief overview on each available report category provided with your SenSage AP software, reports contained in them, and a brief description of each report.

- [Chapter 7: Compliance Analytics Reports](#)—Provides reference on the SenSage AP Compliance Analytics Reports
- [Chapter 8: Foundation Analytics Reports \(Windows\)](#)—Provides reference on the SenSage AP Analytics Foundation Reports for Microsoft Windows
- [Chapter 9: Foundation Analytics Reports \(Unix/Linux\)](#)—Provides reference on the SenSage AP Analytics Foundation Reports for Unix/Linux
- [Chapter 10: Systems Analytics Reports](#)—Provides reference on the following group or reports: EDW command tools usage reports, Collector activity reports, and internal system reports.
- [Chapter 11: McAfee Analytics Reports](#)—Provides reference on the SenSage AP McAfee Analytics Reports
- [Chapter 12: BlueCoat Reports](#)—Provides reference on the SenSage AP BlueCoat Reports
- [Chapter 13: HawkEye G Analytics Reports](#)—Provides reference on the HawkEye G Analytics Reports
- [Chapter 14: Panos Reports](#)—Provides reference on the SenSage AP Panos Reports
- [Chapter 15: SAP Reports](#)—Provides reference on the SenSage AP SAP Reports
- [Chapter 16: Miscellaneous Reports](#)—Provides reference on the SenSage AP Miscellaneous Reports
- Chapters [24](#) through [59](#)—Provide information for System Administrators on how to configure SenSage AP Log Adapters for a variety of sources. Log adapters allow SenSage AP to access and store data from software and hardware devices.
- [Appendix A: Report Libraries Reference](#)—Provide functions for common look-up and conversion operations that apply to SQL reports.
- [Appendix B: SYSLOG-NG Setup](#)—Provides a reference for System Administrators on setting up syslog-ng.

ROAD MAP TO SENSAge AP DOCUMENTATION

This document, the *Analytics Guide*, is part of the larger documentation set of your SenSage AP system. **Figure P-1** illustrates SenSage AP components and modules in the context of their function within the SenSage AP system.

Figure P-1: Road Map to SenSage AP Documentation



The table below describes all the manuals in the SenSage AP documentation set and the user roles to which they are directed.

Role	Tasks	Documentation
Analyst, Report Developer, System Administrator	<ul style="list-style-type: none"> • Create and edit reports, charts, and models • Create and edit dashboards • Manage SenSage AP Users • Manage SenSage AP Models • Create and edit data models • Write SQL code and queries 	<i>Analyzer Guide</i>
Business Analyst or System Administrator	<ul style="list-style-type: none"> • Learn about Analytics • Use IntelliSchema views • Learn about the Foundation and Compliance Analytics packages • Learn about additional Analytics packages 	<i>Analytics Guide</i>
Developer, Report Developer or Security Analyst	<ul style="list-style-type: none"> • Use SenSage AP SQL, SenSage AP SQL functions, and libraries to create reports or query the EDW • Access EDW data using open standards as ANSI SQL, ODBC, and JDBC • Create and use Perl code in SenSage AP SQL statements • Use the DBD Driver to query SenSage AP from other locations 	<i>Event Data Warehouse Guide</i>
Security System Administrator	<ul style="list-style-type: none"> • Configure retrievers, receivers, and collectors • Enable/disable log adapters • Configure SenSage Retriever • Create log adapter PTL files 	<i>Collector Guide</i>
System Administrator	<ul style="list-style-type: none"> • Install SenSage AP • Configure SenSage AP and its components • Configure Vmware 	<i>Installation, Configuration, and Upgrade Guide</i>
System Administrator	<ul style="list-style-type: none"> • Manage the HawkEye Event Data Warehouse (EDW) • Manage the Collector • Manage users, groups, and permissions • Archive to nearline storage • Manage assets & monitor security alerts • Monitor log source health • Monitor system health • Troubleshoot • Error Messages 	<i>Administration Guide</i>
Legal	Monitor third-party licenses	<i>Third-Party Open Source Licensing</i>

TIP: You can access the manuals listed above from:

- SenSage AP Welcome page
- Click the **Documentation** hyperlink.

CONVENTIONS USED IN SENSAge AP DOCUMENTATION

This convention...	Indicates...	Example
bold text	Names of user interface items, such as field names, buttons, menu choices, and keystrokes	Click Clear Filter .
<i>italic text</i>	Indicates a variable name or a new term the first time it appears	<code>http://<host>:<port>/index.mhtml</code>
Courier text	Indicates a literal value, such as a command name, file name, information typed by the user, or information displayed by the system	<code>atquery localhost:8072 myquery.sql</code>
SMALL CAPS	Indicates a key on the computer keyboard	Press ENTER .
{ }	In a syntax line, curly braces surround a set of options from which you must choose one and only one. NOTE: Syntax specifications for SELECT statements include curly braces as part of the <code>{INCLUDE_BAD_LOADS}</code> keyword.	<code>{ start stop restart }</code>
[]	In a syntax line, square brackets surround an optional parameter	<code>atquery [options] <host>:<port> -</code>
	In a syntax line, a pipe within square brackets or curly braces separates a choice between mutually exclusive parameters NOTE: Syntax for defining a Nearline Storage Address (NSA) includes a pipe.	<code>{ start stop restart }</code> <code>[g m]</code>
...	In a syntax line, ellipses indicate a repetition of the previous parameter	The following example indicates you can enter multiple, comma-separated options: <code><option> [, <option> [...]]</code>

This convention...	Indicates...	Example
backslash (\)	A backslash in command-line syntax or in a command example behaves as the escape character on Unix. It removes any special meaning from the character immediately following it. In SenSage AP documentation, a backslash nullifies the special meaning of the newline character as a command terminator. Without the backslash, pressing ENTER at the end of the line causes the Unix system to execute the text preceding the ENTER. Without the backslash, you must allow long commands to wrap over multiple lines as a single line.	atquery --user=administrator \ --pass=pass:p@ss localhost:8072\ -e='SELECT * FROM system.users;'

CONTACTING TECHNICAL SUPPORT

For additional help, call +1 855-529-3929. Also you can log into the IgniteTechTechnical Support web page under Services at <http://www.ignitetech.com> for SenSage AP documentation, product downloads, and additional information on contacting support to escalate help on issues that impact your production environment.

CHAPTER 1

Overview of SenSage AP Analytics

This chapter provides an overview of *SenSage AP Analytics*, a comprehensive solution for reporting on event data stored in the SenSage AP Event Data Warehouse (EDW). SenSage AP Analytics allow you to quickly retrieve and correlate data from multiple log sources without having to understand and manipulate the underlying data store.

SenSage AP Analytics includes the following features, which are discussed in this chapter:

- **Analytics Workbench** is a component in SenSage AP that allows users to execute advanced analytics data processing on the log event data stored in the Event Data Warehouse or other databases. The Analytics Workbench has a drag and drop graphical programming functionality to provide advanced analytic processing capability.
- **IntelliSchema™** is a pre-defined data structure that helps you create reports that display normalized event data for common types of events from various information systems and devices. See “[IntelliSchema](#)”, on page 28.
- **Analytics Reports** are ready-to-run and you can use them to view event data. See “[Analytics Reports](#)”, on page 33.
- **Log adapters** parse raw event data from heterogeneous information systems such as Microsoft Windows and Unix systems, network devices such as routers and firewalls, and applications such as Apache HTTP Server or PeopleSoft into discrete fields for storage in the *Event Data Warehouse Guide*. See “[Log Adapters](#)”, on page 35.
- **Tools for managing Analytics** provide the ability to export and import reports and libraries between SenSage AP deployments. See “[Tools for Managing and Using SenSage AP Analytics](#)”, on page 35.

Figure 1-1: SenSage AP Analytics

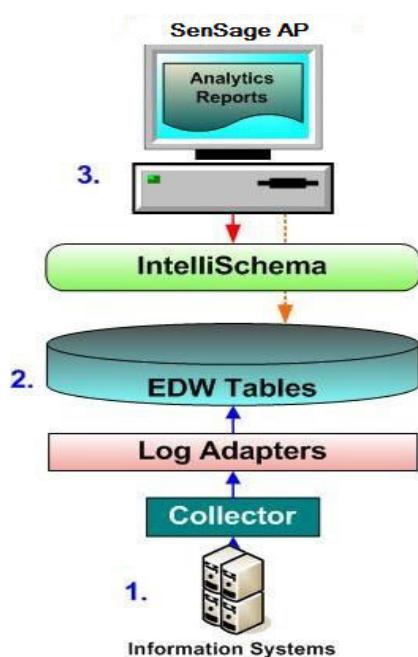


Figure 1-1 shows how data flows from the original event data sources, through IntelliSchema and to the Analytics Reports that you can view or modify using SenSage AP Analyzer. Some reports query EDW tables directly (dotted orange line).

- 1 Event data is collected from monitored information systems using the SenSage Collector.
- 2 Log adapters parse the event data collected from various information systems and store the parsed and normalized data in tables in the EDW.
- 3 Users run pre-defined Analytic reports with SenSage AP Analyzer. These reports can query IntelliSchema views or tables in the EDW. You can view the reports in the AP Analyzer.

ANALYTICS WORKBENCH

The Analytics Workbench is a component in SenSage AP that allows users to execute advanced analytics data processing on the log event data stored in the Event Data Warehouse or other databases. The Analytics workbench has a drag and drop graphical programming functionality to provide advanced analytic processing capability.

A set of analytics processing components put together in the Analytics Workbench is called a model. Models may be created, saved, reused, or even scheduled to execute periodically. One of the capabilities delivered with SenSage AP is a model called the Insider Threat Detection Model, which is described in the Tech Notes titled, *How to Configure and Execute the Insider Threat Detection Model*.

INTELLISchema

IntelliSchema is an abstraction and normalization layer between the raw, un-normalized data collected from log sources and the reports business analysts use to analyze event data. IntelliSchema provides several important advantages for analysis of event data:

- Business analysts can use IntelliSchema to create and view reports on event data gathered from heterogeneous systems without needing to understand the underlying raw data format. Data from various log sources that report on the same type of event are automatically correlated and presented as a single set of data. For example, analysts can create a report of login events that includes login events from Windows systems, Unix systems, and routers, or they can create a report on login events from specific log sources or systems.
- Business analysts can use one of the many ready-to-run Analytics report definitions provided with the SenSage AP distribution to view reports on common event types. Many of these reports use IntelliSchema views as their data source. (See “[Implementation of IntelliSchema](#)”, [next](#).)
- New data sources can be added to your SenSage AP deployment. Business analysts can then query data from these new sources using IntelliSchema and Analytics Reports without the need to modify reports or views. See “[Adding New Event Sources to IntelliSchema](#)”, [on page 165](#).
- IntelliSchema does not modify the data collected from your log sources, it leaves the data available for legal compliance or additional analysis.

Implementation of IntelliSchema

The SenSage EDW contains tables that store event data collected from the information systems monitored by a SenSage AP deployment. As shown in [Figure 1-3, Event Data Warehouse Guide Tables](#) store the event data (after the data is parsed by a log adapter) as a set of *columns* that represent discrete pieces of data contained in the logs, such as IP addresses, user account IDs, time stamps, and application-specific event data. (See “[Log Adapters](#)”, [on page 35](#).) A copy of the raw log data is also saved in the Event Data Warehouse Guide tables.

IntelliSchema uses SQL *views* to create a unified presentation of event data from disparate systems. A SQL view is a virtual table that exposes data contained in one or more tables. You can query a SQL view using the same methodologies you use to query a table.

Connector Views

Each of the tables in the EDW has its own unique schema (the structure of the columns in the table) and each table that is part of IntelliSchema also has one or more associated *connector views*, one for each *Event-type*. (Some Analytics reports do not use IntelliSchema views and query the EDW tables directly.) **Event Types** are high-level categorizations of event data, such as logins, start ups, and shut downs. Connector views normalize the data by enforcing consistent use of column names, data types, and formats, and by consistently presenting disparate event data that indicates the same information. For example, information systems may log a successful connection event using a proprietary event code or a string such as “succeeded”. Connector views normalize this data across all sources by using a consistent string, such as “Success” to indicate a successful connection.

Master Views

Master views reference event-type views to create a unified view of a single event type from multiple, heterogeneous information systems. For instance, you can use the User Logins master view to create a report of user logins from Window systems, Unix systems, routers, and the SenSage AP system itself.

Event-Type Views

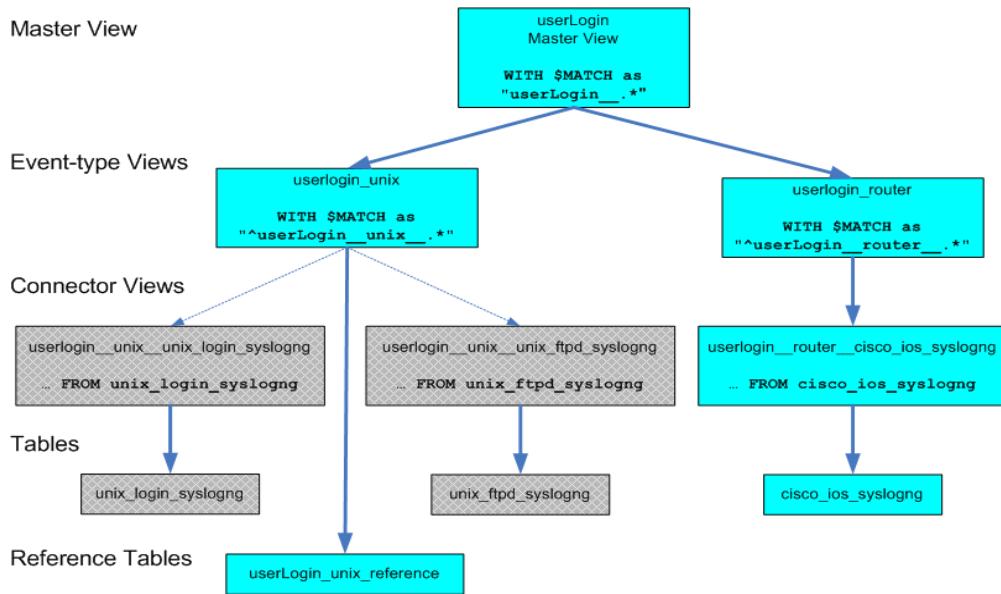
Event-type views also reference multiple connector views to create a unified view of a single event type for a grouping of connector views. Event-type views contain columns that represent data relevant to their groupings as well as columns that are common to the master view for the event type.

Reference Tables

Reference Tables are tables created to accommodate cases where Master or Event-type views reference data for which data collection is not configured. Connector views and tables are created when a log adapter is installed. Most SenSage AP deployments install only a subset of available log adapters, meaning that some tables referenced by views are not created.

NOTE: When you install IntelliSchema, reference tables are automatically created. If you add additional views that refer to tables or views used in IntelliSchema, or if you create a new Log Adapter, use this section to learn how to make sure your views work correctly.

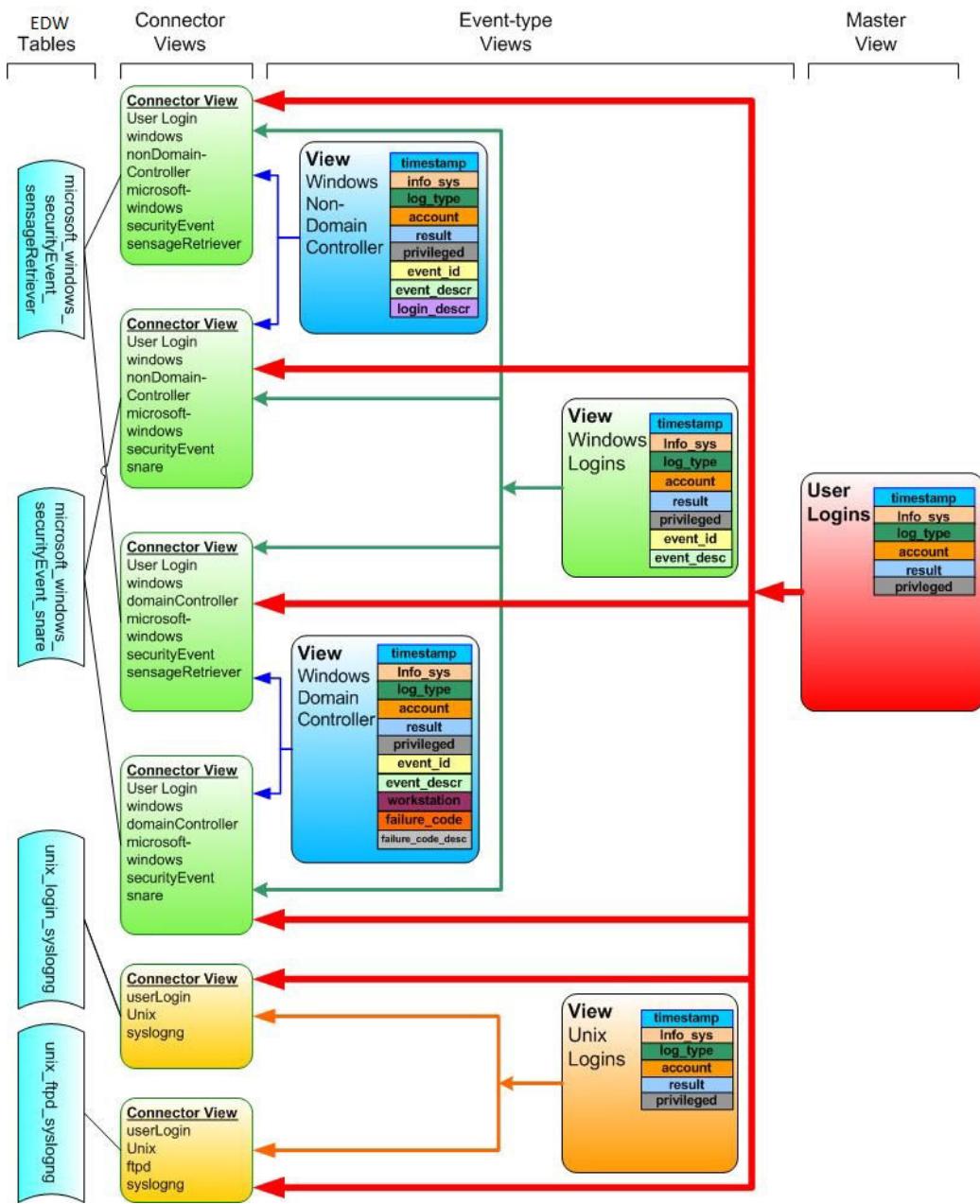
In the example shown in [Figure 1-2](#), if the unix_login_syslogng and unix_ftpd_syslogng log adapters are NOT installed (shown greyed-out), their corresponding tables (unix_login_syslogng and unix_ftpd_syslogng) are not created. When the system attempts to create the userLogin_unix view, it would fail because the tables referenced by the SQL used to create the view (WITH \$MATCH as " ^ userLogin_unix_.*") do not exist. To prevent such failures, a reference table(userLogin_unix_reference) is created before log adapter installation. Because the name of this table is matched by the MATCH statement, the view can be created successfully.

Figure 1-2: Reference Tables

IntelliSchema Architecture

[Figure 1-3](#) shows four Windows connector views and two Unix connector views for the User Logins event type group. [Figure 1-3](#) also shows event-type views for Windows Non-Domain Controller Logins, Windows Domain Controller Logins, Windows Logins, and Unix Logins. The master view for User Logins is shown in red, to the right.

NOTE: The tables, columns, and views shown in [Figure 1-3](#) are only a sample of those available in IntelliSchema and are presented only to demonstrate the architecture of IntelliSchema. Some of the column names may be abbreviated for display purposes. For a complete reference of IntelliSchema views, see “[IntelliSchema Views Reference](#)”, on page 93.

Figure 1-3: IntelliSchema Architecture

Namespaces in IntelliSchema

You can use namespaces to segregate the event data stored in a SenSage AP deployment. For example, you can create a namespace for geographical regions, departments, types of information systems, or other criteria. If you want to use IntelliSchema views to create reports for data stored in a namespace, or use report definitions from an Analytics reports, you need to install a copy of IntelliSchema into each namespace. By default, your data and IntelliSchema views will be located in the default namespace, called “`default`”.

When you install IntelliSchema into a namespace, a sub-namespace is created for IntelliSchema called `intellischema`. For example, if your namespace is called “`EastCoast`”, the namespace containing IntelliSchema would be named `EastCoast.intellischema`.

IntelliSchema connector views exist in a sub-namespace below the IntelliSchema namespace. In this example, the namespace containing IntelliSchema connector views would be named `EastCoast.intellischema.intellischema.__connectors`.

Event Focus

Because information systems log many similar types of events, the SenSage AP Analytics reports are focused on these events rather than their sources. This focus allows the reports to display similar event data from one or more log sources. For example, a report based on the User Access event type might report on user access events that occurred in both Windows and Unix systems.

The Analytics Reports and IntelliSchema views are organized around a set of *event types*, discussed next.

Event Types

IntelliSchema master views are available for the following event types; additional event types can be added at any time. For details on each of these views and related event-type views, see the following sections:

- “[Account Addition and Deletion](#)”, on page 95
- “[Administrative Account Activity](#)”, on page 98
- “[Alert Event](#)”, on page 101
- “[Application Event](#)”, on page 102
- “[Audit Event](#)”, on page 109
- “[Database DDL \(Data Definition Language\)](#)”, on page 111
- “[Database DML \(Data Manipulation Language\)](#)”, on page 111
- “[IDS/IPS Event](#)”, on page 113
- “[Investigation Event](#)”, on page 114
- “[Loss of Audit Messages](#)”, on page 117
- “[Mail Event](#)”, on page 119

- “Malware Event”, on page 120
- “Network Device Connection”, on page 121
- “Parsed Data”, on page 124
- “Password Changes and Resets”, on page 127
- “Privileged Commands”, on page 129
- “Remote Access Event”, on page 133
- “Security Objects”, on page 134
- “Security Objects: Windows”, on page 135
- “System Startup and Shutdown”, on page 136
- “Unparsed Data”, on page 139
- “User Logins”, on page 141
- “Vulnerability Event”, on page 148
- “webProxy Event”, on page 149
- “Wireless Event”, on page 149

Analytics Reports

Your SenSage AP installation include the following eight types of Analytics reports: Compliance Analytics, Foundation Analytics (including Internal Monitoring) McAfee Analytics, and Panos, SAP, and miscellaneous reports.

Foundation Analytics Reports

The Foundation Analytics reports display event data from Microsoft Windows and Unix systems, including internal monitoring data.

LOG SOURCES SUPPORTED

The Foundation Analytics reports supports the following log sources:

- Microsoft Windows—Microsoft Windows Security events on Windows 2003 servers and workstations
- Unix/Linux—System (syslog) events produced on all common Unix/Linux platforms, including Red Hat Enterprise Linux, HP-UX, IBM AIX, Novell Suse, and Sun Solaris.
- SenSage AP—Basic system health and monitoring for a SenSage AP deployment.

For a complete description of the Foundation Analytics reports and descriptions of each report, see [Chapter 8: Foundation Analytics Reports \(Windows\)](#) or [Chapter 9: Foundation Analytics Reports \(Unix/Linux\)](#), and [Chapter 10: Foundation Analytics Internal Monitoring Reports](#).

Compliance Analytics Reports

The Compliance Analytics reports assist customers in meeting specific regulations and monitoring critical areas of their information infrastructure.

LOG SOURCES SUPPORTED

The Compliance Analytics reports supports the following log sources:

- Unix syslog-based sshd
- Unix sudo
- Unix su
- Unix login
- Unix ftpd
- Windows Event Log Security (using the Snare agent)
- Windows Event Log Security (using SenSage Retriever)
- Netscreen Juniper Firewall
- Cisco IOS
- Check Point FW-1
- Cisco Pix

COMPLIANCE REGULATIONS SUPPORTED

The Compliance Analytics reports focus on compliance with the following sets of regulations:

- Sarbane's-Oxley (SOX) - via ISO 27002
- CobiT
- Health Insurance Portability and Accountability Act (HIPAA) & HITECH
- PCI 2.0
- DCID 6.3
- NISPOM
- FISMA

For a complete description of the Compliance Analytics reports, see “[Compliance Analytics Reports](#)”, on page 185.

McAfee Analytics Reports

The McAfee Analytics reports contain reports that display events from the following McAfee products:

- Email and Web Security (EWS)

- ePolicy Orchestrator (ePO)
- Network Security Platform (Intrushield)
- Vulnerability Manager (Foundstone)

For a complete description of the McAfee Analytics reports and descriptions of each, see “[McAfee Analytics Reports Package](#)”, on page 233.

LOG ADAPTERS

Log adapters parse raw event data from common information systems such as Microsoft Windows machines and Unix servers into discrete fields for storage in the Event Data Warehouse. Advanced Users can create new log adapters using the SenSage AP PTL file format.

For convenience, IgniteTech has pre-installed several of the most popular log adapters that parse log data from many common information systems and devices such as firewalls and routers. These adapters have been installed in accordance with IgniteTech-recommended best practices, and can serve as a reference for installing and configuring additional log adapters. The adapters are installed in a “disabled” state. Contact IgniteTech Professional Services to obtain additional log adapters specific to your data sources. New log adapters can be added at any time to your SenSage AP deployment.

For more information, see:

- [Appendix A: SenSage ConsolePTL File Format](#) in the *Collector Guide*.

Log Adapter Verification

The SenSage AP log adapter verification process provides assurance that the format of a log adapter and all related components meets SenSage AP log adapter guidelines and best practices. Verification also provides full, automated regression testing of all components of the log adapter to assure backwards compatibility of any updates. SenSage AP log adapters pass an extensive set of tests, including loading and parsing of specific message types, as well as a code review before they are labeled as “verified”.

IgniteTech Professional Services performs the Log Adapter Verification.

TOOLS FOR MANAGING AND USING SENSAge AP ANALYTICS

This section discusses tools you can use to manage and use SenSage AP Analytics. The following topics are discussed:

- [“Creating, Viewing, and Scheduling Reports”](#), on page 35
- [“Exporting and Importing Analytics Components”](#), on page 36

Creating, Viewing, and Scheduling Reports

Your SenSage AP installation includes an option to install a set of ready-to-run reports and dashboards that enable you to view event data from your information systems. You can run,

schedule, and edit these reports using the SenSage AP Analyzer. For more information, see the SenSage AP Analyzer documentation.

Exporting and Importing Analytics Components

Using the export and import features in the Analyzer, Advanced users can import and export the following items from a SenSage AP 6.x.x deployment to another SenSage AP 6.x.x deployment:

- Report definitions
- Analytics Workbench models

Creating Views and Modifying IntelliSchema

IntelliSchema is provided as part of your SenSage AP distribution and should not be modified. The views used to create IntelliSchema contain many interdependencies and changes to these views could have unintended effects.

IMPORTANT: IgniteTech recommends that you do not modify the IntelliSchema views.

You can, however, add new event sources to IntelliSchema. See [Chapter 5: Adding New Event Sources to IntelliSchema](#).

Advanced users familiar with SQL can, however, create custom views as needed. For more information, see Defining Views with SenSage AP SQL in Chapter 2, “SenSage Using the SenSage Event Data Warehouse (EDW)” in the *Event Data Warehouse Guide*.

CHAPTER 2

Configuring and Executing the Insider Threat Model Detection

This chapter describes how to use Analytics Workbench to configure and execute the Insider Threat Detection Model, known as the *IT Model*, and covers the following topics:

- “[IT Detection Model and the Analytics Workbench](#)”, [next](#)
- “[Overview: The Insider Threat Model Detection \(IT Model\)](#)”, [on page 37](#)
- “[User Requirements for Configuring the IT Model](#)”, [on page 38](#)
- “[How to Modify Configuration Parameters in Analytics Workbench](#)”, [on page 41](#)
- “[Configuring Changes for the Insider Threat Detection Model](#)”, [on page 44](#)
- “[External Inputs Schema and Watchlists, Whitelists, and Blacklists](#)”, [on page 49](#)
- “[Creating an Insider Threat Detection Dashboard](#)”, [on page 53](#)
- “[Drilling down to Log Events from Reports](#)”, [on page 55](#)
- “[Backfilling Data](#)”, [on page 59](#)
- “[Verifying the Model through a Regression Test](#)”, [on page 59](#)
- “[Monitoring Network Upload and Email Behavior](#)”, [on page 61](#)
- “[Executing the Insider Threat Model](#)”, [on page 66](#)
- “[Configuring and Executing the IT Model in a Hybrid Setup](#)”, [on page 66](#)

IT DETECTION MODEL AND THE ANALYTICS WORKBENCH

The *Analytics Workbench* is a component in SenSage AP that allows users to execute advanced analytics data processing on the log event data stored in the Event Data Warehouse or other databases. The Analytics Workbench has a drag and drop graphical programming functionality to provide advanced analytic processing capability.

A set of analytics processing components put together in the Analytics Workbench is called a model. Models may be created, saved, reused, or even scheduled to execute periodically. One of the capabilities delivered with SenSage AP is a model called the *Insider Threat Detection Model*, which is described in the following section.

OVERVIEW: THE INSIDER THREAT MODEL DETECTION (IT MODEL)

The IT Model uses log events and human resources information to compute a daily insider threat risk score and automatically identify users that have a high risk for malicious insider activity. It addresses malicious insider threat to an organization as defined by the Carnegie Mellon University Software Engineering Institute.

According to the Carnegie Mellon definition at http://www.cert.org/insider_threat/ (Carnegie Mellon University Software Engineering Institute - The Computer Emergency Response Team [CERT]Insider Threat Center):

"a current or former employee, contractor, or other business partner" is a threat because this person currently has or had authorized access to an *"organization's network, system, or data and has intentionally exceeded or misused that access in a manner negatively affecting the confidentiality, integrity, or availability of the organization's information or information systems."*

The IT Model uses data stored in the SenSage AP Event Data Warehouse to generate the risk score and other associated metrics for use by the organization to identify users that have high risk of insider threat behavior. The model uses email log events, upload log events, and user login events, all of which are common log events available in a SenSage AP installation.

The model leverages the SenSage AP event normalization layer called IntelliSchema so it has no need to count on the existence of specific networking devices on the network. The IntelliSchema master views that the IT Model uses are: mail, userlogin, and webproxy. The IT Model also expects to use human resources information as a component to risk-scoring. The expected data for human resources information is described in "[Human Resources Table Configuration](#)", on [page 46](#).

USER REQUIREMENTS FOR CONFIGURING THE IT MODEL

Before configuring the IT model, you must meet the requirements noted in this section.

Access and Privileges

Be sure you have:

- Access to the SenSage AP server with privilege to execute a setup command script that sets up the database for the IT Model.
- Ability to import the Insider Threat Detection Model using the SenSage AP Analytics Workbench, make configuration edits to the model and save them so you can complete the configuration modifications necessary for the operational use of the IT Model.
- Ability to import the Insider Threat Detection reports, create a dashboard using SenSage AP, and add pods to the dashboard so you can build an Insider Threat Dashboard.

DEPLOYMENT PACKAGE AND RECOMMENDED DATABASE CLIENT

The following files are needed for deployment of the Insider Threat Model:

- `itm_atpgsql.sql`

NOTE: If you are using the IT Model in a hybrid setup, see “[Configuring and Executing the IT Model in a Hybrid Setup](#)”, on page 66.

In addition, a software package to assist in viewing the database setup is extremely useful. This is not required for the IT Model but quite useful in viewing the database schemas and tables used by the IT Model. A recommended free software download package is **pgadmin**, which you can find at:

<http://www.pgadmin.org/> (recommended version is v1.18.1)

You may install pgadmin as a Windows or Mac client.

CREATING VIEWS/FUNCTION(S), SCHEMAS, AND DATABASE TABLES FOR THE IT MODEL

The IT model requires views and functions to handle the intermediate data generated by the model and historical trending analysis data. To set up these database items, the SQL file containing the execution code, is included in your installation. To execute this code follow the steps in “[Creating Schemas, Tables, Views, and Functions for the IT Model](#)”, on page 67.

After the command is executed, the database items described in the following sections are now installed on your system.

NOTE: You can use the pgadmin client software to view the database structure on the server’s controller database and verify the set up of the database items.

saw_simulated_data schema

This schema is used for regressions testing and verification that the model has been properly installed and is working. The following tables are included:

Table	Description
<code>hr_employee_status</code>	Contains simulated human resources data.
<code>it_saw_weights</code>	Contains the weighting values used in the model.
<code>mail</code>	Contains simulated email log events.
<code>mail_watchlist</code>	Contains a simulated email watchlist, which are used as potential insider threat indicators.
<code>mail_whitelist</code>	Contains a simulated email whitelist.
<code>upload_blacklist</code>	Contains a simulated upload blacklist.
<code>upload_whitelist</code>	Contains a simulated upload whitelist.
<code>hr_employee_status</code>	Contains simulated human resources data
<code>userlogin</code>	Contains simulated user login log events
<code>webproxy</code>	Contains simulated webproxy log events

aa_it_model_internals schema

This schema contains tables used internally by the model, functions used by the model, and views set up for Insider Threat visualization reports and drill down reports. The following are included:

Table, Function, or View contained in aa_it_model_internals	
f_dynaquery function	upload_indicators view
sample_avg_stddev function	userlogin view
windowavg function	webproxy view
all_attr_trends view	webproxy_tuples view
all_attributes_scores_all_days view	all_attributes_scores table
attr_scores_1_day view	email_leaf_scores table
attr_scores_90_day view	email_leaf_values table
attributes view	history_it_model_confs table
current_IT_model_confs view	history_model_timer table
data_users_attributes view	hr_leaf_scores table
email_indicators view	it_model_confs table
hr_information view	it_saw_weights table
it_constants view	login_leaf_scores table
it_last_effective_weights view	login_leaf_values table
last_score_date view	model_logs table
last_score_date_filter view	model_timer table
mail view	score_trends table
mail_tuples view	upload_leaf_scores table
top3_attr_z view	upload_leaf_values table

aa_it_model_external_inputs schema

This schema is used to contain tables used as inputs to the IT Model. The following tables are included:

Table	Description
mail_watchlist table	Contains the watchlist of email addresses; results in metrics used in email_indicators report (default table is blank)
mail_whitelist table	Contains the whitelist of email addresses (default table is blank)
upload_blacklist table	Contains blacklist domains and a magnitude associated with each; results in metrics used in upload indicators report. Note that the default table is populated with mostly file-sharing sites (relatively small magnitudes assigned to file-sharing sites and it also includes wikileaks.org, which has a large magnitude assigned to it)
upload_whitelist table	Contains whitelist upload domains (default table is blank)
upload_blacklist_latest view	Users of the IT Model may populate these tables as required, based on customer policies or other rules.

Table	Description
hr_employee_status	Placeholder sample table; contents to be replaced with customer data.

aa_it_model_baseline schema

This schema contains the expected results from execution of the auto-regression test. The following tables are included and each is tagged with the version of the IT Model.

Table Description	
all_attributes_scores_"version tag"	it_saw_weights_"version tag"
current_it_model_confs_"version tag"	login_leaf_scores_"version tag"
email_leaf_scores_"version tag"	login_leaf_values_"version tag"
email_leaf_values_"version tag"	score_trends_"version tag"
hr_leaf_scores_"version tag"	upload_leaf_scores_"version tag"
hr_leaf_values_"version tag"	upload_leaf_values_"version tag"

CHECK FOR POPULATED EVENTS DATA

It is recommended that you perform a check to ensure that the expected event data exists in the Event Data Warehouse (EDW) for the IT Model. You may do this simply by using pgadmin to view data in each IntelliSchema master view that is used by the IT Model. Default installations of SenSage AP have the **default_analytics_intellischema** as the IntelliSchema name.

- 1 Use pgadmin to navigate to the **default_analytics_intellischema-> views-> mail-> View Data-> View Top 100 Rows**.
- 2 Verify that mail event data exists in the resulting popup window.
- 3 Use pgadmin to navigate to the **default_analytics_intellischema-> views-> userlogin-> View Data-> View Top 100 Rows**.
- 4 Verify that userlogin event data exists in the resulting popup window.
- 5 Use pgadmin to navigate to the **default_analytics_intellischema-> views-> webproxy-> View Data-> View Top 100 Rows**.
- 6 Verify that webproxy event data exists in the resulting popup window.

For the IT Model to properly produce risk scores as designed, data must exist in these IntelliSchema master views. Note that 100 events should be returned for each IntelliSchema master view; if not, this is an indication that the event data is not fully-populated.

HOW TO MODIFY CONFIGURATION PARAMETERS IN ANALYTICS WORKBENCH

In summary, the Analytics Workbench in SenSage AP allows a user to graphically construct a model of analytic components and execute those components to process data from the Event Data Warehouse (EDW).

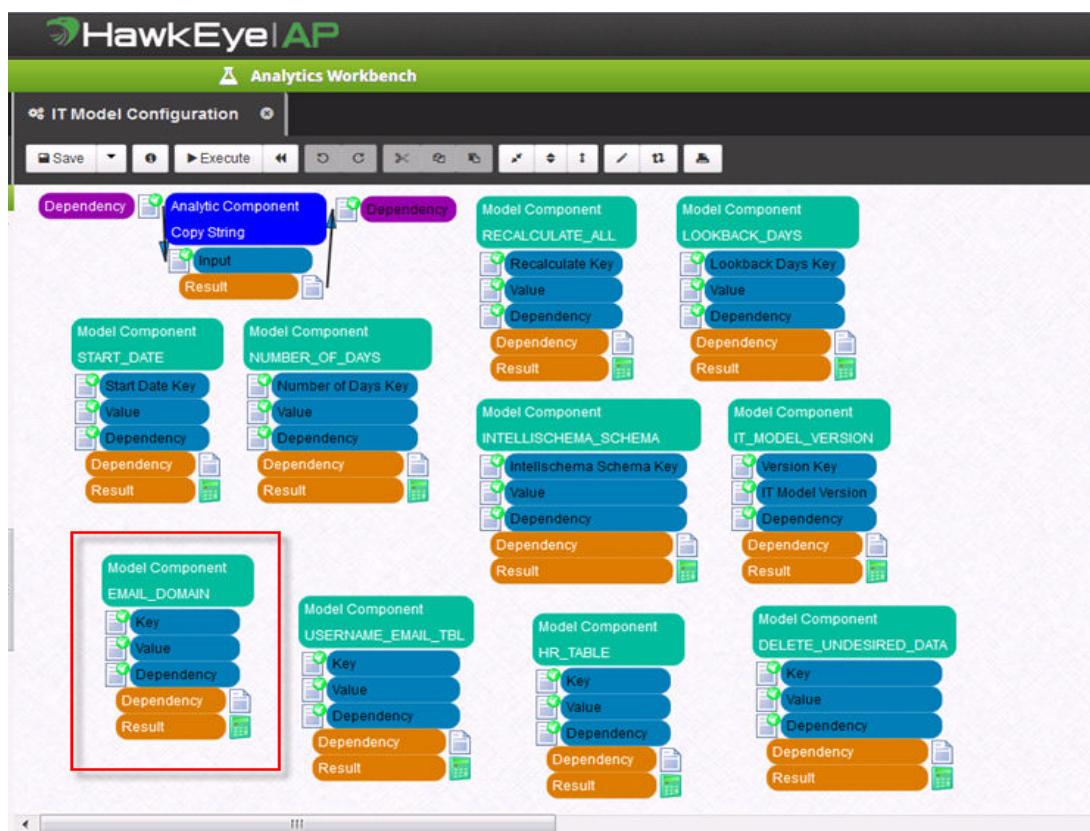
The IT Model is one such model, built using the Analytics Workbench, and consisting of multiple layers of models inside of other models (that is, multiple layers of embedded models). In addition, the IT Model and its embedded models contain several configuration parameters that are unique for an operational IT Model installation.

The component input parameter, described in the following section, is used for all of the configuration items in the IT Model and is displayed directly on the embedded model or analytic component on the canvas. The component input parameter is shown in the example of the "Email Domain" in [Figure 2-3](#).

Component Input Parameter

The *component input parameter* is shown in [Figure 2-1](#) with an example parameter setting for "Email Domain". This parameter is displayed directly on the embedded or analytic component.

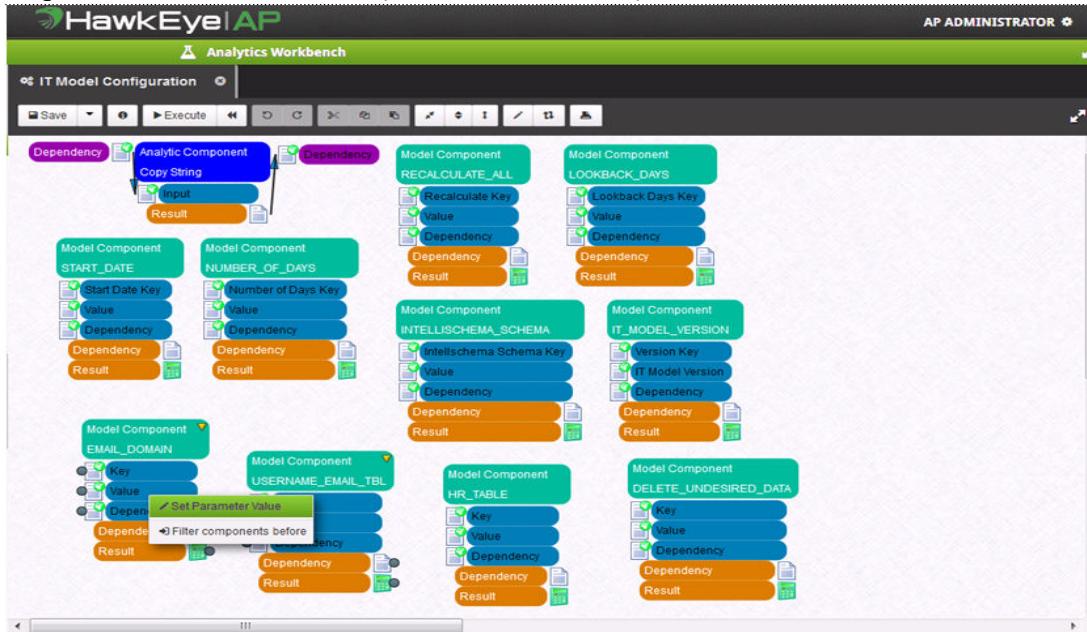
Figure 2-1: Component Input Parameter (Email Domain Example)



To modify the component input parameter:

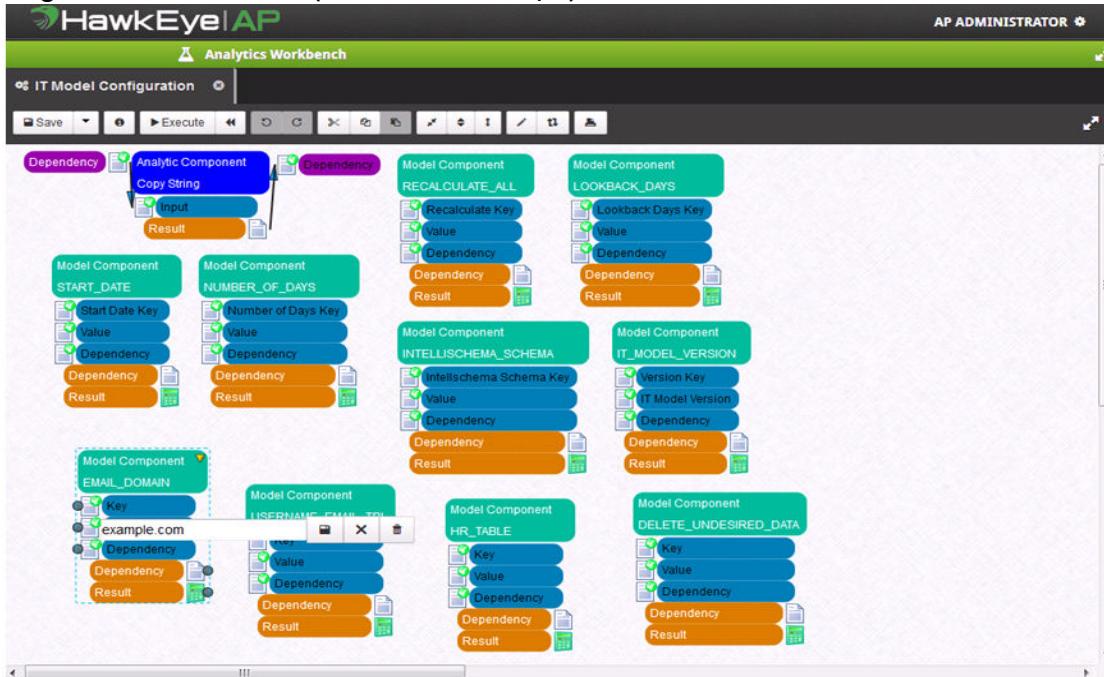
- 1 Right-click on the parameter (as shown in Figure 2-2) and select **Set Parameter Value**.

Figure 2-2: Set Parameter Value (Email Domain Example)



- 2 Edit the text field (as shown in Figure 2-3) and click the **Save** icon directly to the right of the text field.

Figure 2-3: Edit Text Field (Email Domain Example)



NOTE: When you have finished modifying the parameters for any model, click the **Save** button near the top of the model canvas to save your changes as part of that model.

CONFIGURING CHANGES FOR THE INSIDER THREAT DETECTION MODEL

For initial operation deployment of the IT Model, you are required to make some configuration changes to the IntelliSchema Name Configuration and the Email Configuration. Refer to the applicable sections below.

Note that for simplicity the majority of IT Model Configuration items are grouped under a single model for easier location and modification during the configuration process. The model is called Default IT Model Configuration screen and its configuration items are shown in Figure 2-4.

Figure 2-4Default IT Model Configuration



IntelliSchema Name Configuration

The IT Model leverages SenSage AP log event normalization, known as *IntelliSchema Master Views*. The specific database schema name for these IntelliSchema Master Views is configurable, as the name may differ in each deployed system.

To configure the IntelliSchema Name:

- 1 Using the Analytics Workbench, open the Default IT Model Configuration model.

The model parameter is a component input parameter type.

- 2 On the INTELLISchema_SCHEMA component, right click **Value**, **Set Parameter Value**, and edit the text field to contain the IntelliSchema name for the schema of the deployed system.

In addition, the model has the ability to execute using data from Postgres tables. A configuration item, called INTELLISCHEMA_EDW, exists in the model which when set to TRUE uses data from the EDW and when set to FALSE uses data stored in Postgres.

Configuration Summary - IntelliSchema Name

Model Name	Key/Parameter Name	Default Value	Description
Default IT Model Configuration	INTELLISCHEMA_SCHEMA	default_analytics_intellischema	IntelliSchema name used in the SenSage AP deployment
Default IT Model Configuration	INTELLISCHEMA_EDW	TRUE	Flag if the tables/views in the INTELLISCHEMA_SCHEMA refer to event data residing in the Event Data Warehouse

Email Name Configuration

Due to the use of email log events in the IT Model, you are required to configure the organization's email domain. In addition, you must configure an item to specify a database table that contains the mapping of the username to the email address. The IT Model expects this mapping table to contain columns named "username" and "email_address".

The email domain and username-to-email address mapping table configuration items are located in the Default IT Model Configuration model.

To configure the email domain and username-to-email address mapping:

- 1 Using the Analytics Workbench, open the Default IT model Configuration model.

These model parameters are component input parameter types.

- 2 On the EMAIL_DOMAIN component, right-click **Value, Set Parameter Value**, and edit the text field to contain the email domain (for example, hexiscyber.com) for the deployed system.
- 3 On the USERNAME_EMAIL_TBL component, right-click **Value, Set Parameter Value**, and edit the text field to contain the schema name and table name (in schemaName.tableName format) for the deployed system.

Configuration Summary - Email Domain

Model Name	Key/Parameter Name	Default Value	Description
Default IT Model Configuration	EMAIL_DOMAIN	hexiscyber.com	The email domain used by the organization; default based on simulated data
Default IT Model Configuration	USERNAME_EMAIL_TBL	aa_it_model_external_inputs.hr_employee_status	Database table name containing username to email address mapping

NOTE: It is recommended that the USERNAME_EMAIL_TBL table be stored in the aa_it_model_external_inputs schema, which is also the recommended location for the other external input tables in which the data source is not the Event Data Warehouse. For details, see “External Inputs Schema and Watchlists, Whitelists, and Blacklists”, on page 49.

Human Resources Table Configuration

The IT Model uses human resources data as a component in calculating the overall insider threat risk score. The IT model expects to access a Human Resources table containing a variety of flags for each individual in the organization, along with a numeric value representing the most recent performance evaluation for that individual. Figure 2-5 provides a sample of the expected table, using sample names as a part of a simulated data set.

Figure 2-5: Human Resources Table Format used by IT Model

	name	username	email_address	terminating_employment	hrViolation	securityViolation	contractor	performance
	text	text	text	text	text	text	text	text
1	Adam Adams	eadams	eadams@cetus.example.com	no	no	no	no	3
2	Adam Jones	ajones	ajones@cetus.example.com	no	no	no	no	5
3	Alex King	aking	aking@cetus.example.com	no	no	no	no	2
4	Albert Lee	alee	alee@cetus.example.com	no	no	no	no	3
5	Albert Parker	aparker	aparker@cetus.example.com	no	no	no	no	1
6	Albert Rodriguez	arodriguez	arodriguez@cetus.example.com	no	no	no	no	5
7	Anthony Smith	asmith	asmith@cetus.example.com	no	no	no	no	3
8	Christopher Carter	ccarter	ccarter@cetus.example.com	no	no	no	no	3
9	Charles Garcia	cgarcia	ext.cgarcia@cetus.example.com	yes	yes	yes	yes	3
10	Charles Hall	chall	chall@cetus.example.com	no	no	no	no	3
11	Cory Moore	cmore	cmore@cetus.example.com	no	no	no	no	4
12	Cory Robinson	crobinson	crobinson@cetus.example.com	no	no	no	no	1
13	Cory Thomas	cthomas	cthomas@cetus.example.com	no	no	no	no	3
14	Charles Thompson	cthompson	cthompson@cetus.example.com	no	no	no	no	5
15	Cory White	cwhite	cwhite@cetus.example.com	no	no	no	no	2

The IT model expects the flags to be a simple "yes" or "no". The following are the flag definitions:

- **terminating_employment** - User is leaving or has left the organization
- **hrViolation** - User has received a formal documented reprimand or violation
- **securityViolation** - User has a security violation on their record
- **contractor** - User is a contractor

In the case of the numeric value for the performance evaluation, the user has the ability to configure a numeric threshold for poor performance, as different organizations are expected to have a different scale for measuring employee performance. For instance, in the example HR data set, the numeric values ranged from **1-5**, where **5** was a very high performer and **1** was a low

performer. For that example data set, the performance metric threshold for low performance was set to **2**. So, the IT model would consider any individual to be a poor performer if their value was less than or equal to the threshold of **2**.

NOTE: Username and email_address mapping are not required to be in the HR table; this information (with the name configured) may reside in a different table as described in the “[Email Name Configuration](#)”, on page 45.

The IT Model configuration items represent the following:

- HR table name (to include the prepended schema name), which resides in the IT Model configuration model.
- Poor performance threshold, which resides in the Branch - Exfiltration model.

These model parameters are component input parameter types.

To configure the HR table name:

- 1 Using the Analytics Workbench, open the IT Model Configuration model.
- 2 On the HR-TABLE component, right-click **Value, Set Parameter Value**, and edit the text field to contain the human resources table name (to include the schema name prepended).

NOTE: It is recommended that the hr_employee_status table be stored in the aa_it_model_external_inputs schema, which is also the recommended location for other external input tables where the data's source does not from the Event Data Warehouse. For details, see “[External Inputs Schema and Watchlists, Whitelists, and Blacklists](#)”, on page 49

- 3 Open the Branch - HR component, right-click **HR Poor Perf Threshold, Set Parameter Value**, and edit the text field to contain the numeric poor performance threshold value for the deployed system.

Configuration Summary - HR Table

Model Name	Key/Parameter Name	Default value	Description
Default IT Model Configuration	HR_TABLE	aa_it_model_external_inputs.hr_employee_status	Human Resources table name (includes the schema name).
Branch - Exfiltration	HR Poor Perf Threshold (in the Branch - HR component)	2	Numeric value representing poor performance (inclusive); a value of 2 would consider all users with a 2 or less to be poor performers

Time Period Settings

The IT model can be configured to compute and store its internal data for a configurable period of time, with a default of 90 days and a programmable start date. In addition, for historical metrics trending calculations, the IT Model has a configurable sliding window time period setting with a default of 30 days.

The IT model also has the ability to recalculate the results for a programmable time period (in days); in some cases the model will have no need to perform recalculations as the data has already been processed and stored.

Finally, the IT Model has the ability to delete undesired data, that is, data outside of the time period defined by the start date and the number of days. It is recommended that you keep both of these settings at their default values. These settings are found in the Insider Threat Score Generator - Top Level model.

Configuration Summary - Time Period Settings

Model Name	Key/Parameter Name	Default Value	Description
Default IT Model Configuration	START_DATE	now	Start date for the IT Model processing; should be now for operations; default value may be set to a date based on a regression test setting
Default IT Model Configuration	NUMBER_OF_DAYS	90	Number of days of log event data processed
Default IT Model Configuration	LOOKBACK_DAYS	30	Number of days in sliding window for trending averages and statistics
Default IT Model Configuration	RECALCULATE_ALL	0	Number of days for recalculations
Default IT Model Configuration	DELETE_UNDESIRABLE_DATA	1	Flag for deletion of stored IT Model data outside of the time period defined by the start date and number of days parameters (1=Delete; 0=Does not Delete)
Default IT Model Configuration	BACKFILL_STEP_SIZE	1	This is the number of days that the model will execute incrementally in order to backfill the tables with the data needed by the model
Default IT Model Configuration	EXPECTED_RUN_TIME	4 hours	Maximum time period used in a pre-execution check for an already running instance of the IT Model. The model checks to see if a current instance is running and then checks to see if that instance is taking an excessive amount of time.
Default IT Model Configuration	TECHNICAL_SUPPORT	someone@this.org	Email address for individual responsible for IT Model configuration; notified when the model is attempting execution and there is a prior model running that exceeded its maximum expected run time

EXTERNAL INPUTS SCHEMA AND WATCHLISTS, WHITELISTS, AND BLACKLISTS

You can configure the IT Model to use an email watchlist, email whitelist, upload blacklist, and upload whitelist. The model accesses this data from tables stored in Postgres (which gets set up by the SQL script described in “[Creating Views/Function\(s\), Schemas, and Database Tables for the IT Model](#)”, on page 39. The schema name, which contains these input tables, is a configuration item and is called EXTERNAL_INPUTS_SCHEMA.

Configuration Summary - External Inputs Schema

Model Name	Key/Parameter Name	Default value	Description
Default IT Model Configuration	EXTERNAL_TABLE_SCHEMA	aa_it_model_external_inputs	Schema name for external input tables used by the IT Model

NOTE: It is recommended that the hr_employee_status table be stored in schema.

See the tables in the saw_simulated_data schema for examples of correctly formatted mail_watchlist table, mail_watchlist table, mail_whitelist table, upload_blacklist table, and upload_whitelist table.

NOTE: This can be accomplished using pgadmin (database viewing client software mentioned above) and specifying, for example, **saw_simulated_data schema-> upload_blacklist-> View Data-> View all rows**.

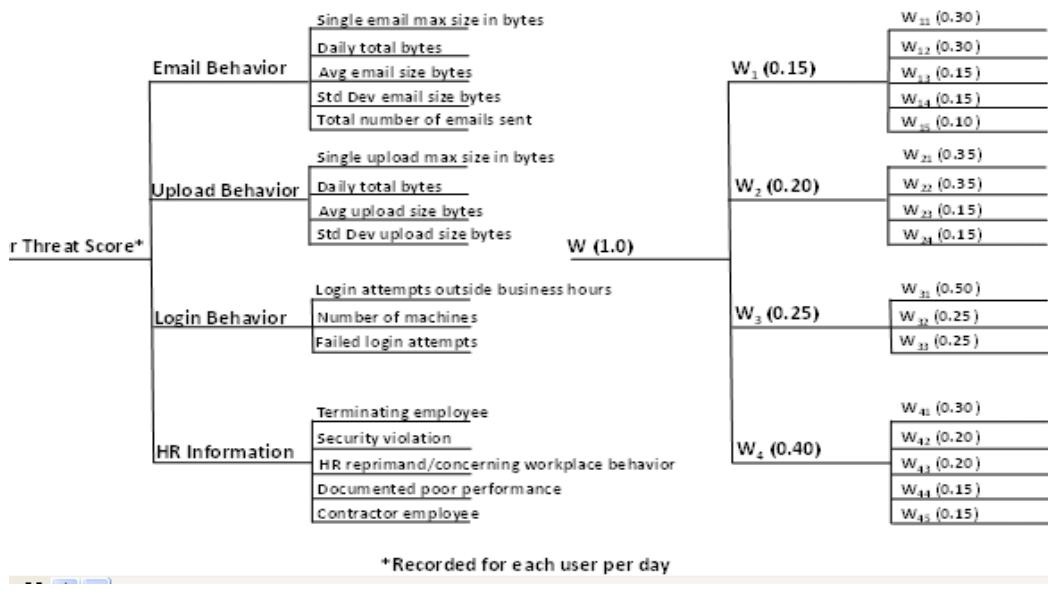
MODIFYING THE WEIGHTING USED IN THE IT MODEL (FOR ADVANCED USERS)

As previously noted, the IT Model uses log events to compute a daily insider threat risk score. The IT Model calculates this score based on weighted metrics gathered from the log events stored in the Event Data Warehouse and also from metrics based on Human Resources information. You may modify the weighting setting as a way to increase or decrease the importance of a particular metric. The IT Model comes configured with default settings for each of the weighting values used in the model.

Modifications to weighting values are recommended for advanced users only, as it has a direct impact on the risk scores calculated by the model.

The IT Model may be represented by a tree structure as shown in [Figure 2-6](#), which also captures an example set of weighting values (tree on the right). Note that the sum of the weights in each branch is 1.0 and the sum of the weights for all of the branches is 1.0.

A higher weighting value means that metric is of higher importance when compared to the other metrics at the same hierarchy level in the tree structure. For example, "single email max size in bytes," with a weight of 0.30, is considered to be of more importance than "Total number of emails sent," with a weight of 0.10.

Figure 2-6: IT Model Tree Structure

The weights may be modified (advanced user only) in the models using the SenSage AP Analytics Workbench. In addition, the models have the ability to automatically assist you in producing weighting values used inside the model that add up to 1.0.

For instance, in the Email Behavior Branch shown above, the user may enter the values 30, 30, 15, 15, 10 as the weighting parameters and the processing inside the model will normalize those values and convert them to decimal weights that sum to 1.0. As another example, 90, 90, 45, 45, 30 is a valid set of advanced user input weights that result in weights used by the IT model of 0.30, 0.30, 0.15, 0.15, 0.10.

Configuration Summary: Model = Branch - Exfiltration

Parameter Name	Model Name	Component Name	Parameter Type	Description	Default value
Attribute Weight	Branch - Exfiltration	Branch - Email	Component Input	Email branch weighting value	0.15
Attribute Weight	Branch - Exfiltration	Branch - Upload	Component Input	Upload branch weighting value	0.20
Attribute Weight	Branch - Exfiltration	Branch - Login	Component Input	Login branch weighting value	0.25
Attribute Weight	Branch - Exfiltration	Branch - HR	Component Input	HR branch weighting value	0.40

Configuration Summary: Model = Scores - Email Leaf Nodes

Parameter Name	Model Name	Component Name	Parameter Type	Description	Default value
Attribute Weight	Scores - Email Leaf Nodes	Create IT Tree Leaf; Attribute Number = 1	Component Input	Single Email Max Size (bytes)	0.30
Attribute Weight	Scores - Email Leaf Nodes	Create IT Tree Leaf; Attribute Number = 2	Component Input	Daily Total Email Size (bytes)	0.30
Attribute Weight	Scores - Email Leaf Nodes	Create IT Tree Leaf; Attribute = 3	Component Input	Avg Email Size (bytes)	0.15
Attribute Weight	Scores - Email Leaf Nodes	Create IT Tree Leaf; Attribute = 4	Component Input	Std Dev of Email Size (bytes)	0.15
Attribute Weight	Scores - Email Leaf Nodes	Create IT Tree Leaf; Attribute = 5	Component Input	Total Number of Emails Sent	0.10

Configuration Summary: Model = Scores - Upload Leaf Nodes

Parameter Name	Model Name	Component Name	Parameter Type	Description	Default value
Attribute Weight	Scores - Upload Leaf Nodes	Create IT Tree Leaf; Attribute Number = 1	Component Input	Single Upload Max Size (bytes)	0.35
Attribute Weight	Scores - Upload Leaf Nodes	Create IT Tree Leaf; Attribute Number = 2	Component Input	Daily Total Upload Size (bytes)	0.35
Attribute Weight	Scores - Upload Leaf Nodes	Create IT Tree Leaf; Attribute = 3	Component Input	Avg Upload Size (bytes)	0.15
Attribute Weight	Scores - Upload Leaf Nodes	Create IT Tree Leaf; Attribute = 4	Component Input	Std Dev of Upload Size (bytes)	0.15

Configuration Summary: Model = Scores - Login Leaf Nodes

Parameter Name	Model Name	Component Name	Parameter Type	Description	Default value
Attribute Weight	Scores - Login Leaf Nodes	Create IT Tree Leaf; Attribute Number = 1	Component Input	Number of Login Attempts Outside of Business Hours	0.50
Attribute Weight	Scores - Login Leaf Nodes	Create IT Tree Leaf; Attribute Number = 2	Component Input	Number of Machine Login Attempts	0.25

Parameter Name	Model Name	Component Name	Parameter Type	Description	Default value
Attribute Weight	Scores - Login Leaf Nodes	Create IT Tree Leaf; Attribute = 3	Component Input	Number of Failed Login Attempts	0.25

Configuration Summary: Model = Scores - HR Leaf Nodes

Parameter Name	Model Name	Component Name	Parameter Type	Description	Default value
Attribute Weight	Scores - HR Leaf Nodes	Create IT Tree Leaf; Attribute Number = 1	Component Input	Terminating Employee	0.30
Attribute Weight	Scores - HR Leaf Nodes	Create IT Tree Leaf; Attribute Number = 2	Component Input	Security Violation	0.20
Attribute Weight	Scores - HR Leaf Nodes	Create IT Tree Leaf; Attribute = 3	Component Input	HR Reprimand/ Concerning Workplace Behavior	0.20
Attribute Weight	Scores - HR Leaf Nodes	Create IT Tree Leaf; Attribute = 4	Component Input	Documented Poor Performance	0.15
Attribute Weight	Scores - HR Leaf Nodes	Create IT Tree Leaf; Attribute = 5	Component Input	Contractor Employee	0.15

CREATING AN INSIDER THREAT DETECTION DASHBOARD

Insider Threat reports are included with SenSage AP as shown in [Figure 2-7](#). You may use these reports to create an Insider Threat dashboard in SenSage AP.

Figure 2-7: Insider Threat Reports

Report name	Last updated
All Attributes Scores Details - Weighted Z	2014-Sep-30 11:13 AM
All Attributes Scores Details - Weighted z	2014-Sep-29 11:04 PM
Current Insider Threat Model Configurations	2014-Sep-29 03:29 PM
Insider Threat Score Summary - Ranked by Weighted Z	2014-Oct-14 10:28 AM
IT Email Events	2014-Sep-23 12:31 PM
IT HR Information	2014-Sep-23 12:37 PM
IT Login Events	2014-Sep-23 12:30 PM
IT Model Configuration	2014-Oct-03 05:56 PM
IT Upload Events	2014-Sep-23 12:35 PM
Report Chart Test	2014-Oct-14 05:05 PM
Top 3 Ranked Users - IT Score Trend	2014-Oct-14 03:14 PM
Top 3 Ranked Users - Weighted Z Score Trend	2014-Oct-14 04:59 PM
Top 3 Ranked Users - Zp Score Trend	2014-Sep-05 01:20 PM
Top 3 Ranked Users - Zu Score Trend	2014-Sep-05 01:22 PM

[Figure 2-8](#) provides a recommended dashboard that contains an Insider Threat Scoring Summary, with users ranked by a metric called the risk score (report name is ITD: Score (Prod) Summary - Top 100). [Figure 2-8](#) also contains two other insider threat indicator reports, ITD: Upload Branch Indicators - Top 10 and ITD: Email Branch Indicators - Top 10 to provide some further information on insider threat risk, based on statistical measures of data computed by the Insider ThreatModel.

The next recommended reports for the dashboard are each trend plots, recommended to be stacked in this priority order in the dashboard (and shown in [Figure 2-9](#)). The chart report names are ITD: Score (Prod) Trend - Top 3, ITD: Score (Raw) Trend - Top 3, and ITD: Score (Weighted Z) Trend - Top 3, respectively.

NOTE: You can toggle the grid display for each trend report pod and stretch each trend report pod across the dashboard as shown below.

Figure 2-8: Insider Threat Dashboard (Top Portion)



Figure 2-9: Insider Threat Dashboard (Bottom Portion)



This Insider Threat dashboard shows a table of ranked users based on Insider Threat risk (highest risk users are at the top of the list). The charts show the insider threat risk due to upload indicators, email indicators, and shows the risk of scores over time, the IT scores over time, and

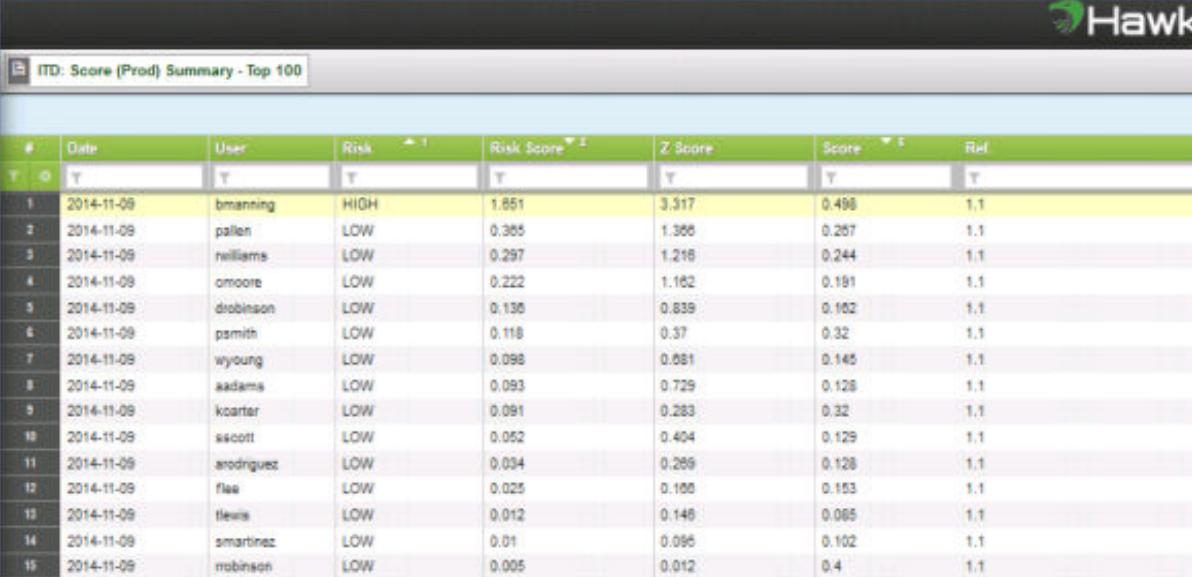
the weighted average of the Z scores over time. Note the Z score is a measure of how far the behavior is away from a sliding window thirty day average.

DRILLING DOWN TO LOG EVENTS FROM REPORTS

In operation, it is necessary to observe the events which cause high risk detections or high risk upload or email indicators. This is done through the use of associated reports. The insider threat reports come with the proper associations already in place so the drill down effort is simple.

- 1 To drill down from the Insider Threat Score Summary (Top 100)
 - a Click tab on the right-hand side of the dashboard report pod to view the original report.
 - b Click on the row for the user of interest (in the example below, **bmanning** is selected.)

Figure 2-10: Insider Threat Score Summary Report



#	Date	User	Risk	Risk Score	Z-Score	Score	Ref
1	2014-11-09	bmanning	HIGH	1.651	3.917	0.498	1.1
2	2014-11-09	pallen	LOW	0.365	1.366	0.267	1.1
3	2014-11-09	williams	LOW	0.297	1.218	0.244	1.1
4	2014-11-09	omroore	LOW	0.222	1.162	0.191	1.1
5	2014-11-09	drabinson	LOW	0.138	0.839	0.162	1.1
6	2014-11-09	psmith	LOW	0.118	0.37	0.32	1.1
7	2014-11-09	wyoung	LOW	0.098	0.681	0.145	1.1
8	2014-11-09	adams	LOW	0.093	0.729	0.128	1.1
9	2014-11-09	kroarter	LOW	0.091	0.283	0.32	1.1
10	2014-11-09	sscott	LOW	0.052	0.404	0.129	1.1
11	2014-11-09	ardriguez	LOW	0.034	0.266	0.128	1.1
12	2014-11-09	flea	LOW	0.025	0.166	0.153	1.1
13	2014-11-09	tlewis	LOW	0.012	0.146	0.065	1.1
14	2014-11-09	smartinez	LOW	0.01	0.066	0.102	1.1
15	2014-11-09	robinson	LOW	0.005	0.012	0.4	1.1

- c Click the associated report button, upper right, under **AP ADMINISTRATOR**.
- d Go to the left dropdown list of report names and select **Score Breakdown All Levels** and click the > button to execute the report.

The result is the attribute score breakdown.

Figure 2-11: All Attributes Scores Report (Drill Down)

#	attribute_id	attribute_description	username	event_id	score_percent	attribute_weight_pct	effective_score	attr_min_score	event_weight_p	total_user_p	total_user_avg	total_user_std	total_group_p	total_group_avg	total_group_std	attribute_id	score_percent
1	1	1	1	1	100.00%	0.400	0.400	0.337	0.54750	0.00000	0.00000	0.29404	0.11000	0.16328	-0.1	2014-11-09	
2	1.1	Issue Create Rate	bmannning	4031	1.000	100.00%	0.400	0.400	0.337	0.38170	0.00000	0.00000	0.20001	0.11000	0.16328	1	2014-11-09
3	1.1.1	Issue Resolution	bmannning	4031	0	100.00%	0	0	0.395	0	0	0	0.17954	0.21207	1.1		2014-11-09
4	1.1.1.1	Single Email User B	bmannning	4031	0	4.00%	0	0	0.377	0	0	0	0.09469	0.10000	0.27149	1.1	2014-11-09
5	1.1.1.2	Daily Total Email B	bmannning	4031	0	4.00%	0	0	0.343	0	0	0	0.02030	0.02042	0.23808	1.1	2014-11-09
6	1.1.1.3	Avg Email Size B	bmannning	4031	0	1.25%	0	0	0.205	0	0	0	-0.04050	0.21952	0.30359	1.1	2014-11-09
7	1.1.1.4	Std Dev of Email B	bmannning	4031	0	2.25%	0	0	0.219	0	0	0	0.09067	0.09090	0.28074	1.1	2014-11-09
8	1.1.1.5	Total Number of Bms	bmannning	4031	0	1.00%	0	0	0.231	0	0	0	-0.00003	0.00000	0.22386	1.1	2014-11-09
9	1.1.2	Upload Behavior	bmannning	2796	30.00%	0.19	0.369	0.391	0.25009	0.19200	0.04000	0.10000	0.11956	0.20747	1.1		2014-11-09
10	1.1.2.1	Single Upload Max	bmannning	4031	2746	7.00%	0.07	1	0.181	0.12110	0.20000	0.43024	0.12024	0.16444	0.21003	1.2	2014-11-09
11	1.1.2.2	Daily Total Uploads	bmannning	4031	2.00	7.00%	0.08	0.081	0.081	0.12020	0.08002	0.28021	0.11798	0.12005	0.16418	1.2	2014-11-09
12	1.1.2.3	Avg Upload Size B	bmannning	4031	2.00	1.00%	0.05	1	0.068	0.02151	0.20000	0.42024	0.11779	0.11956	0.20792	1.2	2014-11-09
13	1.1.2.4	Std Dev of Upload	bmannning	4031	2.00	3.00%	0.05	1	0.049	0.00007	0.16000	0.35231	0.06002	0.11786	0.21007	1.2	2014-11-09
14	1.1.2.5	Large Behavior	bmannning	4031	2718	20.00%	0.188	0.178	0.120	0.10219	0.14000	0.18001	0.45007	0.12046	0.16271	1.3	2014-11-09
15	1.1.3	Number of Logon At...	bmannning	4031	4.000	<0.00%	0.159	1	0.068	0.04219	0.30000	0.24021	0.69174	0.12000	0.14702	1.3	2014-11-09
16	1.1.3.2	Number of Actions	bmannning	4031	1.000	4.00%	0.363	1	0.074	0.00012	0.30000	0.36198	0.11768	0.31008	0.37144	1.3	2014-11-09
17	1.1.3.3	Number of Failed L...	bmannning	4031	0	0.20%	0	0	-0.103	0	0	0	-0.40307	0.18079	0.32077	1.3	2014-11-09
18	1.1.4	Off Computer	bmannning	4031	0.100	40.00%	0.12	0.3	0.099	0	0.5	0	0.9007	0.11103	0.1		2014-11-09
19	1.1.4.5	Suspicious Employee	bmannning	4031	1.000	10.00%	0.12	1	0.010	0	1	0	0.86010	0.87986	0.38163	1.4	2014-11-09
20	1.1.4.6	Boundary Violation	bmannning	4031	0	0.00%	0	0	-0.024	0	0	0	-0.20002	0.02002	0.22130	1.4	2014-11-09
21	1.1.4.7	Off Application Con...	bmannning	4031	0	0.00%	0	0	-0.072	0	0	0	-0.10000	0.05079	0.17400	1.4	2014-11-09
22	1.1.4.8	Documented File P...	bmannning	4031	0	0.00%	0	0	-0.127	0	0	0	0.00000	0.0	0.00001	1.4	2014-11-09
23	1.1.4.9	Corporate Employee	bmannning	4031	0	0.00%	0	0	-0.170	0	0	0	0.20100	0.21799	0.30181	1.4	2014-11-09

e Click the row for the attribute for drill down (for example, **Upload Behavior**).

f Click the associated report button, upper right, under AP ADMINISTRATOR.

g Go to the left dropdown list of report names and select **Upload Events** and click the > button to execute the report.

The result will be the upload events report for that user for that day.

Figure 2-12: Upload Events Drill Down

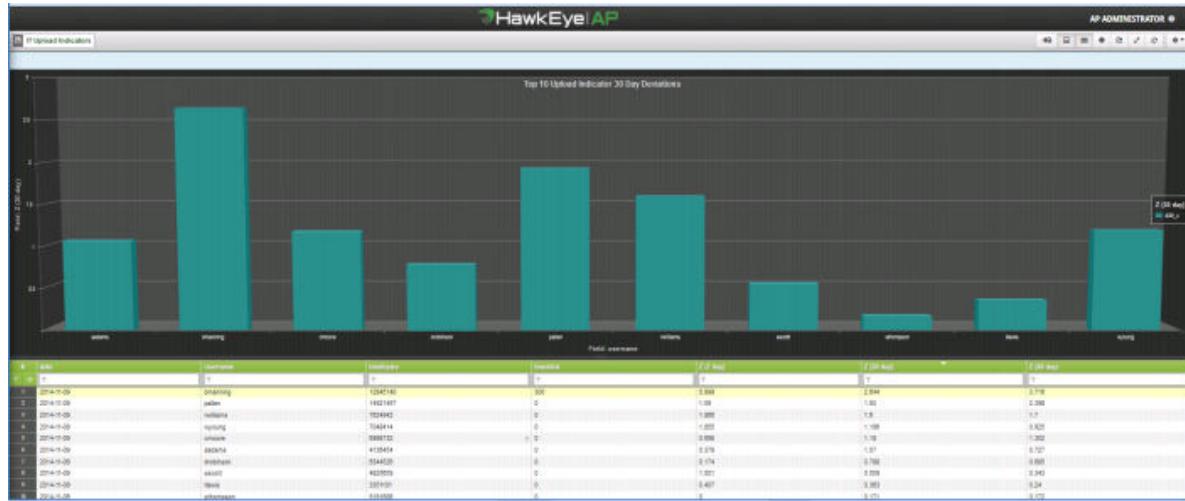
#	ts	src_ipdomain	src_info_sys	cs_bytes	dest_info_sys	event_description	ts_date_ref
1	2014-Nov-09 06:34:21 AM	bmannning	PC-8431	4240677	wikileaks.org	http://wikileaks.org/Juli...	2014-11-09
2	2014-Nov-09 06:43:48 AM	bmannning	PC-8431	3903082	wikileaks.org	http://wikileaks.org/Juli...	2014-11-09
3	2014-Nov-09 06:48:51 AM	bmannning	PC-8431	4701381	wikileaks.org	http://wikileaks.org/Juli...	2014-11-09

h Execute similar steps for Email Events drill down, Login Events drill down, and HR Information drill down.

2 To drill down from Upload Indicators:

- a Click tab on the right-hand side of the dashboard report pod to view the original report.
- b Click on the row for the user of interest.

Figure 2-13: Upload Indicators Report



- c Click the associated report button, upper right, under **AP ADMINISTRATOR**.
- d Go to the left dropdown list of report names and select **Upload Events** and click the > button to execute the report.

The result is the upload events report for that user for that day.

Figure 2-14: Upload Events Drill Down

The table lists three events for user bmanning on 2014-Nov-09. Each event includes details like source account, destination system, bytes transferred, and a link to the event description.

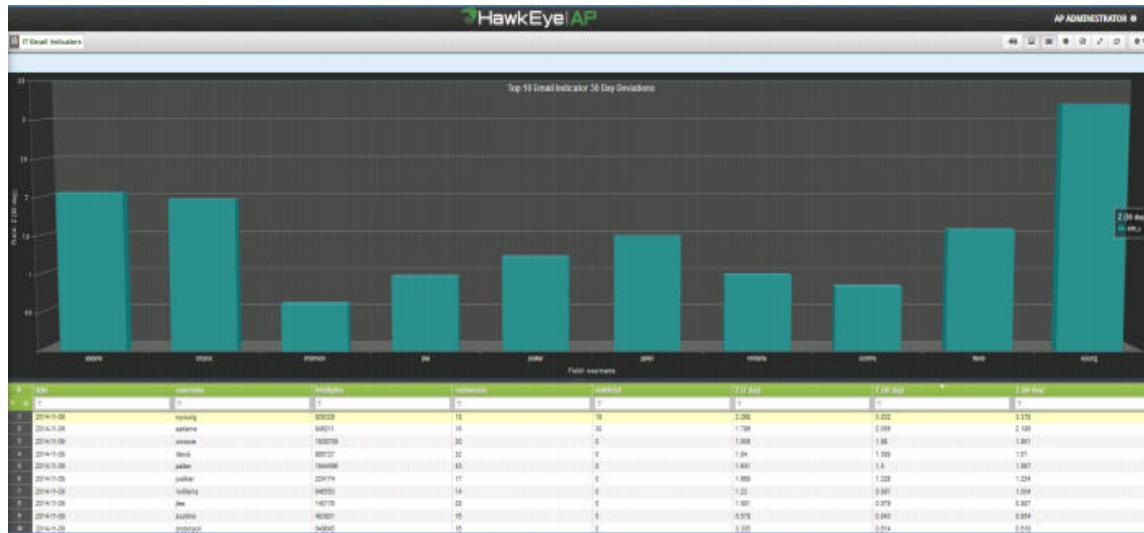
#	ts	sre_account	sre_info_syst	cs_bytes	dest_info_syst	event_description	ts_date_ref
1	2014-Nov-09 06:34:21 AM	bmanning	PC-8431	4240577	wikileaks.org	http://wikileaks.org/Jull...	2014-11-09
2	2014-Nov-09 06:43:48 AM	bmanning	PC-8431	3903082	wikileaks.org	http://wikileaks.org/Jull...	2014-11-09
3	2014-Nov-09 06:48:51 AM	bmanning	PC-8431	4701381	wikileaks.org	http://wikileaks.org/Jull...	2014-11-09

- e Click the row for the attribute for drill down (for example, **Upload Behavior**).
- f Click the associated report button, upper right, under AP ADMINISTRATOR.
- g Go to the left dropdown list of report names and select **Upload Events** and click the > button to execute the report.

3 To drill down from Email Indicators:

- Click tab on the right-hand side of the dashboard report pod to view the original report.
- Click on the row for the user of interest.

Figure 2-15: Email Indicators Report



- Click the associated report button, upper right, under AP ADMINISTRATOR.
- Go to the left dropdown list of report names and select **Email Events** and click the > button to execute the report.

The result is the email events report for that user for that day.

Figure 2-16: Email Events Drill Down

The figure shows a table titled "IT Email Events-v3" with columns: #, ts, username, src_account, dst_account, total_bytes, and ts_date_ref. The table lists 18 rows of email events for user wyoung on November 9, 2014. The data is identical to the table in Figure 2-15.

#	ts	username	src_account	dst_account	total_bytes	ts_date_ref
1	2014-Nov-09 03:37:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	42079	2014-11-09
2	2014-Nov-09 03:36:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	42158	2014-11-09
3	2014-Nov-09 03:34:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	42232	2014-11-09
4	2014-Nov-09 03:33:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	42314	2014-11-09
5	2014-Nov-09 03:32:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	42380	2014-11-09
6	2014-Nov-09 03:25:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	42029	2014-11-09
7	2014-Nov-09 03:24:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	42288	2014-11-09
8	2014-Nov-09 03:23:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	42484	2014-11-09
9	2014-Nov-09 03:22:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	84593	2014-11-09
10	2014-Nov-09 03:21:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	41713	2014-11-09
11	2014-Nov-09 03:20:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	41738	2014-11-09
12	2014-Nov-09 03:18:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	41770	2014-11-09
13	2014-Nov-09 03:17:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	83960	2014-11-09
14	2014-Nov-09 03:16:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	42484	2014-11-09
15	2014-Nov-09 03:13:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	42368	2014-11-09
16	2014-Nov-09 03:12:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	126591	2014-11-09
17	2014-Nov-09 03:10:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	42580	2014-11-09
18	2014-Nov-09 03:09:00 AM	wyoung	wyoung@ctetus.example.com	gregory.roberts@musca.example.com	42559	2014-11-09

- Click the row for the attribute for drill down (for example, **Upload Behavior**).
- Click the associated report button, upper right, under AP ADMINISTRATOR.

- g Go to the left dropdown list of report names and select **Upload Events** and click the > button to execute the report.

BACKFILLING DATA

In operation, the Insider Threat Model executes on a daily basis, generating data from the previous day's network activity. However, the model relies on historical data to generate the risk score information and the other insider threat risk indicators.

This historical data is saved in tables in Postgres. Upon first installation of the model, the historical data does not yet exist. In order to support that initial installation, the model comes configured to automatically backfill the missing data using an iteration mechanism. There is no need for the user to modify the configuration as the model will automatically detect missing data and make the necessary calculations and populate the Postgres tables used by the model.

Backfilling is complete when the model finishes execution. Additionally, you may query the IT Model Postgres tables to see the progress of the model's execution. For example, if the model is supposed to backfill through 2014-11-09, use this simple SQL query via pgadmin to determine how much data has been processed:

```
select max(score_date) from aa_it_model_internals.score_trends
```

When completed, the query returns **2014-11-09**.

VERIFYING THE MODEL THROUGH A REGRESSION TEST

The model includes an automated regression test model that you can use to verify all pieces are properly set up for the model. The regression test model:

- Runs a known set of input data.
- Generates the insider threat metrics for 90 days.
- Automatically, compares the results to a set of expected results.

The following steps execute the regression test:

NOTE: The regression test automatically verifies the backfill of historical data noted above.

- 1 Log in to SenSage AP.
- 2 Navigate to the Analytics Workbench.
- 3 Open the model named Auto Regression Test - IT Model (in the InsiderThreatScoringTesting category).
- 4 Execute the model.

Patience is required as it initially does not seem like the model is running. After a short wait (less than a minute), the model will start executing and you will see gears turning on the model components of the Analytics Workbench canvas. The model will take a few minutes to execute. During this time it is generating 90-days of Insider Threat data using the provided simulated event and HR data. When generation is completed, the model automatically compares the

resulting data to the expected results. When finished, the SenSage AP completion window is displayed.

- 5** The Auto Regression model also back fills data as described above; to observe how far the model is in execution, perform a simple query using pgadmin.

For example, if the regression test mode is supposed to back fill through **2014-11-09**, the user can use this simple SQL query via pgadmin to determine how much data has been processed. When completed, the query returns **2014-11-09**.

- 6** To verify that the model is actually running, you may observe the scrolling of the model's logs:

- a** Log into the server in a Linux window and issue the following command:

```
tail -F /opt/tomcat/logs/catalina.out
```

In the Linux window, you can observe the continuous streaming of log messages, a simple verification that the model is running.

- b** You may also check if the "values" or "scores" tables are being populated; to do this, use pgadmin and navigate to any of the branch values tables in the aa_it_model_internals schema.

For example, **email_leaf_values-> View Data-> View Top 100 Rows or View All Rows**. The data should exist for the users of interest.

- 7** To verify the model is installed properly, go to the results window and check that the value for the Delta Count output parameter=**0** (which indicates proper installation).

NOTE: The Auto Regression test uses an override mechanism for the configuration items needed to properly set up the regression test.

- 8** If the dashboard has not already been set up, refer to "[Creating an Insider Threat Detection Dashboard](#)", on page 53.

- 9** To verify that the dashboard has been populated by the regression test results, check all of the report pods on the dashboard to ensure they are populated with data.

- 10** After this verification is completed, use pgadmin to delete the regression test output tables stored in the aa_it_model_internals schema; this task is recommended to clear the slate for the Insider Threat Model actual IntelliSchema events. The following table lists the tables you need to delete to clear out the slate for the deployed IT Model (aa_it_model_internals schema):

Tables for Deletion	
all_attributes_scores	it_saw_weights
email_leaf_scores	login_leaf_scores
email_leaf_values	login_leaf_values
history_it_model_confs	model_logs
history_it_model_timer	model_timer
hr_leaf_scores	score_trends
hr_leaf_values	upload_leaf_scores
it_model_confs	upload_leaf_values

MONITORING NETWORK UPLOAD AND EMAIL BEHAVIOR

The IT Model has the ability to monitor network upload and email behavior reports based on a set of inputs containing the following information:

- An upload blacklist
- An upload whitelist
- An email watchlist
- An email whitelist

These domains and email addresses are used by the IT Model for handling queries and for generating metrics used in the upload and email indicators reports (mentioned above) and are based on the webproxy event upload hits on the blacklist and the mail event hits on the watchlist.

You may add to the lists (for upload and email indicator purposes) through upload events report or the email events report, or through models. For more details, see the sections below.

As mentioned above, the Insider Threat Detection Model is capable of using specific feedback to control scoring and indicators. In order to reduce false positives and identify user behavior of interest, several external inputs list are used as noted below.

Upload Blacklist Behavior

The Upload Blacklist is used to identify user upload behavior of interest. Your uploads to a blacklist site will trigger a specific user for display as high-risk in the Upload Indicators Report/dashboard pod based on the magnitude of the upload site.

There are two parts to a Blacklist entry:

- Domain (Upload Site) - The domain should be the least common string to identify a specific domain. For example, use **dropbox.com** to match on **www.dropbox.com** as well as **upload.dropbox.com**.
- Magnitude - The magnitude specifies the risk associated with a particular domain. For example, 10 = low risk and 100 = high risk.

Upload Whitelist Behavior

The Upload Whitelist is used to reduce false positives by removing the risk associated with specific user uploads. User uploads to a Whitelist site are ignored in risk score calculations, treating the activity as an internal event. Use the Whitelist to identify common upload sites approved for company use.

There are two parts to a Whitelist entry:

- Domain (Upload Site) - The domain should be the least common string to identify a specific domain. For example, use **dropbox.com** to match on **www.dropbox.com** as well as **upload.dropbox.com**.
- User - Whitelist domains can be applicable to all users or individual users. For example, if only a handful of people are approved to upload documents to **dropbox.com**, then you are only

required to add them to the Whitelist. Uploads to **dropbox.com** for all other users will continue to be scored as an exfiltration risk. To specify that a Whitelist entry should apply to all users, a single dash (-) should be used as the User value.

Email Watchlist

The Email Watchlist is used to identify user email behavior of interest. User emails to a Watchlist Recipient/Domain will likely trigger that user for display as a high risk in the Email Indicators report/dashboard pod.

There are two parts to an Email Watchlist entry:

- To Address (Recipient/Domain) - The Recipient/Domain can specify a single recipient email address (i.e., **user@domain.com**) or an email domain (i.e., **domain.com**). If a domain is specified, the domain should be the least common string to identify a specific domain.
- From Address (Sender) - Watchlist entries can be applicable to all users or individual users. For example, if a user is suspected of emailing attachments to his or her personal email address, a Watchlist entry should be created for that specific sender. However, if all emails sent to a specific Receiver/Domain is of interest, then single dash (-) should be used as the Sender value.

Email Whitelist

The Email Whitelist is used to reduce false positives by removing the risk associated with specific user emails. In risk score calculations, user emails to a Whitelist Recipient/Domain are ignored, as the activity is treated as an internal event. Use the Whitelist to identify common email recipients/domains which have no associated risk.

There are two parts to an Email Whitelist entry:

- To Address (Recipient/Domain) - The Recipient/Domain can specify a single recipient email address (i.e., **user@domain.com**) or an email domain (i.e., **domain.com**). If a domain is specified, the domain should be the least common string to identify a specific domain.
- From Address (Sender) - Whitelist entries can apply to all users or individual users. For example, if a user is suspected of emailing attachments to his or her personal email address, a Whitelist entry should be created for that specific sender. However, if all emails sent to a specific Receiver/Domain is of interest, then single dash (-) should be used as the Sender value.

You can make additions to the Feedback Lists described in the previous section by using an Advanced Analytics Model and also directly from the events report described in the following sections.

Obtaining Model Feedback with Advanced Analytics Models and Events Report

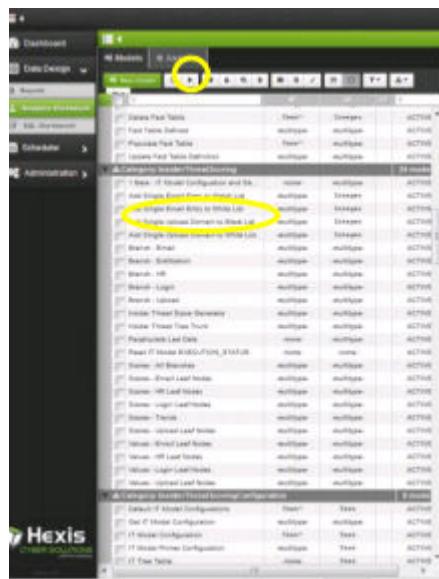
Each list has an associated Advanced Analytics Model which you can use to add entries to the appropriate table as noted below:

Inputs	Model
Upload Blacklist	Add Single Upload Domain to Blacklist
Upload Whitelist	Add Single Upload Domain to Whitelist
Email Watchlist	Add Single Email Entry to Watchlist
Email Whitelist	Add Single Email Entry to Whitelist

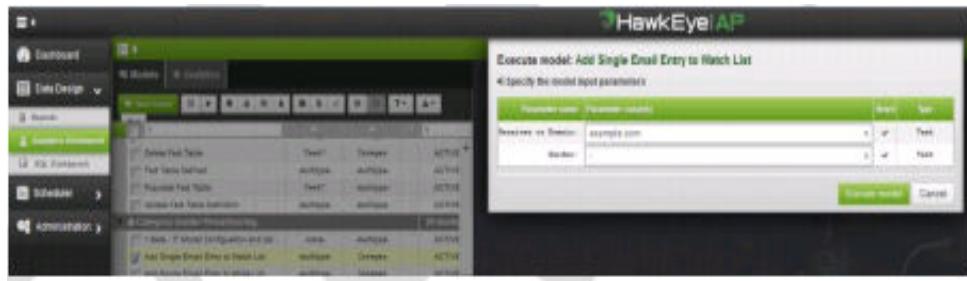
Use the following procedure to add an entry to the desired list:

- 1 Find and select the desired model in the Models tab list of the Analytics Workbench application within SenSage AP.
- 2 Click the Execute button in the toolbar.

Figure 2-17 Execute Button



- 3 Enter the appropriate values in the pop-up window, then click the **Execute model** button.

Figure 2-18: Execute Model Button

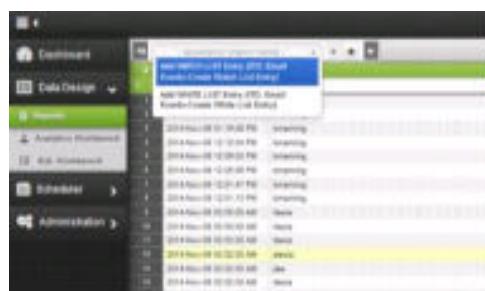
Events Report Associations

In operation, it may be necessary to add entries to one of these lists while analyzing events which cause high-risk detections. Each events report has associated reports to create entries in the appropriate list.

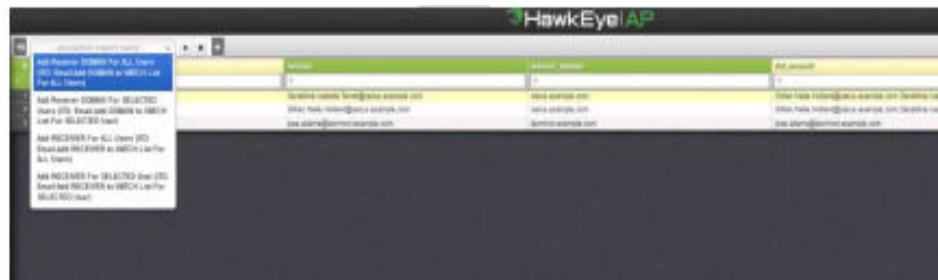
EMAIL BRANCH EVENTS

Use the following procedure to add multiple entries based on Email Branch event rows to the appropriate list:

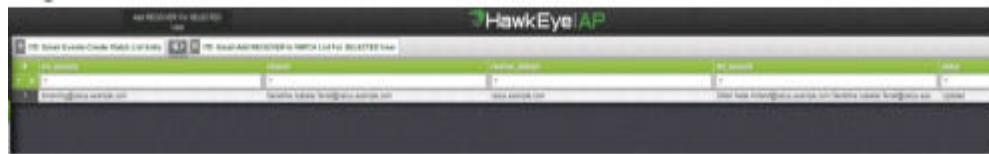
- 1 To drill down from ITD: Email Branch Events:
 - a Click on the row containing the values for addition to the list.
 - b Click the associated report button in the upper right corner.
- 2 Go to the left dropdown list of report associations and select Add WATCH LIST Entry (...). (You can take similar steps for the 'Add WHITE LIST Entry').
- 3 Click the **play** button to run the associated report.

Figure 2-19: Report Associations Dropdown List

The result is a list of all src_account (sender) and receiver pairs from the selected associated events, along with the receiver_domain, dst_account, and a status column.

Figure 2-20: Results

- 4 From this report, you can add an entry into the Email Watch List by selecting the row(s) which contain the desired values and repeating the report association process, selecting one of the following associations:
 - a Add Receiver DOMAIN For ALL Users - Adds the receiver_domain column to the Email Watchlist for all users (User value = "-")
 - b Add Receiver DOMAIN For SELECTED User - Adds the receiver_domain and src_account columns to the Email Watchlist
 - c Add Receiver for ALL Users - Adds the receiver column to the Email Watchlist for all users (User value = "-")
 - d Add RECEIVER For SELECTED User - Adds the receiver and src_account columns to the Email Watchlist
- 5 After running the appropriate report, you will find the status column populated to indicate if the entry was "Added" or "Updated":

Figure 2-21: Results

UPLOAD BRANCH EVENTS

Use the following procedure to update multiple entries based on upload branch event rows to the appropriate list:

- 1 To drill down from ITD: Upload Branch Events:
 - a Click on the row containing the values for addition to the list.
 - b Click the associated report button in the upper right corner.
- 2 Go to the left dropdown list of report associations and select Add WHITE LIST Entry (...). (You can take similar steps for the 'Add BLACK LIST Entry'.)
- 3 Click the play button to run the associated report.

The result is a list of all src_account (user) and dest_info_sys pairs from the selected associated events, along with a status column.

- 4 From this report, add an entry into the Upload White List by selecting the row(s) which contain the desired values and repeating the report association process, selecting one of the following associations:
 - a Add DOMAIN For ALL Users - Adds the dest_info_sys column to the Upload Whitelist for all users (User value = "-")
 - b Add DOMAIN For SELECTED User - Adds the dest_info_sys and src_account columns to the Upload Whitelist
- 5 After running the appropriate report, you will find the status column populated to indicate if the entry was "Added" or "Updated".

EXECUTING THE INSIDER THREAT MODEL

After all of the configuration settings have been verified, the IT Model is ready to execute. To execute the model, follow these steps:

- 1 Open the 1 Beta - IT Model Configuration and Generator model and click the execute button. The backfill process will start and the progress may be monitored as described in described in ["Backfilling Data", on page 59](#).

For proper operation, the IT Model should be executed on a daily basis and the dashboard should be observed for the presence of HIGH risk activity. The time to execute the model will vary based on the number of users and the number of log events in the EDW.

CONFIGURING AND EXECUTING THE IT MODEL IN A HYBRID SETUP

This section describes how to configure and execute the Insider Threat Detection (IT) Model in a hybrid setup. Follow these steps after you have configured the SenSage AP 6.1.x Analyzer to connect to the SenSage AP 5.0.x PostgreSQL server.

AP Analyzer Configuration

In a hybrid setup, the IT Model uses both the AP 5.0.x and the AP 6.1.x PostgreSQL servers for data storage and analysis. In order for a model to connect to the AP 6 PostgreSQL server, you must re-add it to the **app.properties** file.

Perform the following tasks on The AP 6.1.x Analyzer host:

- 1 Go to the Analyzer config directory:

```
cd /opt/hexis/hawkeye-ap/analyzer/config
```

- 2 Edit the app.properties file:

```
vi app.properties
```

Append a second set of database connection properties to the end of the file as shown below:

IMPORTANT: End each property name with **.2** and be sure that the **db.connection.name.2** property is set to **Controller9**.

```
# AP 6 PostgreSQL DB configuration
db.connection.name.2=Controller9
db.connection.driverClassName.2=org.postgresql.Driver
db.connection.url.2=jdbc:postgresql://<AP_6_PG_Server_Host>:5432/
controller?ssl=true&sslfactory=org.postgresql.ssl.NonValidatingFactory
db.connection.username.2=hexit
db.connection.password.2=<ENCRYPTED_PASSWORD>
db.connection.initialSize.2=10
db.connection.maxActive.2=50
db.connection.connectionProperties.2=;
```

- 3 After the app.properties file has been modified, restart the Analyzer for the configuration changes to take effect. You can restart the Analyzer using the Deployment Manager (Ambari) or by restarting the tomcat service.

Creating Schemas, Tables, Views, and Functions for the IT Model

The IT Model requires the presence of specific database objects. You will need to create these IT-specific objects on both the AP 6.1.x and AP 5.0.x PostgreSQL servers. Follow these steps to execute the SQL setup scripts:

- 1 Access the PostgreSQL setup scripts that are delivered along with the Consumer Analytics package in:

```
/opt/hexit/hawkeye-ap/analytics/6.1.0/resources
```

- 2 Use the following tar command to extract the setup scripts:

```
tar -xvzf itm_atpgsql.tgz
```

- 3 Edit the `itm_db_setup.sh` script:

a Access the `itm_db_setup.sh` script.

b Ensure both the `AP5_PG_HOST` and `AP5_PG_USER` variables are set to the appropriate values for the hybrid deployment.

- 4 Execute the `itm_db_setup.sh` script:

a `./itm_db_setup.sh`

b The script (on the AP 6.1.x and AP 5.0.x PostgreSQL servers) will perform the following tasks:

1. Drop the existing ITD PostgreSQL schemas (if they exist), along with all data.
2. Create operational ITD PostgreSQL objects (schemas, tables, views, functions, etc.)
3. Create test ITD PostgreSQL DB objects (schemas, tables, views, functions, etc.) and load with test data.

After the command is executed, the necessary database items are installed on the AP 6.1.x and AP 5.0.x PostgreSQL server.

CHAPTER 3

Sample Models for Working with Analytics Workbench

This chapter contains the following topics:

- “[Listing of Sample Models](#)”, next
- “[Using Data Tables in Sample Models](#)”, on page 72
- “[Implementing Data Tables in Sample Models](#)”, on page 74

LISTING OF SAMPLE MODELS

The following sample models in the table below will get you started in working with the Analytics Workbench. The Analytics components are also included in this table.

Model Name	Used Components	Description
Sample: Add Reference Table: Join Several Tables	CSV to Table, Add Reference Column, Extract Columns, Table to HTML	Sample demonstrates how to join several database tables with components into one resulting table
Sample: Basic: Arithmetic Operations	Multiply Integers, Product, Sum Integers Unbounded, Sum	Sample demonstrates how to do simple arithmetic operations
Sample: Basic: Breakpoints	CSV to Table, Sort Rows by Column, Column To List, Text to Number, Filter by Number Range, Get Item by Location	Sample demonstrates how to work with breakpoints
Sample: Basic: Change Check on Save	Copy String	Sample demonstrates how to work with sessions
Sample: Basic: Conversion Components	Text to Boolean, Double to Integer, Integer to Double, Integer to Boolean	Sample demonstrates how to convert data
Sample: Basic: Text Components	Trim, Text Length, Text Part, Scan Text	Sample demonstrates how to work with text components
Sample: Calculate Distance: Coordinates Difference	Create Table, Add Values to Column, Look Up Addresses, Calculate Distance, Get Table Item, Copy Number, Product, Update Table Item, Table to HTML	Sample demonstrates how to calculate distance between two geo points in meters
Sample: Charts From Table: Pie and Bar Graph	Create Table, Add Values to Column, Table to HTML, Bar Chart PNG from Table, Pie Chart PNG from Table	Sample demonstrates how to draw charts from the data
Sample: Create Database Table: Store Data to Database	Split String, Database Table Exists, Create Table, Add Values to Column, Get Item by Location, Create Database Table, Load Database Table, Concatenate Strings, Query Database	Sample demonstrates how to store calculated data into database

Model Name	Used Components	Description
Sample: Create Excel: Export to Excel File	Create Table, Add Values to Column, Create Excel	Sample demonstrates how to export data into Excel file
Sample: Custom Model: Advanced Iterators - Days Employed to Start Date	Iterator, CSV to Table, Text to Number, Column to List, Double to Integer, Add Columns, Add Values to Column, Table to HTML	This model demonstrates iterative capabilities. The "Days Employed" column is converted and processed through an iterator to provide the start date of the employees in the CSV file. The "Days Employed" column is removed and a new "Start Date" column is added. The data is then converted to an HTML file that can be displayed in a web browser.
Sample: Custom Model: Convert Days Employed to Start Date	Last X Days	Used in conjunction with the "Advanced Iterators - Days Employed to Start Date" model. Note: this model is not to be modified.
Sample: Custom Model: Iterated Add 1	Iterator	Sample demonstrates how to work with iterator as sum of integers values
Sample: Embedded Model: Add 1 to Integer	Sum Integers	Sample model used as component inside different model
Sample: Embedded Model: concatenate Strings with Delimiter	Concatenate Strings	Sample model used as component inside another model
Sample: Embedded Model: Text Match	Text Matches	Sample model used as component inside different model
Sample: Execute Report: Average against Last Value	Execute Report, Column to List, Text to Number, Mean, Get Table Item, Get item by location, Compare Numbers, Create Table, Number to Text, Add Values to Column, Add Columns, Table to HTML	This sample demonstrates the Execute Report component. After it executes, it compares the latest value (amount of copied bytes) with average by last 7 days. Data is from "Collector Daily Load - Trend" report. The output goes to HTML.
Sample: Execute Script: Get Hostname and Content	Execute Script	Sample demonstrates how to execute allowed script
Sample: Failed Logins Threshold Notification	Many embedded models including Send Basic Email	This sample model performs threshold detection and provides notification via email to a programmable email address with a count of the number of threshold crossings. This model is intended to be executed by a report called Sample: Failed Logins Summary -> Provide Notification - Threshold Exceeded. The results of the report get passed to this model for threshold detection and notification via email.

Model Name	Used Components	Description
Sample: Filter By Date: Filter by Date Range and User	CSV to Table, Text to Timestamp, Get Item by Location, Filter by Date, Filter Rows by Column Values	Sample demonstrates how to do group filtering
Sample: Filter by Date: Get Data by Last 7 days	Query Database, Last X Days, Filter by Date, Table to HTML	Sample demonstrates how to work with data for last X days
Sample: Filter by Number Range: Optional Inputs	Filter by Number Range	Sample demonstrates how to work with number range component
Sample: Filter Column by Number: Filter by Number Range	CSV to Table, Filter Column by Number, Table to HTML	Sample demonstrates how to do filtering for table
Sample: Filter Duplicates: Compare List with Filtered	CSV to Table, Column to List, Filter Duplicates, Add Columns, Add Values to Column, Table to HTML	Sample demonstrates how to remove duplicate values from column
Sample: Filter Rows by Column Values: Filter by Text	CSV to Table, Filter Rows by Column Values, Column to List, Copy String, Filter Duplicates, Create Table, Add Values to Column, Filter by External Column	Sample demonstrates how to do filtering by text in a table
Sample: Loop Sample: Concatenate Strings With Delimiter	Text Length, Concatenate Strings, Multiply Integers, Sum Integers Unbounded, Text Part	Sample demonstrates how iterator works with text
Sample: Multiply Integers: Routed Connections	Multiply Integers	This sample demonstrates the ability to add vertices to a connection so it can be routed around other components, providing better visibility of the canvas and workflow. Users may try the following: <ul style="list-style-type: none">• Click on a connection to select it.• Click on a translucent circle on the connection to add a vertex.• Click and drag a vertex to move it.• Double-click on a vertex to delete it. Multiple vertices can be added to each connection.
Sample: Send Basic Email: Send Notification if Value Reached Allowed	Compare Numbers, Copy String, Number to Text, Concatenate Strings, Send Basic Email	Sample demonstrates how to send basic email on reached critical value
Sample: Set Column Type: Load Untyped Data to Database	CSV to Table, Standardize Dates, Set Column Type, Database Table Exists, Create Database Table, Load Database Table	Takes in a CSV file with data of unknown type, then sets the column type for each field and create a database table from that data. Querying the database will show that the created table uses the create column types for each piece of data.
Sample: Show User: Accessible User Information	Copy String, Show User, Concatenate Strings	Sample demonstrates how to display current user name

Model Name	Used Components	Description
Sample: Standardize Date Text: Standardize Date Text & Date Format Options	Standardize Date Text	Sample demonstrates how to work with date formats
Sample: Table is Valid: Standardize Dates & Table is Valid	CSV to Table, Table is Valid, Standardize Dates	Sample demonstrates how to work with date formats in tables
Sample: Table to CSV: Data to CSV and Vice Versa	Create Table, Add Values to Column, Table to CSV, CSV to Table, Column to List	Sample demonstrates how to convert table into CSV and vice versa
Sample: Table to HTML: Custom CSS to HTML Output	CSV to Table, Table to HTML	Sample demonstrates how to use CSS styles on HTML output
Sample: Text Category: Text Category Samples	Copy String, Split String, Text Part, Text Length, Concatenate String, Replace Text, Scan Text, Trim, Text Matches	Sample demonstrates how to work with components from Text category

USING DATA TABLES IN SAMPLE MODELS

A *data table*, as implemented in the sample models, is a daily report which contains metrics and statistics computed over a specific time period based on daily measurements of a specific field of a log event.

For example, a failed login attempt is a type of login event stored in the EDW in SenSage AP. Using the sample model, you can easily construct a data table that computes the daily number of failed login attempts for each user and host machine and other relevant statistics over a 90-day period as shown in [Figure 3-1](#).

Figure 3-1: Failed Logins Data Table

DT_Failed_Logins_Daily_Count_All_Metrics													
#	date	account	info_sys	firstseen	lastseen	value	avg	stddev	zscore	numdays	numdaysw...	median	
T	T	T	T	T	T	T	T	T	T	T	T	T	
1	2014-11-03	rrobinson	ursaminor	2014-09-03	2014-11-03	19	0.578	3.137	5.872	90	3	0.0	
1	2014-11-03	rrobinson	hercules	2014-09-03	2014-11-03	17	0.556	3.010	5.484	90	3	0.0	
3	2014-11-03	rrobinson	mensa	2014-09-03	2014-11-03	15	0.489	2.874	5.426	90	3	0.0	
4	2014-11-03	rrobinson	indus	2014-09-03	2014-11-03	15	0.500	2.712	5.347	90	3	0.0	
5	2014-11-03	rrobinson	andromeda	2014-09-03	2014-11-03	15	0.533	2.892	5.002	90	3	0.0	
6	2014-11-03	rrobinson	cassiopeia	2014-09-03	2014-11-03	15	0.533	2.900	4.999	90	3	0.0	
7	2014-11-03	nscoott	centaurus	2014-08-06	2014-11-03	18	10.356	7.883	0.998	90	59	15.0	
8	2014-11-03	nscoott	indus	2014-08-06	2014-11-03	18	10.456	7.892	0.981	90	59	15.0	
9	2014-11-03	root	andromeda	2014-08-06	2014-11-03	17	10.411	7.888	0.857	90	59	14.5	
10	2014-11-03	mturner	mensa	2014-08-06	2014-11-03	17	10.489	7.768	0.838	90	59	15.0	
11	2014-11-03	kanderson	hercules	2014-08-06	2014-11-03	16	10.222	7.581	0.762	90	59	14.0	
12	2014-11-03	mwilson	octans	2014-08-06	2014-11-03	16	10.256	7.584	0.757	90	59	14.0	
13	2014-11-03	scampbell	cassiopeia	2014-08-06	2014-11-03	16	10.433	7.692	0.724	90	59	15.0	
14	2014-11-03	syoung	caelum	2014-08-06	2014-11-03	16	10.433	7.727	0.720	90	59	15.0	
15	2014-11-03	dtaylor	libra	2014-08-06	2014-11-03	15	10.244	7.581	0.627	90	59	14.0	
16	2014-11-03	ogarcia	poseidon	2014-08-06	2014-11-03	15	10.378	7.639	0.605	90	59	15.0	
17	2014-11-03	owilson	dorado	2014-08-06	2014-11-03	15	10.389	7.693	0.599	90	59	15.0	

In another example, shown in [Figure 3-2](#), a data table that was created using webproxy event logs, in which the metrics of interest are based on the total number of bytes uploaded to the internet per user and host. One use of a data table is to find anomalous user behavior on the

network and a simple method for doing this is by sorting the data table results by any of the various metrics (for example, descending z-score).

Figure 3-2: Bytes Uploaded Data Table

DT: Bytes Uploaded Daily Total All Metrics													
#	date	src_account	src_info_sys	firstseen	lastseen	value	avg	stddev	zscore	numdays	numdaysw...	median	
T	T	T	T	T	T	T	T	T	T	T	T	T	
1	2014-11-03	janderson	WIN-U2J6...	2014-08-12	2014-11-03	12969262	870323.411	2462438.167	4.913	90	20	0.0	
2	2014-11-03	mwilson	WIN-U2J6...	2014-08-11	2014-11-03	15093464	1458158.311	2920801.027	4.868	90	38	0.0	
3	2014-11-03	sthompson	WIN-U2J6...	2014-08-07	2014-11-03	23554782	4025571.633	5061885.249	3.858	90	59	1651126.5	
4	2014-11-03	coarter	WIN-U2J6...	2014-08-07	2014-11-03	11205237	1302060.100	2571311.850	3.851	90	29	0.0	
5	2014-11-03	bmanning	PC-8431	2014-08-09	2014-11-03	9995207	856495.111	2381810.013	3.837	90	13	0.0	
6	2014-11-03	mhill	WIN-U2J6...	2014-08-12	2014-11-03	22423381	2009223.333	5484647.497	3.722	90	15	0.0	
7	2014-11-03	glewis	WIN-U2J6...	2014-08-06	2014-11-03	13855053	1859728.533	3176598.330	3.713	90	48	100008.5	
8	2014-11-03	rtaylor	WIN-U2J6...	2014-08-06	2014-11-03	14916541	1978206.056	3893287.204	3.323	90	29	0.0	
9	2014-11-03	elewis	WIN-U2J6...	2014-08-09	2014-11-03	16227402	2773834.944	4835546.455	2.782	90	40	0.0	
10	2014-11-03	cthompson	WIN-U2J6...	2014-08-06	2014-11-03	7901805	1541937.111	2648778.084	2.403	90	41	0.0	
11	2014-11-03	lyoung	WIN-U2J6...	2014-08-07	2014-11-03	8137205	1998304.422	2965565.619	2.070	90	42	0.0	
12	2014-11-03	owilson	WIN-U2J6...	2014-08-07	2014-11-03	7055443	2018421.278	2846338.143	1.770	90	48	185353.0	
13	2014-11-03	dhill	WIN-U2J6...	2014-08-06	2014-11-03	5960286	1559907.267	2551531.015	1.725	90	29	0.0	
14	2014-11-03	aadams	WIN-U2J6...	2014-08-06	2014-11-03	5531882	1493024.389	2481320.410	1.628	90	36	0.0	
15	2014-11-03	asmith	WIN-U2J6...	2014-08-08	2014-11-03	2285776	623930.356	1195832.054	1.390	90	32	0.0	
16	2014-11-03	kjohnson	WIN-U2J6...	2014-08-06	2014-11-03	6570341	2522247.922	2985815.343	1.356	90	58	1232313.5	
17	2014-11-03	djones	WIN-U2J6...	2014-08-06	2014-11-03	4509672	1648555.389	2259692.365	1.266	90	52	438664.0	
18	2014-11-03	ehill	WIN-U2J6...	2014-08-09	2014-11-03	3024387	708376.844	1851000.612	1.251	90	18	0.0	
19	2014-11-03	swright	WIN-U2J6...	2014-08-07	2014-11-03	7843377	2940529.100	4013859.761	1.221	90	41	0.0	
20	2014-11-03	drobinson	WIN-U2J6...	2014-08-06	2014-11-03	6890790	2710004.556	4130326.297	1.012	90	39	0.0	

IMPLEMENTING DATA TABLES IN SAMPLE MODELS

This section contains beta version instructions for implementing data tables in sample models. It includes the following procedures and examples:

- “Importing Sample Data Table Models”, on page 75
- “Setting up the Database”, on page 75
- “Sample Data Tables Description”, on page 76
- “Sample Data Table Models Description”, on page 77
- “Data Table Programmable Fields”, on page 77
- “Data Table Outputs”, on page 79
- “Scheduling a Data Table”, on page 80
- “Sample Data Table Dashboard and Reports”, on page 81
- “Expected Results of Data Table Samples”, on page 82
- “Creating a New Data Table Using the Samples Provided”, on page 83

Importing Sample Data Table Models

This procedure is only required for versions of SenSage AP *prior* to 6.1.0. In version 6.1.0, the sample data tables are delivered as part of the product.

In versions prior to 6.1.0, sample data table models are provided in a zip file called mp_data-tables.zip. To use these samples in SenSage AP, you must import them using the following steps:

- 1 Open SenSage AP and navigate to the Analytics Workbench and Models tab.
- 2 Click the import icon; select the Import dropdown item.



- 3 Drag and drop the zip file to the Import models window.



Setting up the Database

A model included in the zip package, **DT:Database Setup for Samples**, automatically sets up the database schemas and loads the sample log events to the PostgreSQL database:

- Open the **DT:Database Setup for Samples** model
- Execute the model.

The model performs the following tasks:

- 1 Creates schema aa_data_tables if this schema does not already exist.
- 2 Loads sample log events tables to saw_simulated_data schema (note that the model creates this schema if the schema does not already exist); the sample tables are called userlogin and webproxy; the model does not load any data if the tables already exist.
- 3 Creates an aggregate called array_agg_fn and two other functions named array_sort and unnest. These are used in the median calculation and are necessary so that the median calculation works in PostgreSQL version 8.3.

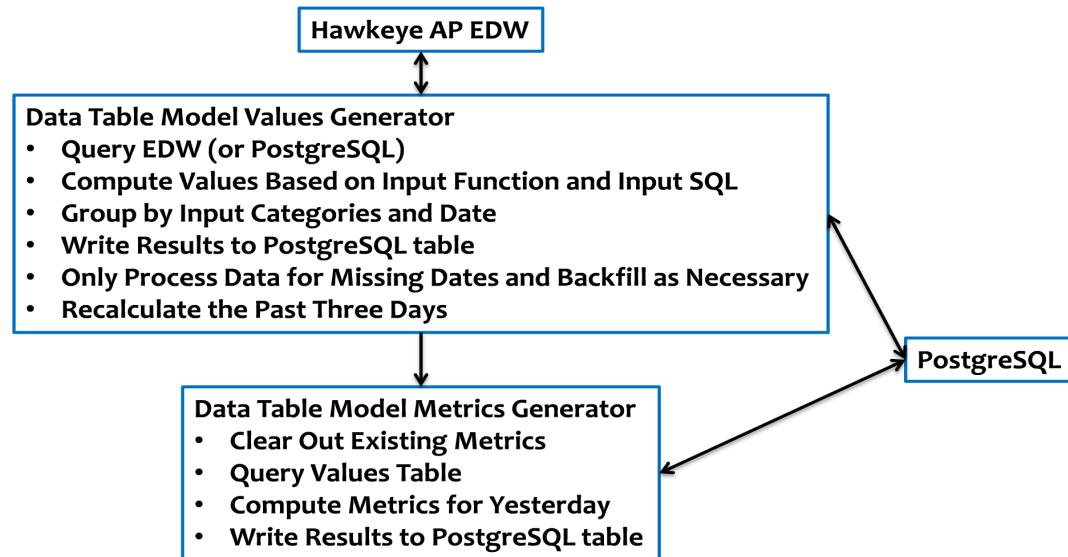
The aa_data_tables schema is used by the data tables for storing the output values and metrics tables.

Sample Data Tables Description

Data Table Components

The sample data table model design consists of two main components: values generation and metrics generation. The resulting data from each component resides in a PostgreSQL database table.

Figure 3-3: Data Table Design



For the sample data tables design, the values generator produces an aggregate measure of data recorded and stored in log events in the SenSage AP EDW (or even a PostgreSQL table), with a separate record stored for a unique pair of categories (such as user and host) for each day. Note that there must be two unique categories.

For example, for the Failed Logins data table, the daily number of failed login attempts for each user and host pair would be recorded. In the sample data table model, the data gets grouped, calculated, and stored in a PostgreSQL database table. In the interest of operational efficiency, the values generator backfills the values table for any missing days between yesterday and the number of days setting (the default number of days is 90). In addition, the values generator defaults to recalculate the previous three days of data so that the metrics may be calculated for any late arriving log events. Note that when the data table model runs for the first time it will backfill for the entire time period.

The metrics generator produces metrics and statistics based on the data generated by the values generator. While the values generator produces values for many days, the metrics generator produces results for a single day (yesterday), including metrics and statistics for each pair of unique categories that had an event on that day. Thus, the analyst reviewing the data table results has the most up-to-date information. The statistics are produced based on the total number of days; for instance, if the desired time period was 90 days, the statistics would be computed using the daily value for each of the 90 days (on days when there is no event, the value used is a 0).

Sample Data Table Models Description

Following are descriptions of two sample data table models.

DT Scheduler: Failed Logins Count - All Metrics

This model computes the daily number of failed login attempts for each unique user and host pair; it also computes several other metric values for the daily total number failed login attempts, including the first seen date, the last seen date, the average daily number of failed logins, the standard deviation, the z-score, and the number of days processed, the total number of days with a failed login, and the median.

DT Scheduler: Daily Bytes Uploaded - All Metrics

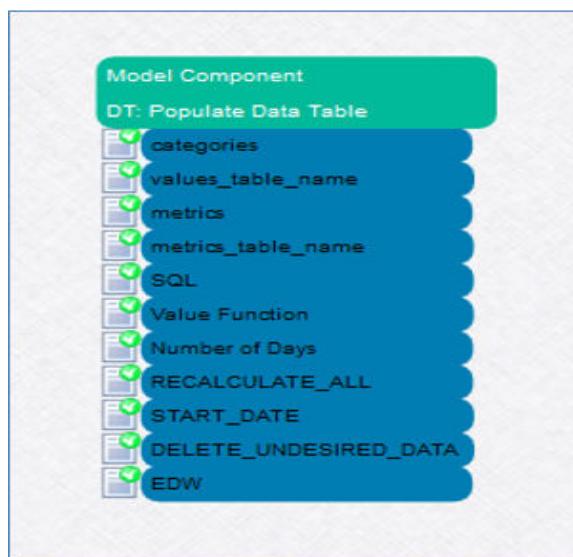
This model computes the daily total number of bytes uploaded to the internet for each unique user and host pair; it also computes several other metric values for the daily total number of bytes uploaded, including the first seen date, the last seen date, the average daily bytes uploaded, the standard deviation, the z-score, and the number of days processed, the total number of days with an upload to the internet, and the median.

Incidentally, the model names start with “DT Scheduler” as a method to organize the models together in the Models tab in SenSage AP and also to signify that the model may be scheduled using the SenSage AP Scheduler.

Data Table Programmable Fields

Data tables may be constructed in SenSage AP using a generic model called DT: Populate Data Table, found in the Analytics Workbench Models tab under the Data Table category. There are several programmable fields that are used in the DT: Populate Data Table to define the data table values, metrics, and time range. They are programmable by right-clicking and choosing **Set Parameter Value**.

Figure 3-4: Programmable Fields



Here is a description of each of the fields (listed here in alphabetical order; the order of the fields in the actual model on the AP canvas is not important):

- 1 categories - This is a comma-separated list of columns (no spaces between categories) in the original log event table (or IntelliSchema master view) used for grouping the data. The model expects there to be two unique categories. These are unique to the specific event and data table metrics are reported based on this unique pair. For instance, categories may be user and host; for the userlogin event table, the column names are **account** and **info_sys** and the categories files is set to **account,info_sys**.
- 2 DELETE_UNDESIRABLE_DATA - This is a flag for removing values data time that is outside of the desired time period window. When set to 1, it will remove any data from the values table that is outside of the 90-day window (based on the start date).
- 3 EDW - This is a flag that specifies if the source log event data is stored in the EDW or not, as the model makes the queries of the log events more efficient. Value is TRUE for EDW source tables; sample models have it set to FALSE because the sample source data is coming from PostgreSQL tables and not the EDW.
- 4 metrics - This a comma-separated list of metrics available for the data table; it may be any combination of the following (but must be at least one of them): avg,stddev,zscore,median. Metric definitions may be found below “[Data Table Outputs](#)”, on page 79
- 5 metrics_table_name - This is the name of the metrics table being stored in the PostgreSQL database; it must include the schema name.
- 6 Number of Days - This is a number representing the time period of interest in days, typically set to 90.
- 7 RECALCULATE_ALL - This is a number representing the number of days to recalculate the values for, typically set to 3.
- 8 SQL - This is a SQL statement used to collect the raw values of interest (prior to the daily aggregate function). The example for Failed Logins is below:

```
SELECT tbl.ts::DATE AS DATE
      ,tbl.account
      ,tbl.info_sys
      ,CASE
          WHEN (tbl.result = '0' OR tbl.result = 'failure') THEN 1
          ELSE 0
        END AS val
  FROM saw_simulated_data.userlogin tbl
 WHERE <<TS_FILTER>>
       AND tbl.account <> '-'
```

This SQL statement (which cannot be executed as-is since the model uses it in context with other parts of the model to automatically create the actual values query during run time) grabs the **ts** column, the account and **info_sys** (which match the **categories** field), and for every failed login attempt noted in the log event, it records a value of **1**; if the event was not a failed login attempt, it records a value of **0**. The source table for the log events is defined here (**saw_simulated_data.userlogin** table). In addition, the use of **<<TS_FILTER>>** is a token that allows the model to populate the values table with only missing data (the token gets replaced downstream in the dataflow of the model). In using this as an example for a different data table, a user would simply modify the highlighted sections and leave untouched the non-highlighted part (SQL repeated here with highlighted sections).

```

SELECT tbl.ts::DATE AS DATE
    ,tbl.account <=This column needs to match one of the categories
    ,tbl.info_sys <=This column needs to match one of the categories
    ,CASE
        WHEN (tbl.result = '0' OR tbl.result = 'failure') THEN 1
        ELSE 0
    END AS val
FROM saw_simulated_data.userlogin tbl
WHERE <>TS_FILTER>>
    AND tbl.account <> '-'<=This clause may need to match a category

```

NOTES:

- The categories in this SQL statement must be of text type.
 - The SQL statement cannot have any embedded comments or it will error out (this is due to some string inputs to analytic components being represented on a single line in AP).
 - The WHERE clause at the end may also need to match a category, depending on the desired values being produced by the model.
- 9** START_DATE - This is the start date that defines the time period, in operation it would be set to "now". In the samples, it is set to a specific date of 2014-11-04, which means the data table metrics are produced with 2014-11-03 as the last day (that is, "yesterday" relative to the start date) in the 90-day time period.
- 10** Value Function - This is the PostgreSQL aggregate function (aggregation on a daily basis). For the Failed Logins and Bytes Uploaded data table examples, the setting is "sum". This means that the values table stored in PostgreSQL will be a daily sum of failed login attempts for each user and host pair.
- 11** values_table_name - This is the name of the values table being stored in the PostgreSQL database; it must include the schema name.

Data Table Outputs

The output columns in the metrics table are the final results of the data table model execution. Here are the definitions of the metrics table output columns.

- 1 date – Most recent date with processed data.
- 2 category1 – The first category for grouping the data (corresponds to user input).
- 3 category2 – The second category for grouping the data (corresponds to user input).
- 4 firstseen – Date of the first time this event has been observed (it is inside the 90 day window).
- 5 lastseen – Date of the most recent time this event has been observed (it will match the date column).
- 6 value – The aggregate value for the data table for that date, for instance the total number of failed logins that day for that user and host pair (i.e. the categories)
- 7 avg – The daily average for that event (averaged over the time period). Note when no events take place, the value for the day is considered 0.

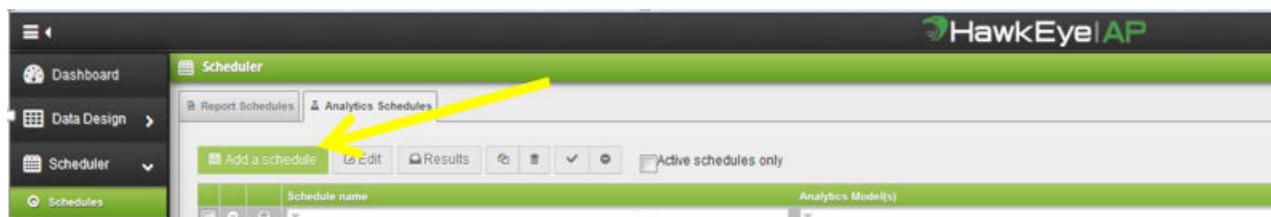
- 8 stddev** – The standard deviation for that event over the time period.
- 9 zscore** – This is the z-Score, a measure of the number of standard deviations the value is from the average. This is a good metric for anomaly detection in data tables.
- 10 numdays** – This is the number of days in the processed time period.
- 11 numdayswithevent** – This is the number of days that had an event, for instance, the number of days with a failed login attempt for this user and host (i.e. the categories).
- 12 median** – This is the median of that event over the time period (note that zeros are used for days without an event and those zeros are part of the median calculation).

In the metrics table, data only appears for category pairs (account,info_sys) that had events on that date. If a specific account and info_sys pair did not have any events on that date, the metrics do not appear in the metrics table.

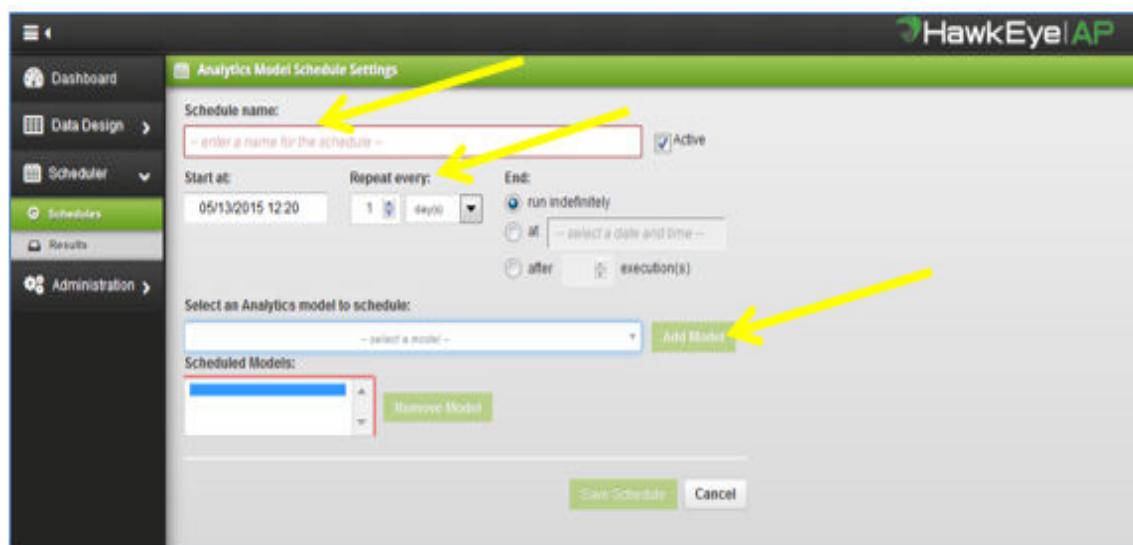
Scheduling a Data Table

Using the SenSage AP Scheduler, you can schedule a data table to execute on a daily basis.

- 1 Navigate to the Scheduler page, click the Analytics Schedules tab, and click **Add a schedule**.



- 2 Name the schedule (for example, Daily Failed Logins Data Table), select the repeat frequency, and select the model using the Add Model button.



Sample Data Table Dashboard and Reports

Reports

Because the output metrics table contains all of the data of interest to an analyst of a data table, a simple report for the data table should contain all of the metrics table columns. Sorting the report by a particular metric of interest, such as z-score, for anomaly detection is recommended. Figure 3-5 sample report wizard edit page from SenSage AP for the failed logins data table:

Figure 3-5: Sample Data Table Report for Failed Logins

In addition, as a nice add-on to a dashboard a report that contains all of the data table names and the most recent processed date can be used to show the existing data tables and the status of the processed data. Here is an example:

Figure 3-6: Latest Date for Data Table Metrics Report

```

select max(date) as most_recent_date, 'Failed Logins Daily Count Data Table' as data_table from aa_data_tables.dt_failed_logins_dailycount_values
UNION ALL
select max(date) as most_recent_date, 'Bytes Uploaded Daily Total Data Table' as data_table from aa_data_tables.dt_bytes_uploaded_dailytotals_values
  
```

Dashboard

A recommended dashboard in SenSage AP would contain a report for each of the data table model output (i.e. the metrics table), along with the status report for the most recent processed date for each of the data tables metrics, as noted above. Here is an example:

Figure 3-7: Sample Data Table Dashboard

SF Failed Logins For Data Table Metrics											SF Failed Logins Daily Count All Metrics																												
#	date	username	last_login_ip	firstseen	lastseen	value	avg	min	max	count#	members	nonmembers	median	#	date	sum	average	min_val	max_val	firstseen	value	avg	min	max	count#	members	nonmembers	median											
1	2014-11-03	mikemar	urkamer	2014-09-03	2014-11-03	19	0.578	0.127	0.472	80	1	0	0.5	1	2014-11-03	jeromek	WnL-U2J..	2014-08-12	12086282	0702023.417	2452438.187	4.813	90	20	0.0														
5	2014-11-03	mikemar	hermes	2014-09-03	2014-11-03	17	0.558	0.310	0.404	80	1	0	0.5	2	2014-11-03	jeromek	WnL-U2J..	2014-08-11	12053494	1450116.371	2620201.327	4.905	90	38	0.0														
3	2014-11-03	mikemar	marcus	2014-09-03	2014-11-03	15	0.488	2.874	5.428	80	1	0	0.5	3	2014-11-03	shempster	WnL-U2J..	2014-08-07	2014-09-03	20864292	420971.013	5001688.249	3.908	90	59	0.0													
2	2014-11-03	mikemar	india	2014-09-03	2014-11-03	18	0.447	2.718	5.040	80	1	0	0.5	4	2014-11-03	user	WnL-U2J..	2014-08-10	12020957	1020050.000	1020050.000	4.905	90	28	0.0														
6	2014-11-03	mikemar	andromeda	2014-09-03	2014-11-03	19	0.533	2.880	5.502	80	1	0	0.5	5	2014-11-03	pcman	WnL-U2J..	2014-08-09	12019597	2300000.000	2300000.000	4.905	90	12	0.0														
7	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.533	2.880	4.988	80	1	0	0.5	6	2014-11-03	midas	WnL-U2J..	2014-08-07	2014-11-03	20421381	3000233.333	1448487.467	3.807	90	18	0.0													
8	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.533	2.880	4.988	80	1	0	0.5	7	2014-11-03	glenix	WnL-U2J..	2014-08-08	2014-11-03	12055002	1500128.333	1170056.000	3.719	90	45	0.000000.0													
9	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.533	2.880	4.988	80	1	0	0.5	8	2014-11-03	mayor	WnL-U2J..	2014-08-09	2014-11-03	1973206.000	3003281.254	3.133	90	29	0.0														
10	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.533	2.880	4.988	80	1	0	0.5	9	2014-11-03	elvis	WnL-U2J..	2014-08-09	2014-11-03	20221462	2770314.400	4031946.498	2.752	90	45	0.0													
11	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	17	0.413	7.000	8.000	80	1	0	0.5	10	2014-11-03	thompson	WnL-U2J..	2014-08-07	2014-11-03	7801770.000	2547073.084	2.403	90	41	0.0														
12	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.400	7.700	8.000	80	1	0	0.5	11	2014-11-03	lynnix	WnL-U2J..	2014-08-07	2014-11-03	8137246	1988604.423	2655595.819	2.079	90	42	0.0													
13	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.422	7.500	8.000	80	1	0	0.5	12	2014-11-03	oakman	WnL-U2J..	2014-08-07	2014-11-03	7039412.278	2064038.143	1.773	90	45	0.000000.0														
14	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.529	7.700	8.000	80	1	0	0.5	13	2014-11-03	ash	WnL-U2J..	2014-08-08	2014-11-03	6860286	1588687.287	2601891.018	1.728	90	28	0.0													
15	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.403	7.700	8.000	80	1	0	0.5	14	2014-11-03	ashley	WnL-U2J..	2014-08-08	2014-11-03	6860286	1588687.287	2601891.018	1.728	90	39	0.0													
16	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.544	7.681	8.027	80	1	0	0.5	15	2014-11-03	ashworth	WnL-U2J..	2014-08-08	2014-11-03	2208176	1198622.054	13865	90	22	6.5														
17	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.539	7.681	8.027	80	1	0	0.5	16	2014-11-03	lynne	WnL-U2J..	2014-08-09	2014-11-03	9070244	2732247.122	293015.243	1.198	90	65	1232113.9													
18	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.579	7.800	8.000	80	1	0	0.5	17	2014-11-03	dances	WnL-U2J..	2014-08-09	2014-11-03	4008972	1605018.369	255982.395	1.298	90	52	418894.0													
19	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.539	7.800	8.000	80	1	0	0.5	20	2014-11-03	ash	WnL-U2J..	2014-08-09	2014-11-03	3024387	795719.844	161000.012	1.251	90	16	0.0													
20	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.521	7.820	8.027	80	1	0	0.5	21	2014-11-03	angie	WnL-U2J..	2014-08-07	2014-11-03	7934327	2046239.150	4030008.781	3.221	90	41	0.0													
21	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.515	7.811	8.027	80	1	0	0.5	22	2014-11-03	drakepear	WnL-U2J..	2014-08-08	2014-11-03	6880704	2710054.333	410328.297	1.012	90	38	0.0													
22	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.515	7.811	8.027	80	1	0	0.5	23	2014-11-03	iggy	WnL-U2J..	2014-08-07	2014-11-03	6880704	2710054.333	1997381.189	1.001	90	28	0.0													
23	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.514	7.811	8.027	80	1	0	0.5	24	2014-11-03	maxwell	WnL-U2J..	2014-08-08	2014-11-03	6880704	2710054.333	2446170.238	0.879	90	18	324894.0													
24	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.514	7.811	8.027	80	1	0	0.5	25	2014-11-03	spike	WnL-U2J..	2014-08-08	2014-11-03	6880704	2710054.333	402005.221	0.819	90	49	323096.0													
25	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.514	7.811	8.027	80	1	0	0.5	26	2014-11-03	raynor	WnL-U2J..	2014-08-07	2014-11-03	47302777	2424212.622	4420384.857	0.869	90	63	107949.0													
26	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.514	7.811	8.027	80	1	0	0.5	27	2014-11-03	spike	WnL-U2J..	2014-08-09	2014-11-03	2424212.622	4522110.735	3.152	90	15	0.0														
27	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.514	7.811	8.027	80	1	0	0.5	28	2014-11-03	espresso	WnL-U2J..	2014-08-09	2014-11-03	126241	787719.744	140000.123	0.459	90	42	0.0													
28	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.514	7.811	8.027	80	1	0	0.5	29	2014-11-03	aking	WnL-U2J..	2014-08-09	2014-11-03	205547	194521.878	231405.893	0.428	90	50	524870.0													
29	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.514	7.811	8.027	80	1	0	0.5	30	2014-11-03	wiztman	WnL-U2J..	2014-08-26	2014-11-03	3270253.944	286873.740	0.418	90	55	67022.0														
30	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.514	7.811	8.027	80	1	0	0.5	31	2014-11-03	Home	WnL-U2J..	2014-08-08	2014-11-03	3086108	270702.422	307016.890	0.381	90	52	0.0													
31	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.514	7.811	8.027	80	1	0	0.5	32	2014-11-03	spike	WnL-U2J..	2014-08-08	2014-11-03	3086108	270702.422	307016.890	0.381	90	50	36209.0													
32	2014-11-03	mikemar	metropolis	2014-09-03	2014-11-03	18	0.514	7.811	8.027	80	1	0	0.5	33	2014-11-03	wyoming	WnL-U2J..	2014-08-08	2014-11-03	441910	296512.213	491173.829	0.326	90	47	215171.0													

Figure 3-8: Failed Logins Data Table - Expected Metrics Results for all 20 Users, Data Sorted by ZScore (Descending)

DT: Failed Logins Daily Count All Metrics													
#	date	account	info_sys	firstseen	lastseen	value	avg	stddev	zscore	numdays	numdaysw...	median	
1	2014-11-03	rrobinson	ursaminor	2014-09-03	2014-11-03	19	0.578	3.137	5.872	90	3	0.0	
2	2014-11-03	rrobinson	hercules	2014-09-03	2014-11-03	17	0.556	3.010	5.454	90	3	0.0	
3	2014-11-03	rrobinson	mensa	2014-09-03	2014-11-03	15	0.489	2.874	5.426	90	3	0.0	
4	2014-11-03	rrobinson	indus	2014-09-03	2014-11-03	15	0.500	2.712	5.347	90	3	0.0	
5	2014-11-03	rrobinson	andromeda	2014-09-03	2014-11-03	15	0.533	2.892	5.002	90	3	0.0	
6	2014-11-03	rrobinson	cassiopeia	2014-09-03	2014-11-03	15	0.533	2.900	4.989	90	3	0.0	
7	2014-11-03	lscott	centaurus	2014-08-06	2014-11-03	18	10.356	7.653	0.998	90	59	15.0	
8	2014-11-03	nscott	indus	2014-08-06	2014-11-03	18	10.456	7.692	0.981	90	59	15.0	
9	2014-11-03	root	andromeda	2014-08-06	2014-11-03	17	10.411	7.688	0.857	90	59	14.5	
10	2014-11-03	mturner	mensa	2014-08-06	2014-11-03	17	10.489	7.768	0.838	90	59	15.0	
11	2014-11-03	kanderson	hercules	2014-08-06	2014-11-03	16	10.222	7.581	0.762	90	59	14.0	
12	2014-11-03	mwilson	octana	2014-08-06	2014-11-03	16	10.256	7.564	0.757	90	59	14.0	
13	2014-11-03	scampbell	cassiopeia	2014-08-06	2014-11-03	16	10.433	7.692	0.724	90	59	15.0	
14	2014-11-03	syoung	caelum	2014-08-06	2014-11-03	16	10.433	7.727	0.720	90	59	15.0	
15	2014-11-03	dtaylor	libra	2014-08-06	2014-11-03	15	10.244	7.581	0.627	90	59	14.0	
16	2014-11-03	ogarcia	poseidon	2014-08-06	2014-11-03	15	10.378	7.639	0.605	90	59	15.0	
17	2014-11-03	cwilson	dorado	2014-08-06	2014-11-03	15	10.389	7.693	0.599	90	59	15.0	
18	2014-11-03	hlopez	apollo	2014-08-06	2014-11-03	15	10.700	7.895	0.545	90	59	15.0	
19	2014-11-03	kallen	camelopard...	2014-08-06	2014-11-03	13	10.211	7.520	0.371	90	59	14.5	
20	2014-11-03	pallen	triangulum	2014-08-06	2014-11-03	13	10.311	7.617	0.353	90	59	15.0	

Figure 3-9: Bytes Uploaded Data Table - Expected Metrics Results for First 20 Users, Data Sorted by ZScore (Descending)

DT: Bytes Uploaded Daily Total All Metrics													
#	date	src_account	src_info_sys	firstseen	lastseen	value	avg	stddev	zscore	numdays	numdaysw...	median	
1	2014-11-03	janderson	WIN-U2J6...	2014-08-12	2014-11-03	12969262	870323.411	2462438.167	4.913	90	20	0.0	
2	2014-11-03	mwilson	WIN-U2J6...	2014-08-11	2014-11-03	15093464	1458158.311	2920801.027	4.868	90	38	0.0	
3	2014-11-03	sthompson	WIN-U2J6...	2014-08-07	2014-11-03	23554762	4025571.633	5061885.249	3.858	90	59	1651126.5	
4	2014-11-03	ccarter	WIN-U2J6...	2014-08-07	2014-11-03	11205237	1302080.100	2571311.858	3.851	90	29	0.0	
5	2014-11-03	bmannning	PC-8431	2014-08-09	2014-11-03	9995207	856495.111	2381810.013	3.837	90	13	0.0	
6	2014-11-03	rhill	WIN-U2J6...	2014-08-12	2014-11-03	22423361	2009223.333	5484847.497	3.722	90	15	0.0	
7	2014-11-03	glewis	WIN-U2J6...	2014-08-06	2014-11-03	13855053	1859728.533	3176596.330	3.713	90	48	100008.5	
8	2014-11-03	rtaylor	WIN-U2J6...	2014-08-06	2014-11-03	14916541	1978208.056	3893287.204	3.323	90	29	0.0	
9	2014-11-03	elewiss	WIN-U2J6...	2014-08-09	2014-11-03	16227402	2773834.944	4835546.455	2.782	90	40	0.0	
10	2014-11-03	cthompson	WIN-U2J6...	2014-08-06	2014-11-03	7901805	1541937.111	2646778.084	2.403	90	41	0.0	
11	2014-11-03	lyoung	WIN-U2J6...	2014-08-07	2014-11-03	8137205	1998304.422	2965565.619	2.070	90	42	0.0	
12	2014-11-03	cwilson	WIN-U2J6...	2014-08-07	2014-11-03	7055443	2018421.278	2846336.143	1.770	90	46	185353.0	
13	2014-11-03	dhill	WIN-U2J6...	2014-08-06	2014-11-03	5980266	1559907.267	2551531.015	1.725	90	29	0.0	
14	2014-11-03	aadams	WIN-U2J6...	2014-08-08	2014-11-03	5531882	1493024.389	2481320.410	1.828	90	36	0.0	
15	2014-11-03	asmith	WIN-U2J6...	2014-08-08	2014-11-03	2285776	623930.356	1196832.054	1.390	90	32	0.0	
16	2014-11-03	kjohnson	WIN-U2J6...	2014-08-05	2014-11-03	8570341	2522247.922	2985815.343	1.356	90	58	1232313.5	
17	2014-11-03	djones	WIN-U2J6...	2014-08-06	2014-11-03	4509672	1648555.389	2256962.385	1.266	90	52	438864.0	
18	2014-11-03	ehill	WIN-U2J6...	2014-08-09	2014-11-03	3024387	708376.844	1851000.612	1.251	90	18	0.0	
19	2014-11-03	swright	WIN-U2J6...	2014-08-07	2014-11-03	7843377	2940529.100	4013859.761	1.221	90	41	0.0	
20	2014-11-03	drobinson	WIN-U2J6...	2014-08-06	2014-11-03	6890790	2710004.556	4130326.297	1.012	90	39	0.0	

Creating a New Data Table Using the Samples Provided

To create a new data table using the samples provided, perform the following steps:

- 1 Create a New Model.
- 2 Drag and drop the DT Populate Data Table model to the canvas.

- 3** Fill out the fields as described in “[Data Table Programmable Fields](#)”, [on page 77](#). Note that it is recommended that you use the SQL Workbench functionality in SenSage AP (or a PostgreSQL client like pgadmin) to debug values queries.
- 4** Execute the model.
- 5** Create a report for the model metrics output and add the report to the data table dashboard.
- 6** Schedule the model.
- 7** Observe dashboard daily for updated results.

Sample Model Description: Notification when a Threshold is Exceeded in a Report

While using SenSage AP users may want to receive notification when certain values in a report exceed a specified threshold. For instance, assume a report generates a daily total count of the number of failed logins per user and host combination; users may want to receive notification any time a total of more than three failed logins per user and host is reached. This chapter provides the sample model that is available in SenSage AP to create this type of notification. It contains the following sections:

- “[Dataflow Description](#)”, [on page 85](#) provides an explanation of the sample data flow
- “[How to Use the Notification Model](#)”, [on page 86](#) describes how (what is known as *report-to-model-to-report*) execution works and provides report/model threshold detection and notification tips.

DATAFLOW DESCRIPTION

In the SenSage AP system, the AP report called **Sample: Failed Logins Summary -> Provide Notification - Threshold Exceeded** produces a daily count of the number of failed logins grouped by account and info_sys (that is, user and host system) from the **default_analytics_intellischema.userlogin** master view.

The report then performs these steps in the following order:

- Executes a model called **Sample: Failed Logins Threshold Notification** that filters log events using the daily failed login count column, which keeps all events with a count greater than three in a table.
- Creates an event routing table with the following format: key, route, destination.

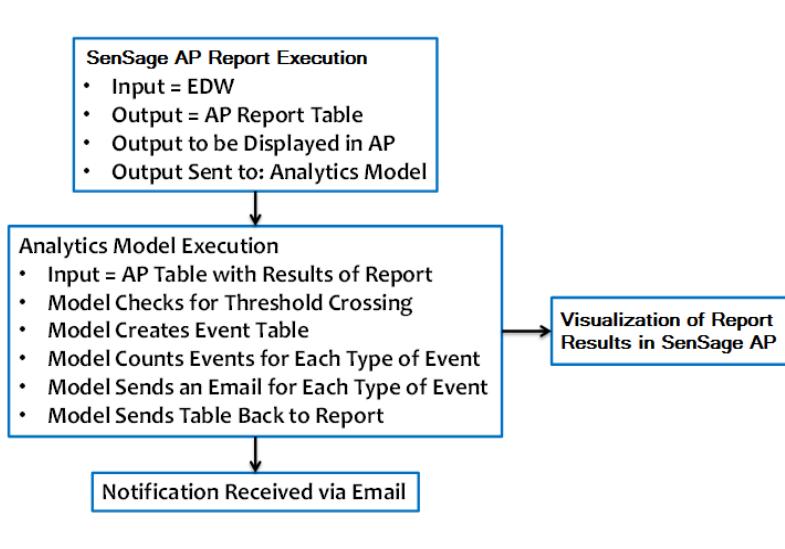
The key is the type of event, in this case the key is **Number of Failed Logins > 3**. The route for this event table is **Email** and the destination is **someone@this.org**. (Note, in the model the key, route, and destination are programmable but only Email is supported for the example route. In addition, if desired, multiple event tables may be combined into a single event table for multiple different threshold checks; however, this example only has one event table).

- Lastly, sends the event table to the embedded notification model.

The model sends an email to the destination for each type of event (or key) along with the count of the number of that type of event.

Figure 4-1 provides a general dataflow diagram.

Figure 4-1: Dataflow Diagram



HOW TO USE THE NOTIFICATION MODEL

The Report Fields tab, Figure 4-2, presents the wizard definition of the sample report, **Sample: Failed Logins Summary -> Provide Notification - Threshold Exceeded**. The report counts the daily number of failed logins per user and host pair using log events from the default_analytics_intellischema.userlogin master view.

Figure 4-2: Report Fields Tab

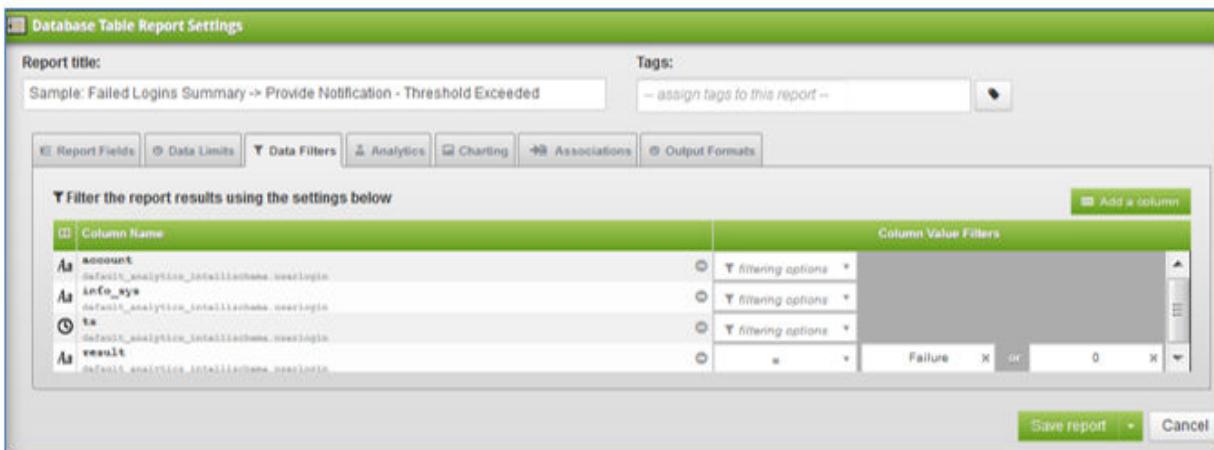
The screenshot shows the 'Database Table Report Settings' dialog box with the 'Report Fields' tab selected. The report title is 'Sample: Failed Logins Summary -> Provide Notification - Threshold Exceeded'. The 'Report Fields' grid contains four rows of data:

#	Cast	Column Name	%	Report Column Header	Group By	Display Value	Sort By
1	none	ts		ts (Day)	1	Day	
2	As	account		account (Field value)	2	Field value	
3	As	info_sys		info_sys (Field value)	3	Field value	
4	As	result		result (Count)		Count	

A checked checkbox 'This is a summary report' is located at the top right of the grid. At the bottom right are 'Save report...' and 'Cancel' buttons.

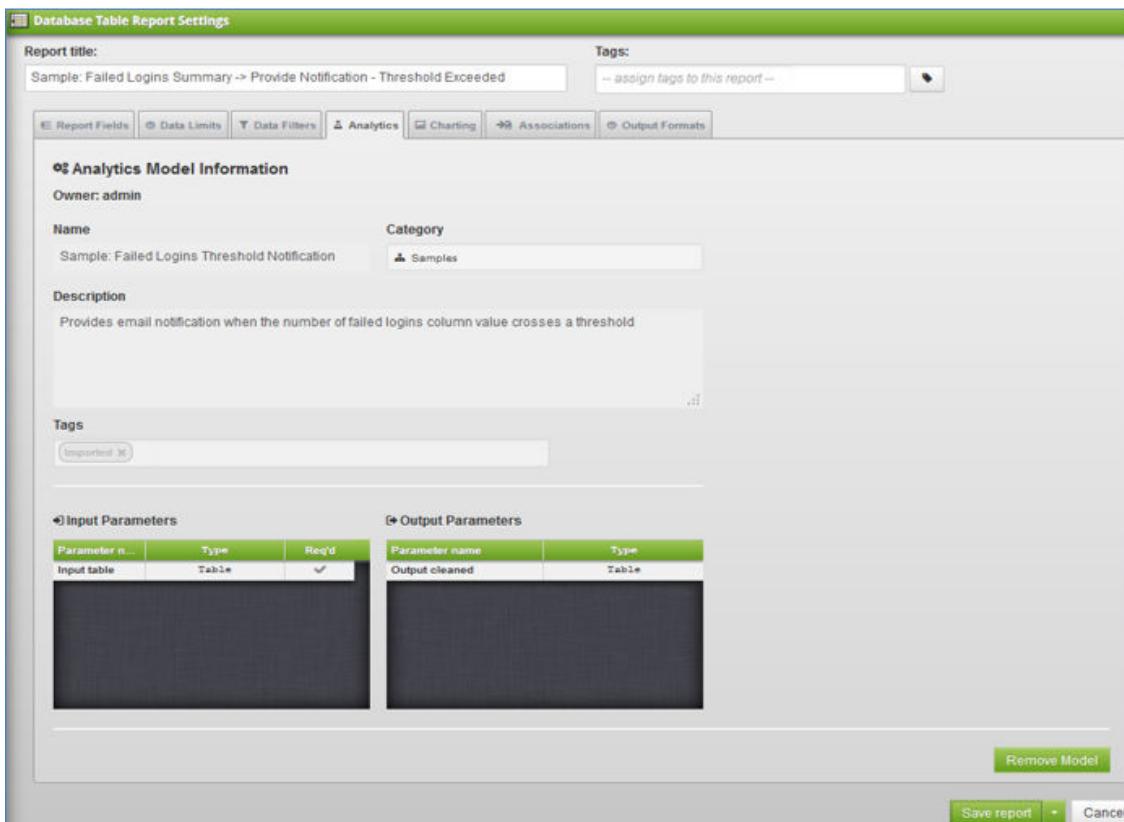
The Data Filter tab defines the failed login conditional filter:

Figure 4-3: Data Filters Tab



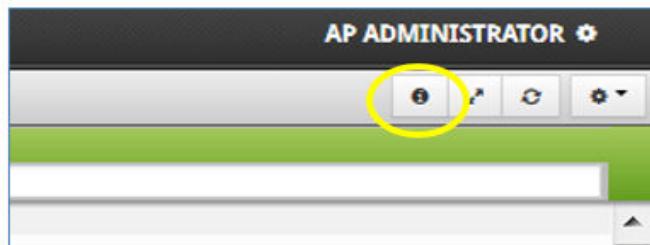
The Analytics tab defines the specific model where the results of the report are sent for threshold detection and notification.

Figure 4-4: Analytics Tab



TIP: After executing a report, the SQL statement used to produce the report can be found by clicking on the "i" icon in upper right of the reports result page.

Figure 4-5: Information Icon on Report Results Page



The following is the SQL for the **Sample: Failed Logins Summary -> Provide Notification - Threshold Exceeded report**.

Note the name assigned to the resulting value of the count of failed logins = count_result (Figure 4-6); it will be necessary to use “count_result” in the threshold detection and notification model:

Figure 4-6: SQL for the Current Report

SQL for the current report:

```

SELECT DATE_TRUNC('day', default_analytics_intellischema.userlogin."ts") as date_trunc_ts,
default_analytics_intellischema.userlogin."account" as account, default_analytics_intellischema
.userlogin."info_sys" as info_sys, COUNT(default_analytics_intellischema.userlogin."result") as
count_result FROM default_analytics_intellischema.userlogin WHERE (default_analytics_intellischem
a.userlogin."result" = 'Failure' OR default_analytics_intellischema.userlogin."result" = '0')
GROUP BY date_trunc_ts, default_analytics_intellischema.userlogin."account", default_analytics_in
tellischema.userlogin."info_sys" ORDER BY date_trunc_ts, default_analytics_intellischema.userlogi
n."account", default_analytics_intellischema.userlogin."info_sys"

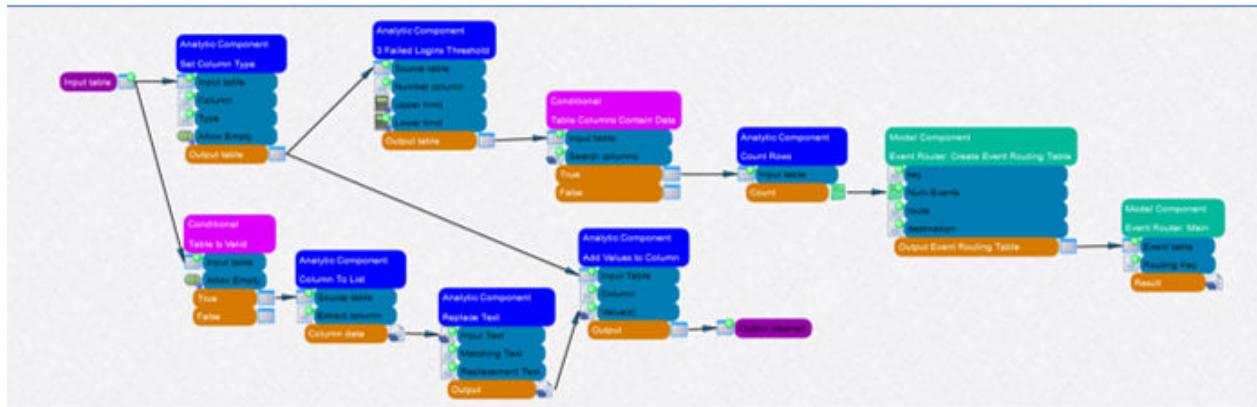
```

Close

The report (as defined above) executes and then sends its results to the model identified in the Analytics tab. In the example, the model uses the report results as an input table and proceeds to execute. The model checks the count_result column for threshold crossings and provides an email alert notification to a programmable email address.

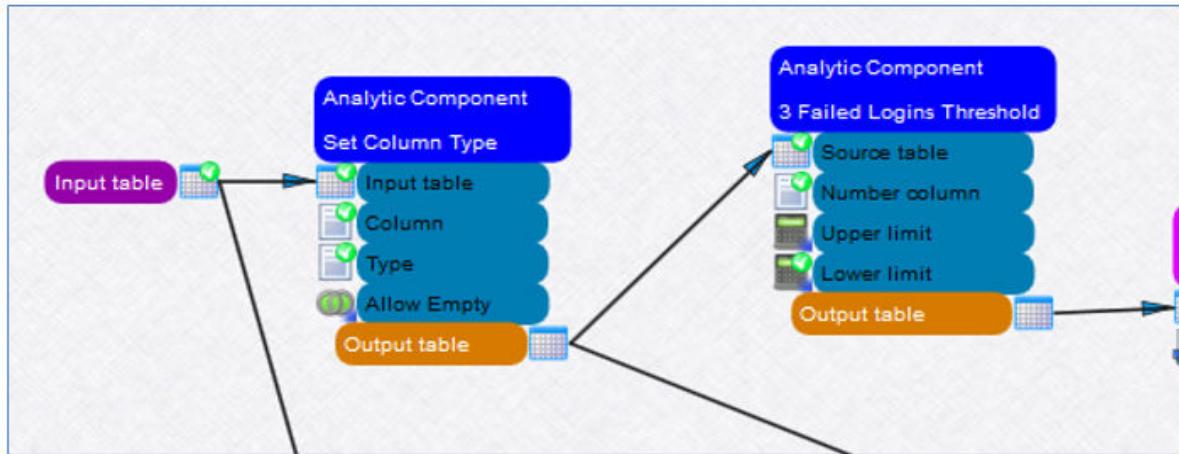
NOTE: To follow along with the descriptions and screenshots that are provided in the following sections, you are encouraged to bring up this sample model in SenSage AP.

Figure 4-7: Sample Model Diagram (Dataflow)



The data flows from left to right in [Figure 4-7](#). The following details will focus on the top portion of the model diagram.

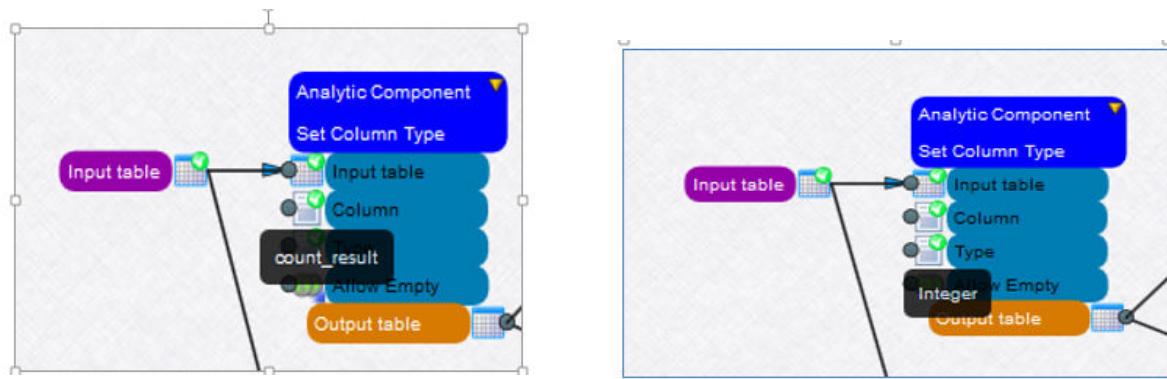
Figure 4-8: Input Table for Sample Model



Input table represents the input to this model, which is coming from the output of the **Sample: Failed Logins Summary -> Provide Notification - Threshold Exceeded** report. The first action the model takes is to convert the column of interest to an integer type so that it can check against the threshold. The column of interest is named **count_result**, as mentioned above and the type is set to integer.

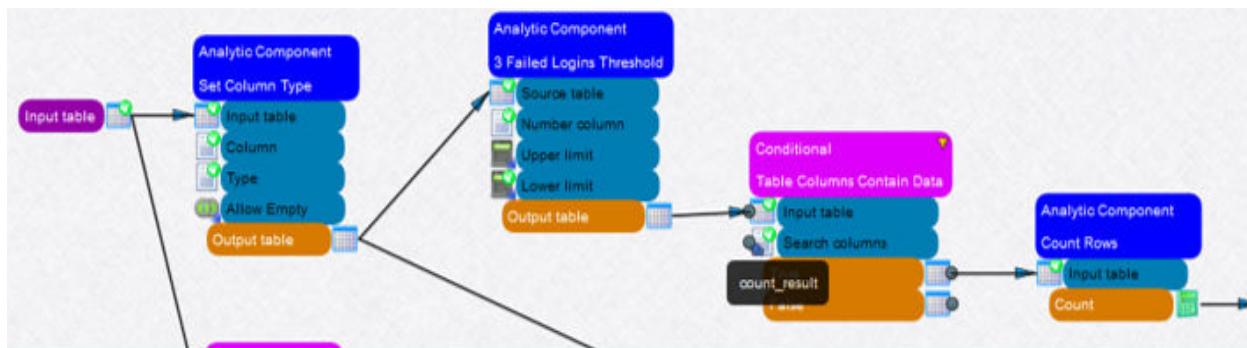
After the type conversion, the results go the threshold filter, again using **count_result** as the desired column for comparison to the threshold, which in this case is a Lower Limit = 3 as shown below:

Figure 4-9: Sample Model Diagram (Dataflow)



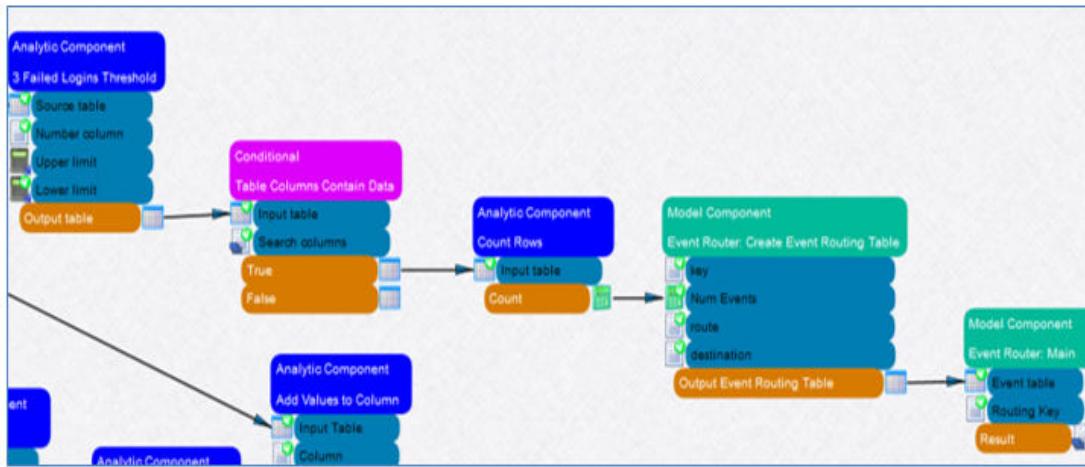
After the data is filtered, the model keeps only the rows in the table that have **count_result** values that are greater than 3; it checks to see if there is data in the table (since table columns contain data) and then counts the number of rows with values of **count_result** that crossed the threshold (note that Search column is set to **count_result**).

Figure 4-10: Count_result value for Sample Model



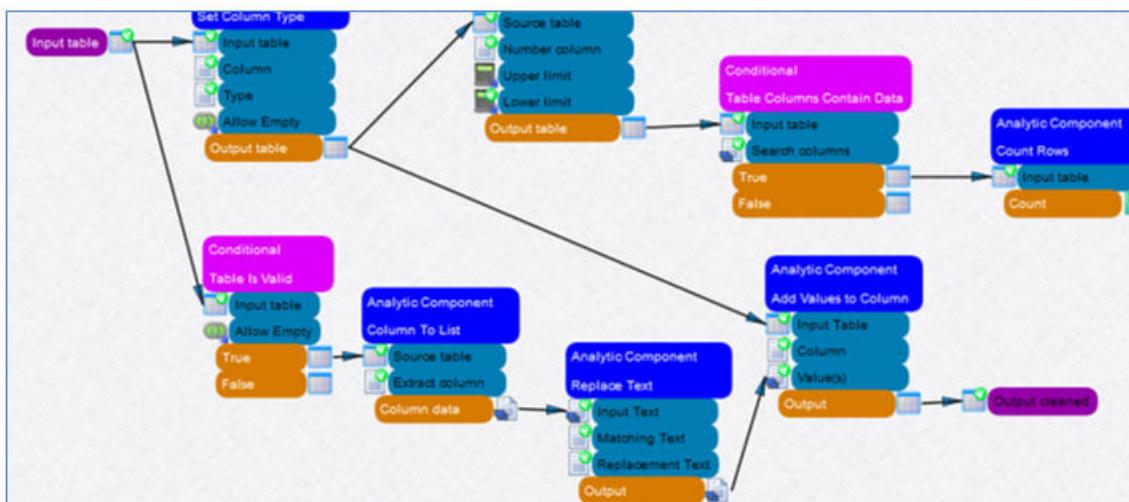
Next, it creates an event route table with an input key (Number of Failed Logins > 3), route (Email), and destination, (someone@this.org). Finally, the model sends the resulting event results to the destination (Event Router: Main embedded model with a Routing key of Email).

Figure 4-11: Event Results Sent to Destination for Sample Model



The bottom portion of the diagram takes the original report output table and does some simple string manipulation for proper formatting of the timestamp (that is, Day, which is named **date_trunc_ts** in the original report SQL; note that the **date_trunc_ts** column name is needed here as well) and sends it back as an output table, which is then sent back to the report for visualization of the report results.

Figure 4-12: Timestamp Format and Visualization of Report Results for Sample Model



CHAPTER 5

IntelliSchema Views Reference

The reference material in this chapter describes the IntelliSchema views you can use to create reports on event data. You can use these views to create reports on specific event types from one or more types of information systems. Each view also references a *connector view*. Connector views query event data stored in a single table to create a view focused on a particular type of event. Each Event Data Warehouse (EDW) table that can be queried by IntelliSchema views has a connector view for each event type.

This chapter contains the following topics:

- “About IntelliSchema Views”, next
- “IntelliSchema Event Type Reference”, on page 93
- “Connector Views and IntelliSchema Views”, on page 150
- “Reference Tables”, on page 164
- “Adding New Event Sources to IntelliSchema”, on page 165

ABOUT INTELLISchema VIEWS

This section provides a reference for IntelliSchema views. For each view, the following information is provided:

- **Description**—Describes the type of data returned by the view.
- **IntelliSchema View Name**—Use this name to reference the view in an SQL statement.
- **Look-up file**—Some views use a "look-up" file to normalize data, for instance, mapping error codes to their descriptions.
- **Columns and Datatypes**— Describes the available columns and their datatypes.
- **Related Views**—Some views have related views that query only specific information systems.
- **Connector Views Referenced**—Lists the connector views referenced by this view.

INTELLISchema EVENT TYPE REFERENCE

The table below lists the event types and their associated IntelliSchema event-type views, which you can use to create reports. Click a cross-reference from the Event Type View column to view additional information about each view.

Event Type	Description	Event-Type Views
Account Addition and Deletion	User accounts added or deleted	<ul style="list-style-type: none">• “Account Addition and Deletion”, on page 95• “Account Addition and Deletion: Windows”, on page 97
Administrative Account Activity	Events that use administrative accounts	<ul style="list-style-type: none">• “Administrative Account Activity”, on page 98• “Administrative Account Activity: Windows”, on page 100
Alert Event	Alerts for all information systems.	<ul style="list-style-type: none">• “Alert Event”, on page 101

Event Type	Description	Event-Type Views
Application Event	Application events for all information systems	<ul style="list-style-type: none"> “Application Event”, on page 102
Arcsight CEF Forwarder	Events for logs in the ArcSight Common Event Format	<ul style="list-style-type: none"> “Arcsight CEF Forwarder Event”, on page 103
Audit Events	Audit events for all information systems	<ul style="list-style-type: none"> “Audit Event”, on page 109
Database DDL	DDL events in databases	<ul style="list-style-type: none"> “Database DDL (Data Definition Language)”, on page 111
Database DML	DML events in databases	<ul style="list-style-type: none"> “Database DML (Data Manipulation Language)”, on page 111
IDS/IPS	Events for all Intrusion Detection (IDS) and Intrusion Prevention (IPS) Systems.	<ul style="list-style-type: none"> “IDS/IPS Event”, on page 113
Investigation	Investigate real-time alerts	<ul style="list-style-type: none"> “Audit Event”, on page 109
Loss of Audit Messages	Number of lost audit message.	<ul style="list-style-type: none"> “Loss of Audit Messages”, on page 117 “Loss of Audit Messages: Windows”, on page 118
Mail	Events for all mail systems	<ul style="list-style-type: none"> “Mail Event”, on page 119
Malware	Events for information about malwares	<ul style="list-style-type: none"> “Malware Event”, on page 120
Network Device Connection	Connections to network devices	<ul style="list-style-type: none"> “Network Device Connection”, on page 121 “Network Device Connection: Router”, on page 122 “Network Device Connection: Firewall”, on page 123
Parsed Data	Parsed data from all information systems.	<ul style="list-style-type: none"> “Parsed Data”, on page 124
Password Changes and Resets	Changes and resets of user passwords	<ul style="list-style-type: none"> “Password Changes and Resets”, on page 127 “Password Changes and Resets: Windows”, on page 128
Privileged Command	Commands executed by users with administrative or root access	<ul style="list-style-type: none"> “Privileged Commands”, on page 129 “Privileged Commands: BSM”, on page 130 “Privileged Commands: Linux/Unix”, on page 131 “Privileged Commands: Windows”, on page 132
Remote access	Events initiated by remote accessing	<ul style="list-style-type: none"> “Remote Access Event”, on page 133
Security Objects	Security Objects Accessed or Deleted	<ul style="list-style-type: none"> “Security Objects”, on page 134 “Security Objects: Windows”, on page 135
System Startup and Shutdown	Startup and Shutdown events	<ul style="list-style-type: none"> “System Startup and Shutdown”, on page 136 “Startup and Shutdown: BSM”, on page 138 “Startup and Shutdown: Windows”, on page 137
Unparsed Data	Parsed data from all information systems.	<ul style="list-style-type: none"> “Unparsed Data”, on page 139

Event Type	Description	Event-Type Views
User Logins	User logins	<ul style="list-style-type: none"> “Unparsed Data”, on page 139 “User Logins: Router”, on page 143 “User Logins: Windows”, on page 144 “User Logins: Windows Non-domain Controller”, on page 145 “User Logins: Windows”, on page 146 “User Logins: Linux/Unix”, on page 147
Vulnerability	Events with information about vulnerabilities	• “Security Objects”, on page 134
webProxy	Web proxy-specific information from all information systems	• “webProxy Event”, on page 149
Wireless	Wireless-specific information from all information systems.	• “Wireless Event”, on page 149

ACCOUNT ADDITION AND DELETION

User accounts added or deleted.

IntelliSchema View Name: accountAdditionAndDeletion

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	<p>Time the account addition or deletion occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format.</p> <p>Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.</p>
log_type	String (text)	Event-log source that recorded the account addition or deletion
info_sys	String (text)	Machine where the account addition or deletion occurred
user_added_deleted	String (text)	User account added or deleted
event_description	String (text)	Description of process that deleted or added the user account.
role	String (text)	Role of domain (“MemberServer” or “DomainController”)

The following Account Addition and Deletion event-type views are also available to create more specialized reports:

- “[Account Addition and Deletion: Windows](#)”, on page 97

CONNECTOR VIEWS REFERENCED

- accountAdditionAndDeletion__oracle__adump
- accountAdditionAndDeletion__oracle__adump__syslogng
- accountAdditionAndDeletion__oracle__database__sysaudit__sensageRetriever
- accountAdditionAndDeletion__microsoft__sql__sensageRetriever
- accountAdditionAndDeletion__microsoft__exchange__mailbox__events__syslogng
- accountAdditionAndDeletion__microsoft__exchange__admin__events__syslogng
- accountAdditionAndDeletion__windows__microsoft_windows2008_securityEvent_sensag eRetriever
- accountAdditionAndDeletion__windows__microsoft_windows2008_securityEvent_snare
- accountAdditionAndDeletion__windows__microsoft_windows_securityEvent__ sensageRetriever
- accountAdditionAndDeletion__windows__microsoft_windows_securityEvent_snare

Account Addition and Deletion: Windows

User accounts added or deleted on Microsoft Windows systems.

IntelliSchema View Name: accountAdditionAndDeletion_windows

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	<p>Time the account addition or deletion occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format.</p> <p>Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.</p>
log_type	String (text)	Event-log source that recorded the account addition or deletion
info_sys	String (text)	Machine where the account addition or deletion occurred
domain	String (text)	Windows domain where the account was added or deleted
caller_user_name	String (text)	User ID used to add or delete the account
user_added_deleted	String (text)	User account added or deleted
eventid	Numeric	Event ID of process that added or deleted the user account
event_description	String (text)	Description of event that added or deleted the user account.
role	String (text)	Role of domain ("MemberServer" or "DomainController")

CONNECTOR VIEWS REFERENCED

- accountAdditionAndDeletion_windows_microsoft_windows_securityEvent_snare
- accountAdditionAndDeletion_windows_microsoft_windows_securityEvent_sensageRetriever
- accountAdditionAndDeletion_windows_microsoft_windows2008_securityEvent_snare
- accountAdditionAndDeletion_windows_microsoft_windows2008_securityEvent_sensageRetriever

ADMINISTRATIVE ACCOUNT ACTIVITY

Events that use accounts with administrative privileges.

IntelliSchema View Name: adminAccountActivity

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the administrative account activity occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
log_type	String (text)	Event-log source that recorded the account addition or deletion
info_sys	String (text)	Machine where the account addition or deletion occurred
account_done_by	String (text)	User ID used for the administrative activity
account_target	String (text)	User account targeted by the administrative activity
action	String (text)	Action performed by the administrative activity

The following Administrative Account Activity event-type views are also available to create more specialized reports:

[“Account Addition and Deletion: Windows”, on page 97](#)

CONNECTOR VIEWS REFERENCED

- adminAccountActivity_windows_microsoft_windows_securityEvent_sensageRetriever
- adminAccountActivity_windows_microsoft_windows_securityEvent_snare
- adminAccountActivity_windows_microsoft_windows2008_securityEvent_sensageRetriever
- adminAccountActivity_windows_microsoft_windows2008_securityEvent_snare

Administrative Account Activity: Linux/unix

Events that use accounts with administrative privileges on Microsoft Windows systems.

IntelliSchema View Name: adminAccountActivity_unix

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	<p>Time the administrative account activity occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format.</p> <p>Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.</p>
log_type	String (text)	Event-log source that recorded the account addition or deletion
info_sys	String (text)	Machine where the account addition or deletion occurred
account_done_by	String (text)	User ID used for the administrative activity
account_target	String (text)	User account targeted by the administrative activity
action	String (text)	Action performed by the administrative activity

CONNECTOR VIEWS REFERENCED

None.

Administrative Account Activity: Windows

Events that use accounts with administrative privileges on Microsoft Windows systems.

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the administrative account activity occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
log_type	String (text)	Event-log source that recorded the account addition or deletion
info_sys	String (text)	Machine where the account addition or deletion occurred
account_done_by	String (text)	User ID used for the administrative activity
account_target	String (text)	User account targeted by the administrative activity
action	String (text)	Action performed by the administrative activity

CONNECTOR VIEWS REFERENCED

- adminAccountActivity_windows_microsoft_windows_securityEvent_sensageRetriever
- adminAccountActivity_windows_microsoft_windows_securityEvent_snare
- adminAccountActivity_windows_microsoft_windows2008_securityEvent_sensageRetriever
- adminAccountActivity_windows_microsoft_windows2008_securityEvent_snare

ALERT EVENT

Alert events for all information systems.

IntelliSchema View Name: alert

COLUMNS

Column	Datatype	Description
ts	timestamp	Time event occurred
log_type	String (text)	Event Source
src_info_sys	String (text)	Source Information system
dest_info_sys	String (text)	Destination Information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
src_account	String (text)	Affected account
event_description	String (text)	Event description
result	String (text)	Possible result of alert
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

- alert__apache_error_syslogng
- alert__cisco_acs_syslogng
- alert__hp_proCurve_tmsz_syslogng
- alert__mcafee_scm_batch
- alert__oracle_alert
- alert__panos_firewall_syslogng
- alert__symantec_endpoint_syslogng
- alert__vmware_esx_vcenter_event_collection

APPLICATION EVENT

Application events for all information systems.

IntelliSchema View Name: event

Look-up File: result.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time event occurred
log_type	String (text)	Event Source
src_info_sys	String (text)	Source Information system
dest_info_sys	String (text)	Destination Information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
src_account	String (text)	Affected account
event_description	String (text)	Event description
result	Numeric	Possible values: • -1 Unknown • 0 Failure • 1 Success
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

- application_catbird_vsecurity_cef_syslogng
- application_cisco_ios_syslogng
- application_microsoft_sharepoint
- application_microsoft_windows2008_appEvent_sensageRetriever
- application_microsoft_windows2008_dirEvent_sensageRetriever
- application_microsoft_windows2008_dnsEvent_sensageRetriever
- application_microsoft_windows2008_frsEvent_sensageRetriever
- application_microsoft_windows2008_sysEvent_sensageRetriever
- application_microsoft_windows_appEvent_sensageRetriever
- application_microsoft_windows_dirEvent_sensageRetriever
- application_microsoft_windows_dnsEvent_sensageRetriever
- application_microsoft_windows_frsEvent_sensageRetriever
- application_microsoft_windows_sysEvent_sensageRetriever
- application_sap_aud_sftp

ARCSIGHT CEF FORWARDER EVENT

Events for logs in the ArcSight Common Event Format.

IntelliSchema View Name: arcsightCefForwarder

Look-up File: result.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the connection occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
applicationProtocol	String (text)	Application level protocol, example values are: HTTP, HTTPS, SSHv2, Telnet, POP, IMAP, IMAPS, etc.
baseEventCount	Numeric	A count associated with this event. How many times was this same event observed?
bytesIn	Numeric	Number of bytes transferred inbound. Inbound relative to the source to destination relationship, meaning that data was flowing from source to destination
bytesOut	Numeric	Number of bytes transferred outbound relative to the source to destination relationship. For example, the byte number of data flowing from the destination to the source.
cef_version	String (text)	Version of the CEF format
destinationAddress	String (text)	Identifies the destination address that the event refers to in an IP network. The format is an IPv4 address. Example: "192.168.10.1"
destinationDnsDomain	String (text)	The DNS domain part of the complete fully qualified domain name (FQDN).
destinationHostName	String (text)	Identifies the destination that an event refers to in an IP network. The format should be a fully qualified domain name associated with the destination node, when a node is available (FQDN). Examples: "host.domain.com"or "host"
destinationMacAddress	String (text)	Six colon-separated hexadecimal numbers. Example: "00:0D:60:AF:1B:61"
destinationNtDomain	String (text)	The Windows domain name of the destination address.
destinationPort	Numeric	The valid port numbers are between 0 and 65535

Column	Datatype	Description
destinationProcessName	String (text)	The name of the event's destination process. Example: "telnetd", or "sshd"
destinationUserId	String (text)	Identifies the destination user by ID. For example, in UNIX, the root user is generally associated with user ID 0.
destinationUserName	String (text)	Identifies the destination user by name. This is the user associated with the event's destination. Email addresses are often mapped into the UserName fields. The recipient is a candidate to put into destinationUserName.
destinationUserPrivileges	String (text)	The typical values are: "Administrator", "User", and "Guest". This identifies the destination user's privileges. In UNIX, for example, activity executed on the root user would be identified with destinationUserPrivileges of "Administrator".
deviceAction	String (text)	Action taken by the device.
deviceAddress	String (text)	Identifies the device address that an event refers to in an IP network. The format is an IPv4 address. Example: "192.168.10.1"
deviceCustomDate1	String (text)	One of two timestamp fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomDate1Label	String (text)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomDate2	String (text)	One of two timestamp fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomDate2Label	String (text)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomIPv6Address1	String (text)	One of four IPV6 address fields available to map fields that do not apply to any other in this dictionary.
deviceCustomIPv6Address1Label	String (text)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomIPv6Address2	String (text)	One of four IPV6 address fields available to map fields that do not apply to any other in this dictionary.
deviceCustomIPv6Address2Label	String (text)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomNumber1	Numeric	One of three number fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.

Column	Datatype	Description
deviceCustomNumber1Label	String (text)	All custom fields have a corresponding label field where the field itself can be described. Each of the fields is a string describing the purpose of this field.
deviceCustomNumber2	Numeric	One of three number fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomNumber2Label	String (text)	All custom fields have a corresponding label field where the field itself can be described. Each of the fields is a string describing the purpose of this field.
deviceCustomNumber3	Numeric	One of three number fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomNumber3Label	String (text)	All custom fields have a corresponding label field where the field itself can be described. Each of the fields is a string describing the purpose of this field
deviceCustomString1	String (text)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible
deviceCustomString1Label	String (text)	All custom fields have a corresponding label field where the field itself can be described. Each of the fields is a string describing the purpose of this field.
deviceCustomString2	String (text)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible
deviceCustomString2Label	String (text)	All custom fields have a corresponding label field where the field itself can be described. Each of the fields is a string describing the purpose of this field.
deviceCustomString3	String (text)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomString3Label	String (text)	All custom fields have a corresponding label field where the field itself can be described. Each of the fields is a string describing the purpose of this field.
deviceCustomString4	String (text)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible
deviceCustomString4Label	String (text)	All custom fields have a corresponding label field where the field itself can be described. Each of the fields is a string describing the purpose of this field.

Column	Datatype	Description
deviceCustomString5	String (text)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible
deviceCustomString5Label	String (text)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible
deviceCustomString6	String (text)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible
deviceCustomString6Label	String (text)	All custom fields have a corresponding label field where the field itself can be described. Each of the fields is a string describing the purpose of this field.
deviceDirection	Numeric	Any information about what direction the observed communication has taken. The following values are supported: "0" for inbound or "1" for outbound
deviceDnsDomain	String (text)	The DNS domain part of the complete fully qualified domain name (FQDN).
deviceEventCategory	String (text)	Represents the category assigned by the originating device. Devices oftentimes use their own categorization schema to classify events. Example: "/Monitor/Disk/Read"
deviceExternalId	String (text)	A name that uniquely identifies the device generating this event.
deviceFacility	String (text)	The facility generating this event. For example, Syslog has an explicit facility associated with every event
deviceHostName	String (text)	qualified domain name associated with the destination node, when a node is available (FQDN). Examples: "host.domain.com" or "host"
deviceInboundInterface	String (text)	Interface on which the packet or data entered the device.
deviceMacAddress	String (text)	Six colon-separated hexadecimal numbers. Example: "00:0D:60:AF:1B:61"
deviceNtDomain	String (text)	The Windows domain name of the device address.
deviceOutboundInterface	String (text)	Interface on which the packet or data left the device.
deviceProcessName	String (text)	Process name associated with the event. An example might be the process generating the syslog entry in UNIX.
deviceProduct	String (text)	Product name
deviceVendor	String (text)	Product vendor
deviceVersion	String (text)	Product version
deviceSeverity	Numeric	Integer and reflects the importance of the event

Column	Datatype	Description
endTime	String (text)	The time at which the activity related to the event ended. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st 1970). An example would be reporting the end of a session.
externalid	String (text)	The ID used by an originating device. They are usually increasing numbers, associated with events.
fileCreateTime	String (text)	Time when the file was created.
fileHash	String (text)	Hash of a file
fileId	String (text)	An ID associated with a file could be the inode.
fileModificationTime	String (text)	Time when the file was last modified
fileName	String (text)	Name of the file.
filePath	String (text)	Full path to the file, including file name itself. Example: C:\ProgramFiles\WindowsNT\Accessories\wordpad.exe or /usr/bin/zip
filePermission	String (text)	Permissions of the file.
fileSize	Numeric	Size of the file
fileType	String (text)	Type of file (pipe, socket, etc.)
message	String (text)	An arbitrary message giving more details about the event. Multi-line entries can be produced by using \n as the new line separator
name	String (text)	String representing a human-readable and understandable description of the event
oldFileCreateTime	String (text)	Time when old file was created.
oldFileHash	String (text)	Hash of the old file.
oldFileId	String (text)	An ID associated with the old file could be the inode.
oldFileModificationTime	String (text)	Time when old file was last modified.
oldFileName	String (text)	Name of the old file.
oldFilePath	String (text)	Full path to the old file, including the file name itself. Examples: C:\ProgramFiles\WindowsNT\Accessories\wordpad.exe and /usr/bin/zip
oldFilePermission	String (text)	Permissions of the old file.
oldFileSize	String (text)	Size of the old file.
oldFileType	String (text)	Type of the old file (pipe, socket, etc.)
requestClientApplication	String (text)	The User-Agent associated with the request.
RequestMethod	String (text)	The method used to access a URL. Possible values: "POST", "GET"
requestUrl	String (text)	In the case of an HTTP request, this field contains the URL accessed. The URL should contain the protocol as well. Example: "http://www.security.com"

Column	Datatype	Description
receiptTime	String (text)	The time at which the event related to the activity was received. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st 1970).
signatureId	String (text)	Unique identifier per event-type
sourceAddress	String (text)	Identifies the source that an event refers to in an IP network. The format is an IPv4 address. Example: "192.168.10.1"
sourceDnsDomain	String (text)	The DNS domain part of the complete fully qualified domain name (FQDN).
sourceHostName	String (text)	Identifies the source that an event refers to in an IP network. The format should be a fully qualified domain name associated with the source node, when a node is available (FQDN). Examples: "host.domain.com"or "host"
sourceMacAddress	String (text)	Six colon-separated hexadecimal numbers. Example: "00:0D:60:AF:1B:61"
sourceNtDomain	String (text)	The Windows domain name for the source address.
sourcePort	Numeric	The valid port numbers are 0 to 65535.
sourceProcessId	Numeric	The ID of the source process associated with the event.
sourceProcessName	String (text)	The name of the event's source process.
sourceServiceName	String (text)	The service which is responsible for generating this event.
sourceUserId	String (text)	Identifies the source user by ID. This is the user associated with the source of the event. For example, in UNIX, the root user is generally associated with user ID 0.
sourceUserName	String (text)	Identifies the source user by name. Email addresses are also mapped into the UserName fields. The sender is a candidate to put into sourceUserName
sourceUserPrivileges	String (text)	The typical values are: "Administrator", "User", and "Guest". It identifies the source user's privileges. In UNIX, for example, activity executed by the root user would be identified with sourceUserPrivileges of "Administrator".
transportProtocol	String (text)	Identifies the Layer-4 protocol used. The possible values are protocols such as TCP or UDP.
cryptoSignature	String (text)	Legacy item. Left for compatibility with older versions of the protocol.
deviceDomain	String (text)	Legacy item. Left for compatibility with older versions of the protocol.
deviceEventClassId	String (text)	Legacy item. Left for compatibility with older versions of the protocol.
devicePayloadId	String (text)	Legacy item. Left for compatibility with older versions of the protocol.

Column	Datatype	Description
deviceReceiptTime	String (text)	Legacy item. Left for compatibility with older versions of the protocol.
flexDate1	String (text)	Legacy item. Left for compatibility with older versions of the protocol.
flexDateLabel	String (text)	Legacy item. Left for compatibility with older versions of the protocol
flexNumber1	Numeric	Legacy item. Left for compatibility with older versions of the protocol.
flexNumber1Label	String (text)	Legacy item. Left for compatibility with older versions of the protocol.
flexNumber2	Numeric	Legacy item. Left for compatibility with older versions of the protocol.
flexNumber2Label	String (text)	Legacy item. Left for compatibility with older versions of the protocol.
flexString1	String (text)	Legacy item. Left for compatibility with older versions of the protocol.
flexString1Label	String (text)	Legacy item. Left for compatibility with older versions of the protocol.
flexString2	String (text)	Legacy item. Left for compatibility with older versions of the protocol.
flexString2Label	String (text)	Legacy item. Left for compatibility with older versions of the protocol.
requestCookies	String (text)	Cookies associated with the request.

CONNECTOR VIEWS REFERENCED

- arcsight_cef_bluecoat_sgproxy_batch
- arcsight_cef_catbird_vsecurity_cef_syslogng
- arcsight_cef_cisco_ironport_maillog_syslogng
- arcsight_cef_f5_asm_cef_syslogng
- arcsight_cef_mcafee_database_activity_monitoring_syslogng
- arcsight_cef_microsoft_windows2008_securityEvent_sensageRetriever
- arcsight_cef_unix_ftpd_syslogng
- arcsight_cef_unix_login_syslogng
- arsight_cef_unix_sshd2_syslogng
- arsight_cef_unix_sudo_syslogng
- arcsight_cef_unix_su_syslogng

AUDIT EVENT

Audit events for all information systems.

IntelliSchema View Name: audit

Look-up File: result.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time event occurred
log_type	String (text)	Event Source
src_info_sys	String (text)	Source Information system
dest_info_sys	String (text)	Destination Information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
src_account	String (text)	Affected account
event_description	String (text)	Event description
result	Numeric	Possible values: <ul style="list-style-type: none">• -1 Unknown• 0 Failure• 1 Success
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

- audit__apache_error_syslogng
- audit__mcafee_epo45_audit_rdbms
- audit__mcafee_epo46_audit_sensageRetriever
- audit__mcafee_epo51_audit_sensageRetriever
- audit__mcafee_epo_audit_rdbms
- audit__microsoft_exchange_admin_events_syslogng
- audit__oracle_adump
- audit__oracle_adump_syslogng
- audit__oracle_database_fga_sensageRetriever
- audit__oracle_database_sysaudit_sensageRetriever
- audit__oracle_listener
- audit__sun_bsm_sftp
- audit__unix_sshd2_syslogng
- audit__unix_sudo_syslogng
- audit__unix_su_syslogng
- audit__vmware_esx_vcenter_event_collection
- audit__vmware_esx_vcenter_log_collection

DATABASE DDL (DATA DEFINITION LANGUAGE)

DDL events in databases.

IntelliSchema View Name: database_ddl

Look-up File: result.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the event occurred
log_type	String (text)	Event Source
src_info_sys	String (text)	Source Information system
dest_info_sys	String (text)	Destination Information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
src_account	String (text)	Account that initiates DB action
event_description	String (text)	DDL statement
result	Numeric	Possible values: • -1 Unknown • 0 Failure • 1 Success
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

- database_ddl_ibm_db2_rdbms
- database_ddl_mcafee_database_activity_monitoring_syslogng
- database_ddl_microsoft_sql_sensageRetriever
- database_ddl_oracle_adump
- database_ddl_oracle_adump_syslogng
- database_ddl_oracle_alert
- database_ddl_oracle_database_fga_sensageRetriever
- database_ddl_oracle_database_sysaudit_sensageRetriever
- database_ddl_oracle_fga_xml_batch
- database_ddl_postgres_audit_csv

DATABASE DML (DATA MANIPULATION LANGUAGE)

DML events in databases.

IntelliSchema View Name: database_dml

Look-up File: result.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the event occurred
log_type	String (text)	Event Source
src_info_sys	String (text)	Source Information system
dest_info_sys	String (text)	Destination Information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
src_account	String (text)	Affected account
event_description	String (text)	Event description
result	Numeric	Possible values: <ul style="list-style-type: none">• -1 Unknown• 0 Failure• 1 Success
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

- database_ddl_ibm_db2_rdbms
- database_ddl_mcafee_database_activity_monitoring_syslogng
- database_ddl_microsoft_sql_sensageRetriever
- database_ddl_oracle_adump
- database_ddl_oracle_adump_syslogng
- database_ddl_oracle_alert
- database_ddl_oracle_database_fga_sensageRetriever
- database_ddl_oracle_database_sysaudit_sensageRetriever
- database_ddl_oracle_fga_xml_batch
- database_ddl_postgres_audit_csv

IDS/IPS EVENT

Events for all Intrusion Detection (IDS) and Intrusion Prevention (IPS) Systems.

IntelliSchema View Name: idsIps

Look-up File: result.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the event occurred
log_type	String (text)	Event Source
src_info_sys	String (text)	Source Information system
dest_info_sys	String (text)	Destination Information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
src_account	String (text)	Account that initiates DB action
event_description	String (text)	DDL statement
result	Numeric	Possible values: • -1 Unknown • 0 Failure • 1 Success
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

- idsIps__checkpoint_opsec_lea
- idsIps__cisco_asa_syslogng
- idsIps__mcafee_intrushield_rdbms
- idsIps__mcafee_intrushield_syslogng
- idsIps__tipping_point_syslogng

INVESTIGATION EVENT

The Investigation Event view is a special view that queries all tables in the EDW that have Investigation connector views. (See [Connector Views Referenced](#), below.) These connector views are installed as part of a standard IntelliSchema installation. You must also install the standard log adapters to make this functionality available.

IntelliSchema View Name: investigation

COLUMNS

Column	Datatype	Description
ts	timestamp	Time event occurred
log_type	String (text)	Event Source
src_account	String (text)	Source Account
dest_account	String (text)	Destination Account
src_info_sys	String (text)	Source Information system
dest_info_sys	String (text)	Destination Information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

- investigation__apache_access_syslogng
- investigation__bluecoat_sgproxy_batch
- investigation__catbird_vsecurity_cef_syslogng
- investigation__checkpoint_opsec_lea
- investigation__cisco_acs_syslogng
- investigation__cisco_asa_syslogng
- investigation__cisco_ios_syslogng
- investigation__cisco_ips_syslogng
- investigation__cisco_ironport_maillog_syslogng
- investigation__cisco_netflow_receiver
- investigation__cisco_pix_syslogng
- investigation__f5_asm_cef_syslogng
- investigation__hp_proCurve_t3t4_syslogng
- investigation__hp_proCurve_tmsz_syslogng
- investigation__ibm_db2_rdbms
- investigation__juniper_netscreenFw_syslogng

- investigation__mcafee_database_activity_monitoring
- investigation__mcafee_epo45_audit_rdbms
- investigation__mcafee_epo45_event_rdbms
- investigation__mcafee_epo46_audit_sensageRetriever
- investigation__mcafee_epo46_event_sensageRetriever
- investigation__mcafee_epo51_audit_sensageRetriever
- investigation__mcafee_epo51_event_sensageRetriever
- investigation__mcafee_epo_audit_rdbms
- investigation__mcafee_epo_event_rdbms
- investigation__mcafee_foundstone_rdbms
- investigation__mcafee_intrushield_rdbms
- investigation__mcafee_intrushield_syslogng
- investigation__mcafee_scm_batch
- investigation__microsoft_exchange_admin_events_syslogng
- investigation__microsoft_exchange_mailbox_events_syslogng
- investigation__microsoft_exchange_tracking_sensageRetrieverAgent
- investigation__microsoft_iis
- investigation__microsoft_sharepoint
- investigation__microsoft_sql_sensageRetriever
- investigation__microsoft_windows2008_securityEvent_sensageRetriever
- investigation__microsoft_windows2008_securityEvent_snare
- investigation__microsoft_windows_securityEvent_sensageRetriever
- investigation__microsoft_windows_securityEvent_snare
- investigation__oracle_adump
- investigation__oracle_adump_syslogng
- investigation__oracle_database_fga_sensageRetriever
- investigation__oracle_database_sysaudit_sensageRetriever
- investigation__oracle_fga_xml_batch
- investigation__oracle_listener
- investigation__panos_firewall_syslogng
- investigation__postgres_audit_csv
- investigation__sap_aud_sftp

- investigation_sun_bsm_sftp
- investigation_syslogng_catchall_syslogng
- investigation_tipping_point_syslogng
- investigation_unix_ftpd_syslogng
- investigation_unix_login_syslogng
- investigation_unix_sshd2_syslogng
- investigation_unix_sudo_syslogng
- investigation_unix_su_syslogng
- investigation_vmware_esx_500_syslogng
- investigation_vmware_esx_vcenter_event_collection

LOSS OF AUDIT MESSAGES

Number of lost audit messages.

IntelliSchema View Name: lossOfAuditMessages

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the audit message loss occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
log_type	String (text)	Event-log source for which audit messages were lost
info_sys	String (text)	Machine where the audit messages were lost
event_description	String (text)	Event causing the loss of audit messages
no_audit_messages_lost	String (text)	Number of lost audit messages

See also: “[Loss of Audit Messages: Windows](#)”, next

CONNECTOR VIEWS REFERENCED

- `lossOfAuditMessages__windows__microsoft_windows_securityEvent_snare`
- `lossOfAuditMessages__windows__microsoft_windows_securityEvent_sensageRetriever`
- `lossOfAuditMessages__windows__microsoft_windows2008_securityEvent_snare`
- `lossOfAuditMessages__windows__microsoft_windows2008_securityEvent_sensageRetriever`

Loss of Audit Messages: Windows

Number of lost audit messages on Microsoft Windows systems.

IntelliSchema View Name: lossOfAuditMessages_windows

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the audit message loss occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
log_type	String (text)	Event-log source for which audit messages were lost
info_sys	String (text)	Machine where the audit messages were lost
event_description	String (text)	Description of the event that caused the loss of audit messages
no_audit_messages_lost	String (text)	Number of lost audit messages
eventid	String (text)	ID of event that caused the loss of audit messages

CONNECTOR VIEWS REFERENCED

- lossOfAuditMessages_windows_microsoft_windows_securityEvent_snare
- lossOfAuditMessages_windows_microsoft_windows_securityEvent_sensageRetriever
- lossOfAuditMessages_windows_microsoft_windows2008_securityEvent_snare
- lossOfAuditMessages_windows_microsoft_windows2008_securityEvent_sensageRetriever

MAIL EVENT

Events for all mail systems.

IntelliSchema View Name: mail

Look-up file: result.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the event occurred.
log_type	String (text)	Event source
src_info_sys	String (text)	Source information system
dest_info_sys	String (text)	Desitnation information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
src_account	String (text)	Source account (sender)
dst_account	String (text)	Destination account (recipient)
total_bytes	Numeric	Size in bytes of mail
event_description	String (text)	Event description
result	Numeric	Possible values: • -1 Unknown • 0 Failure • 1 Success
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

- mail__mcafee_scm_batch
- mail__microsoft_exchange_mailbox_events_syslogng
- mail__microsoft_exchange_tracking_sensageRetrieverAgent

MALWARE EVENT

Events with information about malwares.

IntelliSchema View Name: malware

Look-up file: result.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the event occurred.
log_type	String (text)	Event source
src_info_sys	String (text)	Source information system
dest_info_sys	String (text)	Desitnation information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
src_account	String (text)	Affected account
dst_account	String (text)	Destination account (recipient)
total_bytes	Numeric	Size in bytes of mail
event_description	String (text)	Malware name
result	Numeric	Possible values: • -1 Unknown • 0 Failure • 1 Success
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

- malware__mcafee_epo45_event_rdbms
- malware__mcafee_epo46_event_sensageRetriever
- malware__mcafee_epo51_event_sensageRetriever
- malware__mcafee_epo_event_rdbms
- malware__mcafee_epo_rdbms
- malware__mcafee_scm_batch
- malware__symantec_endpoint_syslogng

NETWORK DEVICE CONNECTION

Connections to network devices.

IntelliSchema View Name: networkDeviceConnection

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the connection occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
info_sys	String (text)	Machine connected to
log_type	String (text)	Event-log source that recorded the connection
protocol	String (text)	Protocol used for the connection
src_ip	String (text)	Source IP address
dest_ip	String (text)	Destination IP address
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
result	Numeric	Result: <ul style="list-style-type: none">• Unknown• Denied• Accepted
direction	String (text)	Direction of the connection
bytes	Numeric	Total bytes transferred

The following Network Device Connection event-type views are also available to create more specialized reports:

- “[Network Device Connection: Router](#)”, on page 122
- “[Network Device Connection: Firewall](#)”, on page 123

CONNECTOR VIEWS REFERENCED

- networkDeviceConnection_catbird_vsecurity_cef_syslogng
- networkDeviceConnection_cisco_netflow_receiver
- networkDeviceConnection_f5_asm_cef_syslogng
- networkDeviceConnection_hp_proCurve_tmsz_syslogng
- networkDeviceConnection_oracle_adump
- networkDeviceConnection_oracle_adump_syslogng

- networkDeviceConnection__oracle_listener
- networkDeviceConnection__firewall_checkpoint_opsec_lea
- networkDeviceConnection__firewall_cisco_asa_syslogng
- networkDeviceConnection__firewall_cisco_pix_syslogng
- networkDeviceConnection__firewall_juniper_netscreenFw_syslogng
- networkDeviceConnection__router_cisco_ios_syslogng

Network Device Connection: Router

Connections to Routers.

IntelliSchema View Name: networkDeviceConnection__router

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the connection occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
info_sys	String (text)	Machine connected to
log_type	String (text)	Event-log source that recorded the connection
protocol	String (text)	Protocol used for connection
src_ip	String (text)	Source IP address
dest_ip	String (text)	Destination IP address
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
result	Numeric	Result: <ul style="list-style-type: none">• Unknown• Denied• Accepted
severity	String (text)	Syslog severity level
acl_name	String (text)	ACL used to authorize the connection
facility	String (text)	Syslog facility name

CONNECTOR VIEWS REFERENCED

- networkDeviceConnection__router_cisco_ios_syslogng

Network Device Connection: Firewall

Connections to firewalls.

IntelliSchema View Name: networkDeviceConnection_firewall

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	<p>Time the connection occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format.</p> <p>Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.</p>
info_sys	String (text)	Machine connected to
log_type	String (text)	Event-log source that recorded the connection
protocol	String (text)	Protocol
src_ip	String (text)	Source IP address
dest_ip	String (text)	Destination IP address
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
result	Numeric	<p>Result:</p> <ul style="list-style-type: none"> • Unknown • Denied • Accepted
severity	String (text)	Severity
rule	String (text)	Firewall rule

CONNECTOR VIEWS REFERENCED

- networkDeviceConnection_firewall_checkpoint_opsec_lea
- networkDeviceConnection_firewall_cisco_pix_syslogng
- networkDeviceConnection_firewall_juniper_netscreenFw_syslogng

PARSSED DATA

Parsed data from all information systems.

IntelliSchema View Name: parsedData

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the event occurred.
log_type	String (text)	Event source
unparsed_message	String (text)	Original data
AUDIT_PARSE_SUCCESS	Numeric	1 if data parsed

CONNECTOR VIEWS REFERENCED

- unparsedData__apache_access_syslogng
- unparsedData__apache_error_syslogng
- unparsedData__bluecoat_sgproxy_batch
- unparsedData__catbird_vsecurity_cef_syslogng
- unparsedData__checkpoint_opsec_lea
- unparsedData__cisco_acs_syslogng
- unparsedData__cisco_asa_syslogng
- unparsedData__cisco_ios_syslogng
- unparsedData__cisco_netflow_receiver
- unparsedData__cisco_pix_syslogng
- unparsedData__hp_proCurve_t3t4_syslogng
- unparsedData__hp_proCurve_tmsz_syslogng
- unparsedData__ibm_db2_rdbms
- unparsedData__juniper_netscreenFw_syslogng
- unparsedData__mcafee_database_activity_monitoring_syslogng
- unparsedData__mcafee_epo45_audit_rdbms
- unparsedData__mcafee_epo45_event_rdbms
- unparsedData__mcafee_epo46_audit_sensageRetriever
- unparsedData__mcafee_epo46_event_sensageRetriever
- unparsedData__mcafee_epo51_audit_sensageRetriever
- unparsedData__mcafee_epo51_event_sensageRetriever
- unparsedData__mcafee_epo_audit_rdbms

- unparsedData__mcafee_epo_event_rdbms
- unparsedData__mcafee_epo_rdbms
- unparsedData__mcafee_foundstone_rdbms
- unparsedData__mcafee_intrushield_rdbms
- unparsedData__mcafee_intrushield_syslogng
- unparsedData__mcafee_scm_batch
- unparsedData__microsoft_dns_debug_sensageRetrieverAgent
- unparsedData__microsoft_exchange_admin_events_syslogng
- unparsedData__microsoft_exchange_mailbox_events_syslogng
- unparsedData__microsoft_exchange_tracking_sensageRetrieverAgent
- unparsedData__microsoft_iis
- unparsedData__microsoft_SharePoint_Audit_sensageRetrieverAgent
- unparsedData__microsoft_sql_sensageRetriever
- unparsedData__microsoft_windows2008_appEvent_sensageRetriever
- unparsedData__microsoft_windows2008_dirEvent_sensageRetriever
- unparsedData__microsoft_windows2008_dnsEvent_sensageRetriever
- unparsedData__microsoft_windows2008_frsEvent_sensageRetriever
- unparsedData__microsoft_windows2008_securityEvent_sensageRetriever
- unparsedData__microsoft_windows2008_securityEvent_snare
- unparsedData__microsoft_windows2008_sysEvent_sensageRetriever
- unparsedData__microsoft_windows_appEvent_sensageRetriever
- unparsedData__microsoft_windows_dirEvent_sensageRetriever
- unparsedData__microsoft_windows_dnsEvent_sensageRetriever
- unparsedData__microsoft_windows_frsEvent_sensageRetriever
- unparsedData__microsoft_windows_securityEvent_sensageRetriever
- unparsedData__microsoft_windows_securityEvent_snare
- unparsedData__microsoft_windows_sysEvent_sensageRetriever
- unparsedData__oracle_adump
- unparsedData__oracle_adump_syslogng
- unparsedData__oracle_alert
- unparsedData__oracle_database_fga_sensageRetriever
- unparsedData__oracle_database_sysaudit_sensageRetriever

- unparsedData__oracle_fga_xml_batch
- unparsedData__oracle_listener
- unparsedData__panos_firewall_syslogng
- unparsedData__postgres_audit_csv
- unparsedData__sap_aud_sftp
- unparsedData__sun_bsm_sftp
- unparsedData__symantec_endpoint_syslogng
- unparsedData__syslogng_catchall_syslogng
- unparsedData__tipping_point_syslogng
- unparsedData__unix_ftpd_syslogng
- unparsedData__unix_login_syslogng
- unparsedData__unix_sshd2_syslogng
- unparsedData__unix_sudo_syslogng
- unparsedData__unix_su_syslogng
- unparsedData__vmware_esx_500_syslogng
- unparsedData__vmware_esx_vcenter_event_collection
- unparsedData__vmware_esx_vcenter_log_collection

PASSWORD CHANGES AND RESETS

Changes and resets of user passwords.

IntelliSchema View Name: passwordChangeAndReset

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	<p>Time the password change occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format.</p> <p>Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.</p>
log_type	String (text)	Event-log source that recorded the password change or reset
info_sys	String (text)	Machine where the password change or reset occurred
domain	String (text)	Domain where the password change occurred
called_by	String (text)	User account used to change the password
target_user	String (text)	User account whose password was changed
eventid	Numeric	Event ID of process that changed password
status	String (text)	Outcome of the password change attempt

See also: “[Password Changes and Resets: Windows](#)”, next.

CONNECTOR VIEWS REFERENCED

- passwordChangeAndReset__microsoft_sql_sensageRetriever
- passwordChangeAndReset__oracle_database_sysaudit_sensageRetriever
- passwordChangeAndReset__windows__microsoft_windows2008_securityEvent_sensageRetriever
- passwordChangeAndReset__windows__microsoft_windows2008_securityEvent_snare
- passwordChangeAndReset__windows__microsoft_windows_securityEvent_sensageRetriever
- passwordChangeAndReset__windows__microsoft_windows_securityEvent_snare

Password Changes and Resets: Windows

Changes and resets of passwords on Microsoft Windows systems.

IntelliSchema View Name: passwordChangeAndReset__windows

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the password change occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
log_type	String (text)	Event-log source that recorded the password change or reset
info_sys	String (text)	Machine where the password change or reset occurred
domain	String (text)	Domain where the password change occurred
called_by	String (text)	User account used to change the password
target_user	String (text)	User account whose password was changed
eventid	String (text)	Event ID of process that changed password
status	String (text)	Outcome of the password change attempt

CONNECTOR VIEWS REFERENCED

- passwordChangeAndReset__windows__microsoft_windows_securityEvent_sensageRetriever
- passwordChangeAndReset__windows__microsoft_windows_securityEvent_snare
- passwordChangeAndReset__windows__microsoft_windows2008_securityEvent_sensageRetriever
- passwordChangeAndReset__windows__microsoft_windows2008_securityEvent_snare

PRIVILEGED COMMANDS

Commands executed by users with administrative or root access.

IntelliSchema View Name: privilegedCommand

Look-up file: privilegedCommand.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the privileged command execution occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
info_sys	String (text)	Machine where the privileged command was executed
log_type	String (text)	Event-log source that recorded the command execution
account	String (text)	User account
event_description	String (text)	Event description
result	Numeric	Result of privileged command. Possible values: <ul style="list-style-type: none">• Unknown• Failure• Success

The following additional Privileged Command event-type views are also available to create more specialized reports:

- “Privileged Commands: BSM”, on page 130
- “Privileged Commands: Linux/Unix”, on page 131
- “Privileged Commands: Windows”, on page 132

CONNECTOR VIEWS REFERENCED

- privilegedCommand__bsm_sun_bsm_sftp
- privilegedCommand__cisco_asa_syslogng
- privilegedCommand__microsoft_exchange_admin_events_syslogng
- privilegedCommand__microsoft_exchange_mailbox_events_syslogng
- privilegedCommand__oracle_adump
- privilegedCommand__oracle_adump_syslogng

- privilegedCommand__oracle_database_sysaudit_sensageRetriever
- privilegedCommand__unix_unix_sudo_syslogng
- privilegedCommand__unix_unix_su_syslog
- privilegedCommand__windows_microsoft_windows2008_securityEvent_sensageRetriever
- privilegedCommand__windows_microsoft_windows2008_securityEvent_snare
- privilegedCommand__windows_microsoft_windows_securityEvent_sensageRetriever
- privilegedCommand__windows_microsoft_windows_securityEvent_snare

Privileged Commands: BSM

Commands executed by users with administrative or root access on systems where Basic Security Module (BSM) is enabled.

IntelliSchema View Name: privilegedCommand__bsm

Look-up file: privilegedCommand.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the privileged command execution occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
info_sys	String (text)	Machine where the privileged command was executed
log_type	String (text)	Event-log source that recorded the command execution
account	String (text)	User account
event_description	String (text)	Event description
result	Numeric	Result of privileged command. Possible values: <ul style="list-style-type: none">• Unknown• Failure• Success

CONNECTOR VIEWS REFERENCED

- privilegedCommand__bsm_sun_bsm_sftp

Privileged Commands: Linux/Unix

Commands executed on Linux or Unix systems by users with administrative or root access.

IntelliSchema View Name: privilegedCommand_unix

Look-up file: privilegedCommand.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	<p>Time the privileged command execution occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format.</p> <p>Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.</p>
info_sys	String (text)	Machine where the privileged command was executed
log_type	String (text)	Event-log source that recorded the command execution
account	String (text)	User account
event_description	String (text)	Event description
result	Numeric	<p>Result of privileged command. Possible values:</p> <ul style="list-style-type: none"> • Unknown • Failure • Success

CONNECTOR VIEWS REFERENCED

- privilegedCommand_unix_unix_su_syslog
- privilegedCommand_unix_unix_sudo_syslogng

Privileged Commands: Windows

Commands executed on Windows systems by users with administrative or root access.

IntelliSchema View Name: privilegedCommand__windows

Look-up file: privilegedCommand.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the privileged command execution occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
info_sys	String (text)	Machine where the privileged command was executed
log_type	String (text)	Event-log source that recorded the command execution
account	String (text)	User account
event_description		Event description
result	Numeric	Result of privileged command. Possible values: <ul style="list-style-type: none">• Unknown• Failure• Success
privileges	String (text)	Privilege used to execute the command
domain	String (text)	Domain name

CONNECTOR VIEWS REFERENCED

- privilegedCommand__windows__microsoft_windows_securityEvent_sensageRetriever
- privilegedCommand__windows__microsoft_windows_securityEvent_snare
- privilegedCommand__windows__microsoft_windows2008_securityEvent_sensageRetriever
- privilegedCommand__windows__microsoft_windows2008_securityEvent_snare

REMOTE ACCESS EVENT

Events initiated by remote accessing.

IntelliSchema View Name: remote_access

Look-up file: result.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the event occurred.
log_type	String (text)	Event source
src_info_sys	String (text)	Source information system
dest_info_sys	String (text)	Desitnation information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
src_account	String (text)	Affected account
event_description	String (text)	Event-specific information
result	Numeric	Possible values: <ul style="list-style-type: none"> • -1 Unknown • 0 Failure • 1 Success
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

- remoteAccess__cisco_acs_syslogng

SECURITY OBJECTS

Security Objects Accessed or Deleted

IntelliSchema View Name: securityObject

Look-up file: securityObject.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the security object was accessed/deleted
info_sys	String (text)	Machine or device where the security object was accessed
user	String (text)	User account used for the access
object	String (text)	Description of the accessed object
domain	String (text)	Domain name
object_type	String (text)	Type of object accessed
access_type	String (text)	Type of access
logon_key	String (text)	Logon key used for deletion
action	Numeric	Possible values: <ul style="list-style-type: none">• Unknown• Object Accessed• Object Deleted

The following Security Objects event-type views are also available to create more specialized reports:

- “[Security Objects: Windows](#)”, on page 135

CONNECTOR VIEWS REFERENCED

- securityObject_sun_bsm_sftp
- securityObject_windows_microsoft_windows2008_securityEvent_sensageRetriever
- securityObject_windows_microsoft_windows2008_securityEvent_snare
- securityObject_windows_microsoft_windows_securityEvent_sensageRetriever
- securityObject_windows_microsoft_windows_securityEvent_snare

SECURITY OBJECTS: WINDOWS

Security Objects Accessed or Deleted for all Microsoft Windows systems

IntelliSchema View Name: securityObject__windows

Look-up file: securityObject.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the security object was accessed/deleted
info_sys	String (text)	Machine or device where the security object was accessed
user	String (text)	User account used for the access
object	String (text)	Description of the accessed object
domain	String (text)	Domain name
object_type	String (text)	Type of object accessed
access_type	String (text)	Type of access
logon_key	String (text)	Logon key used for deletion
action	Numeric	Possible values: <ul style="list-style-type: none"> • Unknown • Object Accessed • Object Deleted

The following Security Objects event-type views are also available to create more specialized reports:

- “[Security Objects: Windows](#)”, on page 135

CONNECTOR VIEWS REFERENCED

- securityObject__windows_microsoft_windows2008__securityEvent_sensageRetriever
- securityObject__windows_microsoft_windows2008__securityEvent_snare
- securityObject__windows_microsoft_windows__securityEvent_sensageRetriever
- securityObject__windows_microsoft_windows__securityEvent_snare

SYSTEM STARTUP AND SHUTDOWN

Startup and Shutdown events for all information systems.

IntelliSchema View Name: startStop

Look-up file: startStop.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the startup or shutdown occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
info_sys	String (text)	Machine started or shutdown
log_type	String (text)	Event-log source that recorded the startup or shutdown
result	Numeric	Result. Possible values: <ul style="list-style-type: none"> • Unknown • Stop • Start

The following System Startup and Shutdown event-type views are also available to create more specialized reports:

- “[Startup and Shutdown: Windows](#)”, on page 137
- “[Startup and Shutdown: BSM](#)”, on page 138

CONNECTOR VIEWS REFERENCED

- startStop__microsoft_sql_sensageRetriever
- startStop__oracle_adump
- startStop__oracle_adump_syslogng
- startStop__oracle_alert
- startStop__vmware_esx_vcenter_log_collection
- startStop__bsm_sun_bsm_sftp
- startStop__windows_microsoft_windows2008_securityEvent_sensageRetriever
- startStop__windows_microsoft_windows2008_securityEvent_snare
- startStop__windows_microsoft_windows_securityEvent_sensageRetriever
- startStop__windows_microsoft_windows_securityEvent_snare

Startup and Shutdown: Windows

Startup and Shutdown events for Microsoft Windows systems.

IntelliSchema View Name: startStop_windows

Look-up file: startStop.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the startup or shutdown occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
info_sys	String (text)	Machine started or shutdown
log_type	String (text)	Event-log source that recorded the startup or shutdown
result	Numeric	Result. Possible values: <ul style="list-style-type: none"> • Unknown • Stop • Start

CONNECTOR VIEWS REFERENCED

- startStop_windows__microsoft_windows_securityEvent_sensageRetriever
- startStop_windows__microsoft_windows_securityEvent_snare
- startStop_windows__microsoft_windows2008_securityEvent_sensageRetriever
- startStop_windows__microsoft_windows2008_securityEvent_snare

Startup and Shutdown: BSM

Startup and Shutdown events on systems where Basic Security Module (BSM) is enabled.

IntelliSchema View Name: startStop_bsm

Look-up file: startStop.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the startup or shutdown occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
info_sys	String (text)	Machine started or shutdown
log_type	String (text)	Event-log source that recorded the startup or shutdown
result	Numeric	Result. Possible values: <ul style="list-style-type: none">• Unknown• Stop• Start

CONNECTOR VIEWS REFERENCED

- startStop__bsm__sun_bsm_sftp

UNPARSED DATA

Unparsed data from all information systems.

IntelliSchema View Name: unparsedData

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the event occurred.
log_type	String (text)	Event source
parsed_message	String (text)	Original data
AUDIT_UNPARSE_SUCCESS	Numeric	1 if data unparsed

CONNECTOR VIEWS REFERENCED

- parsedData__apache_access_syslogng
- parsedData__apache_error_syslogng
- parsedData__bluecoat_sgproxy_batch
- parsedData__catbird_vsecurity_cef_syslogng
- parsedData__checkpoint_opsec_lea
- parsedData__cisco_acs_syslogng
- parsedData__cisco_asa_syslogng
- parsedData__cisco_ios_syslogng
- parsedData__cisco_netflow_receiver
- parsedData__cisco_pix_syslogng
- parsedData__hp_proCurve_tmsz_syslogng
- parsedData__ibm_db2_rdbms
- parsedData__mcafee_database_activity_monitoring_syslogng
- parsedData__mcafee_epo45_event_rdbms
- parsedData__mcafee_epo46_event_sensageRetriever
- parsedData__mcafee_epo51_audit_sensageRetriever
- parsedData__mcafee_epo51_event_sensageRetriever
- parsedData__mcafee_epo_audit_rdbms
- parsedData__mcafee_epo_event_rdbms
- parsedData__mcafee_epo_rdbms
- parsedData__mcafee_foundstone_rdbms

- parsedData__mcafee_intrushield_rdbms
- parsedData__mcafee_intrushield_syslogng
- parsedData__mcafee_scm_batch
- parsedData__microsoft_dns_debug_sensageRetrieverAgent
- parsedData__microsoft_exchange_admin_events_syslogng
- parsedData__microsoft_exchange_mailbox_events_syslogng
- parsedData__microsoft_exchange_tracking_sensageRetrieverAgent
- parsedData__microsoft_iis
- parsedData__microsoft_SharePoint_Audit_sensageRetrieverAgent
- parsedData__microsoft_sql_sensageRetriever
- parsedData__microsoft_windows2008_appEvent_sensageRetriever
- parsedData__microsoft_windows2008_dirEvent_sensageRetriever
- parsedData__microsoft_windows2008_dnsEvent_sensageRetriever
- parsedData__microsoft_windows2008_securityEvent_sensageRetriever
- parsedData__microsoft_windows2008_securityEvent_snare
- parsedData__microsoft_windows_appEvent_sensageRetriever
- parsedData__microsoft_windows_dirEvent_sensageRetriever
- parsedData__microsoft_windows_dnsEvent_sensageRetriever
- parsedData__microsoft_windows_frsEvent_sensageRetriever
- parsedData__microsoft_windows_securityEvent_sensageRetriever
- parsedData__microsoft_windows_securityEvent_snare
- parsedData__microsoft_windows_sysEvent_sensageRetriever
- parsedData__oracle_adump
- parsedData__oracle_adump_syslogng
- parsedData__oracle_alert
- parsedData__oracle_database_fga_sensageRetriever
- parsedData__oracle_database_sysaudit_sensageRetriever
- parsedData__oracle_fga_xml_batch
- parsedData__oracle_listener
- parsedData__panos_firewall_syslogng
- parsedData__postgres_audit_csv
- parsedData__sap_aud_sftp

- parsedData_sun_bsm_sftp
- parsedData_symantec_endpoint_syslogng
- parsedData_syslogng_catchall_syslogng
- parsedData_tipping_point_syslogng
- parsedData_unix_ftpd_syslogng
- parsedData_unix_login_syslogng
- parsedData_unix_sshd2_syslogng
- parsedData_unix_sudo_syslogng
- parsedData_unix_su_syslogng
- parsedData_vmware_esx_500_syslogng
- parsedData_vmware_esx_vcenter_log_collection

USER LOGINS

User logins for all systems.

IntelliSchema View Name: userLogin

Look-up file: userLogin.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	<p>Time the login occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format.</p> <p>Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.</p>
account	String (text)	User Account
info_sys	String (text)	Machine logged into
log_type	String (text)	Event-log source that recorded the login
privileged	Numeric	Privileged account status. Possible values: <ul style="list-style-type: none"> • Privileged • Standard
result	Numeric	Result of login. Possible values: <ul style="list-style-type: none"> • Unknown • Failure • Success

The following User Logins event-type views are also available to create more specialized reports:

- “[User Logins: Router](#)”, on page 143
- “[User Logins: Windows](#)”, on page 144
- “[User Logins: Linux/Unix](#)”, on page 147

CONNECTOR VIEWS REFERENCED

- [userLogin__cisco_asa_syslogng](#)
- [userLogin__hp_proCurve_t3t4_syslogng](#)
- [userLogin__hp_proCurve_tmsz_syslogng](#)
- [userLogin__microsoft_sql_sensageRetriever](#)
- [userLogin__oracle_adump](#)
- [userLogin__oracle_adump_syslogng](#)
- [userLogin__oracle_database_sysaudit_sensageRetriever](#)
- [userLogin__vmware_esx_500_syslogng](#)
- [userLogin__vmware_esx_vcenter_event_collection](#)
- [userLogin__vmware_esx_vcenter_log_collection](#)
- [userLogin__router_cisco_ios_syslogng](#)
- [userLogin__unix_unix_ftpd_syslogng](#)
- [userLogin__unix_unix_login_syslogng](#)
- [userLogin__unix_unix_sshd2_syslogng](#)
- [userLogin__unix_unix_su_syslogng](#)
- [userLogin__windows_domainController_microsoft_windows2008_securityEvent_sensageRetriever](#)
- [userLogin__windows_domainController_microsoft_windows2008_securityEvent_snare](#)
- [userLogin__windows_domainController_microsoft_windows_securityEvent_sensageRetriever](#)
- [userLogin__windows_domainController_microsoft_windows_securityEvent_snare](#)
- [userLogin__windows_nonDomainController_microsoft_windows2008_securityEvent_sensageRetriever](#)
- [userLogin__windows_nonDomainController_microsoft_windows2008_securityEvent_snare](#)
- [userLogin__windows_nonDomainController_microsoft_windows_securityEvent_sensageRetriever](#)
- [userLogin__windows_nonDomainController_microsoft_windows_securityEvent_snare](#)

User Logins: Router

User logins for all routers.

IntelliSchema View Name: userLogin_router

Look-up file: userLogin.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	<p>Time the login occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format.</p> <p>Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.</p>
info_sys	String (text)	Router logged into
log_type	String (text)	Event-log source that recorded the login
account	String (text)	User account
result	Numeric	<p>Result of login. Possible values:</p> <ul style="list-style-type: none"> • Unknown • Failure • Success
privileged	Numeric	<p>Privileged Account. Possible values:</p> <ul style="list-style-type: none"> • Privileged • Standard
src_ip	String (text)	Source IP Address
facility	String (text)	Syslog facility name
severity	String (text)	Syslog security level

CONNECTOR VIEWS REFERENCED

- userLogin_router_cisco_ios_syslogng

User Logins: Windows

Login activity for all Microsoft Windows systems

IntelliSchema View Name: userLogin__windows

Look-up file: userLogin.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the login occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
info_sys	String (text)	Machine logged into
log_type	String (text)	Event-log source that recorded the login
account	String (text)	User account
result	Numeric	Result of login. Possible values: <ul style="list-style-type: none">• Unknown• Failure• Success
privileged	Numeric	Privileged account status. Possible values: <ul style="list-style-type: none">• Privileged• Standard
event_id	Numeric	Event ID
event_description	String (text)	Event description

The following Windows Logins event-type views are also available to create more specialized reports:

- “User Logins: Windows Non-domain Controller”, on page 145
- “User Logins: Windows”, on page 146

CONNECTOR VIEWS REFERENCED

- userLogin__windows__domainController__microsoft_windows_securityEvent_sensageRetriever
- userLogin__windows__domainController__microsoft_windows_securityEvent_snare
- userLogin__windows__nonDomainController__microsoft_windows_securityEvent_sensag eRetriever
- userLogin__windows__nonDomainController__microsoft_windows_securityEvent_snare
- userLogin__windows__domainController__microsoft_windows2008_securityEvent_sensa geRetriever

- userLogin_windows_domainController_microsoft_windows2008_securityEvent_snare
- userLogin_windows_nonDomainController_microsoft_windows2008_securityEvent_se
nsageRetriever
- userLogin_windows_nonDomainController_microsoft_windows2008_securityEvent_sn
are

User Logins: Windows Non-domain Controller

User logins for Microsoft Windows systems using non-domain controllers.

IntelliSchema View Name: userLogin_windows_nonDomainController

Look-up file: userLogin.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the login occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
info_sys	String (text)	Machine logged into
log_type	String (text)	Event-log source that recorded the login
account	String (text)	User account
result	Numeric	Result of login. Possible values: <ul style="list-style-type: none"> • Unknown • Failure • Success
privileged	Numeric	Privileged account status. Possible values: <ul style="list-style-type: none"> • Privileged • Standard
event_id	Numeric	Event ID
event_description	String (text)	Event description
logon_description	String (text)	Login description

CONNECTOR VIEWS REFERENCED

- userLogin_windows_nonDomainController_microsoft_windows_securityEvent_sensag
eRetriever
- userLogin_windows_nonDomainController_microsoft_windows_securityEvent_snare
- userLogin_windows_nonDomainController_microsoft_windows2008_securityEvent_se
nsageRetriever

- userLogin_windows_nonDomainController_microsoft_windows2008_securityEvent_snare

User Logins: Windows

User logins for all Microsoft Windows systems using a domain controller.

IntelliSchema View Name: userLogin_windows_domainController

Look-up file: userLogin.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	Time the login occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format. Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.
info_sys	String (text)	Machine logged into
log_type	String (text)	Event-log source that recorded the login
account	String (text)	SETTING UP THE MICROSOFT_WIND OWS_SECURITYEVE NT
result	Numeric	Possible values: • Standard
privileged	Numeric	Account status. Possible values: • Standard
event_id	Numeric	Event ID
event_description	String (text)	Event description
workstation	String (text)	Workstation
failure_code	String (text)	Failure code
failure_code_description	String (text)	Failure code description

CONNECTOR VIEWS REFERENCED

- userLogin_windows_domainController_microsoft_windows_securityEvent_sensageRetriever
- userLogin_windows_domainController_microsoft_windows_securityEvent_snare
- userLogin_windows_domainController_microsoft_windows2008_securityEvent_sensageRetriever
- userLogin_windows_domainController_microsoft_windows2008_securityEvent_snare

User Logins: Linux/Unix

Logins on Linux or Unix systems.

IntelliSchema View Name: userLogin_unix

Look-up file: userLogin.lookup

COLUMNS

Column	Datatype	Description
ts Date Time Date and Time Day of Week	timestamp	<p>Time the login occurred. The ts column displays a data format that encapsulates both date and time information. You may also use the other date or time columns to display the time stored in the ts column in a more useful format.</p> <p>Note: The format you choose can change the data returned by the report, particularly when using dates for sorting and summarizing events or when using dates as selection criteria.</p>
info_sys	String (text)	Machine logged into
log_type	String (text)	Event-log source that recorded the login
account	String (text)	User account
result	Numeric	<p>Result of login. Possible values:</p> <ul style="list-style-type: none"> • Unknown • Failure • Success
privileged	Numeric	<p>Privileged account status. Possible values:</p> <ul style="list-style-type: none"> • Privileged • Standard

CONNECTOR VIEWS REFERENCED

- userLogin_unix_unix_ftpd_syslogng
- userLogin_unix_unix_login_syslogng
- userLogin_unix_unix_sshd2_syslogng
- userLogin_unix_unix_su_syslogng

VULNERABILITY EVENT

Events with information about vulnerabilities.

IntelliSchema View Name: vulnerability

Look-up file: result.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the event occurred.
log_type	String (text)	Event source
src_info_sys	String (text)	Source information system
dest_info_sys	String (text)	Desitnation information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
src_account	String (text)	Affected account
event_description	String (text)	Event-specific information (threat and filename)
result	Numeric	Possible values: • -1 Unknown • 0 Failure • 1 Success
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

- vulnerability__mcafee_epo45_event_rdbms
- vulnerability__mcafee_epo46_event_sensageRetriever
- vulnerability__mcafee_epo51_event_sensageRetriever
- vulnerability__mcafee_epo_event_rdbms
- vulnerability__mcafee_epo_rdbms
- vulnerability__mcafee_foundstone_rdbms
- vulnerability__symantec_endpoint_syslogng

WEBPROXY EVENT

Web proxy-specific information from all information systems.

IntelliSchema View Name: alert

Look-up file: result.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the event occurred.
log_type	String (text)	Event source
src_info_sys	String (text)	Source information system
dest_info_sys	String (text)	Desitnation information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
src_account	String (text)	Affected account
event_description	String (text)	Event-specific information (referrer)
result	Numeric	Possible values: • -1 Unknown • 0 Failure • 1 Success
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

- webProxy__apache_access_syslogng
- webProxy__bluecoat_sgproxy_batch
- webProxy__microsoft_iis

WIRELESS EVENT

Wireless-specific information from all information systems.

IntelliSchema View Name: wireless

Look-up file: result.lookup

COLUMNS

Column	Datatype	Description
ts	timestamp	Time the event occurred.
log_type	String (text)	Event source
src_info_sys	String (text)	Source information system
dest_info_sys	String (text)	Desitnation information system
src_port	String (text)	Source port number
dest_port	String (text)	Destination port number
src_account	String (text)	Affected account
event_description	String (text)	Event description
result	Numeric	Possible values: • -1 Unknown • 0 Failure • 1 Success
unparsed_log_entry	String (text)	Raw log line

CONNECTOR VIEWS REFERENCED

None

CONNECTOR VIEWS AND INTELLISchema VIEWS

The following table lists connector views and their associated IntelliSchema views:

NOTE: IntelliSchema views query other views by using the SenSage AP `_tablematch()` function in the SQL `FROM` clause, which allows a single query to run against one or more tables or views whose names match a pattern passed to the `_tablematch()` function. Because the views are named consistently, they can use the `_tablematch()` function to query more than one view or table. For more information, see `_tablematch()` in Chapter 4, “SenSage AP ConsoleSenSage AP SQL Functions” in the *Event Data Warehouse Guide*.

For a complete discussion of IntelliSchema architecture, see “[IntelliSchema](#)”, on page 28.

Connector View	Intellischema Views
accountAdditionAndDeletion__microsoft_exchange_adm_in_events_syslogng	• “ Account Addition and Deletion ”, on page 95
accountAdditionAndDeletion__microsoft_exchange_mailbox_events_syslogng	• “ Account Addition and Deletion ”, on page 95
accountAdditionAndDeletion__microsoft_sql_sensageR etriever	• “ Account Addition and Deletion ”, on page 95
accountAdditionAndDeletion__oracle_adump	• “ Account Addition and Deletion ”, on page 95
accountAdditionAndDeletion__oracle_adump_syslogng	• “ Account Addition and Deletion ”, on page 95
accountAdditionAndDeletion__oracle_database_sysaud_it_sensageRetriever	• “ Account Addition and Deletion ”, on page 95

Connector View	Intellischema Views
accountAdditionAndDeletion__windows__microsoft_windows2008_securityEvent_sensageRetriever	• Account Addition and Deletion:Windows", on page 95
accountAdditionAndDeletion__windows2008_securityEvent_snare	• Account Addition and Deletion:Windows", on page 97
accountAdditionAndDeletion__windows__microsoft_windows2008_securityEvent_sensageRetriever	• "Account Addition and Deletion", on page 95 • "Account Addition and Deletion: Windows", on page 97
accountAdditionAndDeletion__windows__microsoft_windows_securityEvent_snare	• "Account Addition and Deletion", on page 95 • "Account Addition and Deletion: Windows", on page 97
adminAccountActivity__microsoft_sql_sensageRetriever	• "Administrative Account Activity", on page 98
adminAccountActivity__windows__microsoft_windows2008_securityEvent_sensageRetriever	• "Administrative Account Activity", on page 98
adminAccountActivity__windows__microsoft_windows2008_securityEvent_snare	• "Administrative Account Activity", on page 98
adminAccountActivity__windows__microsoft_windows_securityEvent_sensageRetriever	• "Administrative Account Activity", on page 98 • "Administrative Account Activity: Windows", on page 100
adminAccountActivity__windows__microsoft_windows_securityEvent_snare	• "Administrative Account Activity", on page 98 • "Administrative Account Activity: Windows", on page 100
alert__apache_error_syslogng	• "Alert Event", on page 101
alert__cisco_acs_syslogng	• "Alert Event", on page 101
alert__hp_proCurve_tmsz_syslogng	• "Alert Event", on page 101
alert__mcafee_scm_batch	• "Alert Event", on page 101
alert__panos_firewall_syslogng	• "Alert Event", on page 101
alert__symantec_endpoint_syslogng	• "Alert Event", on page 101
alert__vmware_esx_vcenter_event_collection	• "Alert Event", on page 101
application__catbird_vsecurity_cef_syslogng	• "Application Event", on page 102
application__cisco_ios_syslogng	• "Application Event", on page 102
application__microsoft_sharepoint	• "Application Event", on page 102
application__microsoft_windows2008_appEvent_sensageRetriever	• "Application Event", on page 102
application__microsoft_windows2008_dirEvent_sensageRetriever	• "Application Event", on page 102
application__microsoft_windows2008_dnsEvent_sensageRetriever	• "Application Event", on page 102
application__microsoft_windows2008_frsEvent_sensageRetriever	• "Application Event", on page 102
application__microsoft_windows2008_sysEvent_sensageRetriever	• "Application Event", on page 102

Connector View	Intellischema Views
application__microsoft_windows_appEvent_sensageRetriever	• “Application Event”, on page 102
application__microsoft_windows_dirEvent_sensageRetriever	• “Application Event”, on page 102
application__microsoft_windows_dnsEvent_sensageRetriever	• “Application Event”, on page 102
application__microsoft_windows_frsEvent_sensageRetriever	• “Application Event”, on page 102
application__microsoft_windows_sysEvent_sensageRetriever	• “Application Event”, on page 102
application__sap_aud_sftp	• “Application Event”, on page 102
audit__apache_error_syslogng	• “Audit Event”, on page 109
audit__mcafee_epo45_audit_rdbms	• “Audit Event”, on page 109
audit__mcafee_epo46_audit_sensageRetriever	• “Audit Event”, on page 109
audit__mcafee_epo51_audit_sensageRetriever	• “Audit Event”, on page 109
audit__mcafee_epo_audit_rdbms	• “Audit Event”, on page 109
audit__microsoft_exchange_admin_events_syslogng	• “Audit Event”, on page 109
audit__oracle_adump	• “Audit Event”, on page 109
audit__oracle_adump_syslogng	• “Audit Event”, on page 109
audit__oracle_database_fga_sensageRetriever	• “Audit Event”, on page 109
audit__oracle_database_sysaudit_sensageRetriever	• “Audit Event”, on page 109
audit__oracle_listener	• “Audit Event”, on page 109
audit__sun_bsm_sftp	• “Audit Event”, on page 109
audit__unix_sshd2_syslogng	• “Audit Event”, on page 109
audit__unix_su_syslogng	• “Audit Event”, on page 109
audit__unix_sudo_syslogng	• “Audit Event”, on page 109
audit__vmware_esx_vcenter_event_collection	• “Audit Event”, on page 109
audit__vmware_esx_vcenter_log_collection	• “Audit Event”, on page 109
database_ddl_ibm_db2_rdbms	• “Database DDL (Data Definition Language)”, on page 111
database_ddl_mcafee_database_activity_monitoring_syslogng	• “Database DDL (Data Definition Language)”, on page 111
database_ddl_microsoft_sql_sensageRetriever	• “Database DDL (Data Definition Language)”, on page 111
database_ddl_oracle_adump	• “Database DDL (Data Definition Language)”, on page 111
database_ddl_oracle_adump_syslogng	• “Database DDL (Data Definition Language)”, on page 111
database_ddl_oracle_alert	• “Database DDL (Data Definition Language)”, on page 111
database_ddl_oracle_database_fga_sensageRetriever	• “Database DDL (Data Definition Language)”, on page 111
database_ddl_oracle_database_sysaudit_sensageRetriever	• “Database DDL (Data Definition Language)”, on page 111

Connector View	Intellischema Views
database_ddl_oracle_fga_xml_batch	• “Database DDL (Data Definition Language)”, on page 111
database_ddl_postgres_audit_csv	• “Database DDL (Data Definition Language)”, on page 111
database_dml_ibm_db2_rdbms	• “Database DML (Data Manipulation Language)”, on page 111
database_dml_mcafee_database_activity_monitoring_syslogng	• “Database DML (Data Manipulation Language)”, on page 111
database_dml_microsoft_sql_sensageRetriever	• “Database DML (Data Manipulation Language)”, on page 111
database_dml_oracle_adump	• “Database DML (Data Manipulation Language)”, on page 111
database_dml_oracle_adump_syslogng	• “Database DML (Data Manipulation Language)”, on page 111
database_dml_oracle_alert	• “Database DML (Data Manipulation Language)”, on page 111
database_dml_oracle_database_fga_sensageRetriever	• “Database DML (Data Manipulation Language)”, on page 111
database_dml_oracle_database_sysaudit_sensageRetriever	• “Database DML (Data Manipulation Language)”, on page 111
database_dml_oracle_fga_xml_batch	• “Database DML (Data Manipulation Language)”, on page 111
database_dml_postgres_audit_csv	• “Database DML (Data Manipulation Language)”, on page 111
idsIps_checkpoint_opsec_lea	• “IDS/IPS Event”, on page 113
idsIps_cisco_asa_syslogng	• “IDS/IPS Event”, on page 113
idsIps_mcafee_intrushield_rdbms	• “IDS/IPS Event”, on page 113
idsIps_mcafee_intrushield_syslogng	• “IDS/IPS Event”, on page 113
idsIps_tipping_point_syslogng	• “IDS/IPS Event”, on page 113
investigation_apache_access_syslogng	• “Investigation Event”, on page 114
investigation_bluecoat_sgproxy_batch	• “Investigation Event”, on page 114
investigation_catbird_vsecurity_cef_syslogng	• “Investigation Event”, on page 114
investigation_checkpoint_opsec_lea	• “Investigation Event”, on page 114
investigation_cisco_acs_syslogng	• “Investigation Event”, on page 114
investigation_cisco_asa_syslogng	• “Investigation Event”, on page 114
investigation_cisco_ios_syslogng	• “Audit Event”, on page 109
investigation_cisco_ips_alert_error	• “Investigation Event”, on page 114
investigation_cisco_ironport_maillog_syslogng	• “Investigation Event”, on page 114
investigation_cisco_netflow_receiver	• “Investigation Event”, on page 114
investigation_cisco_pix_syslogng	• “Investigation Event”, on page 114
investigation_f5_asm_cef_syslogng	• “Investigation Event”, on page 114
investigation_hp_proCurve_t3t4_syslogng	• “Investigation Event”, on page 114
investigation_hp_proCurve_tmsz_syslogng	• “Investigation Event”, on page 114

Connector View	Intellischema Views
investigation__ibm_db2_rdbms	• “Investigation Event”, on page 114
investigation__juniper_netscreenFw_syslogng	• “Investigation Event”, on page 114
investigation__mcafee_database_activity_monitoring_syslogng	• “Investigation Event”, on page 114
investigation__mcafee_epo45_audit_rdbms	• “Investigation Event”, on page 114
investigation__mcafee_epo45_event_rdbms	• “Investigation Event”, on page 114
investigation__mcafee_epo46_audit_sensageRetriever	• “Investigation Event”, on page 114
investigation__mcafee_epo46_event_sensageRetriever	• “Investigation Event”, on page 114
investigation__mcafee_epo51_audit_sensageRetriever	• “Investigation Event”, on page 114
investigation__mcafee_epo51_event_sensageRetriever	• “Investigation Event”, on page 114
investigation__mcafee_epo_audit_rdbms	• “Investigation Event”, on page 114
investigation__mcafee_epo_event_rdbms	• “Investigation Event”, on page 114
investigation__mcafee_foundstone_rdbms	• “Investigation Event”, on page 114
investigation__mcafee_intrushield_rdbms	• “Investigation Event”, on page 114
investigation__mcafee_intrushield_syslogng	• “Investigation Event”, on page 114
investigation__mcafee_scm_batch	• “Investigation Event”, on page 114
investigation__microsoft_exchange_admin_events_syslogng	• “Investigation Event”, on page 114
investigation__microsoft_exchange_mailbox_events_syslogng	• “Investigation Event”, on page 114
investigation__microsoft_exchange_tracking_sensageRetrieverAgent	• “Investigation Event”, on page 114
investigation__microsoft_iis	• “Investigation Event”, on page 114
investigation__microsoft_sharepoint	• “Investigation Event”, on page 114
investigation__microsoft_sql_sensageRetriever	• “Investigation Event”, on page 114
investigation__microsoft_windows2008_securityEvent_sensageRetriever	• “Investigation Event”, on page 114
investigation__microsoft_windows2008_securityEvent_snare	• “Investigation Event”, on page 114
investigation__microsoft_windows_securityEvent_sensageRetriever	• “Investigation Event”, on page 114
investigation__microsoft_windows_securityEvent_snare	• “Investigation Event”, on page 114
investigation__oracle_adump	• “Investigation Event”, on page 114
investigation__oracle_adump_syslogng	• “Investigation Event”, on page 114
investigation__oracle_database_fga_sensageRetriever	• “Investigation Event”, on page 114
investigation__oracle_database_sysaudit_sensageRetriever	• “Investigation Event”, on page 114
investigation__oracle_fga_xml_batch	• “Investigation Event”, on page 114
investigation__oracle_listener	• “Investigation Event”, on page 114
investigation__panos_firewall_syslogng	• “Investigation Event”, on page 114
investigation__postgres_audit_csv	• “Investigation Event”, on page 114

Connector View	Intellischema Views
investigation__sap_aud_sftp	• "Investigation Event", on page 114
investigation__sun_bsm_sftp	• "Investigation Event", on page 114
investigation__syslogng_catchall_syslogng	• "Investigation Event", on page 114
investigation__tipping_point_syslogng	• "Investigation Event", on page 114
investigation__unix_ftpd_syslogng	• "Investigation Event", on page 114
investigation__unix_login_syslogng	• "Investigation Event", on page 114
investigation__unix_sshd2_syslogng	• "Investigation Event", on page 114
investigation__unix_su_syslogng	• "Investigation Event", on page 114
investigation__unix_sudo_syslogng	• "Investigation Event", on page 114
investigation__vmware_esx_500_syslogng	• "Investigation Event", on page 114
investigation__vmware_esx_vcenter_event_collection	• "Investigation Event", on page 114
lossOfAuditMessages__windows_microsoft_windows2008_securityEvent_sensageRetriever	<ul style="list-style-type: none"> • "Loss of Audit Messages", on page 117 • "Loss of Audit Messages: Windows", on page 118
lossOfAuditMessages__windows_microsoft_windows2008_securityEvent_snare	<ul style="list-style-type: none"> • "Loss of Audit Messages", on page 117 • "Loss of Audit Messages: Windows", on page 118
lossOfAuditMessages__windows_microsoft_windows_securityEvent_sensageRetriever	<ul style="list-style-type: none"> • "Loss of Audit Messages", on page 117 • "Loss of Audit Messages: Windows", on page 118
lossOfAuditMessages__windows_microsoft_windows_securityEvent_snare	<ul style="list-style-type: none"> • "Loss of Audit Messages", on page 117 • "Loss of Audit Messages: Windows", on page 118
mail__mcafee_scm_batch	• "Mail Event", on page 119
mail__microsoft_exchange_mailbox_events_syslogng	• "Mail Event", on page 119
mail__microsoft_exchange_tracking_sensageRetriever Agent	• "Mail Event", on page 119
malware__mcafee_epo45_event_rdbms	• "Malware Event", on page 120
malware__mcafee_epo46_event_sensageRetriever	• "Malware Event", on page 120
malware__mcafee_epo51_event_sensageRetriever	• "Malware Event", on page 120
malware__mcafee_epo_event_rdbms	• "Malware Event", on page 120
malware__mcafee_epo_rdbms	• "Malware Event", on page 120
malware__mcafee_scm_batch	• "Malware Event", on page 120
malware__symantec_endpoint_syslogng	• "Malware Event", on page 120
networkDeviceConnection__catbird_vsecurity_cef_syslogng	• "Network Device Connection", on page 39
networkDeviceConnection__cisco_netflow_receiver	• "Network Device Connection", on page 39
networkDeviceConnection__f5_asm_cef_syslogng	• "Network Device Connection", on page 121

Connector View	Intellischema Views
networkDeviceConnection__hp_proCurve_tmsz_syslogng	<ul style="list-style-type: none"> • “Network Device Connection”, on page 121
networkDeviceConnection__oracle_adump	<ul style="list-style-type: none"> • “Network Device Connection”, on page 121
networkDeviceConnection__oracle_adump_syslogng	<ul style="list-style-type: none"> • “Network Device Connection”, on page 121
networkDeviceConnection__oracle_listener	<ul style="list-style-type: none"> • “Network Device Connection”, on page 121
networkDeviceConnection__firewall_checkpoint_opsec_lea	<ul style="list-style-type: none"> • “Network Device Connection”, on page 121 • “Network Device Connection: Firewall”, on page 123
networkDeviceConnection__firewall_cisco_asa_syslogng	<ul style="list-style-type: none"> • “Network Device Connection”, on page 121 • “Network Device Connection: Firewall”, on page 123
networkDeviceConnection__firewall_cisco_pix_syslogng	<ul style="list-style-type: none"> • “Network Device Connection”, on page 121 • “Network Device Connection: Firewall”, on page 123
networkDeviceConnection__firewall_juniper_netscreenFw_syslogng	<ul style="list-style-type: none"> • “Network Device Connection”, on page 121 • “Network Device Connection: Firewall”, on page 123
networkDeviceConnection__router_cisco_ios_syslogng	<ul style="list-style-type: none"> • “Network Device Connection”, on page 121 • “Network Device Connection: Router”, on page 122
parsedData__apache_access_syslogng	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__apache_error_syslogng	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__bluecoat_sgproxy_batch	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__catbird_vsecurity_cef_syslogng	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__checkpoint_opsec_lea	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__cisco_acs_syslogng	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__cisco_asa_syslogng	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__cisco_ios_syslogng	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__cisco_netflow_receiver	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__cisco_pix_syslogng	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__hp_proCurve_t3t4_syslogng	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__hp_proCurve_tmsz_syslogng	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__ibm_db2_rdbms	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__juniper_netscreenFw_syslogng	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__mcafee_database_activity_monitoring_syslogng	<ul style="list-style-type: none"> • “Parsed Data”, on page 124
parsedData__mcafee_epo45_audit_rdbms	<ul style="list-style-type: none"> • “Parsed Data”, on page 124

Connector View	Intellischema Views
parsedData__mcafee_epo45_event_rdbms	• "Parsed Data", on page 124
parsedData__mcafee_epo46_audit_sensageRetriever	• "Parsed Data", on page 124
parsedData__mcafee_epo46_event_sensageRetriever	• "Parsed Data", on page 124
parsedData__mcafee_epo51_audit_sensageRetriever	• "Parsed Data", on page 124
parsedData__mcafee_epo51_event_sensageRetriever	• "Parsed Data", on page 124
parsedData__mcafee_epo_audit_rdbms	• "Parsed Data", on page 124
parsedData__mcafee_epo_event_rdbms	• "Parsed Data", on page 124
parsedData__mcafee_epo_rdbms	• "Parsed Data", on page 124
parsedData__mcafee_foundstone_rdbms	• "Parsed Data", on page 124
parsedData__mcafee_intrushield_rdbms	• "Parsed Data", on page 124
parsedData__mcafee_intrushield_syslogng	• "Parsed Data", on page 124
parsedData__mcafee_scm_batch	• "Parsed Data", on page 124
parsedData__microsoft_SharePoint_Audit_sensageRetrieverAgent	• "Parsed Data", on page 124
parsedData__microsoft_dns_debug_sensageRetrieverAgent	• "Parsed Data", on page 124
parsedData__microsoft_exchange_admin_events_syslogng	• "Parsed Data", on page 124
parsedData__microsoft_exchange_mailbox_events_syslogng	• "Parsed Data", on page 124
parsedData__microsoft_exchange_tracking_sensageRetrieverAgent	• "Parsed Data", on page 124
parsedData__microsoft_iis	• "Parsed Data", on page 124
parsedData__microsoft_sql_sensageRetriever	• "Parsed Data", on page 124
parsedData__microsoft_windows2008_appEvent_sensageRetriever	• "Parsed Data", on page 124
parsedData__microsoft_windows2008_dirEvent_sensageRetriever	• "Parsed Data", on page 124
parsedData__microsoft_windows2008_dnsEvent_sensageRetriever	• "Parsed Data", on page 124
parsedData__microsoft_windows2008_frsEvent_sensageRetriever	• "Parsed Data", on page 124
parsedData__microsoft_windows2008_securityEvent_sensageRetriever	• "Parsed Data", on page 124
parsedData__microsoft_windows2008_securityEvent_snare	• "Parsed Data", on page 124
parsedData__microsoft_windows2008_sysEvent_sensageRetriever	• "Parsed Data", on page 124
parsedData__microsoft_windows_appEvent_sensageRetriever	• "Parsed Data", on page 124
parsedData__microsoft_windows_dirEvent_sensageRetriever	• "Parsed Data", on page 124
parsedData__microsoft_windows_dnsEvent_sensageRetriever	• "Parsed Data", on page 124

Connector View	Intellischema Views
parsedData__microsoft_windows_frsEvent_sensageRetriever	• “Parsed Data”, on page 124
parsedData__microsoft_windows_securityEvent_sensageRetriever	• “Parsed Data”, on page 124
parsedData__microsoft_windows_securityEvent_snare	• “Parsed Data”, on page 124
parsedData__microsoft_windows_sysEvent_sensageRetriever	• “Parsed Data”, on page 124
parsedData__oracle_adump	• “Parsed Data”, on page 124
parsedData__oracle_adump_syslogng	• “Parsed Data”, on page 124
parsedData__oracle_alert	• “Parsed Data”, on page 124
parsedData__oracle_database_fga_sensageRetriever	• “Parsed Data”, on page 124
parsedData__oracle_database_sysaudit_sensageRetriever	• “Parsed Data”, on page 124
parsedData__oracle_fga_xml_batch	• “Parsed Data”, on page 124
parsedData__oracle_listener	• “Parsed Data”, on page 124
parsedData__panos_firewall_syslogng	• “Parsed Data”, on page 124
parsedData__postgres_audit_csv	• “Parsed Data”, on page 124
parsedData__sap_aud_sftp	• “Parsed Data”, on page 124
parsedData__sun_bsm_sftp	• “Parsed Data”, on page 124
parsedData__symantec_endpoint_syslogng	• “Parsed Data”, on page 124
parsedData__syslogng_catchall_syslogng	• “Parsed Data”, on page 124
parsedData__tipping_point_syslogng	• “Parsed Data”, on page 124
parsedData__unix_ftpd_syslogng	• “Parsed Data”, on page 124
parsedData__unix_login_syslogng	• “Parsed Data”, on page 124
parsedData__unix_sshd2_syslogng	• “Parsed Data”, on page 124
parsedData__unix_su_syslogng	• “Parsed Data”, on page 124
parsedData__unix_sudo_syslogng	• “Parsed Data”, on page 124
parsedData__vmware_esx_500_syslogng	• “Parsed Data”, on page 124
parsedData__vmware_esx_vcenter_event_collection	• “Parsed Data”, on page 124
parsedData__vmware_esx_vcenter_log_collection	• “Parsed Data”, on page 124
passwordchangeandreset__microsoft_sql_sensageRetriever	• “Password Changes and Resets”, on page 127
passwordChangeAndReset__oracle_database_sysaudit_sensageRetriever	• “Password Changes and Resets”, on page 127
passwordChangeAndReset__windows_microsoft_windows_2008_securityEvent_sensageRetriever	• “Password Changes and Resets”, on page 127 • “Password Changes and Resets: Windows”, on page 128
passwordChangeAndReset__windows_microsoft_windows_2008_securityEvent_snare	• “Password Changes and Resets”, on page 127 • “Password Changes and Resets: Windows”, on page 128

Connector View	Intellischema Views
passwordChangeAndReset_windows_microsoft_windows_securityEvent_sensageRetriever	<ul style="list-style-type: none"> • “Password Changes and Resets”, on page 127 • “Password Changes and Resets: Windows”, on page 128
passwordChangeAndReset_windows_microsoft_windows_securityEvent_snare	<ul style="list-style-type: none"> • “Password Changes and Resets”, on page 127 • “Password Changes and Resets: Windows”, on page 128
privilegedCommand_bsm_sun_bsm_sftp	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129 • “Privileged Commands: BSM”, on page 130
privilegedCommand_cisco_asa_syslogng	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129
privilegedCommand_microsoft_exchange_admin_events_syslogng	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129
privilegedCommand_microsoft_exchange_mailbox_events_syslogng	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129
privilegedCommand_oracle_adump	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129
privilegedCommand_oracle_adump_syslog	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129
privilegedCommand_oracle_database_sysaudit_sensageRetriever	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129
privilegedCommand_unix_unix_su_syslog	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129 • “Privileged Commands: Linux/ Unix”, on page 131
privilegedCommand_unix_unix_sudo_syslogng	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129 • “Privileged Commands: Linux/ Unix”, on page 131
privilegedCommand_windows_microsoft_windows2008_securityEvent_sensageRetriever	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129 • “Privileged Commands: Windows”, on page 132
privilegedCommand_windows_microsoft_windows2008_securityEvent_snare	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129 • “Privileged Commands: Windows”, on page 132
privilegedCommand_windows_microsoft_windows_securityEvent_sensageRetriever	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129 • “Privileged Commands: Windows”, on page 132
privilegedCommand_windows_microsoft_windows_securityEvent_snare	<ul style="list-style-type: none"> • “Privileged Commands”, on page 129 • “Privileged Commands: Windows”, on page 132
remoteAccess_cisco_acs_syslogng	<ul style="list-style-type: none"> • “Remote Access Event”, on page 133
securityObject_sun_bsm_sftp	<ul style="list-style-type: none"> • “Security Objects: Windows”, on page 135
securityObject_windows_microsoft_windows2008_securityEvent_sensageRetriever	<ul style="list-style-type: none"> • “Security Objects: Windows”, on page 135
securityObject_windows_microsoft_windows2008_securityEvent_snare	<ul style="list-style-type: none"> • “Security Objects: Windows”, on page 135
securityObject_windows_microsoft_windows_securityEvent_sensageRetriever	<ul style="list-style-type: none"> • “Security Objects: Windows”, on page 135

Connector View	Intellischema Views
securityObject__windows_microsoft_windows_securityEvent_snare	<ul style="list-style-type: none"> • “Security Objects: Windows”, on page 135
startStop__bsm_sun_bsm_sftp	<ul style="list-style-type: none"> • “System Startup and Shutdown”, on page 136 • “Startup and Shutdown: BSM”, on page 138
startstop__microsoft_sql_sensageRetriever	<ul style="list-style-type: none"> • “System Startup and Shutdown”, on page 136
startstop__oracle_adump	<ul style="list-style-type: none"> • “System Startup and Shutdown”, on page 136
startStop__oracle_adump_syslogng	<ul style="list-style-type: none"> • “System Startup and Shutdown”, on page 136
startStop__oracle_alert	<ul style="list-style-type: none"> • “System Startup and Shutdown”, on page 136
startStop__vmware_esx_vcenter_log_collection	<ul style="list-style-type: none"> • “System Startup and Shutdown”, on page 136
startStop__windows_microsoft_windows2008_securityEvent_sensageRetriever	<ul style="list-style-type: none"> • “System Startup and Shutdown”, on page 136 • “Startup and Shutdown: Windows”, on page 137
startStop__windows_microsoft_windows2008_securityEvent_snare	<ul style="list-style-type: none"> • “System Startup and Shutdown”, on page 136 • “Startup and Shutdown: Windows”, on page 137
startStop__windows_microsoft_windows_securityEvent_sensageRetriever	<ul style="list-style-type: none"> • “System Startup and Shutdown”, on page 136 • “Startup and Shutdown: Windows”, on page 137
startStop__windows_microsoft_windows2008_securityEvent_snare	<ul style="list-style-type: none"> • “System Startup and Shutdown”, on page 136 • “Startup and Shutdown: Windows”, on page 137
unparsedData__apache_access_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__apache_error_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__bluecoat_sgproxy_batch	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__catbird_vsecurity_cef_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__checkpoint_opsec_lea	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__cisco_acs_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__cisco_asa_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__cisco_ios_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__cisco_netflow_receiver	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__cisco_pix_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__hp_proCurve_t3t4_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__hp_proCurve_tmsz_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__ibm_db2_rdbms	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
unparsedData__juniper_netscreenFw_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139

Connector View	Intellischema Views
unparsedData__mcafee_database_activity_monitoring_syslogng	• “Unparsed Data”, on page 139
unparsedData__mcafee_epo45_audit_rdbms	• “Unparsed Data”, on page 139
unparsedData__mcafee_epo45_event_rdbms	• “Unparsed Data”, on page 139
unparsedData__mcafee_epo46_audit_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__mcafee_epo46_event_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__mcafee_epo51_audit_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__mcafee_epo51_event_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__mcafee_epo_audit_rdbms	• “Unparsed Data”, on page 139
unparsedData__mcafee_epo_event_rdbms	• “Unparsed Data”, on page 139
unparsedData__mcafee_epo_rdbms	• “Unparsed Data”, on page 139
unparsedData__mcafee_foundstone_rdbms	• “Unparsed Data”, on page 139
unparsedData__mcafee_intrushield_rdbms	• “Unparsed Data”, on page 139
unparsedData__mcafee_intrushield_syslogng	• “Unparsed Data”, on page 139
unparsedData__mcafee_scm_batch	• “Unparsed Data”, on page 139
unparsedData__microsoft_SharePoint_Audit_sensageRetrieverAgent	• “Unparsed Data”, on page 139
unparsedData__microsoft_dns_debug_sensageRetrieverAgent	• “Unparsed Data”, on page 139
unparsedData__microsoft_exchange_admin_events_syslogng	• “Unparsed Data”, on page 139
unparsedData__microsoft_exchange_mailbox_events_syslogng	• “Unparsed Data”, on page 139
unparsedData__microsoft_exchange_tracking_sensageRetrieverAgent	• “Unparsed Data”, on page 139
unparsedData__microsoft_iis	• “Unparsed Data”, on page 139
unparsedData__microsoft_sql_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows2008_appEvent_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows2008_dirEvent_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows2008_dnsEvent_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows2008_frsEvent_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows2008_securityEvent_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows2008_securityEvent_snare	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows2008_sysEvent_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows_appEvent_sensageRetriever	• “Unparsed Data”, on page 139

Connector View	Intellischema Views
unparsedData__microsoft_windows_dirEvent_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows_dnsEvent_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows_frsEvent_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows_securityEvent_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows_securityEvent_snare	• “Unparsed Data”, on page 139
unparsedData__microsoft_windows_sysEvent_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__oracle_adump	• “Unparsed Data”, on page 139
unparsedData__oracle_adump_syslogng	• “Unparsed Data”, on page 139
unparsedData__oracle_alert	• “Unparsed Data”, on page 139
unparsedData__oracle_database_fga_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__oracle_database_sysaudit_sensageRetriever	• “Unparsed Data”, on page 139
unparsedData__oracle_fga_xml_batch	• “Unparsed Data”, on page 139
unparsedData__oracle_listener	• “Unparsed Data”, on page 139
unparsedData__panos_firewall_syslogng	• “Unparsed Data”, on page 139
unparsedData__postgres_audit_csv	• “Unparsed Data”, on page 139
unparsedData__sap_aud_sftp	• “Unparsed Data”, on page 139
unparsedData__sun_bsm_sftp	• “Unparsed Data”, on page 139
unparsedData__symantec_endpoint_syslogng	• “Unparsed Data”, on page 139
unparsedData__syslogng_catchall_syslogng	• “Unparsed Data”, on page 139
unparsedData__tipping_point_syslogng	• “Unparsed Data”, on page 139
unparsedData__unix_ftpd_syslogng	• “Unparsed Data”, on page 139
unparsedData__unix_login_syslogng	• “Unparsed Data”, on page 139
unparsedData__unix_sshd2_syslogng	• “Unparsed Data”, on page 139
unparsedData__unix_su_syslogng	• “Unparsed Data”, on page 139
unparsedData__unix_sudo_syslogng	• “Unparsed Data”, on page 139
unparsedData__vmware_esx_500_syslogng	• “Unparsed Data”, on page 139
unparsedData__vmware_esx_vcenter_event_collection	• “Unparsed Data”, on page 139
unparsedData__vmware_esx_vcenter_log_collection	• “Unparsed Data”, on page 139
userLogin__cisco_asa_syslogng	• “User Logins”, on page 141
userLogin__hp_proCurve_t3t4_syslogng	• “User Logins”, on page 141
userLogin__hp_proCurve_tmsz_syslogng	• “User Logins”, on page 141
userLogin__microsoft_sql_sensageRetriever	• “User Logins”, on page 141
userLogin__oracle_adump	• “User Logins”, on page 141
userLogin__oracle_adump_syslogng	• “Unparsed Data”, on page 139

Connector View	Intellischema Views
userLogin__oracle_database_sysaudit_sensageRetriever	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
userLogin__vmware_esx_500_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
userLogin__vmware_esx_vcenter_event_collection	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
userLogin__vmware_esx_vcenter_log_collection	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139
userLogin__router_cisco_ios_syslogng	<ul style="list-style-type: none"> • “User Logins”, on page 141 • “User Logins: Router”, on page 143 •
userLogin__unix_unix_ftpd_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139 • “User Logins: Linux/Unix”, on page 147
userLogin__unix_unix_login_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139 • “User Logins: Linux/Unix”, on page 147
userLogin__unix_unix_sshd2_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139 • “User Logins: Linux/Unix”, on page 147
userLogin__unix_unix_su_syslogng	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139 • “User Logins: Linux/Unix”, on page 147
userLogin__windows_domainController_microsoft_windows2008_securityEvent_sensageRetriever	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139 • “User Logins: Windows”, on page 144 • “User Logins: Windows”, on page 146
userLogin__windows_domainController_microsoft_windows2008_securityEvent_snare	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139 • “User Logins: Windows”, on page 144 • “User Logins: Windows”, on page 146
userLogin__windows_nonDomainController_microsoft_windows_securityEvent_sensageRetriever	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139 • “User Logins: Windows”, on page 144 • “User Logins: Windows Non-domain Controller”, on page 145
userLogin__windows_nonDomainController_microsoft_windows_securityEvent_snare	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139 • “User Logins: Windows”, on page 144 • “User Logins: Windows Non-domain Controller”, on page 145
userLogin__windows_nonDomainController_microsoft_windows2008_securityEvent_sensageRetriever	<ul style="list-style-type: none"> • “Unparsed Data”, on page 139 • “User Logins: Windows”, on page 144 • “User Logins: Windows Non-domain Controller”, on page 145

Connector View	Intellischema Views
userLogin_windows_nonDomainController_microsoft_windows2008_securityEvent_snare	<ul style="list-style-type: none"> “Unparsed Data”, on page 139 “User Logins: Windows”, on page 144 “User Logins: Windows Non-domain Controller”, on page 145
userLogin_windows_nonDomainController_microsoft_windows_securityEvent_sensageRetriever	<ul style="list-style-type: none"> “Unparsed Data”, on page 139 “User Logins: Windows”, on page 144 “User Logins: Windows Non-domain Controller”, on page 145
userLogin_windows_nonDomainController_microsoft_windows_securityEvent_snare	<ul style="list-style-type: none"> “Unparsed Data”, on page 139 “User Logins: Windows”, on page 144 “User Logins: Windows Non-domain Controller”, on page 145
vulnerability_mcafee_epo45_event_rdbms	• “Vulnerability Event”, on page 148
vulnerability_mcafee_epo46_event_sensageRetriever	• “Vulnerability Event”, on page 148
vulnerability_mcafee_epo51_event_sensageRetriever	• “Vulnerability Event”, on page 148
vulnerability_mcafee_epo_event_rdbms	• “Vulnerability Event”, on page 148
vulnerability_mcafee_epo_rdbms	• “Vulnerability Event”, on page 148
vulnerability_mcafee_foundstone_rdbms	• “Vulnerability Event”, on page 148
vulnerability_symantec_endpoint_syslogng	• “Vulnerability Event”, on page 148
webProxy_apache_access_syslogng	• “webProxy Event”, on page 149
webProxy_bluecoat_sgproxy_batch	• “webProxy Event”, on page 149
webProxy_microsoft_iis	• “webProxy Event”, on page 149

REFERENCE TABLES

The following reference tables are created during IntelliSchema installation:

```
analytics.intellischema._connectors.accountAdditionAndDeletion_reference
analytics.intellischema._connectors.accountAdditionAndDeletion_windows_reference
analytics.intellischema._connectors.adminAccountActivity_reference
analytics.intellischema._connectors.adminAccountActivity_unix_reference
analytics.intellischema._connectors.adminAccountActivity_windows_reference
analytics.intellischema._connectors.alert_reference
analytics.intellischema._connectors.application_reference
analytics.intellischema._connectors.audit_reference
analytics.intellischema._connectors.database_ddl_reference
analytics.intellischema._connectors.database_dml_reference
analytics.intellischema._connectors.idsIps_reference
analytics.intellischema._connectors.investigation_reference
analytics.intellischema._connectors.lossOfAuditMessages_reference
analytics.intellischema._connectors.lossOfAuditMessages_windows_reference
analytics.intellischema._connectors.mail_reference
analytics.intellischema._connectors.malware_reference
analytics.intellischema._connectors.networkDeviceConnection_firewall_reference
analytics.intellischema._connectors.networkDeviceConnection_reference
analytics.intellischema._connectors.networkDeviceConnection_router_reference
analytics.intellischema._connectors.parsedData_reference
```

```
analytics.intellischema._connectors.passwordChangeAndReset_reference
analytics.intellischema._connectors.passwordChangeAndReset_windows_reference
analytics.intellischema._connectors.privilegedCommand_bsm_reference
analytics.intellischema._connectors.privilegedCommand_reference
analytics.intellischema._connectors.privilegedCommand_unix_reference
analytics.intellischema._connectors.privilegedCommand_windows_reference
analytics.intellischema._connectors.remoteAccess_reference
analytics.intellischema._connectors.securityObject_reference
analytics.intellischema._connectors.securityObject_windows_reference
analytics.intellischema._connectors.startStop_bsm_reference
analytics.intellischema._connectors.startStop_reference
analytics.intellischema._connectors.startStop_windows_reference
analytics.intellischema._connectors.unparsedData_reference
analytics.intellischema._connectors.userLogin_reference
analytics.intellischema._connectors.userLogin_router_reference
analytics.intellischema._connectors.userLogin_unix_reference
analytics.intellischema._connectors.userLogin_windows_domainController_reference
analytics.intellischema._connectors.userLogin_windows_nonDomainController_reference
analytics.intellischema._connectors.vulnerability_reference
analytics.intellischema._connectors.webProxy_reference
analytics.intellischema._connectors.wireless_reference
```

ADDING NEW EVENT SOURCES TO INTELLISchema

You can add new log sources to IntelliSchema. It is recommended that you contact Hexis Cyber Solutions Technical Support for assistance in adding new sources. Depending on the level of effort, this assistance may require an additional charge. For more information, see “[Contacting Technical Support](#)”, on page 26.

This section provides a high-level overview of the process.

Overview

Adding a new log source is a multi-step process that includes the following basic steps:

- 1 Analyze the log source. See “[Source Analysis](#)”, on page 166
- 2 Create, configure, and deploy a log adapter to collect, parse and store your log data. See the following topics in the Collector Guide: [Appendix A: SenSage ConsolePTL File Format](#) and [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.
- 3 Create connector views and event-type views. See “[Adding a New Event Source](#)”, on page 166.

Related Information

The following topics provide background information for adding event sources:

- “[Overview of SenSage AP Analytics](#)”, on page 27
- “[IntelliSchema Views Reference](#)”, on page 93
- Defining Views with SenSage AP SQL in Chapter 2, “[SenSage Using the SenSage Event Data Warehouse \(EDW\)](#)” in the *Event Data Warehouse Guide*.

- [Appendix A: SenSage ConsolePTL File Format](#) in the *Collector Guide*.
- [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*

Source Analysis

When adding a log source to IntelliSchema, you first examine your log sources to determine if the event data fits into any of the existing event-type category views such as "User Logins" or "Startup and Shutdown" (See ["About IntelliSchema Views", on page 93](#) for a complete list), or if you need to create new views for new event types. For more information on IntelliSchema architecture, see ["IntelliSchema", on page 28](#).

Adding a New Event Source

To add a new event source to IntelliSchema:

- 1 Create or enable a log adapter to parse and normalize the event data. You create a log adapter using SenSage AP PTL format. See [Appendix A: SenSage ConsolePTL File Format](#) in the *Collector Guide*.
- 2 Create a table in the EDW that stores the normalized event data created by your log adapter. Alternatively a table is automatically created the first time you use a log adapter. If data is not initially loaded into the table, you create a reference table, which is simply an EDW table with no rows. (IntelliSchema views requires a table to query against, even if the table contains no data.) See [Chapter 3: Loading Data into the EDW](#) in the *Administration Guide*.
- 3 Analyze your log source to determine the event types for which you will need to create reports. To see the existing event types in IntelliSchema, see ["About IntelliSchema Views", on page 93](#). You can use one of these existing event types or you can create a new event type.
- 4 Create connector views for each event type you want to report on. See ["Defining Data Objects", on page 120](#) in the *Administration Guide*.
 - If an event type is one that is already part of IntelliSchema, create a connector view that includes the same columns as the event-type view. (See ["About IntelliSchema Views", on page 93](#).) You may include additional columns if needed, but a report that queries the event-type view will only return data in the columns defined in the event-type view). Name the view using the IntelliSchema naming convention. See ["IntelliSchema Naming Conventions", on page 167](#).
 - If you are creating a new event type that is not part of IntelliSchema, create a connector view for the new event type. Name the view using the IntelliSchema naming convention. See ["IntelliSchema Naming Conventions", on page 167](#).

NOTE: IntelliSchema views make extensive use of the SenSage AP _tablematch() function. The views use the function in the SQL `FROM` clause, which allows the views to query against one or more tables or views whose names match a pattern passed to the `_tablematch()` function. Because the views are named consistently, you can use the `_tablematch()` function to query more than one view or table. For more information, see `_tablematch()` in Chapter 4, ["SenSage AP ConsoleSenSage AP SQL Functions"](#) in the *Event Data Warehouse Guide*.

TIP: It may be helpful to view the SQL that defines existing IntelliSchema views to see how the `tablematch()` function is used. The SQL files that define these views are located in your SenSage AP deployment at this location:

`<HawkEye AP Home>latest/analytics/intellischema/<Event-type>`

- 5 (Optional) Create one or more *event-type* views. Event type views query one or more connector views to provide reporting on subsets of a master view. For example, the User Login master view reports on login events from all information systems, while the event-type views for Windows and Unix systems report on logins from each of those types of systems.
- 6 Create an IntelliSchema *master* view that queries one or more connector views. This master view can only include columns that are common to all the queried connector views. Name the master view using the IntelliSchema naming convention. See “[IntelliSchema Naming Conventions](#)”, on page 167. The FROM clause of your view should use the `_tablematch()` function to match the names of connector views and namespaces for the event type. For more information, see `_tablematch()` in Chapter 4, “SenSage AP ConsoleSenSage AP SQL Functions” in the *Event Data Warehouse Guide*.

For example, the following SQL statement defines an IntelliSchema view for the `accountAdditionAndDeletion` event type that matches connector views that begin with the string `"accountAdditionAndDeletion_"`:

```
CREATE OR REPLACE VIEW intellischema.accountAdditionAndDeletion AS
WITH $MATCH as "accountAdditionAndDeletion_.*"
WITH $NS as "intellischema.__connectors"
SELECT
    ts,
    log_type,
    info_sys,
    user_added_deleted,
    event_description
FROM @_tablematch($MATCH, $NS)
DURING ALL
```

IntelliSchema Naming Conventions

The names you assign to views and tables must follow the following naming conventions to work within IntelliSchema.

`<Event Type>__<Source Type>__<zero or more Sub Types>__<Log Adapter Name>.sql`

where:

Event Type is the top-level (master) event type. For example, `securityObject` is the master event type in the following view name:

`securityObject__windows__access__microsoft_windows_securityEvent_snare.sql`

Source Type is the type of information system the view queries such as `firewall`, `unix`, `windows`, and `router`. Separate the source type from surrounding values by using *two* underscore characters. For example, `windows` is the source type in the following view name:

`securityObject__windows__access__microsoft_windows_securityEvent_snare.sql`

Sub Type is optional and represents a further division of Source Type. You can use as many sub-types as necessary. Separate the source type from surrounding values by using *two* underscore characters. For example, `access` is a sub type of `windows`, as shown in the following view name:

`securityObject__windows__access__microsoft_windows_securityEvent_snare.sql`

Log Adapter is the full name of the log adapter used to parse event data and create tables queried by this view. Log adapters typically include single underscore characters as part of their name. Precede the log adapter name with *two* underscore characters. For example, the following view name references the `microsoft_windows_securityEvent_snare` log adapter:

```
securityObject__windows__access__microsoft_windows_securityEvent_snare.sql
```

IMPORTANT: Note the usage of single and double underscores when creating view names.

CHAPTER 6

Analytics Reports Listing

IgniteTech provides a set of reports for common information systems. The following sections provide information on each type of report provided with your SenSage AP software, and a brief description of each report.

COMPLIANCE ANALYTICS REPORTS

ADMINISTRATIVE ACTIVITY MONITORING REPORTS

Report	Description	Page
Privileged Account Access Details	Details of logins attempted by privileged ("administrator" or "root") users	page 185
Privileged Account Access Summary	Summary of logins attempted by privileged ("administrator" or "root") users	page 186
Administrative Account Activity	Account activity of administrative ("administrator" or "root") users	page 187
Administrative Account Activity Top 100 Summary	Top 100 summary of administrative account activity	page 188
Privileged Command Summary	Summary of logins using privileged access	page 189

USER-LEVEL REPORTS

Report	Description	Page
User Login Details	Details of login attempts for all user accounts	page 190
User Login Summary	Summary of login attempts for all user accounts	page 192
Logins Outside Business Hours	Displays successful logins outside of business hours on all operating systems, local or remote between the hours of 8:00AM and 6:00PM local time.	page 193
Logins Outside Business Hours Summary	A summary of successful logins outside of business hours on all operating systems, local or remote between the hours of 8:00AM and 6:00PM local time.	page 194

GENERAL COMPLIANCE REPORTS

Report	Description	Page
System Startup and Shutdown	Details the time of system startups and shutdowns for all information systems	page 196
Security Objects Accessed	Details security objects that were accessed.	page 198
Security Objects Deleted	Details security objects that were deleted.	page 199

NETWORK DEVICE MONITORING REPORTS

Report	Description	Page
Router Denied Connections Details	Details of all denied connections to routers and switches.	page 201
Router Authentication Failure Details	Number of authentication failures for all routers and switches.	page 202

FIREWALL MONITORING REPORTS

Report	Description	Page
Firewall Denied Connections Details	Details of denied firewall connections.	page 204
Firewall Denied Connections Summary	Number of denied connections on each firewall by protocol.	page 205
Firewall Accepted Connections Details	Details of accepted connections on each firewall by access list or rule.	page 206
Firewall Accepted Connections Summary	Number of accepted connections and sources on each firewall by protocol and event source.	page 207
Firewall All Connections Details - new	Details of accepted and denied connections on each firewall by access list or rule	page 208

FOUNDATION REPORTS

WINDOWS

Report	Description	Page
Windows Login Activity Details	Details of login activities recorded by Microsoft Windows systems that are not Domain controllers.	page 213
Windows Login Failure Summary	A summary of the number of failed login attempts recorded by Microsoft Windows systems that are not Domain controllers.	page 214
Windows Login Success Summary	A summary of the number of successful logins recorded by Microsoft Windows systems that are not Domain controllers	page 215
Windows Login Failure Details	Details of failed logins and locked out accounts from Microsoft Windows Domain controllers	page 216
Windows Remote Login Details	Details of remote login activities recorded by Microsoft Windows systems that are not Domain controllers.	page 217
Windows Account Addition and Deletion	Details of all activity related to the addition and deletion of user or service accounts on Microsoft Windows systems that are members of a Windows Domain.	page 218
Windows Account Modification	Details of Windows account modification events.	page 219

Report	Description	Page
Windows Group Member Addition and Deletion	Details of all actions on a Windows Domain Controller involving the addition or deletion of an account on a local or global group.	page 220
Windows Group Modification Summary	A summary of group modification activity. Includes the attributes and parameters changed, if available.	page 221
Windows Password Changes and Resets	Details of all password changes that occur on Microsoft Windows systems. Identifies when a user changes their own account, other accounts and when a password is reset.	page 222
Windows User Account Locked and Unlocked by Date	Details each user account that is locked or unlocked by date.	page 223
Windows User Activity Journal	Details of user activity.	page 224
Windows Account Rights Modified	A detailed view of privileged account escalations and de-escalations on Microsoft Windows systems	page 225
Windows User Special Privileges Details	Details of activities on Microsoft Windows systems using privileged accounts	page 226
Windows Privileged Account Access	Details of privileged account access.	page 227
Windows System Startup Summary	Displays startup messages from Microsoft Windows systems	page 228
Windows Audit Log Cleared Summary	Displays attempts by a user on a Microsoft Windows system to clear the event log	page 231
Windows Application Events	Lists each Windows application event per day	page 232
Windows Application Events Summary per Day	Summary of Windows application events per day by computer and Windows application version	page 233
Windows New Process Started	Details of new processes started on Microsoft Windows systems.	page 229
Windows New Process Started Summary	Summary information about new process (total amount of new processes grouped by date, computer, and user.)	page 230
Windows System Events	List of each Windows system event per day	page 234
Windows System Event Summary per Day	Summary of Windows system events per day by computer and Windows system version	page 235
Windows File Replication Service Events	List of each Windows file replication service event per day	page 236
Windows File Replication Service Events Summary per Day	Summary of Windows file replication events per day by computer and Windows system version.	page 237
Windows Error Events	Lists each Windows error event per day	page 238
Windows DNS Server Events	Lists each Windows DNS server event per day	page 239
Windows DNS Server Events Summary per Day	Summary of DNS server events per day by computer and Windows system version	page 240
Windows Directory Service Events	Lists each Windows Directory Service event per day	page 241

Report	Description	Page
Windows Directory Service Events Summary per Day	Summary of Directory Service events per day by computer and Windows system version	page 242
Windows Loss of Audit Messages	Summary of the number of audit messages lost by a Microsoft Windows system	page 244
Windows Major Security Events	Details of Windows major security events.	page 243
Windows Active Directory Object Changes	Details of attempts to change Active Directory objects.	page 245
Windows Active Directory Policy Changes	Details of attempts to change Active Directory policies.	page 246
Windows Active Directory Users: Deleted or Disabled	Details of deleted or disabled Active Directory users.	page 247
Windows Active Directory Users: Lockouts and Password Resets	Details of Active Directory users' events (lockouts and password resets)	page 248
Windows Active Directory Users: New or Enabled	Details of Active Directory users' events (new or enabled).	page 249
Windows Security Objects Accessed	Details of attempts to access a security object on a Microsoft Windows system	page 250
Windows Security Objects Deleted	Details of attempts to delete security objects on a Microsoft Windows system	page 251
Windows Security Objects Access Optimized	Details of attempts to access a security object on a Microsoft Windows system.	page 252

UNIX/LINUX

Report	Description	Page
Unix/Linux Login Details	Details of login attempts on Unix or Linux systems	page 254
Unix/Linux Failed Login Summary by User	Displays the number of failed login attempts by user on Unix or Linux systems for each information system and event source	page 255
Unix/Linux Failed Login Summary by Count	Displays the number of failed login attempts by count on Unix or Linux systems for each information system and event source	page 256
Unix/Linux Failed Login Summary by Server	Displays the number of failed login attempts by server on Unix or Linux systems for each information system and event source.	page 256
Unix/Linux Logins Summary by User	Displays the number of successful and unsuccessful login attempts by user on Unix or Linux systems for each information system and event source	page 258
Unix/Linux Logins Summary by Count	Displays the number of successful and unsuccessful login attempts by count on Unix or Linux systems for each information system and event source	page 259
Unix/Linux Logins Summary by Server	Displays the number of successful and unsuccessful login attempts by count on Unix or Linux systems for each information system and event source	page 260

Report	Description	Page
Unix/Linux SSH and FTP Login Details	Details of login attempts on Unix or Linux systems	page 261
Unix/Linux Privileged Commands Detail	Details of privileged commands executed on Unix or Linux systems	page 262
Unix/Linux Elevated Access (su and sudo) Summary by Count	Displays elevated access (su and sudo) summary by count executed on Unix or Linux systems	page 263
Unix/Linux Elevated Access (su and sudo) Summary by Date	Displays elevated access (su and sudo) summary by date executed on Unix or Linux systems	page 264
Unix/Linux Elevated Access (su and sudo) Summary by Server	Displays elevated access (su and sudo) summary by server executed on Unix or Linux systems	page 265
Unix/Linux Elevated Access Failed Detail (su and sudo) by Date	Displays elevated access (su and sudo) failure detail by date on Unix or Linux systems	page 266
Unix/Linux Elevated Access Failed Summary (su and sudo) by Count	Displays elevated access (su and sudo) failure detail by date on Unix or Linux systems	page 267
Unix/Linux Elevated Access Failed Summary (su and sudo) by Server	Displays elevated access (su and sudo) failure detail by date on Unix or Linux systems	page 268
Unix/Linux Elevated SU Access Failed by Server	Displays elevated access (su and sudo) failure detail by date on Unix or Linux systems	page 269
Unix/Linux Elevated SUDO Access Failed by Date	Displays elevated access (su and sudo) failure detail by date on Unix or Linux systems	page 270
Unix/Linux Elevated SUDO Access Failed by Server	Displays elevated access (su and sudo) failure detail by date on Unix or Linux systems	page 271

SYSTEMS ANALYTICS REPORTS

EDW (SLS) TOOLS MONITORING REPORTS

Report	Description	Page
SLS ATManage Command History	History of EDW (SLS) ATManage tool command usage.	page 27 4
SLS ATQuery Command History	History of EDW (SLS) ATQuery tool command usage.	page 27 5
SLS Command History	History of EDW (SLS) commands.	page 27 6
SLS Command History per User	History of EDW (SLS) command History per User	page 27 7
SLS Command Load History	History of EDW (SLS) Load command	page 27 8

Report	Description	Page
SLS Percent Disk Space Usage	Percent of disk space used for each EDW (SLS) node in SenSage AP deployment.	page 27 9
SLS Percent Disk Space Usage Alerts	Displays status of EDW (SLS) disk space by EDW (SLS) node when free disk space is less than 40% of the total disk space.	page 28 0
SLS Percent Disk Space per Node	Total and free disk space used for each EDW (SLS) node in the SenSage AP deployment.	page 28 1

COLLECTOR ACTIVITY MONITORING REPORTS

Report	Description	Page
Collector Avg Load Size per Event Source	Average size of data loaded by the SenSage AP Collector for each event source	page 27 2
Collector Collection Exceeds x Event per Day -- Exception Report	A summary of daily loads by the SenSage AP Collector with status of thresholds exceeds	page 27 3
Collector Collection Exceeds x GB per Day -- Exception Report	Daily size of loaded records by the SenSage AP Collector with status of thresholds exceeds	page 27 4
Collector Daily Load - Trend	Size of data loaded by the SenSage AP Collector per day	page 27 5
Collector Daily Load per Event Source	Volume of data loaded by the SenSage AP Collector for each event source	page 27 6
Collector Daily Load per loaderEnd Type	Size of data loaded by the SenSage AP Collector per day for loaderEnd Type	page 27 7
Collector EPS Statistics	EPS statistics of data loaded by the SenSage AP Collector	page 27 8
Collector Load Volume per Day	Average size of data loaded by the SenSage AP Collector for each event source	page 27 9
Collector Table Sizes per Time range	Total size of data loaded into a table by SenSage AP Collector for a given time range	page 28 0
Collector Total Load Volume per Event Source	Total number of records and average size of records loaded by the SenSage AP Collector for each event source.	page 28 1
Collector Total Number of Records and Avg Record Size per Source	Total number of records and average size of records loaded by the SenSage AP Collector for each event source.	page 28 2
Collector Table Number of Records in System	Total number of records and size of records loaded by the SenSage AP Collector in the System	page 28 3
Collector Total Records Loaded per Table	Total number of records and size of loaded data by the SenSage AP Collector for each table	page 28 4
Collector Total Records Loaded per Table per Day	Total number of records and size of loaded data by the SenSage AP Collector for each table per day	page 28 5
Collector Total Number of Records in System	Total number of records and size of loaded data for a time range by the SenSage AP Collector	page 28 6

INTERNAL SYSTEM REPORTS

Report	Description	
Internal System Failed Login Details	Details of failed logins to SenSage AP deployment	page 29 9
Internal System Report Activity Details	Details of activities involving a SenSage AP report, by user. Activities include: creating a report, editing a report, running a report, and viewing a report	page 30 0
Internal System Report Activity Summary	Summary of report activity in a SenSage AP deployment. Includes the number of times a report was edited or run and the time the report was last edited or run.	page 30 1
Internal System Successful Admin Login to System	Number of successful admin logins to the SenSage AP system	page 30 2
Internal System Successful Login Details	Details of successful user logins to the SenSage AP system	page 30 3
Internal System Successful Summary Login to System	Summary of successful logins to the SenSage AP system	page 30 4
Internal System User Activity Details	Details of user activities in a SenSage AP deployment	page 30 5
Internal System User Activity Summary	Summary of user activities in a SenSage AP deployment	page 30 6
Internal System User Password Change	Password changes to a SenSage AP deployment	page 30 7

MCAFEE ANALYTICS REPORTS***MCAFEE EMAIL AND WEB SECURITY (EWS)***

Report	Description	Page
EWS Virus Email Details	Displays viruses detected in email	page 309
EWS Virus Web Details	Displays viruses detected in Web pages	page 310
EWS Virus Web Summary	Summary of viruses detected in Web pages whose domain is located outside of the United States	page 311

MCAFEE DATABASE ACTIVITY MONITORING

Report	Description	Page
Detail Last 100 records	Details last 100 events from McAfee Database Activity Monitoring log	page 313
Detail top 100 records	Details the first 100 events from McAfee Database Activity Monitoring log	page 315
Investigation Most Active Agent Host	Displays the most active agent hosts	page 317

Report	Description	Page
Investigation Most Active Agent IP	Displays the most active agent IPs	page 317
Investigation Most Active Command Type	Displays the most active command types	page 319
Investigation Most Active Database Name	Displays the most active database names	page 320
Investigation Most Active Database Type	Displays the most active database types	page 320
Investigation Most Active Database Version	Displays the most active database versions	page 321
Investigation Most Active Exec User	Displays the most active exec users	page 321
Investigation Most Active Module	Displays the most active modules	page 321
Investigation Most Active OS User	Displays the most active OS users	page 322
Investigation Most Active Program	Displays the most active programs	page 323
Investigation Most Active Reporter Host	Displays the most active reporter hosts	page 323
Investigation Most Active Rule Name	Displays the most active rule names	page 324
Investigation Most Active Source Host	Displays the most active source hosts	page 325
Investigation Most Active Source IP	Displays the most active source IPs	page 325
Investigation Wizard	Displays the most active monitoring host	page 326
Statistics Command Type Access by Database Type, Name	Displays the statistics command type access by database name	page 328
Statistics Database Name Access by Database Type	Displays the statistic database name access by database type	page 329
Statistics Transaction Type Access by Database Type, Name	Displays the statistic transaction type access by database type and name	page 330

MCAFEE EPOLICY ORCHESTRATOR (EPO)

Report	Description	Page
ePO Top Threats	Details overall top 20 reported malware threats for all client systems	page 331
ePO Console Logon Activity	Displays ePO server console administrative logons, sorted by time	page 332
ePO Agents by Server	Displays number of client agents being serviced by each ePO server	page 333

Report	Description	Page
ePO Console Activity Summary	Displays count of actions by username	page 334
ePO Agent Communication Detail	Displays last check-in times of ePO client agents, sorted by time	page 335
ePO Agent Communication Top 100 summary	Displays number of times ePO client agents check in, by hostname, IP server, and Analyzer name	page 336

MCAFEE INTRUSHIELD NETWORK SECURITY PLATFORM (NSP)

Report	Description	Page
NSP Possible Successful Exploits (by Target)	IntruShield: displays exploits with some chance of success (by target). Lists systems that may have been compromised, ordered by likelihood of having been successfully compromised.	page 338
NSP Possible Successful Exploits (by Source)	IntruShield: displays exploits with some chance of success (by source). Lists hostile systems, ordered by the likelihood they are actually hostile.	page 339
NSP Attacks Details	IntruShield: displays system attacks by severity with target/source IP and target/source port.	page 340
NSP Attacks Summary	IntruShield: summary of system attacks by severity and count.	page 341
NSP 20 Most Common Events	IntruShield: displays the top 20 most common found events and the number of occurrences of each	page 342
NSP Top 10 Source IP	IntruShield: displays top 10 system attacks by source IP	page 343
NSP Top 10 Target IP	IntruShield: displays top 10 IP attacks with attack description and number of attacks.	page 344
NSP Top 10 Directed Attacks	IntruShield: displays top 10 system attacks by source, destination, and severity. (A directed attack is an attack originating from a single system targeted against another single system.)	page 345

MCAFEE VULNERABILITY MANAGER (FOUNDSTONE)

Report	Description	Page
Foundstone OS & Application Vulnerabilities	Vulnerability Manager: displays number of vulnerabilities reported by category from OS or application layer issues.	page 346
Foundstone Top 20 Affected Hosts	Vulnerability Manager: displays top 20 systems reporting vulnerabilities.	page 348
Foundstone High Risk Vulnerabilities	Vulnerability Manager: Client systems reporting a vulnerability level of 10, the highest risk, items, sorted by date.	page 349
Foundstone High Risk Vulnerabilities Top 100 Summary	Vulnerability Manager: displays number of High Risk (10) Vulnerabilities and their description by IP Address	page 350

BLUECOAT REPORTS

Report	Description	Page
BlueCoat - High Offender List	Displays the number of filtered sources by category and client IP address	page 351
BlueCoat - Individual IP Usage Detail	Displays all BlueCoat logs for an individual client IP address.	page 352
BlueCoat - Top 10 Domains Visited	Displays the top 10 visited domains	page 353
BlueCoat - Top Domains Visited by UserID	Displays top domains visited by a user	page 354
BlueCoat - Top Download Users	Displays top users by the total size of the downloaded content	page 355
BlueCoat - Top Sending Users	Displays report that is equivalent to "BlueCoat - Top Download Users"	page 356
BlueCoat - Top Users with Most Site Visits	Displays the top 100 users with the most site visits	page 357

HAWKEYE G REPORTS

ACTIONS MONITORING REPORTS

Report	Description	Page
Actions: File List Details	Details a file list of events in which an infected host was detected	page 360
Actions: File List Investigation	Details a file list for investigation in which an infected host was detected	page 361
Actions: File List Summary	Details a summary list of hosts and the number of events in which infection was detected	page 362
Actions: Kill Process Details	Details an event listing in which detection of an infected host resulted in a kill process	page 363
Actions: Kill Process Investigation	Details a file list for investigation in which the detection of the infected host resulted in a kill process	page 364
Actions: Kill Process Summary	Details a summary list of hosts and the number of events in which infection was detected, resulting in a kill process	page 365
Actions: Network Connection Details	Details an event listing in which an infected host was detected on a network connection	page 366
Actions: Network Connection List Investigation	Details a file list for investigation in which an infected host was detected on a network connection	page 367
Actions: Network Connection List Summary	Details a summary list of infected hosts on a network connection and the number of events in which infection was detected	page 368

Report	Description	Page
Actions: Process List Details	Details a process listing in which infected hosts were detected	page 369
Actions: Process List Investigation	Details a file list for investigation in which infected hosts were detected during a process	page 370
Actions: Process List Summary	Details a summary list of infected hosts and the number of events in which infection was detected during a process	page 371
Actions: Quarantine File Details	Details quarantine file listing in which infected hosts were quarantined	page 372
Actions: Quarantine File Investigation	Details a file list for investigation of infected hosts that were quarantined	page 373
Actions: Quarantine File Summary	Details a summary list of hosts and the number of events in which infected hosts were quarantined	page 375
Actions: Registry List Details	Details registry file listing of infected hosts	page 376
Actions: Registry List Investigation	Details a registry file list for investigation of infected hosts.	page 378
Actions: Registry List Summary	Details a registry summary list of hosts and the number of events in which the host was infected	page 379
Actions: Undo Quarantine File Details	Details quarantine file listing of infected hosts that were undone	page 380
Actions: Undo Quarantine File Investigation	Details investigation file listing of infected hosts that were undone	page 381
Actions: Undo Quarantine File Summary	A quarantine file summary list of infected hosts and number of events that were undone	page 382

ALL EVENTS MONITORING REPORTS

Report	Description	Page
All Events Details	All events details of infected hosts	page 383
All Events Investigation	All events of infected hosts for investigation	page 385
Actions: File List Summary	All events summary by event type	page 387

DEVICE THREATSYNC MONITORING REPORTS

Report	Description	Page
Device ThreatSync Score Changes Details	Details devices with ThreatSync Score Changes	page 389
Device ThreatSync Score Changes Details Investigation	Details devices with ThreatSync Score Changes for investigation	page 390
Device ThreatSync Score Changes Summary by Host	Summary of devices with ThreatSync Score Changes by host	page 391

HEURISTICS MONITORING ACTIVITY REPORTS

Report	Description	Page
Heuristics: File Details	Details heuristics of infected hosts.	page 393
Heuristics: File Investigation	Details heuristics of infected hosts for investigation	page 394
Heuristics: File Top 100 Summary	Summary of heuristics for top 100 Summary infected hosts	page 395
Heuristics: Process Details	Details of process heuristics for infected hosts	page 396
Heuristics: Process Investigation	Details of process heuristics of infected hosts for investigation	page 397
Heuristics: Process Summary	Summary of process heuristics for infected hosts	page 398
Heuristics: Registry Details	Details of registry heuristics for infected hosts	page 399
Heuristics: Registry Investigation	Details of registry heuristics of infected hosts for investigation	page 400
Heuristics: Registry Summary	Summary of registry heuristics for infected hosts	page 401

EVENT INDICATOR ACTIVITY MONITORING REPORTS

Report	Description	Page
Indicator: DNS Inject Details	Details DNS inject for infected hosts with specific event (Indicator) ID	page 403
Indicator: DNS Inject Investigation	Details DNS inject of infected hosts with specific event (Indicator) ID for investigation	page 405
Indicator: DNS Inject Summary	Summary of DNS injects for infected hosts with a specific Event (Indicator) ID	page 407
Indicator: IP Redirect Details	Details IP redirect of infected hosts with specific event (Indicator) ID	page 408
Indicator: IP Redirect Investigation	Details IP redirect of infected hosts with specific event (Indicator) ID for investigation.	page 410
Indicator: IP Redirect Summary	IP redirect summary of infected hosts with the number of events	page 412
Indicator: URL Match Details	Details URL match (through rule) of infected hosts	page 413
Indicator: URL Match Investigation	Details URL match (through rule) of infected hosts for investigation	page 414
Indicator: URL Match Top 100 Summary	Summary of top 100 URL matches (through rule)	page 415

MIS POTENTIAL MONITORING REPORTS

Report	Description	Page
Malware Identification Service (MIS) Potential: File Details	Details file of hosts potentially infected from malware	page 417
Malware Identification Service (MIS) Potential: File Investigation	Details file of hosts potentially infected from malware for investigation	page 418
Malware Identification Service (MIS) Potential: File Summary	Summary file of hosts potentially infected from malware from a specific indicator (event ID)	page 419
Malware Identification Service (MIS) Potential: Process Details	Details process (from command line) that occurred on infected hosts from malware	page 420
Malware Identification Service (MIS) Potential: Process Investigation	Details process (from command line) that occurred on infected hosts from malware for investigation (Process ID)	page 421
Malware Identification Service (MIS) Potential: Process Summary	Process summary (file) on infected hosts from malware with the number of events	page 422
Malware Identification Service (MIS) Potential: Registry Details	Details registry of infected hosts from malware	page 423
Malware Identification Service (MIS) Potential: Registry Investigation	Details registry of infected hosts from malware for investigation	page 424
Malware Identification Service (MIS) Potential: Registry Summary	Summary registry of infected hosts from malware	page 425

THREAT MATCH MONITORING REPORTS

Report	Description	Page
Threat Match: File Details	Details file of all threat matches on infected hosts	page 427
Threat Match: File Investigation	Detail file of all threat matches on infected hosts for investigation	page 428
Threat Match: File Top 100 Summary	The top 100 summary of infected hosts with threat matches along with the number of events	page 429
Threat Match: Process Details	Details process of infected hosts with threat matches	page 430
Threat Match: Process Investigation	Details process of infected hosts with threat matches for investigation	page 431
Threat Match: Process Top 100 Summary	The top 100 process (command line) summary of infected hosts with threat matches along with the number of events	page 432

Report	Description	Page
Threat Match: Registry Details	Details registry of infected hosts with threat matches.	page 433
Threat Match: Registry Investigation	Details registry of infected hosts with threat matches for investigation	page 434
Threat Match: Registry Top 100 Summary	The top 100 registry summary of Window hosts with threat matches along with the number of events	page 435

PANOS REPORTS

Report	Description	Page
IP Based Data Query	Displays the PanOS Firewall logs for an individual source IP address	page 437
Threats Blocked Per Hour: Total by IAP	Displays threats blocked per hour by total by Internet Access Provider (IAP)	page 438
Top 100 Source-Destination IP Pairs by Session Count	Displays top 100 source-destination IP Pairs by session count	page 439

SAP REPORTS

Report	Description	Page
SAP Security Audit - Program Summary	Displays program summary for SAP Security audit	page 441
SAP Security Audit - Terminal Summary	Displays terminal summary for SAP Security audit.	page 442
SAP Security Audit - Top 10 Records	Displays the top 10 visited domains	page 443
SAP Security Audit - User Summary	Displays user summary for SAP Security audit	page 444

MISCELLANEOUS REPORTS

STANDALONE REPORTS

Report	Description	Page
Investigation Report	Query all data in the EDW collected by standard log adapters that have been enabled for data collection	page 446

MICROSOFT EXCHANGE

Report	Description	Page
Microsoft Exchange - Audit Trail Integrity Events	Display audit trail integrity events for Microsoft Exchange	page 447

CHAPTER 7

Compliance Analytics Reports

The SenSage AP Compliance Analytics reports assist organizations in meeting specific regulations. These reports are designed to monitor critical areas of your information infrastructure, enabling your organization to reach new levels of visibility into the event sources being monitored.

This chapter provides a reference for Compliance Analytics reports, including lists of columns available for reporting and compliance regulations addressed by each report. The Compliance Analytics reports include the following groups of reports:

- “Privileged Account Access Details”, next
- “User-Level Reports”, on page 190
- “General Compliance Reports”, on page 196
- “Firewall Monitoring Reports”, on page 203

ADMINISTRATIVE ACTIVITY MONITORING REPORTS

The Administrative Activity Monitoring group of reports display administrative (privileged) account access information and includes the following reports:

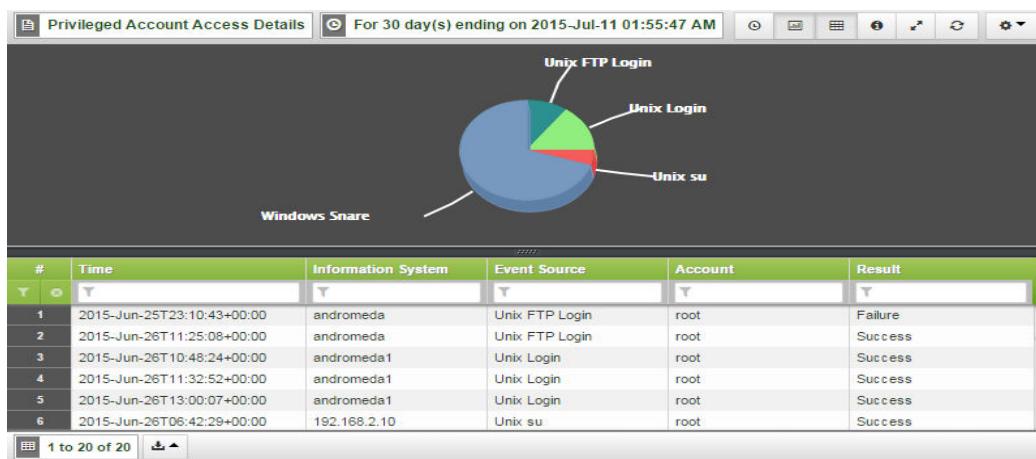
- “Privileged Account Access Details”, next
- “Privileged Account Access Summary”, on page 186
- “Administrative Account Activity”, on page 187
- “Administrative Account Activity Top 100 Summary”, on page 188
- “Privileged Command Summary”, on page 189

Privileged Account Access Details

Details of logins attempted by privileged (“administrator” or “root”) users.

COLUMNS

Columns	Description
Time	Time the privileged access occurred (yyyy-mm-dd hh:mm:ss)
Information System	Machine where the privileged account access occurred
Event Source	Event source that recorded the event
Account	User account used for access
Result	Result of privileged account access. Possible values: <ul style="list-style-type: none">• Failure• Success• Unknown

EXAMPLE**INTELLISchema View**

- “Account Addition and Deletion”, on page 95

TABLES REFERENCED

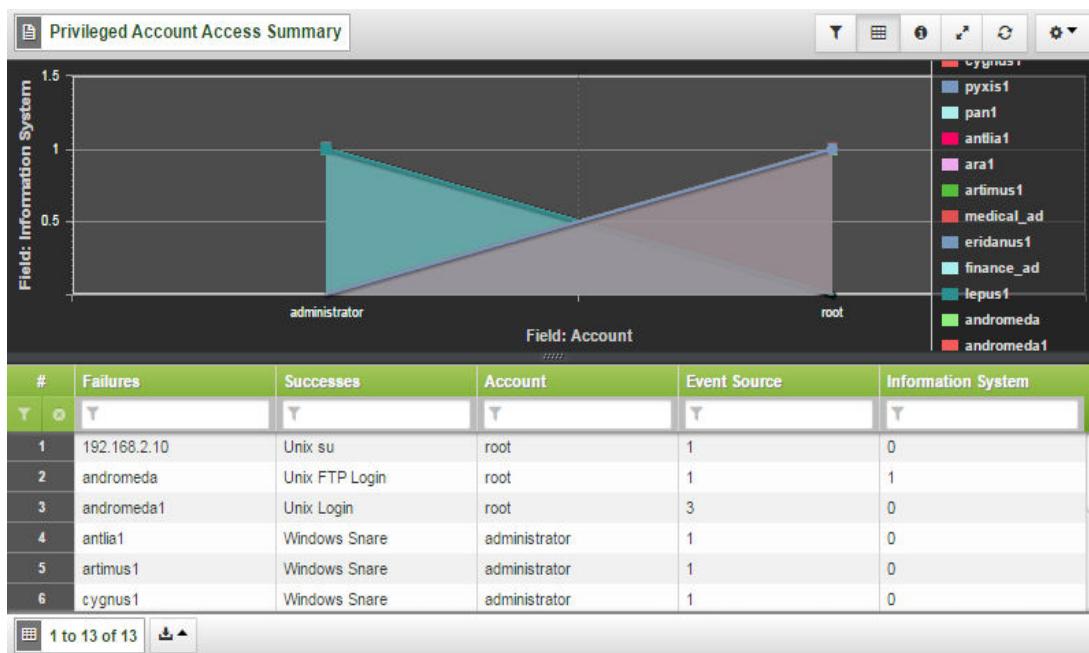
- None

Privileged Account Access Summary

Summary of logins attempted by privileged (“administrator” or “root”) users.

COLUMNS

Columns	Description
Failures	Machines where privileged account access failed.
Successes	Machines where privileged account access was successful.
Account	User account used for access
Event Source	Event source that recorded the event
Information System	Machine where the privileged account access occurred

EXAMPLE**INTELLISchema VIEW**

- “Account Addition and Deletion”, on page 95

TABLES REFERENCED

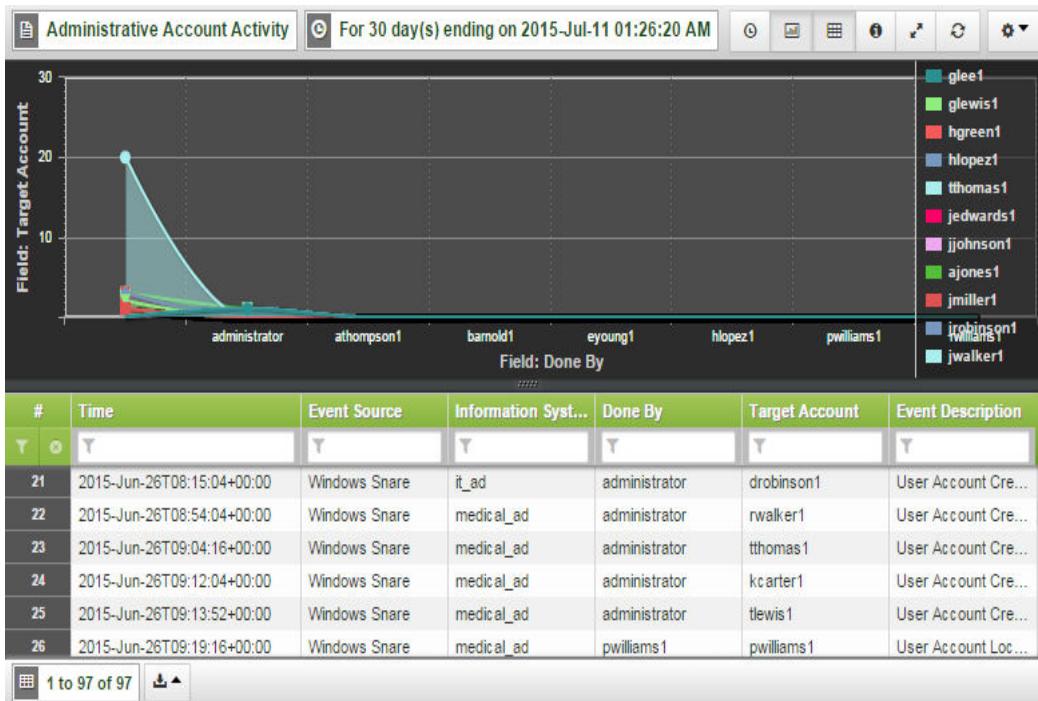
- None

Administrative Account Activity

Account activity of administrative (“administrator” or “root”) users.

COLUMNS

Columns	Description
Time	Time the privileged access occurred (yyyy-mm-dd hh:mm:ss)
Information System	Machine where the privileged account access occurred
Event Source	Event source that recorded the event
Account	User account used for access
Result	Result of privileged account access. Possible values: <ul style="list-style-type: none"> Failure Success Unknown

EXAMPLE**INTELLISchema View**

- “Administrative Account Activity: Windows”, on page 100

TABLES REFERENCED

- None

Administrative Account Activity Top 100 Summary

Top 100 summary of administrative account activity.

COLUMNS

Columns	Description
Time	Time the privileged access occurred (yyyy-mm-dd hh:mm:ss)
Information System	Machine where the privileged account access occurred
Event Source	Event source that recorded the event
Account	User account used for access
Result	Result of privileged account access. Possible values: <ul style="list-style-type: none"> • Failure • Success • Unknown

EXAMPLE

Administrative Account Activity Top 100 Summary					
#	Event Source	Information S...	Done By	Event Descrip...	Number of Ev...
1	Windows Retrie...	corpserv01	admin_jsmith	User Account ...	1
2	Windows Retrie...	testad23	testad23\$	User Account L...	1
3	Windows Retrie...	testad23	administrator	User Account ...	2
4	Windows Retrie...	corpserv01	sys_provisioner	User Account ...	2
5	Windows Retrie...	testad23	administrator	User Account ...	3
6	Windows Retrie...	win-012345abc...		User Account ...	3
7	Windows Snare	c3devweb3			3

1 to 9 of 9

INTELLISchema View

- “Administrative Account Activity: Windows”, on page 100

TABLES REFERENCED

- None

Privileged Command Summary

Summary of logins using privileged access.

COLUMNS

Columns	Description
Time	Time the privileged access occurred (yyyy-mm-dd hh:mm:ss)
Information System	Machine where the privileged account access occurred
Event Source	Event source that recorded the event
Account	User account used for access
Result	Result of privileged account access. Possible values: <ul style="list-style-type: none"> • Failure • Success • Unknown

EXAMPLE

The screenshot shows a software interface titled "Privileged Command Summary". The main area is a table with the following columns: #, Information System, Event Source, Number Successful, and Number Failed. The table contains 7 rows of data. At the bottom left of the table is a page navigation bar showing "1 to 223 of 223".

#	Information System	Event Source	Number Successful	Number Failed
1	16.89.76.78	HP SKM Activity Log	1	0
2	16.89.77.6	HP SKM Activity Log	21	0
3	10.42.1.38	Microsoft Exchange ...	139	0
4	-	Solaris BSM	1	1
5	10.0.0.50	Unix su	10	4
6	aix-01	Unix su	5	4
7	fakehost3	Unix su	3	1

INTELLISchema View

- “Privileged Commands”, on page 129

TABLES REFERENCED

- None

USER-LEVEL REPORTS

The User-Level Reports group of reports displays user login events and includes the following reports:

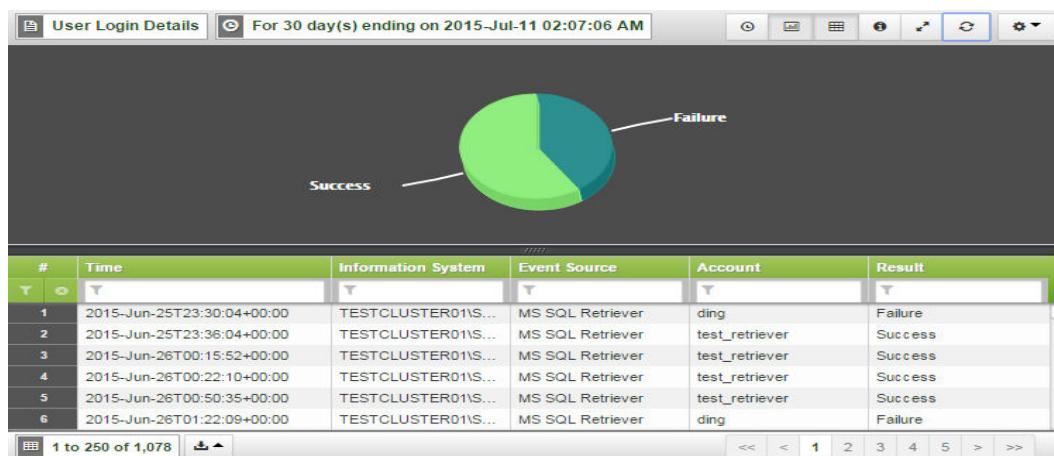
- “User Login Details”, next
- “User Login Summary”, on page 192
- “Logins Outside Business Hours”, on page 193
- “Logins Outside Business Hours Summary”, on page 194

User Login Details

Details of login attempts for all user accounts.

COLUMNS

Column	Description
Time	Time the login occurred (yyyy-mm-dd hh:mm:ss)
Information System	Machine logged into
Event Source	Event-log source that recorded the event
Account	User account logged into
Result	Result of login. Possible values: <ul style="list-style-type: none">• Failure• Success• Unknown

EXAMPLE**INTELLISchema View**

- “User Login Details”, on page 190

TABLES REFERENCED

- None

User Login Summary

Summary of login attempts for all user accounts.

COLUMNS

Column	Description
Time	Time the login occurred (yyyy-mm-dd hh:mm:ss)
Information System	Machine logged into
Event Source	Event-log source that recorded the event
Account	User account logged into
Result	Result of login. Possible values: <ul style="list-style-type: none">• Failure• Success• Unknown

EXAMPLE

#	Information S...	Event Source	Successes	Failures	Accounts
1	15.61.164.89	HP SKM Activit...	21462	1	1
2	oracle.sensage...	Oracle SysAudit	19994	6	3
3	finance_ad	Windows Snare	13572	0	1
4	medical_ad	Windows Snare	11310	0	1
5	it_ad	Windows Snare	3433	0	1
6	hr_ad	Windows Snare	1326	0	1
7	sculptor	Windows Snare	702	0	1

INTELLISchema View

- “User Login Details”, on page 190

TABLES REFERENCED

- None

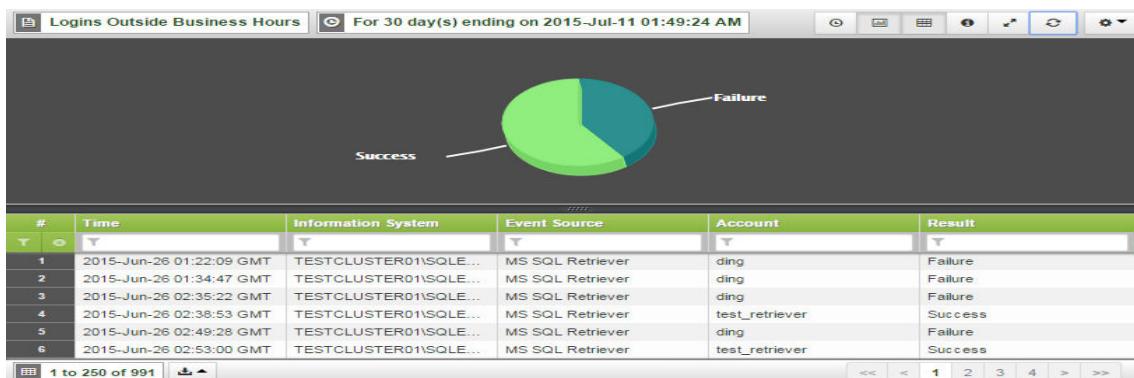
Logins Outside Business Hours

Displays successful logins outside of business hours on all operating systems, local or remote between the hours of 8:00AM and 6:00PM local time. You may change the time zone and business hours used in this report by specifying. See “[Changing the Time Zone and Business hours](#)”, on page 193.

COLUMNS

Column	Description
Time	Time the login occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Information System	Machine logged into
Event Source	Event-log source that recorded the event
Account	User account used for login
Result	Result of login attempt. Possible values: <ul style="list-style-type: none"> • Failure • Success • Unknown

EXAMPLE



INTELLISchema View

- “[User Login Details](#)”, on page 190

TABLES REFERENCED

- None

CHANGING THE TIME ZONE AND BUSINESS HOURS

To change the time zone and business hours, you modify the SQL code that generates this report. You can change setting for time zone, day end time, and day start time. The following SQL statements may need modification:

```
WITH $TZ AS 'PST8PDT'
WITH $DAY_END    as _int64(1800)
WITH $DAY_START  as _int64(0800)
```

To modify the SQL code:

- 1 Change the time zone. This report defaults to use the US/Pacific time zone. Replace the characters "PST8PDT" with the appropriate time zone code for your location. To find the correct code, see [Appendix B: Time Zones](#) in the *Event Data Warehouse Guide*.
- 2 Change the time the day ends. Replace the time the day ends within the parentheses of the line containing "\$DAY_END"
- 3 Change the time the day starts. Replace the time the day starts within the parentheses of the line containing "\$DAY_START".

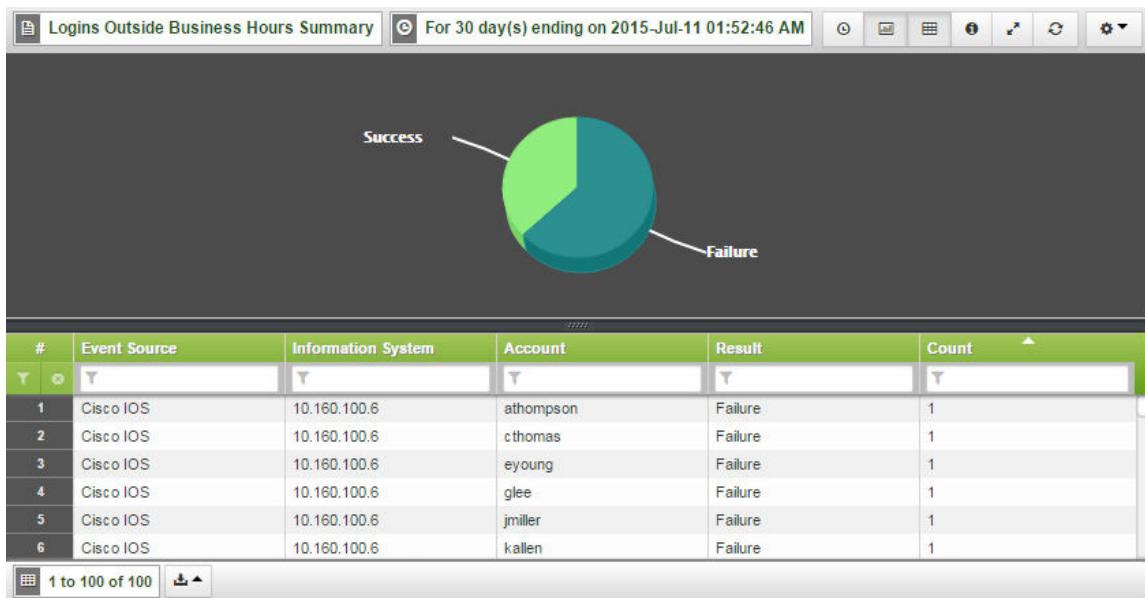
IMPORTANT: To specify time, use 24 hour time notation, without colons or other punctuation. For example, 3:00 PM is represented as (1500).

Logins Outside Business Hours Summary

Displays summary of successful logins outside of business hours on all operating systems, local or remote between the hours of 8:00AM and 6:00PM local time. You may change the time zone and business hours used in this report by specifying. See [“Changing the Time Zone and Business hours”, on page 193](#).

COLUMNS

Column	Description
Event Source	Event-log source that recorded the event
Information System	Machine logged into
Account	User account used for login
Result	Result of login attempt. Possible values: <ul style="list-style-type: none">• Failure• Success• Unknown
Count	Number of logins outside business hours

EXAMPLE**INTELLISchema View**

- “User Login Details”, on page 190

TABLES REFERENCED

- None

CHANGING THE TIME ZONE AND BUSINESS HOURS

To change the time zone and business hours, you modify the SQL code that generates this report to change the time zone, day end time, and day start time. The following SQL statements may need modification:

```
WITH $TZ AS 'PST8PDT'
WITH $DAY_END    as _int64(1800)
WITH $DAY_START as _int64(0800)
```

To modify the SQL code:

- 1 Change the time zone. This report defaults to use the US/Pacific time zone. Replace the characters "PST8PDT" with the appropriate time zone code for your location. To find the correct code, see [Appendix B: Time Zones](#) in the *Event Data Warehouse Guide*.
- 2 Change the time the day ends. Replace the time the day ends within the parentheses of the line containing "\$DAY_END"
- 3 Change the time the day starts. Replace the time the day starts within the parentheses of the line containing "\$DAY_START".

GENERAL COMPLIANCE REPORTS

The General Compliance group of reports displays system startups, shutdowns, and security object access events and includes the following reports:

- “System Startup and Shutdown”, on page 196
- “Security Objects Accessed”, on page 198
- “Security Objects Deleted”, on page 199

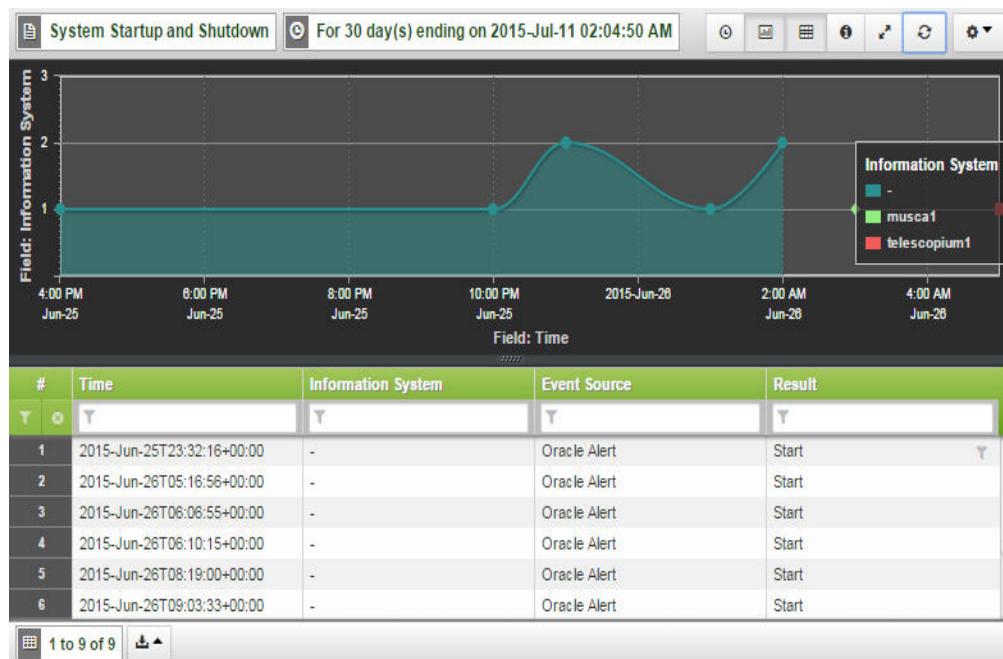
System Startup and Shutdown

Details the time of system startups and shutdowns for all information systems.

COLUMNS

Columns	Description
Time	Time the startup or shutdown occurred (yyyy-mm-dd hh:mm:ss)
Information System	Machine or device that was started or shutdown
Event Source	Event-log source that recorded the event
Result	Result of action. Possible values: <ul style="list-style-type: none"> • Shutdown • Start Up • Unknown

EXAMPLE



INTELLISchema View

- “System Startup and Shutdown”, on page 136

Security Objects Accessed

Details security objects that were accessed.

COLUMNS

Column	Description
Time	Time the login occurred (yyyy-mm-dd hh:mm:ss)
Information System	Machine logged into
User	Event-log source that recorded the event
Object	User account logged into
Domain	Domain name
Object Type	Type of object accessed
Access	Type of Access
Logon	Logon address
Action	Action of the object

EXAMPLE

#	Time	Infor...	User	Object	Domain	Objec...	Acces...	Logo...	Action
1	2008-Aug-15 07:32:47 AM	corps...	admin...	C:\lhr...	PS	File	Network		Object ...
2	2008-Aug-15 05:48:20 AM	corps...	admin...	\REG...	PS	Key	Network		Object ...
3	2008-Aug-15 05:37:46 AM	corps...	sales_...	C:\RE...	PS	File	Network		Object ...
4	2008-Aug-15 05:37:40 AM	corps...	sales_...	C:\sal...	PS	File	Network		Object ...

1 to 19 of 19

NELLISchema View

- “Security Objects”, on page 134.

TABLES REFERENCED

- None

Security Objects Deleted

Details security objects that were deleted.

COLUMNS

Column	Description
Time	Time the login occurred (yyyy-mm-dd hh:mm:ss)
Information System	Machine logged into
User	Event-log source that recorded the event
Object	User account logged into
Domain	Domain name
Object Type	Type of object deleted
Access	Type of Access
Logon	Logon address
Action	Action of the object

EXAMPLE

#	Time	Infor...	User	Object	Domain	Objec...	Acces...	Logo...	Action
1	2008-Aug-15 07:32:47 AM	corps...	admin...	C:\WHR...	PS	File	Network		Object ...
2	2008-Aug-15 05:48:20 AM	corps...	admin...	\REG...	PS	Key	Network		Object ...
3	2008-Aug-15 05:37:46 AM	corps...	sales_...	C:\RE...	PS	File	Network		Object ...
4	2008-Aug-15 05:37:40 AM	corps...	sales_...	C:\sal...	PS	File	Network		Object ...

1 to 19 of 19

NELLIS SCHEMA VIEW

- “Security Objects”, on page 134

TABLES REFERENCED

- None

NETWORK DEVICE MONITORING REPORTS

The Network Device Monitoring group of reports displays router authentication and connection events and includes the following reports:

- “[Router Denied Connections Details](#)”, on page 201
- “[Router Authentication Failure Details](#)”, on page 202

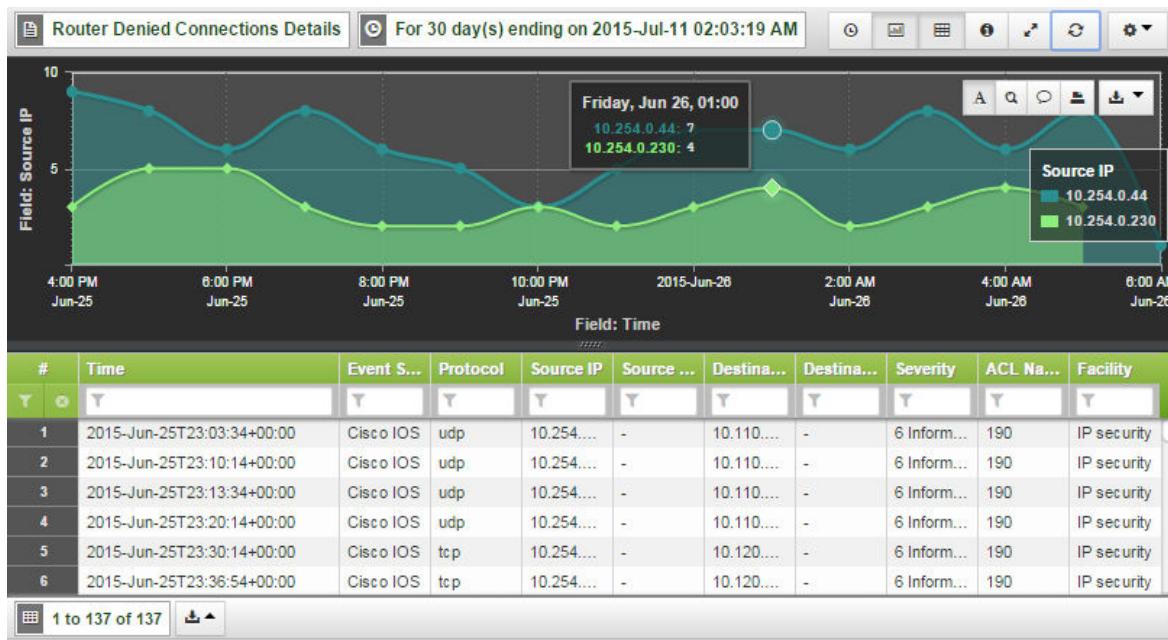
Router Denied Connections Details

Details of all denied connections to routers and switches.

COLUMNS

Column	Description
Time	Time the router connection was denied (yyyy-mm-dd hh:mm:ss)
Event Source	Event-log source that recorded the event
Protocol	Protocol used for the denied connection
Source IP	Source IP of the denied connection
Source Port	Source port of the denied connection (Displays "-" if no port number was recorded)
Destination IP	Destination IP of the denied connection
Destination Port	Destination port of the denied connection (Displays "-" if no port number was recorded)
Severity	Router severity level
ACL Name	ACL used to deny the connection
Facility	Router Facility Name

EXAMPLE



INTELLISchema View

- “Network Device Connection: Router”, on page 122

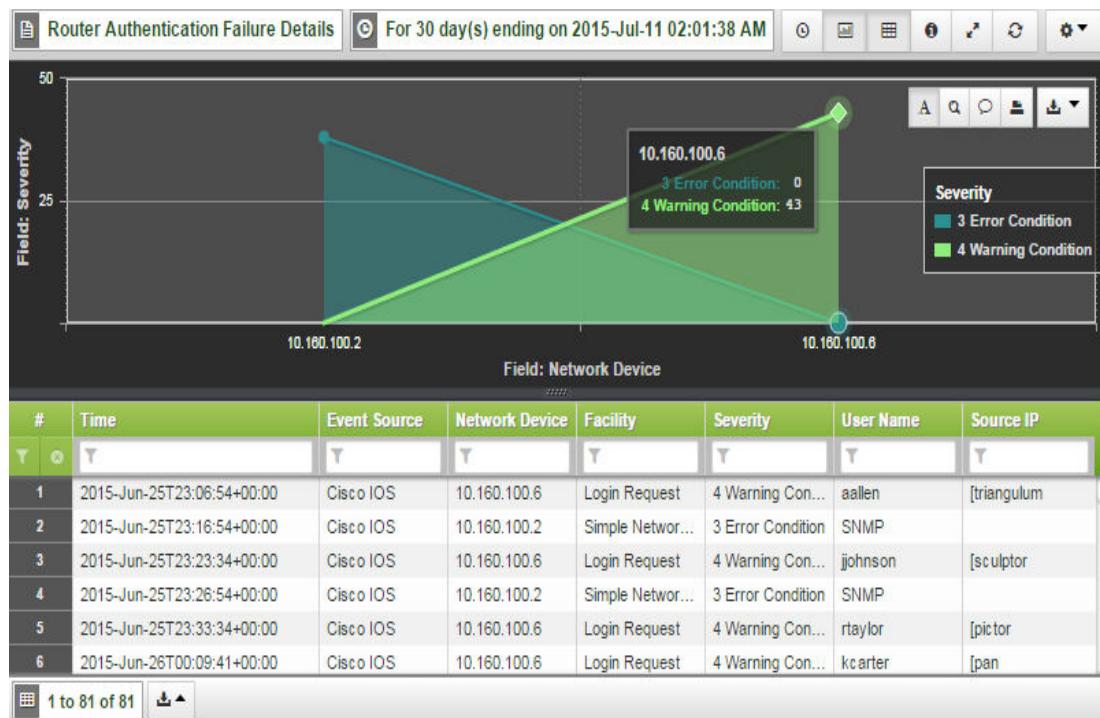
Router Authentication Failure Details

Number of authentication failures for all routers and switches.

COLUMNS

Column	Description
Time	Time authentication failure occurred (yyyy-mm-dd hh:mm:ss)
Event Source	Event-log source that recorded the event
Network Device	Name of the router where authentication failed
Facility	Router facility name
Severity	Router severity level
User Name	Total number of authentication failures
Source IP	Source IP of the authentication failure

EXAMPLE



INTELLISchema View

- “Network Device Connection: Router”, on page 122

FIREWALL MONITORING REPORTS

The Firewall Monitoring group of reports displays firewall authentication and connection events and includes the following reports:

- “Firewall Denied Connections Details”, on page 204
- “Firewall Denied Connections Summary”, on page 205
- “Firewall Accepted Connections Details”, on page 206
- “Firewall Accepted Connections Summary”, on page 207
- “Firewall All Connections Details - new”, on page 208

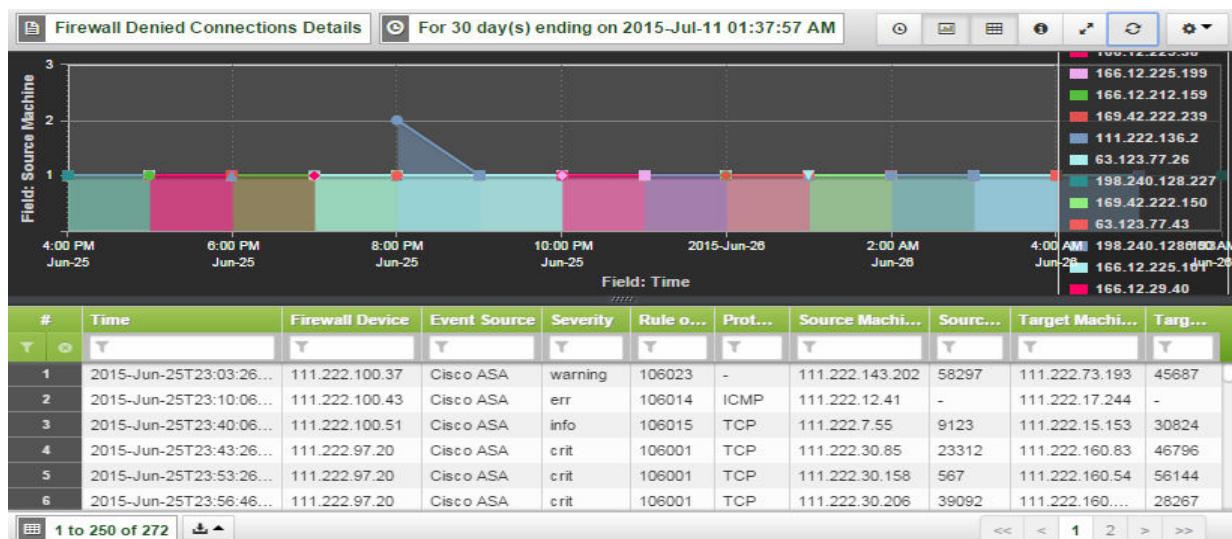
Firewall Denied Connections Details

Details of denied firewall connections.

COLUMNS

Column	Description
Time	Time the firewall denied the connection (yyyy-mm-dd hh:mm:ss)
Firewall Device	Name of the firewall
Event Source	Event-log source that recorded the event
Severity	Firewall severity level
Rule or Access Group	Rule or group used to deny the connection
Protocol	Protocol used for the denied connection
Source Machine	Source IP of the denied connection request
Source Port	Source port of the denied connection request
Target Machine	Name of machine where connection was attempted
Target Port	Port number of machine where connection was attempted

EXAMPLE



INTELLISchema View

- “Network Device Connection: Firewall”, on page 123

Firewall Denied Connections Summary

Number of denied connections on each firewall by protocol.

COLUMNS

Column	Description
Firewall Device	Subsystem or application that requested a connection
Event Source	Event-log source that recorded the event
Total Failures	Total number of denied connections
Protocol	Protocol used for the denied connection
Number of Sources	Number of unique Source IP addresses denied connections

EXAMPLE



INTELLISchema View

- “Network Device Connection: Firewall”, on page 123

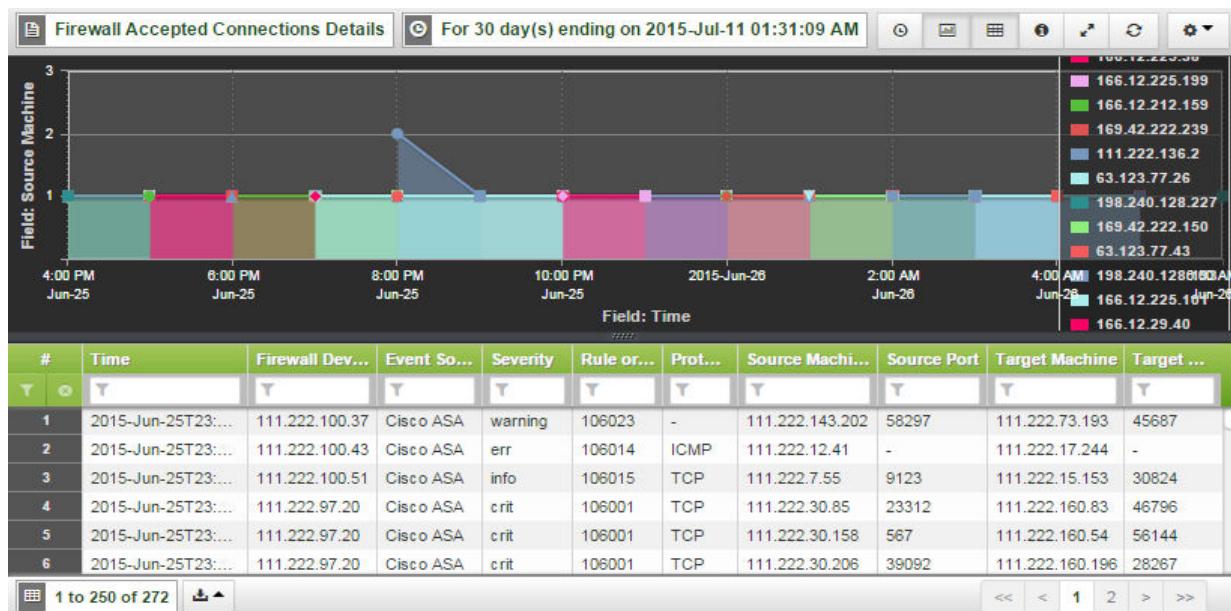
Firewall Accepted Connections Details

Details of accepted connections on each firewall by access list or rule.

COLUMNS

Column	Description
Time	Time the connection was accepted (yyyy-mm-dd hh:mm:ss)
Firewall Device	Name of the router that denied the connection
Event Source	Event-log source that recorded the event
Severity	Firewall severity level
Rule or Access Group	Rule or group used to accept the connection
Protocol	Protocol used for the accepted connection
Source Machine	Source IP of the accepted connection request
Source Port	Source port of the accepted connection request
Target Machine	Name of machine that accepted the connection
Target Port	Port number of machine that accepted the connection

EXAMPLE



INTELLISchema View

- “Network Device Connection: Firewall”, on page 123

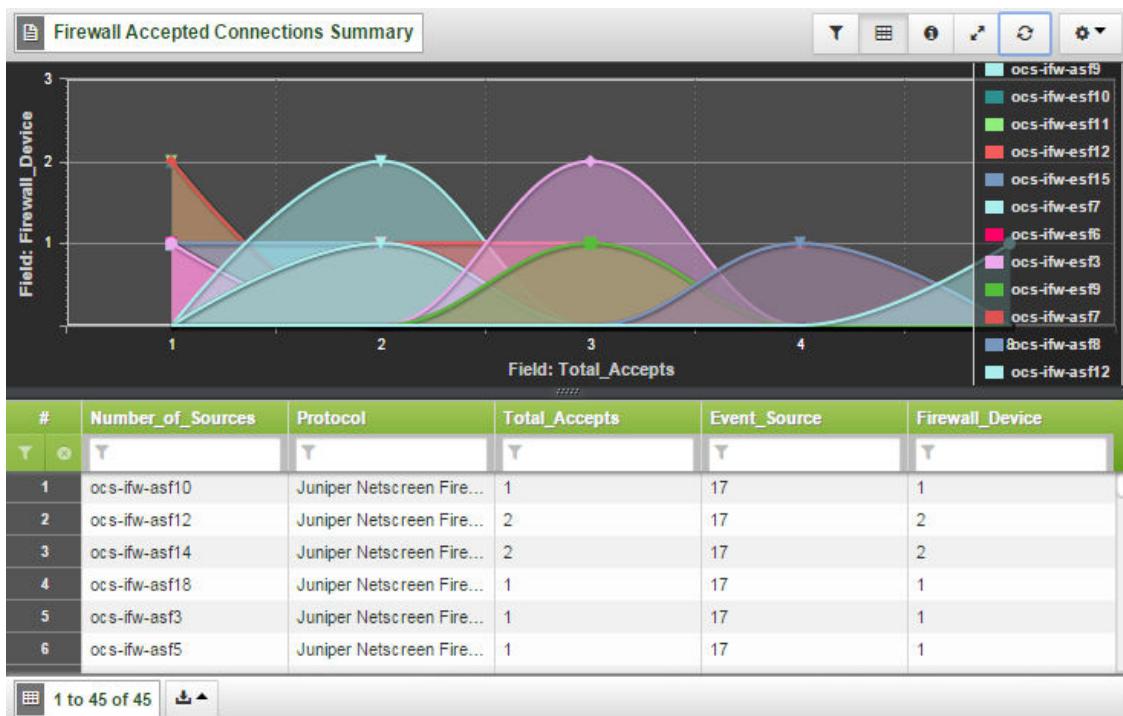
Firewall Accepted Connections Summary

Number of accepted connections and sources on each firewall by protocol and event source.

COLUMNS

Column	Description
Firewall Device	Subsystem or application that requested a connection
Event Source	Event-log source that recorded the event
Total Accepts	Total number of accepted connections
Protocol	Protocol used for the accepted connection
Number of Sources	Number of unique source IP addresses where the connection was accepted

EXAMPLE



INTELLISchema View

- “Network Device Connection: Firewall”, on page 123

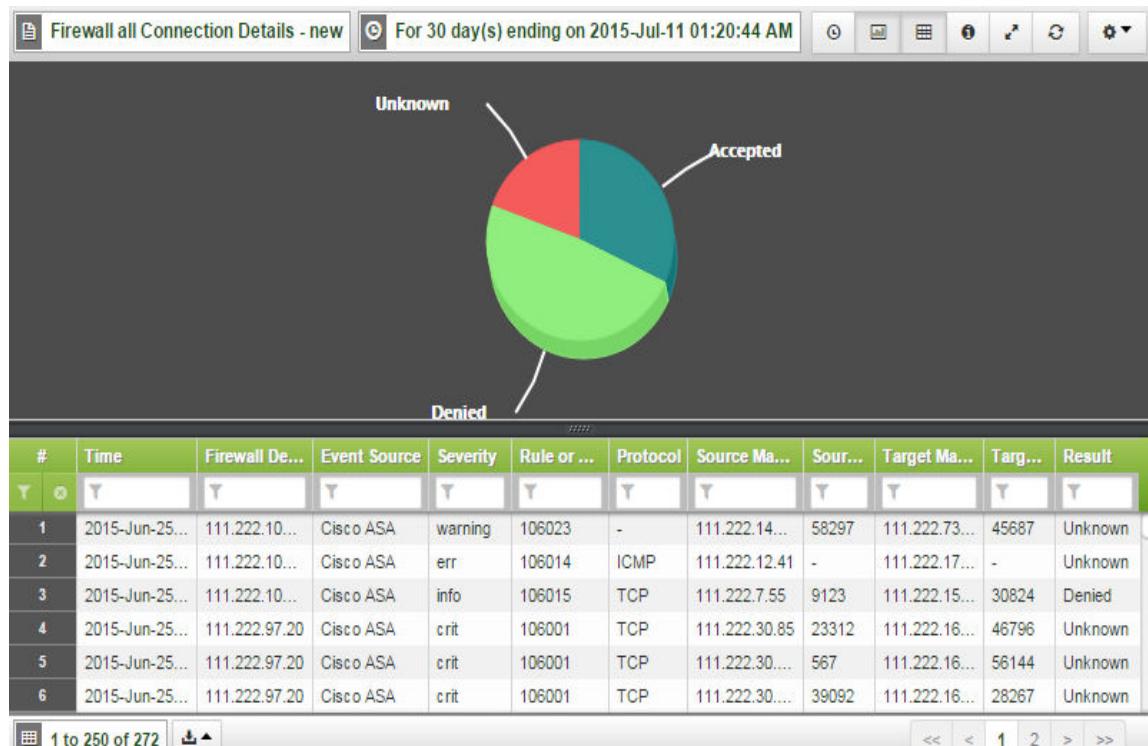
Firewall All Connections Details - new

Details of accepted and denied connections on each firewall by access list or rule.

COLUMNS

Column	Description
Time	Time the connection was accepted (yyyy-mm-dd hh:mm:ss)
Firewall Device	Subsystem or application that requested a connection
Event Source	Event-log source that recorded the event
Severity	Firewall severity level
Rule or Group	Rule or group used to accept the connection
Total Accepts	Total number of accepted connections
Protocol	Protocol used for the accepted connection
Source Machine	Unique source IP addresses where the connection was accepted
Source Port	Source port number
Target Machine	Unique target IP addresses where the connection was accepted
Target	Target port number
Result	Firewall connection result

EXAMPLE



INTELLISchema View

- “Network Device Connection: Firewall”, on page 123

CHAPTER 8

Foundation Analytics Reports (Windows)

The SenSage AP Foundation Analytics reports are designed to enable monitoring of the operational security and effectiveness of your business. The report also includes reports for monitoring the status of your SenSage AP deployment. This chapter provides a reference for the Foundation Analytic reports, which include the associated IntelliSchema views and the columns available for reporting.

MICROSOFT WINDOWS REPORTS

The Microsoft Windows reports display events from Microsoft Windows systems and contains the following reports:

Login Activity reports display information on user login events for Windows systems.

- “Windows Login Activity Details”, on page 213
- “Windows Login Failure Summary”, on page 214
- “Windows Login Success Summary”, on page 215
- “Windows Login Failure Details”, on page 216
- “Windows Remote Login Details”, on page 217

Domain Activity reports display information on login events and modifications to domain objects for Windows systems that are members of a Windows Domain.

- “Windows Account Addition and Deletion”, on page 218
- “Windows Account Modifications”, on page 219
- “Windows Group Member Addition and Deletion”, on page 220
- “Windows Group Modification Summary”, on page 221
- “Windows Password Changes and Resets”, on page 222
- “Windows User Account Locked and Unlocked by Date”, on page 223
- “Windows User Activity Journal”, on page 224

Account Modification Activity reports display changes to user account privileges:

- “Windows Account Rights Modified”, on page 225
- “Windows User Special Privileges Details”, on page 226
- “Windows Privileged Account Access Details”, on page 227

System Activity reports display miscellaneous system events.

- “Windows System Startup Summary”, on page 228
- “Windows New Process Started”, on page 229

- “Windows New Process Started Summary”, on page 230
- “Windows Audit Log Cleared Summary”, on page 231
- “Windows System Events”, on page 234
- “Windows System Event Summary per Day”, on page 235
- “Windows Application Events”, on page 232
- “Windows Application Events Summary per Day”, on page 233
- “Windows File Replication Service Events”, on page 236
- “Windows File Replication Service Events Summary per Day”, on page 237
- “Windows Error Events”, on page 238
- “Windows DNS Server Events”, on page 239
- “Windows DNS Server Events Summary per Day”, on page 240
- “Windows Directory Service Events Summary per Day”, on page 242
- “Windows Major Security Events”, on page 243
- “Windows Loss of Audit Messages”, on page 244

Active Directory (AD) reports display information on AD events for Windows systems.

- “Windows Active Directory Object Changes”, on page 245
- “Windows Active Directory Policy Changes”, on page 246
- “Windows Active Directory Users - Deleted or Disabled”, on page 247
- “Windows Active Directory Users - Lockouts and Password Resets”, on page 248
- “Windows Active Directory Users - New or Enabled”, on page 249

Auditable Event Activity reports display activity enabled for auditing.

- “Windows Security Objects Accessed”, on page 250
- “Windows Security Objects Deleted”, on page 251
- “Windows Security Objects Access Optimized”, on page 252

Windows Login Activity Details

Details of login activities recorded by Microsoft Windows systems.

COLUMNS

Columns	Description
Time	Time the login occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Event Source	Event-log source that recorded the event
Information System	Name of the machine or device the user logged into
Result	Outcome of the event. Possible values: <ul style="list-style-type: none"> • Failure • Success • Unknown
Event ID	Windows Event ID
Account	User account used for login

EXAMPLE

#	Time	Event S...	Inform...	Result	Event ID	Account	Event ...	Logon ...
1	2009-Apr-15 06:04:49 AM	Window...	win-012...	Failure	4625	testadm...	Logon f...	Network
2	2009-Apr-15 06:04:49 AM	Window...	win-012...	Failure	4625	testadm...	Logon f...	Network
3	2009-Apr-15 06:04:49 AM	Window...	win-012...	Failure	4625	testadm...	Logon f...	Network
4	2009-Apr-15 06:04:49 AM	Window...	win-012...	Failure	4625	testadm...	Logon f...	Network
5	2009-Apr-15 07:15:05 AM	Window...	win-012...	Success	4624	win-0t4...	Succes...	Network
6	2009-Apr-15 06:04:49 AM	Window...	win-012...	Failure	4625	testadm...	Logon f...	Network

INTELLISchema View

- “User Logins: Windows”, on page 144

TABLES REFERENCED

- None

Windows Login Failure Summary

A summary of the number of failed login attempts recorded by Microsoft Windows systems.

COLUMNS

Columns	Description
Information System	Name of the machine or device where the logins occurred
Event ID	Windows Event ID
Event Description	Description of the login event
Total Failures	Number of failure logins for each information system

EXAMPLE

#	Information System	Event ID	Event Description	Total Failures
1	c3devweb3	537	Logon failure - the logon attempt was rejected by the security system.	1
2	dssdevis7nt1	529	Logon failure - unknown user name or password.	1
3	hiqaprof1	531	Logon failure - account currently disabled.	1
4	qacluster03vm04	536	Logon failure - the netlogon component failed to respond.	8
5	testad23	535	Logon failure - the specified account does not exist.	1
6	c3devmeta2	529	Logon failure - unknown user name or password.	5
7	c3devweb3	529	Logon failure - unknown user name or password.	9
8	c3devweb3	531	Logon failure - account currently disabled.	5

INTELLISchema View

- “User Logins: Windows”, on page 144

TABLES REFERENCED

- None

Windows Login Success Summary

A summary of the number of successful logins recorded by Microsoft Windows systems.

COLUMNS

Columns	Description
Information System	Name of the machine or device where the logins occurred
Event ID	Windows Event ID
Event Description	Description of login event
Total Successes	Number of successful logins for each Information System

EXAMPLE



The screenshot shows a software interface titled "Windows Login Success Summary". At the top, it says "For 20 year(s) ending on 2015-Jan-18 06:35:52 PM". The main area is a grid with columns: #, Information System, Event ID, Event description, and Total Successes. The data shows various users (aphrodite, ara, aries, cancer, carina) with their respective logon types (Successful logon, Successful network logon) and success counts. At the bottom, it says "1 to 169 of 169".

#	Information System	Event ID	Event description	Total Successes
1	aphrodite	528	Successful logon	78
2	aphrodite	540	Successful network logon	234
3	ara	528	Successful logon	156
4	ara	540	Successful network logon	78
5	aries	528	Successful logon	546
6	cancer	528	Successful logon	156
7	cancer	540	Successful network logon	156
8	carina	528	Successful logon	156

INTELLISchema View

- "User Logins: Windows", on page 144

TABLES REFERENCED

- None

Windows Login Failure Details

Details of failed logins and locked out accounts from Microsoft Windows domain controllers.

COLUMNS

Columns	Description
Time	Time the failed login occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Domain Caller	Caller's domain
Event Source	Event-log source that recorded the login attempt
Information System	Name of the information system that generated the failed login
User	User account for which the login failed
Event ID	Windows Event ID
Event Description	Description of the login event

EXAMPLE

The screenshot shows a report titled "Windows Login Failure Details" with a search filter "For 15 year(s) ending on 2016-Mar-01 09:36:07 PM". The report displays 146 rows of data across seven columns: #, Time, Information Sy..., Event Source, User, Event ID, and Event Description. The data includes various login attempts, mostly from "Windows Snare" and "Windows Retriever" sources, involving users like "win-u2j6mawrllq\$". The "Event Description" column shows entries such as "A Kerberos Auth..." and "Pre-authentication...". The bottom of the interface shows navigation controls for "1 to 146 of 146" and sorting icons.

#	Time	Information Sy...	Event Source	User	Event ID	Event Description
1	2013-Jul-19T19:49:47+00:00	win-u2j6mawrllq....	Windows Snare	win-u2j6mawrllq\$	4768	A Kerberos Auth...
2	2013-Jul-19T19:49:47+00:00	win-u2j6mawrllq....	Windows Snare	win-u2j6mawrllq\$	4768	A Kerberos Auth...
3	2013-Jul-19T19:49:47+00:00	win-u2j6mawrllq....	Windows Snare	win-u2j6mawrllq\$	4768	A Kerberos Auth...
4	2013-Jul-19T19:49:47+00:00	win-u2j6mawrllq....	Windows Snare	win-u2j6mawrllq\$	4768	A Kerberos Auth...
5	2007-Mar-01T00:43:53+00:00	testad23	Windows Retriever	newbie	675	Pre-authentication...
6	2007-Mar-01T00:43:54+00:00	testad23	Windows Retriever	newbie	675	Pre-authentication...
7	2007-Mar-01T00:43:55+00:00	testad23	Windows Retriever	newbie	675	Pre-authentication...
8	2007-Mar-01T00:43:56+00:00	testad23	Windows Retriever	newbie	675	Pre-authentication...

INTELLISchema View

- “User Logins: Windows”, on page 144

TABLES REFERENCED

- None

Windows Remote Login Details

Details of remote login activities recorded by Microsoft Windows systems that are not domain controllers.

COLUMNS

Columns	Description
Time	Time the login occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Information System	Name of the machine or device the user logged into
Remote Host	Name of the remote host
Remote IP	IP address of the remote host
Called By	Called by
Event ID	Windows Event ID
Status	Description of Event
ts	Timestamp (<i>yyyy-mm-dd hh:mm:ss</i>)

EXAMPLE

The screenshot shows a software interface for viewing log data. The title bar reads "Windows Remote Login Details". A filter bar indicates the data is from "From 2007-Sep-26 12:00:00 AM to 2007-Sep-26 11:59:59 PM". The main area is a grid with the following columns: #, Time, Information..., Remote Host, Remote IP, Called By, Event ID, Status, and ts. The grid contains 2,454 rows of data. The first few rows show logins from various hosts like FINANCE_AD, MEDICAL_AD, and HERMES, all occurring at Event ID 528 and status "Successful logon". The timestamp column shows dates ranging from Sep 26, 2007, to Sep 27, 2007.

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

Windows Account Addition and Deletion

Details of all activity related to the addition and deletion of user or service accounts on Microsoft Windows systems that are members of a Windows Domain.

COLUMNS

Column	Description
Time	Time the account addition or deletion occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Event Source	Event-log source that recorded the event
Domain Controller	Name of Windows domain controller
Domain	Name of Windows domain
Done By	User account used to make the addition or deletion
User Added/Deleted	User account that was added or deleted
Event ID	Windows Event ID
Event Description	Description of event. Possible values: • User Account Created • User Account Deleted
Role	Event source role

EXAMPLE

#	Time	Event...	Doma...	Domain	Done by	User ...	Event ID	Event...	Role
1	2005-Jun-17 07:34:16 PM	Windo...	c3dev...				624		Domai...
2	2005-Jun-17 07:31:46 PM	Windo...	c3dev...				630		Domai...
3	2005-Jun-17 07:27:36 PM	Windo...	c3dev...				624		Domai...
4	2008-Aug-15 05:41:27 AM	Windo...	corps...	PS	admin...	user_3	624	User ...	Domai...
5	2008-Aug-15 05:39:36 AM	Windo...	corps...	PS	sys_p...	user_2	624	User ...	Domai...
6	2008-Aug-15 05:39:04 AM	Windo...	corps...	PS	sys_p...	user_1	624	User ...	Domai...

INTELLISchema VIEW

- “Account Addition and Deletion: Windows”, on page 97

TABLES REFERENCED

- None

Windows Account Modifications

Details of Windows account modification events.

COLUMNS

Column	Description
Time	Time the modification occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Domain Controller	Name of Windows domain controller
Domain	Name of the Windows domain
Done By	User account used to modify the account
Target Account Name	Modified account
Event ID	Windows Event ID
Description	Windows Event ID description
Role	Role of domain ("Member Server" or "Domain Controller")

EXAMPLE

Windows Account Modifications								
#	Time	Domain ...	Domain	Done by	Target Ac...	Event ID	Description	Role
1	2009-May...	win-01234...	chamarts		-	4738	A user ac...	Domain Co...
2	2009-Apr-...	win-01234...	chamarts		-	4738	A user ac...	Domain Co...
3	2009-May...	win-01234...	chamarts		-	4738	A user ac...	Domain Co...
4	2009-Apr-...	win-01234...	chamarts		-	4738	A user ac...	Domain Co...
5	2009-May...	win-01234...	chamarts		-	4738	A user ac...	Domain Co...
6	2009-Apr-...	win-01234...	chamarts		-	4738	A user ac...	Domain Co...
7	2005-Jun-...	c3devweb3				642	A user ac...	Domain Co...

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

Windows Group Member Addition and Deletion

Details of all actions on a Windows domain controller involving the addition or deletion of an account on a local or global group.

COLUMNS

Column	Description
Time	Time the group addition or deletion occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Domain Controller	Name of Windows domain controller
Domain	Name of the Windows domain
Group	Name of the group added or deleted
Done By	User account used to add or delete the group
User Added/Removed	User added to or removed from the group
Event ID	Windows Event ID
Event Description	Description of Windows Event
Role	Event source role

EXAMPLE

#	Time	Domain...	Domain	Group	Done By	User Ad...	Event ID	Event D...	Role
1	2009-Ma...	WIN-012...		TestGlo...		CN=Tes...	4752	Member ...	DomainC...
2	2009-Ma...	WIN-012...		TestLoc...		CN=Tes...	4747	Member ...	DomainC...
3	2009-Ma...	WIN-012...		TestLoc...		CN=Srini...	4746	Member ...	DomainC...
4	2009-Ma...	WIN-012...		TestUni...		CN=Tes...	4762	Member ...	DomainC...
5	2009-Ma...	WIN-012...		TestGlo...		CN=Srini...	4751	Member ...	DomainC...
6	2009-Ma...	WIN-012...		TestUni...		CN=Srini...	4761	A memb...	DomainC...

...hexiscyber.com:8090/.../analyzer/

INTELLISchema VIEW

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

Windows Group Modification Summary

A summary of group modification activity. Includes the attributes and parameters changed, if available. Fields that show a “-” as a value indicate that the value has not changed, otherwise, the field contains the modified data.

COLUMNS

Column	Description
Time	Time the group modification occurred (yyyy-mm-dd hh:mm:ss)
Domain Controller	Name of the machine or device where the group modification occurred
Domain	Domain where the group modification occurred
Called By	User account used to modify the group
Target Account	Group whose passwords were modified
Event ID	Windows Event ID
Status	Outcome of modification event
Role	Event source role

EXAMPLE

#	Time	Informat...	Domain	Called By	Target Gr...	Event ID	Status	Role
1	09-May-0...	WIN-0123...			TestLocal...	4745	Local distr...	DomainCon...
2	09-May-0...	WIN-0123...			TestGloba...	4750	Global dist...	DomainCon...
3	09-May-0...	WIN-0123...			TestUnivDist	4760	A security...	DomainCon...
4	09-May-0...	WIN-0123...			TestUnivDist	4759	A security...	DomainCon...
5	09-May-0...	WIN-0123...			TestGloba...	4749	Global dist...	DomainCon...
6	09-May-0...	WIN-0123...			TestLocal...	4744	Local distr...	DomainCon...

1 to 97 of 97

INTELLISchema VIEW

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

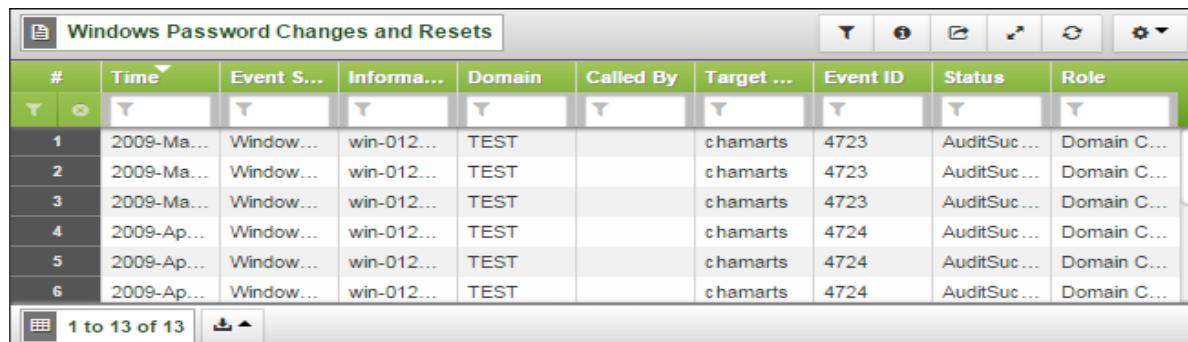
Windows Password Changes and Resets

Details of all password changes that occur on Microsoft Windows systems. Identifies when a user changes their own account, other accounts, and when a password is reset.

COLUMNS

Column	Description
Time	Time the password change occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Event Source	Event-log source that recorded the event
Information System	Name of the machine or device that generated the event
Domain	Name of the Windows domain
Called By	User account used to reset passwords
Target User	User account whose passwords were changed
Event ID	Windows Event ID
Status	Outcome of password change
Role	Event source role

EXAMPLE



The screenshot shows a report titled "Windows Password Changes and Resets". The grid has the following columns: #, Time, Event S..., Informa..., Domain, Called By, Target ..., Event ID, Status, and Role. There are 6 rows of data, each showing a timestamp, event source, information system, domain, called by, target user, event ID, status, and role. The status column shows "AuditSuc..." for most rows, except for the last one which shows "AuditFail...". The role column shows "Domain C..." for all rows. At the bottom left, there is a navigation bar with "1 to 13 of 13" and a search icon.

#	Time	Event S...	Informa...	Domain	Called By	Target ...	Event ID	Status	Role
1	2009-Ma...	Window...	win-012...	TEST		chamarts	4723	AuditSuc...	Domain C...
2	2009-Ma...	Window...	win-012...	TEST		chamarts	4723	AuditSuc...	Domain C...
3	2009-Ma...	Window...	win-012...	TEST		chamarts	4723	AuditSuc...	Domain C...
4	2009-Ap...	Window...	win-012...	TEST		chamarts	4724	AuditSuc...	Domain C...
5	2009-Ap...	Window...	win-012...	TEST		chamarts	4724	AuditSuc...	Domain C...
6	2009-Ap...	Window...	win-012...	TEST		chamarts	4724	AuditSuc...	Domain C...

INTELLISchema VIEW

- “Password Changes and Resets: Windows”, on page 128

TABLES REFERENCED

- None

Windows User Account Locked and Unlocked by Date

Details each user account that is locked or unlocked by date.

COLUMNS

Column	Description
Time	Time the user account was locked or unlocked (<i>yyyy-mm-dd hh:mm:ss</i>)
Account	Windows user account that was locked or unlocked
Account ID	Windows user account ID that was locked or unlocked
Action	Action taken on the account. Possible values: • Locked • Unlocked
Caller Machine	Machine used to lock or unlock the account
Caller User	User account used to lock or unlock the account
Caller Domain	Domain where the user's account was locked or unlocked
Caller Logo	Logo of the user that locked or unlocked the account
Role	Event source role

EXAMPLE

#	Time	Account	Account ID	Action	Caller Mach...	Caller User ...	Caller Dom...	Caller Logo...	Role
1	2007-Mar-01...	test_user	%{S-1-5-21-...}	Locked	TESTAD23	TESTAD23\$	SENSAGE2	(0x0,0x3E7)	Domain Contr...
2	2007-Mar-01...	test_user	%{S-1-5-21-...}	Unlocked		Administrator	SENSAGE2	(0x0,0x4088...)	Domain Contr...
3	2007-Mar-01...	test_user	%{S-1-5-21-...}	Unlocked		Administrator	SENSAGE2	(0x0,0x4088...)	Domain Contr...
4	2009-Apr-29...	chamarts	S-1-5-21-63...	Locked	WIN-0T4GGI...	WIN-0T4GGI...	TEST	0x3e7	Domain Contr...

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- micorsoft_windows2008_securityEvent_snare

Windows User Activity Journal

Details of user activity.

COLUMNS

Column	Description
Time	Time of user activity (<i>yyyy-mm-dd hh:mm:ss</i>)
Information System	System on which the activity occurred
Domain	Name of Windows domain
User Name	User's name
Logon ID	User's logon ID
Event ID	Windows Event ID
Event Description	Windows Event ID description
unparsed_message	Source raw message

EXAMPLE

The screenshot shows a software window titled "Windows User Activity Journal". The interface includes a toolbar with various icons at the top, followed by a grid of data rows. Each row contains nine columns: #, Time, Information System, Domain, User Name, Logon ID, Event ID, Event Desc..., and unparsed_m... . The data grid shows 10 entries, with the first few entries being identical logon failure events from December 14, 2009, and the last entry being a user logoff event from August 14, 2008. At the bottom of the grid, there is a navigation bar with buttons for page numbers (1 to 10) and arrows, along with a status message indicating "1 to 250 of 130,208".

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- micorsoft_windows2008_securityEvent_snare

Windows Account Rights Modified

A detailed view of privileged account escalations and de-escalations on Microsoft Windows systems.

COLUMNS

Column	Description
Time	Time the rights modification occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
User	User account whose rights were modified
Done By	User account used to generate the account modification
Domain	Windows domain
Right Name	Account right that was modified
Event ID	Windows Event ID
Action	Action taken on the account rights. Possible values: • Added • Removed
Description	Description of modified right
Role	Event source role

EXAMPLE

#	Time	User	Done By	Domain	Right N...	Event ID	Action	Descrip...	Role
1	2009-Ma...	S-1-1-0			SeCreat...	4704	Added	Create ...	Domain C...
2	2009-Ma...	S-1-5-21...			SeCreat...	4705	Removed	Create ...	Domain C...
3	2009-Ma...	S-1-5-21...			SeCreat...	4704	Added	Create ...	Domain C...
4	2009-Ma...	S-1-1-0			SeCreat...	4704	Added	Create ...	Domain C...
5	2009-Ma...	S-1-5-21...			SeCreat...	4705	Removed	Create ...	Domain C...
6	2009-Ma...	S-1-5-21...			SeCreat...	4704	Added	Create ...	Domain C...

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

Windows User Special Privileges Details

Details of activities on Microsoft Windows systems using privileged accounts.

COLUMNS

Column	Description
Time	Time the event occurred (yyyy-mm-dd hh:mm:ss)
Domain	Windows domain name
Account	Windows user account
Computer	Name of the computer where the privileges are provided
Privileges	Type of privilege
Event Source	Event-log source that recorded the activity
Result	Outcome of granting the privilege
Log Type	Type of log

EXAMPLE

#	Time	Domain	Account	Computer	Privileges	Event Source	Result	Log Type
1	2009-May-01 01:06:58 PM	win-012...	win-0t4...	TEST	SeTcbP...	Act as p...	Success	Window...
2	2009-May-01 01:06:58 PM	win-012...	win-0t4...	TEST	SeTcbP...	Act as p...	Success	Window...
3	2009-May-01 01:06:58 PM	win-012...	win-0t4...	TEST	SeTcbP...	Act as p...	Success	Window...
4	2009-Apr-15 07:32:22 AM	win-012...	local se...	NT AUT...	SeSecu...	Manage...	Success	Window...
5	2009-Apr-15 07:32:22 AM	win-012...	local se...	NT AUT...	SeSecu...	Manage...	Success	Window...
6	2009-Apr-15 07:32:22 AM	win-012...	local se...	NT AUT...	SeSecu...	Manage...	Success	Window...
7	2008-Aug-15 07:32:06 AM	corpser...	admin_j...	PS	SeShut...	Shut do...	Success	Window...

INTELLISchema View

- “Privileged Commands: Windows”, on page 132

TABLES REFERENCED

- None

Windows Privileged Account Access Details

Details of privileged account access.

COLUMNS

Column	Description
Time	Time of access (yyyy-mm-dd hh:mm:ss)
Computer	Name of accessed machine
Event ID	Windows Event ID
Event Description	Windows Event ID description
Changes	Changes that were done
Performed By	User who initiated changes

EXAMPLE

#	Time	Computer	Event ID	Event Description	Changes	Performed By
1	2007-Mar-01 00:21:...	TESTAD23	643	Domain policy cha...	Domain: SENSAGE2	administrator\SEN...
2	2007-Mar-01 00:21:...	TESTAD23	643	Domain policy cha...	Domain: SENSAGE2	administrator\SEN...
3	2007-Mar-01 00:56:...	TESTAD23	643	Domain policy cha...	Domain: SENSAGE2	TESTAD23\$\SENS...
4	2007-Mar-01 01:06:...	TESTAD23	608	User right assigned	User Right: SeTcb...	TESTAD23\$\SENS...
5	2007-Mar-01 01:11:...	TESTAD23	609	User right removed	User Right: SeTcb...	TESTAD23\$\SENS...
6	2007-Mar-01 01:28:...	TESTAD23	517	The audit log was ...	Security log cleared	Administrator\SEN...
7	2008-Aug-14 19:49:...	CORPSERV01	517	The audit log was ...	Security log cleared	admin_jsmith\PS...
8	2009-May-01 16:14:...	WIN-012345ABCDE...	4704	User right assigned	Target Account: S...	TEST\TEST
9	2009-May-01 16:16:...	WIN-012345ABCDE...	4705	User right removed	Target Account: S...	TEST\TEST
10	2009-May-01 16:54:...	WIN-012345ABCDE...	4704	User right assigned	Target Account: S...	TEST\TEST

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

Windows System Startup Summary

Startup messages from Microsoft Windows systems.

COLUMNS

Columns	Description
Time	Time the startup occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Information System	Name of the machine or device that was started
Event Source	Event-log source that recorded the event

EXAMPLE

The screenshot shows a software application window titled "Windows System Startup Summary". The interface includes a toolbar with various icons, a header row with columns labeled "#", "Time", "Information System", and "Event Source", and a data row below it. The data row contains the value 1 in the # column, the timestamp 2007-Mar-01 11:32:54 AM in the Time column, the machine name testad23 in the Information System column, and Windows Retriever in the Event Source column. At the bottom left, there is a status bar indicating "1 to 1 of 1".

#	Time	Information System	Event Source
1	2007-Mar-01 11:32:54 AM	testad23	Windows Retriever

INTELLISchema VIEW

- “Startup and Shutdown: Windows”, on page 137

TABLES REFERENCED

- None

Windows New Process Started

Details of new processes started on Microsoft Windows systems.

COLUMNS

Column	Description
Time	Time the process was started (<i>yyyy-mm-dd hh:mm:ss</i>)
Domain Computer	Domain of the computer where the new process was started
Computer	Name of the computer where the new process was started
User Name	User account used to start the process
Process ID	Process ID of the started process
Process Name	Description of started process
Token Elevation	Indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

EXAMPLE

#	Time	Domain Co...	Computer ...	User Name	Process ID	Process Na...	Token Eleva...
1	2007-Feb-2...	TESTAD23	SENSAGE2	administrator	2104	C:\WINDOW...	-
2	2007-Feb-2...	TESTAD23	SENSAGE2	TESTAD23	4060	C:\WINDOW...	-
3	2007-Mar-0...	TESTAD23	SENSAGE2	TESTAD23	2272	C:\WINDOW...	-
4	2007-Mar-0...	TESTAD23	SENSAGE2	TESTAD23	3140	C:\WINDOW...	-
5	2007-Mar-0...	TESTAD23	SENSAGE2	TESTAD23	3976	C:\WINDOW...	-
6	2007-Mar-0...	TESTAD23	SENSAGE2	TESTAD23	984	C:\WINDOW...	-

1 to 241 of 241

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

Windows New Process Started Summary

Summary information about new process (total amount of new processes grouped by date, computer, and user).

COLUMNS

Column	Description
Date	Date process started (<i>yyyy-mm-dd</i>)
Computer Name	Name of machine where the new process started
User Name	User who started the new process
Processes	Number of started processes

EXAMPLE

#	Date	Computer Name	User Name	Processes
1	2007-Feb-28	TESTAD23	-	2
2	2007-Mar-01	TESTAD23	-	149
3	2008-Aug-14	CORPSERV01	-	87
4	2009-Apr-15	WIN-012345ABCDE.test.example...		1
5	2013-Jul-19	WIN-U2J6MAWRILQ.analyticsv...	Administrator	10
6	2013-Jul-19	WIN-U2J6MAWRILQ.analyticsv...	LOCAL SERVICE	7
7	2013-Jul-19	WIN-U2J6MAWRILQ.analyticsv...	WIN-U2J6MAWRILQ\$	124

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

Windows Audit Log Cleared Summary

Displays attempts by a user on a Microsoft Windows system to clear the event log.

COLUMNS

Column	Description
Time	Time the attempt to clear the event log occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Information System	Name of the machine or device where the event log was cleared
User	User account used to clear the log
Domain	Windows domain name

EXAMPLE

#	Time	Information System	User	Domain
1	2007-Mar-01 01:28:26 GMT	TESTAD23	Administrator	SENSAGE2
2	2008-Aug-14 19:49:25 GMT	CORPSERV01	admin_jsmith	PS

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

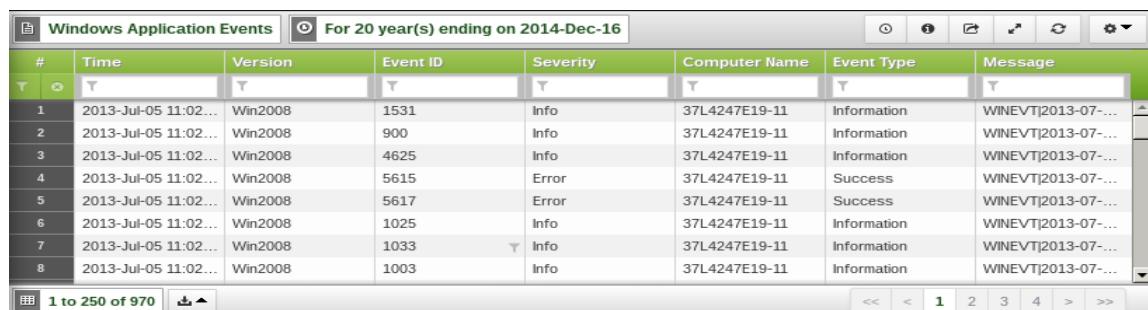
Windows Application Events

Lists each Windows application event per day, detailing the Windows version, Event ID, severity of the event, computer or device on which the event was triggered, event type, and message.

COLUMNS

Column	Description
Time	Time the event occurred (yyyy-mm-dd hh:mm:ss)
Version	Name of the Windows application version on which the event occurred
Event ID	Windows Event ID
Severity	Severity level of the event
Computer Name	Name of the machine or device where the Windows application event occurred
Event Type	Windows event type
Message	Actual message

EXAMPLE



The screenshot shows a report titled "Windows Application Events" with a filter "For 20 year(s) ending on 2014-Dec-16". The grid has columns: #, Time, Version, Event ID, Severity, Computer Name, Event Type, and Message. The data shows 970 rows of events from July 2013, mostly from Win2008, with various Event IDs, severities (Info, Error), and types (Information, Success). The "Message" column contains entries like "WINEVT|2013-07-...". Navigation controls at the bottom show page 1 of 250.

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows_appEvent_sensageRetriever
- microsoft_windows2008_appEvent_sensageRetriever

Windows Application Events Summary per Day

Summary of Windows application events per day by computer and Windows application version.

COLUMNS

Column	Description
date	Date of the event (<i>yyyy-mm-dd</i>)
version	Name of the Windows application version on which the event occurred.
computer_name	Name of the machine or device where the Windows application event occurred

EXAMPLE

#	date	version	computer_name
1	2007-02-28	Win2003	TESTAD23
2	2007-03-01	Win2003	TESTAD23
3	2013-07-05	Win2008	WIN-928F225SYY0
4	2013-07-05	Win2008	37L4247E19-11

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows_appEvent_sensageRetriever
- microsoft_windows2008_appEvent_sensageRetriever

Windows System Events

List of each Windows system event per day, detailing the Windows version, Event ID, severity of the event, computer or device on which the event was triggered, event type, and message.

COLUMNS

Column	Description
Time	Time the event occurred (yyyy-mm-dd hh:mm:ss)
Version	Name of the Windows system version on which the event occurred.
Event ID	Windows Event ID
Severity	Severity level of the event.
Computer Name	Name of the machine or device where the Windows system event occurred
Event Type	Windows event type
Message	Actual message.

EXAMPLE

The screenshot shows a report titled "Windows System Events" for the period "For 20 year(s) ending on 2014-Dec-16". The report displays a grid of 10,800 rows, with the first few rows visible. The columns are labeled: #, Time, Version, Event ID, Severity, Computer Name, Event Type, and Message. All events listed are for July 5, 2013, at 11:18, with Event ID 7036, Severity Info, Computer Name WIN-92BF225SYY0, and Event Type Information. The Message column shows the text "WINEVT|2013-07-...". The interface includes standard reporting tools like sorting, filtering, and navigation buttons at the bottom.

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows2008_sysEvent_sensageRetriever
- microsoft_windows_sysEvent_sensageRetriever

Windows System Event Summary per Day

Summary of Windows system events per day by computer and Windows system version.

COLUMNS

Column	Description
date	Date of the event (<i>yyyy-mm-dd</i>)
version	Name of the Windows system version on which the event occurred
computer_name	Name of the machine or device where the Windows system event occurred
computer_name (Count)	Number of system events

EXAMPLE

#	date	version	computer_name	computer_name(Count)
1	2007-03-09	Win2003	TESTAD23	281
2	2007-03-10	Win2003	TESTAD23	286
3	2007-03-11	Win2003	TESTAD23	3
4	2007-03-12	Win2003	TESTAD23	12
5	2007-03-13	Win2003	TESTAD23	299
6	2007-03-13	Win2003	XC2003ONWIN2003	119
7	2013-07-05	Win2008	WIN-928F225SYY0	9800

INTELLISchema VIEW

- None

TABLES REFERENCED

- microsoft_windows2008_sysEvent_sensageRetriever
- microsoft_windows_sysEvent_sensageRetriever

Windows File Replication Service Events

List of each Windows file replication service event per day, detailing the Windows version, Event ID, severity of the event, computer or device on which the event was triggered, event type, and message.

COLUMNS

Column	Description
Time	Time the file replication event occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Version	Name of the Windows system version on which the file replication service event occurred.
Event ID	Windows Event ID
Severity	Severity level of the event
Computer Name	Name of the machine or device where the Windows file replication service event occurred
Event Type	Windows event type
Message	Actual message

EXAMPLE

#	Time	Version	Event ID	Severity	Computer Name	Event Type	Message
1	2013-Jul-05 11:29...	Win2008	1531	Info	37L4247E19-11	Information	WINEVT 2013-07-...
2	2013-Jul-05 11:29...	Win2008	900	Info	37L4247E19-11	Information	WINEVT 2013-07-...
3	2013-Jul-05 11:29...	Win2008	4625	Info	37L4247E19-11	Information	WINEVT 2013-07-...
4	2013-Jul-05 11:29...	Win2008	5615	Error	37L4247E19-11	Success	WINEVT 2013-07-...
5	2013-Jul-05 11:29...	Win2008	5617	Error	37L4247E19-11	Success	WINEVT 2013-07-...
6	2013-Jul-05 11:29...	Win2008	1025	Info	37L4247E19-11	Information	WINEVT 2013-07-...
7	2013-Jul-05 11:29...	Win2008	1033	Info	37L4247E19-11	Information	WINEVT 2013-07-...
8	2013-Jul-05 11:29...	Win2008	1003	Info	37L4247E19-11	Information	WINEVT 2013-07-...

INTELLISchema VIEW

- None

TABLES REFERENCED

- microsoft_windows_frsEvent_sensageRetriever
- microsoft_windows2008_frsEvent_sensageRetriever

Windows File Replication Service Events Summary per Day

Summary of Windows file replication events per day by computer and Windows system version.

COLUMNS

Column	Description
Version	Date of the event (<i>yyyy-mm-dd</i>)
Date	Name of the Windows system version on which the event occurred
computer_name	Name of the machine or device where the Windows file replication event occurred
computer_name (Count)	Number of Windows file replication events

EXAMPLE

#	version	date	computer_name	computer_name(Count)
1	Win2003	2007-03-13	XC2003ONWIN2003	56
2	Win2003	2007-03-13	TESTAD23	16
3	Win2003	2007-03-09	TESTAD23	14
4	Win2003	2007-03-10	TESTAD23	14
5	Win2008	2013-07-05	WIN-928F225SYY0	946
6	Win2008	2013-07-05	37L4247E19-11	13

INTELLISchema VIEW

- None

TABLES REFERENCED

- microsoft_windows_frsEvent_sensageRetriever
- microsoft_windows2008_frsEvent_sensageRetriever

Windows Error Events

Lists each Windows error event per day, detailing the Windows version, Event ID, severity of the event, computer or device on which the event was triggered, event type, and message.

COLUMNS

Column	Description
Time	Time the file replication event occurred (yyyy-mm-dd hh:mm:ss)
Version	Name of the Windows version on which the error event occurred
Log type	Type of log for the error event
Event ID	Windows Event ID
Severity	Severity level of the event
Computer Name	Name of the machine or device where the Windows error event occurred
Event Type	Windows event type
Message	Actual message

EXAMPLE

The screenshot shows a report titled "Windows Error Events" with a filter "For 20 year(s) ending on 2014-Dec-16". The grid displays 37 rows of data, each representing an error event. The columns are: #, Time, Version, Log Type, Event ID, Severity, Computer Na..., Event Type, and Message. The data shows multiple entries for July 2013, mostly categorized as Application errors with Event IDs like 33, 1005, 1017, 11, and 4005, occurring on Win2008 machines.

#	Time	Version	Log Type	Event ID	Severity	Computer Na...	Event Type	Message
1	2013-Jul-05 11...	Win2008	Application	33	Error	WIN-928F225S...	Error	Microsoft.VC8...
2	2013-Jul-05 11...	Win2008	Application	33	Error	WIN-928F225S...	Error	Microsoft.VC8...
3	2013-Jul-05 11...	Win2008	Application	1005	Error	WIN-928F225S...	Error	OpenIPSecPer...
4	2013-Jul-05 11...	Win2008	Application	1017	Error	WIN-928F225S...	Error	PolicyAgent
5	2013-Jul-05 11...	Win2008	Application	11	Error	WIN-928F225S...	Error	http://www.do...
6	2013-Jul-05 11...	Win2008	Application	11	Error	WIN-928F225S...	Error	http://www.do...
7	2013-Jul-05 11...	Win2008	Application	4005	Error	WIN-928F225S...	Error	
8	2013-Jul-05 11...	Win2008	Application	4609	Error	WIN-928F225S...	Error	d:\longhorn\co...

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows_appEvent_sensageRetriever
- microsoft_windows_dirEvent_sensageRetriever
- microsoft_windows_dnsEvent_sensageRetriever
- microsoft_windows_frsEvent_sensageRetriever
- microsoft_windows_sysEvent_sensageRetriever
- microsoft_windows2008_appEvent_sensageRetriever
- microsoft_windows2008_dirEvent_sensageRetriever
- microsoft_windows2008_dnsEvent_sensageRetriever
- microsoft_windows2008_frsEvent_sensageRetriever
- microsoft_windows2008_sysEvent_sensageRetriever

Windows DNS Server Events

Lists each Windows DNS server event per day, detailing the Windows version, Event ID, severity of the event, computer or device on which the event was triggered, event type, and message.

COLUMNS

Column	Description
Time	Time the file replication event occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Version	Name of the Windows version on which the DNS server event occurred
Event ID	Windows Event ID
Severity	Severity level of the event
Computer Name	Name of the machine or device where the DNS server event occurred
Event Type	Type of event

EXAMPLE

The screenshot shows a report titled "Windows DNS Server Events" with a filter "For 20 year(s) ending on 2014-Dec-16". The grid displays 250 rows of data across columns: #, Time, Version, Event ID, Severity, Computer Name, Event Type, and Message. The first few rows show events from 2013-Jul-05 at 11:25, with Event IDs ranging from 1531 to 1003 and various severities (Info, Error). The "Message" column contains entries like "WINEVT|2013-07-...". Navigation controls at the bottom indicate 1 to 250 of 1,058 total rows, with page 1 selected.

INTELLISchema View

- None

TABLES REFERENCED

- `microsoft_windows_dnsEvent_sensageRetriever`
- `microsoft_windows2008_dnsEvent_sensageRetriever`

Windows DNS Server Events Summary per Day

Summary of DNS server events per day by computer and Windows system version.

COLUMNS

Column	Description
Date	Date of the event (<i>yyyy-mm-dd</i>)
Version	Name of the Windows system version on which the DNS server event occurred
Computer Name	Name of the machine or device where the DNS server event occurred
Count	Number of DNS server events

EXAMPLE

#	Date	Version	Computer Name	Count
1	2007-03-13	Win2003	TESTEDWIN2003	54
2	2007-03-13	Win2003	TESTAD23	45

INTELLISchema VIEW

- None

TABLES REFERENCED

- microsoft_windows_dnsEvent_sensageRetriever
- microsoft_windows2008_dnsEvent_sensageRetriever

Windows Directory Service Events

Lists each Windows Directory Service event per day, detailing the Windows version, Event ID, severity of the event, computer or device on which the event was triggered, event type, and message.

COLUMNS

Column	Description
Time	Time the Directory Service event occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Version	Name of the Windows version on which the Directory Service event occurred
Event ID	Windows Event ID
Severity	Severity level of the event
Computer Name	Name of the machine or device where the Windows Directory Service event occurred
Event Type	Type of event
Message	Actual message

EXAMPLE

#	Time	Version	Event ID	Severity	Computer Name	Event Type	Message
1	2013-Jul-05 11:22...	Win2008	1531	Info	37L4247E19-11	Information	WINEVT 2013-07-...
2	2013-Jul-05 11:22...	Win2008	900	Info	37L4247E19-11	Information	WINEVT 2013-07-...
3	2013-Jul-05 11:22...	Win2008	4625	Info	37L4247E19-11	Information	WINEVT 2013-07-...
4	2013-Jul-05 11:22...	Win2008	5615	Error	37L4247E19-11	Success	WINEVT 2013-07-...
5	2013-Jul-05 11:22...	Win2008	5617	Error	37L4247E19-11	Success	WINEVT 2013-07-...
6	2013-Jul-05 11:22...	Win2008	1025	Info	37L4247E19-11	Information	WINEVT 2013-07-...
7	2013-Jul-05 11:22...	Win2008	1033	Info	37L4247E19-11	Information	WINEVT 2013-07-...
8	2013-Jul-05 11:22...	Win2008	1003	Info	37L4247E19-11	Information	WINEVT 2013-07-...

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows2008_dirEvent_sensageRetriever
- microsoft_windows_dirEvent_sensageRetriever

Windows Directory Service Events Summary per Day

Summary of Directory Service events per day by computer and Windows system version.

COLUMNS

Column	Description
Date	Date of the event (<i>yyyy-mm-dd</i>)
Version	Name of the Windows system version on which the Directory Service event occurred
Computer Name	Name of the machine or device where the Directory Service event occurred
Count	Number of Directory Service events

EXAMPLE

The screenshot shows a report titled "Windows Directory Service Events Summary per Day" with a filter "For 20 year(s) ending on 2015-Jan-26". The table has columns: #, Date, Version, Computer Name, and Count. The data includes:

#	Date	Version	Computer Name	Count
1	2007-03-09	Win2003	TESTAD23	84
2	2007-03-10	Win2003	TESTAD23	90
3	2007-03-11	Win2003	TESTAD23	4
4	2007-03-12	Win2003	TESTAD23	16
5	2013-07-05	Win2008	WIN-928F225SYY0	946
6	2013-07-05	Win2008	37L4247E19-11	13

Page navigation: 1 to 6 of 6

INTELLISchema View

- None

TABLES REFERENCED

- microsoft_windows2008_dirEvent_sensageRetriever
- microsoft_windows_dirEvent_sensageRetriever

Windows Major Security Events

Details of Windows major security events.

COLUMNS

Column	Description
Time	Time of event (<i>yyyy-mm-dd hh:mm:ss</i>)
Computer	Name of machine where the Windows security event occurred.
Event ID	Windows Event ID
Event Description	Windows Event ID description
Change	The change that occurred.
Performed By	User account

EXAMPLE

Windows Major Security Events						
#	Time	Computer	Event ID	Event Description	Change	Performed By
1	2005-Jun-16 20:15:34 GMT	C3QAIS1	643	Domain policy cha...	Domain: C3QAIS1\$	
2	2007-Mar-01 00:21:16 GMT	TESTAD23	643	Domain policy cha...	Domain: SENSAGE2	administrator\SENS...
3	2007-Mar-01 00:21:18 GMT	TESTAD23	643	Domain policy cha...	Domain: SENSAGE2	administrator\SENS...
4	2007-Mar-01 00:56:22 GMT	TESTAD23	643	Domain policy cha...	Domain: SENSAGE2	TESTAD23\$\SENSA...
5	2007-Mar-01 01:06:26 GMT	TESTAD23	608	User right assigned	User Right: SeTcbP...	TESTAD23\$\SENSA...
6	2007-Mar-01 01:11:28 GMT	TESTAD23	609	User right removed	User Right: SeTcbP...	TESTAD23\$\SENSA...
7	2007-Mar-01 01:28:26 GMT	TESTAD23	517	The audit log was c...	Security log cleared	Administrator\SENS...
8	2008-Aug-14 19:49:25 GMT	CORPSERV01	517	The audit log was c...	Security log cleared	admin_jsmith\PS
9	2009-May-01 16:14:05 GMT	WIN-012345ABC...	4704	User right assigned	Target Account: S-1...	TEST\TEST
10	2009-May-01 16:16:15 GMT	WIN-012345ABC...	4705	User right removed	Target Account: S-1...	TEST\TEST

INTELLISchema View

- None

TABLES REFERENCED

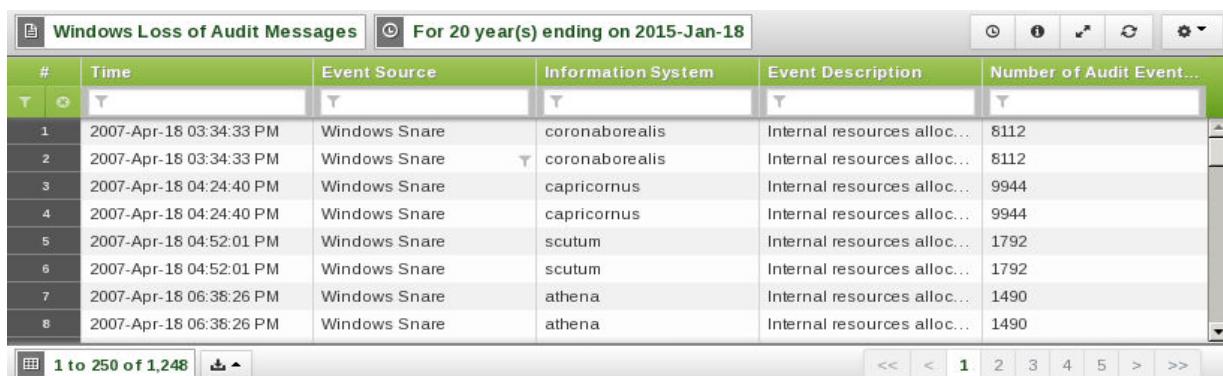
- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

Windows Loss of Audit Messages

COLUMNS

Column	Description
Time	Time the audit message loss occurred (yyyy-mm-dd hh:mm:ss)
Event Source	Event log source where audit messages were lost
Information System	Name of the machine or device that lost audit messages
Event Description	Description of the event
Number of Audit Events	Number of audit events lost

EXAMPLE



The screenshot shows a software interface for viewing audit logs. The title bar reads "Windows Loss of Audit Messages" and "For 20 year(s) ending on 2015-Jan-18". The main area is a grid table with columns: #, Time, Event Source, Information System, Event Description, and Number of Audit Events. The grid contains 8 rows of data. At the bottom, there is a navigation bar with buttons for sorting, filtering, and page navigation.

#	Time	Event Source	Information System	Event Description	Number of Audit Events
1	2007-Apr-18 03:34:33 PM	Windows Snare	coronaborealis	Internal resources alloc...	8112
2	2007-Apr-18 03:34:33 PM	Windows Snare	coronaborealis	Internal resources alloc...	8112
3	2007-Apr-18 04:24:40 PM	Windows Snare	capricornus	Internal resources alloc...	9944
4	2007-Apr-18 04:24:40 PM	Windows Snare	capricornus	Internal resources alloc...	9944
5	2007-Apr-18 04:52:01 PM	Windows Snare	scutum	Internal resources alloc...	1792
6	2007-Apr-18 04:52:01 PM	Windows Snare	scutum	Internal resources alloc...	1792
7	2007-Apr-18 06:38:26 PM	Windows Snare	athena	Internal resources alloc...	1490
8	2007-Apr-18 06:38:26 PM	Windows Snare	athena	Internal resources alloc...	1490

INTELLISchema View

- “Loss of Audit Messages: Windows”, on page 118

TABLES REFERENCED

- None

Windows Active Directory Object Changes

Details of attempts to change Active Directory objects.

COLUMNS

Column	Description
Time	Time the object was changed (<i>yyyy-mm-dd hh:mm:ss</i>)
Domain	Name of Windows domain
Object Type	Type of the Active Directory object changed
Object Name	Name of the Active Directory object changed
Accesses	Accesses what Active Directory objects
Properties	Properties of the Active Directory objects
Changed By	Account used to change Active Directory object

EXAMPLE

#	Time	Domain	Object Type	Object Name	Accesses	Properties	Changed By
1	2007-03-01...		%{19195a5b-6da0-11d...		% % 7685	% % 7685 %{771727b...	SENSAGE2/administ...
2	2007-03-01...		%{19195a5b-6da0-11d...		% % 7685	% % 7685 %{771727b...	SENSAGE2/administ...
3	2007-03-01...		%{19195a5b-6da0-11d...		% % 7685	% % 7685 %{771727b...	SENSAGE2/administ...
4	2007-03-01...		%{bf967a9c-0de6-11d...		% % 7685	% % 7685 %{bc0ac24...	SENSAGE2/administ...
5	2007-03-01...		%{19195a5b-6da0-11d...		% % 7688	% % 7688 %{1131f6aa...	SENSAGE2/TESTAD...
6	2007-03-01...		%{f30e3bc2-9ff0-11d1...		% % 7685	% % 7685 %{771727b...	SENSAGE2/Administ...
7	2007-03-01...		%{f30e3bc2-9ff0-11d1...		% % 7685	% % 7685 %{771727b...	SENSAGE2/Administ...
8	2007-03-01...		%{f30e3bc2-9ff0-11d1...		% % 7685	% % 7685 %{771727b...	SENSAGE2/Administ...
9	2007-03-01...		%{f30e3bc2-9ff0-11d1...		% % 7685	% % 7685 %{771727b...	SENSAGE2/Administ...
10	2007-03-01...		%{f30e3bc2-9ff0-11d1...		% % 7685	% % 7685 %{771727b...	SENSAGE2/Administ...

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

Windows Active Directory Policy Changes

Details of attempts to change Active Directory policies.

COLUMNS

Column	Description
Time	Time the Active Directory policy was changed (<i>yyyy-mm-dd hh:mm:ss</i>)
Information System	Name of user's machine
Event ID	Windows Event ID
Policy	Policy that was changed
Affected	Item that was affected by the policy change such as domain
Caller User Name	User account who changed the Active Directory policy
Caller Domain	Domain of user account who changed the Active Directory policy
Logon Key	Logon Key

EXAMPLE

#	Time	Information System	Event ID	Policy	Affected	Caller User Name	Caller Domain	Logon Key
1	2007-Mar-01 ...	TESTAD23	643	-	SENSAGE2	administrator	SENSAGE2	(0x0,0x2A12AB)
2	2007-Mar-01 ...	TESTAD23	643	-	SENSAGE2	administrator	SENSAGE2	(0x0,0x2A12AB)
3	2007-Mar-01 ...	TESTAD23	643	Lockout Policy	SENSAGE2	TESTAD23\$	SENSAGE2	(0x0,0x3E7)
4	2007-Mar-01 ...	TESTAD23	608	SeTcbPrivilege	%{S-1-5-21-2...}	TESTAD23\$	SENSAGE2	(0x0,0x3E7)
5	2007-Mar-01 ...	TESTAD23	609	SeTcbPrivilege	%{S-1-5-21-2...}	TESTAD23\$	SENSAGE2	(0x0,0x3E7)
6	2005-Jun-16 ...	C3QAIS1	643	Password P...		C3QAIS1\$	DEV	(0x0,0x3E7)
7	2009-May-01 ...	WIN-012345A...	4704	SeCreateTok...	S-1-5-21-634...	WIN-0T4GGI...	TEST	0x3e7
8	2009-May-01 ...	WIN-012345A...	4705	SeCreateTok...	S-1-5-21-634...	WIN-0T4GGI...	TEST	0x3e7
9	2009-May-01 ...	WIN-012345A...	4704	SeCreateTok...	S-1-1-0	WIN-0T4GGI...	TEST	0x3e7

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

Windows Active Directory Users - Deleted or Disabled

Details of deleted or disabled Active Directory users.

COLUMNS

Column	Description
Time	Time the Active Directory user was deleted/disabled (<i>yyyy-mm-dd hh:mm:ss</i>)
Event Source	Event source
Domain Controller	Name of the Windows domain controller
Domain	Name of Windows domain
Done By	User who disabled/deleted Active Directory users
User Added	User added
Event ID	Windows Event ID
Event Description	Windows Event ID description
Role	Role of domain ("Member Server" or "Domain Controller")

EXAMPLE

#	Time	Event Sou...	Domain C...	Domain	Done by	User Added	Event ID	Event Des...	Role
1	2009-04-14...	Windows R...	win-012345...	TEST		chamarts	4726	User Accou...	Domain Co...
2	2007-03-01...	Windows R...	testad23	SENSAGE2	Administrator	test_user	630	User Accou...	Domain Co...
3	2007-03-01...	Windows R...	testad23	SENSAGE2	Administrator	test_user	630	User Accou...	Domain Co...

"/>

INTELLISchema VIEW

- analytics.intellischema.accountadditionanddeletion_windows

TABLES REFERENCED

- None

Windows Active Directory Users - Lockouts and Password Resets

Details of Active Directory users' events (lockouts and password resets)

COLUMNS

Column	Description
Time	Time the lockout or password reset occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Event ID	Windows Event ID
Account	Account that had the lockout/password reset
Account_ID	Account ID
Action	Action name
Caller_Machine Name	Caller machine name
Caller_User Name	Caller user of the event (lockout/password reset)
Caller_Domain	Caller domain
Caller_Login ID	ID of caller login
Role	Role of domain ("Member Server" or "Domain Controller")

EXAMPLE

#	Time	Event ID	Account	Account_ID	Action	Caller_Ma...	Caller_Us...	Caller_Do...	Caller_Lo...	ro...
1	2007-Mar-0...	628	test_user	%{S-1-5-21...}	Password ...		Administrator	SENSAGE2	(0x0,0x3D1...	
2	2007-Mar-0...	628	test_user	%{S-1-5-21...}	Password ...		Administrator	SENSAGE2	(0x0,0x3D1...	
3	2007-Mar-0...	628	test_user	%{S-1-5-21...}	Password ...		Administrator	SENSAGE2	(0x0,0x3D1...	
4	2007-Mar-0...	644	test_user	%{S-1-5-21...}	Locked	TESTAD23\$	TESTAD23\$	SENSAGE2	(0x0,0x3E7)	
5	2007-Mar-0...	671	test_user	%{S-1-5-21...}	Unlocked		Administrator	SENSAGE2	(0x0,0x408...	
6	2007-Mar-0...	671	test_user	%{S-1-5-21...}	Unlocked		Administrator	SENSAGE2	(0x0,0x408...	
7	2007-Mar-0...	627	newbie	%{S-1-5-21...}	Password ...		newbie	SENSAGE2	(0x0,0x416...	
8	2008-Aug-...	628	user_1	%{S-1-5-21...}	Password ...		sys_provis...	PS	(0x0,0x149...	
9	2008-Aug-...	628	user_2	%{S-1-5-21...}	Password ...		sys_provis...	PS	(0x0,0x149...	

INTELLISCHEMIA VIEW

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

Windows Active Directory Users - New or Enabled

Details of Active Directory users' events (new or enabled).

COLUMNS

Column	Description
Time	Time the user created/enabled (yyyy-mm-dd hh:mm:ss)
Event Source	Event-log source that recorded the event
Domain Controller	Name of Windows domain controller
Domain	Name of Windows domain
Done by	Done by
User Added	User that was added
Event ID	Windows Event ID
Event Description	Windows Event ID description
Role	Role of domain ("Member Server" or "Domain Controller")

EXAMPLE

#	Time	Event Sou...	Domain C...	Domain	Done by	User Added	Event ID	Event Des...	Role
1	2009-04-14...	Windows R...	win-012345...	TEST		chamarts	4720	User Accou...	Domain Co...
2	2007-03-01...	Windows R...	testad23	SENSAGE2	Administrator	test_user	624	User Accou...	Domain Co...
3	2007-03-01...	Windows R...	testad23	SENSAGE2	Administrator	test_user	624	User Accou...	Domain Co...
4	2007-03-01...	Windows R...	testad23	SENSAGE2	Administrator	test_user	624	User Accou...	Domain Co...
5	2008-08-14...	Windows R...	corperv01	PS	sys_provisi...	user_1	624	User Accou...	Domain Co...
6	2008-08-14...	Windows R...	corperv01	PS	sys_provisi...	user_2	624	User Accou...	Domain Co...
7	2008-08-14...	Windows R...	corperv01	PS	admin_jsmith	user_3	624	User Accou...	Domain Co...
8	2005-06-17...	Windows S...	c3devweb3	C3DEVWEB3	samadmin	testsnaire	624	User Accou...	Member Se...
9	2005-06-17...	Windows S...	c3devweb3	C3DEVWEB3	samadmin	tsnare	624	User Accou...	Member Se...

1 to 9 of 9

INTELLISchema VIEW

- analytics.intellischema.accountadditionanddeletion_windows

TABLES REFERENCED

- None

Windows Security Objects Accessed

Details of attempts to access a security object on a Microsoft Windows system.

NOTE: Auditing must be enabled on the object.

COLUMNS

Column	Description
Time	Time the security object was accessed (yyyy-mm-dd hh:mm:ss)
Information system	Machine where the security object was accessed
User	User account used to access the security object
Object	Name of accessed security object
Domain	Windows domain name
Object Type	Type of security object accessed
Access Type	Type of access
Logon Key	Logon key
Action	Action taken on the security object

EXAMPLE

#	Time	Information...	User	Object	Domain	Object Type	Access Ty...	Logon Key	Action
1	2009-May-02 07:55:07 PM	win-012345...		PlugPlayS...		Security	% %1553		Objec
2	2008-Aug-15 02:36:09 AM	corpserv01	sales_pbe...	C:\W\sales_...	PS	File	Network		Objec
3	2008-Aug-15 02:36:13 AM	corpserv01	sales_pbe...	C:\W\sales_...	PS	File	Network		Objec
4	2008-Aug-15 02:36:26 AM	corpserv01	sales_pbe...	C:\W\sales_...	PS	File	Network		Objec
5	2008-Aug-15 02:36:38 AM	corpserv01	sales_pbe...	C:\W\sales_...	PS	File	Network		Objec
6	2008-Aug-15 02:37:23 AM	corpserv01	sales_pbe...	C:\W\sales_...	PS	File	Network		Objec
7	2008-Aug-15 02:37:27 AM	corpserv01	sales_pbe...	C:\W\sales_...	PS	File	Network		Objec

INTELLISCALEMIA VIEW

- “Security Objects: Windows”, on page 135.

TABLES REFERENCED

- None

Windows Security Objects Deleted

Details of attempts to delete a Security object on a Microsoft Windows system.

NOTE: Auditing must be enabled on the object.

COLUMNS

Columns	Description
Time	Time the security object was accessed (<i>yyyy-mm-dd hh:mm:ss</i>)
Information System	Machine or device where the security object was accessed
User	User account used to access the security object
Object Type	Type of object deleted
Domain	Domain name
Object Deleted	Description of deleted object
Access Type	Type of access
Logon Key	Logon key used for deletion
Action	Action taken on the deletion.

EXAMPLE

#	Time	Infor...	User	Object	Domain	Objec...	Acces...	Logo...	Action
1	2007-Dec-04 10:03:54 AM		virgo					Local	
2	2008-Aug-15 05:37:46 AM		corps...	sales_...	C:\RE...	PS	File	Network	(0x0,0...)

INTELLISchema VIEW

- “Security Objects: Windows”, on page 135

TABLES REFERENCED

- None

Windows Security Objects Access Optimized

Details of attempts to access a security object on a Microsoft Windows system.

COLUMNS

Columns	Description
Object_Open_Time	Time security object was opened (yyyy-mm-dd hh:mm:ss)
Object_Close_Time	Time security object was closed (yyyy-mm-dd hh:mm:ss)
Information System	Machine where the security object was accessed
Event_ID	Windows Event ID
Domain	Windows domain name
Object_Type	Type of security object accessed
Object_Name	Name of accessed security object
User_Name	User account
Access_Type	Type of access
Caller_User_Name	Caller's user name
Caller_Domain	Caller's domain name

EXAMPLE

The screenshot shows a database grid titled "Windows Security Objects Accessed Optimized". The grid has 11 columns with headers: #, Object_Open_Time, Object_Cl..., Informati..., Event_ID, Domain, Object_Ty..., Object_Na..., User_Name, Access_T..., and Ca... (partially visible). The data consists of 250 rows of security access logs. Each row contains information such as the date and time of access, the type of object (e.g., CAPRICO, CANISMIN, DORADO, GEMINI, MONOCER, SCULPTOR, CARINA, DIONYSUS, CANCER), the domain (e.g., IT, MEDICAL, FINANCE), the file path (e.g., C:\...\DOCU..., C:\...\WINN..., D:\...\oracle..., C:\...\WINN..., C:\...\WINN..., \...\BaseNa..., C:\...\DOCU..., \...\BaseNa..., C:\...\DOCU...), the user name (e.g., s.williams, j.edwards, c.wilson, k.johnson, d.turner, j.johnson, s.martin, g.lee, r.robinson), and the access type (e.g., Network, Network, Network, Network, Network, Network, Network, Network, Network).

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- microsoft_windows_securityEvent_sensageRetriever
- microsoft_windows_securityEvent_snare
- microsoft_windows2008_securityEvent_sensageRetriever
- microsoft_windows2008_securityEvent_snare

CHAPTER 9

Foundation Analytics Reports (Unix/Linux)

The SenSage AP Foundation Analytics reports for Unix/Linux is designed to enable monitoring of the operational security and effectiveness of your business. These reports include those used for monitoring the status of your SenSage AP deployment. This chapter provides a reference for the Foundation Analytic reports, which include the associated IntelliSchema views and the columns available for reporting.

UNIX/LINUX REPORTS

The Unix/Linux reports display events from Unix or Linux systems and include the following:

- “[Unix or Linux Login Details](#)”, on page 254
- “[Unix or Linux Failed Login Summary by User](#)”, on page 255
- “[Unix or Linux Failed Login Summary by Count](#)”, on page 256
- “[Unix or Linux Failed Login Summary by Server](#)”, on page 257
- “[Unix or Linux Success Login Summary by User](#)”, on page 258
- “[Unix or Linux Success Login Summary by Count](#)”, on page 259
- “[Unix or Linux Success Login Summary by Server](#)”, on page 260
- “[Unix or Linux SSH and FTP Login Details](#)”, on page 261
- “[Unix or Linux Privileged Commands Details](#)”, on page 262
- “[Unix or Linux Elevated Access Success \(su and sudo\) Summary by Count](#)”, on page 263
- “[Unix or Linux Elevated Access Success \(su and sudo\) Summary by Date](#)”, on page 264
- “[Unix or Linux Elevated Access Success \(su and sudo\) Summary by Server](#)”, on page 265
- “[Unix or Linux Elevated Access Failed \(su and sudo\) Detail by Date](#)”, on page 266
- “[Unix or Linux Elevated Access Failed \(su and sudo\) Summary by Count](#)”, on page 267
- “[Unix or Linux Elevated Access Failed \(su and sudo\) Summary by Server](#)”, on page 268
- “[Unix or Linux Elevated SU Access Failed by Server](#)”, on page 269
- “[Unix or Linux Elevated SUDO Access Failed by Date](#)”, on page 270
- “[Unix or Linux Elevated SUDO Access Failed by Server](#)”, on page 271

Unix or Linux Login Details

Details of login attempts on Unix or Linux systems.

NOTE: Due to the way login events are logged, a single login may be represented by more than one row.

COLUMNS

Column	Description
Time	Time the login occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Information System	Name of the machine or device where the login occurred
Event Source	Application or subsystem used for the login
Account	User account used for the login
Result	Outcome of login. Possible values: <ul style="list-style-type: none"> • Failure • Success • Unknown

EXAMPLE

#	Time	Information Sys...	Log Type	User	Result
1	2005-Jan-25 08:31:50 PM	roc08650d010	Unix su	root	Success
2	2005-Jan-25 08:31:54 PM	roc08650d045	Unix su	root	Success
3	2005-Jan-25 08:32:45 PM	roc08b80p002e1	Unix su	root	Success
4	2005-Jan-25 08:33:04 PM	roc08650d089	Unix su	a1ui	Failure
5	2005-Jan-25 08:33:05 PM	roc08650d045	Unix su	root	Success
6	2005-Jan-25 08:33:08 PM	roc08650d089	Unix su	a1ui	Success
7	2005-Jan-25 08:33:20 PM	roc08650d037	Unix su	root	Success
8	2005-Jan-25 08:35:01 PM	roc08650p013	Unix su	root	Success

INTELLISchema VIEW

- “User Logins: Linux/Unix”, on page 147

TABLES REFERENCED

- None

Unix or Linux Failed Login Summary by User

The number of failed login attempts by user on Unix or Linux systems for each information system and event source.

COLUMNS

Column	Description
User	Unix/Linux user account.
Information System	Device or computer
Count	Number of failures for the information system.

EXAMPLE

#	User	Information System	Count
1		p12	3
2		192.168.0.83	1
3	a1ef	roc08650d101	1
4	a1i0	roc08650d022	3
5	a1ui	roc08650d089	1
6	a1vr	roc08650d092	1
7	a1xk	roc08650d043	1
8	a1xk	roc.example.com	1

INTELLISchema VIEW

- “User Logins: Linux/Unix”, on page 147

TABLES REFERENCED

- None

Unix or Linux Failed Login Summary by Count

The number of failed login attempts by count on Unix or Linux systems for each information system and event source.

COLUMNS

Column	Description
User	Unix/Linux user account.
Information System	Device or computer
Count	Number of failures for the information system.

EXAMPLE

#	User	Information System	Count
1	root	cs10	9
2	a4bf	roc08650d076	8
3	pathfp	roc08650d026	8
4	ab3p	roc08650d019	6
5	user1	p12	4
6	eginorio	10.0.0.50	4
7	a6a	roc08615p001	4
8	ab2t	roc08650d043	4

INTELLISchema View

- “User Logins: Linux/Unix”, on page 147

TABLES REFERENCED

- None

Unix or Linux Failed Login Summary by Server

The number of failed login attempts by server on Unix or Linux systems for each information system and event source.

COLUMNS

Column	Description
User	Unix/Linux user account.
Information System	Device or computer
Count	Number of failures for the information system.

EXAMPLE

#	User	Information System	Count
1	eginorio	10.0.0.50	4
2	barney	192.168.0.83	1
3		192.168.0.83	1
4	dfg	aix-01	2
5	root	aix-01	4
6	example	aix-01	4
7	abc	aix-01	1
8	jsaxton	aix-01	1

1 to 82 of 82

INTELLISchema View

- “User Logins: Linux/Unix”, on page 147

TABLES REFERENCED

- None

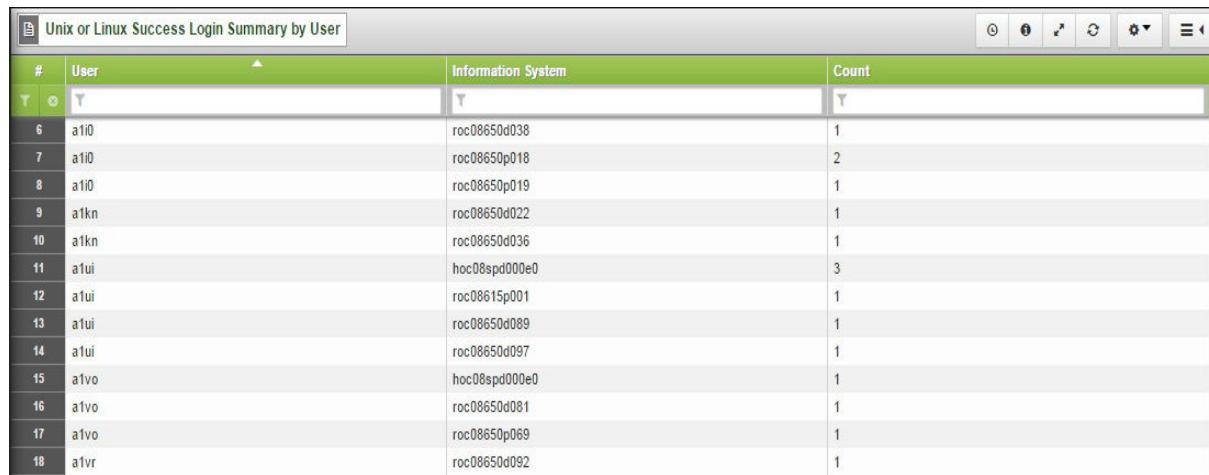
Unix or Linux Success Login Summary by User

The number of successful and unsuccessful login attempts by user on Unix or Linux systems for each information system and event source.

COLUMNS

Column	Description
User	Unix/Linux user account.
Information System	Device or computer
Count	Number of failures for the information system.

EXAMPLE



The screenshot shows a database grid with the following data:

#	User	Information System	Count
6	a10	roc08650d038	1
7	a10	roc08650p018	2
8	a10	roc08650p019	1
9	a1kn	roc08650d022	1
10	a1kn	roc08650d036	1
11	a1ui	hoc08spd000e0	3
12	a1ui	roc08615p001	1
13	a1ui	roc08650d089	1
14	a1ui	roc08650d097	1
15	a1vo	hoc08spd000e0	1
16	a1vo	roc08650d081	1
17	a1vo	roc08650p069	1
18	a1vr	roc08650d092	1

INTELLISchema View

- “User Logins: Linux/Unix”, on page 147

TABLES REFERENCED

- None

Unix or Linux Success Login Summary by Count

The number of successful and unsuccessful login attempts by count on Unix or Linux systems for each information system and event source.

COLUMNS

Column	Description
User	Unix/Linux user account.
Information System	Device or computer
Count	Number of failures for the information system.

EXAMPLE

#	User	Information System	Count
1	root	cs10	438
2	root	roc08b80p002e1	212
3	root	roc08650p034	197
4	root	roc08650p035	172
5	root	roc08650d045	134
6	root	roc08650p056	111
7	root	wkstechlib	103
8	root	roc08650p038	94
9	root	roc08650d001	74
10	root	roc08650p007	68
11	root	roc08650d047	55

INTELLISchema VIEW

- “User Logins: Linux/Unix”, on page 147

TABLES REFERENCED

- None

Unix or Linux Success Login Summary by Server

The number of successful and unsuccessful login attempts by count on Unix or Linux systems for each information system and event source.

COLUMNS

Column	Description
User	Unix/Linux user account.
Information System	Device or computer
Count	Number of failures for the information system.

EXAMPLE

#	User	Information System	Count
1	eginorio	10.0.0.50	10
2	root	aix-01	18
3	jsaxton	aix-01	9
4	jsaxton	aix-02	3
5	root	andromeda1	3
6	dcarter15	andromeda16	1
7	dcarter16	andromeda17	1
8	dcarter25	andromeda26	1
9	dcarter35	andromeda36	1
10	dcarter38	andromeda39	1
11	dcarter3	andromeda4	1

INTELLISchema View

- “User Logins: Linux/Unix”, on page 147

TABLES REFERENCED

- None

Unix or Linux SSH and FTP Login Details

Details of login attempts on Unix or Linux systems.

NOTE: Due to the way login events are logged, a single login may be represented by more than one row.

COLUMNS

Column	Description
Time	Time the login occurred (yyyy-mm-dd hh:mm:ss)
Information System	Name of the machine or device where the login occurred
Process	Process used for the login
Username	User account used for the login
Remote host	Name of the remote host
Event action	Action for event
unparsed_message	Unparsed (source) message

EXAMPLE

The screenshot shows a database query results page for the 'Unix or Linux SSH And FTP Login Details' table. The results are filtered for the last 20 years, ending on 2014-Dec-16. The data grid has 8 rows, each representing a login event. The columns are labeled: #, Time, Information Sy..., Process, Username, Remote host, Event action, and unparsed mes... . The 'Time' column shows dates from November 2014 to November 2013. The 'Event action' column consistently shows 'session opened'. The 'unparsed mes...' column shows the timestamp of the session opening. Navigation controls at the bottom indicate 1 to 250 of 498 rows.

#	Time	Information Sy...	Process	Username	Remote host	Event action	unparsed mes...
1	14-Nov-28 12:59:...	quant01-vm19	sshd	root		session opened	2014-11-28 04:59:...
2	14-Nov-27 13:29:...	quant01-vm19	sshd	root		session opened	2014-11-27 05:29:...
3	14-Nov-26 13:11:...	quant01-vm19	sshd	root		session opened	2014-11-26 05:11:...
4	14-Nov-26 12:50:...	quant01-vm19	sshd	root		session opened	2014-11-26 04:50:...
5	14-Nov-25 20:06:...	quant01-vm19	sshd	root		session opened	2014-11-25 12:06:...
6	14-Nov-25 20:01:...	quant01-vm19	sshd	root		session opened	2014-11-25 12:01:...
7	14-Nov-25 14:38:...	quant01-vm19	sshd	root		session opened	2014-11-25 06:38:...
8	14-Nov-25 04:32:...	quant01-vm19	sshd	root		session opened	2014-11-24 20:32:...

INTELLISchema View

- None

TABLES REFERENCED

- unix_ftpd_syslogng
- unix_sshd2_syslogng

Unix or Linux Privileged Commands Details

Details of privileged commands executed on Unix or Linux systems.

COLUMNS

Column	Description
Time	Time the privileged command was executed (<i>yyyy-mm-dd hh:mm:ss</i>)
Information System	Name of the machine or device where the command was executed
Log Type	Type of log
User	Name of user account that executed the command
Event Description	Description of the command executed
Result	Result of the command execution. Possible values: Failed Success Unknown

EXAMPLE

#	Time	Information System	Log Type	User	Event Description	Result
1	2005-Jan-25 08:31:50 PM	roc08650d010	Unix su	root	su u1z3	Success
2	2005-Jan-25 08:31:54 PM	roc08650d045	Unix su	root	su cmpvcp	Success
3	2005-Jan-25 08:32:45 PM	roc08b80p002e1	Unix su	root	su ctmem	Success
4	2005-Jan-25 08:33:04 PM	roc08650d089	Unix su	a1ui	su root	Failure
5	2005-Jan-25 08:33:05 PM	roc08650d045	Unix su	root	su cmpvcp	Success
6	2005-Jan-25 08:33:08 PM	roc08650d089	Unix su	a1ui	su root	Success
7	2005-Jan-25 08:33:20 PM	roc08650d037	Unix su	root	su cmpvcp	Success
8	2005-Jan-25 08:35:01 PM	roc08650p013	Unix su	root	su dis	Success

INTELLISchema View

- “Privileged Commands: Linux/Unix”, on page 131

TABLES REFERENCED

- None

Unix or Linux Elevated Access Success (su and sudo) Summary by Count

Elevated access (su and sudo) success summary by count executed on Unix or Linux systems.

COLUMNS

Column	Description
User	Unix/Linux user account.
Information System	Device or computer
Count	Number of failures for the information system.

EXAMPLE

#	User	Information System	Count
1	root	roc08b80p002e1	212
2	root	roc08650p034	197
3	root	roc08650p035	172
4	root	rh6-az-06	168
5	root	roc08650d045	134
6	root	roc08650p056	111
7	root	roc08650p038	94
8	root	roc08650d001	74
9	root	roc08650p007	68
10	root	roc08650d047	55
11	root	roc08h80p003	51
12	root	fakehost	48

INTELLISchema View

- “Privileged Commands: Linux/Unix”, on page 131

TABLES REFERENCED

- None

Unix or Linux Elevated Access Success (su and sudo) Summary by Date

Elevated access (su and sudo) success summary by date executed on Unix or Linux systems.

COLUMNS

Column	Description
Result	Outcome of the elevated access attempt
Date	Date of elevated access attempt
Information System	Device or computer where failure occurred
Count	Number of access attempts on the device or computer

EXAMPLE

#	Result	Date	Information System	Count
1	Success	2005-Jan-24	hoc08wuv05	1
2	Success	2005-Jan-24	hoc08spd011e1	1
3	Success	2005-Jan-24	roc08650d016	1
4	Success	2005-Jan-24	hoc08spd007e1	3
5	Success	2005-Jan-24	roc08h80d001e0	14
6	Success	2005-Jan-24	roc08615p001	18
7	Success	2005-Jan-24	roc08650p059	1
8	Success	2005-Jan-24	roc08650d080	1
9	Success	2005-Jan-24	roc08650d093	1
10	Success	2005-Jan-24	roc08650p020	2

INTELLISchema View

- “Privileged Commands: Linux/Unix”, on page 131

TABLES REFERENCED

- None

Unix or Linux Elevated Access Success (su and sudo) Summary by Server

Elevated access (su and sudo) success summary by server executed on Unix or Linux systems.

COLUMNS

Column	Description
User	Unix/Linux user account.
Information System	Device or computer
Count	Number of failures for the information system.

EXAMPLE

#	Information System	User	Count
1	10.0.0.50	eginorio	10
2	aix-01	root	5
3	aix-02	jsaxton	1
4	fakehost	root	48
5	fakehost	openview	1
6	fakehost02	root	2
7	fakehost3	root	2
8	fakehost3	oracle9i	1
9	fakehost603	root	2
10	fakehost703	root	2
11	hoc0843p12	root	1

INTELLISchema View

- “Privileged Commands: Linux/Unix”, on page 131

TABLES REFERENCED

- None

Unix or Linux Elevated Access Failed (su and sudo) Detail by Date

Elevated access (su and sudo) failure detail by date on Unix or Linux systems.

COLUMNS

Column	Description
Time	Time elevated access failure occurred (yyyy-mm-dd hh:mm:ss)
Information System	Device or computer where failure occurred
Account	Unix/Linux user account..
Event Description	Description of the event
Result	Outcome of the elevated access attempt

EXAMPLE

Unix or Linux Elevated Access Failed (su and sudo) Detail by Date						
#	Time	Information System	Account	Event Description	Result	
1	2005-Jan-25 08:33:04 PM	roc08650d089	a1ui	su root	Failure	
2	2005-Jan-25 08:35:26 PM	roc08650d086	u1k2	su cmpvcp	Failure	
3	2005-Jan-25 08:36:15 PM	roc08650d086	u1k2	su cmpvcp	Failure	
4	2005-Jan-25 08:38:27 PM	roc08650d092	a1vr	su selstga	Failure	
5	2005-Jan-25 08:38:30 PM	roc08650d085	tcm9	su ewvald	Failure	
6	2005-Jan-25 08:42:30 PM	roc08650d040	a1xk	su root	Failure	
7	2005-Jan-25 08:52:47 PM	hoc08spd000e0	a4bb	su root	Failure	
8	2005-Jan-25 09:00:39 PM	roc08650d101	a1ef	su root	Failure	

INTELLISchema View

- “Privileged Commands: Linux/Unix”, on page 131

TABLES REFERENCED

- None

Unix or Linux Elevated Access Failed (su and sudo) Summary by Count

Elevated access (su and sudo) failure detail by date on Unix or Linux systems.

COLUMNS

Column	Description
User	Unix/Linux user account.
Information System	Device or computer
Count	Number of failures for the information system.

EXAMPLE

#	User	Information System	Count
1	a4bf	roc08650d076	8
2	ab2t	roc08650d043	4
3	example	aix-01	4
4	eginorio	10.0.0.50	4
5	mkinsley	p12	3
6	tp5	roc08m80p010	3
7	a1i0	roc08650d022	3
8	u1k2	roc08650d086	2

INTELLISchema View

- “Privileged Commands: Linux/Unix”, on page 131

TABLES REFERENCED

- None

Unix or Linux Elevated Access Failed (su and sudo) Summary by Server

Elevated access (su and sudo) failure detail by date on Unix or Linux systems.

COLUMNS

Column	Description
Information System	Device or computer
User	Unix/Linux user account.
Count	Number of failures for the information system.

EXAMPLE

#	Information System ¹	User ²	Count
1	10.0.0.50	eginorio	4
2	aix-01	example	4
3	fakehost	openview	1
4	fakehost02	bscs	1
5	fakehost04	dsfprod	1
6	fakehost2	oracle9i	2
7	fakehost3	oracle9i	1
8	hoc08spd000e0	a1xk	1

INTELLISchema View

- “Privileged Commands: Linux/Unix”, on page 131

TABLES REFERENCED

- None

Unix or Linux Elevated SU Access Failed by Server

Elevated access (su and sudo) failure detail by date on Unix or Linux systems.

COLUMNS

Column	Description
Time	Time the elevated access attempt occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
User	User account used for the elevated access attempt
Event Description	Description of the event
Information System	Name of the machine or device where the elevated access attempt occurred
Log Type	Type of log
Result	Outcome of the elevated access attempt

EXAMPLE

The screenshot shows a table with the following columns and data:

#	Time	User	Event Description	Information System	Log Type	Result
1	2006-Feb-17 07:40:43 PM	eginorio	su root	10.0.0.50	Unix su	Failure
2	2006-Mar-02 09:22:53 PM	eginorio	su root	10.0.0.50	Unix su	Failure
3	2006-Mar-02 09:23:22 PM	eginorio	su root	10.0.0.50	Unix su	Failure
4	2006-Mar-02 09:24:20 PM	eginorio	su ps	10.0.0.50	Unix su	Failure
5	2005-Nov-19 01:11:04 PM	example	su root	aix-01	Unix su	Failure
6	2005-Nov-19 01:11:09 PM	example	su root	aix-01	Unix su	Failure
7	2005-Nov-19 01:11:52 PM	example	su root	aix-01	Unix su	Failure
8	2005-Nov-19 01:14:08 PM	example	su root	aix-01	Unix su	Failure

Page navigation: 1 to 76 of 76

INTELLISchema View

- “Privileged Commands: Linux/Unix”, on page 131

TABLES REFERENCED

- None

Unix or Linux Elevated SUDO Access Failed by Date

Elevated access (su and sudo) failure detail by date on Unix or Linux systems.

COLUMNS

Column	Description
Time	Time the elevated access attempt occurred (yyyy-mm-dd hh:mm:ss)
User	User account used for elevated access
Event Description	Description of event
Information System	Name of the machine or device where the elevated access was attempted
Log Type	Type of log

EXAMPLE

#	Time	User	Event Description	Information System	Log Type
1	2005-Nov-29 11:22:32 PM	mkinsley	sudo /bin/cat /etc/pa...	p12	Unix sudo
2	2005-Nov-29 11:33:54 PM	mkinsley	sudo /bin/cat	p12	Unix sudo
3	2007-Mar-28 02:19:22 AM	openview	sudo opcat -status	fakehost	Unix sudo

INTELLISchema View

- “Privileged Commands: Linux/Unix”, on page 131

TABLES REFERENCED

- None

Unix or Linux Elevated SUDO Access Failed by Server

Elevated access (su and sudo) failure detail by date on Unix or Linux systems.

COLUMNS

Column	Description
Time	Time the elevated access attempt occurred (yyyy-mm-dd hh:mm:ss)
User	User account used for elevated access
Event Description	Description of event
Information System	Name of the machine or device where the elevated access was attempted
Log Type	Type of log

EXAMPLE

Unix or Linux Elevated SUDO Access Failed by Server					
#	Time	User	Event Description	Information System	Log Type
1	2007-Mar-28 02:19:22 AM	openview	sudo opcat -status	fakehost	Unix suc
2	2005-Nov-29 11:22:32 PM	mkinsley	sudo /bin/cat /etc/pa...	p12	Unix suc
3	2005-Nov-29 11:33:54 PM	mkinsley	sudo /bin/cat	p12	Unix suc

1 to 3 of 3

INTELLISchema View

- “Privileged Commands: Linux/Unix”, on page 131

TABLES REFERENCED

- None

Systems Analytics Reports

The SenSage AP Analytics reports display system events such as EDW command tools usage, including disk space, volume of Collector activity, internal system events. This chapter provides a reference for Systems Analytics Reports, including lists of columns available for reporting.

The Systems Analytics Reports include the following groups of reports:

- “[EDW \(SLS\) Command Tools Usage Reports](#)”, next
- “[Collector Activity Monitoring Reports](#)”, on page 282
- “[Internal Systems Reports](#)”, on page 298

EDW (SLS) COMMAND TOOLS USAGE REPORTS

The EDW group of reports display usage of EDW command tools and disk space usage and includes the following reports:

- “[EDW \(SLS\) ATManage Command History](#)”, next
- “[EDW \(SLS\) ATQuery Command History](#)”, on page 275
- “[EDW \(SLS\) Command History](#)”, on page 276
- “[EDW \(SLS\) Command History per User](#)”, on page 277
- “[EDW \(SLS\) Load Command History](#)”, on page 278
- “[EDW \(SLS\) Percent Disk Space Usage](#)”, on page 279
- “[EDW \(SLS\) System Disk Space Usage Alerts](#)”, on page 280
- “[EDW \(SLS\) System Disk Space per Node](#)”, on page 281

EDW (SLS) ATManage Command History

History of EDW (SLS) ATManage tool command usage.

COLUMNS

Column	Description
Command	EDW (SLS) command
Method Name	Name of the method
User	User who ran the command
Source IP	Source IP
Host	Host where command was run

EXAMPLE

The screenshot shows a software interface titled "SLS ATManage Command History". It features a table with six columns: #, Command, Method Name, User, Source IP, and Host. The table has one data row. The "Command" column contains "atmanage", the "Method Name" column contains "Addamark.ExecuteSql", the "User" column contains "administrator", the "Source IP" column contains "0.0.0.0", and the "Host" column contains "quant01-vm08.con2.hex". The table header is green, and the data rows are white. There are navigation buttons at the bottom left, including a grid icon, a "1 to 1 of 1" label, and arrows for sorting or filtering.

#	Command	Method Name	User	Source IP	Host
1	atmanage	Addamark.ExecuteSql	administrator	0.0.0.0	quant01-vm08.con2.hex

INTELLISchema View

- None

TABLES REFERENCED

- sensage_sls_syslogng

EDW (SLS) ATQuery Command History

History of EDW (SLS) ATQuery tool command usage.

COLUMNS

Column	Description
Command	EDW (SLS) command
Method Name	Name of the method
User	User who ran the command
Source IP	Source IP
Host	Host where command was run
Statement	SQL statement

EXAMPLE

#	Command	Method Name	User	Source IP	Host	Statement
1	atquery	Addamark.ExecuteSql	Administrator	0.0.0.0	-	SELECT * FRO
2	atquery	Addamark.ExecuteSql	Administrator	0.0.0.0	-	SELECT * FRO
3	atquery	Addamark.ExecuteSql	administrator	0.0.0.0	-	select 1 = count
4	atquery	Addamark.ExecuteSql	administrator	0.0.0.0	-	-----
5	atquery	Addamark.ExecuteSql	administrator	0.0.0.0	-	CREATE OR RI
6	atquery	Addamark.ExecuteSql	administrator	0.0.0.0	-	CREATE OR RI

INTELLISchema View

- None

TABLES REFERENCED

- sensage_sls_syslogng

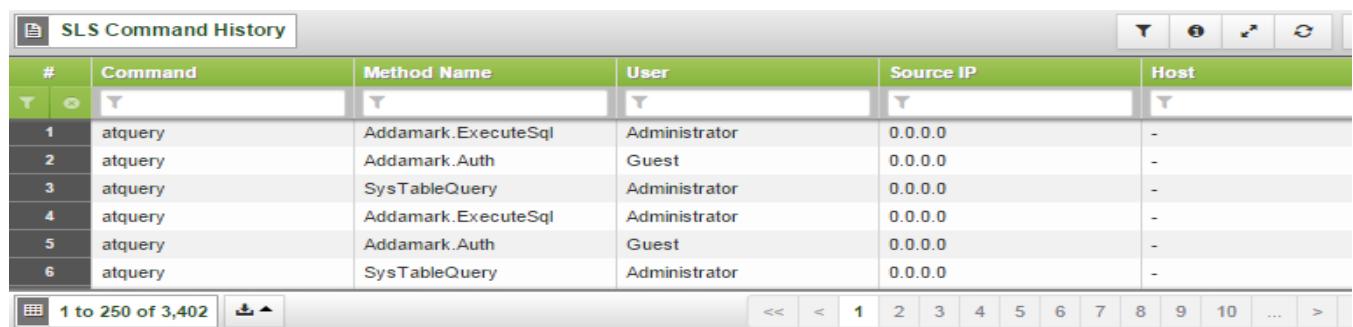
EDW (SLS) Command History

History of EDW (SLS) commands.

COLUMNS

Column	Description
Command	EDW (SLS) command
Method Name	Name of the method
User	User who ran the command
Source IP	Source IP
Host	Host where command was run
Statement	SQL statement

EXAMPLE



The screenshot shows a software interface titled "SLS Command History". The main area is a table with the following columns: #, Command, Method Name, User, Source IP, and Host. The table contains 6 rows of data, all of which show the command "atquery". The "Method Name" column includes entries like "Addamark.ExecuteSql", "Addamark.Auth", and "SysTableQuery". The "User" column shows "Administrator" and "Guest". The "Source IP" column shows "0.0.0.0" and the "Host" column shows "-". At the bottom of the table, there is a navigation bar with buttons for "1 to 250 of 3,402" and a page number selector from 1 to 10.

#	Command	Method Name	User	Source IP	Host
1	atquery	Addamark.ExecuteSql	Administrator	0.0.0.0	-
2	atquery	Addamark.Auth	Guest	0.0.0.0	-
3	atquery	SysTableQuery	Administrator	0.0.0.0	-
4	atquery	Addamark.ExecuteSql	Administrator	0.0.0.0	-
5	atquery	Addamark.Auth	Guest	0.0.0.0	-
6	atquery	SysTableQuery	Administrator	0.0.0.0	-

INTELLISchema View

- None

TABLES REFERENCED

- sensage_sls_syslogng

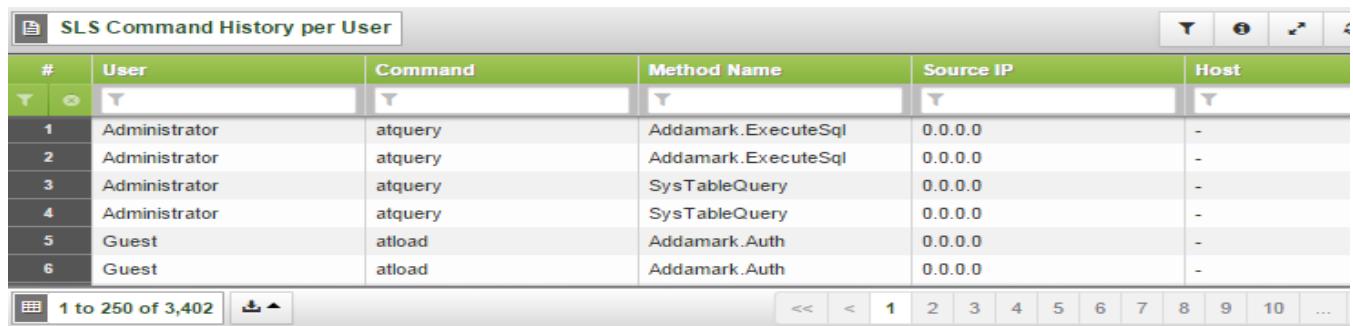
EDW (SLS) Command History per User

History of EDW (SLS) commands per user.

COLUMNS

Column	Description
User	User who ran the command
Command	EDW (SLS) command
Method Name	Name of the method
Source IP	Source IP
Host	Host where command was run

EXAMPLE



The screenshot shows a database table titled "SLS Command History per User". The table has columns: #, User, Command, Method Name, Source IP, and Host. The data shows several rows of command history, mostly from the "Administrator" user running "atquery" commands, with some entries from the "Guest" user running "atload" commands. The table includes standard navigation controls at the bottom.

#	User	Command	Method Name	Source IP	Host
1	Administrator	atquery	Addamark.ExecuteSql	0.0.0.0	-
2	Administrator	atquery	Addamark.ExecuteSql	0.0.0.0	-
3	Administrator	atquery	SysTableQuery	0.0.0.0	-
4	Administrator	atquery	SysTableQuery	0.0.0.0	-
5	Guest	atload	Addamark.Auth	0.0.0.0	-
6	Guest	atload	Addamark.Auth	0.0.0.0	-

INTELLISchema View

- None

TABLES REFERENCED

- sensage_sls_syslogng

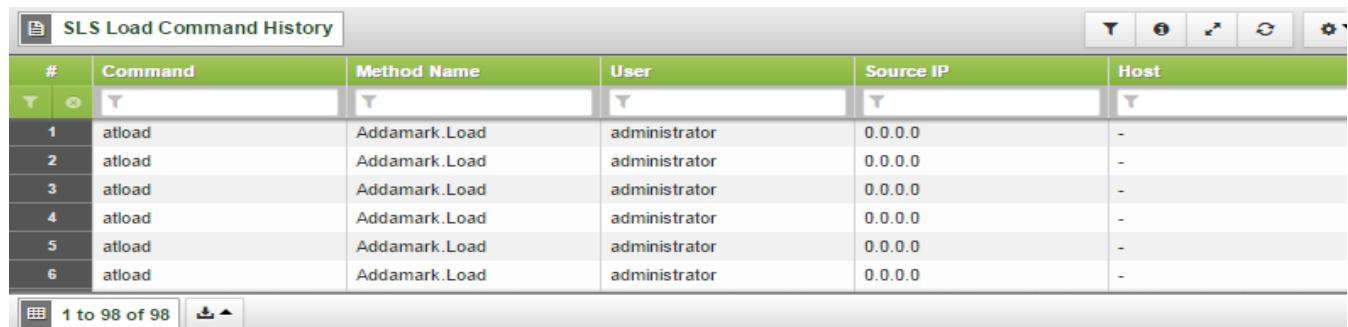
EDW (SLS) Load Command History

History of EDW (SLS) Load command.

COLUMNS

Column	Description
Command	EDW (SLS) command
Method Name	Name of the method
User	User who ran the command
Source IP	Source IP
Host	Host where command was run

EXAMPLE



The screenshot shows a table titled "SLS Load Command History". The table has columns: #, Command, Method Name, User, Source IP, and Host. All rows show the command "atload" and the method name "Addamark.Load". The user is listed as "administrator" and the source IP is "0.0.0.0" for all entries. The host column contains a single dash "-". The table includes standard database navigation buttons at the bottom left.

#	Command	Method Name	User	Source IP	Host
1	atload	Addamark.Load	administrator	0.0.0.0	-
2	atload	Addamark.Load	administrator	0.0.0.0	-
3	atload	Addamark.Load	administrator	0.0.0.0	-
4	atload	Addamark.Load	administrator	0.0.0.0	-
5	atload	Addamark.Load	administrator	0.0.0.0	-
6	atload	Addamark.Load	administrator	0.0.0.0	-

INTELLISchema View

- None

TABLES REFERENCED

- sensage_sls_syslogng

EDW (SLS) Percent Disk Space Usage

Percent of disk space used for each SLS node in SenSage AP deployment.

COLUMNS

Column	Description
SLS Node	Name of the SLS (EDW) Node
Used Percent	Percentage of disk space used

EXAMPLE

SLS Percent Disk Space Usage		
#	SLS Node	Used Percent
1	quant01-vm29.con2.hexiscyber.com	3.3750%
1 to 1 of 1		

INTELLISchema View

- None

TABLES REFERENCED

- cluster_properties

EDW (SLS) System Disk Space Usage Alerts

Displays status of SLS (EDW) disk space by SLS (EDW) node when free disk space is less than 40% of the total disk space.

COLUMNS

Column	Description
SLS Node	Name of the SLS (EDW) Node
Used Percent	Percentage of disk space used

EXAMPLE

SLS System Disk Space Usage Alerts			
#	SLS Node	Node Free Disk Space Percent	Status
1	quant01-vm29.con2.hexiscyber.com	96.624900	OK
1 to 1 of 1			

INTELLISchema VIEW

- None

TABLES REFERENCED

- cluster_properties

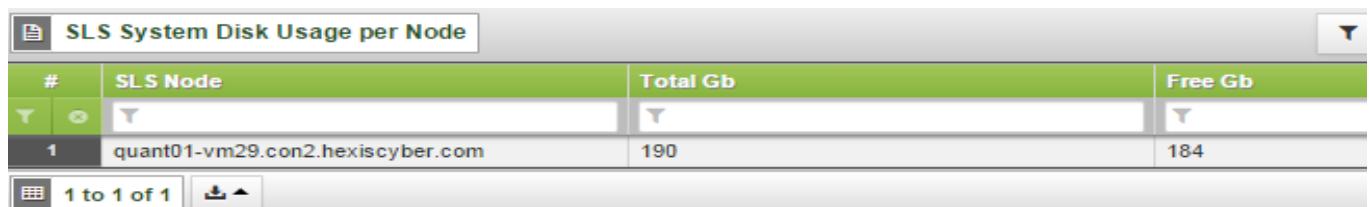
EDW (SLS) System Disk Space per Node

Total and free disk space used for each SLS (EDW) node in the SenSage AP deployment.

COLUMNS

Column	Description
SLS Node	Name of the SLS (EDW) Node
Total Gb	Total disk space in use (in gigabytes)
Free Gb	Total free disk space on disk (in gigabytes)

EXAMPLE



The screenshot shows a database grid with the following data:

#	SLS Node	Total Gb	Free Gb
1	quant01-vm29.con2.hexiscyber.com	190	184

At the bottom left, there is a status bar with the text "1 to 1 of 1".

INTELLISchema VIEW

- None

TABLES REFERENCED

- cluster_properties

COLLECTOR ACTIVITY MONITORING REPORTS

The Collector Activity Monitoring group of reports display volume of Collector activity and includes the following reports:

- “Collector Avg Load Size per Event Source”, next
- “Collector Collection Exceeds x Event per Day -- Exception Report”, on page 284
- “Collector Collection Exceeds x GB per Day -- Exception Report”, on page 285
- “Collector Daily Load - Trend”, on page 286
- “Collector Daily Load per Event Source”, on page 287
- “Collector Daily Load per loaderEnd Type”, on page 288
- “Collector EPS Statistics”, on page 289
- “Collector Load Volume per Day”, on page 290
- “Collector Table Sizes per Timerange”, on page 291
- “Collector Total Load Volume per Event Source”, on page 292
- “Collector Total Number of Records and Avg Record Size per Source”, on page 293
- “Collector Total Number of Records in System”, on page 294
- “Collector Total Records Loaded per Table”, on page 295
- “Collector Total Records Loaded per Table per Day”, on page 296
- “Collector Total Number of Records in System”, on page 297

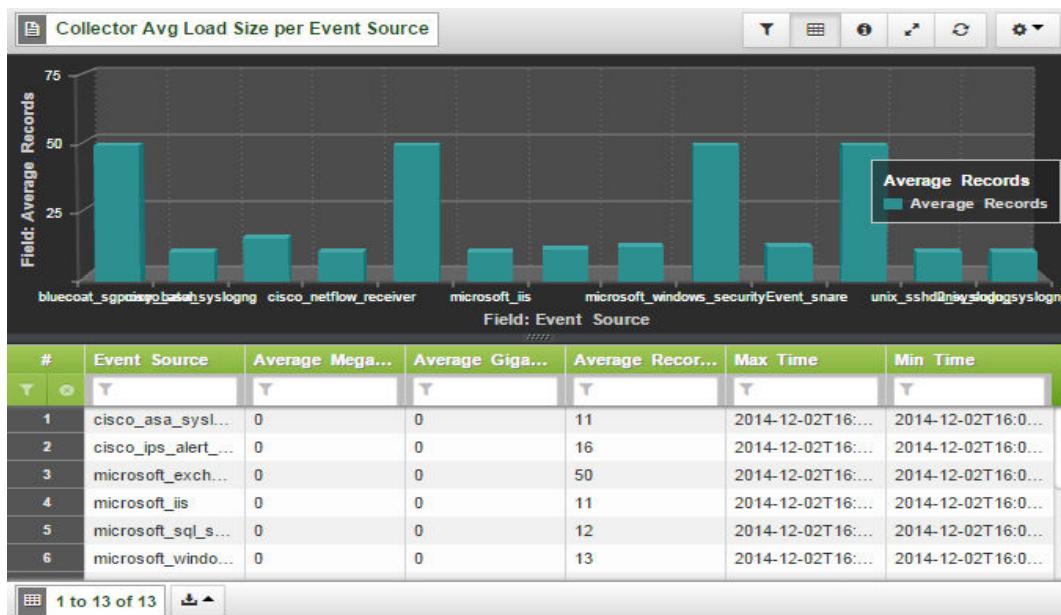
Collector Avg Load Size per Event Source

Average size of data loaded by the SenSage AP Collector for each event source.

COLUMNS

Column	Description
Event Source	Event-log source of loaded data
Average MegaBytes	Average size of loaded data in megabytes for load
Average GigaBytes	Average size of loaded data in gigabytes per load
Average Records	Average loaded record count for load
Max Time	Time of last load for each event source
Min Time	Time of first load for each event source

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- sensage_collectorTransaction_syslogng

Collector Collection Exceeds x Event per Day -- Exception Report

A summary of daily loads by the SenSage AP Collector with status of thresholds exceeds.

COLUMNS

Column	Description
Status	Status of threshold exceeds by daily loads
Day	Date in <i>yyyy-mm-dd</i> format
Records Loaded	Number of loaded records per day

EXAMPLE

#	Status	Day	Records Loaded
1	WARNING	2015-04-10	18149
2	WARNING	2015-04-11	1104
3	WARNING	2015-04-12	1104
4	WARNING	2015-04-13	1104
5	WARNING	2015-04-14	5603
6	WARNING	2015-04-15	1823

INTELLISchema View

- None

TABLES REFERENCED

- sensage_collectorTransaction_syslogng

Collector Collection Exceeds x GB per Day -- Exception Report

Daily size of loaded records by the SenSage AP Collector with status of thresholds exceeds.

COLUMNS

Column	Description
Status	Status of threshold exceeds by daily loads
Day	Date in <i>yyyy-mm-dd</i> format
GB	Size of loaded records in gigabytes

EXAMPLE

#	Status	Day	GB
1	WARNING	2015-06-30	0.026
2	WARNING	2015-07-01	0.001

1 to 2 of 2

INTELLISchema VIEW

- None

TABLES REFERENCED

- sensage_collectorTransaction_syslogng

Collector Daily Load - Trend

Size of data loaded by the SenSage AP Collector per day.

COLUMNS

Column	Description
Day	Date in <i>yyyy-mm-dd</i> format
Records Loaded	Number of records loaded per day
Bytes Copied	Copied bytes for each day

EXAMPLE

#	Day	Records Loaded	Bytes Copied
1	2015-04-10	18149	19830895
2	2015-04-11	1104	1698658
3	2015-04-12	1104	1698400

INTELLISchema VIEW

- None

TABLES REFERENCED

- sensage_collectorTransaction_syslogng

Collector Daily Load per Event Source

Volume of data loaded by the SenSage AP Collector for each event source.

COLUMNS

Column	Description
Day	Date in <i>yyyy-mm-dd</i> format
Event Source	Event-log source of loaded data
Records Loaded	Number of records loaded
Bytes Copied	Total volume of data copied by the Collector (bytes)

EXAMPLE

Collector Daily Load per Event Source				
	Day	Event Source	Records Loaded	Bytes Copied
1	2015-04-10	sensage_collectorTransaction_s...	39	69284
2	2015-04-10	sensage_sls_syslogng	18092	41586417
3	2015-04-10	unix_sshd2_syslogng	2	472
4	2015-04-10	unix_su_syslogng	16	3484
5	2015-04-11	sensage_collectorTransaction_s...	144	262080
6	2015-04-11	sensage_sls_syslogng	960	3340352

INTELLISchema View

- None

TABLES REFERENCED

- sensage_collectorTransaction_syslogng

Collector Daily Load per loaderEnd Type

Size of data loaded by the SenSage AP Collector per day for loaderEnd Type.

COLUMNS

Column	Description
Day	Date in <i>yyyy-mm-dd</i> format
Type	Event-log source of loaded data
Records Loaded	Number of records loaded
Bytes Copied	Total volume of data copied by the Collector (bytes)

EXAMPLE

#	Day	Type	Records Loaded	Bytes Copied
1	2015-04-10	loaderEnd	18149	19830895
2	2015-04-11	loaderEnd	1104	1698658
3	2015-04-12	loaderEnd	1104	1698400
4	2015-04-13	loaderEnd	1104	1698484
5	2015-04-14	loaderEnd	5603	13116748
6	2015-04-15	loaderEnd	1823	2293003

INTELLISchema View

- None

Tables Referenced

- sensage_collectorTransaction_syslogng

Collector EPS Statistics

EPS statistics of data loaded by the SenSage AP Collector.

COLUMNS

Column	Description
Time	Time the event occurred (yyyy-mm-dd hh:mm:ss)
Total Number of Events	Total number of events
Peak Number of Events	Maximum number of events
Average Number of Events	Average number of events

EXAMPLE



The screenshot shows a software interface titled "Collector EPS Statistics". It features a table with five columns: "#", "Time", "Total Number of Events", "Peak Number of Events", and "Average Number of Events". The table contains six rows of data. At the bottom, there is a navigation bar with a page number indicator "1 to 250 of 22,523" and a set of page navigation buttons.

#	Time	Total Number of Events	Peak Number of Events	Average Number of Events
1	2015/06/26 13:15:56	5	37	1
2	2015/06/26 13:17:01	20	37	1
3	2015/06/26 13:17:05	26	37	1
4	2015/06/26 13:17:09	27	37	1
5	2015/06/26 13:17:12	37	37	1
6	2015/06/26 13:17:16	26	37	1

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_analyzeraudit_syslogng
- sensage_applicationManagerAudit_syslogng
- sensage_collectorError_syslogng
- sensage_collectorTransaction_syslogng
- sensage_sls_syslogng

Collector Load Volume per Day

Average size of data loaded by the SenSage AP Collector for each event source.

COLUMNS

Column	Description
Day	Date in <i>yyyy-mm-dd</i> format
Records Loaded	Number of records loaded for each day
Bytes Loaded	Loaded bytes for each day
MegaBytes Loaded	Loaded megabytes for each day
GigaBytes Loaded	Loaded gigabytes for each day

EXAMPLE

The screenshot shows a database viewer interface with the title 'Collector Load Volume per Day'. The table has six columns: '#', 'Day', 'Records Loaded', 'Bytes Loaded', 'MegaBytes Loaded', and 'GigaBytes Loaded'. There are two rows of data: one for June 30, 2015, and one for July 1, 2015. The 'Day' column uses a date format of 'yyyy-mm-dd'. The 'Records Loaded' column shows values 36970 and 552 respectively. The 'Bytes Loaded' column shows values 57397082 and 1861812. The 'MegaBytes Loaded' column shows values 54.738 and 1.776. The 'GigaBytes Loaded' column shows values 0.053 and 0.002. Navigation buttons at the bottom indicate '1 to 2 of 2'.

#	Day	Records Loaded	Bytes Loaded	MegaBytes Loaded	GigaBytes Loaded
1	2015-06-30	36970	57397082	54.738	0.053
2	2015-07-01	552	1861812	1.776	0.002

INTELLISchema VIEW

- None

TABLES REFERENCED

- sensage_collectorTransaction_syslogng

Collector Table Sizes per Timerange

Total size of data loaded into a table by SenSage AP Collector for a given timerange.

COLUMNS

Column	Description
Table Name	The name of the table.
Total Bytes	Total size of the loaded data into the table by a specified timerange

EXAMPLE

#	Table Name	Total Bytes
1	bluecoat_sgproxy_batch	7531564
2	cisco_asa_syslogng	9263933
3	cisco_ios_syslogng	9563548
4	cisco_ips_alert_error	34687433
5	cisco_netflow_receiver	11107161
6	cisco_pix_syslogng	8328516

INTELLISchema View

- None

TABLES REFERENCED

- sensage_collectorTransaction_syslogng

Collector Total Load Volume per Event Source

Total number of records and average size of records loaded by the SenSage AP Collector for each event source.

COLUMNS

Column	Description
Day	Date (yyyy-mm-dd)
Event Source	Event log source
Records Loaded	Number of loaded records
Bytes Loaded	Size of loaded data in bytes
MegaBytes Loaded	Size of loaded data in megabytes
GigaBytes Loaded	Size of loaded data in gigabytes

EXAMPLE

#	Day	Event Source	Records Loaded	Bytes Loaded	MegaBytes Loaded	GigaBytes Loaded
1	2015-04-10	sensage_collectorTr...	39	69284	0.066	0.000
2	2015-04-10	sensage_sls_syslogng	18092	41586417	39.660	0.039
3	2015-04-10	unix_sshd2_syslogng	2	472	0.000	0.000
4	2015-04-10	unix_su_syslogng	16	3484	0.003	0.000
5	2015-04-11	sensage_collectorTr...	144	262080	0.250	0.000
6	2015-04-11	sensage_sls_syslogng	960	3340352	3.186	0.003

INTELLISchema VIEW

- None

TABLES REFERENCED

- sensage_collectorTransaction_syslogng

Collector Total Number of Records and Avg Record Size per Source

Total number of records and average size of records loaded by the SenSage AP Collector for each event source.

COLUMNS

Column	Description
Source Type	Event-log source type
Records Loaded	Total number of loaded records
Avg Record Size	Average size of loaded record

EXAMPLE

Collector Total Number of Records and Avg Record Size per Source			
#	Source Type	Records Loaded	Avg Record Size
1	_bluecoat_sgproxy_batch	50	4.803199999999993e+02
2	_cisco_asa_syslogng	11	1.750909090909093e+02
3	_cisco_ips_alert_error	16	6.795625000000000000e+02
4	_cisco_netflow_receiver	11	2.15454545454545467e+02
5	_microsoft_exchange_tracking_sensageRetri...	50	4.09360000000000014e+02
6	_microsoft_iis	11	3.70545454545454561e+02

1 to 35 of 35

INTELLISchema View

- None

TABLES REFERENCED

- sensage_collectorTransaction_syslogng

Collector Total Number of Records in System

Total number of records and size of records loaded by the SenSage AP Collector in the System.

COLUMNS

Column	Description
# of Records	Total number of loaded records into the System
Bytes Copied	Size of copied data in bytes

EXAMPLE

The screenshot shows a database viewer window titled "Collector Total Number of Records in System". The table has two columns: "# of Records" and "Bytes Copied". There is one row with data: "# of Records" is 37522 and "Bytes Copied" is 28341632. The bottom of the window shows navigation buttons: "1 to 1 of 1" and "1" (with up and down arrows).

#	# of Records	Bytes Copied
1	37522	28341632

INTELLISchema VIEW

- None

TABLES REFERENCED

- sensage_collectorTransaction_syslogng

Collector Total Records Loaded per Table

Total number of records and size of loaded data by the SenSage AP Collector for each table.

COLUMNS

Column	Description
Table	Name of the table
Records Loaded	Number of loaded records per table
Bytes Copied	Size of copied data in bytes per table

EXAMPLE



#	Table	Records Loaded	Bytes Copied
1	bluecoat_sgproxy_batch	47	21608
2	cisco_asa_syslogng	815	143539
3	cisco_ios_syslogng	815	149804
4	cisco_ips_alert_error	815	532098
5	cisco_netflow_receiver	815	174731
6	cisco_pix_syslogng	815	129845

INTELLISchema VIEW

- None

TABLES REFERENCED

- sensage_collectorTransaction_syslogng

Collector Total Records Loaded per Table per Day

Total number of records and size of loaded data by the SenSage AP Collector for each table per day.

COLUMNS

Column	Description
Day	Date (yyyy-mm-dd)
Table	Name of the table
Records Loaded	Number of loaded records per table
Bytes Copied	Size of copied data in bytes per table

EXAMPLE

Collector Total Records Loaded per Table per Day				
#	Day	Table	Records Loaded	Bytes Copied
1	2015-06-30	bluecoat_sgproxy_batch	47	21608
2	2015-06-30	cisco_asa_syslogng	815	143539
3	2015-06-30	cisco_ios_syslogng	815	149804
4	2015-06-30	cisco_ips_alert_error	815	532098
5	2015-06-30	cisco_netflow_receiver	815	174731
6	2015-06-30	cisco_pix_syslogng	815	129845

INTELLISchema View

- None

TABLES REFERENCED

- sensage_collectorTransaction_syslogng

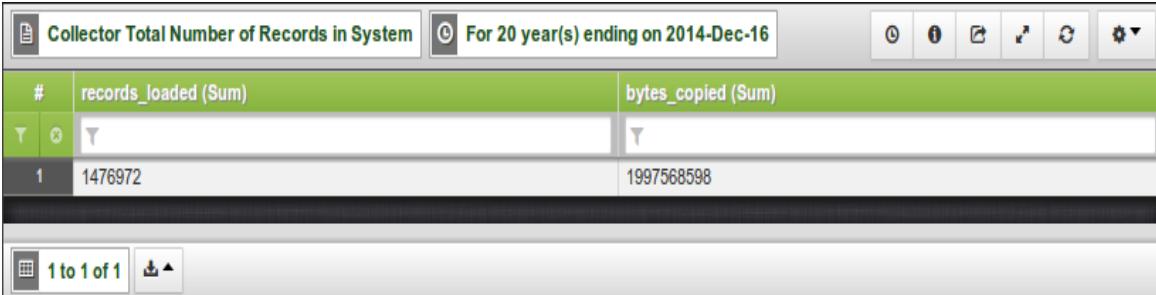
Collector Total Number of Records in System

Total number of records and size of loaded data in a time range by the SenSage AP Collector

COLUMNS

Column	Description
records_loaded (Sum)	Number of records loaded.
bytes_copied (Sum)	Number of bytes_copied.

EXAMPLE



The screenshot shows a database query results window. The title bar says "Collector Total Number of Records in System". The filter bar says "For 20 year(s) ending on 2014-Dec-16". The results table has two columns: "#", "records_loaded (Sum)", and "bytes_copied (Sum)". There is one row with value 1 in the "#" column, 1476972 in the "records_loaded (Sum)" column, and 1997568598 in the "bytes_copied (Sum)" column. At the bottom left, it says "1 to 1 of 1".

#	records_loaded (Sum)	bytes_copied (Sum)
1	1476972	1997568598

INTELLISchema View

- None

TABLE REFERENCED

- None

INTERNAL SYSTEMS REPORTS

The SenSage AP Internal Systems reports displays internal system events and includes the following reports:

- “Internal System Failed Login Details”, next
- “Internal System Report Activity Details”, on page 300
- “Internal System Report Activity Summary”, on page 301
- “Internal System Successful Admin Login to System”, on page 302
- “Internal System Successful Login Details”, on page 303
- “Internal System Successful Summary Login to System”, on page 304
- “Internal System User Activity Details”, on page 305
- “Internal System User Activity Summary”, on page 306
- “Internal System User Password Change”, on page 307

Internal System Failed Login Details

Details of failed logins to SenSage AP deployment.

COLUMNS

Column	Description
Time	Time the failed login occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Account	User account for which the login failed
Source IP	IP address of host from which the failed login occurred
Error Code	Error message code
Error Message	Text of error message

EXAMPLE

Internal System Failed Login Details					
#	Time	Account	Source IP	Error Message	Error Code
1	2014-Aug-19 13:00:59 GMT	administrator	172.16.103.70	Login denied for user: administrator	1010
2	2014-Aug-19 13:27:30 GMT	administrator	172.16.103.70	Login denied for user: administrator	1010
3	2014-Aug-19 13:36:49 GMT	administrator	172.16.103.70	Login denied for user: administrator	1010
4	2014-Aug-19 13:45:10 GMT	administrator	172.16.103.70	Login denied for user: administrator	1010
5	2014-Aug-19 13:48:55 GMT	administrator	172.16.103.70	Login denied for user: administrator	1010
6	2014-Aug-19 13:56:07 GMT	administrator	172.16.103.70	Login denied for user: administrator	1010

INTELLISchema View

- None

TABLES REFERENCED

- sensage_applicationManager_sftp
- sensage_applicationManagerAudit_syslogng

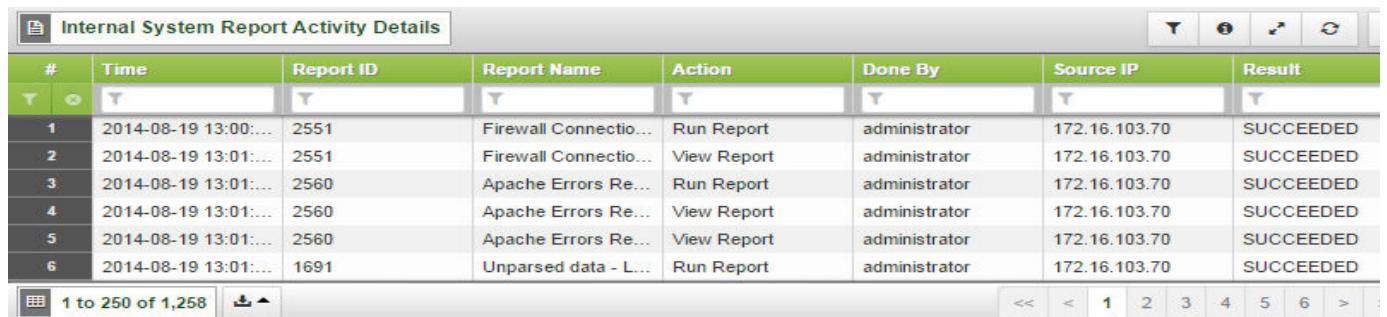
Internal System Report Activity Details

Details of activities involving a SenSage AP report, by user. Activities include: creating a report, editing a report, running a report, and viewing a report.

COLUMNS

Column	Description
Time	Time the event occurred (yyy-mm-dd hh:mm:ss)
Report ID	A unique, internal identifier assigned to each report by the SenSage AP system. Because a report can be re-named, this internal ID tracks activity on the report, regardless of name changes.
Report Name	Name of report viewed
Action	Action performed on the report. Possible values: <ul style="list-style-type: none"> • Create Report • Edit Report • Run Report • View Report • Delete Report
Done By	User who accessed the report
Source IP	IP address of the machine from which the report activity occurred
Result	Result of the Report Access. Possible values: <ul style="list-style-type: none"> • SUCCEEDED • FAILED

EXAMPLE



#	Time	Report ID	Report Name	Action	Done By	Source IP	Result
1	2014-08-19 13:00:00	2551	Firewall Connectio...	Run Report	administrator	172.16.103.70	SUCCEEDED
2	2014-08-19 13:01:00	2551	Firewall Connectio...	View Report	administrator	172.16.103.70	SUCCEEDED
3	2014-08-19 13:01:00	2560	Apache Errors Re...	Run Report	administrator	172.16.103.70	SUCCEEDED
4	2014-08-19 13:01:00	2560	Apache Errors Re...	View Report	administrator	172.16.103.70	SUCCEEDED
5	2014-08-19 13:01:00	2560	Apache Errors Re...	View Report	administrator	172.16.103.70	SUCCEEDED
6	2014-08-19 13:01:00	1691	Unparsed data - L...	Run Report	administrator	172.16.103.70	SUCCEEDED

INTELLISchema View

- None

TABLES REFERENCED

- sensage_applicationManager_sftp
- sensage_applicationManagerAudit_syslogng

Internal System Report Activity Summary

Summary of report activity in a SenSage AP deployment. Includes the number of times a report was edited or run and the time the report was last edited or run.

COLUMNS

Column	Description
Report ID	A unique, internal identifier assigned to each report by the SenSage AP system. Because a report can be re-named, this internal ID tracks activity on the report, regardless of name changes.
Report Name	Name of the report
Last Edited	Date and time the report was last edited
Last Run	Date and time the report was last run
Number of Edits	Number of times the report was edited
Number of Runs	Number of times the report was run

EXAMPLE

Internal System Report Activity Summary						
	Report ID	Report Name	Last Edited	Last Run	Number of Edits	Number of Runs
116	Windows Loss of Audi...	Never	2014-Aug-19 13:37:24	-	-	1
12	McAfee ePO Console ...	Never	2014-Aug-19 13:29:45	-	-	1
122	Windows Login Succe...	Never	2014-Aug-19 13:43:37	-	-	1
1244	Microsoft SharePoint -...	Never	2014-Aug-19 13:33:00	-	-	1
1257	Juniper Netscreen Fir...	Never	2014-Aug-19 13:28:03	-	-	1
1263	Juniper Netscreen Fir...	Never	2014-Aug-19 13:54:44	-	-	2

1 to 248 of 248

INTELLISchema View

- None

TABLES REFERENCED

- sensage_applicationManager_sftp
- sensage_applicationManagerAudit_syslogng

Internal System Successful Admin Login to System

Number of successful admin logins to the SenSage AP system.

COLUMNS

Column	Description
Total Root Logins	Number of successful admin logins to the SenSage AP system.

EXAMPLE

Internal System Successful Admin Login to System	
#	Total Root Logins
1	2
1 to 1 of 1	

INTELLISchema VIEW

- None

TABLES REFERENCED

- sensage_applicationManager_sftp
- sensage_applicationManagerAudit_syslogng

Internal System Successful Login Details

Number of successful admin logins to the SenSage AP system.

COLUMNS

Column	Description
Time	Time the login occurred (yyyy-mm-dd hh:mm:ss)
Account	User account used for the login
Source IP	IP address of host from which the login occurred

EXAMPLE

#	Time	Account	Source IP
1	2014-Aug-19 13:45:57 GMT	administrator	172.16.103.70
2	2014-Aug-19 13:53:12 GMT	administrator	172.16.103.70
3	2014-Aug-19 13:45:57 GMT	administrator	172.16.103.70
4	2014-Aug-19 13:53:12 GMT	administrator	172.16.103.70

INTELLISchema VIEW

- None

TABLES REFERENCED

- sensage_applicationManager_sftp
- sensage_applicationManagerAudit_syslogng

Internal System Successful Summary Login to System

Summary of successful logins to the SenSage AP system.

COLUMNS

Column	Description
Account	User account used for the login
Total Logins	Number of successful logins to the SenSage AP system.

EXAMPLE

#	Account	Total Logins
1	administrator	4

INTELLISchema VIEW

- None

TABLES REFERENCED

- sensage_applicationManager_sftp
- sensage_collectorTransaction_syslogng

Internal System User Activity Details

Details of user activities in a SenSage AP deployment.

COLUMNS

Column	Description
Time	Time the activity occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
Source IP	IP address from which the user logged in
Action	Activity performed by the user. Possible values: <ul style="list-style-type: none"> • Create Dashboard • Edit Dashboard • Delete Dashboard • Create Report • Edit Report • Delete Report • View Report • Run Report • Create Library • Update Library • Delete Library • Authentication
Object Accessed	Name of SenSage AP object accessed.
Result	Result of activity. Possible values: <ul style="list-style-type: none"> • SUCCEEDED • FAILED

EXAMPLE

Internal System User Activity Details						
#	Time	Account	Source IP	Action	Object Accessed	Result
1	2014-Aug-19 13:00:42 ...	administrator	172.16.103.70	Run Report	Firewall Connections D...	SUCCEEDED
2	2014-Aug-19 13:01:00 ...	administrator	172.16.103.70	View Report	Firewall Connections D...	SUCCEEDED
3	2014-Aug-19 13:01:05 ...	administrator	172.16.103.70	Run Report	Apache Errors Report	SUCCEEDED
4	2014-Aug-19 13:01:07 ...	administrator	172.16.103.70	View Report	Apache Errors Report	SUCCEEDED
5	2014-Aug-19 13:01:07 ...	administrator	172.16.103.70	View Report	Apache Errors Report	SUCCEEDED

INTELLISchema VIEW

- None

TABLES REFERENCED

- sensage_applicationManager_sftp
- sensage_applicationManagerAudit_syslogng

Internal System User Activity Summary

Summary of user activities in a SenSage AP deployment.

COLUMNS

Column	Description
Account	User account used to perform the activity
Source IP	IP address from which the user logged in
Action	Activity performed by the user. Possible values: <ul style="list-style-type: none">• Create Dashboard• Edit Dashboard• Delete Dashboard• Create Report• Edit Report• Delete Report• View Report• Run Report• Create Library• Update Library• Delete Library• Authentication
Object Accessed	Name of SenSage AP object accessed.
Result	Result of activity. Possible values: <ul style="list-style-type: none">• SUCCEEDED• FAILED
Count	Number of activities

EXAMPLE

#	Account	Source IP	Action	Result	Count
1	administrator	172.16.103.70	Authentication	SUCCEEDED	2
2	administrator	172.16.103.70	Run Report	SUCCEEDED	286
3	administrator	172.16.103.70	View Report	SUCCEEDED	972

INTELLISchema VIEW

- None

TABLES REFERENCED

- sensage_applicationManager_sftp
- sensage_applicationManagerAudit_syslogng

Internal System User Password Change

Password changes to a SenSage AP deployment.

COLUMNS

Column	Description
Time	Time the activity occurred (<i>yyyy-mm-dd hh:mm:ss</i>)
User	User account used to generate the password change
Source IP Address	IP address of the user
Result	Result of activity. Possible values: • SUCCEEDED • FAILED

EXAMPLE

#	Time	User	Source IP Address	Result
1	2014-Aug-19 13:00:42 GMT	administrator	172.16.103.70	SUCCEEDED
2	2014-Aug-19 13:00:42 GMT	administrator	172.16.103.70	SUCCEEDED
3	2014-Aug-19 13:00:44 GMT	administrator	172.16.103.70	SUCCEEDED
4	2014-Aug-19 13:00:46 GMT	administrator	172.16.103.70	SUCCEEDED
5	2014-Aug-19 13:00:48 GMT	administrator	172.16.103.70	SUCCEEDED
6	2014-Aug-19 13:00:50 GMT	administrator	172.16.103.70	SUCCEEDED

INTELLISchema View

- None

TABLES REFERENCED

- sensage_applicationManager_sftp
- sensage_applicationManagerAudit_syslogng

CHAPTER 11

McAfee Analytics Reports

The McAfee Reports include the following groups of reports:

- “Email and Web Security (EWS)”, next
- “Database Activity Monitoring”, on page 312
- “ePolicy Orchestrator (ePO)”, on page 331
- “Network Security Platform (IntruShield)”, on page 337
- “Vulnerability Manager (Foundstone)”, on page 346

EMAIL AND WEB SECURITY (EWS)

The McAfee Email and Web Security (EWS) report group includes the following reports:

- “McAfee EWS Virus Email Details”, on page 309
- “McAfee EWS Virus Web Details”, on page 310
- “McAfee EWS Virus Web Summary”, on page 311

McAfee EWS Virus Email Details

Viruses detected in email.

COLUMNS

Columns	Description
source_ip	IP address where the email originated
Virus Name	Name of the virus
Message ID	Message ID
Infected File	Name of file infected with the virus

EXAMPLE

The screenshot shows a software interface titled "McAfee EWS Virus Email Details". At the top, there is a toolbar with various icons. Below the toolbar is a table with five columns: "#", "source_ip", "Virus Name", "Message ID", and "Infected File". The table contains 8 rows of data. The first row has the number "1" and the IP "192.168.0.152". The "Virus Name" column shows "Obfuscated JScript (com...)" repeated for all rows. The "Message ID" column shows unique identifiers for each row. The "Infected File" column shows file names like "NewCar_adplib.js", "pt.js", "index.php", etc. At the bottom of the table, there is a pagination control showing "1 to 250 of 1,954" and a set of navigation arrows.

#	source_ip	Virus Name	Message ID	Infected File
1	192.168.0.152	Obfuscated JScript (com...)	2cb8_a670a896_b804_1...	NewCar_adplib.js
2	192.168.0.150	Obfuscated JScript (com...)	07b2_470c28fa_b816_11...	pt.js
3	192.168.0.150	Obfuscated JScript (com...)	678e_e7009532_b819_1...	pt.js
4	192.168.0.151	Obfuscated JScript (com...)	6578_0e61708a_b822_1...	pt.js
5	192.168.0.150	Obfuscated JScript (com...)	65ad_d9c8726e_b831_1...	index.php
6	192.168.0.150	Obfuscated JScript (com...)	65ad_d9c8726e_b831_1...	index.php
7	192.168.0.150	Obfuscated JScript (com...)	65dc_99ac1f4e_b856_11...	index.php
8	192.168.0.150	Obfuscated JScript (com...)	6869_1738e2c8_b87d_1...	pt.js

INTELLISchema View

- None

TABLES REFERENCED

- mcAfee_scm_batch

McAfee EWS Virus Web Details

Viruses detected in Web pages.

COLUMNS

Columns	Description
Virus Name	Name of the virus
Domain	Domain of Web URL
URL	Web URL

EXAMPLE

The screenshot shows a software interface titled "McAfee EWS Virus Web Details". The main area is a table with columns: #, source_ip, Virus Name, Domain, and URL. The table contains 8 rows of data. The footer of the interface shows the URL "quant01-vm25.con2.hexiscyber.com:8090/analyzer/#".

#	source_ip	Virus Name	Domain	URL
1	192.168.0.152	ASpack (compressed file...)	uniextract.example.com	http://uniextract.example....
2	192.168.0.152	Obfuscated JScript (com...)	www.example.com	http://www.example.com/j...
3	192.168.0.152	JS/Exploit-SWFSpoofer (tro...)	example.com	http://example.com/home/i...
4	192.168.0.152	UPX (compressed file)	ftp.example.com	ftp://ftp.example.com/pub/...
5	192.168.0.152	UPX (compressed file)	ftp.example.com	ftp://ftp.example.com/pub/...
6	192.168.0.151	EICAR test file (test NOT ...)	www.example.org	http://www.example.org/d...
7	192.168.0.150	Obfuscated JScript (com...)	www.example.co.uk	http://www.example.co.uk...
8	192.168.0.150	New Script (virus)	www.example.org	http://www.example.org/s...

INTELLISchema View

- None

TABLES REFERENCED

- mcAfee_scm_batch

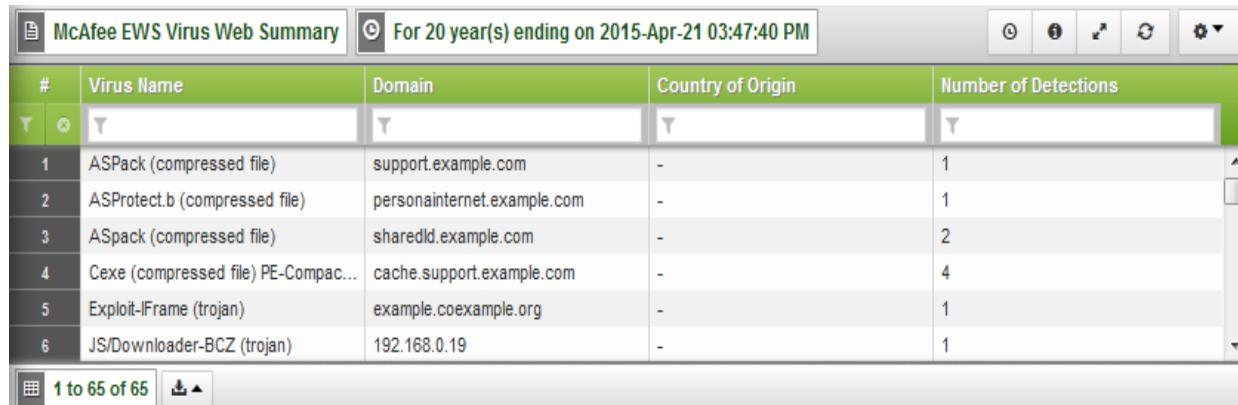
McAfee EWS Virus Web Summary

Summary of viruses detected in Web pages whose domain is located outside of the United States.

COLUMNS

Columns	Description
Virus Name	Name of the virus
Domain	Domain of Web URL
Country of Origin	Country where the Web URL is located. Displayed as a two-character code using ISO 3166-1-alpha-2 code elements. See English country names and code elements for a complete list.
Number of Detections	Number of times the virus was detected

EXAMPLE



The screenshot shows a software interface titled "McAfee EWS Virus Web Summary". At the top, it says "For 20 year(s) ending on 2015-Apr-21 03:47:40 PM". Below is a table with the following data:

#	Virus Name	Domain	Country of Origin	Number of Detections
1	ASPack (compressed file)	support.example.com	-	1
2	ASProtect.b (compressed file)	personalinternet.example.com	-	1
3	ASpack (compressed file)	sharedId.example.com	-	2
4	Cexe (compressed file) PE-Compac...	cache.support.example.com	-	4
5	Exploit-IFrame (trojan)	example.coexample.org	-	1
6	JS/Downloader-BCZ (trojan)	192.168.0.19	-	1

At the bottom left, it says "1 to 65 of 65".

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_scm_batch

DATABASE ACTIVITY MONITORING

The McAfee Database Activity Monitoring report group includes the following reports:

- “[McAfee - Detail Last 100 Records](#)”, on page 313
- “[McAfee - Detail Top 100 Records](#)”, on page 315
- “[McAfee - Investigation Most Active Agent Host](#)”, on page 317
- “[McAfee - Investigation Most Active Agent IP](#)”, on page 317
- “[McAfee - Investigation Most Active Database Version](#)”, on page 320
- “[McAfee - Investigation Most Active Exec User](#)”, on page 321
- “[McAfee - Investigation Most Active Module](#)”, on page 321
- “[McAfee - Investigation Most Active OS User](#)”, on page 322
- “[McAfee - Investigation Most Active Program](#)”, on page 323
- “[McAfee - Investigation Most Active Reporter Host](#)”, on page 323
- “[McAfee - Investigation Most Active Rule Name](#)”, on page 324
- “[McAfee - Investigation Most Active Source Host](#)”, on page 325
- “[McAfee - Investigation Most Active Source IP](#)”, on page 325
- “[McAfee - Investigation Wizard](#)”, on page 326
- “[McAfee - Statistics Command Type Access by Database Type, Name](#)”, on page 328
- “[McAfee - Statistics Database Name Access by Database Type](#)”, on page 329
- “[McAfee - Statistics Command Type Access by Database Type, Name](#)”, on page 330

McAfee - Detail Last 100 Records

This report displays the database activity detail of the last 100 records.

COLUMNS

Columns	Description
ts	Date and time on which the activity occurred
adapter_ver	Version of Log Adapter
app_name	Product Name of the source application
app_vendor	Vendor name of the source application
timezone	Timezone
facility	Facility name
priority	Priority
rptr_host	Reporter host name
rptr_app	Reporter app name
mcafee_tx	McAfee timestamp
alert_id	Alert ID
exec_time	Execution time in millis format
session_id	Session ID
agent_ip	IP address of the monitoring agent
agent_host	Host name address of the monitoring agent
rule_name	The name of the rule
exec_user	Exec user
os_user	OS user
program	Executing program
logon_time	Session logon time
db_type	Database Type (ORACLE, MSSQL, MSSQL2000, SYBASE, DB2, MYSQL)
db_name	Database Name
cmd_type	The SQL command type; for example, SELECT
accessed_obj	List of accessed objects pipe delimited
statement	SQL statement
src_host	Source host
src_ip	Source IP
end_user_name	End user name
end_user_action	End user action
end_user_ip	End user IP
end_user_module	End user module
inflow_obj_name	Inflow accessed objects pipe delimited

Columns	Description
inflow_statement	Inflow SQL statement
action	Action
client_id	Client_id
client_info	Client_info
module	Module
serial	Serial
ms_context	MS SQL context info field
db_ver	Version of the database
terminal	Terminal
severity	Serveyrity of the alert
audit_parse_success	Flag that indicates that source log line was parsed successfully (if 1) and failed (if not 0 or -1)d
unparsed_message	Raw log record

EXAMPLE

McAfee Database Activity Monitoring - Detail Last 100 Records										
#	ts	adapter_ver	app_name	app_vendor	app_version	timezone	facility	priority	rptr_host	
1	2011-Nov-23 06:56:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1	
2	2011-Nov-23 03:11:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1	
3	2011-Nov-23 02:21:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1	
4	2011-Nov-23 01:21:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1	
5	2011-Nov-23 01:11:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1	
6	2011-Nov-23 01:11:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1	
7	2011-Nov-23 01:11:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1	
8	2011-Nov-23 01:11:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1	

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Detail Top 100 Records

This report displays the first 100 events from McAfee Database Activity Monitoring log.

COLUMNS

Columns	Description
ts	Date and time on which the activity occurred
adapter_ver	Version of Log Adapter
app_name	Product Name of the source application
app_vendor	Vendor name of the source application
timezone	Timezone
facility	Facility name
priority	Priority
rptr_host	Reporter host name
rptr_app	Reporter app name
mcafee_tx	McAfee timestamp
alert_id	Alert ID
exec_time	Execution time in millis format
session_id	Session ID
agent_ip	IP address of the monitoring agent
agent_host	Host name address of the monitoring agent
rule_name	The name of the rule
exec_user	Exec user
os_user	OS user
program	Executing program
logon_time	Session logon time
db_type	Database Type (ORACLE, MSSQL, MSSQL2000, SYBASE, DB2, MYSQL)
db_name	Database Name
cmd_type	The SQL command type; for example, SELECT
accessed_obj	List of accessed objects pipe delimited
statement	SQL statement
src_host	Source host
src_ip	Source IP
end_user_name	End user name
end_user_action	End user action
end_user_ip	End user IP
end_user_module	End user module
inflow_obj_name	Inflow accessed objects pipe delimited

Columns	Description
inflow_statement	Inflow SQL statement
action	Action
client_id	Client_id
client_info	Client_info
module	Module
serial	Serial
ms_context	MS SQL context info field
db_ver	Version of the database
terminal	Terminal
severity	Serveyrity of the alert
audit_parse_success	Flag that indicates that source log line was parsed successfully (if 1) and failed (if not 0 or -1)d
unparsed_message	Raw log record

EXAMPLE

McAfee Database Activity Monitoring - Detail Top 100 Records									
#	ts	adapter_ver	app_name	app_vendor	app_version	timezone	facility	priority	rptr_host
1	2011-Nov-23 01:11:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1
2	2011-Nov-23 01:11:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1
3	2011-Nov-23 01:11:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1
4	2011-Nov-23 01:11:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1
5	2011-Nov-23 01:21:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1
6	2011-Nov-23 02:21:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1
7	2011-Nov-23 03:11:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1
8	2011-Nov-23 06:56:13 PM	1.0	Database A...	mcafee	4.2	GMT	user	debug	hostname-1

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Agent Host

This report displays the most active agent hosts.

COLUMNS

Columns	Description
Source IP	Host name address of the monitoring agent
Total Database Events	Number of logs

EXAMPLE

McAfee Database Activity Monitoring - Investigation Most Active Agent Host		For 20 year(s) ending on 2015-Jan-29
#	Source IP	Total Database Events
1	hhh5000d-bkup	4
1 to 1 of 1		

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Agent IP

This report displays the most active agent IPs..

COLUMNS

Columns	Description
Agent IP	IP address of the monitoring agent
Total Database Events	Count number for that IP address

EXAMPLE

McAfee Database Activity Monitoring - Investigation Most Active Agent IP		For 20 year(s) ending on 2015-Apr-20 08:33:31 PM
#	Agent IP	Total Database Events
1	111.222.33.111	2
1 to 1 of 1		

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Command Type

This report displays the most active command types.

COLUMNS

Columns	Description
Command Type	Database command type
Total Command Type Events	Total number of command type events

EXAMPLE

The screenshot shows a report titled "McAfee Database Activity Monitoring - Investigation Most Active Command Type". The report lists three command types: New Session, End Session, and SELECT, along with their respective event counts. The interface includes standard reporting tools like filters, sort options, and navigation buttons.

#	Command Type	Total Command Type Events
1	New Session	3
2	End Session	3
3	SELECT	2

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Database Name

This report displays the most active database names.

COLUMNS

Columns	Description
Database Name	Database Name
Total Database Events	The total number of events for the database

EXAMPLE

McAfee Database Activity Monitoring - Investigation Most Active Database Name		For 20 year(s) ending on 2015-Jan-18
#	Database Name	Total Database Events
1	x2dba5a1	2
1 to 1 of 1		

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Database Type

This report displays the most active database types.

COLUMNS

Columns	Description
Database Type	Database Type (for example, ORACLE, MSSQL, MYSQL, etc.)
Total Database Events	Total activity for the Database Type

EXAMPLE

McAfee Database Activity Monitoring - Investigation Most Active Database Type		For 20 year(s) ending on 2015-Jan-18
#	Database Type	Total Database Events
1	ORACLE	2
1 to 1 of 1		

INTELLISchema View

- None

Tables Referenced

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Database Version

This report displays the most active database versions.

Columns

Columns	Description
Database Version	Version of the database
Total Database Events	Number of logs

Example

#	Database Version	Total Database Events
1	11.2.0.2.0	4

INTELLISchema View

- None

Tables Referenced

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Exec User

This report displays the most active exec user.

COLUMNS

Columns	Description
Exec User	Exec user
Total User Activity	Total activity for the Exec user

EXAMPLE

McAfee Database Activity Monitoring - Investigation Most Active Exec User		For 20 year(s) ending on 2015-Jan-18
#	Exec User	Total User Activity
1	OPS\$PATROL	2
1 to 1 of 1		

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Module

This report displays the most active modules

COLUMNS

Columns	Description
Source IP	Source IP
Total Database Events	The total number of events for the source IP

EXAMPLE

McAfee Database Activity Monitoring - Investigation Most Active Module		For 20 year(s) ending on 2015-Jan-18
#	Source IP	Total Database Events
1	SQL*Plus	2
1 to 1 of 1		

INTELLISchema View

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active OS User

This report displays the most active OS users.

COLUMNS

Columns	Description
OS User	OS user
Total User Activity	Total activity for the OS user

EXAMPLE

McAfee Database Activity Monitoring - Investigation Most Active OS User		For 20 year(s) ending on 2015-Jan-18
#	OS User	Total User Activity
1	patrol	2
1 to 1 of 1		▼

INTELLISchema View

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Program

This report displays the most active programs.

COLUMNS

Columns	Description
Program	Executing program
Total Program Events	The total number of events for the program

EXAMPLE

McAfee Database Activity Monitoring - Investigation Most Active Program		For 20 year(s) ending on 2015-Jan-18
#	Program	Total Program Events
1	sqlplus@hhh5000d (TNS V1-V3)	2
1 to 1 of 1		▲ ▾

INTELLISchema View

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Reporter Host

This report displays the most active reporter hosts

COLUMNS

Columns	Description
Source IP	Reporter host name
Total Database Events	The total number of events for the rule.

EXAMPLE

McAfee Database Activity Monitoring - Investigation Most Active Reporter Host		For 20 year(s) ending on 2015-Jan-18
#	Source IP	Total Database Events
1	hostname-123.dddd.example.com	2
1 to 1 of 1		▲ ▾

INTELLISchema View

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Rule Name

This report displays the most active rule names.

COLUMNS

Columns	Description
Rule Name	The name of the rule
Total Rule Events	The total number of events for the rule.

EXAMPLE

McAfee Database Activity Monitoring - Investigation Most Active Rule Name		For 20 year(s) ending on 2015-Jan-18
#	Rule Name	Total Rule Events
1	test	2
1 to 1 of 1		▼ ▲

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Source Host

This report displays the most active source hosts.

COLUMNS

Columns	Description
Source Host	Source host
Total Database Events	Total number number of database events for the Source Host

EXAMPLE

McAfee Database Activity Monitoring - Investigation Most Active Source Host		For 20 year(s) ending on 2015-Jan-18
#	Source Host	Total Database Events
1	hhh5000d	2
1 to 1 of 1		▲ ▼

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Most Active Source IP

This report displays the most active source IPs.

COLUMNS

Columns	Description
Source IP	Source IP
Total Database Events	Total number number of database events for the Source IP

EXAMPLE

McAfee Database Activity Monitoring - Investigation Most Active Source IP		For 20 year(s) ending on 2015-Jan-18
#	Source IP	Total Database Events
1	111.222.11.111	2
1 to 1 of 1		▲ ▼

INTELLISchema View

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Investigation Wizard

This report displays the McAfee Database Activity Monitoring logs filtered by date.

COLUMNS

Columns	Description
tx	Date and time on which the activity occurred
rptr_host	Reporter host name
agent_host	Host name address of the monitoring agent
agent_ip	IP address of the monitoring agent
db_name	Database Name
db_type	Database Type (ORACLE, MSSQL, MSSQL2000, SYBASE, DB2, MYSQL)
src_host	Source host
src_ip	Source IP
alert_id	Alert ID
db_ver	Version of the database
module	The name of the module
rule_name	The name of the rule
severity	Severity of the alert
exec_time	Execution time in millis format
exec_user	Exec user
session_id	Session ID
logon_time	Session logon time
os_user	OS user
program	Executing program
accessed_obj	List of accessed objects pipe delimited
cmd_type	The SQL command type, for example, SELECT
statement	SQL statement

EXAMPLE


The screenshot shows a software interface titled "McAfee Database Activity Monitoring - Investigation Wizard". The main area is a table with the following columns: #, ts, rptr_host, agent_host, agent_ip, db_name, db_type, src_host, src_ip, and alert_id. The table contains 8 rows of data, each representing a database activity log entry. The data is as follows:

#	ts	rptr_host	agent_host	agent_ip	db_name	db_type	src_host	src_ip	alert_id
1	2011-Nov-23 06:56:13 PM	hostname-1...	hhh5000d-b...	111.222.33....	x2dba5a1	ORACLE	hhh5000d	111.222.11....	0
2	2011-Nov-23 03:11:13 PM	hostname-1...	hhh5000d-b...	111.222.33....	x2dba5a1	ORACLE	hhh5000d	111.222.11....	0
3	2011-Nov-23 02:21:13 PM	hostname-1...	hhh5000d-b...	111.222.33....	x2dba5a1	ORACLE	hhh5000d	111.222.11....	0
4	2011-Nov-23 01:21:13 PM	hostname-1...	hhh5000d-b...	111.222.33....	x2dba5a1	ORACLE	hhh5000d	111.222.11....	0
5	2011-Nov-23 01:11:13 PM	hostname-1...	hhh5000d-b...	111.222.33....	x2dba5a1	ORACLE	hhh5000d	111.222.11....	0
6	2011-Nov-23 01:11:13 PM	hostname-1...	hhh5000d-b...	111.222.33....	x2dba5a1	ORACLE	hhh5000d	111.222.11....	0
7	2011-Nov-23 01:11:13 PM	hostname-1...	hhh5000d-b...	111.222.33....	x2dba5a1	ORACLE	hhh5000d	111.222.11....	0
8	2011-Nov-23 01:11:13 PM	hostname-1...	hhh5000d-b...	111.222.33....	x2dba5a1	ORACLE	hhh5000d	111.222.11....	0

At the bottom left of the table area, there is a navigation bar with the text "1 to 8 of 8" and icons for sorting and filtering.

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Statistics Command Type Access by Database Type, Name

This report displays the statistics command type access by database name.

COLUMNS

Columns	Description
DB Type	Database Type (ORACLE, MMSQL, MMSQL2000, SYBASE, DB2, MYSQL)
DB Name	Database Name
Command Type	The SQL command type, for example, SELECT
Total Events	Number of logs

EXAMPLE

The screenshot shows a report titled "McAfee Database Activity Monitoring - Statistics Command Type Access by Database Type, Name". The table has four columns: #, DB Type, DB Name, Command Type, and Total Events. There is one row of data: #1, ORACLE, x2dba5a1, SELECT, and Total Events 2. At the bottom left, it says "1 to 1 of 1".

#	DB Type	DB Name	Command Type	Total Events
1	ORACLE	x2dba5a1	SELECT	2

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Statistics Database Name Access by Database Type

This report displays the statistic database name access by database type.

COLUMNS

Columns	Description
DB Type	Database Type (ORACLE, MMSQL, MMSQL2000, SYBASE, DB2, MYSQL)
DB Name	Database Name
Total Events	Number of logs

EXAMPLE

McAfee Database Activity Monitoring - Statistics Database Name Access by Database Type			
#	DB Type	DB Name	Total Events
1	ORACLE	x2dba5a1	2
1 to 1 of 1			

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

McAfee - Statistics Command Type Access by Database Type, Name

This report displays the statistic command type access by database type and name.

COLUMNS

Columns	Description
DB Type	Database Type (ORACLE, MMSQL, MMSQL2000, SYBASE, DB2, MYSQL)
DB Name	Database Name
CommandType	Command Type
Total Events	Number of events

EXAMPLE

McAfee Database Activity Monitoring - Statistics Command Type Access by Database Type, Name				
#	DB Type	DB Name	Command Type	Total Events
1	ORACLE	x2dba5a1	SELECT	2
1 to 1 of 1				▲ ▼

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_database_activity_monitoring_syslogng

EPOLICY ORCHESTRATOR (EPO)

The McAfee ePO report group includes the following reports:

- “McAfee ePO Top Threats”, on page 331
- “McAfee ePO Console Logon Activity”, on page 332
- “McAfee ePO Agents by Server”, on page 333
- “McAfee ePO Console Activity Summary”, on page 334
- “McAfee ePO Agent Communication Detail”, on page 335
- “McAfee ePO Agent Communication Top 100 Summary”, on page 336

McAfee ePO Top Threats

Overall top 20 reported malware threats for all client systems.

COLUMNS

Columns	Description
Threat Name	Description of threat
Threat Severity	Level of severity
Threat Category	Category of threat
Number of Occurrences	Number of times the threat occurred

EXAMPLE

The screenshot shows a report titled "McAfee ePO Top Threats". The table has columns: #, Threat Name, Threat Severity, Threat Category, and Number of Occurrences. The data is as follows:

#	Threat Name	Threat Severity	Threat Category	Number of Occurrences
1	Anti-spyware Maximum Pr...	5	hip.file	32
2	Prevent Internet Explorer f...	5	hip.file	20
3	-	1	mail.filter	20
4	Anti-virus Standard Protec...	5	hip.file	4
5	Anti-virus Maximum Protec...	5	hip.file	2
6	Anti-virus Standard Protec...	5	hip.file	2

At the bottom left, it says "1 to 6 of 6".

INTELLISCEMMA VIEW

- None

TABLES REFERENCED

- mcafee_epo_event_rdbms
- macfee_epo45_event_rdbms
- macfee_epo46_event_sensageRetriever
- macfee_epo51_event_sensageRetriever

McAfee ePO Console Logon Activity

ePO server console administrative logons, sorted by time.

COLUMNS

Columns	Description
Time	Time the administrative logon occurred
Username	Username used for administrative logon
Detail	Status message returned by logon

EXAMPLE

#	Time	Username	Detail
1	2008-Apr-28 16:47:20 GMT		Failed logon for user "schamarth" fr...
2	2008-Apr-28 16:47:32 GMT		Failed logon for user "schamarth" fr...
3	2008-Apr-29 20:27:56 GMT		Failed logon for user "flast" from IP ...
4	2008-Apr-30 15:42:31 GMT		Failed logon for user "trivia" from IP ...
5	2008-Apr-30 18:15:18 GMT		Failed logon for user "trivia" from IP ...
6	2008-Apr-30 18:44:24 GMT		Failed logon for user "trivia" from IP ...
7	2008-Apr-30 18:44:32 GMT		Failed logon for user "trivia" from IP ...
8	2008-Apr-30 19:45:02 GMT		Failed logon for user "flast" from IP ...

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_epo_event_rdbms
- mcafee_epo45_event_rdbms
- mcafee_epo46_event_sensageRetriever
- mcafee_epo51_event_sensageRetriever

McAfee ePO Agents by Server

Number of client agents being serviced by each ePO server

COLUMNS

Columns	Description
Server ID	ID of ePO Server
Number of agents	Number of ePO Client Agents

EXAMPLE

#	Server ID	Number of agents
1	AB09XY11	14

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_epo_event_rdbms
- macfee_epo45_event_rdbms
- macfee_epo46_event_sensageRetriever
- macfee_epo51_event_sensageRetriever

McAfee ePO Console Activity Summary

Count of actions by username.

COLUMNS

Columns	Description
Action	Type of console activity
Username	User
Number of occurrences	Number of occurrences

EXAMPLE

#	Action	Username	Number of Occurrences
1	LdapSync: Sync across users from...	admin	240
2	Login attempt	admin	190
3	User Logout	admin	178
4	Active Directory Sync	master	176
5	Login attempt	master	142
6	User Logout	master	140
7	Run command as task	flast	140
8	Reload Revoked Extension List	system	118
9	Deploy Agents	flast	96
10	Download Software Product List	admin	90
11	Repository Pull	admin	84

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_epo_event_rdbms
- macfee_epo45_event_rdbms
- macfee_epo46_event_sensageRetriever
- macfee_epo51_event_sensageRetriever

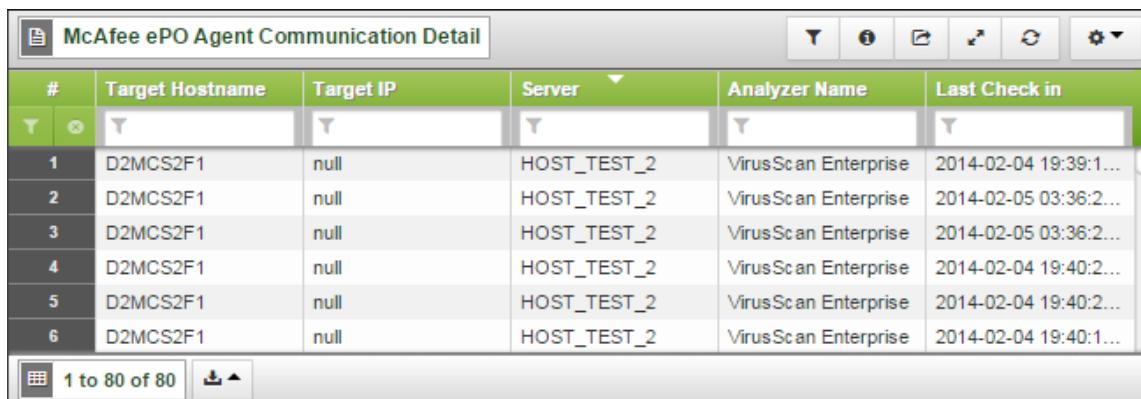
McAfee ePO Agent Communication Detail

Last check-in times of ePO client agents, sorted by time

COLUMNS

Columns	Description
Target Hostname	Hostname of target
Target IP	IP Address of target
Server	Server ID
Analyzer Name	Name of Analyzer component
Last Check in	Date and time the last agent checked in

EXAMPLE



The screenshot shows a table titled "McAfee ePO Agent Communication Detail". The table has columns: #, Target Hostname, Target IP, Server, Analyzer Name, and Last Check in. The data is as follows:

#	Target Hostname	Target IP	Server	Analyzer Name	Last Check in
1	D2MCS2F1	null	HOST_TEST_2	VirusScan Enterprise	2014-02-04 19:39:1...
2	D2MCS2F1	null	HOST_TEST_2	VirusScan Enterprise	2014-02-05 03:36:2...
3	D2MCS2F1	null	HOST_TEST_2	VirusScan Enterprise	2014-02-05 03:36:2...
4	D2MCS2F1	null	HOST_TEST_2	VirusScan Enterprise	2014-02-04 19:40:2...
5	D2MCS2F1	null	HOST_TEST_2	VirusScan Enterprise	2014-02-04 19:40:2...
6	D2MCS2F1	null	HOST_TEST_2	VirusScan Enterprise	2014-02-04 19:40:1...

At the bottom left, it says "1 to 80 of 80".

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_epo_event_rdbms
- macfee_epo45_event_rdbms
- macfee_epo46_event_sensageRetriever
- macfee_epo51_event_sensageRetriever

McAfee ePO Agent Communication Top 100 Summary

Number of times ePO client agents check in, by Hostname, IP, Server, and Analyzer Name

COLUMNS

Columns	Description
Target Hostname	Hostname of target
Target IP	IP Address of target
Server	Server ID
Analyzer Name	Name of Analyzer component
Number of Events	Number of times the event occurred

EXAMPLE

#	Target Hostname	Target IP	Server	Analyzer Name	Number of Events
1	D2MCS2F1	168.135.43.75	HOSTABC	VirusScan Enterprise	22
2		128.0.0.0	AB09XY11	GS Domino	20
3	XX-70186640-DSV	255.0.0.1	AB09XY11	VirusScan Enterprise	20
4	D2MCS2F1	null	HOST_TEST_2	VirusScan Enterprise	14
5	D2MCS2F1	null	HOSTABC	VirusScan Enterprise	2
6	D2MCS2F1	null	HOST_TEST	VirusScan Enterprise	2

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_epo_event_rdbms
 - macfee_epo45_event_rdbms
 - macfee_epo46_event_sensageRetriever
 - macfee_epo51_event_sensageRetriever

NETWORK SECURITY PLATFORM (INTRUSHIELD)

The McAfee Network Security Platform (NSP) report group includes the following reports:

- “[McAfee NSP Possible Successful Exploits \(by Target\)](#)”, on page 338
- “[McAfee NSP Possible Successful Exploits \(by Source\)](#)”, on page 339
- “[McAfee NSP Attacks Details](#)”, on page 340
- “[McAfee NSP Attacks Summary](#)”, on page 341
- “[McAfee NSP Top 20 Most Common Events](#)”, on page 342
- “[McAfee NSP Top 10 Source IP](#)”, on page 343
- “[McAfee NSP Top 10 Target IP](#)”, on page 344
- “[McAfee NSP Top 10 Directed Attacks](#)”, on page 345

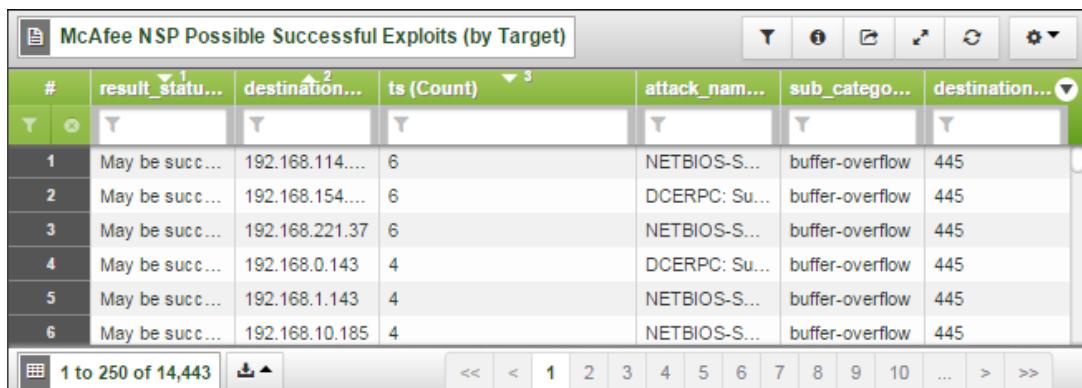
McAfee NSP Possible Successful Exploits (by Target)

IntruShield: Exploits with some chance of success (by target). Lists systems that may have been compromised, ordered by likelihood of having been successfully compromised.

COLUMNS

Columns	Description
result_status (Field value)	Possible level of success of the exploit: Possible values: <ul style="list-style-type: none">• Successful• May be successful
destination_ip (Field value)	IP address of the targeted system
ts (Count)	# of times the exploit occurred
attack_name (Field value)	Name of the attack
sub_category (Field)	Sub-category of the exploit
destination_port (Field value)	Port number of the destination system

EXAMPLE



#	result_status ¹	destination ²	ts (Count) ³	attack_name...	sub_catego...	destination...
1	May be succ...	192.168.114....	6	NETBIOS-S...	buffer-overflow	445
2	May be succ...	192.168.154....	6	DCERPC: Su...	buffer-overflow	445
3	May be succ...	192.168.221.37	6	NETBIOS-S...	buffer-overflow	445
4	May be succ...	192.168.0.143	4	DCERPC: Su...	buffer-overflow	445
5	May be succ...	192.168.1.143	4	NETBIOS-S...	buffer-overflow	445
6	May be succ...	192.168.10.185	4	NETBIOS-S...	buffer-overflow	445

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_intrushield_syslogng

McAfee NSP Possible Successful Exploits (by Source)

IntruShield: Exploits with some chance of success (by source). Lists hostile systems, ordered by the likelihood they are actually hostile.

COLUMNS

Columns	Description
Result Status (Count)	Possible level of success of the exploit: Possible values: <ul style="list-style-type: none">• Successful• May be successful
source_ip (Count)	IP address of the source system
ts (Count)	# of times the exploit occurred
attack_name (Count)	Description of the exploit
sub_category	Sub-category of the exploit
destination_port (Count)	Port number of the destination system

EXAMPLE

#	result_status	source_ip	ts (Count)	attack_name	sub_category	destination_port
1	May be successful	192.168.100.7	6	DCERPC: Su...	buffer-overflow	445
2	May be successful	192.168.17.251	6	NETBIOS-S...	buffer-overflow	445
3	May be successful	192.168.184....	6	NETBIOS-S...	buffer-overflow	445
4	May be successful	192.168.192....	6	NETBIOS-S...	buffer-overflow	445
5	May be successful	192.168.71.66	6	NETBIOS-S...	buffer-overflow	445
6	May be successful	192.168.96.203	6	SMB: Gener...	protocol-violation	N/A

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_intrushield_syslogng

McAfee NSP Attacks Details

IntruShield: System attacks by severity with target/source IP and target/source port.

COLUMNS

Columns	Description
Attack Name	Name of the attack
Severity Name	Severity of the attack
Source IP	Source IP address of the attack
Source Port	Source Port number of the attack
Target IP	IP address of the attacked system
Target Port	Port number of the attacked system
Protocol	Protocol used for the attack

EXAMPLE

The screenshot shows a software interface titled "McAfee NSP Attacks Details". The main area is a table with columns: #, Attack Name, Severity Na..., Source IP, Source Port, Target IP, Target Port, and Protocol. The table contains 9 rows of data, each representing an attack entry. The first few rows show attacks like "HTTP: ExAir..." with various source and target details. At the bottom left, it says "1 to 250 of 1,000". At the bottom right, there are navigation buttons for page numbers (1, 2, 3, 4, >, >>) and search/filter icons.

#	Attack Name	Severity Na...	Source IP	Source Port	Target IP	Target Port	Protocol
1	HTTP: ExAir...	Low	192.168.1.1	-	192.168.4.2	-	-
2	HTTP: ExAir...	Low	192.168.1.1	59256	192.168.4.2	80	6
3	HTTP: ExAir...	Low	192.168.1.1	-	192.168.4.2	-	-
4	HTTP: ExAir...	Low	192.168.1.1	31894	192.168.4.2	80	6
5	HTTP: ExAir...	Low	192.168.1.1	4392	192.168.4.2	80	6
6	HTTP: Malfo...	Low	192.168.1.1	30514	192.168.4.2	80	6
7	HTTP: Malfo...	Low	192.168.1.1	-	192.168.4.2	-	-
8	HTTP: Malfo...	Low	192.168.1.1	-	192.168.4.2	-	-
9	HTTP: ExAir...	Low	192.168.1.1	6449	192.168.4.2	80	6

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcAfee_intrushield_rdbms

McAfee NSP Attacks Summary

IntruShield: System attacks by severity and count.

COLUMNS

Columns	Description
Attack Name	Type of attack
Severity Name	Severity level of the attack
Severity	Numeric severity level of the attack
Number of Occurrences	Number of times the attack occurred

EXAMPLE

The screenshot shows a report titled "McAfee NSP Attacks Summary" generated "For 20 year(s) ending on 2015-Apr-21 03:41:24 PM". The report lists 11 attacks, each with its name, severity, and occurrence count. The attacks are categorized by severity: Low (6 occurrences), Medium (4 occurrences), and High (1 occurrence). The report includes navigation controls at the bottom.

#	Attack Name	Severity Name	Severity	Number of Occurrences
1	HTTP: ExAir Sample Scripts DoS	Low	1	2
2	HTTP: GoAhead Web Server Sourc...	Low	1	2
3	HTTP: Possible Apache Directory In...	Low	1	2
4	PUP: HotBar	Low	1	4
5	BACKDOOR: SSH Server Running ...	Low	1	1
6	FTP: Root/Administrator Login Attempt	Low	1	2

1 to 11 of 11

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcAfee_intrushield_rdbms

McAfee NSP Top 20 Most Common Events

IntruShield: Top 20 most common found events and the number of occurrences of each

COLUMNS

Columns	Description
Event Description	Description of the Event
Sub Category	Sub-classification of the event
Number of Occurrences	Number of times the event occurred

EXAMPLE

#	Event Description	Sub Category	Number of Occurrences
1	ARP: MAC Address Flip-Flop	restricted-access	7558
2	SMB: Generic Buffer Overflow Attempt Dete...	protocol-violation	4882
3	DCERPC: Suspicious DCERPC Call	buffer-overflow	4431
4	NETBIOS-SS: Microsoft Server Service Re...	buffer-overflow	4429
5	TCP: SYN Host Sweep	host-sweep	1860
6	TCP: Full-Connect Host Sweep	host-sweep	1045
7	DCERPC: Microsoft RPC DCOM Buffer Ove...	protocol-violation	1007
8	UDP: Host Sweep	host-sweep	665

1 to 20 of 20

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_intrushield_syslogng

McAfee NSP Top 10 Source IP

IntruShield: Top 10 system attacks by source IP.

COLUMNS

Columns	Description
Source IP	Source IP address of the attack
Attack Name	Name of the attack
Alert Severity	Severity of the attack
Number of Attacks	Number of times an attack from this IP address occurred

EXAMPLE

#	Source IP	Attack Name	Alert Severity	Number of Attacks
1	192.168.1.1	HTTP: ExAir Sample Scripts DoS	Low	7
2	192.168.1.1	HTTP: Malformed HTTP request	Low	3

INTELLISchema VIEW

- None

TABLES REFERENCED

- mcafee_intrushield_rdbms

McAfee NSP Top 10 Target IP

IntruShield: Top 10 IP attacks with attack description and number of attacks.

COLUMNS

Columns	Description
Target IP	Target IP address of the attack
Attack Name	Name of the attack
Alert Severity	Severity of the attack
Number of Attacks	Number of times an attack targeting this IP address occurred

EXAMPLE

#	Target IP	Attack Name	Alert Severity	Number of Attacks
1	192.168.4.2	HTTP: ExAir Sample Scripts DoS	Low	7
2	192.168.4.2	HTTP: Malformed HTTP request	Low	3

TABLES REFERENCED

- mcAfee_intrushield_rdbms

INTELLISCHEMA VIEW

- None

McAfee NSP Top 10 Directed Attacks

IntruShield: Top 10 system attacks by source, destination, and severity. (A directed attack is an attack originating from a single system targeted against another single system.)

COLUMNS

Columns	Description
Source IP	Source IP address of the attack
Target IP	Target IP address of the attack
Attack Name	Name of the attack
Alert Severity	Severity of the attack
Number of Attacks	Number of times the directed attack occurred

EXAMPLE

The screenshot shows a table titled "McAfee NSP Top 10 Directed Attacks" with a filter "For 20 year(s) ending on 2015-Jan-18". The table has columns: #, Source IP, Target IP, Attack Name, Alert Severity, and Number of Attacks. There are two rows of data:

#	Source IP	Target IP	Attack Name	Alert Severity	Number of Attacks
1	192.168.1.1	192.168.4.2	HTTP: ExAir Sample Scri...	Low	7
2	192.168.1.1	192.168.4.2	HTTP: Malformed HTTP r...	Low	3

At the bottom left, it says "1 to 2 of 2" with up and down arrows.

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_intrushield_rdbms

VULNERABILITY MANAGER (FOUNDSTONE)

The McAfee Foundstone report group includes the following reports:

- “[McAfee Foundstone OS & Application Vulnerabilities](#)”, on page 346
- “[McAfee Foundstone Top 20 Affected Hosts](#)”, on page 348
- “[McAfee Foundstone High Risk Vulnerabilities](#)”, on page 349
- “[McAfee Foundstone High Risk Vulnerabilities Top 100 Summary](#)”, on page 350

McAfee Foundstone OS & Application Vulnerabilities

Vulnerability Manager - Number of vulnerabilities reported by category from OS or application layer issues.

COLUMNS

Columns	Description
Category	Category of vulnerability
Number of Occurrences	Number of times the vulnerability occurred

EXAMPLE



INTELLISchema View

- None

Tables Referenced

- mcafee_foundstone_rdbms

McAfee Foundstone Top 20 Affected Hosts

Vulnerability Manager Top 20 systems reporting vulnerabilities.

COLUMNS

Columns	Description
Hostname	Hostname of device affected by vulnerability
Number of Occurrences	Number of times the host was affected by the vulnerability

EXAMPLE

#	hostname	hostname (Count)
1	gc._msdc.s.w2k3corp.mydomain.com	7
2	mdtwnjlab2kts01.w2k3ugd.mydomain.com	6
3	mdtwnjlabdc02.w2k3ugd.mydomain.com	6
4	mdtwnjlabdc99.w2k3corp.mydomain.com	1

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_foundstone_rdbms

McAfee Foundstone High Risk Vulnerabilities

Vulnerability Manager - Client systems reporting a vulnerability level of 10, the highest risk, items, sorted by date.

COLUMNS

Columns	Description
Alert date	Date of alert
IP Address	IP Address of device affected by the vulnerability
Hostname	Hostname of device affected by the vulnerability
Vulnerability	Description of vulnerability

EXAMPLE

#	Alert date	IP Address	Hostname	Vulnerability
1	2014-Aug-20 12:21:23 GMT	10.24.195.72	ccp9cw00.lab.cif.mydom...	(MS04-036) Microsoft Win...
2	2014-Aug-20 12:21:23 GMT	10.10.14.11	[Unknown]	HP Web-enabled Manage...
3	2014-Aug-20 12:21:23 GMT	10.10.68.46	[Unknown]	HP Web-enabled Manage...
4	2014-Aug-20 12:21:23 GMT	10.10.14.3	[Unknown]	HP Web-enabled Manage...
5	2014-Aug-20 12:21:23 GMT	10.10.134.6	[Unknown]	HP Web-enabled Manage...
6	2014-Aug-20 12:21:23 GMT	10.10.68.45	[Unknown]	HP Web-enabled Manage...
7	2014-Aug-20 12:21:23 GMT	10.30.1.88	[Unknown]	Oracle Alert 68 Numerous...

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_foundstone_rdbms

McAfee Foundstone High Risk Vulnerabilities Top 100 Summary

Vulnerability Manager: Number of High Risk (10) Vulnerabilities and their description by IP Address

COLUMNS

Columns	Description
IP Address	IP Address of device affected by the vulnerability
Vulnerability	Description of vulnerability
Number of Occurrences	Number of times the vulnerability occurred

EXAMPLE

#	IP Address	Vulnerability	Number of Occurrences
1	10.0.0.127	Oracle Releases July 2007 Critical Patch U...	9
2	10.0.0.127	Oracle Releases October 2007 Critical Pat...	9
3	10.0.0.127	Oracle April 2008 Critical Patch Update	9
4	10.0.0.127	Oracle January 2008 Critical Patch Update	9
5	10.0.0.127	Oracle Releases October 2006 Oracle Critic...	9
6	10.0.0.127	Oracle July 2008 Critical Patch Update	8
7	10.0.0.17	HP Web-enabled Management Software Re...	2
8	10.0.0.25	Microsoft IIS newdsn.exe Command Executi...	2

1 to 100 of 100

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- mcafee_foundstone_rdbms

CHAPTER 12

BlueCoat Reports

The SenSage AP BlueCoat reports assist organizations in compiling offenders.

This chapter provides a reference for BlueCoat reports, including lists of columns available for reporting.

The BlueCoat reports includes the following:

- “BlueCoat - High Offender List”, on page 351
- “BlueCoat - Individual IP Usage Detail”, on page 352
- “BlueCoat - Top 10 Domains Visited”, on page 353
- “BlueCoat - Top Domains Visited by UserId”, on page 354
- “BlueCoat - Top Download Users”, on page 355
- “BlueCoat - Top Sending Users”, on page 356
- “BlueCoat - Top Users with Most Site Visits”, on page 357

BLUECOAT - HIGH OFFENDER LIST

This report displays the number of filtered sources by category and client IP address.

COLUMNS

Columns	Description
c_ip	The IP address of the client that made the request.
Category	Content category of the requested URL.
Count	Number of times the content category was filtered.

EXAMPLE

#	c_ip	Category	Count
1	10.10.0.11	Web Advertisements	5
2	10.10.0.25	Web Advertisements	4
3	10.10.0.22	Web Advertisements	3
4	10.10.0.18	Web Advertisements	3
5	10.10.0.6	Web Advertisements	3
6	10.10.0.41	Web Advertisements	3

1 to 34 of 34

TABLES REFERENCED

- bluecoat_sgproxy_batch

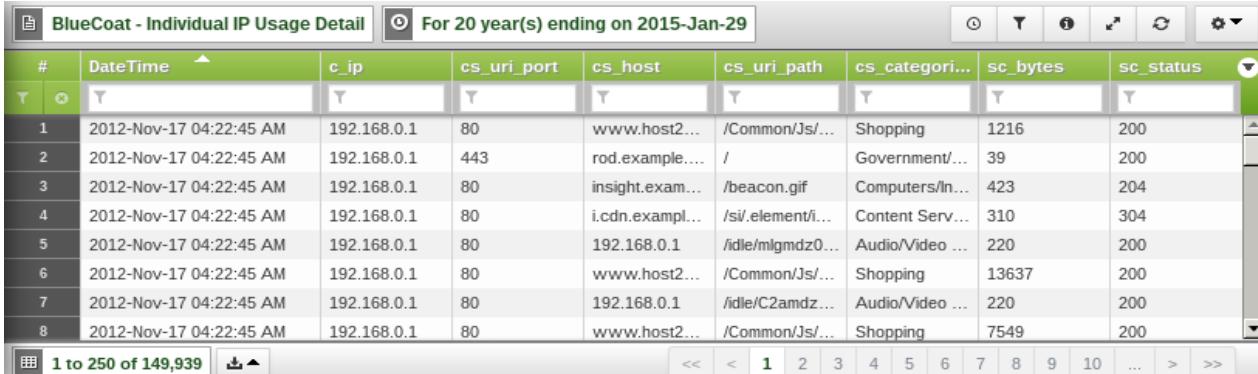
BLUECOAT - INDIVIDUAL IP USAGE DETAIL

This report displays all BlueCoat logs for an individual client IP address.

COLUMNS

Column	Description
DateTime	Date and time on which the activity occurred
c_ip	Client IP address
cs_url_port	The port number the client is connected to
cs_host	The host name the client is connected to
cs_url_path	The requested URI
cs_categories	Content category of the request URL
sc_bytes	Number of bytes returned by the server
sc_status	The HTTP code returned to the client

EXAMPLE



The screenshot shows a software interface for viewing BlueCoat logs. At the top, there's a title bar with the report name and a date range from "For 20 year(s) ending on 2015-Jan-29". Below the title bar is a toolbar with various icons. The main area is a data grid with the following columns: #, DateTime, c_ip, cs_uri_port, cs_host, cs_uri_path, cs_categories, sc_bytes, and sc_status. The data grid contains 8 rows of log entries. At the bottom of the grid, there's a footer with navigation links like '<<', '<', '1' (highlighted), '2', '3', '4', '5', '6', '7', '8', '9', '10', '...', '>', and '>>'.

#	DateTime	c_ip	cs_uri_port	cs_host	cs_uri_path	cs_categories	sc_bytes	sc_status
1	2012-Nov-17 04:22:45 AM	192.168.0.1	80	www.host2...	/Common/Js/...	Shopping	1216	200
2	2012-Nov-17 04:22:45 AM	192.168.0.1	443	rod.example....	/	Government/...	39	200
3	2012-Nov-17 04:22:45 AM	192.168.0.1	80	insight.exam...	/beacon.gif	Computers/In...	423	204
4	2012-Nov-17 04:22:45 AM	192.168.0.1	80	i.cdn.exAMPL...	/si/.element/i...	Content Serv...	310	304
5	2012-Nov-17 04:22:45 AM	192.168.0.1	80	192.168.0.1	/idle/mlgmdz0...	Audio/Video ...	220	200
6	2012-Nov-17 04:22:45 AM	192.168.0.1	80	www.host2...	/Common/Js/...	Shopping	13637	200
7	2012-Nov-17 04:22:45 AM	192.168.0.1	80	192.168.0.1	/idle/C2amdz...	Audio/Video ...	220	200
8	2012-Nov-17 04:22:45 AM	192.168.0.1	80	www.host2...	/Common/Js/...	Shopping	7549	200

TABLES REFERENCED

- bluecoat_sgproxy_batch

BLUECOAT - TOP 10 DOMAINS VISITED

This report displays the top visited domains..

COLUMNS

Column	Description
Domain name	Domain name
Number of visits	Number of visits

EXAMPLE

#	Domain name	Number of visits
1	192.168.0.1	2
2	www.host21.example.com	5
3	us.js1.example.com	2326
4	us.i1.example.com	6927

TABLES REFERENCED

- bluecoat_sgproxy_batch

BLUECOAT - TOP DOMAINS VISITED BY USERID

This report displays top domains visited by a user.

COLUMNS

Columns	Description
User ID	UserId
Domain Name	Domain name
Number of visits	Number of visits

EXAMPLE

#	User ID	Domain Name	Number of visits
1	-	speed.example.com	136
2	caferme	www.host21.example.com	5
3	jmklug	rod.example.com	3
4	fharris447	domain.example.com	2
5	guest_192.168.0.1	192.168.0.1	2
6	aadams386	64.4.55.45	1
7	aadams402	motionslow.espn.example.com	1
8	aallen238	64.4.55.45	1

TABLES REFERENCED

- bluecoat_sgproxy_batch

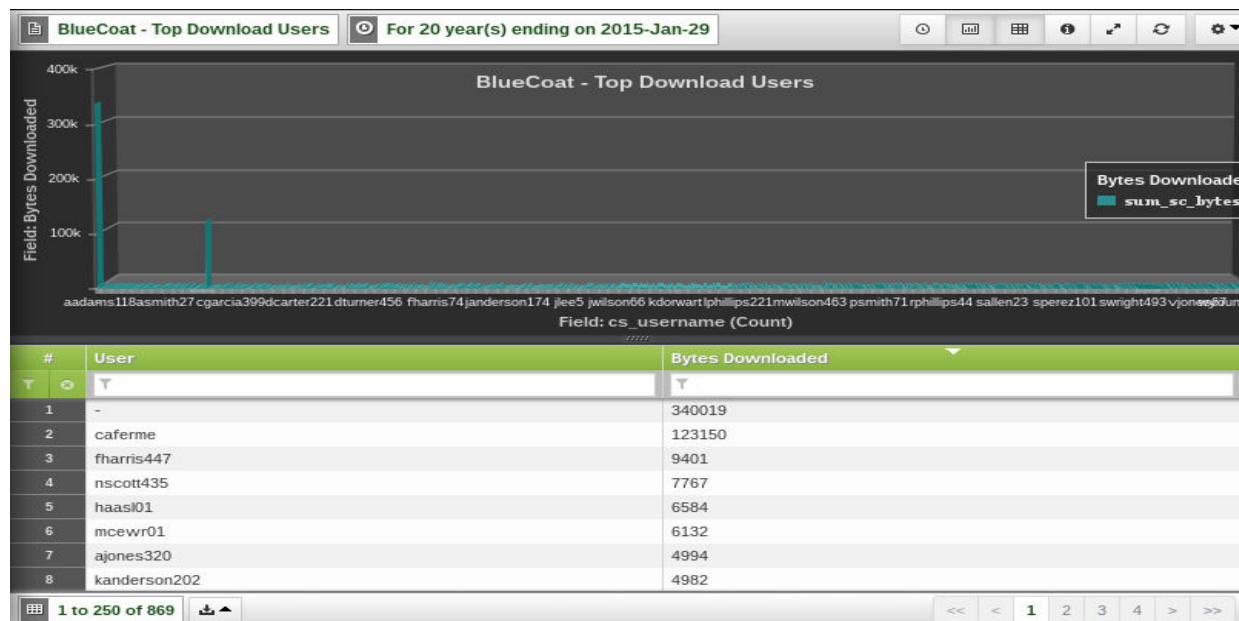
BLUECOAT - TOP DOWNLOAD USERS

This report displays top users by the total size of the downloaded content.

COLUMNS

Columns	Description
User	UserId
Bytes Downloaded	Total size of the downloaded content by the user

EXAMPLE



TABLES REFERENCED

- bluecoat_sgproxy_batch

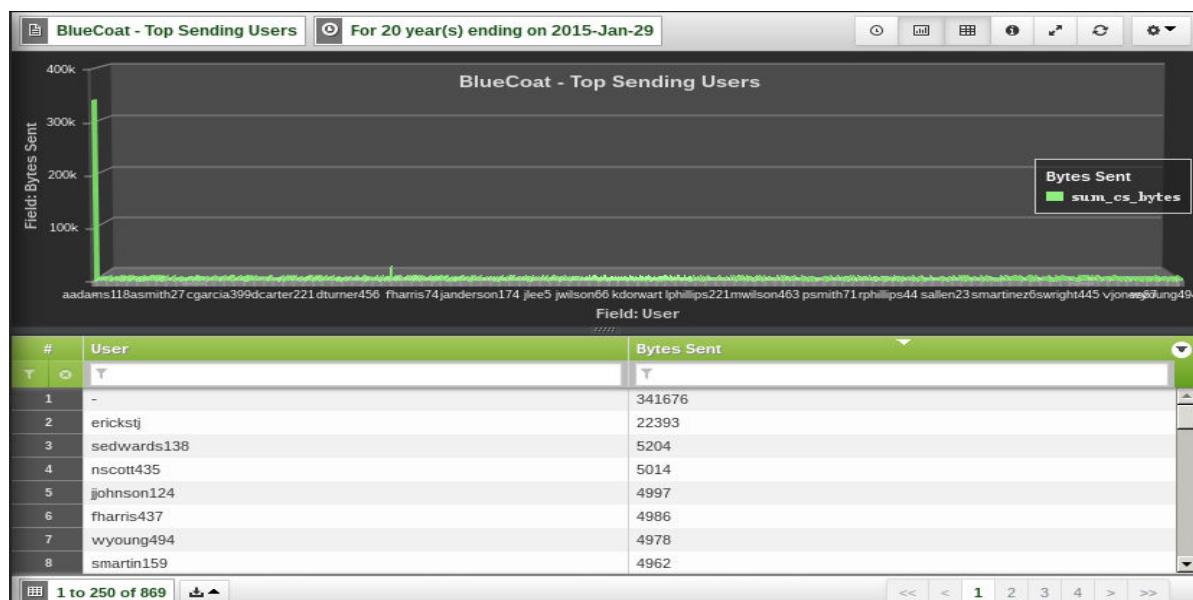
BLUECOAT - TOP SENDING USERS

NOTE: This report is equivalent to "BlueCoat - Top Download Users".

COLUMNS

Columns	Description
User	UserId
Bytes Sent	Total size of the downloaded content by the user

EXAMPLE



TABLES REFERENCED

- bluecoat_sgproxy_batch

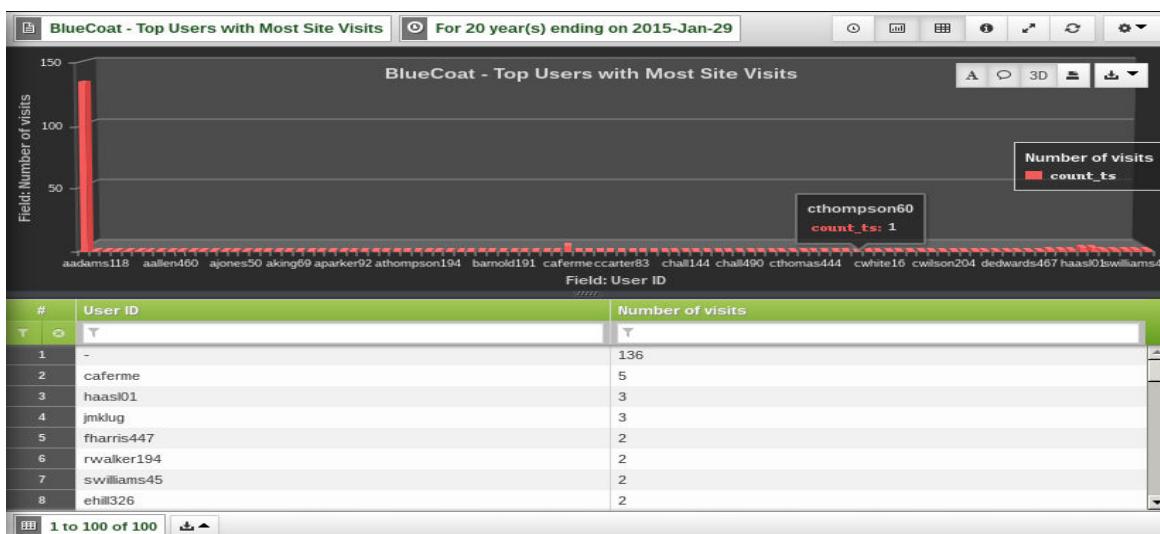
BLUECOAT - TOP USERS WITH MOST SITE VISITS

This report shows the top 100 users with the most site visits.

COLUMNS

Columns	Description
User ID	User ID
Number of visits	Number of visits

EXAMPLE



TABLES REFERENCED

- bluecoat_sgproxy_batch

CHAPTER 13

HawkEye G Analytics Reports

The HawkEye G Analytics reports assist organizations in meeting specific regulations. These reports are designed to monitor critical threat areas, enabling your organization to respond quickly and efficiently to infected hosts.

This chapter provides HawkEye G Analytics reports, including lists of columns available for reporting.

The HawkEye G Analytics reports contains following reporting groups:

- “Actions Monitoring Reports”, next
- “All Events Monitoring Reports”, on page 383
- “Device ThreatSync Monitoring Reports”, on page 388
- “Heuristics Monitoring Activity”, on page 392
- “Event Indicator Activity Monitoring reports”, on page 402
- “MIS Potential Monitoring reports”, on page 416
- “Threat Match Monitoring Reports”, on page 426

ACTIONS MONITORING REPORTS

The Actions Monitoring reports group displays a file listing of specific threat events requiring action and includes the following reports:

- “Actions: File List Details”, next
- “Actions: File List Investigation”, on page 361
- “Actions: File List Summary”, on page 362
- “Actions: Kill Process Details”, on page 363
- “Actions: Kill Process Investigation”, on page 364
- “Actions: Kill Process Summary”, on page 365
- “Actions: Network Connection List Details”, on page 366
- “Actions: Network Connections List Investigation”, on page 367
- “Actions: Network Connections List Summary”, on page 368
- “Actions: Process List Details”, on page 369
- “Actions: Process List Investigation”, on page 370
- “Actions: Process List Summary”, on page 371
- “Actions: Quarantine File Details”, on page 372
- “Actions: Quarantine File Investigation”, on page 373
- “Actions: Quarantine File Summary”, on page 375
- “Actions: Registry List Details”, on page 376
- “Actions: Registry List Investigation”, on page 378
- “Actions: Registry List Summary”, on page 379
- “Actions: Undo Quarantine File Details”, on page 380
- “Actions: Undo Quarantine File Investigation”, on page 381
- “Actions: Undo Quarantine File Summary”, on page 382

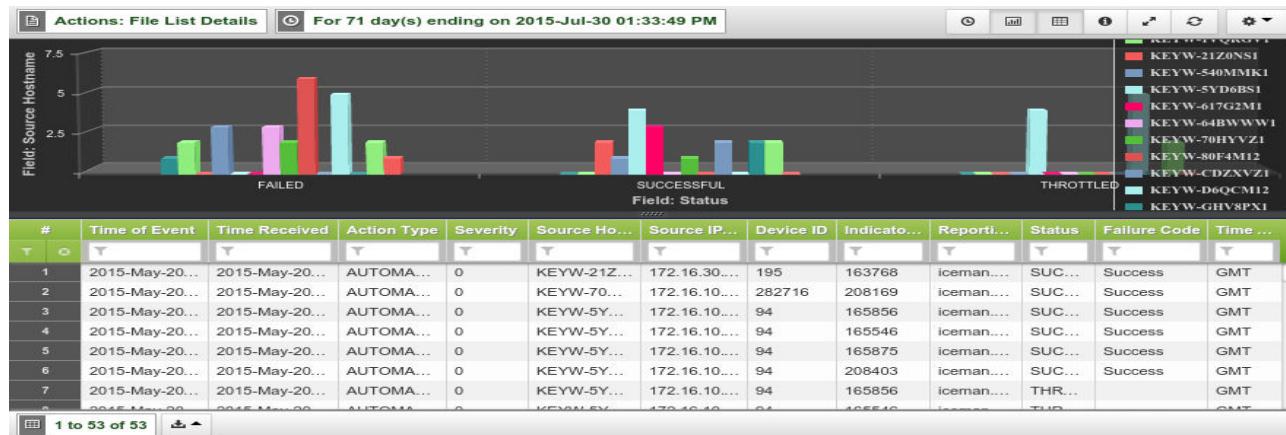
Actions: File List Details

Details a file list of events in which an infected host was detected.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none"> AUTOMATIC MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Failure Code	Shows an error code if the action is failed
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

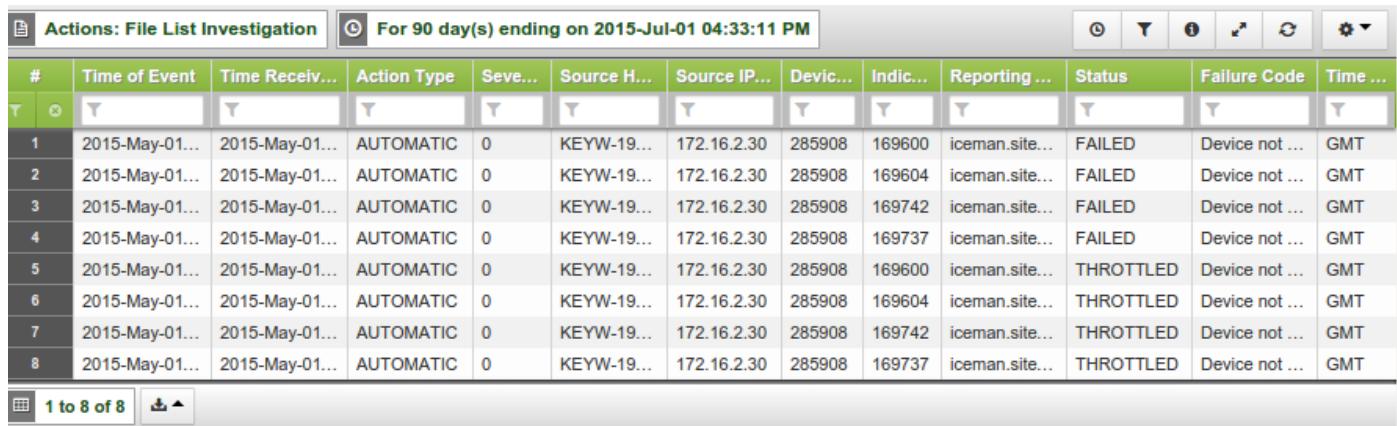
Actions: File List Investigation

Details a file list for investigation in which an infected host was detected.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none"> • AUTOMATIC • MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Failure Code	Shows an error code if the action is failed
Time Zone	Time zone in which the event occurred

EXAMPLE



The screenshot shows a database grid with the following columns and data:

#	Time of Event	Time Receiv...	Action Type	Seve...	Source H...	Source IP...	Devic...	Indic...	Reporting ...	Status	Failure Code	Time ...
1	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-19...	172.16.2.30	285908	169600	iceman.site...	FAILED	Device not ...	GMT
2	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-19...	172.16.2.30	285908	169604	iceman.site...	FAILED	Device not ...	GMT
3	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-19...	172.16.2.30	285908	169742	iceman.site...	FAILED	Device not ...	GMT
4	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-19...	172.16.2.30	285908	169737	iceman.site...	FAILED	Device not ...	GMT
5	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-19...	172.16.2.30	285908	169600	iceman.site...	THROTTLED	Device not ...	GMT
6	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-19...	172.16.2.30	285908	169604	iceman.site...	THROTTLED	Device not ...	GMT
7	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-19...	172.16.2.30	285908	169742	iceman.site...	THROTTLED	Device not ...	GMT
8	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-19...	172.16.2.30	285908	169737	iceman.site...	THROTTLED	Device not ...	GMT

Page navigation: 1 to 8 of 8

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Actions: File List Summary

Details a summary list of hosts and the number of events in which infection was detected.

COLUMNS

Columns	Description
Source Hostname	Name of the infected host
Count of Events	The number of events detected

EXAMPLE

The screenshot shows a report titled "Actions: File List Summary" for a 30-day period ending on June 17, 2015, at 03:00:07 PM. The table has two columns: "Source Hostname" and "Count of Events". The data is as follows:

#	Source Hostname	Count of Events
1	KEYW-MXL0381YD0	40
2	KEYW-GKBZVL1	32
3	KEYW-H13TWW1	24
4	KEYW-D6QCM12	20
5	KEYW-3783L12	13
6	KEYW-5YD6BS1	12
7	KEYW-80F4M12	11
8	KEYW-4293L12	10
9	KEYW-G6NM2R1	9
10	KEYW-G52NHV1	8

INTELLISchema View

- None

Tables Referenced

- hexis_hawkeye_g_cef_syslogng

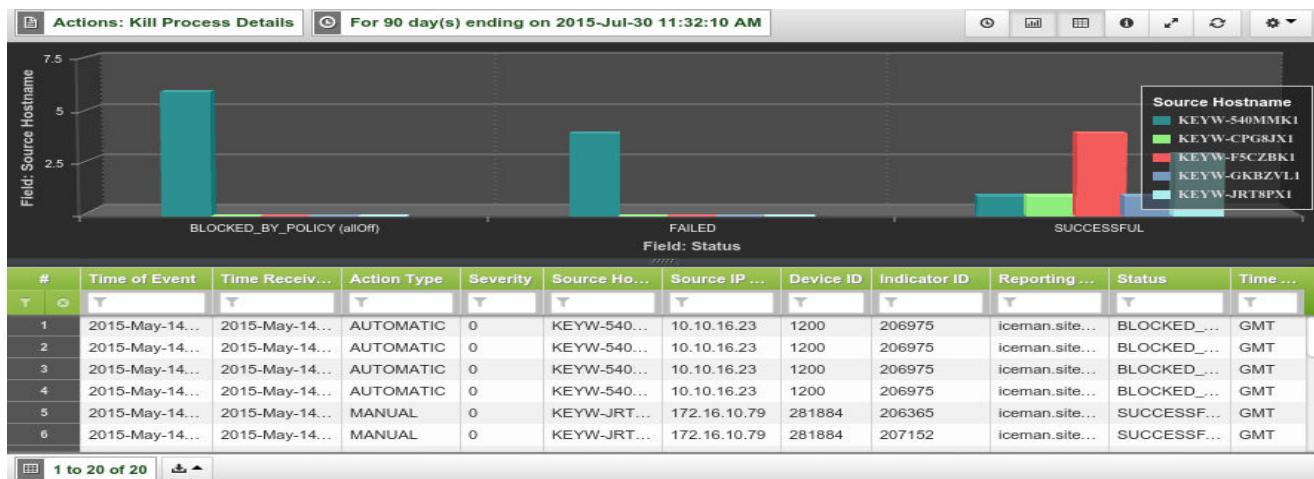
Actions: Kill Process Details

Details an event listing in which detection of an infected host resulted in a kill process.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none">• AUTOMATIC• MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Actions: Kill Process Investigation

Details a file list for investigation in which the detection of the infected host resulted in a kill process.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD).
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none">• AUTOMATIC• MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Time Zone	Time zone in which the event occurred

EXAMPLE

#		Time of Event	Time Received	Action Type	Severity	Source Ho...	Source IP ...	Device ID	Indic...	Reporting...	Status	Time Zone
1		2015-May-14T...	2015-May-14T...	AUTOMATIC	0	KEYW-540...	10.10.16.23	1200	206975	iceman.site...	BLOCKED...	GMT
2		2015-May-14T...	2015-May-14T...	AUTOMATIC	0	KEYW-540...	10.10.16.23	1200	206975	iceman.site...	BLOCKED...	GMT
3		2015-May-14T...	2015-May-14T...	AUTOMATIC	0	KEYW-540...	10.10.16.23	1200	206975	iceman.site...	BLOCKED...	GMT
4		2015-May-14T...	2015-May-14T...	AUTOMATIC	0	KEYW-540...	10.10.16.23	1200	206975	iceman.site...	BLOCKED...	GMT
5		2015-May-15T...	2015-May-15T...	MANUAL	0	KEYW-540...	10.10.16.23	1200	206977	iceman.site...	SUCCESS...	GMT
6		2015-May-20T...	2015-May-20T...	AUTOMATIC	0	KEYW-540...	10.10.16.23	1200	207713	iceman.site...	FAILED	GMT
7		2015-May-20T...	2015-May-20T...	AUTOMATIC	0	KEYW-540...	10.10.16.23	1200	207713	iceman.site...	BLOCKED...	GMT
8		2015-May-20T...	2015-May-20T...	AUTOMATIC	0	KEYW-540...	10.10.16.23	1200	207713	iceman.site...	BLOCKED...	GMT
9		2015-May-21T...	2015-May-21T...	AUTOMATIC	0	KEYW-540...	10.10.16.23	1200	207713	iceman.site...	FAILED	GMT
10		2015-May-21T...	2015-May-21T...	AUTOMATIC	0	KEYW-540...	10.10.16.23	1200	207713	iceman.site...	FAILED	GMT

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Actions: Kill Process Summary

Details a summary list of hosts and the number of events in which infection was detected, resulting in a kill process.

COLUMNS

Columns	Description
Source Hostname	Name of the infected host
Count of Events	The number of events detected

EXAMPLE

#	Source Hostname	Count of Events
1	KEYW-540MMK1	6

INTELLISchema VIEW

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

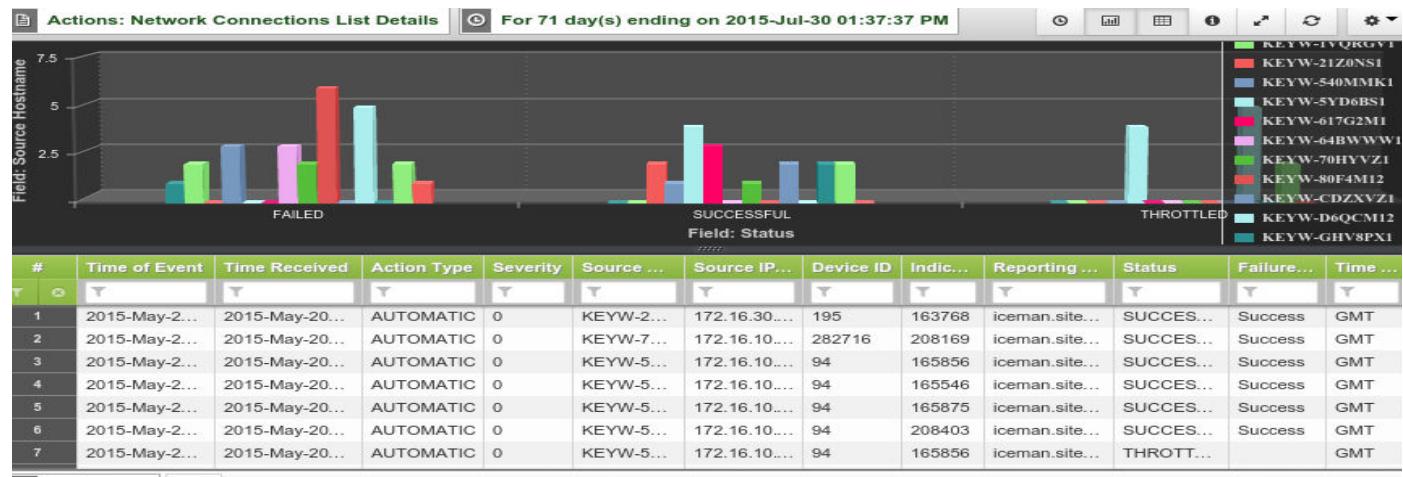
Actions: Network Connection List Details

Details an event listing in which an infected host was detected on a network connection.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none">• AUTOMATIC• MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Failure Code	Shows an error code if the action is failed
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

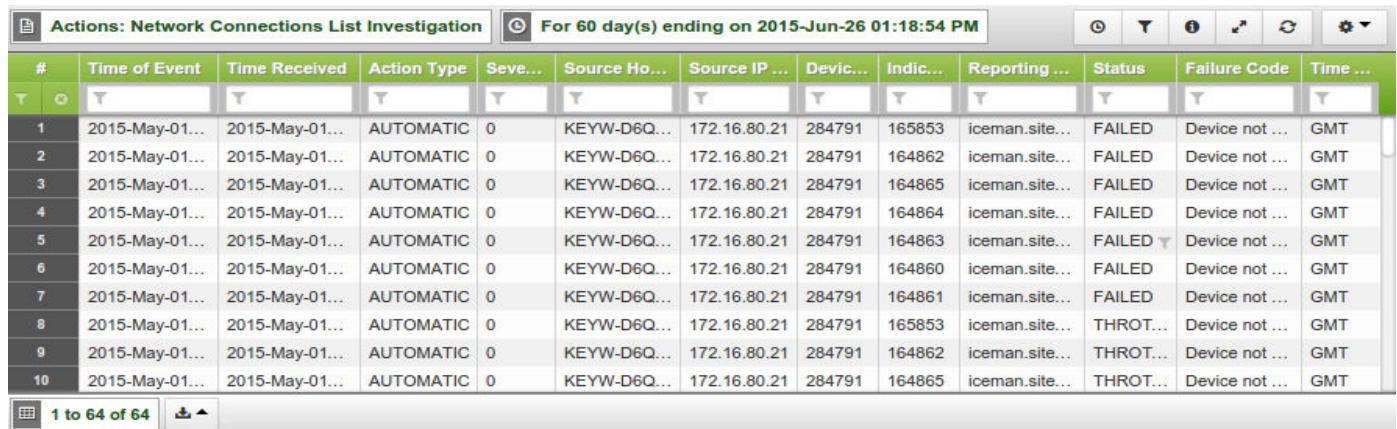
Actions: Network Connections List Investigation

Details a file list for investigation in which an infected host was detected on a network connection.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none">• AUTOMATIC• MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Failure Code	Shows an error code if the action is failed
Time Zone	Time zone in which the event occurred

EXAMPLE



The screenshot shows a database grid titled "Actions: Network Connections List Investigation" with a timestamp of "For 60 day(s) ending on 2015-Jun-26 01:18:54 PM". The grid has 14 columns: #, Time of Event, Time Received, Action Type, Seve..., Source Ho..., Source IP ..., Devic..., Indic..., Reporting..., Status, Failure Code, Time The data consists of 10 rows of network connection details, such as automatic actions on specific dates and times, involving various source hosts and devices, with statuses like FAILED or THROTTLED.

#	Time of Event	Time Received	Action Type	Seve...	Source Ho...	Source IP ...	Devic...	Indic...	Reporting...	Status	Failure Code	Time ...
1	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-D6Q...	172.16.80.21	284791	165853	iceman.site...	FAILED	Device not ...	GMT
2	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-D6Q...	172.16.80.21	284791	164862	iceman.site...	FAILED	Device not ...	GMT
3	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-D6Q...	172.16.80.21	284791	164865	iceman.site...	FAILED	Device not ...	GMT
4	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-D6Q...	172.16.80.21	284791	164864	iceman.site...	FAILED	Device not ...	GMT
5	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-D6Q...	172.16.80.21	284791	164863	iceman.site...	FAILED	Device not ...	GMT
6	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-D6Q...	172.16.80.21	284791	164860	iceman.site...	FAILED	Device not ...	GMT
7	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-D6Q...	172.16.80.21	284791	164861	iceman.site...	FAILED	Device not ...	GMT
8	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-D6Q...	172.16.80.21	284791	165853	iceman.site...	THROTT...	Device not ...	GMT
9	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-D6Q...	172.16.80.21	284791	164862	iceman.site...	THROTT...	Device not ...	GMT
10	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-D6Q...	172.16.80.21	284791	164865	iceman.site...	THROTT...	Device not ...	GMT

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Actions: Network Connections List Summary

Details a summary list of infected hosts on a network connection and the number of events in which infection was detected.

COLUMNS

Columns	Description
Source Hostname	Name of the infected host
Count of Events	The number of events detected

EXAMPLE

#	Source Hostname	Count of Events
1	KEYW-MXL0381YD0	40
2	KEYW-GKBZVL1	34
3	KEYW-H13TWW1	24
4	KEYW-D6QCM12	20
5	KEYW-3783L12	13
6	KEYW-5YD6BS1	12
7	KEYW-80F4M12	11
8	KEYW-4293L12	10
9	KEYW-G52NHV1	8
10	KEYW-1VQRGV1	6

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

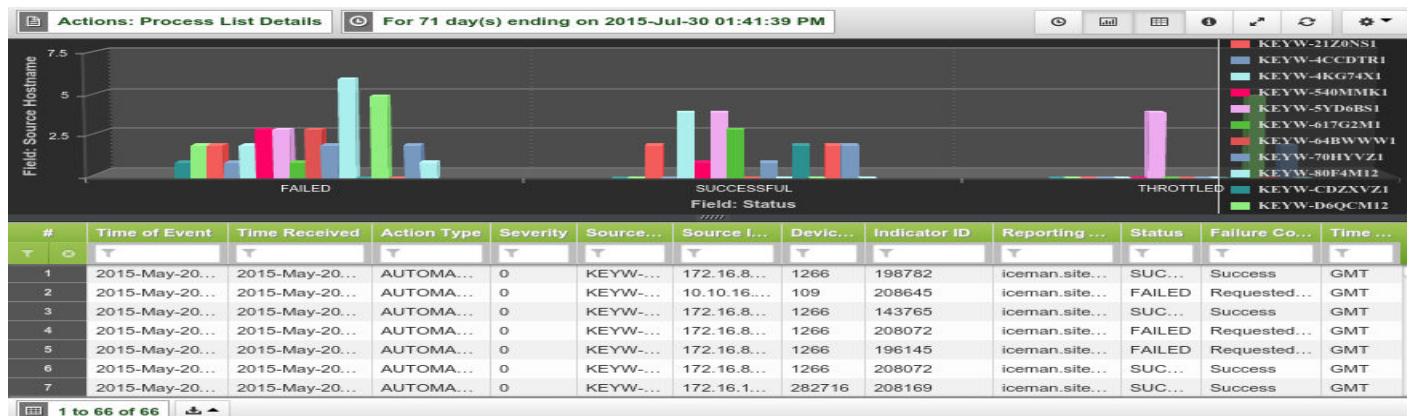
Actions: Process List Details

Details a process listing in which infected hosts were detected.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none">• AUTOMATIC• MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Failure Code	Shows an error code if the action is failed
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Actions: Process List Investigation

Details a file list for investigation in which infected hosts were detected during a process.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none">• AUTOMATIC• MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Failure Code	Shows an error code if the action is failed.
Time Zone	Time zone in which the event occurred

EXAMPLE

Actions: Process List Investigation													
For 90 day(s) ending on 2015-Jul-31 09:53:22 AM													
#	Time of Event	Time Received	Action Type	Severity	Source H...	Source IP...	Device ID	Indicator ID	Repo...	Status	Failure Code	Time ...	
1	2015-May-03...	2015-May-03...	AUTOMATIC	0	Unnamed: ...	172.16.70.1...	282902	164451	icem...	FAILED	Device not ...	GMT	
2	2015-May-03...	2015-May-03...	AUTOMATIC	0	Unnamed: ...	172.16.70.1...	282902	1875	icem...	FAILED	Device not ...	GMT	
3	2015-May-03...	2015-May-03...	AUTOMATIC	0	Unnamed: ...	172.16.70.1...	282902	189089	icem...	FAILED	Device not ...	GMT	
4	2015-May-03...	2015-May-03...	AUTOMATIC	0	Unnamed: ...	172.16.70.1...	282902	164451	icem...	THR...	Device not ...	GMT	
5	2015-May-03...	2015-May-03...	AUTOMATIC	0	Unnamed: ...	172.16.70.1...	282902	1875	icem...	THR...	Device not ...	GMT	
6	2015-May-03...	2015-May-03...	AUTOMATIC	0	Unnamed: ...	172.16.2.220	282767	165735	icem...	FAILED	Device not ...	GMT	
7	2015-May-03...	2015-May-04...	AUTOMATIC	0	Unnamed: ...	172.16.2.220	282767	1884	icem...	FAILED	Device not ...	GMT	
8	2015-May-03...	2015-May-04...	AUTOMATIC	0	Unnamed: ...	172.16.2.220	282767	164483	icem...	FAILED	Device not ...	GMT	
9	2015-May-03...	2015-May-04...	AUTOMATIC	0	Unnamed: ...	172.16.2.220	282767	189541	icem...	FAILED	Device not ...	GMT	
10	2015-May-03...	2015-May-04...	AUTOMATIC	0	Unnamed: ...	172.16.2.220	282767	165735	icem...	THR...	Device not ...	GMT	

INTELLISCHEMIA VIEW

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Actions: Process List Summary

Details a summary list of infected hosts and the number of events in which infection was detected during a process.

COLUMNS

Columns	Description
Source Hostname	Name of the infected host
Count of Events	The number of events detected

EXAMPLE

#	Source Hostname	Count of Events
1	KEYW-MXL0381YD0	42
2	KEYW-GKBZVL1	36
3	KEYW-H13TWW1	25
4	KEYW-D6QCM12	20
5	KEYW-5YD6BS1	17
6	KEYW-3783L12	13
7	KEYW-80F4M12	11
8	KEYW-4293L12	10
9	KEYW-G6NM2R1	9
10	KEYW-G52NHF1	8

1 to 39 of 39

INTELLISchema View

- None

Tables Referenced

- hexis_hawkeye_g_cef_syslogng

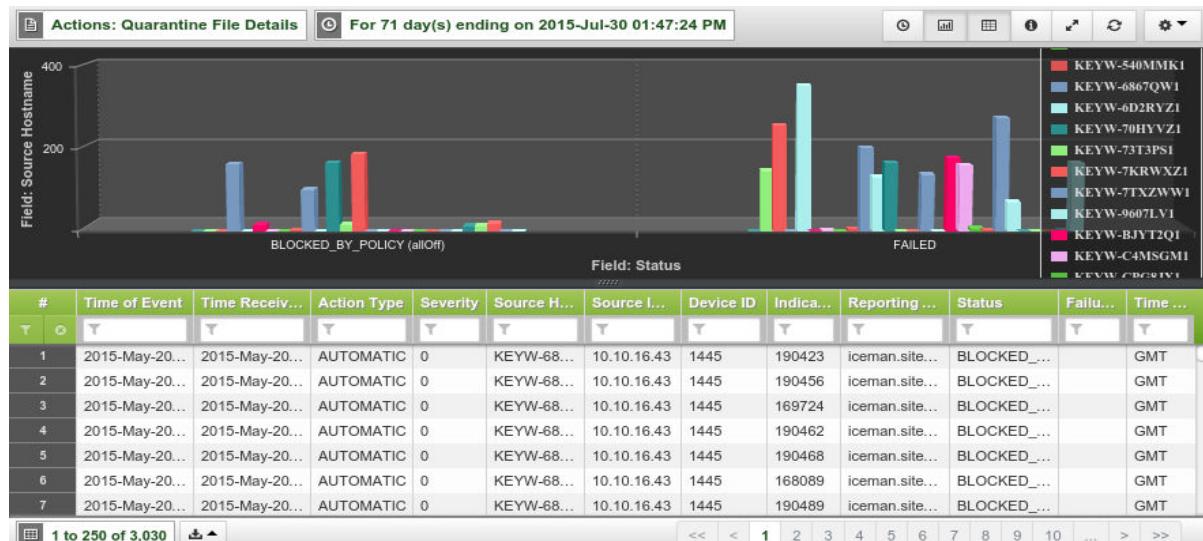
Actions: Quarantine File Details

Details quarantine file listing in which infected hosts were quarantined.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none"> AUTOMATIC MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Failure Code	Shows an error code if the action is failed
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Actions: Quarantine File Investigation

Details a file list for investigation of infected hosts that were quarantined.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: • AUTOMATIC • MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Failure Code	Shows an error code if the action is failed
Time Zone	Time zone in which the event occurred

EXAMPLE

Actions: Quarantine File Investigation														For 90 day(s) ending on 2015-Jul-31 09:57:12 AM	
#	Time of Event	Time Received	Action Type	Severity	Source H...	Source IP ...	Device ID	Indicator ID	Report...	Status	Failure Code	Time ...			
1	2015-May-05...	2015-May-05...	AUTOMA...	0	HANOVE...	172.16.7.10	73	175337	iceman...	BLO...				GMT	
2	2015-May-05...	2015-May-05...	AUTOMA...	0	HANOVE...	172.16.7.10	73	175342	iceman...	BLO...				GMT	
3	2015-May-05...	2015-May-05...	AUTOMA...	0	HANOVE...	172.16.7.10	73	188658	iceman...	BLO...				GMT	
4	2015-May-05...	2015-May-05...	AUTOMA...	0	HANOVE...	172.16.7.10	73	173600	iceman...	BLO...				GMT	
5	2015-May-05...	2015-May-05...	AUTOMA...	0	HANOVE...	172.16.7.10	73	175339	iceman...	BLO...				GMT	
6	2015-May-05...	2015-May-05...	AUTOMA...	0	HANOVE...	172.16.7.10	73	175348	iceman...	BLO...				GMT	
7	2015-May-05...	2015-May-05...	AUTOMA...	0	HANOVE...	172.16.7.10	73	175338	iceman...	BLO...				GMT	
8	2015-May-05...	2015-May-05...	AUTOMA...	0	HANOVE...	172.16.7.10	73	175345	iceman...	BLO...				GMT	
9	2015-May-05...	2015-May-05...	AUTOMA...	0	HANOVE...	172.16.7.10	73	175340	iceman...	BLO...				GMT	
10	2015-May-05...	2015-May-05...	AUTOMA...	0	HANOVE...	172.16.7.10	73	175335	iceman...	BLO...				GMT	

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Actions: Quarantine File Summary

Details a summary list of hosts and the number of events in which infected hosts were quarantined.

COLUMNS

Columns	Description
Source Hostname	Name of the infected host
Count of Events	The number of events detected

EXAMPLE

#	Source Hostname	Count of Events
1	KEYW-2VPTHK1	178456
2	KEYW-5NHHBW1	86405
3	KEYW-4GWXKM1	64915
4	KEYW-1LNYL12	60078
5	KEYW-F5CZBK1	59183
6	KEYW-2GYZ4S1	55088
7	KEYW-1607LV1	49419
8	KEYW-18B0HX1	49152
9	KEYW-1H3KPW1	48198
10	KEYW-29Z6HQ1	43376

1 to 185 of 185

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

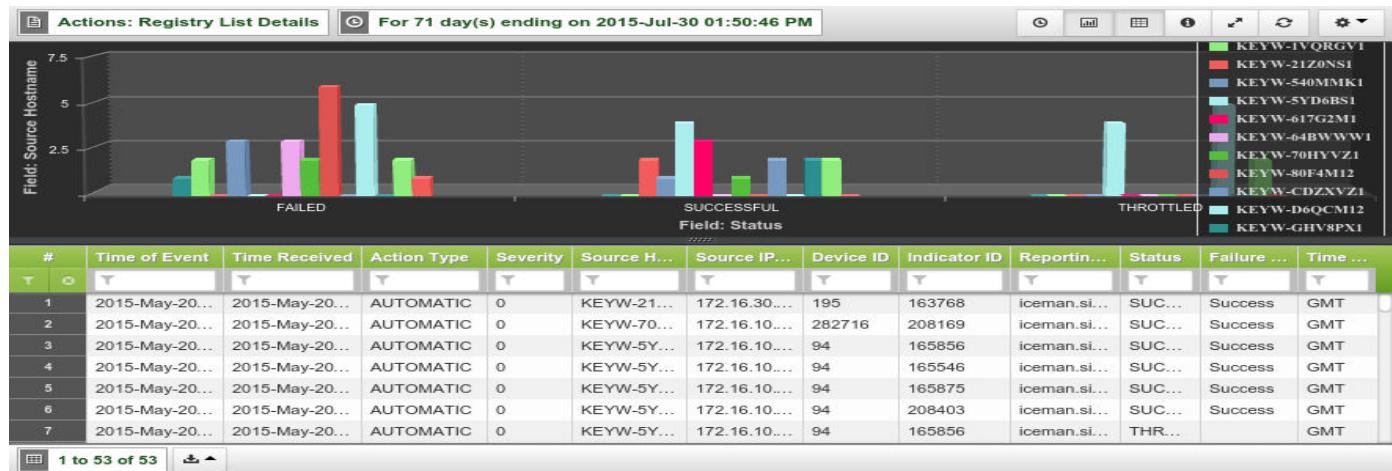
Actions: Registry List Details

Details registry file listing of infected hosts.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none"> AUTOMATIC MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Failure Code	Shows an error code if the action failed.
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Actions: Registry List Investigation

Details a registry file list for investigation of infected hosts.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none">• AUTOMATIC• MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Failure Code	Shows an error code if the action is failed
Time Zone	Time zone in which the event occurred

EXAMPLE

Actions: Registry List Investigation For 90 day(s) ending on 2015-Jul-01 03:17:42 PM												
#	Time of Event	Time Receiv...	Action Type	Seve...	Source Ho...	Source IP ...	Devi...	Indic...	Reporting ...	Status	Failu...	Time ...
1	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-BZF...	172.16.80.20	1261	173536	iceman.site...	THROTTLED		GMT
2	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-BZF...	172.16.80.20	1261	173536	iceman.site...	THROTTLED		GMT
3	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-BZF...	172.16.80.20	1261	173519	iceman.site...	SUCCESSFUL	Succ...	GMT
4	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-BZF...	172.16.80.20	1261	173519	iceman.site...	THROTTLED		GMT
5	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-BZF...	172.16.80.20	1261	173535	iceman.site...	FAILED	Requ...	GMT
6	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-BZF...	172.16.80.20	1261	173519	iceman.site...	SUCCESSFUL	Succ...	GMT
7	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-BZF...	172.16.80.20	1261	173536	iceman.site...	SUCCESSFUL	Succ...	GMT
8	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-BZF...	172.16.80.20	1261	173535	iceman.site...	SUCCESSFUL	Succ...	GMT
9	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-BZF...	172.16.80.20	1261	173534	iceman.site...	SUCCESSFUL	Succ...	GMT
10	2015-May-01...	2015-May-01...	AUTOMATIC	0	KEYW-BZF...	172.16.80.20	1261	173547	iceman.site...	SUCCESSFUL	Succ...	GMT

INTELLISchema View

- None

Tables Referenced

- hexis_hawkeye_g_cef_syslogng

Actions: Registry List Summary

Details a registry summary list of hosts and the number of events in which the host was infected.

COLUMNS

Columns	Description
Source Hostname	Name of the infected host
Count of Events	The number of events detected

EXAMPLE

#	Source Hostname	Count of Events
1	KEYW-MXL0381YD0	40
2	KEYW-GKBZVL1	32
3	KEYW-H13TWW1	24
4	KEYW-D6QCM12	20
5	KEYW-3783L12	13
6	KEYW-5YD6BS1	12
7	KEYW-4293L12	10
8	KEYW-G6NM2R1	9
9	KEYW-G52NHV1	8
10	KEYW-80042	6

1 to 37 of 37

INTELLISchema View

- None

Tables Referenced

- hexis_hawkeye_g_cef_syslogng

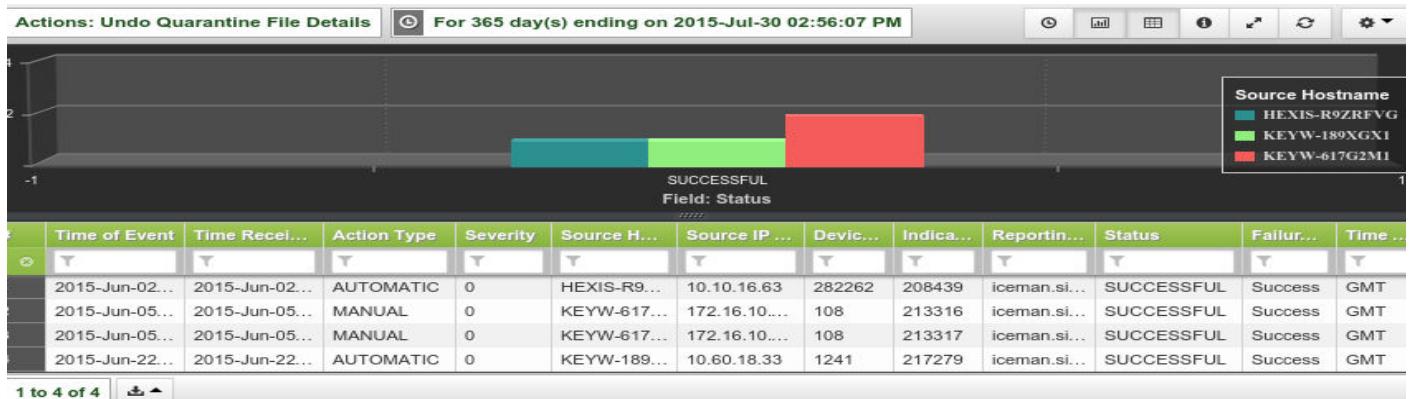
Actions: Undo Quarantine File Details

Details quarantine file listing of infected hosts that were undone.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none"> AUTOMATIC MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
Reporting Host	Name of the reporting host
Status	Result of the action
Failure Code	Shows an error code if the action is failed
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Actions: Undo Quarantine File Investigation

Details investigation file listing of infected hosts that were undone.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none">• AUTOMATIC• MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Indicator ID	ID of the event
MD5	The MD5 of the file
Reporting Host	Name of the reporting host
Status	Result of the action
Failure Code	Shows an error code if the action is failed
Time Zone	Time zone in which the event occurred

EXAMPLE

#		Time of Event	Time Received	Action Type	Seve...	Source H...	Source I...	Device ID	Indicator ID	MD5	Repo...	Status	Failure C...	Time ...
1		2015-Jun-02...	2015-Jun-02...	AUTOMA...	0	HEXIS-R...	10.10.16...	282262	208439		icem...	SUC...	Success	GMT
2		2015-Jun-05...	2015-Jun-05...	MANUAL	0	KEYW-61...	172.16.1...	108	213316		icem...	SUC...	Success	GMT
3		2015-Jun-05...	2015-Jun-05...	MANUAL	0	KEYW-61...	172.16.1...	108	213317		icem...	SUC...	Success	GMT
4		2015-Jun-22...	2015-Jun-22...	AUTOMA...	0	KEYW-18...	10.60.18...	1241	217279		icem...	SUC...	Success	GMT

1 to 4 of 4

INTELLISchema View

- None

Tables Referenced

- hexis_hawkeye_g_cef_syslogng

Actions: Undo Quarantine File Summary

A quarantine file summary list of infected hosts and number of events that were undone.

COLUMNS

Columns	Description
Source Hostname	Name of the infected host
Count of Events	The number of events detected

EXAMPLE

#	Source Hostname	Count of Events
1	KEYW-617G2M1	2
2	KEYW-189XGX1	1
3	KEYW-2J6CDP1	1
4	HEXIS-R9ZRFVG	1

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

ALL EVENTS MONITORING REPORTS

The All Events Monitoring reports group displays a file listing of event types for infected hosts and includes the following reports:

- “[All Events Details](#)”, next
- “[All Events Investigation](#)”, on page 385
- “[All Events Summary by Event Type](#)”, on page 387

All Events Details

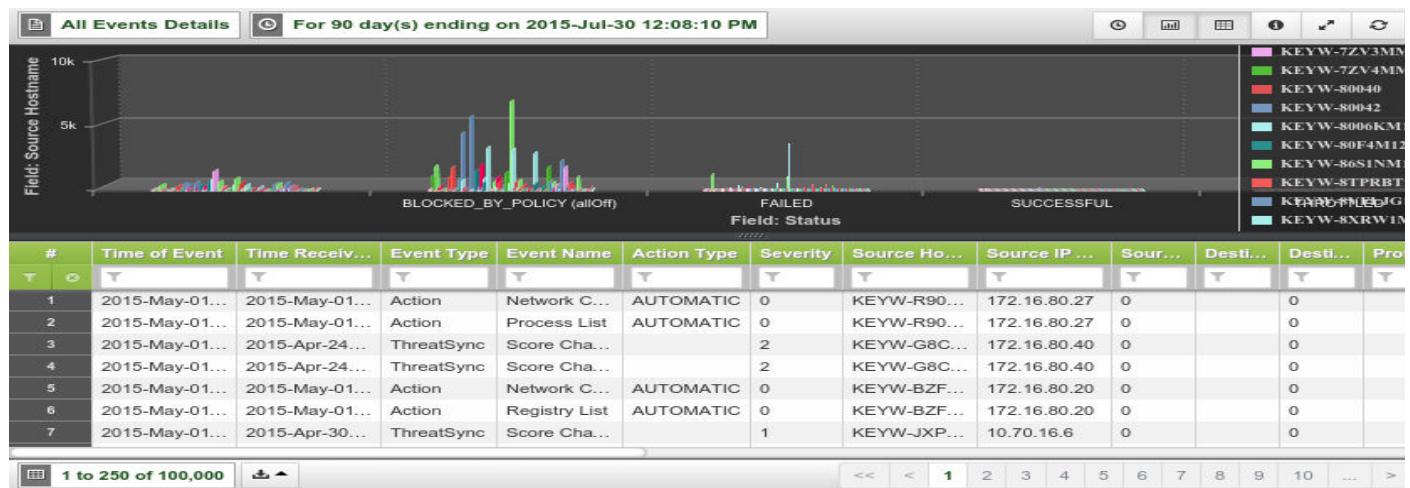
All events details of infected hosts.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Event Type	The event type, which can be one of the following: <ul style="list-style-type: none"> • ThreatSync • Indicators • Actions
Event Name	Name of the event
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none"> • AUTOMATIC • MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Source Port	Port of the infected host
Destination IP Address	The "bad" IP address
Destination Port	The "bad" IP destination port
Protocol	The transport protocol
Device ID	ID of the device
Process ID	ID of the process
DNS Domain	The requested DNS domain
DNS Rule Type	The type of rule
File Path	Full path to the file on the infected host
Command Line	The command line of the process
Indicator ID	ID of the event
MD5	MD5 of the file

Columns	Description
Packet Modified	Value "1" if HGNS modified the DNS response
Registry Value	Registry value whose data points to the matching file
Reporting Host	The name of the reporting host
Rule Match	The matched threat feed item
Status	The result of the action
Failure Code	Shows an error code if the action is failed
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

All Events Investigation

All events of infected hosts for investigation.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Event Type	The event type, which can be one of the following: <ul style="list-style-type: none"> • ThreatSync • Indicators • Actions
Event Name	Name of the event
Action Type	The action that was initiated, which can be one of the following: <ul style="list-style-type: none"> • AUTOMATIC • MANUAL
Severity	ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Source Port	Port of the infected host
Destination IP Address	The "bad" IP address
Destination Port	The "bad" IP destination port
Protocol	The transport protocol
Device ID	ID of the device
Process ID	ID of the process
DNS Domain	The requested DNS domain
DNS Rule Type	The type of rule
File Path	Full path to the file on the infected host
Command Line	The command line of the process
Indicator ID	ID of the event
MD5	MD5 of the file
Packet Modified	Value "1" if HGNS modified the DNS response
Registry Value	Registry value whose data points to the matching file
Reporting Host	The name of the reporting host
Rule Match	The matched threat feed item
Status	The result of the action
Failure Code	Shows an error code if the action is failed
Time Zone	Time zone in which the event occurred

EXAMPLE

All Events Investigation For 90 day(s) ending on 2015-Jul-31 10:09:05 AM

#	Time of Event	Time Received	Event T...	Event N...	Action	Seve...	Source H...	Source...	Source...	Desti...	Desti...	Proto...	Devi...	Proc...
1	2015-May-1...	2015-May-14...	Action	Kill Proc...	MANU...	0	KEYW-G...	10.60.1...	0			0		263
2	2015-May-1...	2015-May-14...	Action	Quarant...	MANU...	0	KEYW-G...	10.60.1...	0			0		263
3	2015-May-1...	2015-May-14...	Action	Quarant...	MANU...	0	KEYW-F5...	10.60.1...	0			0		206
4	2015-May-1...	2015-May-14...	Action	Kill Proc...	MANU...	0	KEYW-F5...	10.60.1...	0			0		206
5	2015-May-1...	2015-May-14...	Action	Kill Proc...	MANU...	0	KEYW-F5...	10.60.1...	0			0		206
6	2015-May-1...	2015-May-14...	Action	Kill Proc...	MANU...	0	KEYW-F5...	10.60.1...	0			0		206
7	2015-May-1...	2015-May-14...	Action	Kill Proc...	MANU...	0	KEYW-F5...	10.60.1...	0			0		206
8	2015-May-0...	2015-May-02...	Action	Quarant...	AUTO...	0	KEYW-86...	10.60.1...	0			0		904
9	2015-May-0...	2015-May-02...	Action	Quarant...	AUTO...	0	KEYW-86...	10.60.1...	0			0		904
10	2015-May-0...	2015-May-02...	Action	Quarant...	AUTO...	0	KEYW-86...	10.60.1...	0			0		904

1 to 250 of 408,017 << < 1 2 3 4 5 6 7 8 9 10 ... > >>

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

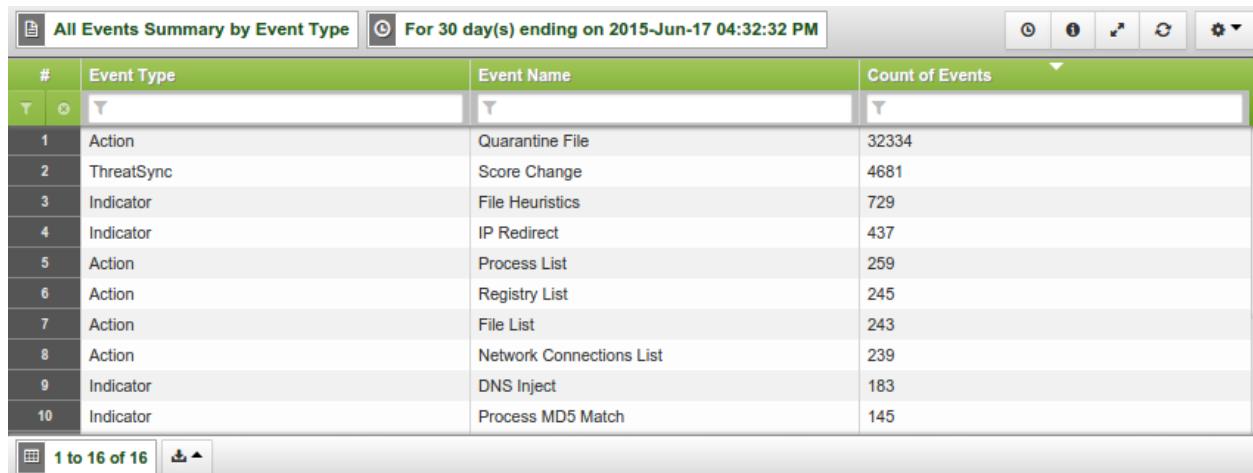
All Events Summary by Event Type

A summary list of all events by event type.

COLUMNS

Columns	Description
Event Type	The event type, which can be one of the following: <ul style="list-style-type: none">• ThreatSync• Indicators• Actions
Event Name	Name of the event
Count of Events	The number of events detected

EXAMPLE



The screenshot shows a software interface for viewing event data. At the top, there are two tabs: 'All Events Summary by Event Type' and 'For 30 day(s) ending on 2015-Jun-17 04:32:32 PM'. Below the tabs is a toolbar with various icons. The main area is a table with four columns: '#', 'Event Type', 'Event Name', and 'Count of Events'. The table contains 10 rows of data. The data is as follows:

#	Event Type	Event Name	Count of Events
1	Action	Quarantine File	32334
2	ThreatSync	Score Change	4681
3	Indicator	File Heuristics	729
4	Indicator	IP Redirect	437
5	Action	Process List	259
6	Action	Registry List	245
7	Action	File List	243
8	Action	Network Connections List	239
9	Indicator	DNS Inject	183
10	Indicator	Process MD5 Match	145

At the bottom left, there is a pagination control showing '1 to 16 of 16'.

INTELLISchema VIEW

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

DEVICE THREATSYNC MONITORING REPORTS

The Device ThreatSync Monitoring reports group displays a file listing of ThreatSync score changes on infected hosts and includes the following reports:

- “Device ThreatSync Score Changes Details”, next
- “Device ThreatSync Score Changes Investigation”, on page 390
- “Device ThreatSync Score Changes Summary by Host”, on page 391

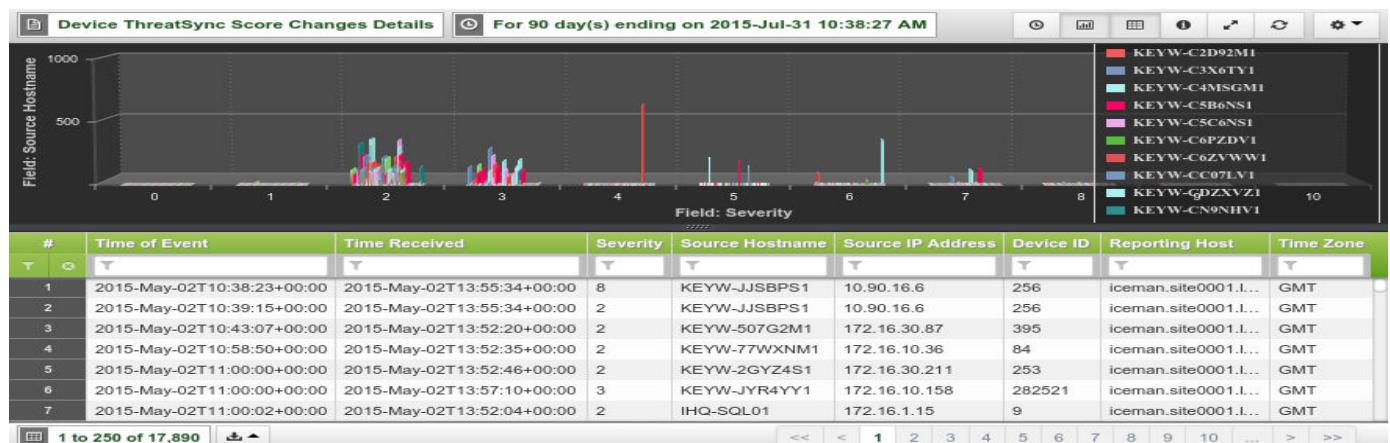
Device ThreatSync Score Changes Details

Details devices with ThreatSync Score changes.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The device's current score
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Device ThreatSync Score Changes Investigation

Details devices with ThreatSync Score changes for investigation.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The device's current score
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE

Device ThreatSync Score Changes Investigation									
For 90 day(s) ending on 2015-Jul-31 10:12:41 AM									
#	Time of Event	Time Received	Severity	Source Hostname	Source IP Address	Device ID	Reporting Host	Time Zone	
1	2015-May-02T10:16:28+00:00	2015-May-02T13:51:55+00:00	2	DAYT-DC01	10.50.10.10	285993	iceman.site000...	GMT	
2	2015-May-02T10:16:34+00:00	2015-May-02T13:51:42+00:00	2	ihq-avamardl	172.16.1.104	283239	iceman.site000...	GMT	
3	2015-May-02T10:26:39+00:00	2015-May-02T13:56:12+00:00	2	KEYW-36HFQW1	172.16.30.98	227	iceman.site000...	GMT	
4	2015-May-02T10:26:47+00:00	2015-May-02T13:51:38+00:00	2	KEYW-64PLN12	172.16.10.89	285148	iceman.site000...	GMT	
5	2015-May-02T10:33:57+00:00	2015-May-02T13:56:12+00:00	2	KEYW-36HFQW1	172.16.30.98	227	iceman.site000...	GMT	
6	2015-May-02T10:34:30+00:00	2015-May-02T14:22:00+00:00	3	KEYW-73T3PS1	172.16.30.85	1075	iceman.site000...	GMT	
7	2015-May-02T10:34:32+00:00	2015-May-02T13:51:49+00:00	2	NAFLD-DC01	10.100.10.10	282747	iceman.site000...	GMT	
8	2015-May-02T10:34:42+00:00	2015-May-02T13:56:12+00:00	2	KEYW-36HFQW1	172.16.30.98	227	iceman.site000...	GMT	
9	2015-May-02T10:38:23+00:00	2015-May-02T13:55:34+00:00	8	KEYW-JJSBPS1	10.90.16.6	256	iceman.site000...	GMT	
10	2015-May-02T10:39:15+00:00	2015-May-02T13:55:34+00:00	2	KEYW-JJSBPS1	10.90.16.6	256	iceman.site000...	GMT	

INTELLISchema View

- None

Tables Referenced

- hexis_hawkeye_g_cef_syslogng

Device ThreatSync Score Changes Summary by Host

Summary of devices with ThreatSync Score changes by host.

COLUMNS

Columns	Description
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Count of Events	The number of events with ThreatSync score changes detected

EXAMPLE

#	Source Hostname	Source IP Address	Count of Events
1	Unnamed: 172.16.1.125	172.16.1.125	636
2	KEYW-4GWXKM1	172.16.30.26	366
3	KEYW-JT33SW1	172.16.10.46	354
4	Unnamed: 192.168.1.232	192.168.1.232	338
5	KEYW-6KKYVZ1	10.10.16.39	337
6	KEYW-18B0HX1	172.16.30.11	325
7	KEYW-JT3CSW1	172.16.10.55	295
8	KEYW-5TXZWW1	10.100.16.58	293
9	TCOCHRAN	172.16.30.80	277
10	KEYW-CDZXVZ1	10.70.16.2	259

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

HEURISTICS MONITORING ACTIVITY

The Heuristics Monitoring Activity reports group displays contains the following reports:

- “[Heuristics: File Details](#)”, next
- “[Heuristics: File Investigation](#)”, on page 394
- “[Heuristics: File Top 100 Summary](#)”, on page 395
- “[Heuristics: Process Details](#)”, on page 396
- “[Heuristics: Process Investigation](#)”, on page 397
- “[Heuristics: Process Summary](#)”, on page 398
- “[Heuristics: Registry Details](#)”, on page 399
- “[Heuristics: Registry Investigation](#)”, on page 400
- “[Heuristics: Registry Summary](#)”, on page 401

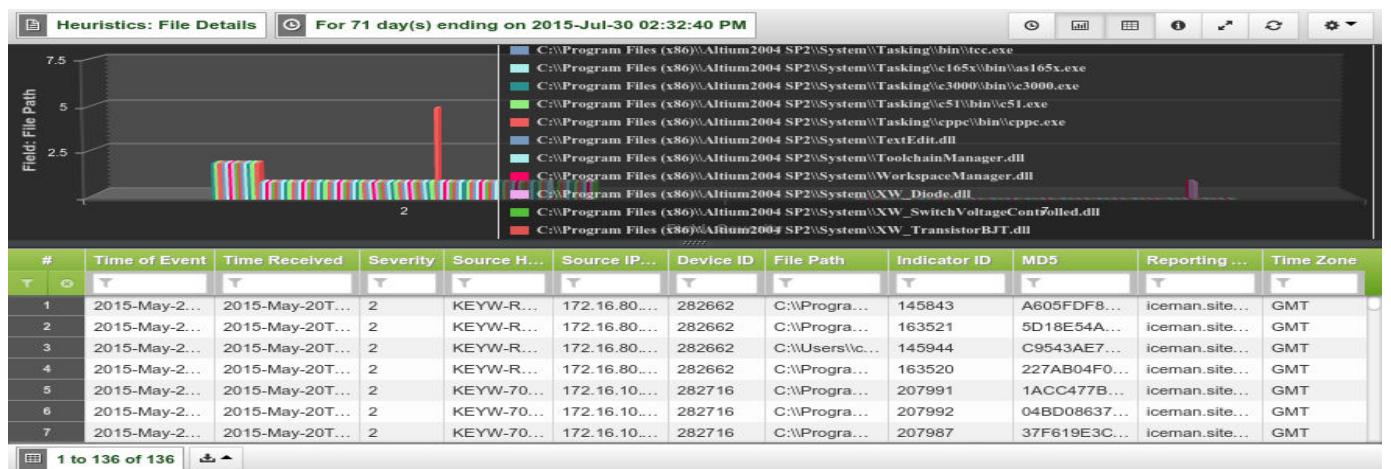
Heuristics: File Details

Details heuristics of infected hosts.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HaewkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

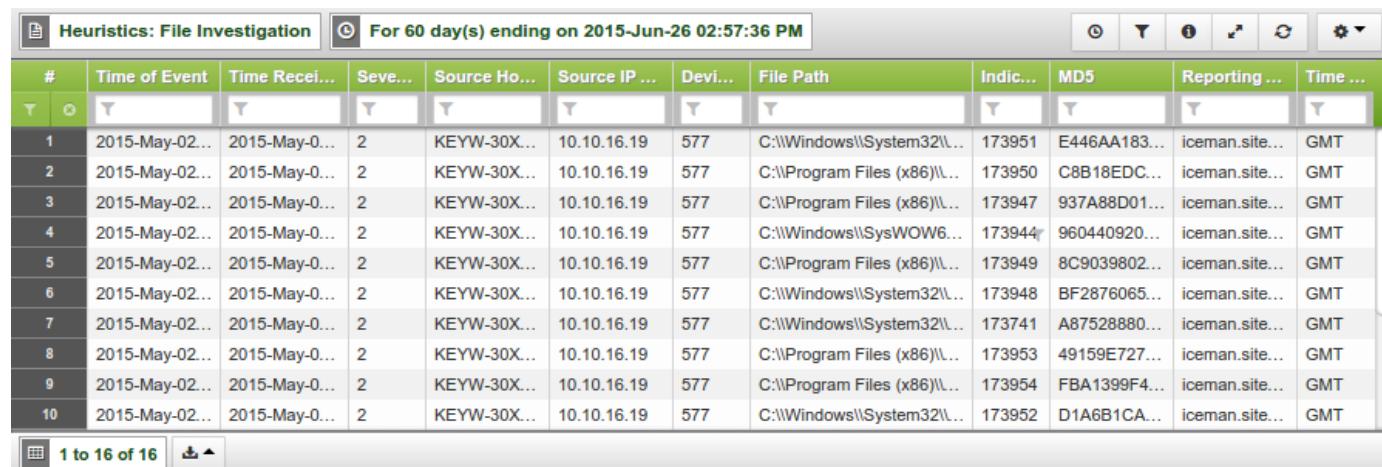
Heuristics: File Investigation

Details heuristics of infected hosts for investigation

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	ID of the device
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



The screenshot shows a database query results page titled "Heuristics: File Investigation" with a search filter "For 60 day(s) ending on 2015-Jun-26 02:57:36 PM". The table has 13 columns: #, Time of Event, Time Recei..., Seve..., Source Ho..., Source IP..., Devi..., File Path, Indic..., MD5, Reporting ..., and Time The data consists of 10 rows of event details, such as file paths like C:\Windows\System32\... and MD5 values like E446AA183... and FBA1399F4... . The bottom of the screen shows navigation controls and a message "1 to 16 of 16".

#	Time of Event	Time Recei...	Seve...	Source Ho...	Source IP...	Devi...	File Path	Indic...	MD5	Reporting ...	Time ...
1	2015-May-02...	2015-May-0...	2	KEYW-30X...	10.10.16.19	577	C:\Windows\System32\...	173951	E446AA183...	iceman.site...	GMT
2	2015-May-02...	2015-May-0...	2	KEYW-30X...	10.10.16.19	577	C:\Program Files (x86)\...	173950	C8B18EDC...	iceman.site...	GMT
3	2015-May-02...	2015-May-0...	2	KEYW-30X...	10.10.16.19	577	C:\Program Files (x86)\...	173947	937A88D01...	iceman.site...	GMT
4	2015-May-02...	2015-May-0...	2	KEYW-30X...	10.10.16.19	577	C:\Windows\SysWOW6...	173944	960440920...	iceman.site...	GMT
5	2015-May-02...	2015-May-0...	2	KEYW-30X...	10.10.16.19	577	C:\Program Files (x86)\...	173949	8C9039802...	iceman.site...	GMT
6	2015-May-02...	2015-May-0...	2	KEYW-30X...	10.10.16.19	577	C:\Windows\System32\...	173948	BF2876065...	iceman.site...	GMT
7	2015-May-02...	2015-May-0...	2	KEYW-30X...	10.10.16.19	577	C:\Windows\System32\...	173741	A87528880...	iceman.site...	GMT
8	2015-May-02...	2015-May-0...	2	KEYW-30X...	10.10.16.19	577	C:\Program Files (x86)\...	173953	49159E727...	iceman.site...	GMT
9	2015-May-02...	2015-May-0...	2	KEYW-30X...	10.10.16.19	577	C:\Program Files (x86)\...	173954	FBA1399F4...	iceman.site...	GMT
10	2015-May-02...	2015-May-0...	2	KEYW-30X...	10.10.16.19	577	C:\Windows\System32\...	173952	D1A6B1CA...	iceman.site...	GMT

INTELLISchema View

- None

Tables Referenced

- hexis_hawkeye_g_cef_syslogng

Heuristics: File Top 100 Summary

Summary of heuristics for top 100 Summary infected hosts.

COLUMNS

Columns	Description
File Path	The full path to the file.
Counts of Events	Represents the number of events

EXAMPLE

The screenshot shows a software interface titled "Heuristics: File Top 100 Summary". At the top, there is a filter bar indicating "For 30 day(s) ending on 2015-Jun-19 02:43:31 PM". Below the filter bar is a table with two columns: "# File Path" and "Count of Events". The table lists the top 10 files with their respective event counts. The first entry is "C:\Program Files (x86)\Google\Chrome\Application\42.0.2311.90\chrome..." with 5 events. The last entry is "C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\plug_ins\Checkers.api" with 2 events. At the bottom left of the table area, there is a pagination control showing "1 to 100 of 100".

#	File Path	Count of Events
1	C:\Program Files (x86)\Google\Chrome\Application\42.0.2311.90\chrome...	5
2	C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\plug_ins\Compare.api	2
3	C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\plug_ins\DVVA.api	2
4	C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\plug_ins\DistillerPI.api	2
5	C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\plug_ins\ImageConv...	2
6	C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\plug_ins\Scan.api	2
7	C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\plug_ins\XPS2PDF.api	2
8	C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\plug_ins\reflow.api	2
9	C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\plug_ins\Checkers.api	2
10	C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\plug_ins\MakeAcces...	2

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

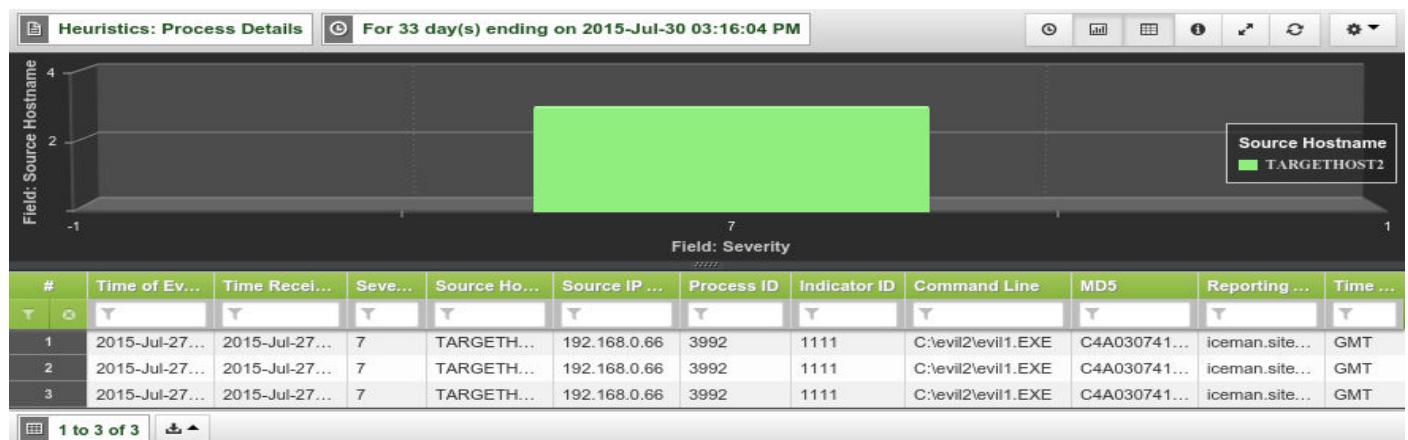
Heuristics: Process Details

Details of process heuristics for infected hosts.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Process ID	ID of the process
Indicator ID	The ID of the event
Command Line	The command line of the process
MD5	The MD5 of the file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Heuristics: Process Investigation

Details of process heuristics of infected hosts for investigation.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Process ID	ID of the process
Indicator ID	The ID of the event
MD5	The MD5 of the file
Command Line	The command line of the process
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE

#	Time of Event	Time Receiv...	Severity	Source Hos...	Source IP...	Process ID	Indicator ID	MD5	Command Line	Reporting ...	Time ...
1	2015-Jul-27...	2015-Jul-27...	7	TARGETHO...	192.168.0....	3992	1111	C4A030741...	C:\levil2\levil1.EXE	iceman.site...	GMT
2	2015-Jul-27...	2015-Jul-27...	7	TARGETHO...	192.168.0....	3992	1111	C4A030741...	C:\levil2\levil1.EXE	iceman.site...	GMT
3	2015-Jul-27...	2015-Jul-27...	7	TARGETHO...	192.168.0....	3992	1111	C4A030741...	C:\levil2\levil1.EXE	iceman.site...	GMT

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Heuristics: Process Summary

Summary of process heuristics for infected hosts.

COLUMNS

Columns	Description
Process ID	ID of the process
Count of Events	The number of events

EXAMPLE

#	Process ID	Count of Events
1	3992	3

INTELLISchema View

- None

Tables Referenced

- hexis_hawkeye_g_cef_syslogng

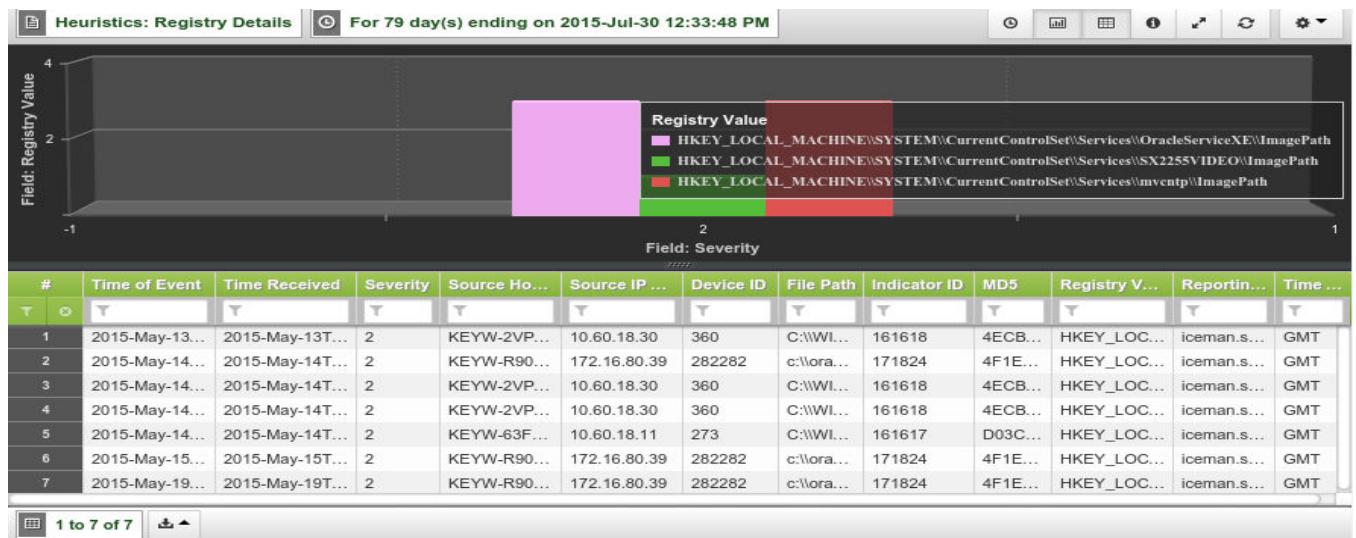
Heuristics: Registry Details

Details of registry heuristics for infected hosts.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of infected host
Device ID	ID of the device
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Registry Value	The registry whose data points to the matching file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

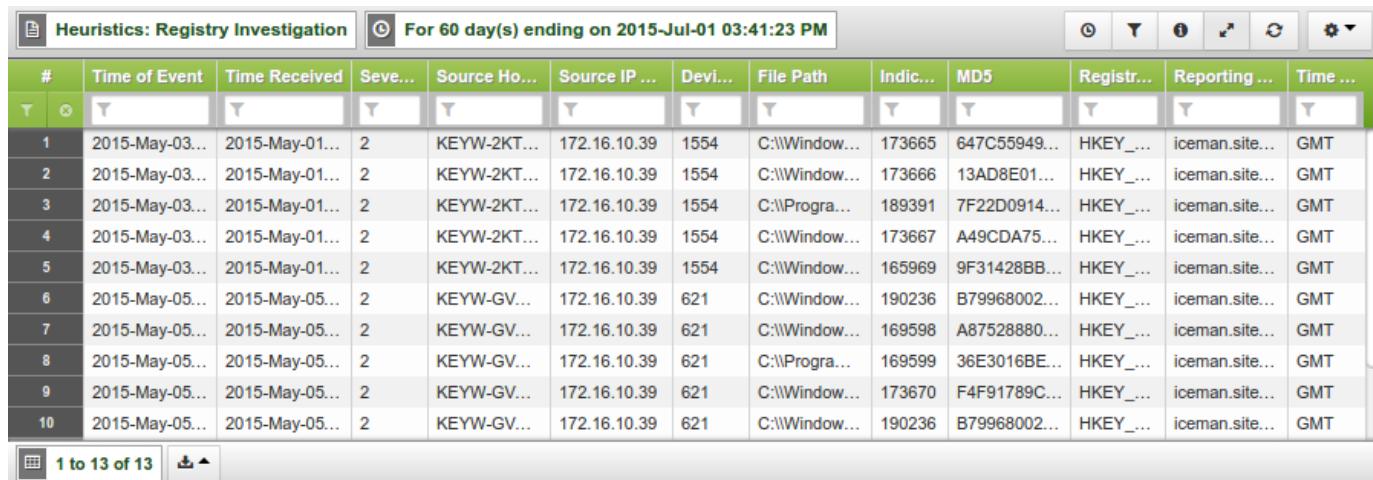
Heuristics: Registry Investigation

Details of registry heuristics of infected hosts for investigation.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP device address of infected host
Device ID	ID of the device
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Registry Value	The registry whose data points to the matching file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



The screenshot shows a database grid titled "Heuristics: Registry Investigation" with a search filter "For 60 day(s) ending on 2015-Jul-01 03:41:23 PM". The grid has 14 columns: #, Time of Event, Time Received, Seve..., Source Ho..., Source IP ..., Devi..., File Path, Indic..., MD5, Registr..., Reporting..., and Time The data consists of 10 rows of registry investigation details, including file paths like C:\Windows\Temp\keyw-2kt... and MD5 values such as A49CDA75... and F4F91789C... . The reporting host is listed as iceman.site... and the time zone is GMT for all entries.

#	Time of Event	Time Received	Seve...	Source Ho...	Source IP ...	Devi...	File Path	Indic...	MD5	Registr...	Reporting...	Time ...
1	2015-May-03...	2015-May-01...	2	KEYW-2KT...	172.16.10.39	1554	C:\Windows\...	173665	647C55949...	HKEY_...	iceman.site...	GMT
2	2015-May-03...	2015-May-01...	2	KEYW-2KT...	172.16.10.39	1554	C:\Windows\...	173666	13AD8E01...	HKEY_...	iceman.site...	GMT
3	2015-May-03...	2015-May-01...	2	KEYW-2KT...	172.16.10.39	1554	C:\Program...	189391	7F22D0914...	HKEY_...	iceman.site...	GMT
4	2015-May-03...	2015-May-01...	2	KEYW-2KT...	172.16.10.39	1554	C:\Windows\...	173667	A49CDA75...	HKEY_...	iceman.site...	GMT
5	2015-May-03...	2015-May-01...	2	KEYW-2KT...	172.16.10.39	1554	C:\Windows\...	165969	9F31428BB...	HKEY_...	iceman.site...	GMT
6	2015-May-05...	2015-May-05...	2	KEYW-GV...	172.16.10.39	621	C:\Windows\...	190236	B79968002...	HKEY_...	iceman.site...	GMT
7	2015-May-05...	2015-May-05...	2	KEYW-GV...	172.16.10.39	621	C:\Windows\...	169598	A87528880...	HKEY_...	iceman.site...	GMT
8	2015-May-05...	2015-May-05...	2	KEYW-GV...	172.16.10.39	621	C:\Program...	169599	3E63016BE...	HKEY_...	iceman.site...	GMT
9	2015-May-05...	2015-May-05...	2	KEYW-GV...	172.16.10.39	621	C:\Windows\...	173670	F4F91789C...	HKEY_...	iceman.site...	GMT
10	2015-May-05...	2015-May-05...	2	KEYW-GV...	172.16.10.39	621	C:\Windows\...	190236	B79968002...	HKEY_...	iceman.site...	GMT

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Heuristics: Registry Summary

Summary of registry heuristics for infected hosts.

COLUMNS

Columns	Description
Registry Value	The registry whose data points to the matching file
Count of Events	The number of events

EXAMPLE

The screenshot shows a software interface titled "Heuristics: Registry Summary". At the top, there is a search bar with the placeholder "For 60 day(s) ending on 2015-Jun-19 02:58:06 PM" and several filter and export icons. Below the search bar is a table with two columns: "# Registry Value" and "Count of Events". The table lists 10 registry entries, each with a numerical ID and a long registry key. The "Count of Events" column shows the number of events associated with each registry value. At the bottom of the table, there is a pagination indicator "1 to 175 of 175" and a small navigation icon.

#	Registry Value	Count of Events
1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrUsbSe...	493
2	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrUsbMd...	339
3	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\igfx\ima...	248
4	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WDC_S...	62
5	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IntcAzAu...	43
6	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\laksfridge...	29
7	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\hasplms\...	29
8	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\laksdf\lm...	29
9	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\hardlock\...	26
10	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrFillUp\...	20

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

EVENT INDICATOR ACTIVITY MONITORING REPORTS

The Event Indicator Activity Monitoring report group displays ID of events for infected hosts:

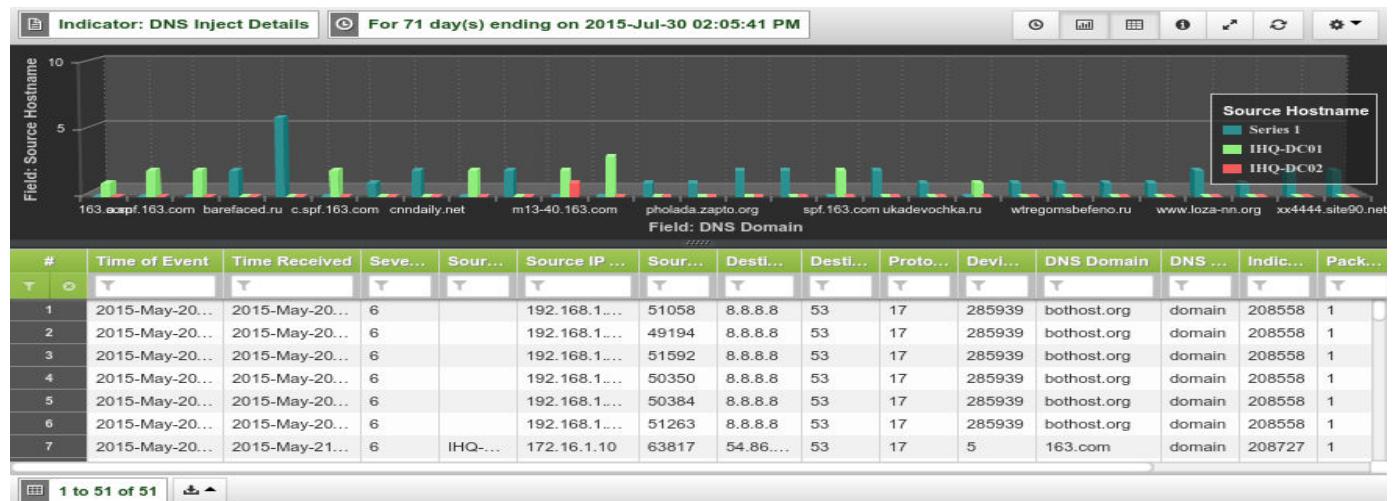
- “Indicator: DNS Inject Details”, next
- “Indicator: DNS Inject Investigation”, on page 405
- “Indicator: DNS Inject Summary”, on page 407
- “Indicator: IP Redirect Details”, on page 408
- “Indicator: IP Redirect Investigation”, on page 410
- “Indicator: IP Redirect Summary”, on page 412
- “Indicator: URL Match Details”, on page 413
- “Indicator: URL Match Investigation”, on page 414
- “Indicator: URL Match Top 100 Summary”, on page 415

Indicator: DNS Inject Details

Details DNS inject for infected hosts with specific event (Indicator) ID.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Source Port	Port of the infected host
Destination IP Address	Represents the IP address of the DNS server responsible for the "bad" domain
Destination Port	The destination port of the DNS server
Protocol	The transport protocol
Device ID	The ID of the device
DNS Domain	The requested domain
DNS Rule Type	The type of rule
Indicator ID	The ID of the event
Packet Modified	"1" if HGNS modified the DNS response
Reporting Host	The name of the reporting host
Rule Match	Rule match for the threat feed item
Time Zone	Time zone in which the event occurred

EXAMPLE*INTELLISchema View*

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Indicator: DNS Inject Investigation

Details DNS inject of infected hosts with specific event (Indicator) ID for investigation.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Source Port	Port of the infected host
Destination IP Address	Represents the IP address of the DNS server responsible for the "bad" domain
Destination Port	The destination port of the DNS server.
Protocol	The transport protocol
Device ID	The ID of the device
DNS Domain	The requested domain
DNS Rule Type	The type of rule
Indicator ID	The ID of the event
Packet Modified	"1" if HGNS modified the DNS response
Reporting Host	The name of the reporting host
Rule Match	Rule match for the threat feed item
Time Zone	Time zone in which the event occurred

EXAMPLE

Indicator: DNS Inject Investigation For 60 day(s) ending on 2015-Jun-30 11:08:55 AM														
#	Time of Event	Time Received	Seve...	Sour...	Source IP ...	Sour...	Desti...	Desti...	Proto...	Devi...	DNS Domain	DNS ...	Indic...	Pack...
1	2015-May-01...	2015-May-01...	6	VHQ...	172.16.8.10	56586	208.8...	53	17	74	www.secur...	domain	173548	1
2	2015-May-01...	2015-May-01...	6		192.168.1.2...	5235	192.3...	53	17	285939	www.321w...	domain	173555	1
3	2015-May-01...	2015-May-01...	6		192.168.1.2...	50354	8.8.8.8	53	17	285939	www.321w...	domain	173555	1
4	2015-May-01...	2015-May-01...	6		192.168.1.2...	50315	8.8.8.8	53	17	285939	www.321w...	domain	173555	1
5	2015-May-01...	2015-May-01...	6		192.168.1.2...	60335	192.5...	53	17	285939	www.321w...	domain	173555	1
6	2015-May-01...	2015-May-01...	6		192.168.1.2...	50354	8.8.4.4	53	17	285939	www.321w...	domain	173555	1
7	2015-May-01...	2015-May-01...	6		192.168.1.2...	50077	8.8.8.8	53	17	285939	apps.memo...	domain	173556	1
8	2015-May-01...	2015-May-01...	6		192.168.1.2...	49734	8.8.8.8	53	17	285939	apps.memo...	domain	173556	1
9	2015-May-01...	2015-May-01...	6		192.168.1.2...	50012	8.8.8.8	53	17	285939	www.321w...	domain	173555	1
10	2015-May-01...	2015-May-01...	6		100.100.1.2	31740	100.5...	53	17	285939	www.321w...	domain	173555	1

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Indicator: DNS Inject Summary

Summary of DNS injects for infected hosts with a specific Event (Indicator) ID.

COLUMNS

Columns	Description
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Count of Events	The number of events

EXAMPLE

#	Source Hostname	Source IP Address	Count of Events
1		192.168.1.232	595
2	IHQ-DC01	172.16.1.10	139
3	SEVERN-DC	172.16.3.200	12
4	NAFLD-DC01	10.100.10.10	4
5	VHQ-DC01	172.16.8.10	4
6	IHQ-DC02	172.16.1.11	2

INTELLISchema View

- None

Tables Referenced

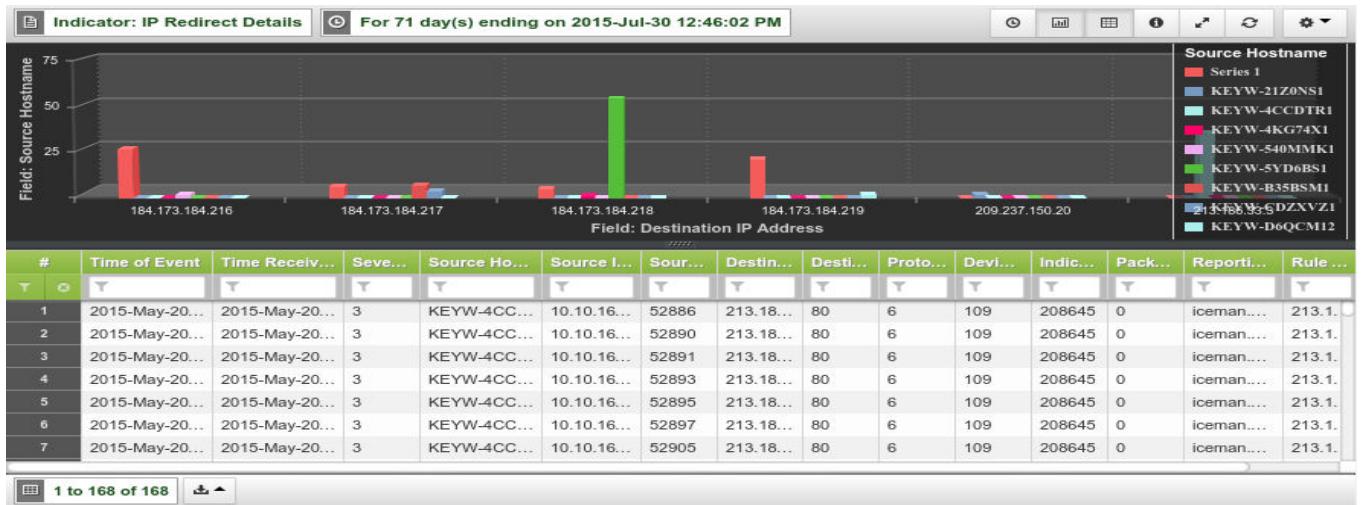
- hexis_hawkeye_g_cef_syslogng

Indicator: IP Redirect Details

Details IP redirect of infected hosts with specific event (Indicator) ID.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Source Port	Port of the infected host
Destination IP Address	The "bad" destination IP address.
Destination Port	The "bad" IP destination port.
Protocol	The transport protocol
Device ID	The ID of the device
Indicator ID	The ID of the event
Packet Modified	"1" if HGNS modified the DNS response
Reporting Host	The name of the reporting host
Rule Match	Rule match for the threat feed item
Time Zone	Time zone in which the event occurred

EXAMPLE**INTELLISchema View**

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Indicator: IP Redirect Investigation

Details IP redirect of infected hosts with specific event (Indicator) ID for investigation.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Source Port	Port of the infected host
Destination IP Address	The "bad" destination IP address.
Destination Port	The "bad" IP destination port.
Protocol	The transport protocol
Device ID	The ID of the device
Indicator ID	The ID of the event
Packet Modified	"1" if HGNS modified the DNS response
Reporting Host	The name of the reporting host
Rule Match	Rule match for the threat feed item
Time Zone	Time zone in which the event occurred

EXAMPLE

#		Time of Event	Time Received	Seve...	Sour...	Sour...	Desti...	Desti...	Proto...	Devi...	Indic...	Pack...	Repo...	Rule ...	Time ...
▼	○	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼
1		2015-May-1...	2015-May-14...	3	keyw...	172.1...	61285	184.1...	80	6	180	207250	0	icem...	184.1... GMT
2		2015-May-1...	2015-May-14...	3	keyw...	172.1...	61286	184.1...	80	6	180	207250	0	icem...	184.1... GMT
3		2015-May-1...	2015-May-14...	3	keyw...	172.1...	61188	184.1...	80	6	180	207250	0	icem...	184.1... GMT
4		2015-May-1...	2015-May-14...	3	keyw...	172.1...	61187	184.1...	80	6	180	207250	0	icem...	184.1... GMT
5		2015-May-0...	2015-May-06...	3	WCA...	172.1...	59117	217.1...	80	6	48	198326	0	icem...	217.1... GMT
6		2015-May-0...	2015-May-06...	3	WCA...	172.1...	59110	217.1...	80	6	48	198326	0	icem...	217.1... GMT
7		2015-May-0...	2015-May-06...	3	WCA...	172.1...	59119	217.1...	80	6	48	198326	0	icem...	217.1... GMT
8		2015-May-0...	2015-May-06...	3	WCA...	172.1...	59120	217.1...	80	6	48	198326	0	icem...	217.1... GMT
9		2015-May-0...	2015-May-06...	3	WCA...	172.1...	59121	217.1...	80	6	48	198326	0	icem...	217.1... GMT
10		2015-May-0...	2015-May-06...	3	WCA...	172.1...	59109	217.1...	80	6	48	198326	0	icem...	217.1... GMT

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Indicator: IP Redirect Summary

IP redirect summary of infected hosts with the number of events.

COLUMNS

Columns	Description
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Count of Events	The number of events

EXAMPLE

#	Source Hostname	Source IP Address	Count of Events
1	KEYW-5YD6BS1	172.16.10.39	1432
2	KEYW-5YD6BS1	172.16.10.44	1364
3	HEXIS-R902WP4L	10.10.16.49	483
4	KEYW-6QL8PX1	10.60.19.10	401
5	KEYW-5YD6BS1	172.16.10.34	374
6	KEYW-R900KX85	172.16.80.53	198
7	KEYW-MXL0381YD0	172.16.30.14	185
8	KEYW-D8GRYW1	172.16.30.101	102
9	KEYW-D6QCM12	172.16.80.21	92
10	KEYW-4KG74X1	172.16.80.52	57

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

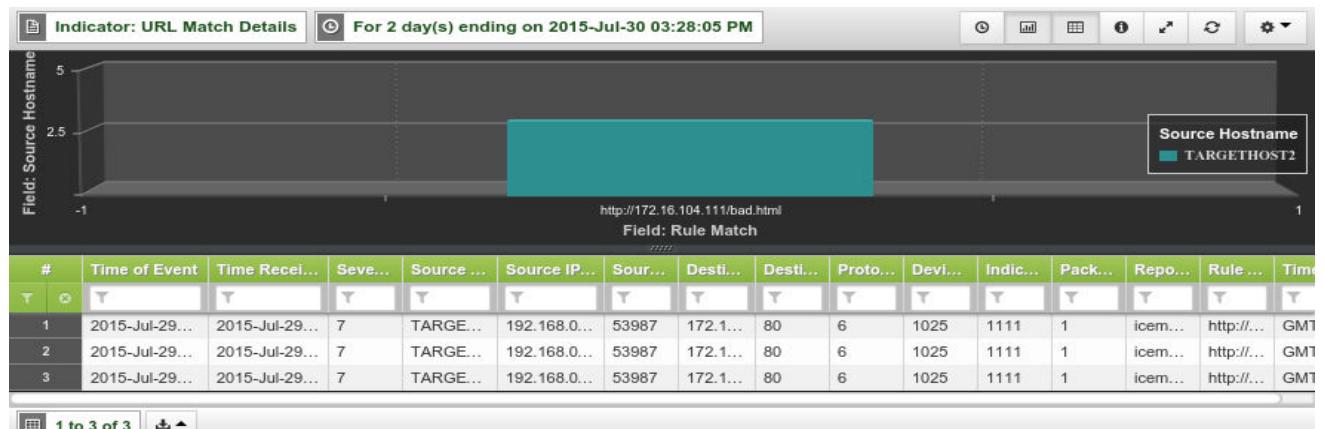
Indicator: URL Match Details

Details URL match (through rule) of infected hosts.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Source Port	Port of the infected host
Destination IP Address	The "bad" destination IP address.
Destination Port	The "bad" IP destination port.
Protocol	The transport protocol
Device ID	The ID of the device
Indicator ID	The ID of the event
Packet Modified	"1" if HGNS modified the DNS response
Reporting Host	The name of the reporting host
Rule Match	Rule match for the threat feed item
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Indicator: URL Match Investigation

Details URL match (through rule) of infected hosts for investigation.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Source Port	Port of the infected host
Destination IP Address	The "bad" destination IP address.
Destination Port	The "bad" IP destination port.
Protocol	The transport protocol
Device ID	The ID of the device
Indicator ID	The ID of the event
Packet Modified	"1" if HGNS modified the DNS response
Reporting Host	The name of the reporting host
Rule Match	Rule match for the threat feed item
Time Zone	Time zone in which the event occurred

EXAMPLE

#	Time of Event	Time Recei...	Seve...	Sour...	Sour...	Sour...	Desti...	Desti...	Proto...	Devi...	Indic...	Pack...	Repo...	Rule Ma...	Time ...
1	2015-Jul-29...	2015-Jul-29...	7	TAR...	192.1...	53987	172.1...	80	6	1025	1111	1	icem...	http://17...	GMT
2	2015-Jul-29...	2015-Jul-29...	7	TAR...	192.1...	53987	172.1...	80	6	1025	1111	1	icem...	http://17...	GMT
3	2015-Jul-29...	2015-Jul-29...	7	TAR...	192.1...	53987	172.1...	80	6	1025	1111	1	icem...	http://17...	GMT

1 to 3 of 3

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Indicator: URL Match Top 100 Summary

Summary of top 100 URL matches (through rule).

COLUMNS

Columns	Description
Rule Match	Rule match for the threat feed item
Count of Events	The number of events

EXAMPLE

#	Rule Match	Count of Events
1	http://172.16.104.111/bad.html	3

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

MIS POTENTIAL MONITORING REPORTS

The MIS Potential Activity Monitoring report group displays hosts that are experiencing a potential Malware Service infection.

- “[Malware Identification Service \(MIS\) Potential: File Details](#)”, next
- “[Malware Identification Service \(MIS\) Potential: File Investigation](#)”, on page 418
- “[Malware Identification Service \(MIS\) Potential: File Summary](#)”, on page 419
- “[Malware Identification Service \(MIS\) Potential: Process Details](#)”, on page 420
- “[Malware Identification Service \(MIS\) Potential: Process Investigation](#)”, on page 421
- “[Malware Identification Service \(MIS\) Potential: Process Summary](#)”, on page 422
- “[Malware Identification Service \(MIS\) Potential: Registry Details](#)”, on page 423
- “[Malware Identification Service \(MIS\) Potential: Registry Investigation](#)”, on page 424
- “[Malware Identification Service \(MIS\) Potential: Registry Summary](#)”, on page 425

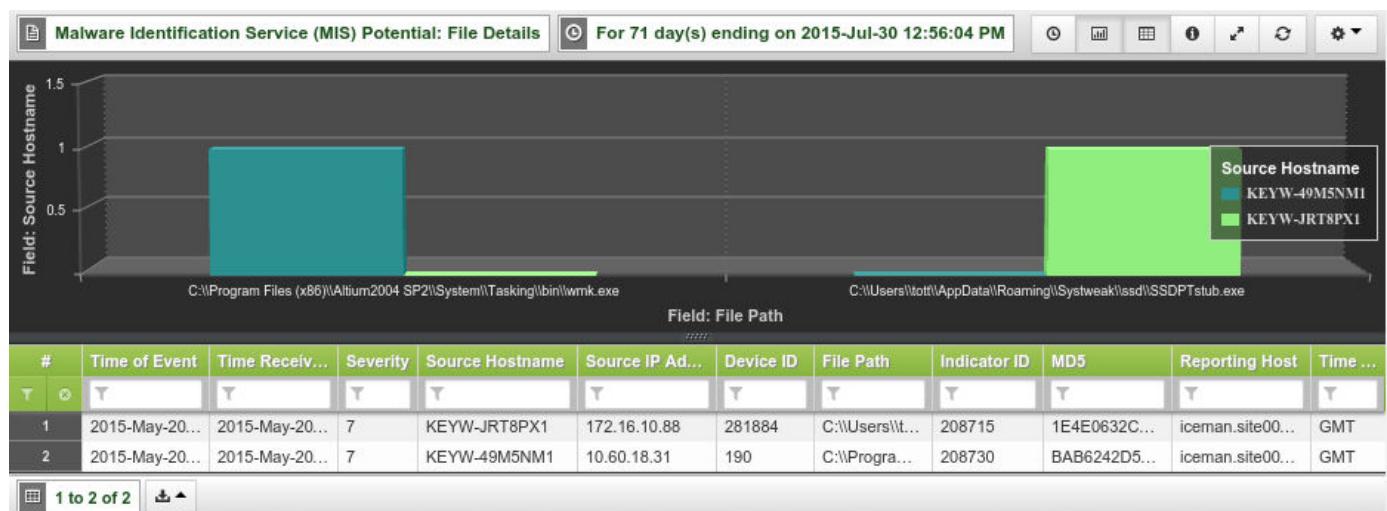
Malware Identification Service (MIS) Potential: File Details

Details file of hosts potentially infected from malware.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	The ID of the device
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Malware Identification Service (MIS) Potential: File Investigation

Details file of hosts potentially infected from malware for investigation.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	The ID of the device
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE

Malware Identification Service (MIS) Potential: File Investigation

For 60 day(s) ending on 2015-Jun-30 11:33:57 AM

#	Time of Event	Time Receiv...	Seve...	Source Hos...	Source IP ...	Devi...	File Path	Indic...	MD5	Reporting ...	Time ...
1	2015-May-12...	2015-May-12...	7	KEYW-JRT8...	172.16.10.84	281884	C:\Users\lott\AppData\Roami...	206383	E0DF66E7...	iceman.site...	GMT
2	2015-May-12...	2015-May-12...	7	KEYW-JRT8...	172.16.10.84	281884	C:\Users\lott\AppData\Roami...	206382	8229DB4E...	iceman.site...	GMT
3	2015-May-13...	2015-May-13...	7	KEYW-JRT8...	172.16.10.88	281884	C:\Users\lott\AppData\Roami...	206382	8229DB4E...	iceman.site...	GMT
4	2015-May-13...	2015-May-13...	7	KEYW-JRT8...	172.16.10.88	281884	C:\Users\lott\AppData\Roami...	206383	E0DF66E7...	iceman.site...	GMT
5	2015-May-14...	2015-May-14...	7	KEYW-JRT8...	172.16.10.79	281884	C:\Users\lott\AppData\Roami...	206383	E0DF66E7...	iceman.site...	GMT
6	2015-May-14...	2015-May-14...	7	KEYW-JRT8...	172.16.10.79	281884	C:\Users\lott\AppData\Roami...	207221	C134B8455...	iceman.site...	GMT
7	2015-May-14...	2015-May-14...	7	KEYW-JRT8...	172.16.10.79	281884	C:\Users\lott\AppData\Roami...	207222	34BA770E...	iceman.site...	GMT
8	2015-May-14...	2015-May-14...	7	KEYW-JRT8...	172.16.10.79	281884	C:\Users\lott\AppData\Roami...	206382	8229DB4E...	iceman.site...	GMT
9	2015-May-15...	2015-May-15...	7	KEYW-JRT8...	172.16.10.22	281884	C:\Users\lott\AppData\Roami...	207655	386B88945...	iceman.site...	GMT
10	2015-May-15...	2015-May-15...	7	KEYW-JRT8...	172.16.10.22	281884	C:\Users\lott\AppData\Roami...	207654	AAF42A00...	iceman.site...	GMT

1 to 13 of 13

INTELLISchema View

- None

Tables Referenced

- hexis_hawkeye_g_cef_syslogng

Malware Identification Service (MIS) Potential: File Summary

Summary file of hosts potentially infected from malware from a specific indicator (event ID).

COLUMNS

Columns	Description
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Count of Events	The number of events

EXAMPLE

#	File Path	Indicator ID	MD5	Count of Events
1	C:\Users\tott\AppData\Roaming\Sh...	206383	E0DF66E7A5654F956442DFF81009...	3
2	C:\Users\tott\AppData\Roaming\Sh...	206382	8229DB4E61BD119ACAC35FF83CC...	3
3	C:\Users\tott\AppData\Roaming\Sh...	207654	AAF42A00AE49E8B02E4DE14D8A85...	2
4	C:\Users\tott\AppData\Roaming\Sh...	207655	386B88945F182E98F7521A7F2D570...	2
5	C:\temp\From Thumbdrive\Intel Tuni...	207970	90DB0DC7F88A778B4937A776DA73...	2
6	C:\Windows\System32\drivers\b99...	207969	216D01CB247EF89248EB8E62CEC5...	1
7	C:\Program Files (x86)\Altium2004 S...	208730	BAB6242D52D254C849B93538F01F...	1
8	C:\Program Files (x86)\AskPartnerN...	206977	9882E67A4555EA41CF177051C2BA...	1
9	C:\Program Files\Trend Micro\Office...	207505	1F17DE38D656D38C1BB4C507EDF...	1
10	C:\Users\jhfox\Downloads\Internatio...	207764	482281CF2FA535E4E8EB06413F6...	1

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

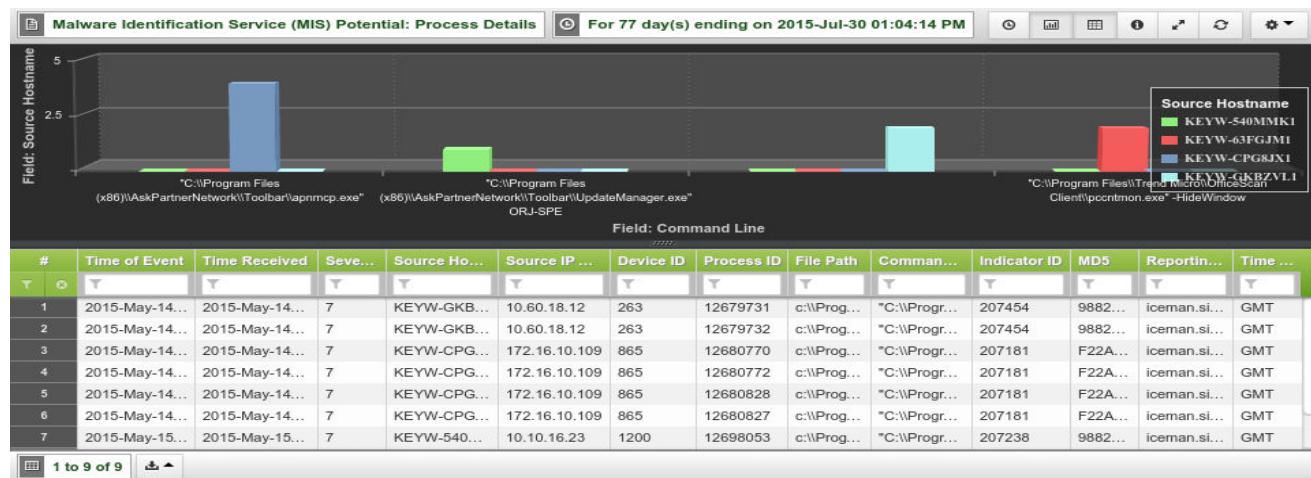
Malware Identification Service (MIS) Potential: Process Details

Details process (from command line) that occurred on infected hosts from malware.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	The ID of the device
Process ID	The ID of the process
File Path	The full path to the file on the infected host
Command Line	The command line of the process
Indicator ID	The ID of the event
MD5	The MD5 of the file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

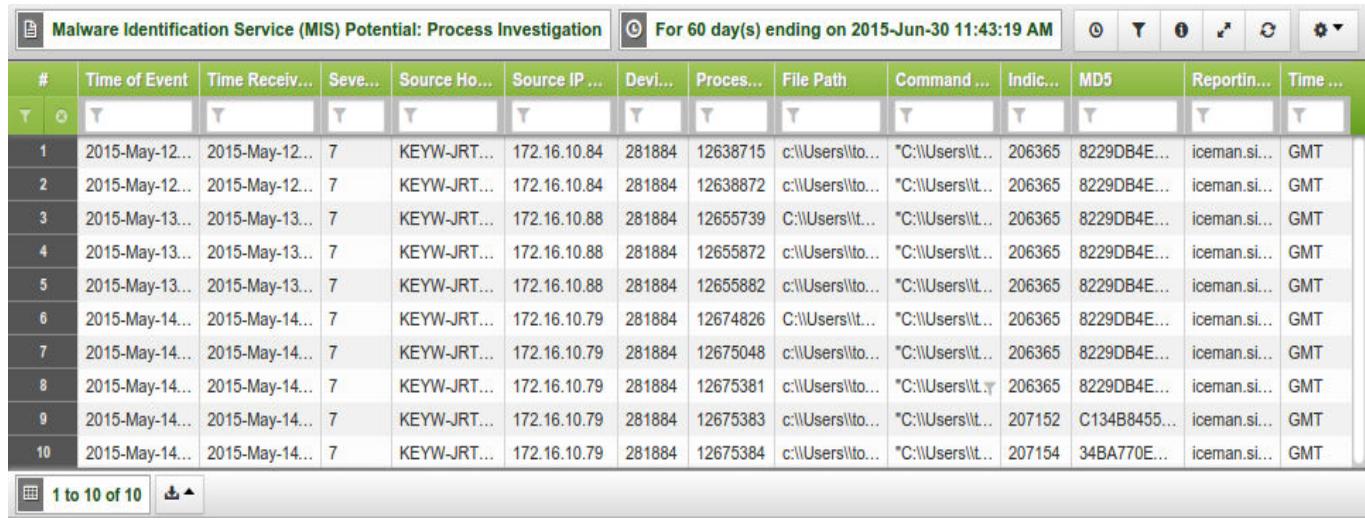
Malware Identification Service (MIS) Potential: Process Investigation

Details process (from command line) that occurred on infected hosts from malware for investigation (Process ID).

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	The ID of the device
Process ID	The ID of the process
File Path	The full path to the file on the infected host
Command Line	The command line of the process
Indicator ID	The ID of the event
MD5	The MD5 of the file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



The screenshot shows a database grid titled "Malware Identification Service (MIS) Potential: Process Investigation". A filter bar at the top indicates "For 60 day(s) ending on 2015-Jun-30 11:43:19 AM". The grid has 15 columns with headers: #, Time of Event, Time Receiv..., Seve..., Source Ho..., Source IP..., Devi..., Proces..., File Path, Command ..., Indic..., MD5, Reportin..., and Time The data consists of 10 rows of process details, such as file paths like "C:\Users\lto..." and command lines like "C:\Users\lto...". The last two columns show MD5 values and reporting host names.

#	Time of Event	Time Receiv...	Seve...	Source Ho...	Source IP...	Devi...	Proces...	File Path	Command ...	Indic...	MD5	Reportin...	Time ...
1	2015-May-12...	2015-May-12...	7	KEYW-JRT...	172.16.10.84	281884	12638715	c:\Users\lto...	"C:\Users\lto...	206365	8229DB4E...	iceman.si...	GMT
2	2015-May-12...	2015-May-12...	7	KEYW-JRT...	172.16.10.84	281884	12638872	c:\Users\lto...	"C:\Users\lto...	206365	8229DB4E...	iceman.si...	GMT
3	2015-May-13...	2015-May-13...	7	KEYW-JRT...	172.16.10.88	281884	12655739	C:\Users\lto...	"C:\Users\lto...	206365	8229DB4E...	iceman.si...	GMT
4	2015-May-13...	2015-May-13...	7	KEYW-JRT...	172.16.10.88	281884	12655872	c:\Users\lto...	"C:\Users\lto...	206365	8229DB4E...	iceman.si...	GMT
5	2015-May-13...	2015-May-13...	7	KEYW-JRT...	172.16.10.88	281884	12655882	c:\Users\lto...	"C:\Users\lto...	206365	8229DB4E...	iceman.si...	GMT
6	2015-May-14...	2015-May-14...	7	KEYW-JRT...	172.16.10.79	281884	12674826	C:\Users\lto...	"C:\Users\lto...	206365	8229DB4E...	iceman.si...	GMT
7	2015-May-14...	2015-May-14...	7	KEYW-JRT...	172.16.10.79	281884	12675048	c:\Users\lto...	"C:\Users\lto...	206365	8229DB4E...	iceman.si...	GMT
8	2015-May-14...	2015-May-14...	7	KEYW-JRT...	172.16.10.79	281884	12675381	c:\Users\lto...	"C:\Users\lto...	206365	8229DB4E...	iceman.si...	GMT
9	2015-May-14...	2015-May-14...	7	KEYW-JRT...	172.16.10.79	281884	12675383	c:\Users\lto...	"C:\Users\lto...	207152	C134B8455...	iceman.si...	GMT
10	2015-May-14...	2015-May-14...	7	KEYW-JRT...	172.16.10.79	281884	12675384	c:\Users\lto...	"C:\Users\lto...	207154	34BA770E...	iceman.si...	GMT

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Malware Identification Service (MIS) Potential: Process Summary

Process summary (file) on infected hosts from malware with the number of events

COLUMNS

Columns	Description
File Path	The full path to the file on the infected host
Count of Events	The number of events

EXAMPLE

The screenshot shows a software interface titled "Malware Identification Service (MIS) Potential: Process Summary". A status bar at the top indicates "For 90 day(s) ending on 2015-Jun-19 03:54:30 PM". The main area is a table with two columns: "# File Path" and "Count of Events". The table lists nine entries, each with a file path and its corresponding event count. The bottom of the interface shows navigation controls including a page number "1 to 9 of 9" and a search bar.

#	File Path	Count of Events
1	c:\Program Files (x86)\AskPartnerNetwork\Toolbar\apnmcp.exe	7
2	c:\Users\lott\AppData\Roaming\ShopAtHome\ShopAtHomeHelper\ShopAtHomeHel...	6
3	c:\Program Files (x86)\AskPartnerNetwork\Toolbar\UpdateManager.exe	4
4	c:\Program Files\AskPartnerNetwork\Toolbar\UpdateManager.exe	2
5	c:\Program Files\Trend Micro\OfficeScan Client\PccNTMon.exe	2
6	C:\Users\lott\AppData\Roaming\ShopAtHome\ShopAtHomeHelper\ShopAtHomeHel...	2
7	c:\Users\lott\AppData\Roaming\ShopAtHome\ShopAtHomeHelper\ShopAtHomeWat...	1
8	c:\Users\lott\AppData\Roaming\ShopAtHome\ShopAtHomeHelper\ShopAtHomeUpd...	1
9	C:\Program Files (x86)\AskPartnerNetwork\Toolbar\UpdateManager.exe	1

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

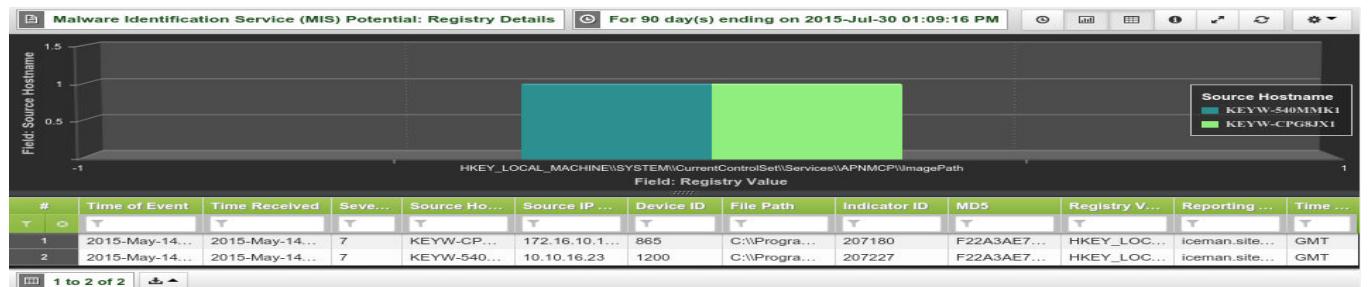
Malware Identification Service (MIS) Potential: Registry Details

Details registry of infected hosts from malware.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	The ID of the device
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Registry Value	The registry value whose data points to the matching file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

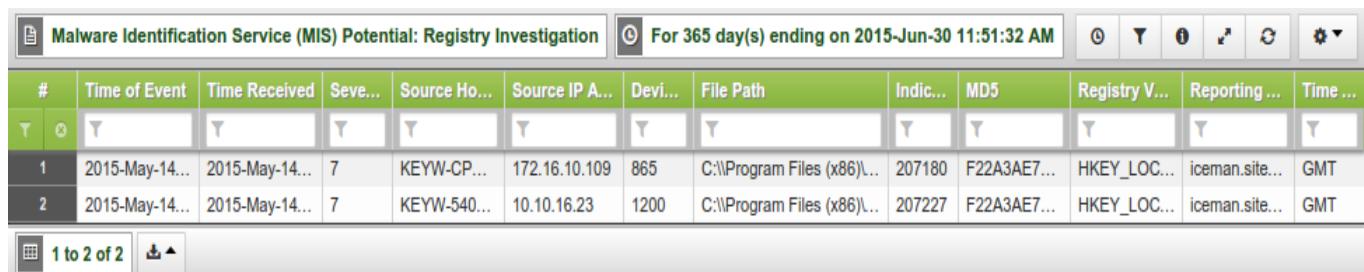
Malware Identification Service (MIS) Potential: Registry Investigation

Details registry of infected hosts from malware for investigation.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	The ID of the device
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Registry Value	The registry value whose data points to the matching file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



The screenshot shows a database query results page. The title bar says "Malware Identification Service (MIS) Potential: Registry Investigation" and the filter bar says "For 365 day(s) ending on 2015-Jun-30 11:51:32 AM". The table has 14 columns: #, Time of Event, Time Received, Seve..., Source Ho..., Source IP A..., Devi..., File Path, Indic..., MD5, Registry V..., Reporting ..., and Time There are two rows of data:

#	Time of Event	Time Received	Seve...	Source Ho...	Source IP A...	Devi...	File Path	Indic...	MD5	Registry V...	Reporting ...	Time ...
1	2015-May-14...	2015-May-14...	7	KEYW-CP...	172.16.10.109	865	C:\Program Files (x86)\...	207180	F22A3AE7...	HKEY_LOC...	iceman.site...	GMT
2	2015-May-14...	2015-May-14...	7	KEYW-540...	10.10.16.23	1200	C:\Program Files (x86)\...	207227	F22A3AE7...	HKEY_LOC...	iceman.site...	GMT

At the bottom left, it says "1 to 2 of 2".

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Malware Identification Service (MIS) Potential: Registry Summary

Summary registry of infected hosts from malware.

COLUMNS

Columns	Description
Registry Value	The registry value whose data points to the matching file
Count of Events	The number of events

EXAMPLE

The screenshot shows a software interface titled "Malware Identification Service (MIS) Potential: Registry Summary". At the top, it says "For 365 day(s) ending on 2015-Jul-01 04:06:34 PM". Below is a table with two columns: "# Registry Value" and "Count of Events". There is one row with the value "1 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\APNMCP\Imag..." and a count of "2". At the bottom left, it says "1 to 1 of 1".

#	Registry Value	Count of Events
1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\APNMCP\Imag...	2

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

THREAT MATCH MONITORING REPORTS

The Threat Match Monitoring report group displays threat matches on infected hosts and displays the following reports:

- “[Threat Match: File Details](#)”, next
- “[Threat Match: File Investigation](#)”, on page 428
- “[Threat Match: File Top 100 Summary](#)”, on page 429
- “[Threat Match: Process Details](#)”, on page 430
- “[Threat Match: Process Investigation](#)”, on page 431
- “[Threat Match: Process Top 100 Summary](#)”, on page 432
- “[Threat Match: Registry Details](#)”, on page 433
- “[Threat Match: Registry Investigation](#)”, on page 434
- “[Threat Match: Registry Top 100 Summary](#)”, on page 435

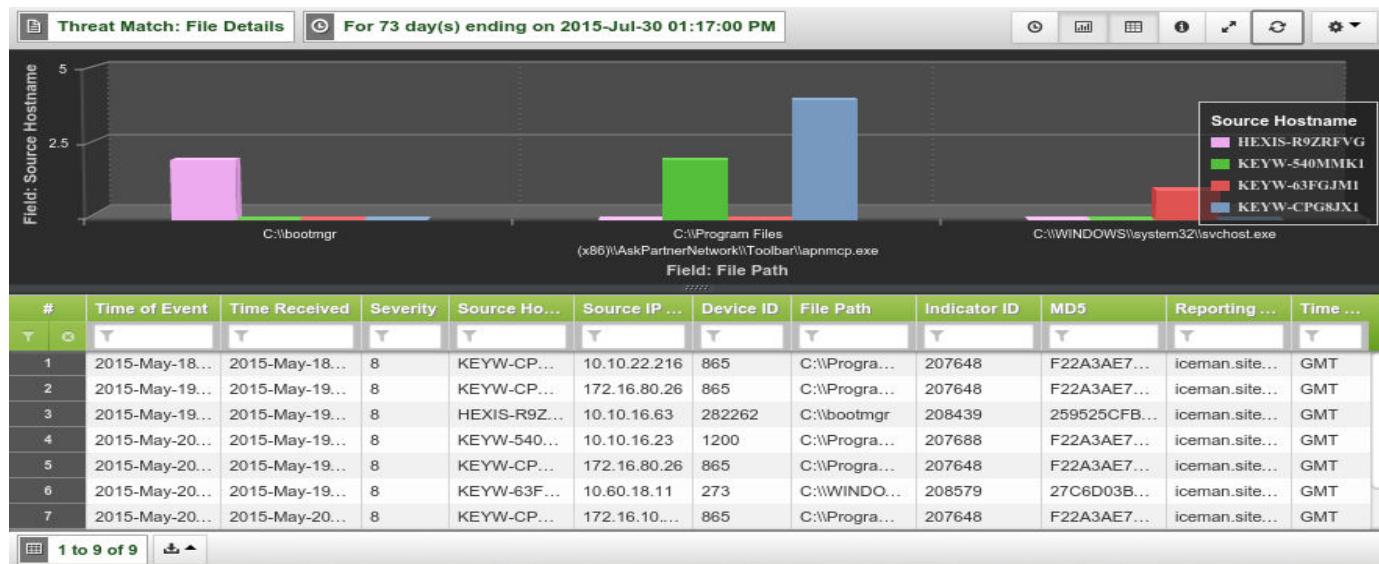
Threat Match: File Details

Details file of all threat matches on infected hosts.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	The ID of the device
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

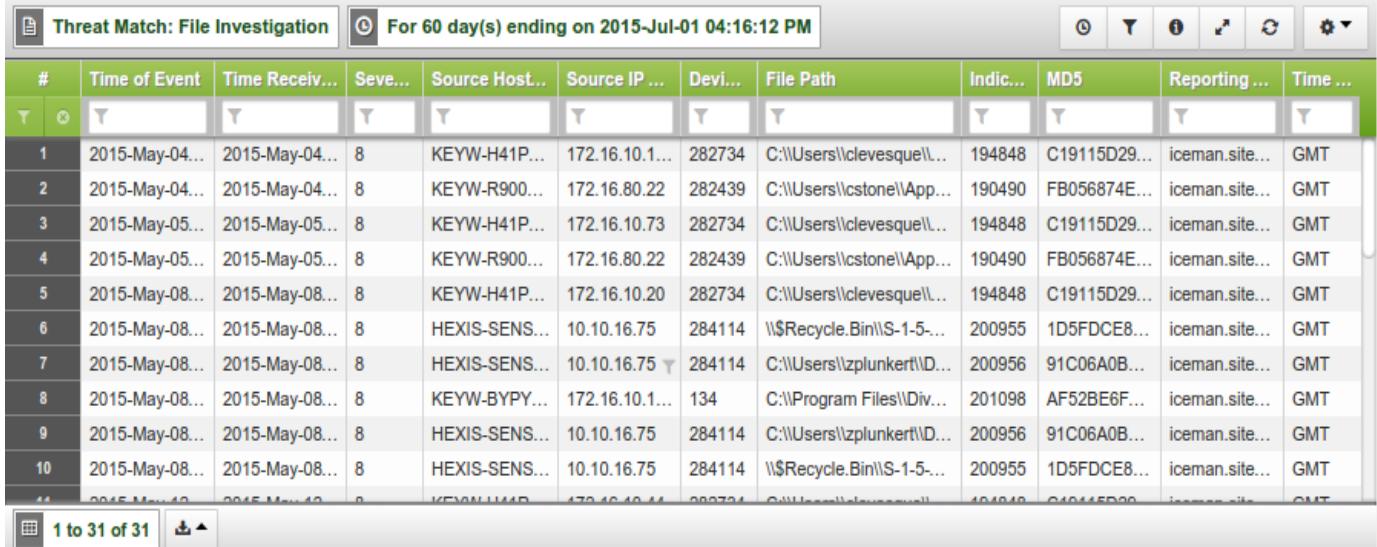
Threat Match: File Investigation

Detail file of all threat matches on infected hosts for investigation.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	The ID of the device
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



The screenshot shows a table titled "Threat Match: File Investigation" with a filter "For 60 day(s) ending on 2015-Jul-01 04:16:12 PM". The table has 13 columns: #, Time of Event, Time Receiv..., Seve..., Source Host..., Source IP ..., Devi..., File Path, Indic..., MD5, Reporting..., and Time The data consists of 10 rows of threat matches, each with a unique ID, timestamp, severity, source host, source IP, device ID, file path, indicator ID, MD5 hash, reporting host, and time zone. The reporting host for all entries is "iceman.site..." and the time zone is "GMT".

#	Time of Event	Time Receiv...	Seve...	Source Host...	Source IP ...	Devi...	File Path	Indic...	MD5	Reporting ...	Time ...
1	2015-May-04...	2015-May-04...	8	KEYW-H41P...	172.16.10.1...	282734	C:\Users\clevesque\...	194848	C19115D29...	iceman.site...	GMT
2	2015-May-04...	2015-May-04...	8	KEYW-R900...	172.16.80.22	282439	C:\Users\cstone\App...	190490	FB056874E...	iceman.site...	GMT
3	2015-May-05...	2015-May-05...	8	KEYW-H41P...	172.16.10.73	282734	C:\Users\clevesque\...	194848	C19115D29...	iceman.site...	GMT
4	2015-May-05...	2015-May-05...	8	KEYW-R900...	172.16.80.22	282439	C:\Users\cstone\App...	190490	FB056874E...	iceman.site...	GMT
5	2015-May-08...	2015-May-08...	8	KEYW-H41P...	172.16.10.20	282734	C:\Users\clevesque\...	194848	C19115D29...	iceman.site...	GMT
6	2015-May-08...	2015-May-08...	8	HEXIS-SENS...	10.10.16.75	284114	\\$Recycle.Bin\S-1-5...	200955	1D5FDCE8...	iceman.site...	GMT
7	2015-May-08...	2015-May-08...	8	HEXIS-SENS...	10.10.16.75	284114	C:\Users\zplunkert\I...	200956	91C06A0B...	iceman.site...	GMT
8	2015-May-08...	2015-May-08...	8	KEYW-BPY...	172.16.10.1...	134	C:\Program Files\Div...	201098	AF52BE6F...	iceman.site...	GMT
9	2015-May-08...	2015-May-08...	8	HEXIS-SENS...	10.10.16.75	284114	C:\Users\zplunkert\I...	200956	91C06A0B...	iceman.site...	GMT
10	2015-May-08...	2015-May-08...	8	HEXIS-SENS...	10.10.16.75	284114	\\$Recycle.Bin\S-1-5...	200955	1D5FDCE8...	iceman.site...	GMT
11	2015-May-10...	2015-May-10...	0	KEYW-H41P...	172.16.10.44	282734	C:\Users\clevesque\...	194848	C19115D29...	iceman.site...	GMT

INTELLISchema View

- None

Tables Referenced

- hexis_hawkeye_g_cef_syslogng

Threat Match: File Top 100 Summary

The top 100 summary of infected hosts with threat matches along with the number of events.

COLUMNS

Columns	Description
File Path	The full path to the file on the infected host
Count of Events	The number of events

EXAMPLE

The screenshot shows a software interface titled "Threat Match: File Top 100 Summary" with a filter "For 90 day(s) ending on 2015-Jun-19 04:15:28 PM". The main area is a table with two columns: "# File Path" and "Count of Events". The table lists 10 entries, with the first few rows shown below:

#	File Path	Count of Events
1	C:\Program Files (x86)\AskPartnerNetwork\Toolbar\apnmcp.exe	11
2	C:\Users\clevesque\AppData\Roaming\Binkiland\UpdateProc\UpdateTa...	4
3	C:\Users\zplunkert\Desktop\Sensor Test.txt	2
4	\\$RECYCLE.BIN\\$-1-5-21-2897712185-219933976-1385229856-48196\...	2
5	\\$Recycle.Bin\\$-1-5-21-936145172-3276281300-3106000987-1005\RC...	2
6	C:\Users\lystone\AppData\Local\Temp\is1751165634\14014555_stp\b...	2
7	C:\Program Files\DivX\DivX Plus Player\DivX Plus Player.exe	2
8	C:\Users\smarcussen\AppData\Local\Temp\is1275519350\6528207_st...	2
9	C:\bootmgr	2
10	C:\ProgramData\Browser\prompt.exe	1

At the bottom left, there is a pagination indicator "1 to 15 of 15" and a refresh button.

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

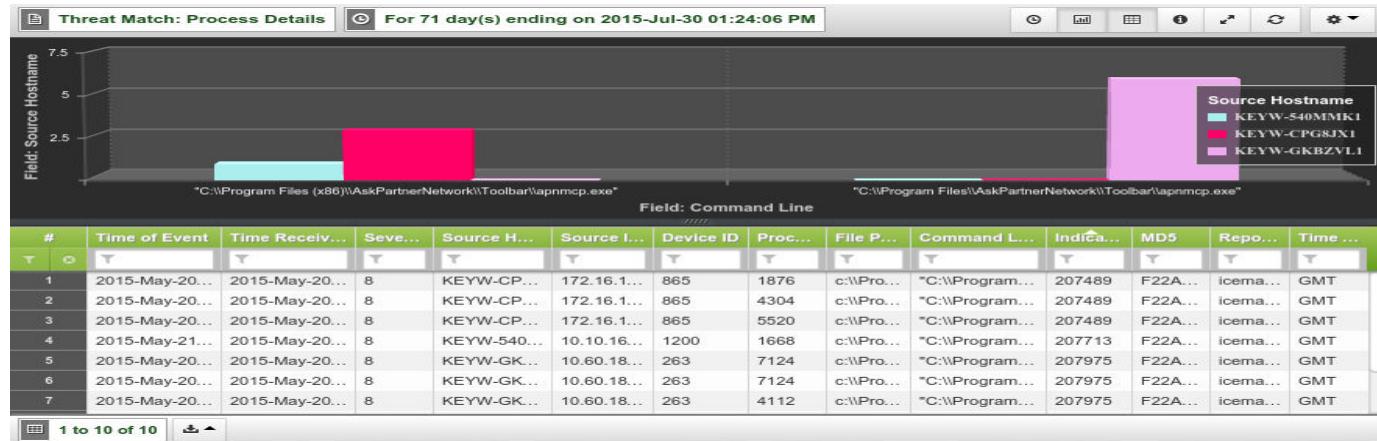
Threat Match: Process Details

Details process of infected hosts with threat matches.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	The ID of the device
Process ID	The ID of the process
File Path	The full path to the file on the infected host
Command Line	The command line of the process
Indicator ID	The ID of the event
MD5	The MD5 of the file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Threat Match: Process Investigation

Details process of infected hosts with threat matches for investigation

COLUMNS

Columns		Description											
Time of Event		Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00											
Time Received		Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)											
Severity		The ThreatSync score HawkEye G assigns											
Source Hostname		Name of the infected host											
Source IP Address		IP address of the infected host											
Device ID		The ID of the device											
Process ID		The ID of the process											
File Path		The full path to the file on the infected host											
Command Line		The command line of the process											
Indicator ID		The ID of the event											
MD5		The MD5 of the file											
Reporting Host		The name of the reporting host											
Time Zone		Time zone in which the event occurred											

EXAMPLE

威胁匹配：进程调查		在 2015 年 7 月 1 日 04:22:39 PM 结束的 60 天内											
#	事件时间	接收时间	严重性	源主机名	源 IP 地址	设备 ID	进程 ID	文件路径	命令行	指示器 ID	MD5	报告主机	时区
1	2015-05-15 13:02:46	2015-05-15 13:02:46	8	KEYW-C...	172.16.80.26	865	1269...	c:\Program...	"C:\Progra...	207489	F22A...	icem...	GMT
2	2015-05-15 13:02:46	2015-05-15 13:02:46	8	KEYW-C...	172.16.80.26	865	1269...	C:\Progra...	"C:\Progra...	207489	F22A...	icem...	GMT
3	2015-05-15 13:02:46	2015-05-15 13:02:46	8	KEYW-C...	172.16.80.26	865	1269...	c:\Program...	"C:\Progra...	207489	F22A...	icem...	GMT
4	2015-05-15 13:02:46	2015-05-15 13:02:46	8	KEYW-C...	172.16.80.26	865	1269...	C:\Progra...	"C:\Progra...	207489	F22A...	icem...	GMT
5	2015-05-15 13:02:46	2015-05-15 13:02:46	8	KEYW-C...	172.16.80.26	865	1269...	C:\Progra...	"C:\Progra...	207489	F22A...	icem...	GMT
6	2015-05-15 13:02:46	2015-05-15 13:02:46	8	KEYW-C...	172.16.80.26	865	1269...	c:\Program...	"C:\Progra...	207489	F22A...	icem...	GMT
7	2015-05-15 13:02:46	2015-05-15 13:02:46	8	KEYW-C...	172.16.80.26	865	1269...	c:\Program...	"C:\Progra...	207489	F22A...	icem...	GMT
8	2015-05-15 13:02:46	2015-05-15 13:02:46	8	KEYW-C...	172.16.80.26	865	1269...	C:\Progra...	"C:\Progra...	207489	F22A...	icem...	GMT
9	2015-05-15 13:02:46	2015-05-15 13:02:46	8	KEYW-C...	172.16.80.26	865	1269...	c:\Program...	"C:\Progra...	207489	F22A...	icem...	GMT
10	2015-05-15 13:02:46	2015-05-15 13:02:46	8	KEYW-C...	172.16.80.26	865	1269...	C:\Progra...	"C:\Progra...	207489	F22A...	icem...	GMT

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Threat Match: Process Top 100 Summary

The top 100 process (command line) summary of infected hosts with threat matches along with the number of events.

COLUMNS

Columns	Description
Command Line	The command line of the process
Count of Events	The number of events

EXAMPLE

The screenshot shows a table titled "Threat Match: Process Top 100 Summary" for a 60-day period ending on 2015-Jul-01 04:24:29 PM. The table has two columns: "Command Line" and "Count of Events". The data is as follows:

#	Command Line	Count of Events
1	"C:\Program Files (x86)\AskPartnerNetwork\Toolbar\apnmcp.exe"	308
2	"C:\Program Files\AskPartnerNetwork\Toolbar\apnmcp.exe"	303
3	C:\WINDOWS\system32\svchost.exe -k LocalService	2
4	C:\WINDOWS\System32\svchost.exe -k netsvcs	1
5	C:\WINDOWS\system32\svchost -k DcomLaunch	1
6	C:\WINDOWS\system32\svchost -k rpcss	1
7	C:\WINDOWS\system32\svchost.exe -k NetworkService	1

At the bottom left, it says "1 to 7 of 7".

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

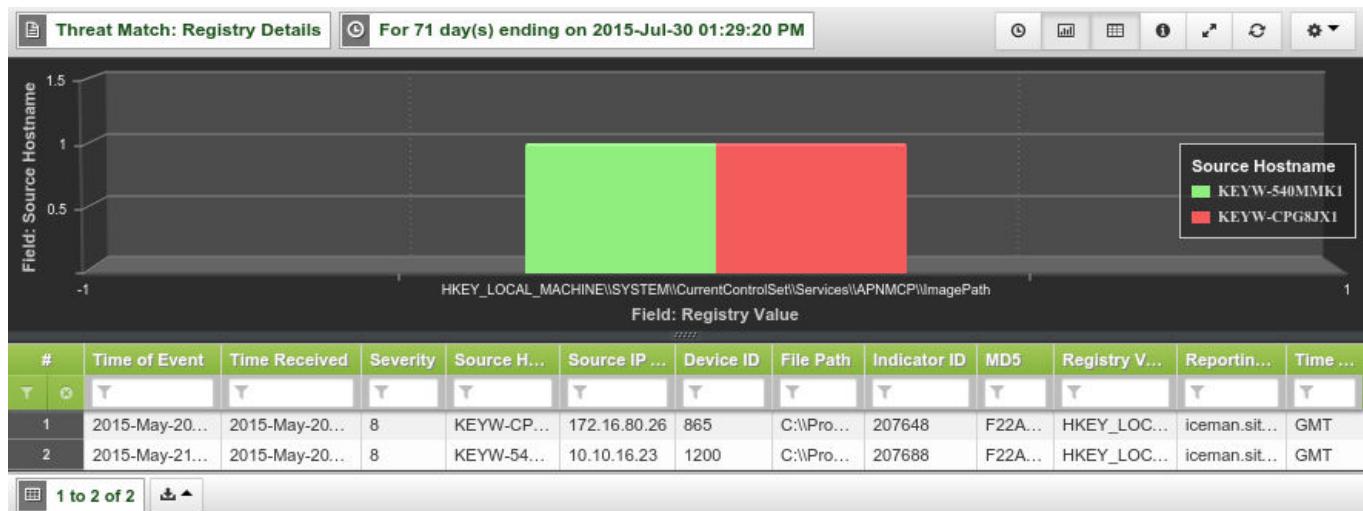
Threat Match: Registry Details

Details registry of infected hosts with threat matches.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	The name of the infected host
Source IP Address	IP address of the infected host
Device ID	The ID of the device
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Registry Value	The registry value whose data points to the matching file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

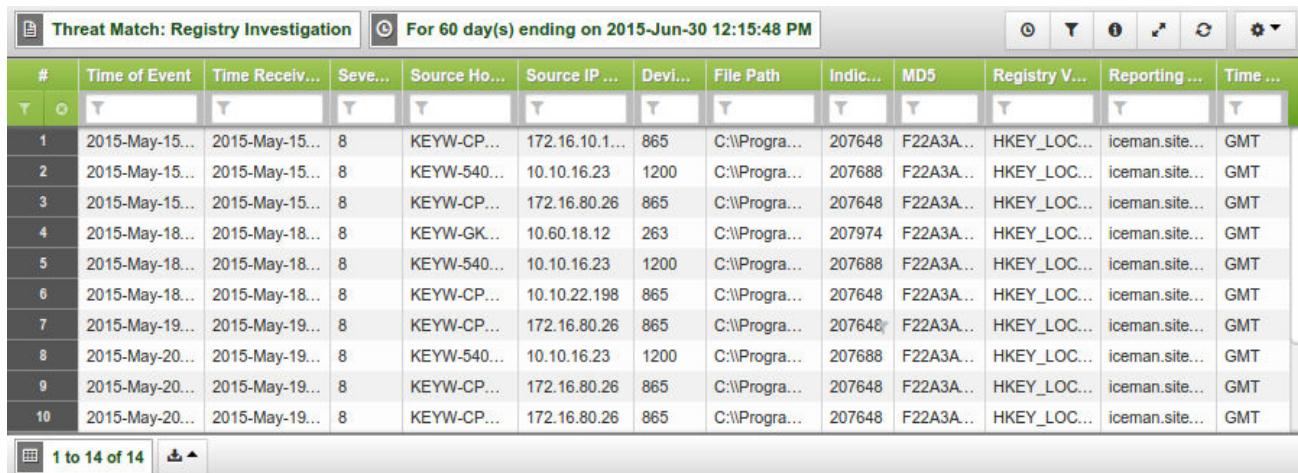
Threat Match: Registry Investigation

Details registry of infected hosts with threat matches for investigation.

COLUMNS

Columns	Description
Time of Event	Time event occurred in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD). For example: 2015-May-01T13:02:46+00:00
Time Received	Time the log was received in complete date plus hours, minutes and seconds (YYYY-MM-DDThh:mm:ssTZD)
Severity	The ThreatSync score HawkEye G assigns
Source Hostname	Name of the infected host
Source IP Address	IP address of the infected host
Device ID	The ID of the device
File Path	The full path to the file on the infected host
Indicator ID	The ID of the event
MD5	The MD5 of the file
Registry Value	The registry value whose data points to the matching file
Reporting Host	The name of the reporting host
Time Zone	Time zone in which the event occurred

EXAMPLE



The screenshot shows a database grid titled "Threat Match: Registry Investigation". The search criteria is set to "For 60 day(s) ending on 2015-Jun-30 12:15:48 PM". The grid has 13 columns: #, Time of Event, Time Receiv..., Seve..., Source Ho..., Source IP ..., Devi..., File Path, Indic..., MD5, Registry V..., Reporting ..., and Time The data consists of 10 rows of threat match details, such as file paths like C:\Program Files\ and registry keys like HKEY_LOC... . All entries show a severity of 8 and a reporting host of iceman.site... . The time zone is listed as GMT for all rows.

#	Time of Event	Time Receiv...	Seve...	Source Ho...	Source IP ...	Devi...	File Path	Indic...	MD5	Registry V...	Reporting ...	Time ...
1	2015-May-15...	2015-May-15...	8	KEYW-CP...	172.16.10.1...	865	C:\Progra...	207648	F22A3A...	HKEY_LOC...	iceman.site...	GMT
2	2015-May-15...	2015-May-15...	8	KEYW-540...	10.10.16.23	1200	C:\Progra...	207688	F22A3A...	HKEY_LOC...	iceman.site...	GMT
3	2015-May-15...	2015-May-15...	8	KEYW-CP...	172.16.80.26	865	C:\Progra...	207648	F22A3A...	HKEY_LOC...	iceman.site...	GMT
4	2015-May-18...	2015-May-18...	8	KEYW-GK...	10.60.18.12	263	C:\Progra...	207974	F22A3A...	HKEY_LOC...	iceman.site...	GMT
5	2015-May-18...	2015-May-18...	8	KEYW-540...	10.10.16.23	1200	C:\Progra...	207688	F22A3A...	HKEY_LOC...	iceman.site...	GMT
6	2015-May-18...	2015-May-18...	8	KEYW-CP...	10.10.22.198	865	C:\Progra...	207648	F22A3A...	HKEY_LOC...	iceman.site...	GMT
7	2015-May-19...	2015-May-19...	8	KEYW-CP...	172.16.80.26	865	C:\Progra...	207648	F22A3A...	HKEY_LOC...	iceman.site...	GMT
8	2015-May-20...	2015-May-19...	8	KEYW-540...	10.10.16.23	1200	C:\Progra...	207688	F22A3A...	HKEY_LOC...	iceman.site...	GMT
9	2015-May-20...	2015-May-19...	8	KEYW-CP...	172.16.80.26	865	C:\Progra...	207648	F22A3A...	HKEY_LOC...	iceman.site...	GMT
10	2015-May-20...	2015-May-19...	8	KEYW-CP...	172.16.80.26	865	C:\Progra...	207648	F22A3A...	HKEY_LOC...	iceman.site...	GMT

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

Threat Match: Registry Top 100 Summary

The top 100 registry summary of Window hosts with threat matches along with the number of events.

COLUMNS

Columns	Description
File Path	The full path to the file on the infected host
MD5	The MD5 of the file
Registry Value	The registry value whose data points to the matching file
Count of Events	The number of events

EXAMPLE

Threat Match: Registry Top 100 Summary					For 60 day(s) ending on 2015-Jul-01 04:26:45 PM		
#	File Path	MD5	Registry Value	Count of Events			
1	C:\Program Files (x86)\AskPartnerNe...	F22A3AE791C78A31763499585180E...	HKEY_LOCAL_MACHINE\SYSTEM\...	11			
2	C:\Program Files\AskPartnerNetworkl...	F22A3AE791C78A31763499585180E...	HKEY_LOCAL_MACHINE\SYSTEM\...	1			
3	C:\WINDOWS\System32\svchost.exe	27C6D03BCDB8CFEB96B716F3D8B...	HKEY_LOCAL_MACHINE\SYSTEM\...	1			
4	C:\WINDOWS\system32\svchost.exe	27C6D03BCDB8CFEB96B716F3D8B...	HKEY_LOCAL_MACHINE\SYSTEM\...	1			

INTELLISchema View

- None

TABLES REFERENCED

- hexis_hawkeye_g_cef_syslogng

CHAPTER 14

Panos Reports

The SenSage AP Panos reports assist organizations in determining possible threats.

This chapter provides a reference for the Panos reports, including lists of columns available for reporting.

The Panos reports include the following:

- “Panos - IP Based Data Query”, on page 437
- “Panos - Threats Blocked Per Hour: total and by IAP”, on page 438
- “Panos - Top 100 Source-Destination IP Pairs by Session Count”, on page 439

PANOS - IP BASED DATA QUERY

This report displays the PanOS Firewall logs for an individual source IP address.

COLUMNS

Columns	Description
source_port	Source port
destination_ip	Destination IP
destination_port	Destination port
destination_user	Destination user

EXAMPLE

The screenshot shows a software interface titled "PANOS - IP-based Data Query". At the top, there is a search bar with the placeholder "For 20 year(s) ending on 2014-Dec-16" and various filter and export buttons. Below the search bar is a table with the following columns: #, source_port, destination_ip, destination_port, and destination_user. The table contains 5 rows of data:

#	source_port	destination_ip	destination_port	destination_user
1	53	192.168.0.138	56757	
2	0	192.168.0.5	0	FINANCEpturner
3	1001	192.168.0.192	443	
4	1113	192.168.0.133	80	
5	3229	192.168.0.220	80	

At the bottom left, it says "1 to 250 of 9,553". At the bottom right, there is a navigation bar with buttons for <<, <, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, ..., >, >>.

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- panos_firewall_syslogng

PANOS - THREATS BLOCKED PER HOUR: TOTAL AND BY IAP

This report displays threats blocked per hour by total and by Internet Access Provider (IAP).

COLUMNS

Column	Description
source_zone (Count)	Source zone
ts (Date_Trunc:hour)	Date and time on which the activity occurred.
source_zone (Count)	Total number

EXAMPLE

The screenshot shows a database grid titled "PANOS - Threats Blocked Per Hour: total and by IAP". The filter is set to "For 20 year(s) ending on 2014-Dec-16". The grid has three columns: "#", "source_zone (Count)", and "ts (Date_Trunc:hour)". The data shows 8 rows of "Internal_Trust" entries with counts ranging from 25 to 29 across various hours in December 2014. The bottom navigation bar indicates "1 to 250 of 494" and shows page 1 of 2.

#	source_zone (Count)	ts (Date_Trunc:hour)	source_zone (Count)
1	Internal_Trust	2014-Dec-08 06:00 AM	29
2	Internal_Trust	2014-Nov-25 07:00 AM	27
3	Internal_Trust	2014-Dec-13 06:00 AM	26
4	Internal_Trust	2014-Dec-02 06:00 AM	25
5	Internal_Trust	2014-Nov-27 06:00 AM	25
6	Internal_Trust	2014-Dec-05 07:00 AM	25
7	Internal_Trust	2014-Dec-16 07:00 AM	25
8	Internal_Trust	2014-Nov-27 05:00 AM	25

INTELLISchema VIEW

- None

TABLES REFERENCED

- panos_firewall_syslogng

PANOS - TOP 100 SOURCE-DESTINATION IP PAIRS BY SESSION COUNT

This report displays the top 100 source-destination IP pairs by Session Count.

COLUMNS

Column	Description
source_ip	Source IP
destination_ip	Destination IP
destination_port	Destination port
bytes	Sum of bytes
Total	Number of sessions

EXAMPLE

#	source_ip	destination_ip	destination_port	bytes	Total
1	192.168.0.4	192.168.0.5	0	512	2
2	192.168.0.6	192.168.0.7	0	312	2

1 to 2 of 2

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- panos_firewall_syslogng

CHAPTER 15

SAP Reports

The SenSage AP SAP reports assist organizations in compiling SAP Security information.

This chapter provides a reference for the SAP reports, including lists of columns available for reporting.

The SAP reports include the following:

- “[SAP Security Audit - Program Summary](#)”, on page 441
- “[SAP Security Audit - Terminal Summary](#)”, on page 442
- “[SAP Security Audit - Top 10 Records](#)”, on page 443
- “[SAP Security Audit - User Summary](#)”, on page 444

SAP SECURITY AUDIT - PROGRAM SUMMARY

This report displays program summary for SAP Security audit.

COLUMNS

Columns	Description
Program	Program
Total	Program summary total

EXAMPLE

#	Program	Total
1	SAPMSYST	29
2	/1BCDWB/DBZTV_SVC_CNTRL	10
3	SAPMSUU0	7

INTELLISchema View

- None

TABLES REFERENCED

- sap_aud_sftp

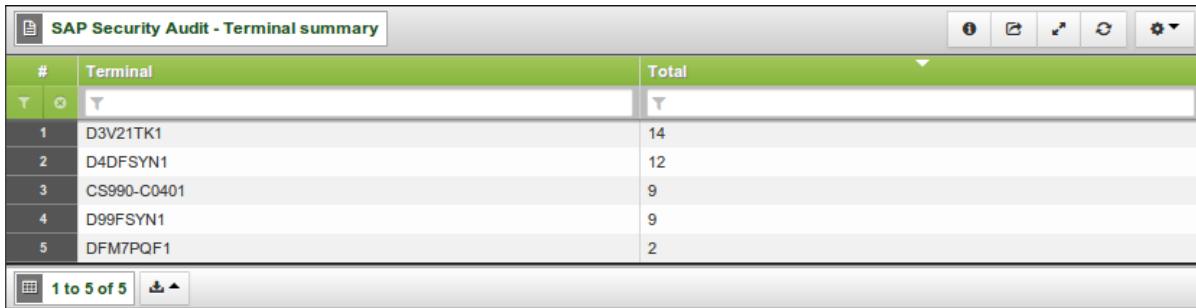
SAP SECURITY AUDIT - TERMINAL SUMMARY

This report displays terminal summary for SAP Security audit.

COLUMNS

Column	Description
Terminal	Terminal
Total	Terminal summary

EXAMPLE



The screenshot shows a SAP report titled "SAP Security Audit - Terminal summary". The table has two columns: "# Terminal" and "Total". The data rows are:

#	Terminal	Total
1	D3V21TK1	14
2	D4DFSYN1	12
3	CS990-C0401	9
4	D99FSYN1	9
5	DFM7PQF1	2

At the bottom left, it says "1 to 5 of 5".

INTELLISchema View

- None

Tables Referenced

- sap_aud_sftp

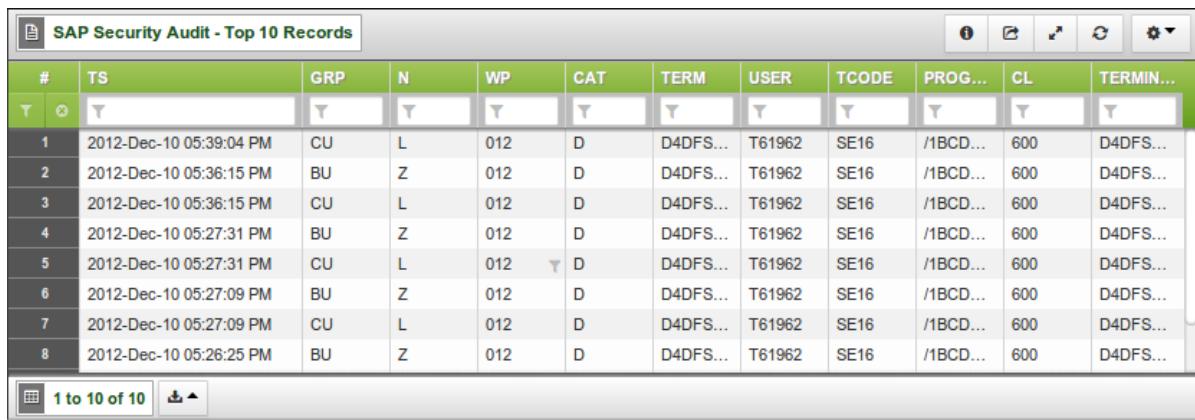
SAP SECURITY AUDIT - TOP 10 RECORDS

This report displays the top 10 visited domains.

COLUMNS

Column	Description
TS	Date and time activity
GRP	GRP
N	N
WP	WP
CAT	CAT
TERM	TERM
USER	User
TCODE	TCODE
PROGRAM	Program
CL	CL
TERMINAL	Terminal

EXAMPLE



The screenshot shows a SAP report titled "SAP Security Audit - Top 10 Records". The report has a green header bar with the title. Below it is a table with 13 columns: #, TS, GRP, N, WP, CAT, TERM, USER, TCODE, PROG..., CL, and TERMIN... The first column is a row number. The TS column contains dates and times. The GRP column contains codes like CU, BU, Z, L. The N column contains letters like 012, D, D4DFS... The CAT, TERM, USER, TCODE, PROG..., CL, and TERMIN... columns contain various SAP codes and numbers. At the bottom left, there is a footer bar with the text "1 to 10 of 10" and navigation icons.

#	TS	GRP	N	WP	CAT	TERM	USER	TCODE	PROG...	CL	TERMIN...
1	2012-Dec-10 05:39:04 PM	CU	L	012	D	D4DFS...	T61962	SE16	/1BCD...	600	D4DFS...
2	2012-Dec-10 05:36:15 PM	BU	Z	012	D	D4DFS...	T61962	SE16	/1BCD...	600	D4DFS...
3	2012-Dec-10 05:36:15 PM	CU	L	012	D	D4DFS...	T61962	SE16	/1BCD...	600	D4DFS...
4	2012-Dec-10 05:27:31 PM	BU	Z	012	D	D4DFS...	T61962	SE16	/1BCD...	600	D4DFS...
5	2012-Dec-10 05:27:31 PM	CU	L	012	D	D4DFS...	T61962	SE16	/1BCD...	600	D4DFS...
6	2012-Dec-10 05:27:09 PM	BU	Z	012	D	D4DFS...	T61962	SE16	/1BCD...	600	D4DFS...
7	2012-Dec-10 05:27:09 PM	CU	L	012	D	D4DFS...	T61962	SE16	/1BCD...	600	D4DFS...
8	2012-Dec-10 05:26:25 PM	BU	Z	012	D	D4DFS...	T61962	SE16	/1BCD...	600	D4DFS...

INTELLISchema VIEW

- None

TABLES REFERENCED

- sap_aud_sftp

SAP SECURITY AUDIT - USER SUMMARY

This report displays user summary for SAP Security audit.

COLUMNS

Columns	Description
User	User
Total	User Summary

EXAMPLE

#	User	Total
1	T203448	14
2	T61962	12
3	T410539	9
4	T92884	9
5	T119543	2

INTELLISchema VIEW

- None

TABLES REFERENCED

- sap_aud_sftp

CHAPTER 16

Miscellaneous Reports

This chapter provides a reference for miscellaneous and standalone reports, including lists of columns available for reporting.

These reports include the following:

- “[Investigation Report](#)”, on page 446
- “[Microsoft Exchange - Audit Trail Integrity Events](#)”, on page 447

INVESTIGATION REPORT

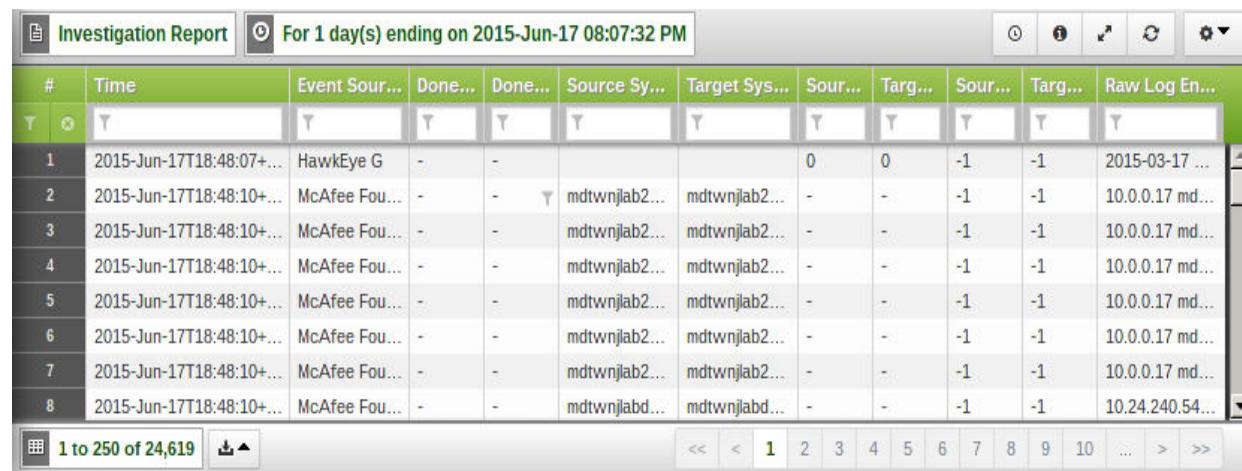
This report queries all data in the EDW collected by standard log adapters that have been enabled for data collection.

TIP: This report queries many tables in the EDW; therefore it may take longer to run than reports that query only one or a few tables.

COLUMNS

Columns	Description
Time	Time the event occurred (yyyy-mm-dd hh:mm:ss)
Event Source	Application or source of the event
Done By	Event description
Done To	User account accessed
Source System	Information system that initiated the login
Target System	Information system logged into
Source Port	Port of Source System (if available)
Target Port	Port of Target System (if available)
Source Malware	If specified in last.lookup file, the value of the Source System column is displayed.
Target Malware	If specified in last.lookup file, the value of Target System column is displayed.
Raw Log	Entry Unparsed message text

EXAMPLE



The screenshot shows a software interface titled "Investigation Report" with a filter "For 1 day(s) ending on 2015-Jun-17 08:07:32 PM". The main area displays a grid of log entries with the following columns: #, Time, Event Sour..., Done..., Done..., Source Sy..., Target Sys..., Sour..., Targ..., Sour..., Targ..., Raw Log En... . The grid contains 8 rows of data, each representing a log entry with specific timestamp, source, target, and raw log details. At the bottom, there is a navigation bar showing "1 to 250 of 24,619" and a page number "1" with other page numbers 2, 3, 4, 5, 6, 7, 8, 9, 10, ..., >, >>.

INTELLISCHEMA VIEW

- “Investigation Event”, on page 114

TABLE REFERENCED

- None

MICROSOFT EXCHANGE - AUDIT TRAIL INTEGRITY EVENTS

This report displays audit trail integrity events for Microsoft Exchange.

COLUMNS

Columns	Description
Occurred	Date and time on which the activity occurred
Event ID	Event ID
Event description	Event description
Action	Action
Performed By	Performed By
Details	Details

EXAMPLE

#	Occurred	Event ID	Event description	Action	Performed By	Details
1	2/27/2013 2:59:49 PM	25190	New-AdminAuditLogS...	-	sp2010.com/Users/A...	Object Modified: Audit...
2	2/27/2013 2:59:49 PM	25210	New-MailboxAuditLog...	-	sp2010.com/Users/A...	Object Modified: Audit...
3	2/27/2013 3:59:50 PM	25190	New-AdminAuditLogS...	-	sp2010.com/Users/A...	Object Modified: Audit...
4	2/27/2013 3:59:50 PM	25210	New-MailboxAuditLog...	-	sp2010.com/Users/A...	Object Modified: Audit...
5	2/27/2013 4:59:50 PM	25190	New-AdminAuditLogS...	-	sp2010.com/Users/A...	Object Modified: Audit...
6	2/27/2013 4:59:50 PM	25210	New-MailboxAuditLog...	-	sp2010.com/Users/A...	Object Modified: Audit...
7	2/27/2013 5:59:51 PM	25190	New-AdminAuditLogS...	-	sp2010.com/Users/A...	Object Modified: Audit...
8	2/27/2013 5:59:51 PM	25210	New-MailboxAuditLog...	-	sp2010.com/Users/A...	Object Modified: Audit...

INTELLISCHEMA VIEW

- None

TABLES REFERENCED

- microsoft_exchange_admin_events_syslogng
- microsoft_exchange_mailbox_events_syslogng

CHAPTER 17

Log Adapters Listing

IgniteTech provides a set of log adapters for common information systems. The following sections provide information on setup and configuration as well as related reports, IntelliSchema views, and rules for each log adapter. The following log adapters are provided with your SenSage AP software:

APACHE

- “[apache_access_syslogng](#)”, on page 453
- “[apache_error_syslogng](#)”, on page 459

CATBIRD

- “[catbird_vsecurity_syslogng](#)”, on page 465

CHECKPOINT

- “[checkpoint_opsec_lea](#)”, on page 467

CISCO

- “[cisco_asa_syslogng](#)”, on page 459
- “[cisco_acs_syslogng](#)”, on page 471
- “[cisco_ios_syslogng](#)”, on page 479
- “[cisco_ips_alert_error](#)”, on page 483
- “[cisco_Ironport_Email_Security_Appliances](#)”, on page 487
- “[cisco_netflow_receiver](#)”, on page 491
- “[cisco_pix_syslogng](#)”, on page 495

HEWLETT-PACKARD

- “[hp_nonStop_ems_cinset_nset](#)”, on page 511
- “[hp_proCurve_t3t4_syslogng](#)”, on page 517
- “[hp_proCurve_tmsz_syslogng](#)”, on page 519
- “[tipping_point_syslogng](#)”, on page 643

MICROSOFT WINDOWS

- “[microsoft_dns_debug_sensageRetrieverAgent](#)”, on page 553
- “[microsoft_exchange_admin_events_syslogng](#)”, on page 557
- “[microsoft_exchange_mailbox_events_syslogng](#)”, on page 561

- “microsoft_exchange_tracking_sensageRetrieverAgent”, on page 565
- “microsoft_sharepoint_audit_sensageRetrieverAgent”, on page 571
- “microsoft_windows_NonSecurityEvent_sensageRetriever”, on page 577
- “microsoft_windows_securityEvent_sensageRetriever”, on page 579
- “microsoft_windows_securityEvent_snare”, on page 595
- “microsoft_windows2008_securityEvent_sensageRetriever”, on page 587
- “microsoft_windows2008_securityEvent_snare”, on page 557

MCAFEE

- “mcafee_epo_audit_rdbms”, on page 533
- “mcafee_epo_event_rdbms”, on page 537
- “mcafee_epo_event_sensageRetriever”, on page 351
- “mcafee_epo_audit_sensageRetriever”, on page 347
- “mcafee_foundstone_rdbms”, on page 541
- “mcafee_intrushield_rdbms”, on page 545
- “mcafee_intrushield_syslogng”, on page 549

ORACLE

- “oracle_adump”, on page 615
- “oracle_adump_syslogng”, on page 617
- “oracle_database_fga_sensageRetriever”, on page 621
- “oracle_database_sysaudit_sensageRetriever”, on page 625
- “oracle_fga_xml_batch”, on page 627

UNIX/LINUX

- “unix_ftpd_syslogng”, on page 645
- “unix_login_syslogng”, on page 649
- “unix_sshd2_syslogng”, on page 653
- “unix_su_syslogng”, on page 657
- “unix_sudo_syslogng”, on page 661

VMWARE

- “vmware_esx_500_syslogng”, on page 665

MISCELLANEOUS

- “f5_asm_cef_syslogng”, on page 499
- “hexis_hawkeye_g_cef_syslogng”, on page 505

- “[ibm_db2_rdbms](#)”, on page 521
- “[juniper_netscreenFw_syslogng](#)”, on page 529
- “[panos_firewall_syslogng](#)”, on page 441
- “[sap_aud_sftp](#)”, on page 631
- “[sun_bsm_sftp](#)”, on page 633
- “[symantec_endpoint_syslogng](#)”, on page 635
- “[syslogng_catchall_syslogng](#)”, on page 639

CHAPTER 18

apache_access_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	apache_access_syslogng
Version	1.0.0
Source Vendor	Apache
Source Product	Apache HTTP server
Source Component	N/A
Source Version	1.3.x/2.x
Source Host OS	Cross-Platform
Transport Mechanism	syslog-ng
PTL Filename	apache_error_syslogng.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none">• httpAccess__webServer_apache_access_syslogng• investigation_apache_access_syslogng• parsedData_apache_access_syslogng• unparsedData_apache_access_syslogng• webProxy_apache_access_syslogng• web_server_apache_access_syslogng
Look-up file	Not required
Scripts	Not required
Source-Specific Reports	None
Event Types	Access Events

SETTING UP APACHE_ACCESS_SYSLOGNG LOG ADAPTER

This section describes how to configure the apache_access_syslogng log adapter. The following steps are required:

- “Source System Setup”, next

- “SenSage Collector Configuration”, on page 456

Source System Setup

By default, the Apache HTTP Server is set up to generate error logs and access logs, and to store them in your default logging directory (normally: `/var/log/httpd`).

Where the logs go and how they are formatted is determined by your `httpd.conf` configuration file, normally located in `/etc/httpd/conf/`.

If you have not changed any of the default logging statements in your configuration files, then by default, you should only need to add two additional lines and your logs will be ready to send to SenSage AP:

```
ErrorLog "|/usr/bin/logger -p local1.info -t apache_error"
CustomLog "|/usr/bin/logger -p local1.info -t apache_access" combined
```

If you have made changes to the file or you are uncertain of your changes, please verify that your configuration contains the following statements, which are noted in **red** highlight:

```
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here. If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog logs/error_log
#
# Send Logs to SenSage AP logger program
ErrorLog "|/usr/bin/logger -p local1.info -t apache_error"
#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here. Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
#CustomLog logs/access_log common
#
# If you would like to have separate agent and referer logfiles, uncomment
# the following directives.
```

```

#
#CustomLog logs/referer_log referer
#
# For a single logfile with access, agent, and referer information
# (Combined Logfile Format), use the following directive:
#
CustomLog logs/access_log combined
#
# Send Logs to SenSage AP logger program
CustomLog "|/usr/bin/logger -p local1.info -t apache_access" combined
#

```

For the access logs, you can specify from among several default formats or you can create your own format. In order for SenSage AP to properly parse your access log data, the data must be in the combined log format. This is achieved by providing the logging statements in the configuration file shown above.

Unlike access logs, error logs cannot be modified; the only options available to error logs are the raising or lowering of the error levels. If you choose to raise or lower the logging level on the error logs, SenSage AP will be able to parse that data without any issues; so it is the responsibility of the SenSage AP Administrator to dictate which logging level is desired for Apache reporting. Note that the default is for Apache to report on the **warning** level.

It is acceptable to have other log formats specified in your **httpd.conf** file, as that data is sent somewhere other than SenSage AP (as SenSage AP will not be able to parse that data). The Apache HTTP Server allows you to pick different formats for access logs and send copies to various places. As long as you have one logging statement in your **httpd.conf** that is formatting a copy that SenSage AP is able to parse, any other logging statements should not interfere with the collection process.

Apache HTTP server can save log data to files or can send data via pipe to any binary.

Logs cannot be saved to files and sent to the binary at the same time (will be used as the last option for ErrorLog and CustomLog in config file).

If we want to work logging to file and sending log data to binary at the same time we can use simple bash script.

Error Log Example

```

-----
#!/bin/bash

logfile='/var/log/httpd/error_log'
logger='/usr/bin/logger -p local1.info -t apache_access'

while read x
do
    echo $x >> $logfile
    echo $x | $logger
done
-----
```

The script should be added to config file:

```
ErrorLog "|/path/to/script/logger.sh"
```

This script will get data from pipe, will save data to log file and will sent via pipe to binary.

SenSage Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open the syslog-ng configuration file <*SenSage AP Home*>/etc/syslog-ng/syslog-ng.conf on the host running the SenSage AP Collector.
- 2 Make sure the following destination filter and log statement are configured as shown below:

```
destination d_apache_access_syslogng {  
    file("<SenSage AP Home>/incoming/syslog-ng/apache_access_syslogng/  
apache_access_syslogng.log"  
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST  
$MSGHDR$MSG\n")  
        template_escape(no) );  
};  
  
filter f_apache_access_syslogng {  
    program('apache_error');  
};  
  
log {  
    source(s_network_std); source(s_network_tls);  
    filter(f_apache_access_syslogng);  
    destination(d_apache_access_syslogng);  
    flags(final);  
};
```

- 3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

- 4 Edit the SenSage AP Collector **config.xml** with sections for logqueue, retriever, and loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.
- 5 (Optional). Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

Sample Configuration Files

The following are sample configuration files:

Collector Configuration (**config.xml**)

```
<LogQueue encoding="UTF-8" minMBFree="100" name="q_apache_access_syslogng"  
path="queue/apache_access_syslogng"/>  
  
<Retriever deleteOriginal="1" enabled="1" method="copy"  
name="r_apache_access_syslogng" type="filesystem">  
    <RunOnHost>localhost</RunOnHost>  
    <LogQueue>q_apache_access_syslogng</LogQueue>  
    <SourceDir>/opt/hexis/incoming/syslog-ng/apache_access_syslogng</  
SourceDir>  
    <Plugin name="Default">
```

```

<File ai="ignore" id="1">.*</File>
<File ai="accept" id="2">.*\loadme$</File>
</Plugin>
</Retriever>

<Loader enabled="1" name="l_apache_access_syslogng">
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_apache_access_syslogng</LogQueue>
<SLSInstance>analytics.example.com:8072</SLSInstance>
<SLSUser>administrator</SLSUser>
<SLSSharedKey>file:/opt/sensage/etc/sls/instance/mysls/shared_secret.asc</
SLSSharedKey>
<PTL namespace="analytics" table="apache_access_syslogng" type="file">
<Location>/opt/hexis/hawkeye-ap/analytics/adapters/
apache_access_syslogng/apache_access_syslogng.ptl</Location>
<LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
</PTL>
</Loader>

```

Syslog-*ng* Configuration Entries (*syslog-*ng.conf**)

```

destination d_apache_access_syslogng {
    file("/opt/hexis/incoming/syslog-ng/apache_access_syslogng/
apache_access_syslogng.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};

filter f_apache_access_syslogng {
    program('apache_access');
};

log {
    source(s_network_std); source(s_network_tls);
    filter(f_apache_access_syslogng);
    destination(d_apache_access_syslogng);
    flags(final);
};

```

TROUBLESHOOTING

Some systems come preinstalled with SELinux, the NSA's Security Enhanced Linux system. This system can be complicated and difficult to use unless you are already familiar with it; if installed the system may be running by default and will prevent any of your log messages from getting to syslog via the SenSage AP logger program. The easiest way to fix this problem is to disable SELinux; from doing this, **su** to the root user, and issue this command:

```
/usr/sbin/setenforce 0
```

After you have done this, the error logs from Apache should start to appear in your syslog feed.

apache_error_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	apache_error_syslogng
Version	1.0.0
Source Vendor	Apache
Source Product	Apache HTTP server
Source Component	N/A
Source Version	1.3.x/2.x
Source Host OS	Cross-Platform
Transport Mechanism	syslog-ng
PTL Filename	apache_error_syslogng.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none"> • alert__apache_error_syslogng • audit__apache_error_syslogng • parsedData__apache_error_syslogng • unparsedData__apache_error_syslogng
Look-up file	Not required
Scripts	Not required
Source-Specific Reports	None
Event Types	Error Events

SETTING UP APACHE_ERROR_SYSLOGNG LOG ADAPTER

This section describes how to configure the apache_error_syslogng log adapter. The following steps are required:

- “[Source System Setup](#)”, next
- “[SenSage Collector Configuration](#)”, on page 462

Source System Setup

By default, the Apache HTTP Server is set up to generate error logs and access logs, and to store them in your default logging directory (normally: `/var/log/httpd`).

Where the logs go and how they are formatted is determined by your `httpd.conf` configuration file, normally located in `/etc/httpd/conf/`.

If you have not changed any of the default logging statements in your configuration files, then by default, you should only need to add two additional lines and your logs will be ready to send to SenSage AP:

```
ErrorLog "|/usr/bin/logger -p local1.info -t apache_error"
CustomLog "|/usr/bin/logger -p local1.info -t apache_access" combined
```

If you have made changes to the file or you are uncertain of your changes, please verify that your configuration contains the following statements, which are noted in red highlight:

```
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here. If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog logs/error_log
#
# Send Logs to HawkEye AP logger program
ErrorLog "|/usr/bin/logger -p local1.info -t apache_error"
#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here. Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
#CustomLog logs/access_log common
#
# If you would like to have separate agent and referer logfiles, uncomment
# the following directives.
#
#CustomLog logs/referer_log referer
```

```

#
# For a single logfile with access, agent, and referer information
# (Combined Logfile Format), use the following directive:
#
CustomLog logs/access_log combined
#
# Send Logs to HawkEye AP logger program
CustomLog "|/usr/bin/logger -p local1.info -t apache_access" combined
#

```

For the access logs, you can specify from among several default formats or you can create your own format. In order for SenSage AP to properly parse your access log data, the data must be in the combined log format. This is achieved by providing the logging statements in the configuration file shown above.

Unlike access logs, error logs cannot be modified; the only options available to error logs are the raising or lowering of the error levels. If you choose to raise or lower the logging level on the error logs, SenSage AP will be able to parse that data without any issues; so it is the responsibility of the SenSage AP Administratior to dictate which logging level is desired for Apcache reporting. Note that the defaultt is for Apache to report on the **warning** level.

It is acceptable to have have other log formats specified in your **httpd.conf** file, as that data is sent somewhere other than SenSage AP (as SenSage AP will not be able to parse that data). The Apache HTTP Server allows you to pick different formats for access logs and send copies to various places. As long as you have one logging statement in your **httpd.conf** that is formatting a copy that SenSage AP is able to parse, any other logging statements should not interfere with the collection process.

Apache HTTP server can save log data to files or can send data via pipe to any binary.

Logs can't be saved to files and sent to the binary at the same time (Will be used last option for ErrorLog and CustomLog in config file).

If should works logging to file and sending log data to binary at the same time we can use simple bash script.

Example for error log

```
-----
#!/bin/bash

logfile='/var/log/httpd/error_log'
logger='/usr/bin/logger -p local1.info -t apache_access'

while read x
do
    echo $x >> $logfile
    echo $x | $logger
done
-----
```

The script should be added to config file:

```
ErrorLog "|/path/to/script/logger.sh"
```

This script will get data from pipe, will save data to log file and will sent via pipe to binary.

SenSage Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open the syslog-ng configuration file <SenSage AP Home>/etc/syslog-ng/syslog-ng.conf on the host running the SenSage Collector.
- 2 Make sure the following destination filter and log statement are configured as shown below:

```
destination d_apache_error_syslogng {  
    file("<SenSage AP Home>/incoming/syslog-ng/apache_error_syslogng/  
apache_error_syslogng.log"  
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST  
$MSGHDR$MSG\n")  
        template_escape(no) );  
};  
  
filter f_apache_error_syslogng {  
    program('apache_error');  
};  
  
log {  
    source(s_network_std); source(s_network_tls);  
    filter(f_apache_error_syslogng);  
    destination(d_apache_error_syslogng);  
    flags(final);  
};
```

- 3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

- 4 Edit the SenSage Collector **config.xml** with sections for logqueue, retriever, and loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

```
kill -HUP `cat /var/run/syslog.pid`
```

- 5 (Optional). Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

SAMPLE CONFIGURATION FILES

The following are sample configuration files:

Collector Configuration (**config.xml**)

```
<LogQueue encoding="UTF-8" minMBFree="100" name="q_apache_error_syslogng"  
path="queue/apache_error_syslogng"/>  
  
<Retriever deleteOriginal="1" enabled="1" method="copy"  
name="r_apache_error_syslogng" type="filesystem">  
    <RunOnHost>localhost</RunOnHost>  
    <LogQueue>q_apache_error_syslogng</LogQueue>  
    <SourceDir>/opt/hexis/incoming/syslog-ng/apache_error_syslogng</SourceDir>  
    <Plugin name="Default">
```

```

<File ai="ignore" id="1">.*</File>
<File ai="accept" id="2">.*\loadme$</File>
</Plugin>
</Retriever>

<Loader enabled="1" name="l_apache_error_syslogng">
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_apache_error_syslogng</LogQueue>
<SLSInstance>analytics.example.com:8072</SLSInstance>
<SLSUser>administrator</SLSUser>
<SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>
<PTL namespace="analytics" table="apache_error_syslogng" type="file">
<Location>/opt/hexis/hawkeye-ap/analytics/adapters/
apache_error_syslogng/apache_error_syslogng.ptl</Location>
<LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
</PTL>
</Loader>

```

Syslog-*ng* Configuration Entries (*syslog-*ng.conf**)

```

destination d_apache_error_syslogng {
    file("/opt/hexis/incoming/syslog-ng/apache_error_syslogng/
apache_error_syslogng.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};

filter f_apache_error_syslogng {
    program('apache_error');
};

log {
    source(s_network_std); source(s_network_tls);
    filter(f_apache_error_syslogng);
    destination(d_apache_error_syslogng);
    flags(final);
};

```

TROUBLESHOOTING

Some systems come preinstalled with SELinux, the NSA's Security Enhanced Linux system. This system can be complicated and difficult to use unless you are already familiar with it; if installed the system may be running by default and will prevent any of your log messages from getting to syslog via the SenSage AP logger program. The easiest way to fix this problem is to disable SELinux; to do this, su to the root user and issue this command:

```
/usr/sbin/setenforce 0
```

After you have done this, the error logs from Apache should start to appear in your syslog feed.

CHAPTER 20

catbird_vsecurity_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	catbird_vsecurity_syslogng
Log Adapter Version	1.0.0
Source Vendor	Catbird
Source Product	HypervisorShield
Source Component	vSecurity
Source Version	5.0
Source Host OS	Red Hat 5 or 6
Transport Mechanism	syslog
PTL Filename	catbird_vsecurity_syslog.ptl
Parsing Rule	catbird_vsecurity_syslog.rule
Alerting Rule	catbirdEventMatch_template.rule.xml
Connector Views	<ul style="list-style-type: none">networkDeviceConnection_catbird_vsecurity_cef_syslogng.sqlinvestigation_catbird_vsecurity_cef_syslongng.sql
Look-up file	Not required.
Scripts	Not required
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none">“Network Device Connection”, on page 121“Audit Event”, on page 109

SETTING UP THE CATBIRD_VSECURITY_SYSLOGNG

This document describe how to configure the catbird_vsecurity_syslogng log adapter. The following steps are required:

- [“Source System syslog Setup”, next](#)
- [“SenSage AP Collector syslog-ng Setup”, on page 466](#)

SOURCE SYSTEM SYSLOG SETUP

Configure your Catbird device to forward event information to the **SenSage AP** Collector following standard procedures defined by Catbird. If you need additional assistance configuring your source device please contact Professional Services.

SEN SAGE AP COLLECTOR SYSLOG-NG SETUP

To configure your log adapter, make the following configuration change on the host running the **SenSage AP** Collector:

- 1 Edit `/etc/syslog-nginx.conf` on the host running the **SenSage AP** Collector, configuring a filter statement, a destination statement, and a log statement as shown below:

- Filter statement:

```
filter f_cat { match("Catbird-1.0" value ("MESSAGE")); };
```

- Destination statement:

```
destination d_cat {  
    file("HawkEye AP Home/incoming/syslog-nginx/catbird_vsecurity_cef_syslogng/  
        catbird_vsecurity_cef_syslogng.log"  
        template  
        ("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST $MSG\n")  
        template_escape(no) );  
};
```

NOTE: Change the path and file name of the “file” argument to match the location of your log file. This argument must match the location of your retriever as specified in the Collector config.xml.

- Log statement:

```
log {  
  
    source(s_network_std);  
    filter(f_cat);  
    destination(d_cat);  
    flags(final);  
};
```

- 2 Restart the syslog-nginx daemon.

- 3 Edit the **SenSage AP** Collector config.xml with sections for logqueue, retriever, loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

- 4 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

CHAPTER 21

checkpoint_opsec_lea

SUMMARY INFORMATION

Log Adapter Component	Details
Name	checkpoint_opsec_lea
Version	1.0.0
Source Vendor	Checkpoint
Source Product	OPSEC
Source Component	Checkpoint OPSEC
Source Version	R75
Source Host OS	Windows Server 2003 Windows Server 2008 IPSO 6.2 SecurePlatform Crossbeam XOS 9.5 or later
Transport Mechanism	LEA
PTL Filename	checkpoint_opsec_lea.ptl
Parsing Rule	checkpoint_opsec_lea.rule
Alerting Rule	<ul style="list-style-type: none">• checkpoint_opsec_unpatched_CVE.alert.rule• checkpoint_opsec_blklst_outbnd_conn.alert.rule• checkpoint_opsec_blklst_inbnd_conn.alert.rule
Connector Views	<ul style="list-style-type: none">• networkDeviceConnection__firewall__checkpoint_opsec_lea.sql• investigation__checkpoint_opsec_lea.sql
Look-up file	Not required
Scripts	<ul style="list-style-type: none">• checkpoint_opsec_blklst_inbnd_conn.alert.pl• checkpoint_opsec_blklst_outbnd_conn.alert.pl• checkpoint_opsec_unpatched_CVE.alert.pl
Source-Specific Reports	None
Event Types	None

SETTING UP THE CHECKPOINT_OPSEC_LEA LOG ADAPTER

This section describes how to configure the checkpoint_opsec_sftp log adapter. The following procedures are required:

- “Source System syslog Setup”, next
- “SenSage AP System Setup”, on page 468

SOURCE SYSTEM SYSLOG SETUP

To configure the source system (enabling SIC for the OPSEC client), make the following configuration changes on your log source host(s):

- 1 Configure the firewall:
 - a Change the fwospec.conf file on the firewall, specifying the following:

```
lea_server      port 0
lea_server      auth_port 18184
lea_server      auth_type sslca
```
 - b Restart the firewall
- 2 Create the Host Object:
 - a Create an object in SmartDashboard for the Client (that is, the Collector) under **Servers and OPSEC Application -> OPSEC Application**, specifying **LEA** in **Client Entities**. Provide the host IP of the host running the SmartDashboards to IgniteTech.
 - b Name this object appropriately (**logtrack** is suggested) and provide the name to Sensage.
 - c Select as "Host" the LEA server to which the Collector will connect.
 - d Add an activation key in the **SIC Communications** button. Remember this key as you will be asked for it later.
- 3 Locate the firewall (provider 1) to which the client will connect. This will be found in SmartDashboard (**Network Objects -> CheckPoint**).
- 4 Provide to IgniteTech the DN for this object (located in the SIC Communications area at the bottom of the edit view).

SENSAGE AP SYSTEM SETUP

To configure your SenSage AP Collector, the following set up tasks are required:

- SenSage AP Collector Setup
- Custom Alerts Setup

SenSage AP Collector Setup

- 1 Use the logtrack binary to validate that you can pull data:
 - a Create a file called **leacfg** in the following location: <SenSage AP Home>/etc/collector/
 - b Add the following line to this file (note the **IP** is that of the firewall being pulled from):

```
10.0.1.27 18184 0 0 fw.log OPSEC_SSLCA <SenSage AP Home>/etc/collector/
logtrack.conf
```

NOTE: If you are not using SSL communications, use this line in the **leacfg** file to test:

```
10.0.1.27 18184 0 0
```

To test run this command:

```
<SenSage AP Home>/bin/logtrack -file=
<SenSage AP Home>/etc/collector/leacfg
```

When running this command, you should see data streaming to the screen.

- 2 To configure your SenSage Collector, you can use the following template in the adapter's directory: **collector_config_template.xml**

opt/hexis/hawkeye-ap/etc/collector/adapters/checkpoint_opsec_lea/config.xml, make sure that you have following r_checkpoint_opsec_lea retriever section:

```
<Retriever name="r_checkpoint_opsec_lea" type="lea" enabled="1">
  <LogQueue>q_checkpoint_opsec_lea</LogQueue>
  <SourceHost SIC="SSLCA_OPSEC" opsecFile="/opt/hexis/hawkeye-ap/etc/
  collector/logtrack.conf">10.0.1.27</SourceHost>
  <Mode>unified</Mode>
  <PollInterval>1200</PollInterval>
</Retriever>
```

NOTES:

- PollInterval is in seconds and represents how often the log file rolls to be loaded.
- if not using SSL specify SourceHost as in the following example:

```
<SourceHost>10.0.1.27</SourceHost>
```

- 3 After adding the Retriever and restarting the Collector, go to:

```
<log_queue>/scratch/<retriever_name>
```

where:

- <**log_queue**> - is the log adapter queue specified in **collector_config_collector.xml**, as in:

```
<SenSage AP Home>/data/collector/queue/checkpoint_opsec_lea/
```

In <**log_queue**>/scratch/<retriever_name>, you should see a file named with the IP of the firewall. This is the output file..tail, which shows data coming in. After the Polling Interval, it rotates into the queue for loading.

Custom Alerts Setup

1 Go to the Adapter folder:

```
cd /opt/hexis/hawkeye-ap/analytics/adapters/checkpoint_opsec_lea/
```

2 Add those CVEs that you do not require to trigger an alert to the **patched_CVEs** file.

3 Run the installation step:

```
./real_time/alerts/checkpoint_opsec_unpatched_CVE.alert.pl
```

4 Check the RuleStatus Directory to verify that the new rule exists and the status is 'Ok'.

```
cat '/opt/hexis/hawkeye-ap/data/rt/Parser/RuleStatus/
checkpoint_opsec_unpatched_CVE.alert.rule.status'
```

5 Test the alert with sample data:

```
nc localhost 5014 < ./real_time/alerts/CVE_sample
```

6 If the **patched_CVEs** file is updated on a regular basis, add the installation script to cron:

```
crontab -e
```

```
0 1 * * *
/opt/hexis/hawkeye-ap/analytics/adapters/checkpoint_opsec_lea/real_time/
alerts/checkpoint_opsec_unpatched_CVE.alert.pl > /dev/null 2>&1
```

7 Add those IPs that you require to trigger an outbound alert to the **outbound_IPs_blacklist** file.

```
crontab -e
```

8 Run the installation script:

```
./real_time/alerts/checkpoint_opsec_blklst_outbnd_conn.alert.pl
```

9 Check the RuleStatus Directory to verify the new rule exists and the status is 'OK'.

```
cat
'/opt/hexis/hawkeye-ap/data/rt/Parser/RuleStatus/
checkpoint_opsec_blklst_outbnd_conn.alert.rule.status'
```

10 Test the alert with sample data:

```
nc localhost 5014 < ./real_time/alerts/outbound_sample
```

11 If the **outbound_IPs_blacklist** file is updated on a regular basis, add the installation script to cron:

```
crontab -e
```

```
0 1 * * *
/opt/hexis/hawkeye-ap//analytics/adapters/checkpoint_opsec_lea/real_time/
alerts/checkpoint_opsec_blklst_inbnd_conn.alert.pl > /dev/null 2>&1
```

CHAPTER 22

cisco_acs_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	cisco_acs_syslogng
Version	1.1.0
Source Vendor	Cisco Systems
Source Product	Access Control Server
Source Component	N/A
Source Version	8.x
Source Host OS	Appliance
Transport Mechanism	syslog-ng
PTL Filename	cisco_acs_syslogng.ptl
Parsing Rule	N/A
Alerting Rule	<ul style="list-style-type: none">• cisco_asa_syslogng.eventid.library.rule• cisco_asa_syslogng.library.rule• cisco_asa_syslogng.rule
Connector Views	<ul style="list-style-type: none">• alert_cisco_acs_syslogng• investigation_cisco_acs_syslogng• parsedData_cisco_acs_syslogng• remoteAccess_cisco_acs_syslogng• unparsedData_cisco_acs_syslogng
Look-up file	None
Scripts	Not required
Source-Specific Reports	None
Event Types	Remote Access

SETTING UP CISCO_ACS_SYSLOGNG LOG ADAPTER

This section describes how to configure the cisco_acs_syslogng log adapter. The following steps are required:

- “[Source System Setup](#)”, next

- “[HawkEye Collector Configuration](#)”, on page 422

Source System Setup

To enable or disable a CSV log:

1 In the navigation bar, click **System Configuration**.

2 Click **Syslog Logging disable**.

3 Click the name of the CSV log that you want to enable.

The CSV log Comma-Separated Values File Configuration Page is displayed. Note that the log name is the CSV log that you just selected.

4 To enable the log, under **Enable Logging**, check the Log to CSV Log Report. check box. Note that the log name is the CSV log that you selected in Step 3.

5 Click **Submit**.

If you enabled the log, ACS begins logging information for the log that you selected. If you disabled the log, ACS stops logging information for the log that you selected.

SenSage AP Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage Collector:

1 Open syslog-ng configuration file <SenSage AP Home>/etc/syslog-ng/syslog-ng.conf on the host running the SenSage AP Collector.

2 Make sure that following destination, filter, and log statements are configured as shown below:

```
# External Destinations - Cisco ACS
destination d_acs {
    file("/opt/hexis/incoming/syslog-ng/cisco_acs_syslogng/cisco_acs.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSG\n")
        template_escape(no) );
};

filter f_acs {
    message("CSCOacs_") or message("CisACS_");
};

log {
    source(s_network_std);
    source(s_network_tls);
    filter(f_acs);
    destination(d_acs);
    flags(final);
};
```

3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

- 4 Edit the SenSage Collector **config.xml** with sections for logqueue, retriever, and loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.
- 5 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

Configuration Files Samples

The section contains the following configuration file samples:

- Collector configuration (**config.xml**)
- Syslog-ng configuration entries (**syslog-ng.conf**)

Collector Configuration (**config.xml**)

```
<Retriever enabled='1' type='filesystem' name='r_cisco_acs_syslogng'
deleteOriginal='1' method='copy'>
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_cisco_acs_syslogng</LogQueue>
<SourceDir>/opt/hexis/incoming/syslog-ng/cisco_acs_syslogng</SourceDir>
<Plugin name='Default'>
<File ai='ignore' id='1'>.*</File>
<File ai='accept' id='2'>.*\.loadme$</File>
</Plugin>
</Retriever>

<LogQueue path='queue/cisco_acs_syslogng' minMBFree='100'
name='q_cisco_acs_syslogng' encoding='UTF-8' />

<Loader enabled='1' name='l_cisco_acs_syslogng'>
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_cisco_acs_syslogng</LogQueue>
<SLSInstance>cisco-device-04.net.company.com:8072</SLSInstance>
<SLSUser>administrator</SLSUser>
<SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>
<PTL table='cisco_acs_syslogng' namespace='analytics' type='file'>
<Location>/opt/hexis/hawkeye-ap/analytics/adapters/cisco_acs_syslogng/
cisco_acs_syslogng.ptl</Location>
<LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
</PTL>
</Loader>
```

Syslog-ng Configuration Entries (**syslog-ng.conf**)

```
destination d_acs {
    file("/opt/hexis/incoming/syslog-ng/cisco_acs_syslogng/cisco_acs.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSG\n")
        template_escape(no) );
};

filter f_acs {
    message("CSCOacs_") or message("CisACS_");
};
```

```
log {  
    source(s_network_std);  
    source(s_network_tls);  
    filter(f_acs);  
    destination(d_acs);  
    flags(final);  
};
```

CHAPTER 23

cisco_asa_syslogng**SUMMARY INFORMATION**

Log Adapter Component	Details
Name	cisco_asa_syslogng
Version	1.0.6
Source Vendor	Cisco Systems
Source Product	Adaptive Security Appliance
Source Component	N/A
Source Version	8.x
Source Host OS	Appliance
Transport Mechanism	syslog-ng
PTL Filename	cisco_asa_syslogng.ptl
Parsing Rule	cisco_asa_syslogng.rule cisco_asa_syslogng.library.rule cisco_asa_syslogng.eventid.library.rule
Alerting Rule	cisco_asa_syslogng.eventid.library.rule cisco_asa_syslogng.library.rule cisco_asa_syslogng.rule
Connector Views	<ul style="list-style-type: none"> • idsIps__cisco_asa_syslogng • investigation__cisco_asa_syslogng • networkDeviceConnection__firewall__cisco_asa_syslogng • parsedData__cisco_asa_syslogng • privilegedCommand__cisco_asa_syslogng • unparsedData__cisco_asa_syslogng • userLogin__cisco_asa_syslogng
Look-up file	None
Scripts	Not required
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none"> • NetworkDeviceConnection • User Login

SETTING UP CISCO ASA SYSLOGNG LOG ADAPTER

This section describes how to configure the cisco_asa_syslogng log adapter. The following steps are required:

- “Source System Setup”, next
- “SenSage AP Collector Configuration”, on page 476

Source System Setup

- 1 Login to device and enter command `show logging`.
- 2 Check the output and note the logging for syslog that is disabled. For example:
 - Syslog logging: disabled
 - ◆ Facility: 20
 - ◆ *Timestamp logging: disabled*
 - ◆ *Standby logging: disabled*
 - ◆ *Deny Conn when Queue Full: disabled*
 - ◆ *Console logging: disabled*
 - ◆ *Monitor logging: disabled*
 - ◆ *Buffer logging: disabled*
 - ◆ *Trap logging: disabled*
 - ◆ *History logging: disabled*
 - ◆ *Device ID: disabled*
 - ◆ *Mail logging: disabled*
 - ◆ *ASDM logging: disabled*
- 3 If logging is disabled, then enter the command `logging enable`.

SenSage AP Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open syslog-ng configuration file <HawkEye AP Home>/etc/syslog-ng/syslog-ng.conf on the host running the SenSage AP Collector.
- 2 Make sure that following destination, filter, and log statements are configured as shown below:

```
# External Destinations - Cisco ASA
destination d_asa {
    file("/opt/hexis/incoming/syslog-ng/cisco_asa_syslogng/cisco_asa.log")
```

```

        template ("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) ;
};

filter f_asa {
    program(%ASA) or message(%ASA);
};

log {
    source(s_network_std);
    source(s_network_tls);
    filter(f_asa);
    destination(d_asa);
    flags(final);
};

```

3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

4 Edit the SenSage AP Collector **config.xml** with sections for logqueue, retriever, loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

5 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

Configuration Files Samples

The section contains the following configuration file samples:

- Collector configuration ([config.xml](#))
- Syslog-*ng* configuration entries ([syslog-*ng*.conf](#))

Collector Configuration ([config.xml](#))

```

<Retriever type='filesystem' enabled='1' name='r_cisco_asa_syslogng'
deleteOriginal='1' method='copy'>
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_cisco_asa_syslogng</LogQueue>
    <SourceDir>/opt/hexis/incoming/syslog-ng/cisco_asa_syslogng</SourceDir>
    <Plugin name='Default'>
        <File ai='ignore' id='1'>.*</File>
        <File ai='accept' id='2'>.*\loadme$</File>
    </Plugin>
</Retriever>

<LogQueue path='queue/cisco_asa_syslogng' minMBFree='100'
name='q_cisco_asa_syslogng' encoding='UTF-8' />

<Loader enabled='1' name='l_cisco_asa_syslogng'>
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_cisco_asa_syslogng</LogQueue>
    <SLSInstance>analytics.example.com:8072</SLSInstance>
    <SLSUser>administrator</SLSUser>
    <SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>

```

```
<PTL table='cisco_asa_syslogng' namespace='analytics' type='file'>
<Location>/opt/hexis/hawkeye-ap/analytics/adapters/cisco_asa_syslogng/
cisco_asa_syslogng.ptl</Location>
<LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
</PTL>
</Loader>
```

Syslog-NG Configuration Entries (**syslog-NG.conf**)

```
destination d_asa {
    file("/opt/hexis/incoming/syslog-NG/cisco_asa_syslogng/cisco_asa.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};

filter f_asa {
program(%ASA) or message(%ASA);
};

log {
source(s_network_std);
source(s_network_tls);
filter(f_asa);
destination(d_asa);
flags(final);
};
```

CHAPTER 24

cisco_ios_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	cisco_ios_syslogng
Version	2.1.0
Source Vendor	Cisco Systems
Source Product	IOS Firewall
Source Component	None
Source Version	11.x
Source Host OS	Appliance
Transport Mechanism	syslogng
PTL Filename	cisco_ios_syslogng.ptl
Parsing Rule	cisco_ios_syslogng.rule
Alerting Rule Template	Cisco IOS Substring Match Rule
Connector Views	<ul style="list-style-type: none">• investigation_cisco_ios_syslogng• networkDeviceConnection_firewall_cisco_ios_syslogng• userLogin_router_cisco_ios_syslogng
Look-up file	None
Scripts	None
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none">• “Network Device Connection”, on page 121• “Audit Event”, on page 109• “User Logins: Router”, on page 143• “Unparsed Data”, on page 139

SETTING UP THE CISCO_IOS_SYSLOGNG LOG ADAPTER

This document describe how to configure the cisco_ios_syslogng log adapter. The following steps are required:

- “Source System Setup”, next
- “SenSage AP Collector syslog-ng Setup”, on page 480

For more information about configuring Cisco routers, see http://www.cisco.com/en/US/products/sw/cscowohrk/ps2073/products_tech_note09186a00800a7275.shtml.

SOURCE SYSTEM SETUP

To configure your Cisco IOS source device:

- 1 Login to the device and enter CONFIG T mode.
- 2 Ensure that logging is enabled by issuing the `logging on` command:

```
Router(config)# logging on
```

- 3 Set the logging level using the following command.

```
Router(config)#logging trap informational
```

The informational portion of the command signifies severity level 6. This means all messages from level 0-5 (from emergencies to notifications) are logged to the SenSage AP Collector.

- 4 To verify that the device sends syslog messages, run the `sh logging` command to see the syslog messages that are sent. If you do not see syslog messages, make sure the following are configured:

- `logging on`
- `logging console debug`
- `logging monitor debug`
- `logging trap debug`
- `logging host <IP_address> transport tcp port 5140`

- 5 Exit the CONFIG mode by typing `CTRL+Z`

- 6 Save your changes by typing the following command:

```
Write Mem
```

SENSAGE AP COLLECTOR SYSLOG-NG SETUP

This section discusses setting up syslog-`ng` on the SenSage AP Collector. For more information on using `syslog-ng` in your SenSage AP deployment, see [Appendix B: SYSLOG-`NG` Setup](#).

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Edit `/etc/syslog-ng.conf` on the host running the SenSage AP Collector, configuring a `filter` statement, a `destination` statement, and a `log` statement as shown in the following example:

- Filter statement:

```
filter f_ios { facility(local7); };
```

NOTE: Any log sources using facility “local7” will be collected.

■ Destination statement:

```
destination d_ios {  
    file("<SenSage AP Home>/incoming/syslog-ng/cisco_ios_syslogng/  
cisco_ios_syslogng.log")  
    template  
    ("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST $MSG\n")  
    template_escape(no) );  
};
```

■ Log statement:

```
log { source(s_network_ssi); filter(f_ios); destination(d_ios);  
flags(final); }
```

2 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

3 Edit the **SenSage AP Collector config.xml**, including sections for `logqueue`, `retriever`, and `loader`. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

(Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

CHAPTER 25

cisco_ips_alert_error

SUMMARY INFORMATION

Log Adapter Component	Details
Name	cisco_ips_alert_error
Version	1.0.0
Source Vendor	Cisco Systems
Source Product	IPS Appliance
Source Component	N/A
Source Version	6.x/7.x
Source Host OS	Appliance
Transport Mechanism	Script retriever
PTL Filename	cisco_ips_alert_error.ptl
Parsing Rule	N/A
Alerting Rule	N/A
Connector Views	<ul style="list-style-type: none">investigation_cisco_ips_alert_error.sql
Look-up file	N/A
Scripts	<ul style="list-style-type: none">cisco_ips_alert_error.retriever.plSS_SDEE.pm
Source-Specific Reports	None
Event Types	Investigation Event

SETTING UP CISCO_IPS_ALERT_ERROR LOG ADAPTER

This section describes how to configure the cisco_ips_alert_error adapter. The following steps are required:

- “Source System Setup”, next
- “HawkEye Collector Configuration”, on page 435

Source System Setup

There are two methods for setting up a Viewer user role on a Cisco IPS appliance: either using the web interface or the command line interface. Since the web interface varies from software version 6 to version 7, the instructions provided below are for adding a user via the command line interface. Note that the Viewer user role is limited to viewing data only and does not have permission to make device modifications or to even log in to the device.

- 1 Log in to the IPS appliance as the Administrator user and on the command line issue the following commands:

- a Enter configuration mode:

```
sensor# configure terminal
```

- b Issue the username command to add the user:

```
sensor(config)# username username privilege viewer
```

Example: Adding a SenSage AP User with a Viiewer Role Privilege:

```
sensor(config)# username sensage privilege viewer
Enter Login Password: *****
Re-enter Login Password: *****
sensor(config) #
```

For more information on how to set up your Cisco IPS Appliance, please refer to the configuration guides on Ciscos support web site:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_installation_and_configuration_guides_list.html

- 2 Configure the IPS conf file:

Before you can test the script retriever, you first must modify the configuration file. A sample configuration file is included in the package, called **cisco_ips_alert_error.retriever.conf**.

In the script are several required fields, including the username and password of the user on the Cisco IPS Appliance, and the actual appliances IP number.

The format looks like the following:

```
host : 10.10.10.10
user : sensage
pass : sensage1
state_dir : /opt/sensage/latest/data/collector/state
startTime : 1199211920886180000
```

You can add comments with the pound sign (#) anywhere in the file except on the same line as one of the options.

REQUIRED:

On the host line, you will want to enter the IP number of the IPS Appliance.

On the user line, you will want to enter the user name that you have set up on the IPS Appliance for use with this retriever (the same user name that was created in section 1b.).

On the pass line, you will want to enter the password for the user above.

OPTIONAL:

On the path line, you can leave this value alone, unless you want the Collector to pick up the log files generated from the retriever in some other place.

On the startTime line, you can leave this value alone. It sets the initial start time to look for events and is ignored after the first time the retriever has run.

If you wish to run the retriever against multiple IPS Appliances, it is common practice to just name each configuration file after the IPS Appliance you are running it against, like **192.168.10.5.conf**, **192.168.10.6.conf**, etc.

3 Test the retriever:

Before you set up the script retriever to run on a normal basis, test it first. To do this, start the retriever via the command line. Access the SenSage AP box on which you are installing the retriever.

After the Viewer user role has been set up and you have filled out the configuration file, you can test the script by running it, as in:

```
./cisco_ips_alert_error.retriever.pl cisco_ips_alert_error.retriever.conf /  
opt/sensage/incoming/cisco_ips_alert_error/cisco_ips_alert_error.log
```

The script creates the following three files:

- A lock file--This file is created to ensure only one retriever is run against a specific IPS appliance at any one time, and will be named after the IP of the device with ".lock" at the end.
- A data file (specified in command line)--This file contain the actual data retrieved from the IPS appliance and is preformatted and ready to be loaded into SenSage.
- A state file (in the state dir)--This file starts with a UNIX epoch timestamp and ends with ".state". This file keeps the state of our retriever and when the last set of data was retrieved from, so it knows where to start on the next retrieval.

If there were no errors and all three files have been created successfully, you are ready to set up the script retriever in collector configuration file.

SenSage AP Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open the SenSage AP Collector **config.xml** configuration file <*SenSage_Home*>/etc/collector/**config.xml** on the host running the SenSage Collector.
- 2 Edit the SenSage AP Collector **config.xml** with sections for logqueue, retriever, loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

SAMPLE CONFIGURATION FILES

The following are sample configuration files:

Collector Configuration (**config.xml**)

```
<Retriever type='filescript' enabled='1' name='r_cisco_ips_alert_error'
deleteOriginal='1' method='copy'>
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_cisco_ips_alert_error</LogQueue>
    <SourceCommand>/opt/sensage/latest/analytics/adapters/
cisco_ips_alert_error/cisco_ips_alert_error.retriever.pl /opt/sensage/latest/
analytics/adapters/cisco_ips_alert_error/cisco_ips_alert_error.retriever.conf
%F</SourceCommand>
    <PollInterval>3600</PollInterval>
</Retriever>

<LogQueue path='queue/cisco_ips_alert_error' minMBFree='100'
name='q_cisco_ips_alert_error' encoding='UTF-8'>

<Loader enabled='1' name='l_cisco_ips_alert_error'>
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_cisco_ips_alert_error</LogQueue>
    <SLSInstance>analytics.example.com:8072</SLSInstance>
    <SLSUser>administrator</SLSUser>
    <SLSSharedKey>file:/opt/sensage/latest/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>
    <PTL table='cisco_ips_alert_error' namespace='analytics' type='file'>
        <Location>/opt/sensage/latest/analytics/adapters/cisco_ips_alert_error/
cisco_ips_alert_error.ptl</Location>
        <LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
    </PTL>
</Loader>
```

Cisco_IPS_Alert_Error.Retriever.Conf Entries

```
host : 168.75.102.56
user : cisco
pass : sp00n*bill
state_dir : /opt/sensage/latest/data/collector/state
startTime : 1199211920886180000
```

CHAPTER 26

cisco_ironport_Email_Security_Appliances**SUMMARY INFORMATION**

Log Adapter Component	Details
Name	<ul style="list-style-type: none"> • cisco_ironport_antispam • cisco_ironport_antivirus • cisco_ironport_auth • cisco_ironport_bounce • cisco_ironport_cli • cisco_ironport_ftp • cisco_ironport_http • cisco_ironport_maillog_archive • cisco_ironport_ntp • cisco_ironport_query • cisco_ironport_report • cisco_ironport_slbl • cisco_ironport_spam_quarantine • cisco_ironport_spam_quarantine_gui
Version	1.0.0
Source Vendor	Cisco IronPort
Source Product	C series Email Security Appliance (ESA)
Source Component	<ul style="list-style-type: none"> • AntiSpam Log • AV Log • Auth Log • Bounce Log • CLI Log • FTPD Log • HTTP Log • Mail log archive • NTP Log • Query Log • Reportd Log • SLBL Log • EUQ Log • EUQ GUI Log • Updater Log
Source Version	6.x
Source Host OS	Appliance
Transport Mechanism	FTP/SCP

Log Adapter Component	Details
PTL Filename	<ul style="list-style-type: none"> • cisco_ironport_antispam.ptl • cisco_ironport_antivirus.ptl • cisco_ironport_auth.ptl • cisco_ironport_bounce.ptl • cisco_ironport_cli.ptl • cisco_ironport_ftp.ptl • cisco_ironport_http.ptl • cisco_ironport_maillog_archive.ptl • cisco_ironport_ntp.ptl • cisco_ironport_query.ptl • cisco_ironport_report.ptl • cisco_ironport_slbl.ptl • cisco_ironport_spam_quarantine.ptl • cisco_ironport_spam_quarantine_gui.ptl • cisco_ironport_updater.ptl
Parsing Rule	N/A
Alerting Rule	N/A
Connector Views	N/A
Look-up file	Not required
Scripts	Not required
Source-Specific Reports	None
Event Types	N/A

SETTING UP CISCO_IRONPORT_EMAIL_SECURITY_APPLIANCES LOG ADAPTER

This document describe how to configure the cisco_ironport_Email_Security_Appliances adapter. The following steps are required:

- “[Source System Setup](#)”, next
- “[SenSage AP Collector Configuration](#)”, on page 489

Source System Setup

- 1 Connect to your Iron Port device.
- 2 Select the System Administration tab.
- 3 Select **Log Subscriptions** from the menu in the left pane.

- 4** Select the Log Name; for example, **mail_logs**.
- 5** Select the Information log level.
- 6** Select for logs to be sent by FTP or SCP on the Remote Server.
- 7** Select the connection information relating to the FTP/SSH server.
- 8** Click the **Submit** button.

SenSage AP Collector Configuration

Edit the SenSage AP Collector config.xml with sections for logqueue, retriever, and loader. For more information see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

Configuration Files Samples

The section contains the following configuration file samples:

- Collector configuration (**config.xml**)

Collector Configuration (**config.xml**)

```

<Retriever type='filesystem' enabled='1' name='r_cisco_ironport_antivirus'
deleteOriginal='1' method='copy'>
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_cisco_ironport_antivirus</LogQueue>
    <SourceDir>/opt/hexis/incoming/cisco_ironport_antivirus</SourceDir>
    <Plugin name='Default'>
        <File ai='ignore' id='1'>.*</File>
        <File ai='accept' id='2'>.*\loadme$</File>
    </Plugin>
</Retriever>

<LogQueue path='queue/cisco_ironport_antivirus' minMBFree='100'
name='q_cisco_ironport_antivirus' encoding='UTF-8' />

<Loader enabled='1' name='l_cisco_ironport_antivirus'>
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_cisco_ironport_antivirus</LogQueue>
    <SLSInstance>analytics.example.com:8072</SLSInstance>
    <SLSUser>administrator</SLSUser>
    <SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>
        <PTL table='cisco_ironport_antivirus' namespace='analytics' type='file'>
            <Location>/opt/hexis/hawkeye-ap/analytics/adapters/
cisco_ironport_antivirus/cisco_ironport_antivirus.ptl</Location>
            <LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
        </PTL>
</Loader>
```


CHAPTER 27

cisco_netflow_receiver

SUMMARY INFORMATION

Log Adapter Component	Details
Name	cisco_netflow_receiver
Log Adapter Version	1.0.0
Source Vendor	Cisco Systems
Source Product	Netflow
Source Component	Netflow Receiver
Source Version	10
Source Host OS	Cisco IOS
Transport Mechanism	Netflow Receiver
PTL Filename	cisco_netflow_receiver.ptl
Parsing Rule	cisco_netflow_receiver.rule
Alerting Rule	N/A
Connector Views	<ul style="list-style-type: none">• investigation_cisco_netflow_receiver• networkDeviceConnection_cisco_netflow_receiver
Look-up file	Lookup file with malware IPs. This lookup file is used in a report to identify destination IPs that are malware sites.
Scripts	Netflow Receiver is required.
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none">• “Network Device Connection”, on page 121• “Audit Event”, on page 109

SETTING UP THE CISCO_NETFLOW_RECEIVER LOG ADAPTER

This document describe how to configure the cisco_netflow_receiver log adapter. The following steps are required:

- “Source System Setup”, next
- “SenSage AP Collector Setup”, on page 492

SOURCE SYSTEM SETUP

To set up the source system, refer to instructions below and the noted links.

- 1 Download **nfdump-1.6.9.tar.gz** from <http://sourceforge.net/projects/nfdump/> (You can go to 'Browse All Files' for old releases):
 - a tar xvzf nfdump-1.6.9.tar.gz
 - b cd nfdump-1.6.9
- 2 Run commands `'./configure -prefix=/opt/hexis; make; make install'`
- 3 Enable the NetFlow feature.
 - See the section "[Enabling the NetFlow Feature](#)"
- 4 Define a flow record by specifying keys and fields to the flow.
 - See the section "[Creating a Flow Record](#)"
- 5 Define an optional flow exporter by specifying the export format, protocol, destination, and other parameters. For the destination, enter the IP address or hostname of the Collector.
 - See the section "[Creating a Flow Exporter](#)"
- 6 Define a flow monitor based on the flow record and flow exporter.
 - See the section "[Creating a Flow Monitor](#)"
- 7 Apply the flow monitor to a source interface, sub-interface, and VLAN interface. See the sections:
 - "[Applying a Flow to an Interface](#)"
OR for a VLAN
 - "[Configuring Bridged NetFlow](#)"

SEN\$AGE AP COLLECTOR SETUP

To configure your log adapter, make the following configuration change on the host running the Sen\$age AP Collector:

- 1 Install/update the Consumer Analytics reports from RPM:

```
rpm -Uvh lms-analytics-consumer-1.0.3.noarch.rpm
```

- 2 Install/update Consumer Analytics:

```
addAnalytics --user=administrator --password=USERPASS --collision=update --  
src=<HawkEye AP Home>/analytics/1.0.3 --dbPassword=DBPASSWORD
```

- 3 Edit the **Sen\$age AP Collector config.xml**, including sections for `logqueue`, `retriever`, and `loader`. For more information, see [Chapter 2: Sen\\$age AP Collector Configuration](#) in the [Collector Guide](#).

4 Restart the Collector.

■ Start Client:

```
/opt/hexis/hawkeye-ap/netflow_client /opt/hexis/hawkeye-ap/etc/netflow/  
netflow_client.prop
```

NOTE: To stop the client add –s before the path to .prop file as shown above.

■ Start Server:

```
/opt/hexis/hawkeye-ap/bin/netflow_server /opt/hexis/hawkeye-ap/etc/netflow/  
netflow_server.prop
```

NOTE: To stop the server add –s before the path to the .prop file as shown above.

5 Send netflow data from your source to port 8888.**6** Check **/tmp/netflow_collector_logs** to see if netflow events are being captured.

CHAPTER 28

cisco_pix_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	cisco_pix_syslogng
Version	2.1.0
Source Vendor	Cisco Systems
Source Product	PIX Firewall
Source Component	None
Source Version	6.x;7.x
Source Host OS	Appliance
Transport Mechanism	syslog-ng
PTL Filename	cisco_pix_syslogng.ptl
Parsing Rule	cisco_pix_syslogng.rule
Alerting Rule	<ul style="list-style-type: none">• Cisco Firewall Event Match Template• Cisco Firewall User Match Template• Cisco PIX Substring Match Rule
Connector Views	<ul style="list-style-type: none">• investigation_cisco_pix_syslogng• networkDeviceConnection_firewall_cisco_pix_syslogng• parsedData_cisco_pix_syslogng• unparsedData_cisco_pix_syslogng
Look-up file	Yes
Scripts	None
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none">• “Network Device Connection”, on page 121• “Audit Event”, on page 109

SETTING UP THE CISCO_PIX_SYSLOGNG LOG ADAPTER

This document describe how to configure the cisco_pix_syslogng log adapter. The following steps are required:

- “Source System Setup”, next

- “[HawkEye Collector Configuration](#)”, on page 496

SOURCE SYSTEM SETUP

- 1 Login to device and enter CONFIG T mode.
- 2 To ensure that logging is enabled, issue the `logging on` command.

```
Router(config)# logging on
```

- 3 Set the logging level to `debug`:

```
Router(config)#logging trap debug
```

- 4 Set the Logging host:

```
logging host ###.###.###.###
```

Where `###.###.###.###` is the IP address of the host running the HawkEye Collector.

- 5 Exit CONFIG mode by typing **CTRL+Z**

- 6 Save your changes by typing the following command:

```
Write Mem
```

HAWKEYE COLLECTOR CONFIGURATION

To configure your log adapter, make the following configuration change on the host running the HawkEye collector:

- 1 Open syslog-ng configuration file `<HawkEye AP Home>/etc/syslog-ng/syslog-ng.conf` on the host running the SenSage collector.
- 2 Make sure that following destination, filter and log statements are configured as shown below:

```
# External Destinations - Cisco PIX
destination d_pix {
    file("<HawkEye AP Home>/incoming/syslog-ng/cisco_pix_syslogng/cisco_pix.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};

filter f_pix {
    program(%PIX) or program(%FWSM) or message(%PIX) or message(%FWSM);
};

log {
    source(s_network_std);
    filter(f_pix);
    destination(d_pix);
    flags(final);
```

3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

4 Edit the SenSage collector config.xml with sections for logqueue, retriever, loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

5 Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

SAMPLE CONFIGURATION FILES

This section contains the following sample configuration files:

- Collector Configuration (**config.xml**)
- Syslog-ng Configuration entries (**syslog-ng.conf**)

Collector Configuration (**config.xml**)

```
<Retriever enabled='1' type='filesystem' name='r_cisco_pix_syslogng'
deleteOriginal='1' method='copy'>
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_cisco_pix_syslogng</LogQueue>
    <SourceDir>/opt/hexis/incoming/syslog-ng/cisco_pix_syslogng</SourceDir>
    <Plugin name='Default'>
        <File ai='ignore' id='1'>.*</File>
        <File ai='accept' id='2'>.*\loadme$</File>
    </Plugin>
</Retriever>

<LogQueue path='queue/cisco_pix_syslogng' minMBFree='100'
name='q_cisco_pix_syslogng' encoding='UTF-8' />

<Loader enabled='1' name='l_cisco_pix_syslogng'>
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_cisco_pix_syslogng</LogQueue>
    <SLSInstance>analytics.example.com:8072</SLSInstance>
    <SLSUser>administrator</SLSUser>
    <SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>
        <PTL table='cisco_pix_syslogng' namespace='analytics' type='file'>
            <Location>/opt/hexis/hawkeye-ap/analytics/adapters/cisco_pix_syslogng/
cisco_pix_syslogng.ptl</Location>
            <LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
        </PTL>
</Loader>
```

Syslog-ng Configuration Entries (**syslog-ng.conf**)

```
destination d_pix {
    file("/opt/hexis/incoming/syslog-ng/cisco_pix_syslogng/cisco_pix.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};
```

```
filter f_pix {  
    program(%PIX) or program(%FWSM) or message(%PIX) or message(%FWSM);  
};  
  
log {  
    source(s_network_std);  
    filter(f_pix);  
    destination(d_pix);  
    flags(final);  
};
```

CHAPTER 29

f5_asm_cef_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	f5_asm_cef_syslogng
Version	2.0.0
Source Vendor	F5
Source Product	ASM
Source Component	N/A
Source Version	10.x.x
Source Host OS	Appliance
Transport Mechanism	syslog-ng
PTL Filename	f5_asm_cef_syslogng.ptl
Parsing Rule	f5_asm_cef_syslogng.rule
Alerting Rule	F5 Application Security Manager Source or Destination IP Match Rule
Connector Views	<ul style="list-style-type: none">• arcsight_cef_f5_asm_cef_syslogng.sql• investigation_f5_asm_cef_syslogng.sql• networkDeviceConnection_f5_asm_cef_syslogng.sql
Look-up file	Not required
Scripts	Not required
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none">• NetworkDeviceConnection• User Login

SETTING UP F5_ASM_CEF_SYSLOGNG LOG ADAPTER

This document describe how to configure the f5_asm_cef_syslogng adapter. The following steps are required:

- “Source System Setup”, next
- “Configuring the Storage Filter”, on page 502

- “[Setting Event Severity Levels for Security Policy Violations](#)”, on page 503
- “[HawkEye Collector Configuration](#)”, on page 454

Source System Setup

Logging Web Application Data

Logging profiles specify how and where the system stores request, response, and violation data for security policies. When you configure a security policy, you select the logging profile for that security policy. You can use one of the system-supplied logging profiles, or you can create a custom logging profile. Note that the system-supplied logging profiles log data locally.

Additionally, you can choose to log the request data locally, on a remote storage system (such as a syslog server), on a reporting server (as key/value pairs), or on an ArcSight server (in CEF format).

NOTE: If running Application Security Manager on a BIG-IP system using Virtualized Clustered Multiprocessing (VCMP), for best performance, F5 recommends configuring remote logging to store Application Security Manager logs remotely rather than locally.

A logging profile has two parts: the storage configuration and the storage filter. The storage configuration specifies where the logs are stored, either locally and/or remotely. The storage filter determines what information gets stored.

Response Logging Content Headers

If you enable response logging in the logging profile, the system can log only responses with the following content headers:

- "text/..."
- "application/x-shockwave-flash"
- "application/sgml"
- "application/x-javascript"
- "application/xml"
- "application/x-asp"
- "application/x-aspx"
- "application/xhtml+xml"
- "application/soap+xml"
- "application/json"

Creating Logging Profiles

To create a logging profile:

- 1 On the Main tab, expand **Application Security**, point to **Options**, and then click **Logging Profiles**.

The Logging Profiles screen opens.

- 2 Above the Logging Profiles area, click the **Create** button.

The Create New Logging Profile screen opens.

- 3 For the Configuration setting, select **Advanced**.

- 4 For the Profile Name setting, type a unique name for the logging profile.

- 5 Clear the Local Storage check box because we do not want to log data locally on the BIG-IP system.

- 6 From the Response Logging list, select one of the following options.

Option	Purpose
Off	Do not log responses.
For Illegal Requests Only	Log responses for illegal requests.
For All Requests	Log responses for all requests. when the Storage Filter Request Type is set to All Requests. (Otherwise, logs only illegal requests.)

NOTE: By default, the system logs the first 10000 bytes of responses, up to 10 responses per second. You can change the limits by using the response logging internal parameters.

- 7 Do not create the profile yet. Continue to Step 8 to set up remote logging.

- 8 From the Create New Logging Profile screen, select the Remote Storage check box.

The screen displays additional settings.

- 9 From the Remote Storage Type, select **ArcSight**, which is the appropriate type:

- 10 For the Protocol setting, select the protocol that the remote storage server uses, either **TCP** (the default setting), **TCP-RFC3195**, or **UDP**.

- 11 For Server Addresses, specify one or more remote servers and reporting servers. Type the IP address, port number (default is 514), and click **Add**.

- 12 If using the Remote storage type, for Facility, select the facility category of the logged traffic. The possible values are **LOG_LOCAL0** through **LOG_LOCAL7**.

TIP: If you have more than one security policy you can use the same remote logging server for both applications, and use the facility filter to sort the data for each.

- 13 For Maximum Request Size, specify how much of a request the server logs. Select **Any** to log the entire request, or type the length in bytes.
- 14 If using the Remote storage type for Maximum Headers Size, specify how much of the header the server logs. Select **Any** to log the entire header, or type the length in bytes.
- 15 If using the Remote or Reporting Server storage types, for Maximum Query String Size, specify how much of a query string the server logs. Select **Any** to log the entire query string, or type the length in bytes.
- 16 For Maximum Entry Length, you can specify how much of the entry length the server logs. The default length is **1K** for remote servers that support the UDP protocol and **2K** for remote servers that support the TCP and TCP-RFC3195 protocols. You can change the default maximum entry length for remote servers that support the TCP protocol.
- 17 Select **Report Detected Anomalies** if you want the system to send a report string to the remote system log when a brute force attack, denial of service attack, IP enforcer attack, or web scraping attack starts and ends.
- 18 In the Storage Filter area, make any changes as required. (refer to Configuring the storage filter, in the official F5 documentation for your appliance.)
- 19 Click the **Create** button.

The screen refreshes, and displays the new logging profile on the Logging Profiles screen.

After creating the logging profile, you can apply it to any security policy.

- 20 To apply a logging profile to a security policy, on the main tab, click **Security Policies**.
- 21 Click the name of the security policy.
- 22 For Logging Profile, select the profile you want to use for the security policy.
- 23 Click **Update**.

Configuring the Storage Filter

The storage filter of a logging profile determines the type of requests the system or server logs.

NOTE: The following procedure describes configuring the storage filter for an existing logging profile. You can also do this while creating a new one.

To configure the storage filter

- 1 On the Main tab, expand Application Security, point to Options, and then click **Logging Profiles**.
The Logging Profiles screen opens.
- 2 In the Logging Profiles area, click the name of an existing logging profile.
The Edit Logging Profile screen opens.
- 3 For the Storage Filter setting, select **Advanced**.

The screen refreshes to display additional settings.

- 4 For the Logic Operation setting, select the manner in which the system associates the criteria you specify. The criteria are the remaining settings in the storage filter.
 - OR:
Select this operator if you want the system to log the data that meets one or more of the criteria.
 - AND:
Select this operator if you want the system to log the data that meets all of the criteria.
- 5 For the Request Type setting, select the kind of requests that you want the system to store in the log.
- 6 For the Protocols setting, select whether logging occurs for HTTP and HTTPS protocols or a specific protocol.
- 7 For the Response Status Codes setting, select whether logging occurs for all response status codes or specific ones.
- 8 For the HTTP Methods setting, select whether logging occurs for all methods or specific methods.
- 9 For the Request Containing String setting, select whether the request logging is dependent on a specific string.
- 10 Click the **Update** button.

Setting Event Severity Levels for Security Policy Violations

You can customize the severity levels of security policy violations for application security events that the system displays in the Security Alerts screen. This is also event severity message logged in the Syslog, in response to violations. The event severity levels are Informational, Notice, Warning, Error, Critical, Alert, and Emergency. They range from least severe (Informational) to most severe (Emergency).

NOTE: When you make changes to the event severity level for security policy violations, the changes apply globally to all security policies.

To customize event severity level for security policy violations:

- 1 On the Main tab, expand Application Security, point to Options.
- 2 From the Advanced Configuration menu, choose Severities.
- 3 For each violation, change the severity level as required.
- 4 Click the **Save** button to retain any changes.

TIP: If you modify the event severity levels for any of the security policy violations, and later decide you want to use the system-supplied default values instead, click the **Restore Defaults** button.

SenSage AP Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open the syslog-ng configuration file <SenSage AP Home>/etc/syslog-ng/syslog-ng.conf on the host running the SenSage AP Collector.
- 2 Make sure that following destination, filter and log statements are configured as shown below:

```
destination d_f5_asm {  
    file("<SenSage AP Home>/incoming/syslog-ng/f5_asm_cef_syslogng/  
f5_asm_cef_syslogng.log"  
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST  
$MSG\n")  
        template_escape(no));  
};  
  
log {  
    source(s_network_std);  
    source(s_network_tls);  
    filter(f_f5_asm);  
    destination(d_f5_asm);  
    flags(final);  
};  
  
filter f_f5_asm {  
match("|F5|ASM|" value ("MESSAGE"));  
};
```

- 3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

- 4 Edit the SenSage AP Collector **config.xml** with sections for logqueue, retriever, and loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

- 5 Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

CHAPTER 30

hexis_hawkeye_g_cef_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	hexis_hawkeye_g_cef_syslogng
Version	1.0.0
Source Vendor	Hexit Cyber Solutions
Source Product	HawkEye
Source Component	G
Source Version	6.*
Source Host OS	RedHat
Transport Mechanism	syslog- <i>ng</i> (cef format)
PTL Filename	hexis_hawkeye_g_cef_syslogng.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	• investigation_hexis_hawkeye_g_cef_syslogng.sql
Look-up file	None
Scripts	None
Source-Specific Reports	None
Event Types	Investigation events

SETTING UP HEXIS_HAWKEYE_G_CEF_SYSLOGNG LOG ADAPTER

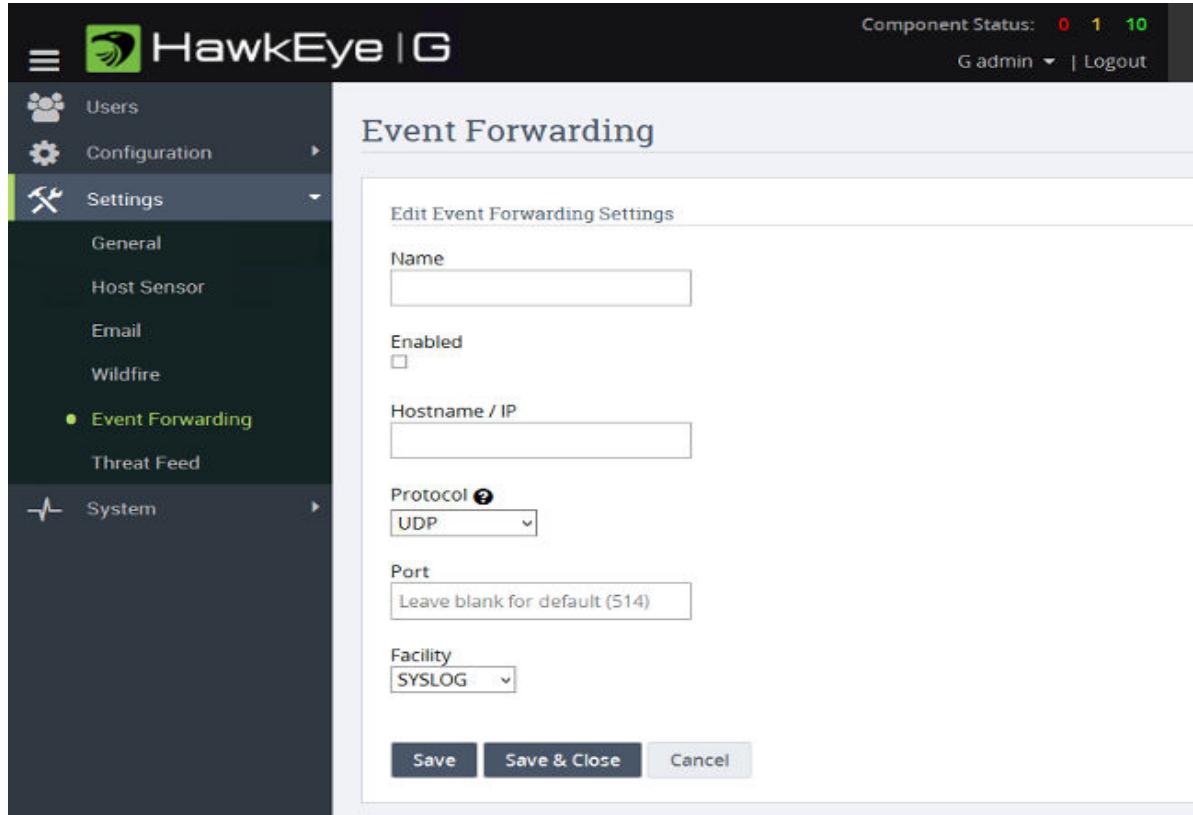
This document describes how to configure the hexis_hawkeye_g_cef_syslogng log adapter. The following steps are required:

- “Source System Setup”, next
- “SenSage AP Collector Configuration”, on page 507

Source System Setup

To configure your source system, make the following configuration changes on your log source host:

- 1 Login to the Administration interface.
- 2 On the navigation menu click **Settings** and then click **Event Forwarding**.
- 3 Click the **Add Server** button on the top-right corner.



- 4 On the Event Forwarding form, enter a name. Note that this field is optional.
- 5 Click the **Enabled** checkbox.
- 6 Enter the Hostname/IP address of the SenSage AP Collector.
- 7 Select a protocol and enter a port number.
- 8 Select SYSLOG as the facility.
- 9 Click the **Save** button.
- 10 Click the name of the security policy.
- 11 For Logging Profile, select the profile you want to use for the security policy.
- 12 Click **Update**.

SenSage AP Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open the syslog-ng configuration file <SenSage AP Home>/etc/syslog-ng/syslog-ng.conf on the host running the SenSage Collector.
- 2 Make sure that following destination, filter and log statements are configured as shown below:

```
destination d_hawkeye_g {
    file("/opt/hexis/hawkeye-ap/incoming/syslog-ng/
hexis_hawkeye_g_cef_syslogng/hexis_hawkeye_g_cef_syslogng.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};

filter f_hawkeye_g {
    message("CEF:") and message("HawkEyeG");
};

log {
    source(s_network_std);
    filter(f_hawkeye_g);
    destination(d_hawkeye_g);
};
```

- 3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

- 4 Edit the SenSage AP Collector config.xml with sections for logqueue, retriever, and loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.
- 5 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

SAMPLES OF CONFIGURATION FILES

This section contains the following sample configuration files:

- collector configuration (config.xml)
- syslog-ng configuration entries (syslog-ng.conf)

Collector Configuration (Config.xml)

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Collector SYSTEM "config.dtd">
<Collector version='6.0' enabled='1'>
    <LogQueues>
        <LogQueue path='queue/hexitis_hawkeye_g_cef_syslogng' minMBFree='100'
name='q_hexis_hawkeye_g_cef_syslogng' encoding='UTF-8'/>
    </LogQueues>
    <Retrievers>
        <Retriever enabled='1' type='filesystem'
name='r_hexis_hawkeye_g_cef_syslogng' deleteOriginal='1' method='copy'>
            <RunOnHost>localhost</RunOnHost>
            <LogQueue>q_hexis_hawkeye_g_cef_syslogng</LogQueue>
            <SourceDir>/opt/hexitis/hawkeye-ap/incoming/syslog-ng/
hexis_hawkeye_g_cef_syslogng</SourceDir>
            <Plugin name='Default'>
                <File ai='ignore' id='1'>.*</File>
                <File ai='accept' id='2'>.*\.loadme$</File>
            </Plugin>
        </Retriever>
    </Retrievers>
    <Loaders>
        <Loader enabled='1' name='l_hexis_hawkeye_g_cef_syslogng'>
            <RunOnHost>localhost</RunOnHost>
            <LogQueue>q_hexis_hawkeye_g_cef_syslogng</LogQueue>
            <SLSInstance>analytics.example.com:8072</SLSInstance>
            <SLSUser>administrator</SLSUser>
            <SLSSharedKey>file:/opt/hexitis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>
            <PTL table='hexis_hawkeye_g_cef_syslogng' namespace='analytics'
type='file'>
                <Location>/opt/hexitis/hawkeye-ap/analytics/6.0.1/adapters/
hexis_hawkeye_g_cef_syslogng/hexitis_hawkeye_g_cef_syslogng.ptl</Location>
                <LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
            </PTL>
        </Loader>
    </Loaders>
</Collector>
```

Syslog-NG Configuration Entries (syslog-ng.conf)

```
destination d_hexis_hawkeye_g {
    file("/opt/hexitis/hawkeye-ap/incoming/syslog-ng/hexitis_hawkeye_g_cef_syslogng/
hexis_hawkeye_g_cef_syslogng.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};

filter f_hexis_hawkeye_g {
    message("CEF:") and message("HawkEyeG");
};

log {
    source(s_network_std);
    filter(f_hexis_hawkeye_g);
```

```
destination(d_hawkeye_g);
```


CHAPTER 31

hp_nonStop_ems_cinset_nset

SUMMARY INFORMATION

Log Adapter Component	Details
Name	hp_nonStop_ems_cinset_nset
Version	None
Source Vendor	Hewlett-Packard
Source Product	NonStop O/s
Source Component	EMS
Source Version	Hewlett-Packard
Source Host OS	NonStop
Transport Mechanism	NSET Scripts
PTL Filename	hp_nonStop_ems_cinset_nset.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	None
Look-up file	None
Scripts	None
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none">• “Audit Event”, on page 109• “Password Changes and Resets”, on page 127• “Privileged Commands”, on page 129• “Unparsed Data”, on page 139

SETTING UP THE HP_NONSTOP_EMSCINSET_NSET LOG ADAPTER

CINSET collects EMS and Safeguard event and audit data from NonStop systems and makes it available for analysis in SenSage AP. The tar file consists of the following components:

- `call_nonstop_retriever.pl` This is the retriever Perl script executed by the `crontab`. It uses `ems_retriever.pl` and `safeguard_retriever.pl` to SSH into each NonStop device and executes the `getsgd` TACL script to collect safeguard audit data; then runs `emdist` to collect EMS data. This script is owned by the `Ims` user.
- `nonstop_retriever_config`. This is an input file `call_nonstop_retriever.pl` reads to tell it the IP addresses of the NonStop machines to collect data from and the user names to log onto those machines as. The file resides in the `Ims` user home directory.
- `getsgd`. This is a TACL script (get Safeguard data) that is executed on NonStop systems. It must be placed in `$SYSTEM.NSET` on each NonStop system safeguard data is to be retrieved from.
- `hp_nonstop_config.xml`. Sample Collector `config.xml` file showing modifications needed to support CINSET on SenSage AP.
- `make_nonstop_directories.sh`. Simple script to create additional directories needed to support CINSET

In the `hp_nonstop_safeguard` sub-directory:

- `safeguard.audit_reduction.ptl`. This is the ptl file that specifies the parsing rules for the NonStop Safeguard audit stream.
- `safeguard.retriever.pl`. This directly SSH's into a NonStop machine to retrieve Safeguard audit data. Executed by `call_nonstop_retriever.pl`
- `safeguard.audit_reduction.preproc` This is preprocessor for the Safeguard audit data.

In the `hp_nonstop_ems` sub-directory:

- `nonstop_ems.ptl`. This is the ptl file that specifies the parsing rules for the NonStop EMS event stream.
- `ems_retriever.pl`. This directly SSH's into a NonStop machine to retrieve EMS event log data. Executed by `call_nonstop_retriever.pl`
- `nonstop_ems.preproc`. This is the pre-processor for the EMS data.

STEPS TO IMPLEMENT CINSET

The sections below describe the steps that should be implemented in order for CINSET to become operational in a customer environment.

Step 1: Install Log Adapters and Modify config.xml

Modify the SenSage AP `config.xml` file per the `hp_nonstop_config.xml` example file included in the tar. Also execute the `make_nonstop_directories.sh` script to create appropriate incoming directories and the statefiles sub-directory under `Ims`.

Also appropriately install the `nonstop_ems.ptl`, `ems_retriever.pl`, `nonstop_ems.preproc`, `safeguard.audit_reduction.preproc`, `safeguard.retriever.pl`, `safeguard.audit_reduction.ptl` files to their appropriate directories.

Step 2: Creating SSH Keying Relationship

The `call_nonstop_retriever.pl` script will call `safeguard.retriever.pl` and `ems_retriever.pl` to actually use SSH to log into each NonStop machine and initiate the `getsgd` script and the `emsdist` command. In order to use SSH, a DSA public/private key pair must be created, then the fingerprint of the DSA public key must be established on each NonStop system SenSage AP will be accessing.

The key pair will be generated for the `lms` user. If a key pair already exists (there will be a `.ssh` sub-directory in the `/home/lms` directory), then one can simply use the existing key. Execute the following command to display the fingerprint of the DSA public key that has already generated:

```
ssh-keygen -l -f /home/lms/.ssh/ide_dsa.pub
```

After noting the key fingerprint, `cd` to the `.ssh` directory and issue the following commands:

```
% cp id_dsa.pub safeguard_id_dsa.pub  
% cp id_dsa safeguard_id_dsa
```

If a key pair has not already been generated for the `lms` user, then execute the following command

```
% ssh-keygen -t dsa
```

Again do this as the `lms` user. Do not specify a passphrase for the private key and again make sure you save a copy of the public key fingerprint (as you will be using it on the NonStop systems you want to gain access to).

Again, when you execute the `keygen` command the keys will be placed in the home directory of the `lms` user, under a `.ssh` directory. Observe in this `ssh` directory the names of the files will be:

```
id_dsa.pub  
id_dsa
```

You will need to copy these file to

```
safeguard_id_dsa.pub  
safeguard_id_dsa
```

using the `cp` commands shown above.

Step 3: Actions Needed in the NonStop Environment

Next, on each NonStop machine SenSage AP must interact with, the public key fingerprint must be installed for the NonStop user SenSage AP is logging in as. For this example assume the user is `<user-name>` and the public key is

```
a1:b1:c2:d3:11:12:13:14:21:24:25:31:34:b2:c3:d4
```

To do this one needs to execute the following on the NonStop machine.

```
2> sshcom $zss0
```

(note each customer's ssh processes will vary; that is, it might not be labeled \$zss0. Consult the system administrator for the appropriate stack to use. Stacks can be listed using the following commands

```
3> scf
```

```
1-> info process $zzkrn.#ssh*
```

After you get the sshcom prompt (after entering the sshcom command) enter the following command:

```
% alter user <user-name>, publickey key1 fingerprint  
a1:b1:c2:d3:11:12:13:14:21:24:25:31:34:b2:c3:d4  
OK, user <user-name> altered  
% quit  
3>
```

Here <user_name> is the user SenSage AP logs in as on that particular NonStop system.

Repeat these steps on every machine SenSage AP must log into. Note if the sshcom command is not recognized, you might need to explicitly specify the path:

```
1> run $system.zssh.sshcom $zss0
```

Finally, install the getsqd script on each NonStop machine SenSage AP must access. The script must be installed under \$system.nset and is thus invoked by SenSage AP perl scripts as \$system.nset.getsqd

Step 4: Getting Things Ready to Run

Modify the crontab to run call_nonstop_retriever.pl at a regular intervals, for instance every hour. Next modify the nonstop_retriever_config file (to be placed in the lms home directory) with the IP addresses and user names SenSage AP should utilize to log into every NonStop machine event data is to be retrieved from. For example, it might look like the following:

```
16.107.145.27:super.super  
16.107.145.34:super.super  
16.107.145.39:bad.dude
```

In this example, SenSage AP gets data from 3 NonStop machines. On the first two NonStop machines SenSage AP logs in as super.super. On the last machine it log in as user bad.dude.

Additionally you may wish to modify the \$TIME_INTERVAL variable in the safeguard.retriever.pl and or the ems_retriever.pl file so that on the first run on the scripts more than one previous hour of EMS and Safeguard data is collected.

Please note that while the above example uses the super.super account it IS NOT recommended to use the super.super account for SenSage AP access in production environments. Please create a new SenSage AP user on your NonStop system that has only the privileges necessary to run the getsqd script, emsdist, and SAFEART.

Step 5: Preliminary Testing

After performing the steps discussed above it is wise to do some preliminary testing to make sure the keying relationships have been properly established. As the `lms` user on the SenSage AP head node (in the `/home/lms` directory) execute the following command:

```
ssh -i /home/lms/.ssh/safeguard_id_dsa -s  
<nonstop_user_to_log_on_as>@<ip_address_of_nonstop> tacl -c '$system.nset.getsgd  
-help'
```

The first time you execute this test you will be asked to accept the key from the NonStop device. Respond “yes” to the question to accept. Next you should see usage output from the `getsgd` script. If you get a prompt for a password, you have somehow installed the public key of the SenSage AP user improperly on the NonStop machine. You may need to delete the key you have established; then retry entering the key. To delete a key use the following command (after you have entered `sshcom`)

```
alter user <user_name> delete publickey <keyname>
```

From the previous example in [Step 2: Creating SSH Keying Relationship](#):

```
alter user <user_name> delete publickey key1
```

Repeat this test on every NonStop machine SenSage AP accesses so you can make sure to accept the NonStop SSH key SenSage AP will be seeing.

TROUBLE SHOOTING GUIDE

If you do not appear to be getting any EMS data, some NonStop systems might require the following command to be executed before `emsdist` outputs data to the `tty` (and hence the established SSH channel SenSage AP opens).

```
#set #informat tacl
```


CHAPTER 32

hp_proCurve_t3t4_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	hp_proCurve_t3t4_syslogng
Version	1.0
Source Vendor	Hewlett-Packard
Source Product	HP ProCurve
Source Component	Core Switching
Source Version	<ul style="list-style-type: none"> • Titan Series 3 • Titan Series 4
Source Host OS	n/a
Transport Mechanism	syslog-ng
PTL Filename	hp_proCurve_t3t4_syslogng.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none"> • investigation__hp_proCurve_t3t4_syslogng.sql • userLogin__hp_proCurve_t3t4_syslogng.sql
Look-up file	None
Scripts	None
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none"> • "Audit Event", on page 109 • "Unparsed Data", on page 139

CHAPTER 33

hp_proCurve_tmsz_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	hp_proCurve_tmsz_syslogng
Version	1.0
Source Vendor	Hewlett-Packard
Source Product	HP ProCurve
Source Component	HP Threat Management Services zl Module
Source Version	
Source Host OS	n/a
Transport Mechanism	syslog-ng
PTL Filename	hp_proCurve_tmsz_syslogng.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none"> • investigation__hp_proCurve_tmsz_syslogng.sql • userLogin__hp_proCurve_tmsz_syslogng.sql
Look-up file	None
Scripts	None
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none"> • “Audit Event”, on page 109 • “Unparsed Data”, on page 139

CHAPTER 34

ibm_db2_rdbms

SUMMARY INFORMATION

Log Adapter Component	Details
Name	ibm_db2_rdbms
Version	1.0.0
Source Vendor	IBM
Source Product	DB2
Source Component	Audit (AUDIT, CHECKING, CONTEXT, EXECUTE, OBJMAINT, SECMAINT, SYSADMIN, VALIDATE) logs
Source Version	9.7
Source Host OS	AIX, HP-UX, Linux, Solaris, Windows
Transport Mechanism	Custom database retriever
PTL Filename	ibm_db2_rdbms.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none">• database_ddl_ibm_db2_rdbms.sql• database_dml_ibm_db2_rdbms.sql• investigation_ibm_db2_rdbms.sql• parsedData_ibm_db2_rdbms.sql• unparsedData_ibm_db2_rdbms.sql
Look-up file	Not required.
Scripts	database retriever: retriever/DB2Retriever.jar
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none">• database_ddl• database_dml• “Investigation Event”, on page 114

SETTING UP THE IBM_DB2_RDBMS LOG ADAPTER

This document describe how to configure the ibm_db2_rdbms log adapter. The following steps are required:

- “Source System Setup”, next
- “SenSage AP Collector Setup”, on page 524

SOURCE SYSTEM SETUP

Before you can work with audit data in the database tables, you need to create the tables to store the data. You should consider creating these tables in a separate schema to isolate the data in the tables from unauthorized users:

- 1 Create tables to hold DB2 audit data. The tables can be created in a separate schema; for example:

```
'AUDIT':  
  
# db2 -t <<EOF  
CREATE SCHEMA AUDIT;  
SET CURRENT SCHEMA = 'AUDIT';  
EOF  
# db2 +o -tf sqllic/misc/db2audit.ddl
```

NOTE: "db2audit.ddl" is shipped with db2.

- 2 Activate DB2 audit by running the following commands for configuration:

```
a # db2audit configure scope audit status FAILURE  
b # db2audit configure scope checking status BOTH  
c # db2audit configure scope context status BOTH  
d # db2audit configure scope objmaint status BOTH  
e # db2audit configure scope secmaint status BOTH  
f # db2audit configure scope sysadmin status BOTH  
g # db2audit configure scope validate status BOTH  
h # db2audit configure errortype NORMAL  
i # db2audit configure datapath '/var/log/db2/audit'  
j # db2audit configure archivepath '/var/log/db2/auditarchive'
```

NOTES:

- Although items I and J above specify directories for saving logs, you can specify any other existing directory.
- The command for listing current settings is: 'db2audit describe'

- 3 Run the following command to start audit logging:

```
# db2audit start
```

4 Create audit policy DB2AUDIT_DBA_POLICY:

```
# db2 'CREATE AUDIT POLICY DB2AUDIT_DBA_POLICY
CATEGORIES
CHECKING STATUS BOTH,
OBJMAINT STATUS BOTH,
SECMAINT STATUS BOTH,
VALIDATE STATUS BOTH,
EXECUTE WITH DATA STATUS BOTH
ERROR TYPE NORMAL'
```

5 Associate that policy with the user (or with database, table, context, group, rule etc see IBM DB2 documentation):

```
# db2 'AUDIT USER some_db2_user USING POLICY DB2AUDIT_DBA_POLICY'
```

6 Extract the data:

```
# db2audit flush
# db2audit archive to '/var/log/db2/auditarchive'
# db2audit extract delasc to /tmp/auditextract/ from files /var/log/db2/
auditarchive/db2audit.<....>
```

NOTES:

- File **/var/log/db2/auditarchive/db2audit.<....>** is created after the **db2audit archive** command
- After the **db2audit extract** command is created, the ***.del** files for each category (**audit.del**, **checking.del**, **execute.del** and others) are created in the **/tmp/auditextract/ directory**.

7 Load the extracted data into the appropriate tables:

- a** # db2 'load from /tmp/auditextract/execute.del of del lobs from /tmp/
auditextract/ modified by delprioritychar lobsinfile messages /tmp/load.msg
tempfiles path /tmp insert into AUDIT.EXECUTE statistics no nonrecoverable
PARTITIONED DB CONFIG MODE PARTITION_AND_LOAD TRACE 10'
- b** # db2 'load from /tmp/auditextract/audit.del of del lobs from /tmp/
auditextract/ modified by delprioritychar lobsinfile messages /tmp/load.msg
tempfiles path /tmp insert into AUDIT.AUDIT statistics no nonrecoverable
PARTITIONED DB CONFIG MODE PARTITION_AND_LOAD TRACE 10'
- c** # db2 'load from /tmp/auditextract/checking.del of del lobs from /tmp/
auditextract/ modified by delprioritychar lobsinfile messages /tmp/load.msg
tempfiles path /tmp insert into AUDIT.CHECKING statistics no nonrecoverable
PARTITIONED DB CONFIG MODE PARTITION_AND_LOAD TRACE 10'
- d** # db2 'load from /tmp/auditextract/context.del of del lobs from /tmp/
auditextract/ modified by delprioritychar lobsinfile messages /tmp/load.msg
tempfiles path /tmp insert into AUDIT.CONTEXT statistics no nonrecoverable
PARTITIONED DB CONFIG MODE PARTITION_AND_LOAD TRACE 10'
- e** # db2 'load from /tmp/auditextract/objmaint.del of del lobs from /tmp/
auditextract/ modified by delprioritychar lobsinfile messages /tmp/load.msg
tempfiles path /tmp insert into AUDIT.OBJMAINT statistics no nonrecoverable
PARTITIONED DB CONFIG MODE PARTITION_AND_LOAD TRACE 10'

```
f # db2 'load from /tmp/auditextract/secmaint.del of del lobs from /tmp/
auditextract/ modified by delprioritychar lobsinfile messages /tmp/load.msg
tempfiles path /tmp insert into AUDIT.SECMAINT statistics no nonrecoverable
PARTITIONED DB CONFIG MODE PARTITION_AND_LOAD TRACE 10'

g # db2 'load from /tmp/auditextract/sysadmin.del of del lobs from /tmp/
auditextract/ modified by delprioritychar lobsinfile messages /tmp/load.msg
tempfiles path /tmp insert into AUDIT.SYSADMIN statistics no nonrecoverable
PARTITIONED DB CONFIG MODE PARTITION_AND_LOAD TRACE 10'

h # db2 'load from /tmp/auditextract/validate.del of del lobs from /tmp/
auditextract/ modified by delprioritychar lobsinfile messages /tmp/load.msg
tempfiles path /tmp insert into AUDIT.VALIDATE statistics no nonrecoverable
PARTITIONED DB CONFIG MODE PARTITION_AND_LOAD TRACE 10'
```

- 8** Remove files from directories **/var/log/db2/auditarchive** and **/tmp/auditextract/**.

SENsAGE AP COLLECTOR SETUP

To configure your log adapter, make the following configuration change on the host running the SenSAGE AP Collector:

- 1** Edit the SenSAGE AP Collector config.xml with sections for logqueue, retriever, loader. For more information, see [Chapter 2: SenSAGE AP Collector Configuration](#) in the *Collector Guide*.

NOTE: You should specify the custom db retriever in the 'Retriever' section, see Step 2 below:

- 2** Configure the custom database retriever.

- 3** Specify the following parameters in **<path_to_adapter>/retriever/DB2Config.properties**:

- **hostname** - DB2 database hostname
- **port** - port to connect to DB2
- **dbname** - database name
- **username and password** - credentials for connect
- **statefileinfo** - Full path to state file (example: **/opt/hexis/hawkeye-ap/data/collector/state/DB2Retriever.state**)
- **sqlstatement** - SQL statement for retrieving data. (example: **SELECT * FROM AUDIT.EXECUTE**)
- **logfile** - full path to retriever log (example: **/opt/hexis/hawkeye-ap/var/log/collector/DB2Retriever.log**)

- 4** Configure the following optional parameters:

- **startfromlatest** - start from latest record (false by default)
- **retrievalCount** - limit for selecting records (100000 by default)
- **logFileSize, rollingLogFileCount** - parameters for rotating logs
- **logLevel** - log level for retriever log

WARNING: Do not change 'delimiter' as its value is used in the PTL for splitting rows.

SAMPLE CONFIGURATION FILES

This section contains the following sample configuration files:

- Collector Configuration (**config.xml**)
- DB2 Configuration (**DB2Config.properties.config**)

Collector Configuration (**config.xml**)

```

<LogQueue encoding="UTF-8" minMBFree="100" name="q_ibm_db2_rdbms" path="queue/
ibm_db2_rdbms"/>

<Retriever type="filescript" name="ibm_db2_rdbms_audit" deleteOriginal="1"
enabled="1">
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_ibm_db2_rdbms</LogQueue>
    <SourceCommand>/opt/hexis/hawkeye-ap/java/bin/java -jar -DCONFIG=/opt/hexis/
hawkeye-ap/analytics/adapters/ibm_db2_rdbms/retriever/
DB2Config_audit.properties /opt/hexis/hawkeye-ap/analytics/adapters/
ibm_db2_rdbms/retriever/DB2Retriever.jar %F</SourceCommand>
    <Preprocess id="1" type="file" match="./*">/opt/hexis/hawkeye-ap/analytics/
adapters/ibm_db2_rdbms/ibm_db2_rdbms.proc</Preprocess>
    <PollInterval>3600</PollInterval>
</Retriever>
<Retriever type="filescript" name="ibm_db2_rdbms_checking" deleteOriginal="1"
enabled="1">
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_ibm_db2_rdbms</LogQueue>
    <SourceCommand>/opt/hexis/hawkeye-ap/java/bin/java -jar -DCONFIG=/opt/hexis/
hawkeye-ap/analytics/adapters/ibm_db2_rdbms/retriever/
DB2Config_checking.properties /opt/hexis/hawkeye-ap/analytics/adapters/
ibm_db2_rdbms/retriever/DB2Retriever.jar %F</SourceCommand>
    <Preprocess id="1" type="file" match="./*">/opt/hexis/hawkeye-ap/analytics/
adapters/ibm_db2_rdbms/ibm_db2_rdbms.proc</Preprocess>
    <PollInterval>3600</PollInterval>
</Retriever>
<Retriever type="filescript" name="ibm_db2_rdbms_context" deleteOriginal="1"
enabled="1">
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_ibm_db2_rdbms</LogQueue>
    <SourceCommand>/opt/hexis/hawkeye-ap/java/bin/java -jar -DCONFIG=/opt/hexis/
hawkeye-ap/analytics/adapters/ibm_db2_rdbms/retriever/
DB2Config_context.properties /opt/hexis/hawkeye-ap/analytics/adapters/
ibm_db2_rdbms/retriever/DB2Retriever.jar %F</SourceCommand>
    <Preprocess id="1" type="file" match="./*">/opt/hexis/hawkeye-ap/analytics/
adapters/ibm_db2_rdbms/ibm_db2_rdbms.proc</Preprocess>
    <PollInterval>3600</PollInterval>
</Retriever>
<Retriever type="filescript" name="ibm_db2_rdbms_execute" deleteOriginal="1"
enabled="1">
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_ibm_db2_rdbms</LogQueue>
    <SourceCommand>/opt/hexis/hawkeye-ap/java/bin/java -jar -DCONFIG=/opt/hexis/
hawkeye-ap/analytics/adapters/ibm_db2_rdbms/retriever/
DB2Config_execute.properties /opt/hexis/hawkeye-ap/analytics/adapters/
ibm_db2_rdbms/retriever/DB2Retriever.jar %F</SourceCommand>

```

```

<Preprocess id="1" type="file" match=".*">/opt/hexis/hawkeye-ap/analytics/
adapters/ibm_db2_rdbms/ibm_db2_rdbms.preproc</Preprocess>
<PollInterval>3600</PollInterval>
</Retriever>
<Retriever type="filescript" name="ibm_db2_rdbms_objmaint" deleteOriginal="1"
enabled="1">
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_ibm_db2_rdbms</LogQueue>
<SourceCommand>/opt/hexis/hawkeye-ap/java/bin/java -jar -DCONFIG=/opt/hexis/
hawkeye-ap/analytics/adapters/ibm_db2_rdbms/retriever/
DB2Config_objmaint.properties /opt/hexis/hawkeye-ap/analytics/adapters/
ibm_db2_rdbms/retriever/DB2Retriever.jar %F</SourceCommand>
<Preprocess id="1" type="file" match=".*">/opt/hexis/hawkeye-ap/analytics/
adapters/ibm_db2_rdbms/ibm_db2_rdbms.preproc</Preprocess>
<PollInterval>3600</PollInterval>
</Retriever>
<Retriever type="filescript" name="ibm_db2_rdbms_secmaint" deleteOriginal="1"
enabled="1">
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_ibm_db2_rdbms</LogQueue>
<SourceCommand>/opt/hexis/hawkeye-ap/java/bin/java -jar -DCONFIG=/opt/hexis/
hawkeye-ap/analytics/adapters/ibm_db2_rdbms/retriever/
DB2Config_secmaint.properties /opt/hexis/hawkeye-ap/analytics/adapters/
ibm_db2_rdbms/retriever/DB2Retriever.jar %F</SourceCommand>
<Preprocess id="1" type="file" match=".*">/opt/hexis/hawkeye-ap/analytics/
adapters/ibm_db2_rdbms/ibm_db2_rdbms.preproc</Preprocess>
<PollInterval>3600</PollInterval>
</Retriever>
<Retriever type="filescript" name="ibm_db2_rdbms_sysadmin" deleteOriginal="1"
enabled="1">
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_ibm_db2_rdbms</LogQueue>
<SourceCommand>/opt/hexis/hawkeye-ap/java/bin/java -jar -DCONFIG=/opt/hexis/
hawkeye-ap/analytics/adapters/ibm_db2_rdbms/retriever/
DB2Config_sysadmin.properties /opt/hexis/hawkeye-ap/analytics/adapters/
ibm_db2_rdbms/retriever/DB2Retriever.jar %F</SourceCommand>
<Preprocess id="1" type="file" match=".*">/opt/hexis/hawkeye-ap/analytics/
adapters/ibm_db2_rdbms/ibm_db2_rdbms.preproc</Preprocess>
<PollInterval>3600</PollInterval>
</Retriever>
<Retriever type="filescript" name="ibm_db2_rdbms_validate" deleteOriginal="1"
enabled="1">
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_ibm_db2_rdbms</LogQueue>
<SourceCommand>/opt/hexis/hawkeye-ap/java/bin/java -jar -DCONFIG=/opt/hexis/
hawkeye-ap/analytics/adapters/ibm_db2_rdbms/retriever/
DB2Config_validate.properties /opt/hexis/hawkeye-ap/analytics/adapters/
ibm_db2_rdbms/retriever/DB2Retriever.jar %F</SourceCommand>
<Preprocess id="1" type="file" match=".*">/opt/hexis/hawkeye-ap/analytics/
adapters/ibm_db2_rdbms/ibm_db2_rdbms.preproc</Preprocess>
<PollInterval>3600</PollInterval>
</Retriever>

<Loader enabled="1" name="l_ibm_db2_rdbms">
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_ibm_db2_rdbms</LogQueue>
<SLSInstance>analytics.example.com:8072</SLSInstance>
<SLSUser>administrator</SLSUser>

```

```
<SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>
<PTL namespace="analytics" table="ibm_db2_rdbms" type="file">
<Location>/opt/hexis/hawkeye-ap/analytics/adapters/ibm_db2_rdbms/
ibm_db2_rdbms.ptl</Location>
<LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
</PTL>
</Loader>
```

DB2 Configuration (DB2Config.properties.config)

The following example shows only DB2Config_execute.properties.

```
hostname=db2.example.com
port=50002
dbname=SAMPLE
username=db2nis
password=password

#optional parameters

outputfileinfo=
startfromlatest=false
retrievalCount=100000
statefileinfo=/opt/hexis/hawkeye-ap/data/collector/state/
DB2Retriever_execute.state
delimiter=@@@
sqlstatement=SELECT * FROM AUDIT.EXECUTE
logfile=/opt/hexis/hawkeye-ap/var/log/collector/DB2Retriever_execute.log
logFileSize=
rollingLogFileCount=
```


juniper_netscreenFw_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	juniper_netscreenFw_syslogng
Version	1.01
Source Vendor	Juniper Networks
Source Product	Netscreen IDPI
Source Component	n/a
Source Version	4.0.x
Source Host OS	Appliance_NS-208
Transport Mechanism	syslog
PTL Filename	juniper_netscreenFw_syslogng.ptl
Parsing Rule	None
Alerting Rule	
Connector Views	<ul style="list-style-type: none"> • investigation_juniper_netscreenFw_syslogng.sql • networkDeviceConnection_firewall_juniper_netscreenFw_syslogng.sql
Look-up file	None
Scripts	None
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none"> • “Audit Event”, on page 109 • “Network Device Connection”, on page 121

SETTING UP THE JUNIPER_NETSCREENFW_SYSLOGNG LOG ADAPTER

This document describe how to configure the juniper_netscreenFw_syslogng log adapter. The following steps are required:

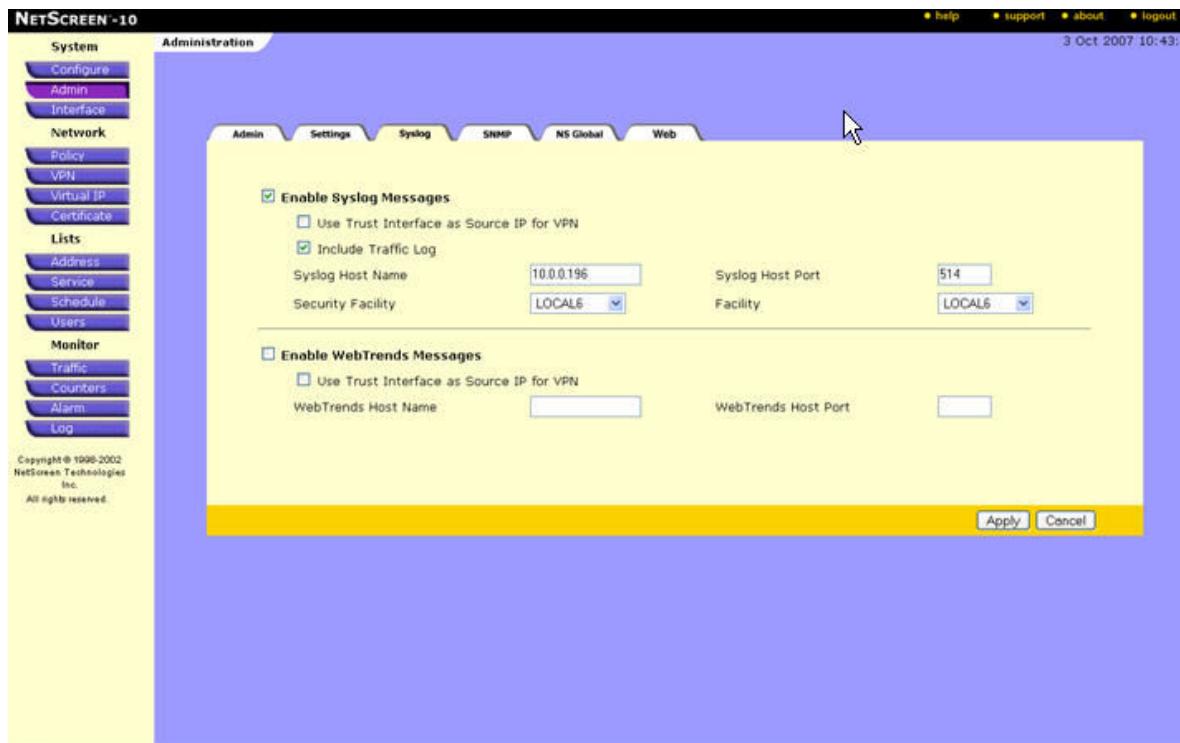
- “Source System Setup”, next
- “SenSage AP Collector syslog-ng Setup”, on page 531

SOURCE SYSTEM SETUP

For each device in your environment:

- 1 Log in to the administration interface for the network device.
- 2 Click on the Admin navigation menu to bring up the administration screen.
- 3 Click on the Syslog tab.
- 4 Check the Enable Syslog Messages box.
- 5 Check the Include Traffic Log box.
- 6 For the Syslog Host Name, enter the IP Address of the host running the SenSage AP Collector.
- 7 For the Syslog Port enter "514".
- 8 For the Security Facility and the Facility selectors select the default.

The screen appears as follows:



- 9 Click Apply to save your settings.
- 10 Under Monitor, select Log on the navigation menu to bring up the Log Severity Levels screen
- 11 Check the boxes for all levels you want to process.

The screen appears as follows:

Destinations	Log Severity Levels						
	Emergency	Alert	Critical	Error	Warning	Notification	Information Debugging
Console	<input type="checkbox"/>						
Internal	<input checked="" type="checkbox"/>						
Email	<input checked="" type="checkbox"/>						
SNMP	<input checked="" type="checkbox"/>						
Syslog	<input checked="" type="checkbox"/>						
Webtrends	<input checked="" type="checkbox"/>						
Global	<input checked="" type="checkbox"/>						
Global-Pro	<input checked="" type="checkbox"/>						
OneSecure	<input checked="" type="checkbox"/>						
PCMCIA	<input checked="" type="checkbox"/>						

12 Click Apply to save your settings.

SEN SAGE AP COLLECTOR SYSLOG-NG SETUP

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Edit /etc/syslog-NG.conf on the host running the SenSage AP Collector, configuring a filter statement, a destination statement, and a log statement as shown below:

- Filter statement:

```
filter f_netscreen           { match("NetScreen device_id="); };
```

- Destination statement:

```
# External Destinations - Juniper Netscreen
destination d_netscreen {
    file("<HawkEye AP Home>/incoming/syslog-NG/juniper_netscreenFw_syslogng/
juniper_netscreenFw_syslogng.log"
template
    ("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST $MSG\n")
template_escape(no) );
};
```

NOTE: Change the path and file name of the "file" argument to match the location of your log file.

■ Log statement:

```
log {  
    source(s_network_std);  
    filter(f_netscreen);  
    destination(d_netscreen);  
    flags(final);  
};
```

- 2 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

- 3 Edit the SenSage AP Collector config.xml with sections for logqueue, retriever, loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.
- 4 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

CHAPTER 32

mcafee_epo_audit_rdbms

SYSTEM INFORMATION

Name	mcafee_epo_audit_rdbms
Version	4.0
Source Vendor	McAfee
Source Product	McAfee ePolicy Orchestrator
Source Component	None
Source Version	4.0
Source Host OS	Any
Transport Mechanism	RDBMS
PTL Filename	mcafee_epo_audit_rdbms.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none">• investigation_mcafee_epo_audit_rdbms
Look-up file	None
Scripts	mcafee_epo_rdbms_retriever.pl
Reports	<ul style="list-style-type: none">• “McAfee ePO Console Logon Activity”, on page 332• “McAfee ePO Console Activity Summary”, on page 334
Event Types	<ul style="list-style-type: none">• “Audit Event”, on page 109

SETTING UP THE MCAFEE_EPO_AUDIT_RDBMS LOG ADAPTER

The McAfee ePO product stores its event data in a relational database. You configure a database retriever to collect its data. This document describe how to configure a database retriever for the mcafee_epo_audit_rdbms log adapter and contains the following sections:

- “Configuring the RDBMS Retriever”, on page 534
- “Sample sources.conf file”, on page 535
- “Sample freetds.conf file”, on page 536

CONFIGURING THE RDBMS RETRIEVER

To configure log collection for the mcafee_epo_audit_rdbms log adapter

1 Configure the `sources.conf` file.

This file contains one or more blocks defining database servers. Each block begins with the database name of the server instance enclosed in square brackets. For example: `[MyServer]`. Locate the block for your database or create a new block if needed. The database name may be a value of your choosing. When you run the script, you pass the server instance as the value for the `--source` parameter.

a Open the following file for editing:

```
<SenSage AP Home>/analytics/adapters/mcafee_epo_audit_rdbms/
mcafee_epo_rdbms_retriever/conf/sources.conf
```

b Edit the first line of the block to include the database name enclosed in square brackets. For example: `[EPO]`.

c Add the following name/value pairs:

<code>db_name</code>	Name of database
<code>db_host</code>	Database Hostname
<code>db_port</code>	Database Port Number
<code>db_user</code>	Database User Name
<code>db_pass</code>	Database Password
<code>output_dir</code>	Output directory. Recommend location: <code><SenSage AP Home>/incoming/syslog-ng/mcafee_epo_audit_rdbms</code> The output filename is created automatically, has a <code>.log</code> extension, and includes a timestamp.

See “[Sample sources.conf file](#)”, on page 535 for a sample of the `sources.conf` file

2 Edit the `freetds.conf` file to define connectivity to your Microsoft SQL Server instance.

a Open the following file for editing:

```
<SenSage AP Home>/etc/atperl58/freetds.conf
```

This file contains one or more blocks defining connectivity to SQL Server instances. Each block begins with the database name of the server instance enclosed in square brackets. For example: `[MyServer]`. Locate the block for your database or create a new block if needed. The database name must match the value of the `db_name` parameter you specified in [Step c](#), above, in the `sources.conf` file.

b Change the following values:

db_name	Name of database
host	Hostname of the database server
db_port	Port number of the database server
tds version	7.0
encryption	required

See “[Sample freetds.conf file](#)”, on page 536 for a sample of the `freetds.conf` file.

c Save the `freetds.conf` file

- 3** Test the script by executing it and passing the name of the source with the `--source` parameter:

```
<SenSage AP Home>/analytics/adapters/mcafee_epo_audit_rdbms/
mcafee_epo_rdbms_retriever/mcafee_epo_rdbms_retriever.pl --source=<db_name>
```

The value of `db_name` must match the value you specify in the `source.conf` file.

For example:

```
/opt/hexis/hawkeye-ap/analytics/adapters/mcafee_epo_event_rdbms/
mcafee_epo_rdbms_retriever/mcafee_epo_rdbms_retriever.pl --source=EPOAgent
```

Reloading Data

The retrievers maintain state in files to avoid loading duplicate data from external data sources. The state file is maintained in the following location:

```
<SenSage AP Home>/analytics/adapters/mcafee_epo_audit_rdbms/
mcafee_epo_rdbms_retriever/conf/mcafee_epo_audit_rdbms.state
```

If you would like to reload the data from the beginning of the available data, delete the state file. The retriever recreates this file the next time it runs.

Sample sources.conf file

NOTE: Comments lines begin with a “#” character. Make sure that there are no extra spaces in the source name. Each block begins with [`<SourceName>`].

```
[192.168.0.100]
db_name : foo
db_host : bar
db_port : 1234
db_user : jsmith
db_pass : abracadabra
output_dir : /tmp

[dbserver02]
db_name : foo
```

```
db_host : 10.172.13.2
db_port : 1234
db_user : jsmith
db_pass : abracadabra
output_dir : /tmp
```

Sample freetds.conf file

```
# A typical Microsoft SQL Server 2005 configuration
[Foundstone]
host = myhost.cbsf.foobar.com
port = 1433
tds version = 7.0
encryption = required
```

CHAPTER 33

mcafee_epo_event_rdbms

SYSTEM INFORMATION

Log Adapter Component	Details
Name	mcafee_epo_event_rdbms
Version	4.0
Source Vendor	McAfee
Source Product	McAfee ePolicy Orchestrator
Source Component	None
Source Version	4.0
Source Host OS	Any
Transport Mechanism	RDBMS
PTL Filename	mcafee_epo_event_rdbms.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none">• investigation__mcafee_epo_event_rdbms
Look-up file	None
Scripts	mcafee_epo_rdbms_retriever.pl
Source-Specific Reports	<ul style="list-style-type: none">• “McAfee ePO Top Threats”, on page 331• “McAfee ePO Agents by Server”, on page 333• “McAfee ePO Agent Communication Detail”, on page 335• “McAfee ePO Agent Communication Top 100 Summary”, on page 336
Event Types	<ul style="list-style-type: none">• “Audit Event”, on page 109

SETTING UP THE MCAFEE_EPO_EVENT_RDBMS LOG ADAPTER

The McAfee ePO product stores its event data in a relational database. You configure a database retriever to collect its event data. This document describe how to configure a database retriever for the mcafee_epo_event_rdbms log adapter and contains the following sections:

- “Configuring the RDBMS Retriever”, on page 538
- “Sample sources.conf file”, on page 539
- “Sample freetds.conf file”, on page 540

CONFIGURING THE RDBMS RETRIEVER

To configure log collection for the mcafee_epo_event_rdbms log adapter

1 Configure the `sources.conf` file.

This file contains one or more blocks defining database servers. Each block begins with the database name of the server instance enclosed in square brackets. For example: `[MyServer]`. Locate the block for your database or create a new block if needed. The database name may be a value of your choosing. When you run the script, you pass the server instance as the value for the `--source` parameter.

a Open the following file for editing:

```
<SenSage AP Home>/analytics/adapters/mcafee_epo_event_rdbms/
mcafee_epo_rdbms_retriever/conf/sources.conf
```

b Edit the first line of the block to include the database name enclosed in square brackets. For example: `[EPO]`.

c Add the following name/value pairs:

<code>db_name</code>	Name of database
<code>db_host</code>	Database Hostname
<code>db_port</code>	Database Port Number
<code>db_user</code>	Database User Name
<code>db_pass</code>	Database Password
<code>output_dir</code>	Output directory. Recommend location: <code><SenSage AP Home>/incoming/syslog-ng/mcafee_epo_event_rdbms</code> The output filename is created automatically, has a <code>.log</code> extension, and includes a timestamp.

See “[Sample sources.conf file](#)”, on page 539 for a sample of the `sources.conf` file

2 Edit the `freetds.conf` file to define connectivity to your Microsoft SQL Server instance.

a Open the following file for editing:

```
<SenSage AP Home>/etc/atperl58/freetds.conf
```

This file contains one or more blocks defining connectivity to SQL Server instances. Each block begins with the database name of the server instance enclosed in square brackets. For example: `[MyServer]`. Locate the block for your database or create a new block if needed. The database name must match the value of the `db_name` parameter you specified in [Step c](#), above, in the `sources.conf` file.

b Change the following values:

db_name	Name of database
host	Hostname of the database server
db_port	Port number of the database server
tds version	7.0
encryption	required

See “[Sample freetds.conf file](#)”, on page 540 for a sample of the `freetds.conf` file.

c Save the `freetds.conf` file

- 3** Test the script by executing it and passing the name of the source with the `--source` parameter:

```
<SenSage AP Home>/analytics/adapters/mcafee_epo_event_rdbms/
mcafee_epo_rdbms_retriever/mcafee_epo_rdbms_retriever.pl --source=<db_name>
```

The value of `db_name` must match the value you specify in the `source.conf` file.

For example:

```
/opt/hexis/hawkeye-ap/analytics/adapters/mcafee_epo_event_rdbms/
mcafee_epo_rdbms_retriever/mcafee_epo_rdbms_retriever.pl --source=EPO
```

Reloading Data

The retrievers maintain state in files to avoid loading duplicate data from external data sources. The state file is maintained in the following location:

```
<SenSage AP Home>/analytics/adapters/mcafee_epo_event_rdbms/
mcafee_epo_rdbms_retriever/conf/mcafee_epo_event_rdbms.state
```

If you would like to reload the data from the beginning of the available data, delete the state file. The retriever recreates this file the next time it runs.

Sample sources.conf file

NOTE: Comments lines begin with a “#” character. Make sure that there are no extra spaces in the source name. Each block begins with [`<SourceName>`].

```
[192.168.0.100]
db_name : foo
db_host : bar
db_port : 1234
db_user : jsmith
db_pass : abracadabra
output_dir : /tmp

[dbserver02]
db_name : foo
```

```
db_host : 10.172.13.2
db_port : 1234
db_user : jsmith
db_pass : abracadabra
output_dir : /tmp
```

Sample freetds.conf file

```
# A typical Microsoft SQL Server 2005 configuration
[Foundstone]
host = myhost.cbsf.foobar.com
port = 1433
tds version = 7.0
encryption = required
```

CHAPTER 34

mcafee_foundstone_rdbms

SYSTEM INFORMATION

Log Adapter Component	Details
Name	mcafee_foundstone_rdbms
Version	4.0
Source Vendor	McAfee
Source Product	McAfee Foundstone
Source Component	
Source Version	4.0
Source Host OS	Any
Transport Mechanism	RDBMS
PTL Filename	mcafee_foundstone_rdbms.ptl
Parsing Rule	
Alerting Rule	
Connector Views	<ul style="list-style-type: none">investigation_mcafee_foundstone_rdbms
Look-up file	
Scripts	mcafee_foundstone_rdbms_retriever.pl
Source-Specific Reports	<ul style="list-style-type: none">"McAfee Foundstone OS & Application Vulnerabilities", on page 346"McAfee Foundstone Top 20 Affected Hosts", on page 348"McAfee Foundstone High Risk Vulnerabilities", on page 349"McAfee Foundstone High Risk Vulnerabilities Top 100 Summary", on page 350
Event Types	<ul style="list-style-type: none">"Audit Event", on page 109

SETTING UP THE MCAFEE_FOUNDSTONE_RDBMS LOG ADAPTER

The McAfee Foundstone product stores its event data in a relational database. You configure a database retriever to collect its event data. This document describes how to configure a database retriever for the mcafee_foundstone_rdbms log adapter and contains the following sections:

- "Configuring the RDBMS Retriever", on page 542
- "Sample sources.conf file", on page 543

- “[Sample freetds.conf file](#)”, on page 544

CONFIGURING THE RDBMS RETRIEVER

To configure log collection for the `mcafee_foundstone_rdbms` log adapter:

1 Configure the `sources.conf` file.

This file contains one or more blocks defining database servers. Each block begins with the database name of the server instance enclosed in square brackets. For example: `[MyServer]`. Locate the block for your database or create a new block if needed. The database name may be a value of your choosing. When you run the script, you pass the server instance as the value for the `--source` parameter.

a Open the following file for editing:

```
<SenSage AP Home>/analytics/adapters/mcafee_foundstone_rdbms/  
mcafee_foundstone_rdbms_retriever/conf/sources.conf
```

b Edit the first line of the block to include the database name enclosed in square brackets. For example: `[EPO]`.

c Add the following name/value pairs:

<code>db_name</code>	Name of database
<code>db_host</code>	Database Hostname
<code>db_port</code>	Database Port Number
<code>db_user</code>	Database User Name
<code>db_pass</code>	Database Password
<code>output_dir</code>	Output directory. Recommend location: <code><SenSage AP Home>/incoming/syslog-ng/mcafee_foundstone_rdbms</code> The output filename is created automatically, has a <code>.log</code> extension, and includes a timestamp.

See “[Sample sources.conf file](#)”, on page 543 for a sample of the `sources.conf` file

2 Edit the `freetds.conf` file to define connectivity to your Microsoft SQL Server instance.

a Open the following file for editing:

```
<SenSage AP Home>/etc/atperl58/freetds.conf
```

This file contains one or more blocks defining connectivity to SQL Server instances. Each block begins with the database name of the server instance enclosed in square brackets. For example: `[MyServer]`. Locate the block for your database or create a new block if needed. The database name must match the value of the `db_name` parameter you specified in [Step c](#), above, in the `sources.conf` file.

b Change the following values:

db_name	Name of database
host	Hostname of the database server
db_port	Port number of the database server
tds version	7.0
encryption	required

See “[Sample freetds.conf file](#)”, on page 544 for a sample of the `freetds.conf` file.

c Save the `freetds.conf` file

- 3** Test the script by executing it and passing the name of the source with the `--source` parameter:

```
<SenSage AP Home>/analytics/adapters/mcafee_foundstone_rdbms/
mcafee_foundstone_rdbms_retriever/mcafee_foundstone_rdbms_retriever.pl --
source=<db_name>
```

The value of `db_name` must match the value you specify in the `source.conf` file.

For example:

```
/opt/hexis/hawkeye-ap/analytics/adapters/mcafee_foundstone_rdbms/
mcafee_foundstone_rdbms_retriever/mcafee_foundstone_rdbms_retriever.pl --
source=EPO
```

Reloading Data

The retrievers maintain state in files to avoid loading duplicate data from external data sources. The state file is maintained in the following location:

```
<SenSage AP Home>/analytics/adapters/mcafee_foundstone_rdbms/
mcafee_epo_rdbms_retriever/conf/mcafee_foundstone_rdbms.state
```

If you would like to reload the data from the beginning of the available data, delete the state file. The retriever recreates this file the next time it runs.

Sample sources.conf file

NOTE: Comments lines begin with a “#” character. Make sure that there are no extra spaces in the source name. Each block begins with [`<SourceName>`].

```
[192.168.0.100]
db_name : foo
db_host : bar
db_port : 1234
db_user : jsmith
db_pass : abracadabra
output_dir : /tmp
```

```
[dbserver02]
db_name : foo
db_host : 10.172.13.2
db_port : 1234
db_user : jsmith
db_pass : abracadabra
output_dir : /tmp
```

Sample freetds.conf file

```
# A typical Microsoft SQL Server 2005 configuration
[Foundstone]
host = myhost.cbsf.foobar.com
port = 1433
tds version = 7.0
encryption = required
```

CHAPTER 35

mcafee_intrushield_rdbms

SYSTEM INFORMATION

Log Adapter Component	Details
Name	mcafee_intrushield_rdbms
Version	4.0
Source Vendor	McAfee
Source Product	McAfee Intrushield
Source Component	None
Source Version	4.1.3.19
Source Host OS	Any
Transport Mechanism	RDBMS
PTL Filename	mcafee_intrushield_rdbms.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none">investigation__mcafee_intrushield_rdbms
Look-up file	None
Scripts	<ul style="list-style-type: none">mcafee_intrushield_retriever.plmake_keys_hash.plmake_parser_hash.plmake_sql_insert.pl
Source-Specific Reports	<ul style="list-style-type: none">"McAfee NSP Attacks Details", on page 340"McAfee NSP Attacks Summary", on page 341"McAfee NSP Top 10 Source IP", on page 343"McAfee NSP Top 10 Target IP", on page 344"McAfee NSP Top 10 Directed Attacks", on page 345
Event Types	<ul style="list-style-type: none">"Audit Event", on page 109

SETTING UP THE MCAFEE_INTRUSHIELD_RDBMS LOG ADAPTER

The McAfee ePO product stores its event data in a relational database. You configure a database retriever to collect its event data. This document describe how to configure a database retriever for the mcafee_intrushield_rdbms log adapter and contains the following sections:

- “Configuring the RDBMS Retriever”, on page 546
- “Sample sources.conf file”, on page 547

CONFIGURING THE RDBMS RETRIEVER

To configure log collection for the mcafee_intrushield_rdbms log adapter

1 Configure the `sources.conf` file.

This file contains one or more blocks defining database servers. Each block begins with the database name of the server instance enclosed in square brackets. For example: [MyServer]. Locate the block for your database or create a new block if needed. The database name may be a value of your choosing. When you run the script, you pass the server instance as the value for the `--source` parameter.

a Open the following file for editing:

```
<SenSage AP Home>/analytics/adapters/mcafee_intrushield_rdbms/
mcafee_intrushield_rdbms_retriever/conf/sources.conf
```

b Edit the first line of the block to include the database name enclosed in square brackets. For example: [MyIntrushield].

c Add the following name/value pairs:

<code>db_name</code>	Name of database
<code>db_host</code>	Database Hostname
<code>db_port</code>	Database Port Number
<code>db_user</code>	Database User Name
<code>db_pass</code>	Database Password
<code>output_dir</code>	<p>Output directory. Recommend location: <code><SenSage AP Home>/incoming/syslog-ng/</code></p> <p>mcafee_intrushield_rdbms</p> <p>The output filename is created automatically, has a <code>.log</code> extension, and includes a timestamp.</p>

See “[Sample sources.conf file](#)”, on page 547 for a sample of the `sources.conf` file

2 Test the script by executing it and passing the name of the source with the `--source` parameter:

```
<SenSage AP Home>/analytics/adapters/mcafee_intrushield_rdbms/
mcafee_intrushield_rdbms_retriever/mcafee_intrushield_rdbms_retriever.pl --
source=<db_name>
```

The value of `db_name` must match the value you specify in the `source.conf` file.

For example:

```
/opt/hexis/hawkeye-ap/analytics/adapters/mcafee_intrushield_event_rdbms/
mcafee_intrushield_rdbms_retriever/mcafee_intrushield_rdbms_retriever.pl --
source=myIntrushield
```

Reloading Data

The retrievers maintain state in files to avoid loading duplicate data from external data sources.
The state file is maintained in the following location:

```
<SenSage AP Home>/analytics/adapters/mcafee_intrushield_rdbms/
mcafee_intrushield_rdbms_retriever/conf/mcafee_intrushield_rdbms.state
```

If you would like to reload the data from the beginning of the available data, delete the state file.
The retriever recreates this file the next time it runs.

SAMPLE SOURCES.CONF FILE

NOTE: Comments lines begin with a “#” character. Make sure that there are no extra spaces in the source name. Each block begins with [*<SourceName>*].

```
[192.168.0.100]
db_name : foo
db_host : bar
db_port : 1234
db_user : jsmith
db_pass : abracadabra
output_dir : /tmp

[dbserver02]
db_name : foo
db_host : 10.172.13.2
db_port : 1234
db_user : jsmith
db_pass : abracadabra
output_dir : /tmp
```


CHAPTER 36

mcafee_intrushield_syslogng

SYSTEM INFORMATION

Log Adapter Component	Details
Name	mcafee_intrushield_syslogng
Version	4.1
Source Vendor	McAfee
Source Product	McAfee Intrushield
Source Component	
Source Version	4.1.3.19
Source Host OS	Any
Transport Mechanism	syslog- <i>ng</i>
PTL Filename	mcafee_intrushield_syslogng.ptl
Parsing Rule	mcafee_intrushield.rule
Alerting Rule	None
Connector Views	<ul style="list-style-type: none">• investigation__mcafee_intrushield_syslogng
Look-up file	None
Scripts	None
Source-Specific Reports	<ul style="list-style-type: none">• “McAfee NSP Possible Successful Exploits (by Target)”, on page 338• “McAfee NSP Possible Successful Exploits (by Source)”, on page 339• “McAfee NSP Top 20 Most Common Events”, on page 342
Event Types	<ul style="list-style-type: none">• “Audit Event”, on page 109

SETTING UP THE MCAFEE_INTRUSHIELD_SYSLOGNG LOG ADAPTER

The mcafee_intrushield_syslogng log adapter forwards events from McAfee Intrushield IPS to a syslog receiver. The following steps are required:

- “Source System Setup”, next
- “SenSage AP Collector syslog-*ng* Setup”, on page 550

SOURCE SYSTEM SETUP

To configure Intrushield to send events to syslog-ng:

- 1 Open the following page in the ISM user interface: Alert-Domain-Name > Alert Notification > Syslog Forwarder.
- 2 In the Syslog Server (IP Address Or Host Name) field, enter the Host IP address or Host name of the host running the SenSage AP Collector.
- 3 Open the following page in the ISM user interface: Alert-Domain-Name > Fault Notification > Syslog Forwarder.
- 4 In the Syslog Server (IP Address Or Host Name) field, enter the Host IP address or Host name of the host running the SenSage AP Collector.
- 5 Open the Syslog configuration page.
- 6 Copy and paste the following text into the configuration:

```
ALERT_ID||ALERT_TYPE||ATTACK_TIME||ATTACK_NAME||ATTACK_ID||ATTACK_SEVERITY||ATTACK_SIGNATURE||ATTACK_CONFIDENCE||ADMIN_DOMAIN||SENSOR_NAME||INTERFACE||SOURCE_IP||SOURCE_PORT||DESTINATION_IP||DESTINATION_PORT||CATEGORY||SUB_CATEGORY||DIRECTION||RESULT_STATUS||DETECTION_MECHANISM||APPLICATION_PROTOCOL||NETWORK_PROTOCOL||RELEVANCE||QUARANTINE_END_TIME||REMEDIATION_END_TIME||MCAFEE_NAC_FORWARDED_STATUS||MCAFEE_NAC_MANAGED_STATUS||MCAFEE_NAC_ERROR_STATUS||MCAFEE_NAC_ACTION_STATUS
```

SEN SAGE AP COLLECTOR SYSLOG-NG SETUP

This section discusses setting up syslog-ng on the SenSage AP Collector. For more information on using syslog-ng in your SenSage AP deployment, see [Appendix B: SYSLOG-NG Setup](#).

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Edit `/etc/syslog-ng.conf` on the host running the SenSage AP Collector, configuring a filter statement, a destination statement, and a log statement as shown in the following example:

■ Filter statement:

```
filter f_mcafee_ids { program(SyslogAlertForwarder); };
```

■ Destination statement:

```
destination d_mcafee_ids {
    file("/opt/hexis/hawkeye-ap/incoming/syslog-ng/mcafee_intrushield_syslogng/mcafee_intrushield_syslogng.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY
$HOST $MSG\n")
        template_escape(no) );
};
```

- Log statement:

```
log { source(s_network_std); filter(f_mcafee_ids);
destination(d_mcafee_ids); flags(final); };
```

- 2 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

- 3 Edit the SenSage AP Collector config.xml, including sections for logqueue, retriever, and loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

- 4 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

microsoft_dns_debug_sensageRetrieverAgent

SUMMARY INFORMATION

Log Adapter Component	Details
Name	microsoft_dns_debug_sensageRetrieverAgent
Version	1.0.0
Source Vendor	Microsoft
Source Product	Windows
Source Component	DNS Server
Source Version	2008, 2012
Source Host OS	Windows Server 2008/2012
Transport Mechanism	SenSage Retriever Agent
PTL Filename	microsoft_dns_debug_sensageRetrieverAgent.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none"> • parsedData__microsoft_dns_debug_sensageRetrieverAgent.sql • unparsedData__microsoft_dns_debug_sensageRetrieverAgent.sql
Look-up file	Not required
Scripts	microsoft_dns_debug_sensageRetrieverAgent.preproc
Source-Specific Reports	<ul style="list-style-type: none"> • “Microsoft Exchange - Audit Trail Integrity Events”, on page 447
Event Types	None

SETTING UP MICROSOFT_DNS_DEBUG_SENSAGERETRIEVER LOG ADAPTER

This section describes how to configure the microsoft_dns_debug_sensageRetrieverAgent Log adapter. The following steps are required:

- [“Source System Setup”, next](#)
- [“HawkEye Collector Configuration”, on page 504](#)

Source System Setup

- 1 Enable debug logging options on the DNS server at 2.

<http://technet.microsoft.com/en-us/library/cc759581%28v=ws.10%29.aspx>

NOTE: Set the log file path outside the Windows directory; for example,
C:\DNS_DEBUG_LOGS\dns_debug.log.

- 2 Install the Windows Retriever Agent:

a Unzip **WindowsRetriever.zip** to any folder (for example in **C:\WindowsRetriever**).

b Edit **conf/wrapper.conf** to set the java exe path to:
wrapper.java.command=C:\java\bin\java.exe

c Edit **conf/agent.prop** to set the reader and writer:

```
reader1=file,C:\DNS_DEBUG_LOGS\dns_debug.log  
writer=syslog,IP,514
```

where **IP** is **YOUR_PUBLIC_COLLECTOR_IP**

d To install retriever, run **bin\InstallWinRetriever.bat**

- 3 To start the service, open Windows Services, find "Sensage Windows Event Retriever" and start it.

- 4 Check logs/retriever.

SenSage AP Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open syslog-ng configuration file <*SenSage_AP_Home*>/**etc/syslog-ng/syslog-ng.conf** on the host running the SenSage AP Collector.
- 2 Set Microsoft DNS server host for filter f_microsoft_dns_debug_sensageRetrieverAgent.
- 3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

NOTE: The syslog configuration template, **syslog-ng_config_template.conf**, resides in the adapter directory.

SAMPLE CONFIGURATION FILES

This section contains the following sample configuration files:

- **SenSage AP Collector Configuration ([config.xml](#)) ([config.xml](#))**
- **Syslog-ng Configuration Entries ([syslog-ng.conf](#)) ([syslog-ng.conf](#))**

SenSage AP Collector Configuration (**config.xml**)

```

<LogQueue path='queue/microsoft_dns_debug_sensageRetrieverAgent' minMBFree='100'
name='q_microsoft_dns_debug_sensageRetrieverAgent' encoding='UTF-8'/>

<Retriever type='filesystem' enabled='1'
name='r_microsoft_dns_debug_sensageRetrieverAgent' deleteOriginal='1'
method='copy'>
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_microsoft_dns_debug_sensageRetrieverAgent</LogQueue>
    <SourceDir>/opt/hexis/incoming/microsoft_dns_debug_sensageRetrieverAgent</
SourceDir>
    <Preprocess type='file' id='1' match='.*'>/opt/hexis/hawkeye-ap/analytics/
adapters/microsoft_dns_debug_sensageRetrieverAgent/
microsoft_dns_debug_sensageRetrieverAgent.preproc</Preprocess>
    <Plugin name='Default'>
        <File ai='ignore' id='1'>.*</File>
        <File ai='accept' id='2'>.*\log$</File>
    </Plugin>
</Retriever>

<Loader enabled='1' name='l_microsoft_dns_debug_sensageRetrieverAgent'>
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_microsoft_dns_debug_sensageRetrieverAgent</LogQueue>
    <SLSInstance>example.com:8072</SLSInstance>
    <SLSUser>administrator</SLSUser>
    <SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>
        <PTL table='microsoft_dns_debug_sensageRetrieverAgent' namespace='analytics'
type='file'>
            <Location>/opt/hexis/hawkeye-ap/analytics/adapters/
microsoft_dns_debug_sensageRetrieverAgent/
microsoft_dns_debug_sensageRetrieverAgent.ptl</Location>
            <LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
        </PTL>
    </Loader>

```

Syslog-ng Configuration Entries (**syslog-ng.conf**)

```

# Microsoft DNS debug Log
destination d_microsoft_dns_debug_sensageRetrieverAgent {
    file("/opt/hexis/incoming/microsoft_dns_debug_sensageRetrieverAgent/
microsoft_dns_debug_sensageRetrieverAgent.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};

filter f_microsoft_dns_debug_sensageRetrieverAgent { facility(user) and
host("192.168.0.1"); };

log { source(s_network_std); source(s_network_tls);
filter(f_microsoft_dns_debug_sensageRetrieverAgent);
destination(d_microsoft_dns_debug_sensageRetrieverAgent);      flags(final); };

```


microsoft_exchange_admin_events_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	microsoft_exchange_admin_events_syslogng
Version	1.0.0
Source Vendor	Microsoft
Source Product	Exchange Server
Source Component	None
Source Version	2010
Source Host OS	Windows Server 2008/2012
Transport Mechanism	syslog-ng
PTL Filename	microsoft_exchange_admin_events_syslogng.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none"> • accountAddition__microsoft_exchange_admin_events_syslogng • audit__microsoft_exchange_admin_events_syslogng • investigation__microsoft_exchange_admin_events_syslogng • parsedData__microsoft_exchange_admin_events_syslogng • privilegedCommand__microsoft_exchange_admin_events_syslogng • unparsedData__microsoft_exchange_admin_events_syslogng
Look-up file	Not required
Scripts	Not required
Source-Specific Reports	<ul style="list-style-type: none"> • “Microsoft Exchange - Audit Trail Integrity Events”, on page 447
Event Types	Admin Events

SETTING UP MICROSOFT_EXCHANGE_ADMIN_EVENTS_SYSLOGNG LOG ADAPTER

This section describes how to configure the microsoft_exchange_admin_events_syslogng Log adapter. The following steps are required:

- “Source System Setup”, next
- “SenSage AP Collector Configuration”, on page 558

Source System Setup

For installation and configuring refer to the official LOGbinder EX Documentation:
<http://www.logbinder.com/PublicFiles/LBEXGettingStartedGuide>

NOTE: Specify the output format as "Syslog in generic format" and specify the IP address of the host running the SenSage AP Collector.

SenSage AP Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open syslog-ng configuration file <SenSage AP Home>/etc/syslog-ng/syslog-ng.conf on the host running the SenSage AP Collector.
- 2 Make sure the following destination, filter and log statements are configured as shown below:

```
destination d_microsoft_exchange_admin_events {  
    file("/opt/hexis/incoming/syslog-ng/  
microsoft_exchange_admin_events_syslogng/  
microsoft_exchange_admin_events_syslogng.log"  
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST  
$MSGHDR$MSG\n")  
        template_escape(no) );  
};  
  
filter f_microsoft_exchange_admin_events { message ("New-AdminAuditLogSearch  
"); };  
  
log { source(s_network_std); source(s_network_tls);  
filter(f_microsoft_exchange_admin_events);  
destination(d_microsoft_exchange_admin_events); flags(final); };
```

- 3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

- 4 Edit the SenSage Collector **config.xml** with sections for logqueue, retriever, loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

- 5 Optional) Set up log file rotation. See [“Setting Up Syslog-NG Log Rotation”, on page 677](#).

SAMPLE CONFIGURATION FILES

This section contains the following sample configuration files:

- Collector Configuration (**config.xml**)
- Syslog-NG Configuration entries (**syslog-ng.conf**)

SenSage AP Collector Configuration (`config.xml`)

```

<LogQueue path='queue/microsoft_exchange_admin_events_syslogng' minMBFree='100'
name='q_microsoft_exchange_admin_events_syslogng' encoding='UTF-8' />

    <Retriever type='filesystem' enabled='1'
name='r_microsoft_exchange_admin_events_syslogng' deleteOriginal='1'
method='copy'>
        <RunOnHost>localhost</RunOnHost>
        <LogQueue>q_microsoft_exchange_admin_events_syslogng</LogQueue>
        <SourceDir>/opt/hexis/incoming/syslog-ng/
microsoft_exchange_admin_events_syslogng</SourceDir>
        <Plugin name='Default'>
            <File ai='ignore' id='1'>.*</File>
            <File ai='accept' id='2'>.*\.loadme$</File>
        </Plugin>
    </Retriever>

    <Loader enabled='1' name='l_microsoft_exchange_admin_events_syslogng'>
        <RunOnHost>localhost</RunOnHost>
        <LogQueue>q_microsoft_exchange_admin_events_syslogng</LogQueue>
        <SLSInstance>analytics.example.com:8072</SLSInstance>
        <SLSUser>administrator</SLSUser>
        <SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>
            <PTL table='microsoft_exchange_admin_events_syslogng'
namespace='analytics' type='file'>
                <Location>/opt/hexis/hawkeye-ap/analytics/adapters/
microsoft_exchange_admin_events_syslogng/
microsoft_exchange_admin_events_syslogng.ptl</Location>
                <LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
            </PTL>
    </Loader>

```

Syslogng Configuration Entries (`syslog-nginx.conf`)

```

destination d_microsoft_exchange_admin_events {

    file("/opt/hexis/incoming/syslog-ng/
microsoft_exchange_admin_events_syslogng/
microsoft_exchange_admin_events_syslogng.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};

filter f_microsoft_exchange_admin_events { message ("New-AdminAuditLogSearch
"); };

log { source(s_network_std); source(s_network_tls);
filter(f_microsoft_exchange_admin_events);
destination(d_microsoft_exchange_admin_events); flags(final); };

```


microsoft_exchange_mailbox_events_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	microsoft_exchange_admin_events_syslogng
Version	1.0.0
Source Vendor	Microsoft
Source Product	Exchange Server
Source Component	N/A
Source Version	2010
Source Host OS	Windows Server 2008/2012
Transport Mechanism	syslog-ng
PTL Filename	microsoft_exchange_mailbox_events_syslogng.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none"> • accountAddition__microsoft_exchange_mailbox_events_syslogng • investigation__microsoft_exchange_mailbox_events_syslogng • mail__microsoft_exchange_mailbox_events_syslogng • parsedData__microsoft_exchange_mailbox_events_syslogng • privilegedCommand__microsoft_exchange_mailbox_events_syslogng • unparsedData__microsoft_exchange_mailbox_events_syslogng
Look-up file	Not required
Scripts	Not required
Source-Specific Reports	<ul style="list-style-type: none"> • “Microsoft Exchange - Audit Trail Integrity Events”, on page 447
Event Types	Mailbox Events

SETTING UP MICROSOFT_EXCHANGE_MAILBOX_EVENTS_SYSLOGNG LOG ADAPTER

This section describes how to configure the microsoft_exchange_mailbox_events_syslogng Log adapter. The following steps are required:

- “[Source System Setup](#)”, next
- “[HawkEye Collector Configuration](#)”, on page 512

Source System Setup

For installation and configuring refer to the official LOGbinder EX Documentation
<http://www.logbinder.com/PublicFiles/LBEXGettingStartedGuide>.

NOTE: Specify the output format as "Syslog in Generic Format" and specify IP address of the host running the SenSage AP Collector.

SenSage AP Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open syslog-ng configuration file <*SenSage AP Home*>/etc/syslog-ng/syslog-ng.conf on the host running the SenSage AP Collector.
- 2 Make sure that the following destination, filter, and log statements are configured as shown below:

```
destination d_microsoft_exchange_mailbox_events {  
    file("/opt/hexis/incoming/syslog-ng/  
microsoft_exchange_mailbox_events_syslogng/  
microsoft_exchange_mailbox_events_syslogng.log"  
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST  
$MSGHDR$MSG\n")  
        template_escape(no) );  
};  
  
filter f_microsoft_exchange_mailbox_events { message("New-  
MailboxAuditLogSearch "); };  
  
log { source(s_network_std); source(s_network_tls);  
filter(f_microsoft_exchange_mailbox_events);  
destination(d_microsoft_exchange_mailbox_events); flags(final); };
```

- 3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

- 4 Edit the SenSage collector **config.xml** with sections for logqueue, retriever, loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.
- 5 Optional) Set up log file rotation. See [Setting Up Syslog-NG Log Rotation](#).

SAMPLE CONFIGURATION FILES

This section contains the following sample configuration files:

- Collector Configuration (**config.xml**)

- Syslog-ng Configuration Entries (**syslog-ng.conf**)

Collector Configuration (**config.xml**)

```

<LogQueue path='queue/microsoft_exchange_mailbox_events_syslogng'
minMBFree='100' name='q_microsoft_exchange_mailbox_events_syslogng'
encoding='UTF-8' />

    <Retriever enabled='1' type='filesystem'
name='r_microsoft_exchange_mailbox_events_syslogng' deleteOriginal='1'
method='copy'>
        <RunOnHost>localhost</RunOnHost>
        <LogQueue>q_microsoft_exchange_mailbox_events_syslogng</LogQueue>
        <SourceDir>/opt/hexis/incoming/syslog-ng/
microsoft_exchange_mailbox_events_syslogng</SourceDir>
        <Plugin name='Default'>
            <File ai='ignore' id='1'>.*</File>
            <File ai='accept' id='2'>.*\loadme$</File>
        </Plugin>
    </Retriever>

    <Loader enabled='1' name='l_microsoft_exchange_mailbox_events_syslogng'>
        <RunOnHost>localhost</RunOnHost>
        <LogQueue>q_microsoft_exchange_mailbox_events_syslogng</LogQueue>
        <SLSInstance>analytics.example.com:8072</SLSInstance>
        <SLSUser>administrator</SLSUser>
        <SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>
        <PTL table='microsoft_exchange_mailbox_events_syslogng'
namespace='analytics' type='file'>
            <Location>/opt/hexis/hawkeye-ap/analytics/adapters/
microsoft_exchange_mailbox_events_syslogng/
microsoft_exchange_mailbox_events_syslogng.ptl</Location>
            <LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
        </PTL>
    </Loader>

```

Syslog-ng Configuration Entries (**syslog-ng.conf**)

```

destination d_microsoft_exchange_admin_events {
    file("/opt/hexise/incoming/syslog-ng/
microsoft_exchange_admin_events_syslogng/
microsoft_exchange_admin_events_syslogng.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};

filter f_microsoft_exchange_admin_events { message ("New-AdminAuditLogSearch
"); };

log { source(s_network_std); source(s_network_tls);
filter(f_microsoft_exchange_admin_events);
destination(d_microsoft_exchange_admin_events); flags(final); };

```


CHAPTER 40

microsoft_exchange_tracking_sensageRetrieverAgent

SUMMARY INFORMATION

Log Adapter Component	Details
Name	microsoft_exchange_tracking_sensageRetrieverAgent
Version	1.1.0
Source Vendor	Microsoft
Source Product	Exchange
Source Component	Tracking logs
Source Version	Exchange 2010
Source Host OS	Windows Server 2008 SP2 x64 or Windows Server 2008 R2 x64 or later
Transport Mechanism	Windows Retriever Agent
PTL Filename	microsoft_exchange_tracking_sensageRetrieverAgent.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	investigation_microsoft_exchange_tracking_sensageRetrieverAgent
Look-up file	Not required
Scripts	Not required
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none">• “Audit Event”, on page 109

SETTING UP MICROSOFT_EXCHANGE_TRACKING_SENSAGERETRIEVERAGENT LOG ADAPTER

This document describe how to configure the microsoft_exchange_tracking_sensageRetrieverAgent log adapter. The following steps are required:

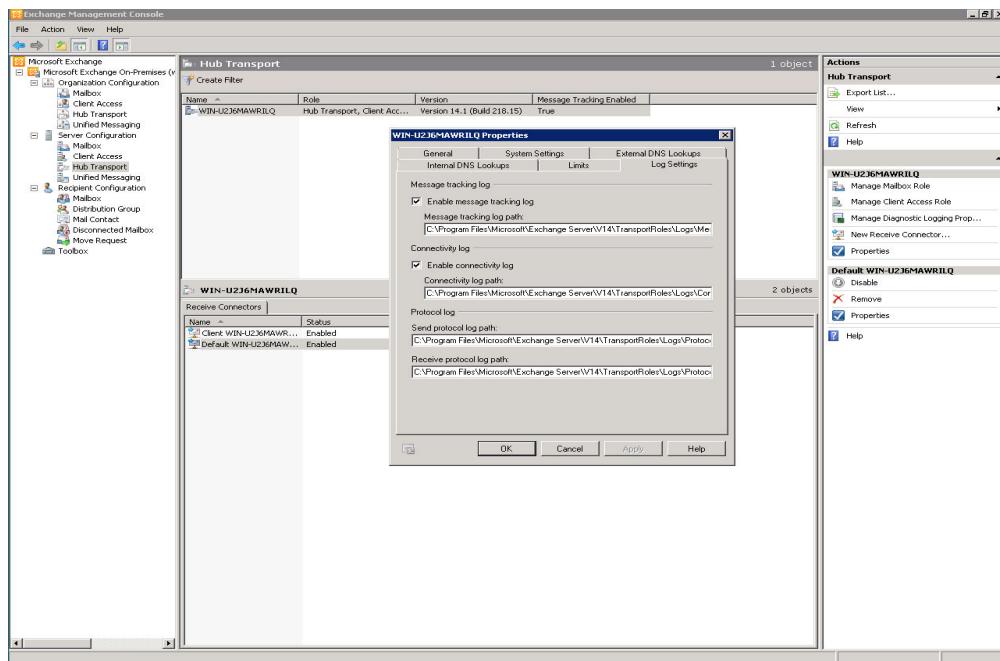
- [“Source System Setup”, on page 566](#)
- [“HawkEye Retriever Setup”, on page 567](#)

SOURCE SYSTEM SETUP

To enable tracking logs in Microsoft Exchange Management see the instructions below for either the Console or the Shell.

Exchange Management Console

- 1 Start the Exchange Management console.



- 2 Perform the following task, referring to the appropriate instructions for the transport server you are using:

- **For Edge Transport Server:**

Select **Edge Transport** and in the action pane, click the **Properties** link that is under the server name.

- **For Hub Transport Server:**

In the Console tree, click **Server Configuration** folder and select **Hub Transport**. In the action pane, click the **Properties** link that is under the server name

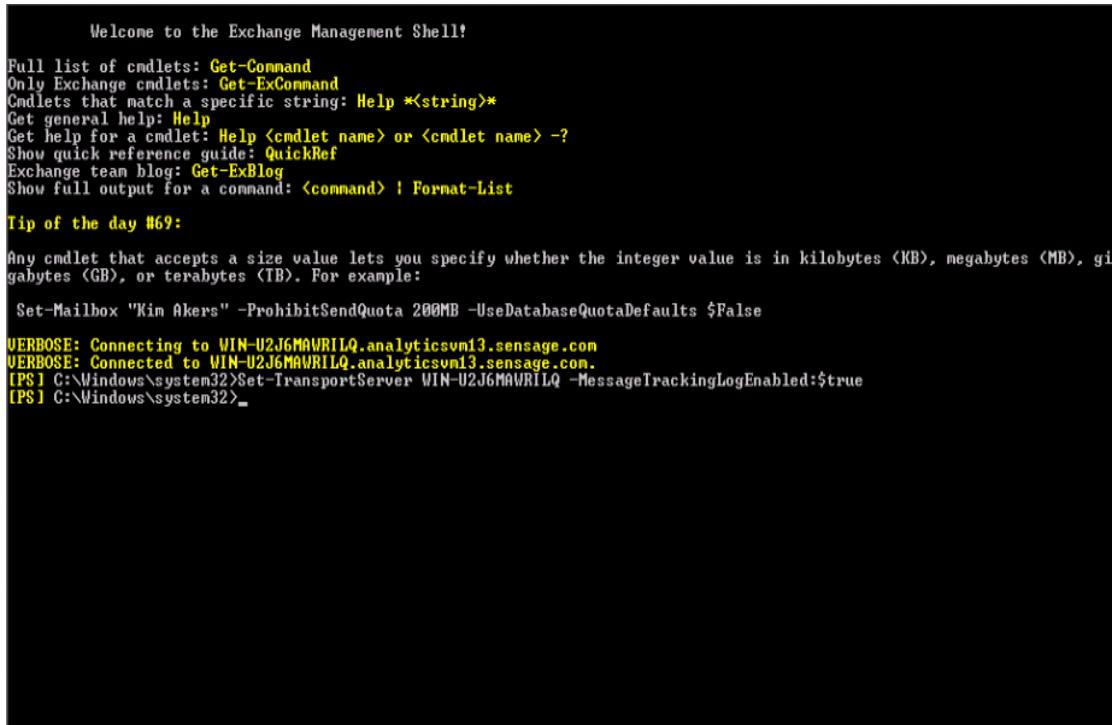
- 3 On the Properties page, click the tab **Log Settings**.

- 4 Ensure that the box **Enable message tracking log** is checked.

- 5 Click **OK**.

Exchange Management Shell

Instructions for the Shell are displayed in the screenshot below:



```
Welcome to the Exchange Management Shell!
Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Show quick reference guide: QuickRef
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List

Tip of the day #69:
Any cmdlet that accepts a size value lets you specify whether the integer value is in kilobytes <KB>, megabytes <MB>, gi
gabytes <GB>, or terabytes <TB>. For example:
Set-Mailbox "Kin Akers" -ProhibitSendQuota 200MB -UseDatabaseQuotaDefaults $False
VERBOSE: Connecting to WIN-U2J6MAWRILQ.analyticsvm13.sensage.com
VERBOSE: Connected to WIN-U2J6MAWRILQ.analyticsvm13.sensage.com.
[PS] C:\Windows\system32>Set-TransportServer WIN-U2J6MAWRILQ -MessageTrackingLogEnabled:$true
[PS] C:\Windows\system32>
```

SENSAGE AP COLLECTOR SETUP

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1** Open the syslog-ng configuration file: <*HawkEye AP Home*>etc/syslog-ng/syslog-ng.conf.
- 2** Specify Exchange host for the filter
`f_microsoft_exchange_tracking_sensageRetrieverAgent.`
- 3** Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

NOTE: The syslog configuration template, **syslog-ng_config_template.conf**, resides in the adapter directory.

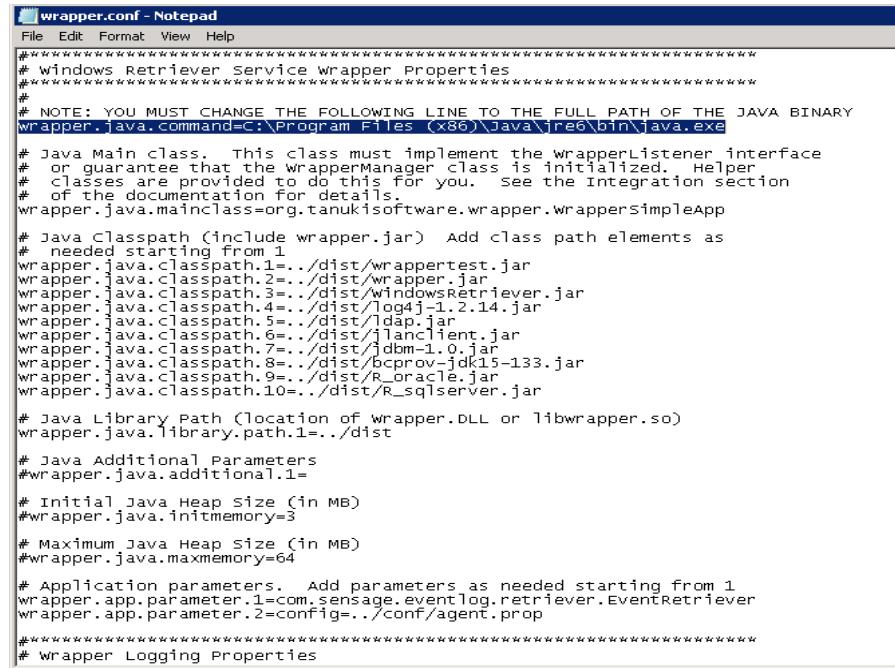
HawkEye Retriever Setup

- 1** Install Windows Retriever Agent on Exchange Server:
 - a** Download WindowsRetriever.zip.

b Unzip WindowsRetriever.zip to any folder. For example: **C:\WindowsRetriever**.

2 Edit conf/wrapper.conf to set your java .exe path. For example:

```
wrapper.java.command=C:\Program Files (x86)\java\jref6\bin\java.exe
```



```
# windows Retriever Service Wrapper Properties
# *****
# NOTE: YOU MUST CHANGE THE FOLLOWING LINE TO THE FULL PATH OF THE JAVA BINARY
wrapper.java.command=C:\Program Files (x86)\Java\jref6\bin\java.exe

# Java Main class. This class must implement the wrapperListener interface
# or guaranteed that the wrapperManager class is initialized. Helper
# classes are provided to do this for you. see the Integration section
# of the documentation for details.
wrapper.java.mainclass=org.tanukisoftware.wrapper.wrappersimpleapp

# Java Classpath (include wrapper.jar) Add class path elements as
# needed starting from 1
wrapper.java.classpath.1=../dist/wrappertest.jar
wrapper.java.classpath.2=../dist(wrapper.jar
wrapper.java.classpath.3=../dist/windowsRetriever.jar
wrapper.java.classpath.4=../dist/log4j-1.2.14.jar
wrapper.java.classpath.5=../dist/ldap.jar
wrapper.java.classpath.6=../dist/jlancient.jar
wrapper.java.classpath.7=../dist/jdbm-1.0.jar
wrapper.java.classpath.8=../dist/bcprov-jdk15-133.jar
wrapper.java.classpath.9=../dist/R_oracle.jar
wrapper.java.classpath.10=../dist/R_sqlserver.jar

# Java Library Path (location of wrapper.DLL or libwrapper.so)
wrapper.java.library.path.1=../dist

# Java Additional Parameters
#wrapper.java.additional.1=

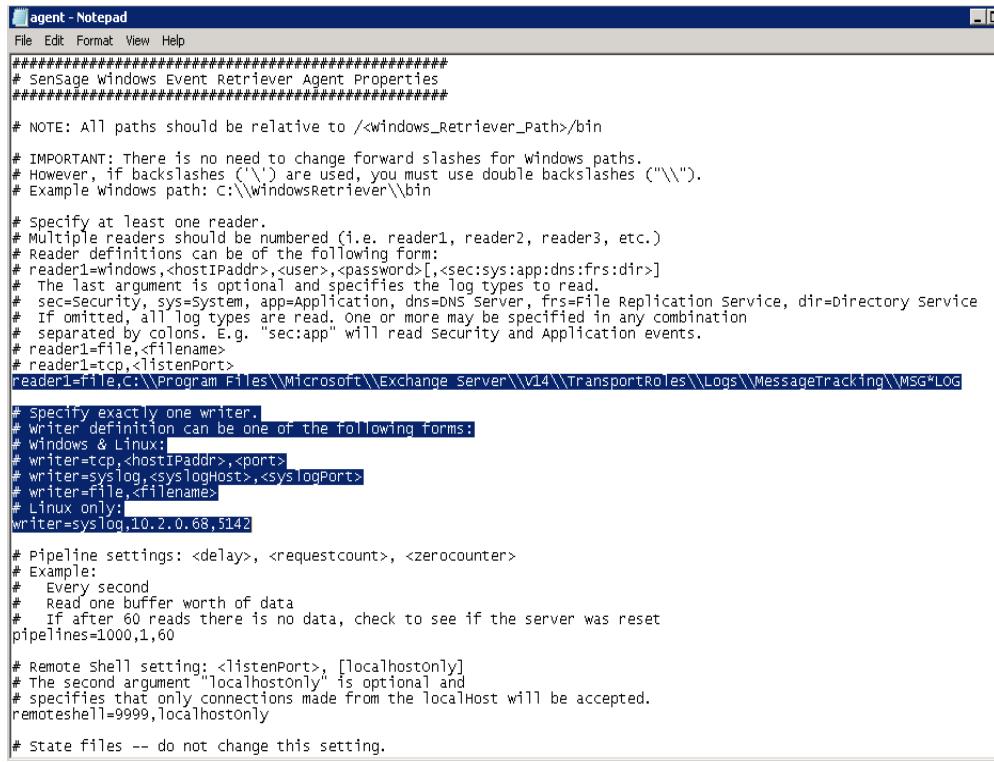
# Initial Java Heap size (in MB)
#wrapper.java.initmemory=3

# Maximum Java Heap size (in MB)
#wrapper.java.maxmemory=64

# Application parameters. Add parameters as needed starting from 1
wrapper.app.parameter.1=com.sensage.eventlog.retriever.EventRetriever
wrapper.app.parameter.2=config:./conf/agent.prop
# *****
# Wrapper Logging Properties
```

3 Edit conf/agent.prop to set your reader and writer. For example:

```
reader1=file,C:\\Program\\Files\\Microsoft\\Exchange\\Server\\V14\\Transport\\Roles\\Logs\\Message\\Tracking\\MSG*LOG
writer1=syslog,IP,5142
(where IP is YOUR_PUBLIC_COLLECTOR_IP and 5142 is port number)
```



```

agent - Notepad
File Edit Format View Help
#####
# SenSage Windows Event Retriever Agent Properties
#####

# NOTE: All paths should be relative to /<windows_Retriever_Path>/bin

# IMPORTANT: There is no need to change forward slashes for windows_paths.
# However, if backslashes ('\\') are used, you must use double backslashes ("\\").
# Example windows path: C:\\windowsRetriever\\bin

# Specify at least one reader.
# Multiple readers should be numbered (i.e. reader1, reader2, reader3, etc.)
# Reader definitions can be of the following form:
# reader1=windows,<hostIPaddr>,<user>,<password>[,<sec:sys:app:dns:frs:dir>]
# The last argument is optional and specifies the log types to read.
# sec=Security, sys=System, app=Application, dns=DNS Server, frs=File Replication Service, dir=Directory Service
# If omitted, all log types are read, one or more may be specified in any combination
# separated by colons. E.g. "sec:app" will read security and Application events.
# reader1=file,<filename>
# reader1=tcp,<listenPort>
reader1=file,C:\\Program Files\\Microsoft\\Exchange Server\\v14\\TransportRoles\\Logs\\MessageTracking\\MSG*LOG

# Specify exactly one writer.
# Writer definition can be one of the following forms:
# Windows & Linux:
# writer=tcp,<hostIPaddr>,<port>
# writer=syslog,<syslogHost>,<sys logPort>
# writer=file,<filename>
# Linux only:
writer=syslog,10.2.0.68,5142

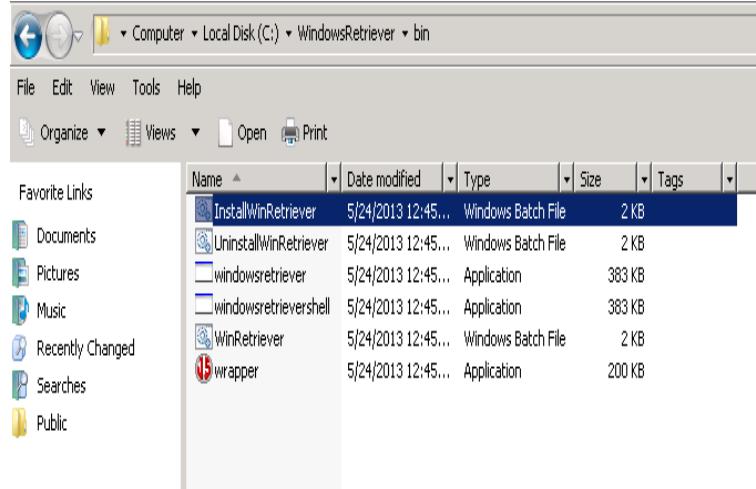
# Pipeline settings: <delay>, <requestcount>, <zerocounter>
# Example:
#   Every second
#   Read one buffer worth of data
#   If after 60 reads there is no data, check to see if the server was reset
pipelines=1000,1,60

# Remote Shell setting: <listenPort>, [localhostonly]
# The second argument "localhostonly" is optional and
# specifies that only connections made from the localhost will be accepted.
remoteshell=9999,localhostonly

# State files -- do not change this setting.

```

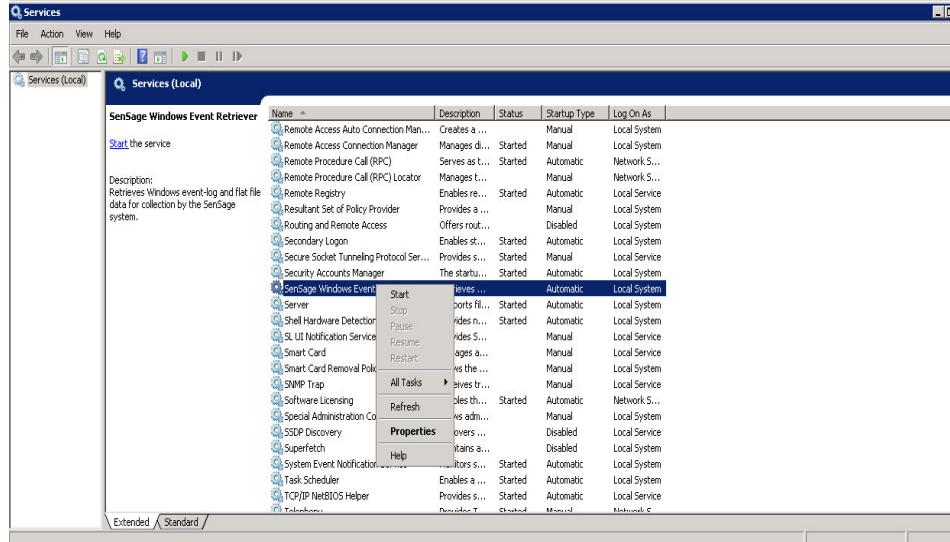
4 Install retriever and run bin/InstallWinRetriever.bat.



5 Start the service:

a Click **Start -> Administrative Tools -> Services**

b Find "HawkEye Windows Event Retriever"; then right-click on it and click **Start**.



6 Check the log file logs/retriever

Screenshot of a Windows File Explorer window showing a folder named 'retriever - Notepad'. The folder contains three files: 'placeholder' (5/24/2013 12:45...), 'retriever' (6/5/2013 4:02 AM), and 'service' (6/7/2013 1:19 AM). The 'retriever' file is selected.

```

INFO 2013-06-05 03:59:59,338: (WrapperSimpleAppMain) FileEventReader using a search pattern of C:\Program Files\Microsoft\Exchange Server\v14\TransportRoles\Logs\MessageTracking\MSG.*LOG starting from the top level directory ofC:\Program Files\Microsoft\Exchange Server\v14
WARN 2013-06-05 03:59:59,338: (WrapperSimpleAppMain) Config property not set: event.reader.reader1.requestcount, using default: 1000
WARN 2013-06-05 03:59:59,338: (WrapperSimpleAppMain) Config property not set: event.reader.reader1.prepend, using default: false
INFO 2013-06-05 03:59:59,338: (WrapperSimpleAppMain) Config property not set: event.reader.reader1.eventtype, so defaulting to no event type
WARN 2013-06-05 03:59:59,338: (WrapperSimpleAppMain) event.writer.writer.facility or event.writer.writer.severity was not set, the syslog writer will send a fully formed syslog message
WARN 2013-06-05 03:59:59,338: (WrapperSimpleAppMain) Missing config property: event.writer.writer.serializer.date.format, using default: yyyy-MM-dd
HTTP/1.1 200 OK
WARN 2013-06-05 03:59:59,338: (WrapperSimpleAppMain) Missing config property: event.writer.writer.serializer.delimiter, using default: |
WARN 2013-06-05 03:59:59,354: (WrapperSimpleAppMain) Config property not set: event.remotemanager.enabled so remote log management is disabled
WARN 2013-06-05 03:59:59,354: (WrapperSimpleAppMain) Config property not set: pipeline.monitor.enabled, using default: true
WARN 2013-06-05 03:59:59,354: (WrapperSimpleAppMain) Config property not set: pipeline.monitor.interval.seconds, using default: 60
WARN 2013-06-05 03:59:59,354: (WrapperSimpleAppMain) Config property not set: stats.monitor.enabled stats will not be collected
INFO 2013-06-05 03:59:59,354: (Thread-1) starting all pipeline threads now
INFO 2013-06-05 03:59:59,370: (Thread-3) Remote shell server listening on port: 9999
INFO 2013-06-05 03:59:59,370: (Thread-3) Remote shell accepting localhost connections only: true
INFO 2013-06-05 03:59:59,370: (Thread-4) Pipeline Monitor: checking for broken pipelines every 60 seconds.
INFO 2013-06-05 03:59:59,432: (Thread-2) Pipeline[pipeLine1] started.
INFO 2013-06-05 03:59:59,432: (Thread-2) Pipeline[pipeLine1] has become idle.
INFO 2013-06-05 04:00:07,479: (Thread-2) Pipeline[pipeLine1] is no longer idle. 7 records read.
INFO 2013-06-05 04:00:08,479: (Thread-2) Pipeline[pipeLine1] has become idle.
INFO 2013-06-05 04:00:13,495: (Thread-2) Pipeline[pipeLine1] is no longer idle. 7 records read.
INFO 2013-06-05 04:00:14,495: (Thread-2) Pipeline[pipeLine1] has become idle.
INFO 2013-06-05 04:00:19,510: (Thread-2) Pipeline[pipeLine1] is no longer idle. 17 records read.
INFO 2013-06-05 04:00:20,510: (Thread-2) Pipeline[pipeLine1] has become idle.
INFO 2013-06-05 04:00:25,526: (Thread-2) Pipeline[pipeLine1] is no longer idle. 6 records read.
INFO 2013-06-05 04:00:26,526: (Thread-2) Pipeline[pipeLine1] has become idle.
INFO 2013-06-05 04:00:31,526: (Thread-2) Pipeline[pipeLine1] is no longer idle. 13 records read.
INFO 2013-06-05 04:00:32,557: (Thread-2) Pipeline[pipeLine1] has become idle.
INFO 2013-06-05 04:00:59,370: (Thread-4) Pipeline Monitor: all pipelines appear to be working.
INFO 2013-06-05 04:01:59,370: (Thread-4) Pipeline Monitor: all pipelines appear to be working.
INFO 2013-06-05 04:02:48,743: (Thread-0) Attempting to stop pipelines

```

CHAPTER 41

microsoft_sharepoint_audit_sensageRetrieverAgent

SUMMARY INFORMATION

Log Adapter Component	Details
Name	microsoft_sharepoint_audit_sensageRetrieverAgent
Version	5.0.1
Source Vendor	Microsoft
Source Product	SharePoint
Source Component	SharePoint Server 2010
Source Version	2010 / 4.1
Source Host OS	Windows Server 2008 SP2 x64 or Windows Server 2008 R2 x64 or later
Transport Mechanism	Sensage Retriever Agent
PTL Filename	microsoft_sharepoint_audit_sensageRetrieverAgent.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	investigation_microsoft_sharepoint.sql
Look-up file	Not required
Scripts	Not required
Source-Specific Reports	None
Event Types	None

SETTING UP MICROSOFT_SHAREPOINT_AUDIT_SENSAGERETRIEVERAGENT LOG ADAPTER

This section describes how to configure the microsoft_sharepoint_audit_sensageRetrieverAgent log adapter. The following steps are required:

- “Source System Setup”, on page 572
- “SenSage AP Collector Setup”, on page 572

SOURCE SYSTEM SETUP

- 1 Make sure you have SharePoint Server 2010 installed and running.
 - 2 Open the site (not Central Admin CP) that you want to enable logging for in your browser. For example: <http://win-u2j6mawrlq/sites/test>
 - 3 Log in with an administrative account.
 - 4 Go to **Sites Action -> Site Settings**.
 - 5 Under the "Site Collection Administrator" section, choose **Site collection audit settings**.
 - 6 Check all boxes (or only those you need) in the "Document and Items" and "Lists, Libraries, and Sites" sections and press **OK**.
- Audit Logging for the site is now enabled. Next, you need to export logging items into files.
- 7 Download the **SPAuditLogExport** folder (`microsoft_SharePoint_Audit_sensageRetrieverAgent/source_system_setup/SPAuditLogExport`) to the PC that is running SharePoint (for example, to `C:\...`)
 - 8 Open the folder `%CommonProgramFiles%\Microsoft Shared\Web Server Extensions\14\CONFIG\POWERSHELL\Registration\`, locate the file `SharePoint.ps1`, and copy the file into the **SPAuditLogExport** folder.
 - 9 Check if the script is working by running:

```
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\PowerShell.exe  
C:\SPAuditLogExport\SPAuditLogExport.ps1
```

NOTE: The script exports "yesterday's" logs to the **SPAuditLogExport\exported** folder. If you have just enabled logging for today, the result file is empty because "yesterday" it was not enabled.

- 10 Place the script in the Task Scheduler and schedule the script to run daily. You can use **SharePoint Audit Log export.xml** as an example file to import into Task Scheduler

NOTE: The export script deletes log files older than 7 days.

SENSAGE AP COLLECTOR SETUP

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open the syslog-ng configuration file: `<HawkEye AP Home>/etc/syslog-ng/syslog-ng.conf`.
- 2 Set Microsoft SharePoint host for filter
`f_microsoft_Sharepoint_Audit_sensageRetrieverAgent.`
- 3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

NOTE: The syslog configuration template, **syslog-ng_config_template.conf**, resides in the adapter directory.

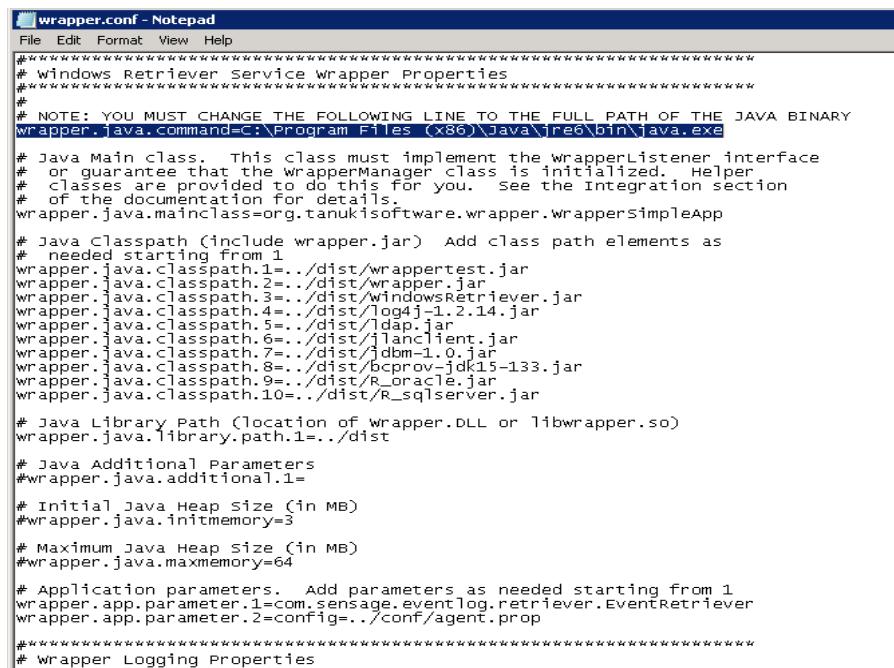
SenSage AP Retriever Setup

Install Windows Retriever Agent:

1 Unzip **WindowsRetriever.zip** to any folder. For example: **C:\WindowsRetriever**.

2 Edit **conf/wrapper.conf** to set your **java .exe** path. For example:

```
wrapper.java.command=C:\Program Files (x86)\java\jref6\bin\java.exe
```



```
wrapper.conf - Notepad
File Edit Format View Help
*****
# windows Retriever Service Wrapper Properties
*****
# NOTE: YOU MUST CHANGE THE FOLLOWING LINE TO THE FULL PATH OF THE JAVA BINARY
wrapper.java.command=C:\Program Files (x86)\Java\jref6\bin\java.exe

# Java Main class. This class must implement the wrapperlistener interface
# or guarantee that the WrapperManager class is initialized. Helper
# classes are provided to do this for you. See the Integration section
# of the documentation for details.
wrapper.java.mainclass=org.tanukisoftware.wrapper.WrapperSimpleApp

# Java Classpath (include wrapper.jar) Add class path elements as
# needed starting from 1
wrapper.java.classpath.1=../dist/wrappertest.jar
wrapper.java.classpath.2=../dist(wrapper.jar
wrapper.java.classpath.3=../dist/windowsretriever.jar
wrapper.java.classpath.4=../dist/log4j-1.2.14.jar
wrapper.java.classpath.5=../dist/1ancient.jar
wrapper.java.classpath.6=../dist/1ancient.jar
wrapper.java.classpath.7=../dist/1dbm-1.0.jar
wrapper.java.classpath.8=../dist/bcprov-jdk15-133.jar
wrapper.java.classpath.9=../dist/R_oracle.jar
wrapper.java.classpath.10=../dist/R_sqlserver.jar

# Java Library Path (location of wrapper.DLL or libwrapper.so)
wrapper.java.library.path.1=../dist

# Java Additional Parameters
#wrapper.java.additional.1=

# Initial Java Heap Size (in MB)
#wrapper.java.initmemory=3

# Maximum Java Heap Size (in MB)
#wrapper.java.maxmemory=64

# Application parameters. Add parameters as needed starting from 1
wrapper.app.parameter.1=com.sense.eventlog.retriever.EventRetriever
wrapper.app.parameter.2=config..conf/agent.prop
*****
# wrapper Logging Properties
```

3 Edit **conf/agent.prop** to set your reader and writer. For example:

```
reader1=file,C:\Program\Files\Microsoft\Exchange\Server\V14\Transport\Roles
\Logs\Message\Tracking\MSG*LOG
writer1=syslog,IP,514
```

(where IP is YOUR_PUBLIC_COLLECTOR_IP and 514 is port number)

```

agent.prop - Notepad
File Edit Format View Help
#####
# Sensage Windows Event Retriever Agent Properties
#####

# NOTE: All paths should be relative to /<windows_Retriever_Path>/bin

# IMPORTANT: There is no need to change forward slashes for windows path
# However, if backslashes ('\\') are used, you must use double backslashes
# Example windows path: C:\\WindowsRetriever\\bin

# Specify at least one reader.
# Multiple readers should be numbered (i.e. reader1, reader2, reader3, etc)
# Reader definitions can be of the following form:
# reader1=windows,<hostIPAddr>,<user>,<password>[,<sec:sys:app:dns:frs:>]
#   The last argument is optional and specifies the log types to read.
#   sec=security, sys=System, app=Application, dns=DNS Server, frs=File Replication Service
#   If omitted, all log types are read. One or more may be specified in a colon-separated list.
#   reader1=file,<filename>
#   reader1=tcp,<listenPort>

reader1=file,C:\\\\SPAuditLogExport\\\\exported\\\\AuditLogReport_For_*.csv

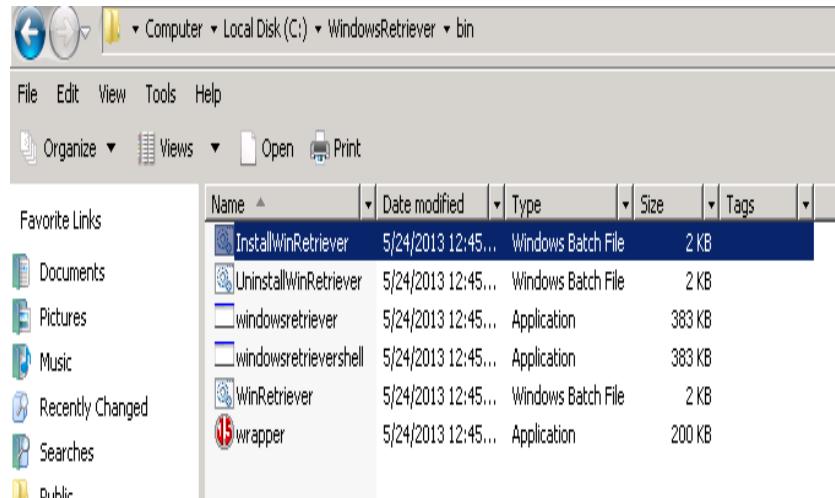
# Specify exactly one writer.
# Writer definition can be one of the following forms:
# windows & Linux:
# writer=tcp,<hostIPAddr>,<port>
# writer=syslog,<syslogHost>,<syslogPort>
# writer=file,<filename>
# Linux only:
writer=syslog,192.168.0.13,5142

# Pipeline settings: <delay>, <requestcount>, <zzerocounter>
# Example:
#   Every second
#   Read one buffer worth of data
#   If after 60 reads there is no data, check to see if the server was shutdown
# pipelines=1000,1,60

# Remote shell setting: <listenPort>, [localhostonly]
# The second argument "localhostonly" is optional and
# specifies that only connections made from the localhost will be accepted
remoteshell=9988,localhostonly

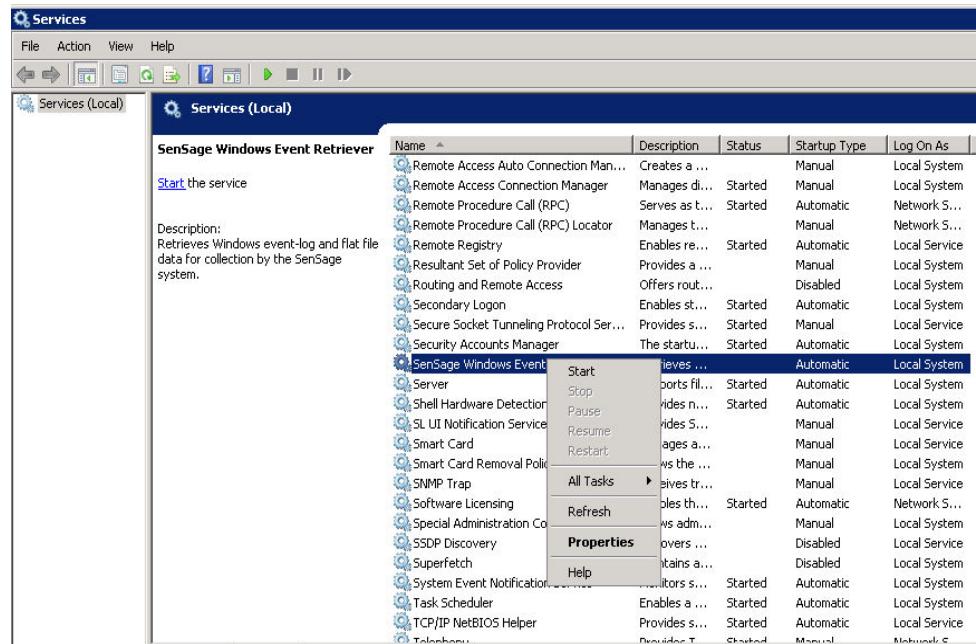
```

4 Install retriever and run bin/InstallWinRetriever.bat.



5 Start the service:

- Click **Start** -> **Administrative Tools** -> **Services**
- Find "SenSage AP Windows Event Retriever"; then right-click on it and click **Start**.



6 Check the log file logs/retriever.

retriever - Notepad

```

INFO 2013-06-05 03:59:59,338: (WrappersSimpleAppMain) FileeventReader using a search pattern of C:\Program Files\Microsoft\Exchange Server\V14
\\TransportRoles\Log\MessageTracking\MSG.*LOG starting from the top level directory of c:\Program Files\Microsoft\Exchange Server\V14
\TransportRoles\Log\MessageTracking
WARN 2013-06-05 03:59:59,338: (WrappersSimpleAppMain) Config property not set: event.reader.reader1.requestcount, using default: 1000
WARN 2013-06-05 03:59:59,338: (WrappersSimpleAppMain) Config property not set: event.reader.reader1.prepend, using default: false
INFO 2013-06-05 03:59:59,338: (WrappersSimpleAppMain) Config property not set: event.reader.reader1.eventtype, so defaulting to no event type.
WARN 2013-06-05 03:59:59,338: (WrappersSimpleAppMain) event.writer.writer.facility was not set, the syslog writer will
not send a fully formed syslog message
WARN 2013-06-05 03:59:59,338: (WrappersSimpleAppMain) Missing config property: event.writer.writer.serializer.date.format, using default: yyyy-MM-dd
HTTPPort=2
WARN 2013-06-05 03:59:59,338: (WrappersSimpleAppMain) Missing config property: event.writer.writer.serializer.delimiter, using default: |
WARN 2013-06-05 03:59:59,338: (WrappersSimpleAppMain) Config property not set: event.remotemanager.enabled so remote log management is disabled
WARN 2013-06-05 03:59:59,338: (WrappersSimpleAppMain) Config property not set: pipeline.monitor.enabled, using default: true
WARN 2013-06-05 03:59:59,338: (WrappersSimpleAppMain) Config property not set: pipeline.monitor.interval.seconds, using default: 60
INFO 2013-06-05 03:59:59,338: (Thread-1) starting all pipeline threads now
INFO 2013-06-05 03:59:59,370: (Thread-3) Remote shell server listening on port: 9999
INFO 2013-06-05 03:59:59,370: (Thread-3) Remote shell accepting localhost connections only: true
INFO 2013-06-05 03:59:59,370: (Thread-4) Pipeline Monitor: checking for broken pipelines every 60 seconds.
INFO 2013-06-05 03:59:59,432: (Thread-2) Pipeline[0|pipeline1] started.
INFO 2013-06-05 03:59:59,495: (Thread-2) Pipeline[0|pipeline1] has become idle.
INFO 2013-06-05 04:00:07,495: (Thread-2) Pipeline[0|pipeline1] is no longer idle. 7 records read.
INFO 2013-06-05 04:00:08,479: (Thread-2) Pipeline[0|pipeline1] has become idle.
INFO 2013-06-05 04:00:13,495: (Thread-2) Pipeline[0|pipeline1] is no longer idle. 7 records read.
INFO 2013-06-05 04:00:14,495: (Thread-2) Pipeline[0|pipeline1] has become idle.
INFO 2013-06-05 04:00:19,510: (Thread-2) Pipeline[0|pipeline1] is no longer idle. 17 records read.
INFO 2013-06-05 04:00:20,510: (Thread-2) Pipeline[0|pipeline1] has become idle.
INFO 2013-06-05 04:00:25,526: (Thread-2) Pipeline[0|pipeline1] is no longer idle. 6 records read.
INFO 2013-06-05 04:00:26,526: (Thread-2) Pipeline[0|pipeline1] has become idle.
INFO 2013-06-05 04:00:31,526: (Thread-2) Pipeline[0|pipeline1] is no longer idle. 13 records read.
INFO 2013-06-05 04:00:32,557: (Thread-2) Pipeline[0|pipeline1] has become idle.
INFO 2013-06-05 04:00:59,370: (Thread-4) Pipeline Monitor: all pipelines appear to be working.
INFO 2013-06-05 04:01:59,370: (Thread-4) Pipeline Monitor: all pipelines appear to be working.
INFO 2013-06-05 04:02:48,745: (Thread-0) Attempting to stop pipelines

```


CHAPTER 42

microsoft_windows_NonSecurityEvent_sensageRetriever

Log Adapter Component	Details
Name	<ul style="list-style-type: none"> • microsoft_windows_appEvent_sensageRetriever • microsoft_windows_dirEvent_sensageRetriever • microsoft_windows_dnsEvent_sensageRetriever • microsoft_windows_frsEvent_sensageRetriever • microsoft_windows_sysEvent_sensageRetriever • microsoft_windows2008_appEvent_sensageRetriever • microsoft_windows2008_dirEvent_sensageRetriever • microsoft_windows2008_dnsEvent_sensageRetriever • microsoft_windows2008_frsEvent_sensageRetriever • microsoft_windows2008_sysEvent_sensageRetriever
Version	1.0.0
Source Vendor	Microsoft
Source Product	Windows
Source Component	Application, Directory Service, DNS server, File Replication Service and System Events
Source Version	Server 2003 (English), Server 2008
Source Host OS	Windows Server 2003, Windows Server 2008
Transport Mechanism	sftp
PTL Filename	<ul style="list-style-type: none"> • microsoft_windows_appEvent_sensageRetriever.ptl • microsoft_windows_dirEvent_sensageRetriever.ptl • microsoft_windows_dnsEvent_sensageRetriever.ptl • microsoft_windows_frsEvent_sensageRetriever.ptl • microsoft_windows_sysEvent_sensageRetriever.ptl • microsoft_windows2008_appEvent_sensageRetriever.ptl • microsoft_windows2008_dirEvent_sensageRetriever.ptl • microsoft_windows2008_dnsEvent_sensageRetriever.ptl • microsoft_windows2008_frsEvent_sensageRetriever.ptl • microsoft_windows2008_sysEvent_sensageRetriever.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	None
Look-up file	Not required
Scripts	None

Log Adapter Component	Details
Source-Specific Reports	<ul style="list-style-type: none">• “Windows Application Events”, on page 232• “Windows Application Events Summary per Day”, on page 233• “Windows Directory Service Events”, on page 241• “Windows Directory Service Events Summary per Day”, on page 242• “Windows DNS Server Events”, on page 239• “Windows DNS Server Events Summary per Day”, on page 240• “Windows File Replication Service Events”, on page 236• “Windows File Replication Service Events Summary per Day”, on page 237• “Windows System Events”, on page 234• “Windows File Replication Service Events Summary per Day”, on page 237
Event Types	None

SETTING UP THE MICROSOFT_WINDOWS_NONSECURITYEVENT_SENSAGERETR IEVER

To configure Microsoft_Windows_NonSecurityEvent_sensageRetreiver log, refer to the following procedure: *Source System Setup* in Chapter 43, “microsoft_windows_securityEvent_sensageRetriever”.

CHAPTER 43

microsoft_windows_securityEvent_sensageRetriever

SYSTEM INFORMATION

Log Adapter Component	Details
Name	microsoft_windows_securityEvent_sensageRetriever
Version	1.0.0
Source Vendor	Microsoft
Source Product	Windows
Source Component	Security Events
Source Version	Server 2003 (English), Server 2008
Source Host OS	Windows 2003 Server
Transport Mechanism	sftp
PTL Filename	microsoft_windows_securityEvent_sensageRetriever.ptl
Parsing Rule	microsoft_windows_securityEvent_sensageRetriever.rule
Alerting Rule	<ul style="list-style-type: none"> • Microsoft Windows Security EVENTID Match Rule • Microsoft Windows Security Host and EVENTID Match Rule • Microsoft Windows Security Substring Match Rule • windowsSourceHealth.alert.rule
Connector Views	<ul style="list-style-type: none"> • accountAdditionAndDeletion_windows_microsoft_windows_securityEvent_sensageRetriever.sql • adminAccountActivity_windows_microsoft_windows_securityEvent_sensageRetriever.sql • investigation_microsoft_windows_securityEvent_sensageRetriever.sql • lossOfAuditMessages_windows_microsoft_windows_securityEvent_sensageRetriever.sql • passwordChangeAndReset_windows_microsoft_windows_securityEvent_sensageRetriever.sql • privilegedCommand_windows_microsoft_windows_securityEvent_sensageRetriever.sql • startStop_windows_microsoft_windows_securityEvent_sensageRetriever.sql • userLogin_windows_domainController_microsoft_windows_securityEvent_sensageRetriever.sql • userLogin_windows_nonDomainController_microsoft_windows_securityEvent_sensageRetriever.sql
Look-up file	None

Log Adapter Component	Details
Scripts	None
Source-Specific Reports	<ul style="list-style-type: none"> • “Windows Login Activity Details”, on page 213 • “Windows Login Failure Summary”, on page 214 • “Windows Login Success Summary”, on page 215 • “Windows Remote Login Details”, on page 217 • “Windows Group Member Addition and Deletion”, on page 220 • “Windows Password Changes and Resets”, on page 222 • “Windows User Account Locked and Unlocked by Date”, on page 223 • “Windows Account Rights Modified”, on page 225 • “Windows User Special Privileges Details”, on page 226 • “Windows System Startup Summary”, on page 228 • “Windows New Process Started”, on page 229 • “Windows Audit Log Cleared Summary”, on page 231 • “Windows System Events”, on page 234 • “Windows Loss of Audit Messages”, on page 244 • “Windows Active Directory Object Changes”, on page 245 • “Windows Security Objects Deleted”, on page 251
Event Types	<ul style="list-style-type: none"> • “Account Addition and Deletion”, on page 95 • “Administrative Account Activity”, on page 98 • “Audit Event”, on page 109 • “Loss of Audit Messages”, on page 117 • “Password Changes and Resets”, on page 127 • “Privileged Commands”, on page 129 • “System Startup and Shutdown”, on page 136 • “Unparsed Data”, on page 139 • “User Logins: Windows Non-domain Controller”, on page 145 • “User Logins: Windows”, on page 146

SETTING UP THE MICROSOFT_WINDOWS_SECURITYEVENT_SENSAGERETRIEVER LOG ADAPTER

This document describe how to configure the microsoft_windows_securityEvent_sensageRetriever log adapter. The following steps are required:

- “Source System Setup”, next
- “SenSage AP Collector Configuration”, on page 585

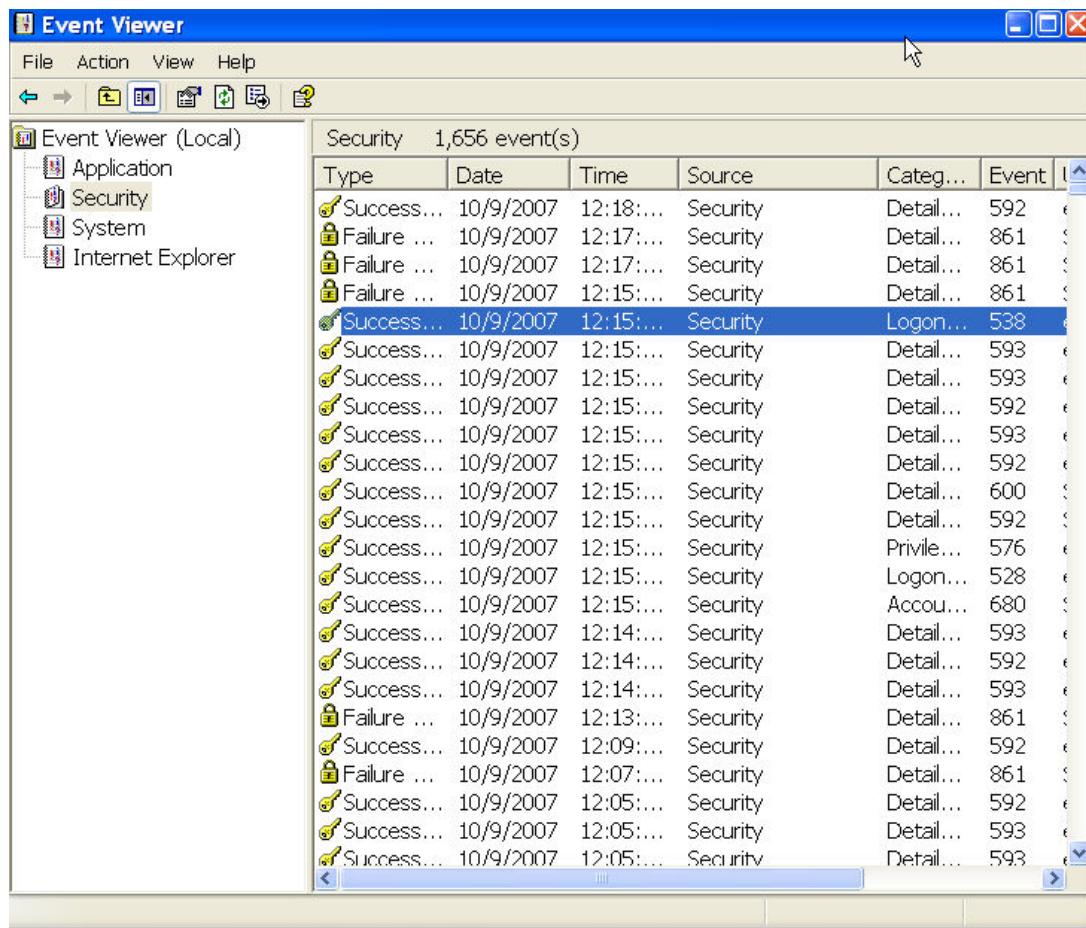
SOURCE SYSTEM SETUP

You set up the Windows Event Retriever to collect data from the following types of Windows deployments:

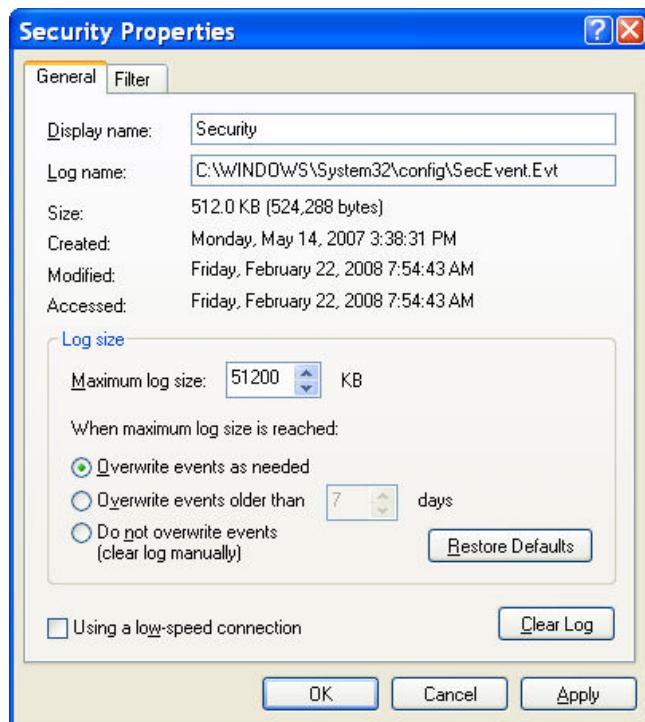
- Independent Windows machines that are not part of an Active Directory domain. See “Source System Setup for Windows machines (no Active Directory)”, next.
- Windows machines that are part of an Active Directory domain. See “Source System Setup for Windows machines (Active Directory domain)”, on page 584.

Source System Setup for Windows machines (no Active Directory)

- 1 Log in to the Windows machine from which you need to collect logs. You must log in using an account that has administrative privileges.
- 2 Click Start --> Control Panel -> Administrative Tools -> Event Viewer.
- 3 Select the **Security** event category.

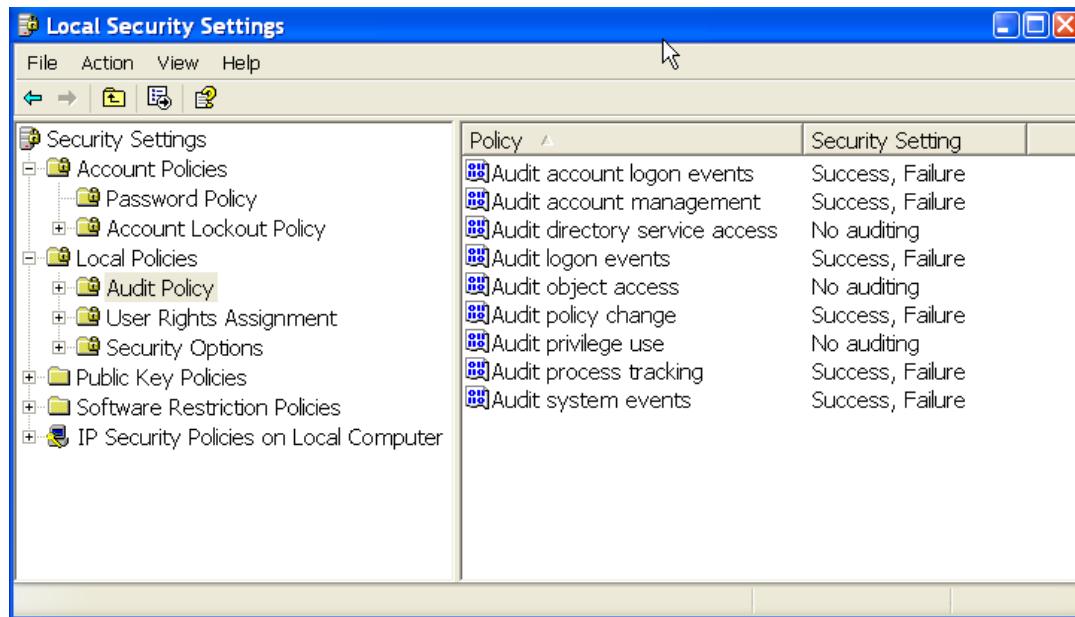


- 4 Right-click Security and select **Properties**. The following dialog box is displayed:



- 5 Set the **Maximum log size** to 51200 KB. Depending on the level of activity on the monitored system, you may need to increase this setting to avoid losing log messages.
- 6 Select **Overwrite events as needed**.
- 7 Click **OK** to close the Security Properties dialog box.
- 8 Click **File -> Exit** to close the Event Viewer dialog box.
- 9 Click **Start -> Control Panel -> Administrative Tools -> Local Security Policy**.

- 10 On the left-hand navigation tree double click **Local Policies** to open it, and then select **Audit Policy**.



- 11 Double-click on each of the nine policies except **Audit object access** and enable auditing for both Success and Failure. Enable auditing only for Success for **Audit object access**.



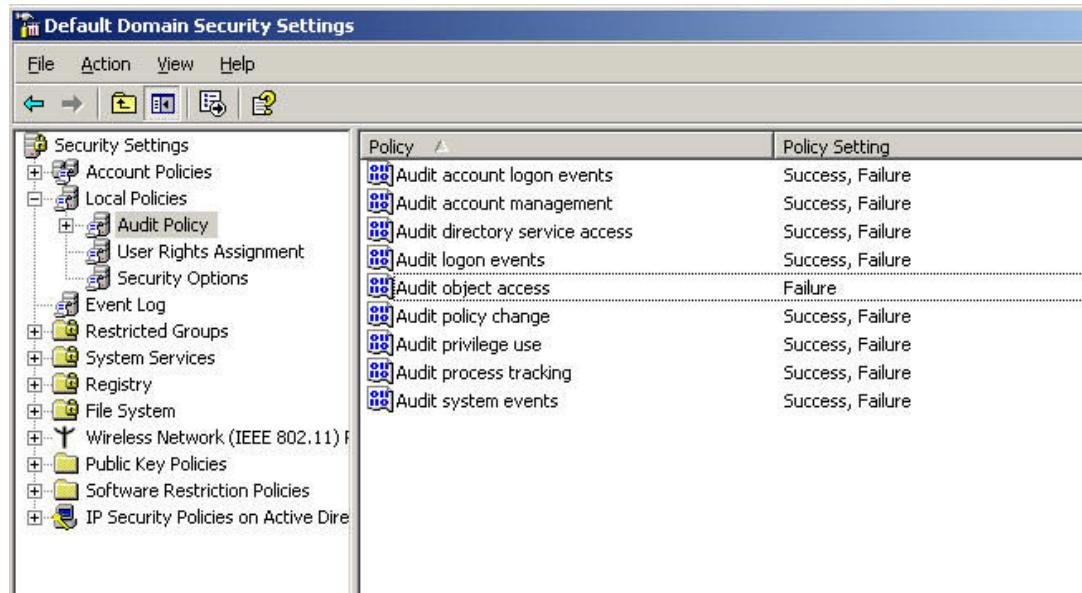
- 12 Click **OK** to close the Audit Properties dialog box.

- 13 Click **File -> Exit** to close the Local Security Settings dialog box.

- 14 Configure the SenSage AP Windows Retriever using the instructions found in the "Receiver Configuration" and "Windows Event Retriever" chapters of the *Event Collection Guide*, available from the SenSage AP Documentation page.

Source System Setup for Windows machines (Active Directory domain)

- 1 Log in to the Windows machine hosting the domain controller for the machines from which you need to collect logs. You must log in using an account that has administrative privileges.
- 2 Click **Start -> Settings -> Control Panel -> Administrative Tools -> Domain Security Policy.**



- 3 On the left-hand navigation tree double click **Local Policies** to open it, and then select **Audit Policy**.
- 4 Double-click on each of the nine policies except **Audit object access** and enable auditing for both Success and Failure. Enable auditing only for Success for **Audit object access**.



SENSAGE AP COLLECTOR CONFIGURATION

Set up the SenSage AP Collector to use batch collection from the Windows domain controller host where the SenSage AP Windows Event Retriever is running.

For more information, see:

- [Chapter 2: Configuring SenSage AP Collector Modules](#) in the *Collector Guide*.
- [Chapter 4: SenSage AP Retriever Configuration](#) in the *Collector Guide*.

CHAPTER 44

microsoft_windows2008_securityEvent_sensageRetriever

SYSTEM INFORMATION

Log Adapter Component	Details
Name	microsoft_windows2008_securityEvent_sensageRetriever
Version	1.0.0
Source Vendor	Microsoft
Source Product	Windows
Source Component	Security Events
Source Version	Server 2008, Server 2012
Source Host OS	Windows 2008 Server, Windows 2012 Server
Transport Mechanism	sftp
PTL Filename	microsoft_windows2008_securityEvent_sensageRetriever.ptl
Parsing Rule	microsoft_windows_securityEvent_sensageRetriever.rule
Alerting Rule	<ul style="list-style-type: none"> • Microsoft Windows Security EVENTID Match Rule • Microsoft Windows Security Host and EVENTID Match Rule • Microsoft Windows Security Substring Match Rule • windowsSourceHealth.alert.rule
Connector Views	<ul style="list-style-type: none"> • accountAdditionAndDeletion__windows__microsoft_windows2008_securityEvent_sensageRetriever.sql • adminAccountActivity__windows__microsoft_windows2008_securityEvent_sensageRetriever.sql • investigation__microsoft_windows2008_securityEvent_sensageRetriever.sql • lossOfAuditMessages__windows__microsoft_windows2008_securityEvent_sensageRetriever.sql • passwordChangeAndReset__windows__microsoft_windows2008_securityEvent_sensageRetriever.sql • privilegedCommand__windows__microsoft_windows2008_securityEvent_sensageRetriever.sql • userLogin__windows__domainController__microsoft_windows2008_securityEvent_sensageRetriever.sql • userLogin__windows__nonDomainController__microsoft_windows2008_securityEvent_sensageRetriever.sql
Look-up file	None
Scripts	None

Log Adapter Component	Details
Source-Specific Reports	<ul style="list-style-type: none"> • “Windows Login Activity Details”, on page 213 • “Windows Login Failure Summary”, on page 214 • “Windows Login Success Summary”, on page 215 • “Windows Remote Login Details”, on page 217 • “Windows Group Member Addition and Deletion”, on page 220 • “Windows Password Changes and Resets”, on page 222 • “Windows User Account Locked and Unlocked by Date”, on page 223 • “Windows Account Rights Modified”, on page 225 • “Windows User Special Privileges Details”, on page 226 • “Windows System Startup Summary”, on page 228 • “Windows New Process Started”, on page 229 • “Windows Audit Log Cleared Summary”, on page 231 • “Windows System Events”, on page 234 • “Windows Loss of Audit Messages”, on page 244 • “Windows Active Directory Object Changes”, on page 245 • “Windows Security Objects Deleted”, on page 251
Event Types	<ul style="list-style-type: none"> • “Account Addition and Deletion”, on page 95 • “Administrative Account Activity”, on page 98 • “Audit Event”, on page 109 • “Loss of Audit Messages”, on page 117 • “Loss of Audit Messages: Windows”, on page 118 • “Password Changes and Resets”, on page 127 • “Privileged Commands”, on page 129 • “System Startup and Shutdown”, on page 136 • “Unparsed Data”, on page 139 • “User Logins: Windows Non-domain Controller”, on page 145 • “User Logins: Windows”, on page 146

SETTING UP THE MICROSOFT_WINDOWS2008_SECURITYEVENT_ SENSAGERETRIEVER LOG ADAPTER

This document describe how to configure the microsoft_windows2008_securityEvent_sensageRetriever log adapter. The following steps are required:

- “Source System Setup”, next
- “SenSage AP Collector Configuration”, on page 593

SOURCE SYSTEM SETUP

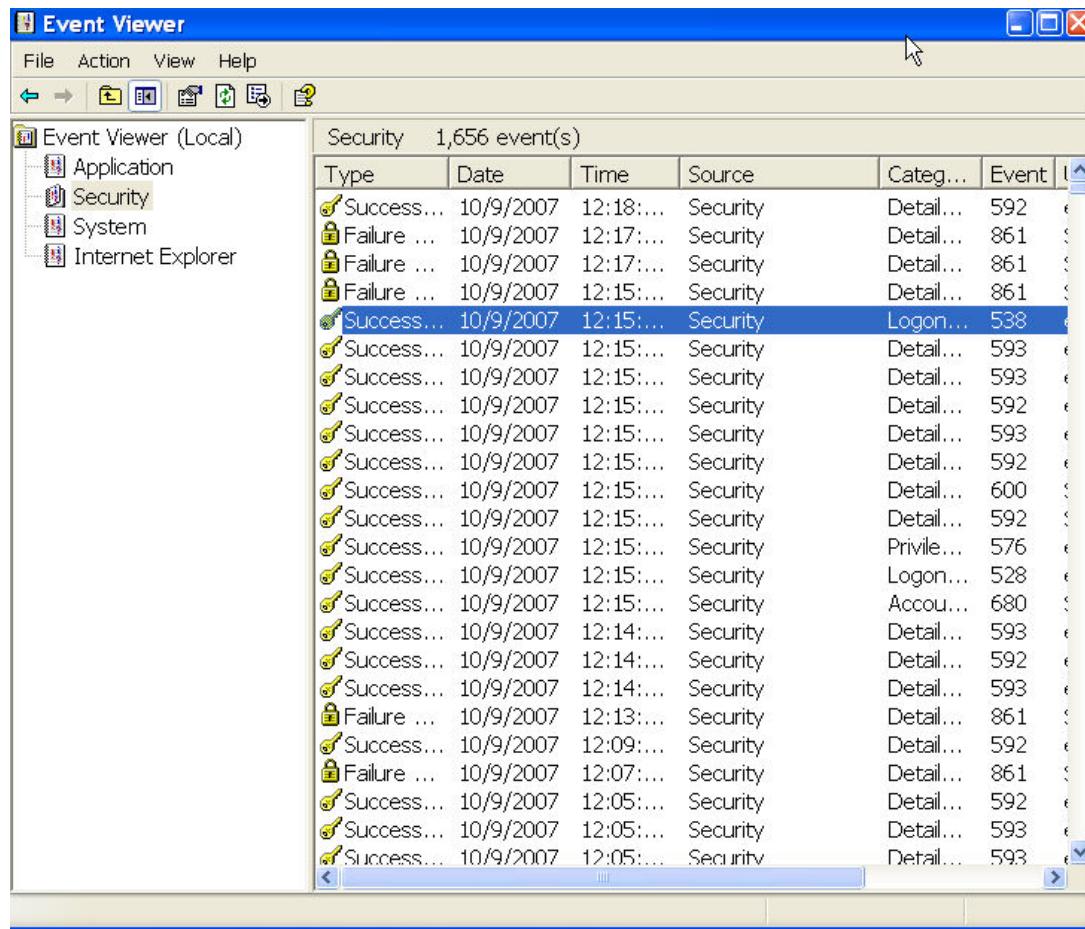
You set up the Windows Event Retriever to collect data from the following types of Windows deployments:

- Independent Windows machines that are not part of an Active Directory domain. See “Source System Setup for Windows Machines (no Active Directory)”, next.

- Windows machines that are part of an Active Directory domain. See “Source System Setup for Windows Machines (Active Directory Domain)”, on page 591.

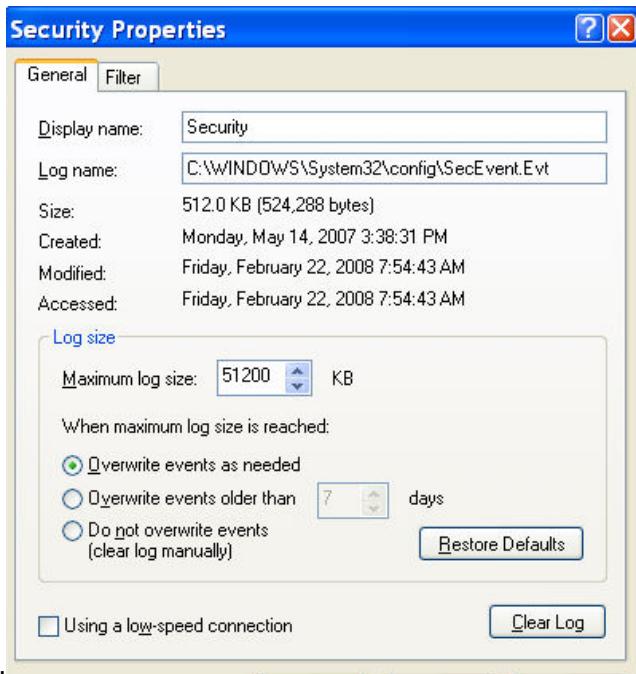
Source System Setup for Windows Machines (no Active Directory)

- 1 Log in to the Windows machine from which you need to collect logs. You must log in using an account that has administrative privileges.
- 2 Click on Start -> Control Panel -> Administrative Tool -> Event Viewer.
- 3 Select the **Security** event category.



- 4 Right-click **Security** and select **Properties**.

The following dialog box is displayed:

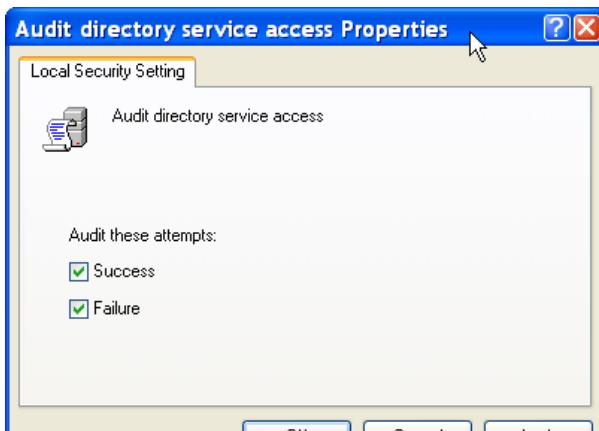


- 5 Set the Maximum log size to 51200 KB. Depending on the level of activity on the monitored system, you may need to increase this setting to avoid losing log messages.
- 6 Select **Overwrite events as needed**.
- 7 Click **OK** to close the Security Properties dialog box.
- 8 Click **File -> Exit** to close the Event Viewer dialog box.
- 9 Click **Start -> Control Panel -> Administrative Tools -> Local Security Policy**.
- 10 In the left-hand navigation tree, double click **Local Policies** to open it, and then select **Audit Policy**.

Local Security Settings

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit privilege use	No auditing
Audit process tracking	Success, Failure
Audit system events	Success, Failure

- 11 Double-click on each of the nine policies except **Audit object access** and enable auditing for both Success and Failure. Enable auditing only for **Audit object access**, both Success and Failure.



- 12 Click **OK** to close the Audit Properties dialog box.
- 13 Click **File -> Exit** to close the Local Security Settings dialog box.
- 14 Configure the SenSage AP Windows Retriever using the instructions found in the “Receiver Configuration” and “Windows Event Retriever” chapters of the *Event Collection Guide*, available from the SenSage AP Documentation page.

Source System Setup for Windows Machines (Active Directory Domain)

- 1 Log in to the Windows machine hosting the domain controller for the machines from which you need to collect logs. You must log in using an account that has administrative privileges.
- 2 Click **Start -> Settings -> Control Panel -> Administrative Tools -> Domain Security Policy.**

Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

- 3 On the left-hand navigation tree double-click **Local Policies** to open it, and then select **Audit Policy**.
- 4 Double-click on each of the nine policies except **Audit object access** and enable auditing for both Success and Failure. Enable auditing only for Success for **Audit object access**:



For source system running Windows 2008 Server, also perform the following steps:

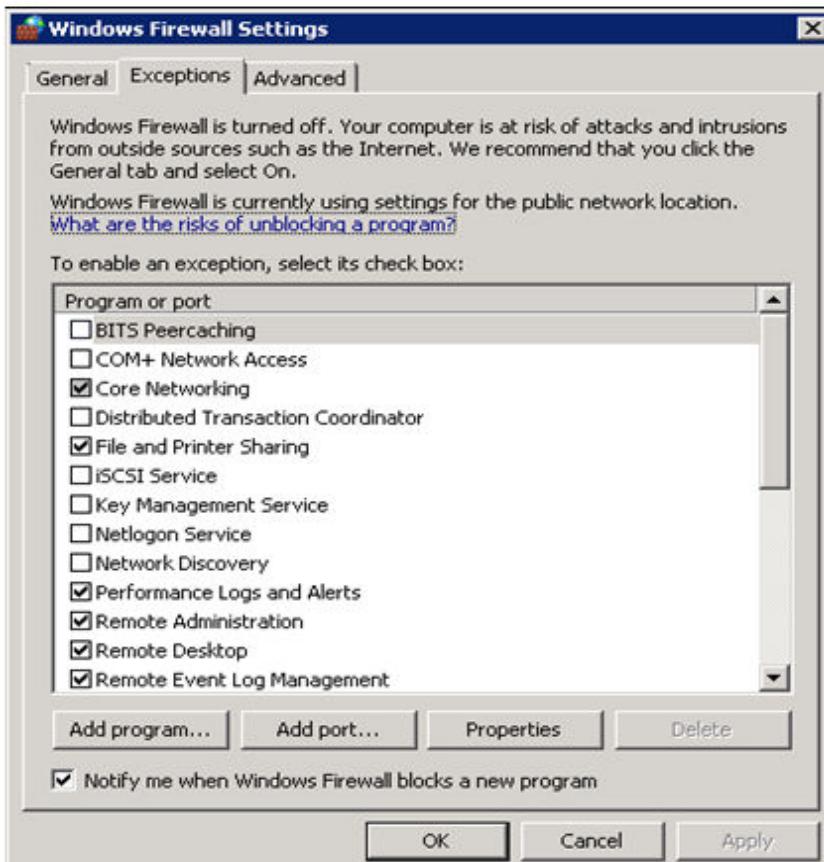
- 1 Open the Windows Control Panel (**Start > Control Panel**).
- 2 Double-click **Windows Firewall**.
- 3 Click the **Change settings** link.



- 4 Select the Exceptions tab.

5 Enable the following:

- Remote Event Log Management
- File and Print Services



SenSage AP Collector Configuration

Set up the SenSage AP Connector to use batch collection from the Windows domain controller host where the SenSage AP Windows Event Retriever is running. for more information, see:

- Chapter 2: Configuring SenSage AP Collector Modules in the *Collector Guide*.
- Chapter 4: SenSage AP Retriever Configuration in the *Collector Guide*.

microsoft_windows_securityEvent_snare

SYSTEM INFORMATION

Log Adapter Component	Details
Name	microsoft_windows_securityEvent_snare
Version	3.1.13
Source Vendor	Microsoft
Source Product	Windows
Source Component	Windows Security Events
Source Version	Server 2003
Source Host OS	Windows 2003 (English, Japanese)
Transport Mechanism	Snare
PTL Filename	microsoft_windows_securityEvent_snare.ptl
Parsing Rule	microsoft_windows_securityEvent_snare.rule
Alerting Rule	None
Connector Views	<ul style="list-style-type: none"> • accountAdditionAndDeletion__windows__microsoft_windows_securityEvent_snare.sql • adminAccountActivity__windows__microsoft_windows_securityEvent_snare.sql • investigation__microsoft_windows_securityEvent_snare.sql;lossOfAuditMessages__windows__microsoft_windows_securityEvent_snare.sql • lossOfAuditMessages__windows__microsoft_windows_securityEvent_snare.sql • passwordChangeAndReset__windows__microsoft_windows_securityEvent_snare.sql • privilegedCommand__windows__microsoft_windows_securityEvent_snare.sql • startStop__windows__microsoft_windows_securityEvent_snare.sql • userLogin__windows__domainController__microsoft_windows_securityEvent_snare.sql • userLogin__windows__nonDomainController__microsoft_windows_securityEvent_snare.sql
Look-up file	None
Scripts	None

Log Adapter Component	Details
Source-Specific Reports	<ul style="list-style-type: none"> • “Windows Login Activity Details”, on page 213 • “Windows Login Failure Summary”, on page 214 • “Windows Login Success Summary”, on page 215 • “Windows Remote Login Details”, on page 217 • “Windows Group Member Addition and Deletion”, on page 220 • “Windows Password Changes and Resets”, on page 222 • “Windows User Account Locked and Unlocked by Date”, on page 223 • “Windows Account Rights Modified”, on page 225 • “Windows User Special Privileges Details”, on page 226 • “Windows System Startup Summary”, on page 228 • “Windows New Process Started”, on page 229 • “Windows Audit Log Cleared Summary”, on page 231 • “Windows System Events”, on page 234 • “Windows Loss of Audit Messages”, on page 244 • “Windows Active Directory Object Changes”, on page 245 • “Windows Security Objects Deleted”, on page 251
Event Types	<ul style="list-style-type: none"> • “Account Addition and Deletion”, on page 95 • “Administrative Account Activity”, on page 98 • “Audit Event”, on page 109 • “Loss of Audit Messages”, on page 117 • “Loss of Audit Messages: Windows”, on page 118 • “Password Changes and Resets”, on page 127 • “Privileged Commands”, on page 129 • “System Startup and Shutdown”, on page 136 • “Unparsed Data”, on page 139 • “User Logins: Windows Non-domain Controller”, on page 145 • “User Logins: Windows”, on page 146

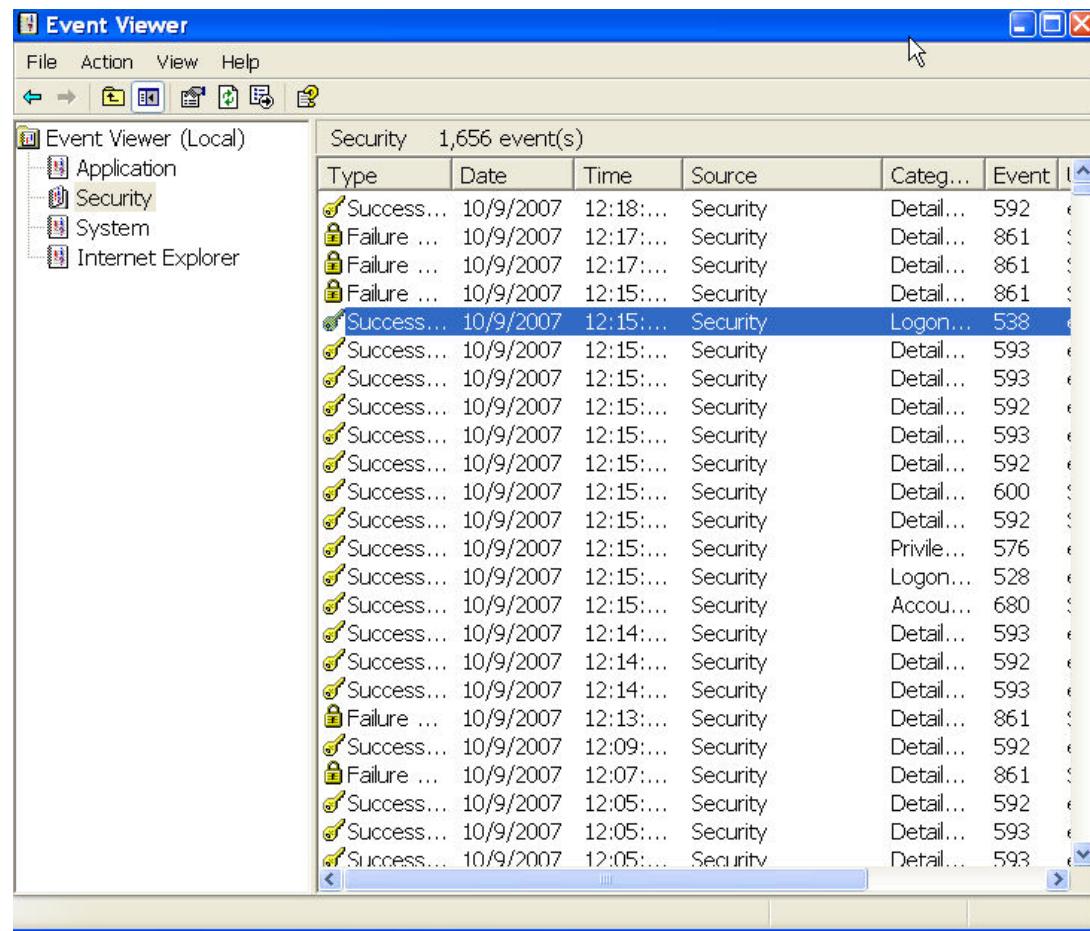
SETTING UP THE MICROSOFT_WINDOWS_SECURITYEVENT_SNARE LOG ADAPTER

This document describes how to configure the microsoft_windows_securityEvent_snare log adapter. The following steps are required:

- “Source System Setup:”, on page 596
- “Configuring Snare Agent”, on page 603
- “SenSage AP Collector syslog-ng Setup”, on page 604

SOURCE SYSTEM SETUP:

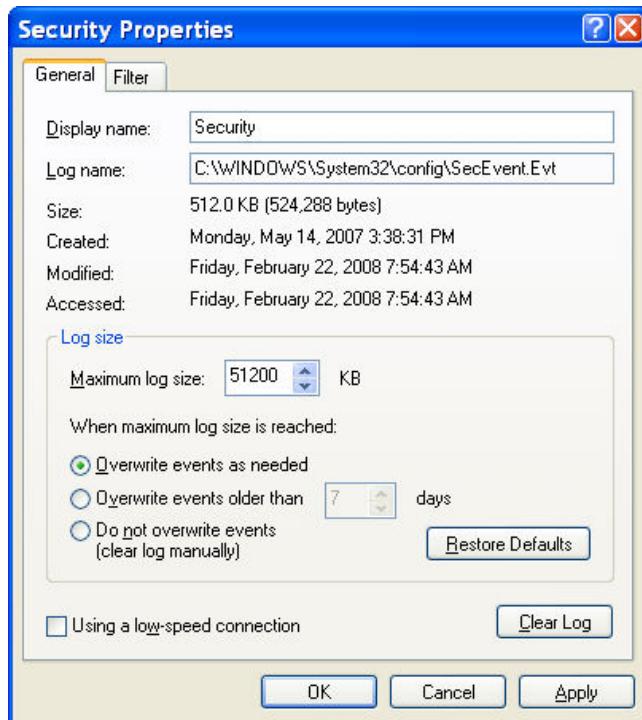
- 1 Log in to each server from which you need to collect logs using an account that has administrative privileges.
- 2 Click on **Start -> Control Panel -> Administrative Tool -> Event Viewer**.

3 Select the Security event category:

The screenshot shows the Windows Event Viewer window titled "Event Viewer (Local)". The left pane displays four categories: Application, Security, System, and Internet Explorer. The "Security" category is selected. The right pane shows a table of 1,656 security events. The columns are Type, Date, Time, Source, Category, Event ID, and Logon ID. Most events are of type "Success" or "Failure" and are categorized under "Security". The first event in the list is a "Success" event for "Logon" with Event ID 538.

Type	Date	Time	Source	Category	Event ID	Logon ID
Success...	10/9/2007	12:18:...	Security	Detail...	592	
Failure ...	10/9/2007	12:17:...	Security	Detail...	861	
Failure ...	10/9/2007	12:17:...	Security	Detail...	861	
Failure ...	10/9/2007	12:15:...	Security	Detail...	861	
Success...	10/9/2007	12:15:...	Security	Logon...	538	
Success...	10/9/2007	12:15:...	Security	Detail...	593	
Success...	10/9/2007	12:15:...	Security	Detail...	593	
Success...	10/9/2007	12:15:...	Security	Detail...	592	
Success...	10/9/2007	12:15:...	Security	Detail...	593	
Success...	10/9/2007	12:15:...	Security	Detail...	592	
Success...	10/9/2007	12:15:...	Security	Detail...	600	
Success...	10/9/2007	12:15:...	Security	Detail...	592	
Success...	10/9/2007	12:15:...	Security	Privile...	576	
Success...	10/9/2007	12:15:...	Security	Logon...	528	
Success...	10/9/2007	12:15:...	Security	Accou...	680	
Success...	10/9/2007	12:14:...	Security	Detail...	593	
Success...	10/9/2007	12:14:...	Security	Detail...	592	
Success...	10/9/2007	12:14:...	Security	Detail...	593	
Failure ...	10/9/2007	12:13:...	Security	Detail...	861	
Success...	10/9/2007	12:09:...	Security	Detail...	592	
Failure ...	10/9/2007	12:07:...	Security	Detail...	861	
Success...	10/9/2007	12:05:...	Security	Detail...	592	
Success...	10/9/2007	12:05:...	Security	Detail...	593	
Success...	10/9/2007	12:05:...	Security	Detail...	593	

4 Right-click **Security** and select **Properties**.



5 Select **Overwrite events as needed**.

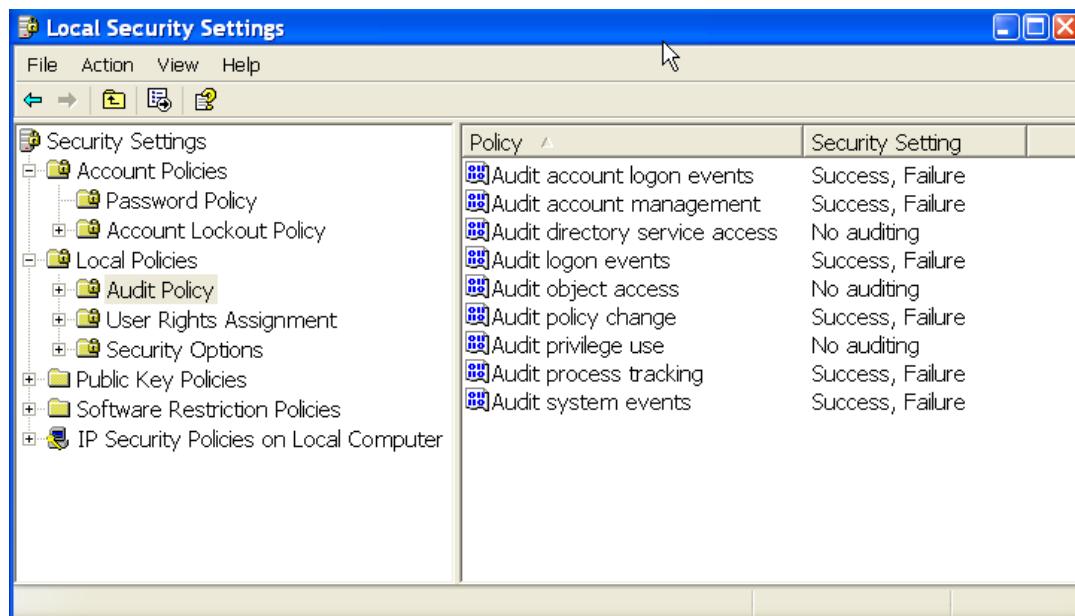
6 Set the Maximum log size to 51200 KB. Depending on the level of activity on the monitored system, you may need to increase this setting to avoid losing log messages.

7 Click **OK** to close the Security Properties dialog box.

8 Click **File -> Exit** to close the Event Viewer dialog box.

9 Click **Start -> Control Panel -> Administrative Tools -> Local Security Policy**.

- 10 In the left-hand navigation tree, double click **Local Policies** to open it, and then select **Audit Policy**.



- 11 Double-click on each of the nine policies and enable auditing for both Success and Failure.



- 12 Click **OK** to close the Audit Properties dialog box.

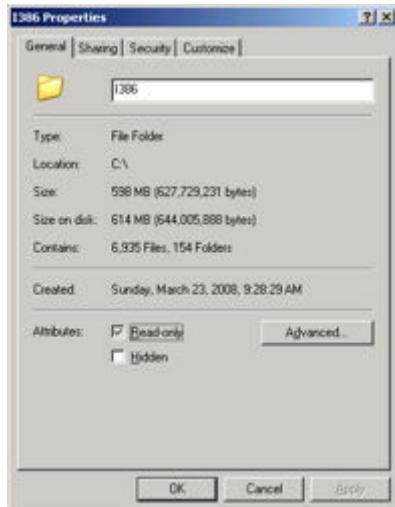
- 13 Click **File -> Exit** to close the Local Security Settings dialog box.

- 14 (Optional) Enable Sensitive Object Access Logging

- 15 Enabling Sensitive Object Access Logging can create large quantities of log data. However, this logging is required in some environments where the files contain sensitive information

such as customer lists or credit card numbers. If you need this log information, follow these steps on the local Windows file server for directories containing sensitive files:

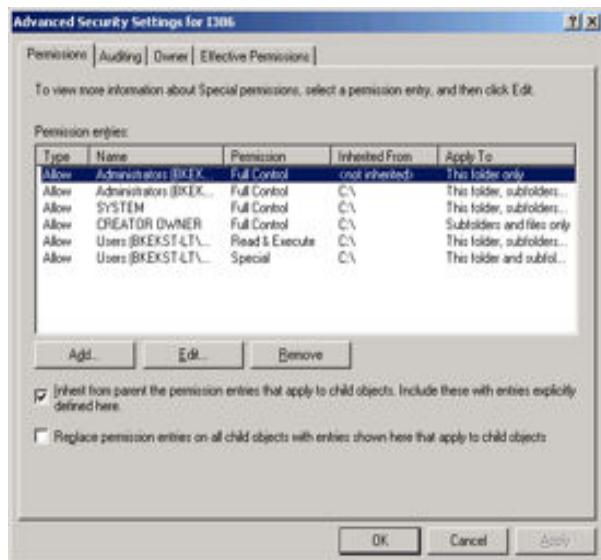
- a Right-click on the folder you would like to enable for auditing and select **Properties**:



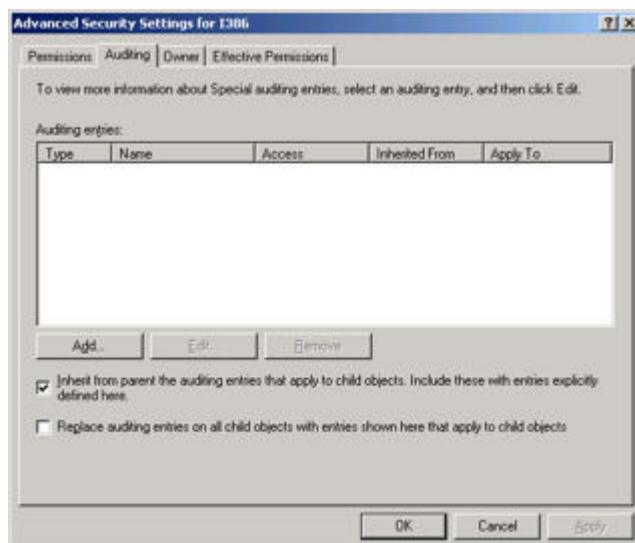
- b Select the **Security** tab.



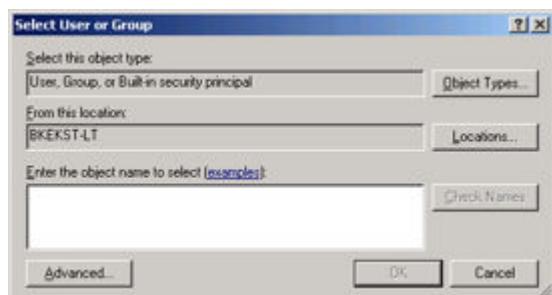
- c Click the **Advanced** button.



d Click the Auditing tab.



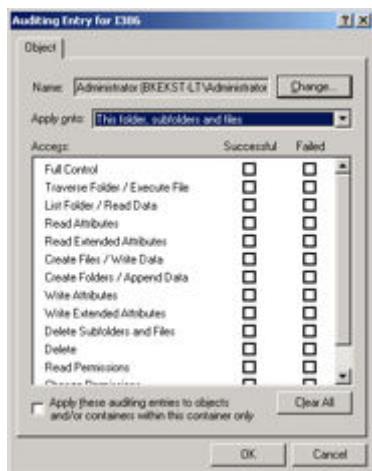
e Click the Add... button.



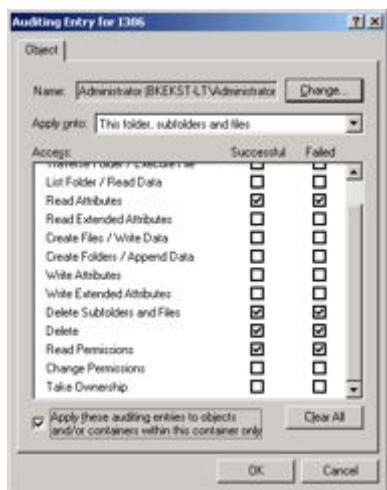
f Type the names of the objects you want to have audited, for example, user accounts or domains. Click the **Check Names button to verify the objects exist.**



g Click **OK**. The following dialog box displays:



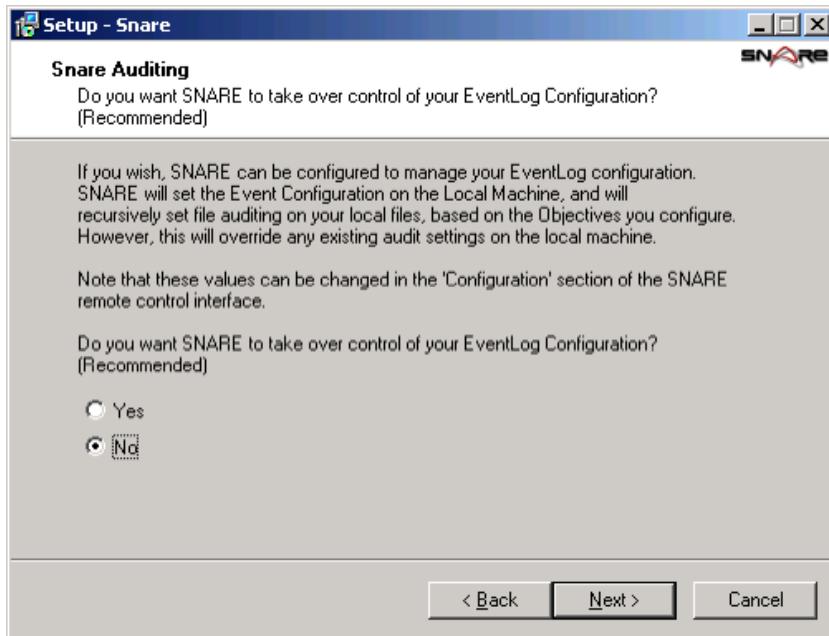
- h** Check the box at the bottom labeled **Apply these auditing entries to objects and/or containers within this container only**.
- i** Check at least the Successful and Failed columns for the rows **Read Attributes**, **Delete Subfolders and Files**, **Delete**, **Read Permissions**.



- j** Click **OK**.

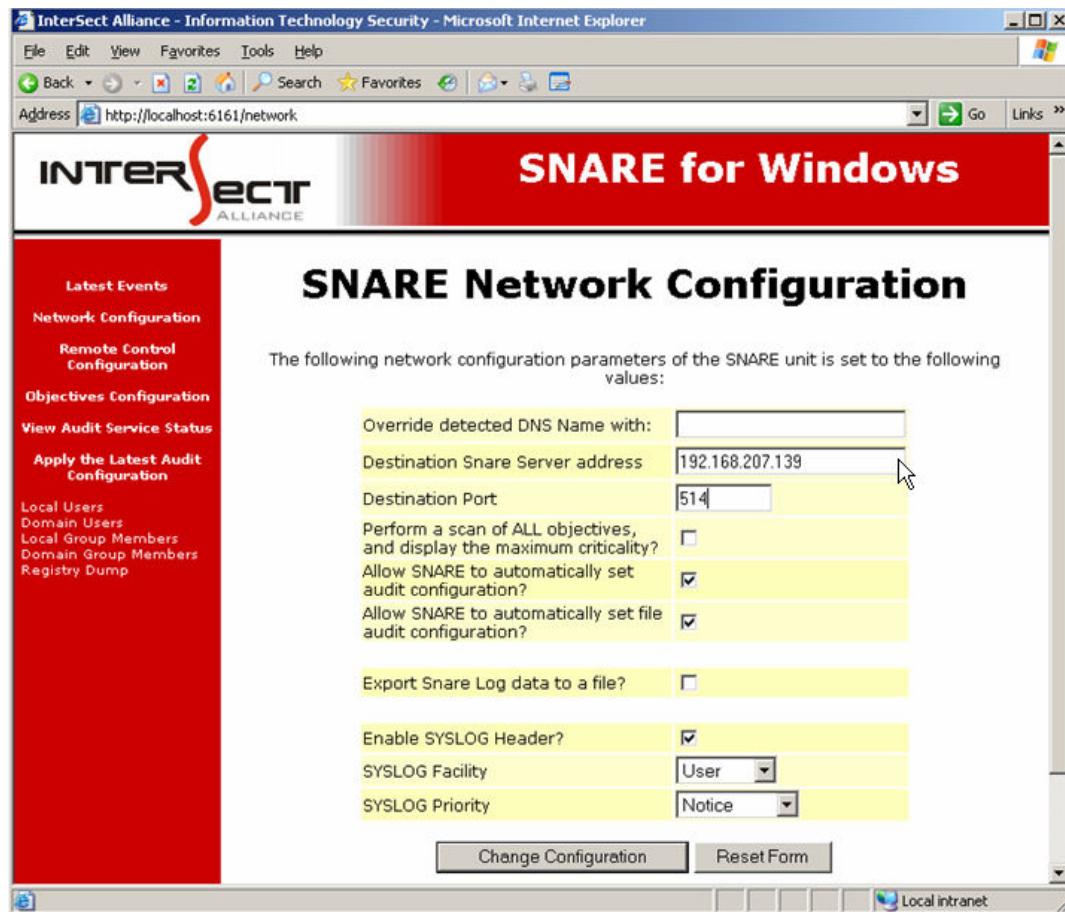
Configuring Snare Agent

- 1 Download and install the open source Snare Windows agent from Intersect Alliance at <http://www.intersectalliance.com/projects/SnareWindows/index.html#Download> and follow installation instructions.
- 2 During the installation, when prompted for the Snare Auditing configuration, select NO when asked "Do you want SNARE to take over control of your EventLog Configuration?"



- 3 Log into the local administration page.
- 4 Click on Network Configuration and configure the following settings:
 - a Set the Destination Snare Server to the IP address of your SenSage AP syslog-ng server.
 - b Set the Destination Port to 514 .

- c Leave the other settings with their default values.



5 Click **Change Configuration** to save the settings.

SEN\$AGE AP COLLECTOR SYSLOG-NG SETUP

To configure your log adapter, make the following configuration change on the host running the Sen\$age AP Collector:

- 1 Edit `/etc/syslog-ng.conf` on the host running the Sen\$age AP Collector, configuring a filter statement, a destination statement, and a log statement as shown below:

■ Filter statement:

```
filter f_win_event_security { match("MSWinEventLog.[0-9].Security"); };
```

■ Destination statement:

```
destination d_win_security_event {
    file("<HawkEye AP Home>/incoming/syslog-ng/
microsoft_windows_securityEvent_snare/
microsoft_windows_securityEvent_snare.log"
template
    ("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSG\n")
```

```
template_escape(no) ) ;
};
```

NOTE: Change the path and file name of the “file” argument to match the location of your log file.

■ Log statement:

```
log {
source(s_network_std);
filter(f_win_event_security);
destination(d_win_security_event);
flags(final);
};
```

2 Restart the syslog-ng daemon.

3 Edit the SenSage AP Collector config.xml with sections for logqueue, retriever, loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

4 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

CHAPTER 46

microsoft_windows2010_appEvent_SensageRetriever (for Windows 7, 8, 10)

Log Adapter Component	Details
Name	microsoft_windows2010_appEvent_SensageRetriever
Version	1.0.0
Source Vendor	Microsoft
Source Product	Windows
Source Component	Application Events
Source Version	Windows 7, 8, and 10
Source Host OS	Windows 7, 8, and 10
Transport Mechanism	SenSage AP Windows Retriever
PTL Filename	microsoft_windows2010_appEvent_sensageRetriever.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none">• application_microsoft_windows10_appEvent_sensageRetriever• parsedData_microsoft_windows10_appEvent_sensageRetriever• unparsedData_microsoft_windows10_appEvent_sensageRetriever
Look-up file	None
Scripts	None
Source-Specific Reports	<ul style="list-style-type: none">• Windows Application Events
Event Types	<ul style="list-style-type: none">• None

SETTING UP THE MICROSOFT_WINDOWS2010_APPEVENT_SENSAGERETRIEVER LOG ADAPTER

To configure Microsoft_Windows10_AppEvent_sensageRetriever log, refer to the following:
microsoft_windows_securityEvent_sensageRetriever in [Chapter 46: “Source System Setup”, on page 580](#).

CHAPTER 47

microsoft_windows2010_sysEvents_sensageRetriever

SYSTEM INFORMATION

Log Adapter Component	Details
Name	microsoft_windows2010 sysEvent SensageRetriever
Version	1.0
Source Vendor	Microsoft
Source Product	Windows
Source Component	Windows Systems Events
Source Version	Windows 7, 8, and 10
Source Host OS	Windows 7, 8, and 10
Transport Mechanism	SenSage AP Windows Retriever
PTL Filename	microsoft windows2010 sysEvent_sensageRetriever.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none">• application__microsoft_windows10_sysEvent_sensageRetriever• parsedData__microsoft_windows10_sysEvent_sensageRetriever• unparsedData__microsoft_windows10_sysEvent_sensageRetriever
Look-up file	None
Scripts	None
Source-Specific Reports	<ul style="list-style-type: none">• “Windows System Events”, on page 234
Event Types	<ul style="list-style-type: none">• None

SETTING UP THE MICROSOFT_WINDOWS2010_SYSEVENT_LOG ADAPTER

To configure Microsoft_Windows10_sysEvent_sensageRetriever log, refer to the following:
microsoft_windows_securityEvent_sensageRetriever in [Chapter 47: “Source System Setup”, on page 580](#).

CHAPTER 48

oracle_adump

SUMMARY INFORMATION

Log Adapter Component	Details
Name	oracle_adump
Version	1.0.1
Source Vendor	Oracle
Source Product	Database
Source Component	Sys Audit (audit files)
Source Version	9, 10, 11, 12
Source Host OS	Linux/Windows
Transport Mechanism	SFTP
PTL Filename	oracle_adump.ptl
Parsing Rule	N/A
Alerting Rule	N/A
Connector Views	<ul style="list-style-type: none">• investigation__oracle_adump• parsedData__oracle_adump• privilegedCommand__oracle_adump• startStop__oracle_adump• database_ddl__oracle_adump• database_dml__oracle_adump• accountAdditionAndDeletion__oracle_adump• networkDeviceConnection__oracle_adump• unparsedData__oracle_adump• userLogin__oracle_adump
Look-up file	Not Required
Scripts	oracle_adump.preproc oracle_adump_tar.preproc
Source-Specific Reports	None

Log Adapter Component	Details
Event Types	<ul style="list-style-type: none"> • investigation • parsedData • privilegedCommand • startStop • database_ddl • database_dml • accountAdditionAndDeletion • networkDeviceConnection • unparsedData • userLogin

SETTING UP ORACLE_ADUMP LOG ADAPTER

This section describes how to configure the oracle_adump log adapter. The following steps are required:

- “Source System Setup”, next

Source System Setup

- 1 Connect to Oracle as SYS
- 2 Execute SHOW parameter audit
- 3 Make sure that following parameters are set as below:

```
audit_trail=OS
audit_syslog_level=''
audit_sys_operations=TRUE (if you also want to audit actions performed by SYS user)
```

- 4 Modify settings if needed as described above by executing:

```
ALTER system SET audit_trail=os scope=spfile;
ALTER system SET audit_syslog_level='' scope=spfile;
ALTER system SET audit_sys_operations=TRUE scope=spfile;
```

- 5 Shut down database.

```
shutdown immediate
```

- 6 Start up database.

```
startup
```

CHAPTER 49

oracle_adump_syslogng**SUMMARY INFORMATION**

Log Adapter Component	Details
Name	oracle_adump_syslogng
Version	1.1.0
Source Vendor	Oracle
Source Product	Database
Source Component	Sys Audit (audit files)
Source Version	9, 10, 11, 12
Source Host OS	Linux/Windows
Transport Mechanism	Syslog-ng
PTL Filename	oracle_adump_syslogng.ptl
Parsing Rule	N/A
Alerting Rule	N/A
Connector Views	<ul style="list-style-type: none"> • accountAdditionAndDeletion__oracle_adump_syslogng • database_ddl__oracle_adump_syslogng • database_dml__oracle_adump_syslogng • investigation__oracle_adump_syslogng • networkDeviceConnection__oracle_adump_syslogng • parsedData__oracle_adump_syslogng • privilegedCommand__oracle_adump_syslogng • startStop__oracle_adump_syslogng • unparsedData__oracle_adump_syslogng • userLogin__oracle_adump_syslogng
Look-up file	Not required
Scripts	N/A
Source-Specific Reports	None

Log Adapter Component	Details
Event Types	<ul style="list-style-type: none"> • accountAdditionAndDeletion • database_ddl • database_dml • investigation • networkDeviceConnection • parsedData • privilegedCommand • startStop • unparsedData • userLogin

SETTING UP ORACLE_ADUMP_SYSLOGNG LOG ADAPTER

This section describes how to configure the oracle_adump log adapter. The following steps are required:

- “Source System Setup”, next
- “SenSage AP Collector Configuration”, on page 619

Source System Setup

- 1 Connect to Oracle as SYS.
- 2 Execute SHOW parameter audit.
- 3 Make sure that following parameters are set as below:

```
audit_trail=OS
audit_syslog_level='user.notice'
audit_sys_operations=TRUE (if you also want to audit actions performed by SYS
user)
```

- 4 Modify settings if needed as described above by executing:

```
ALTER system SET audit_trail=os scope=spfile;
ALTER system SET audit_syslog_level='' scope=spfile;
ALTER system SET audit_sys_operations=TRUE scope=spfile;
```

- 5 Shut down database.

```
shutdown immediate
```

- 6 Start up database.

```
startup
```

SenSage AP Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open the syslog-ng configuration file <SenSage AP Home>/etc/syslog-ng/syslog-ng.conf on the host running the SenSage AP Collector.
- 2 Make sure the following destination filter and log statement are configured as shown below:

```
destination d_oracle_adump_syslogng {
    file("<SenSage AP Home>/incoming/syslog-ng/oracle_adump_syslogng/
oracle_adump_syslogng.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};

filter d_oracle_adump_syslogng {
    message('Oracle Audit');
};

log {
    source(s_network_std); source(s_network_tls);
    filter(d_adump_syslogng);
    destination(d_oracle_adump_syslogng);
    flags(final);
};
```

- 3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

- 4 Edit the SenSage AP Collector config.xml with sections for logqueue, retriever, and loader. For more information, [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.
- 5 (Optional). Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

SAMPLE CONFIGURATION FILES

The following section contains these sample configuration files:

- Collector configuration (config.xml)

Collector Configuration (config.xml)

```
<Retriever type='filesystem' enabled='1' name='r_oracle_adump_syslogng'
deleteOriginal='1' method='copy'>
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_oracle_adump_syslogng</LogQueue>
<SourceDir>/opt/hexis/incoming/syslog-ng/oracle_adump_syslogng/</
SourceDir>
<Plugin name='Default'>
<File ai='ignore' id='1'>.*</File>
<File ai='accept' id='2'>.*\aud$</File>
```

```
</Plugin>
</Retriever>

<LogQueue path='queue/oracle_adump_syslogng' minMBFree='100'
name='q_oracle_adump_syslogng' encoding='UTF-8'>

<Loader enabled='1' name='l_oracle_adump_syslogng'>
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_oracle_adump_syslogng</LogQueue>
<SLSInstance>sls.host.com:8072</SLSInstance>
<SLSUser>administrator</SLSUser>
<SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/my_sls_8072/
shared_secret.asc</SLSSharedKey>
<PTL table='oracle_adump_syslogng' namespace='analytics' type='file'>
<Location>/opt/hexis/hawkeye-ap/analytics/adapters/
oracle_adump_syslogng/oracle_adump_syslogng.ptl</Location>
<LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
</PTL>
</Loader>
```

CHAPTER 50

oracle_database_fga_sensageRetriever

Log Adapter Component	Details
Name	oracle_database_fga_sensageRetriever
Log Adapter Version	1.0.0
Source Vendor	Oracle
Source Product	Database
Source Component	DBA_FGA_AUDIT_TRAIL view
Source Version	10, 11, and 12
Source Host OS	Red Hat 5.5
Transport Mechanism	SenSage AP Retriever
PTL Filename	oracle_database_fga_sensageRetriever.ptl
Parsing Rule	Not required.
Alerting Rule	Not required.
Connector Views	<ul style="list-style-type: none"> • investigation__oracle_database_fga_sensageRetriever
Look-up file	Lookup file for Oracle Environment (map DBID to DB Host and DB Name)
Scripts	SenSage AP Retriever
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none"> • “Audit Event”, on page 109

**SETTING UP THE ORACLE_DATABASE_FGA
SENSAGERETRIEVER**

This document describe how to configure the oracle_database_fga_sensageRetriever log adapter. The following steps are required:

- “Source System Setup”, next
- “Configuring the Agentless Retriever”, on page 623
- “SenSage AP Collector Setup”, on page 623

SOURCE SYSTEM SETUP

Fine Grained Audit

Fine grained audit brings more flexibility than the detailed audit. You can specify columns to audit as well as define a condition for auditing. If the result of a specific request matches the audit condition, then a trace is generated in the audit trail with the number of lines that match the condition.

The FGA audit handles the following statements: SELECT, UPDATE, DELETE, and MERGE. A procedure can be executed if a statement matches the audit condition, audit columns, and the type of statement to audit.

The FGA audit feature is enabled using the DBMS_FGA package through the use of the DBMS_FGA.ADD_POLICY procedure, as noted below:

```
CONNECT
DBMS_FGA_ADD_POLICY
object_schema => '...',
object_name => "...",
policy_name => '...',
audit_condition => 'employee_id > 10',
audit_column => 'EMP_ID, SALARY',
handler_schema => 'audit_schema',
handler_module => 'log_audit_proc',
enable => TRUE,
statement_types => 'SELECT,INSERT,UPDATE,DELETE'
);
```

The FGA policy cannot be deleted using DBMS_FGA_DROP_POLICY. Also, the FGA policy cannot be enabled/disabled using the following: DBMS_FGA.ENABLE_POLICY and DBMS_FGA.DISABLE_POLICY.

To enable the SYSDBA users audit, you must change the value of the audit_sys_operations database property to true.

```
ALTER SYSTEM SET
audit_sys_operations=TRUE
COMMENT='Begin auditing SYS'
SCOPE=SPFILE;
```

Then, restart the database instance.

```
SHUTDOWN IMMEDIATE
STARTUP
```

CONFIGURING THE AGENTLESS RETRIEVER

This procedure below describes how to configure the agentless version of the SenSage AP Retriever.

To configure an agentless retriever:

1 Copy the `agentless_oracle_database_fga_sensageRetriever/agentless_oracle_database_fga_sensageRetriever.prop`<`Sensage_Home`>/latest/etc/collector/

2 Change the directory to Collector config. The default location is:

`<Sensage_Home>/latest/etc/collector/`

3 Update the `agentless_oracle_database_fga_sensageRetriever.prop` file with correct values:

```
reader_NAME=oracleauditlog,HOST,USER,PASSWORD,SERVICENAME,PORT,SQL_STRING_NAME
,,orapw,10
```

where :

```
HOST - Oracle Hostname,
USER - Oracle username
PASSWORD - Oracle Password
SERVICENAME - Oracle SID
PORT - Oracle Port
```

For more info please refer to `agentless_oracle_database_fga_sensageRetriever.prop`.

SENSAGE AP COLLECTOR SETUP

To set up SenSage AP Collector:

1 Edit the `config.xml` file to name and define the retriever and point to its properties file.

2 Restart the Collector.

3 Examine the SenSage AP Retriever log file for errors. The default location is:

`<Sensage_Home>/latest/var/log/collector/windowsretriever.log`

oracle_database_sysaudit_sensageRetriever

SUMMARY INFORMATION

Log Adapter Component	Details
Name	oracle_database_sysaudit_sensageRetriever
Log Adapter Version	1.0.0
Source Vendor	Oracle
Source Product	Database
Source Component	DBA_AUDIT_TRAIL view
Source Version	10, 11, and 12
Source Host OS	Red Hat 5.5
Transport Mechanism	HawkEye Retriever
PTL Filename	oracle_database_sysaudit_sensageRetriever.ptl
Parsing Rule	Not required.
Alerting Rule	Not required
Connector Views	<ul style="list-style-type: none"> • userLogin_oracle_database_sysaudit_sensageRetriever.sql • privilegedCommand_oracle_database_sysaudit_sensageRetriever.sql • passwordChangeAndReset_oracle_database_sysaudit_sensageRetriever.sql • accountAdditionAndDeletion_oracle_database_sysaudit_sensageRetriever.sql • investigation_oracle_database_sysaudit_sensageRetriever.sql
Look-up file	Lookup file for Oracle Environment (map DBID to DB Host and DB Name) Create a lookup file of privileged commands.
Scripts	Using HawkEye Retriever
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none"> • accountAdditionAndDeletioninvestigation • passwordChangeAndResetprivilegedCommanduserLogin

SETTING UP THE ORACLE_DATABASE_SYSAUDIT SENSAGERETRIEVER

This document describe how to configure the oracle_database_sysaudit_sensageRetriever log

adapter. The following steps are required:

- “Configuring the AgentLess Retriever”, next
- “SenSage AP Collector Setup”, on page 626

CONFIGURING THE AGENTLESS RETRIEVER

The procedure below documents how to configure the agentless version of the SenSage AP Retriever. To configure an agentless retriever:

- 1 Copy the `agentless_oracle_database_sysaudit_sensageRetriever.prop` which comes with the adapter to the Collector Config folder:**

```
cp <SenSage AP Home>/analytics/adapters/  
agentless_oracle_database_sysaudit_sensageRetriever/  
agentless_oracle_database_sysaudit_sensageRetriever.prop <SenSage AP Home>/  
etc/collector/
```

- 2 Change the directory to Collector config. The default location is:**

```
<SenSage AP Home>/etc/collector/
```

- 3 Update the `agentless_oracle_database_sysaudit_sensageRetriever.prop` file with correct values:**

```
reader_NAME=oracleauditlog,HOST,USER,PASSWORD,SERVICENAME,PORT,SQL_STRING_NAME  
,,orapw,10  
where:  
HOST - Oracle Hostname  
USER - Oracle username  
PASSWORD - Oracle Password  
SERVICENAME - Oracle SID  
PORT - Oracle Port
```

For more information please refer to
`agentless_oracle_database_sysaudit_sensageRetriever.prop`

SENSAGE AP COLLECTOR SETUP

- 1 Edit the `config.xml` file to name and define the retriever and point to its properties file.**

- 2 Restart the Collector.**

- 3 Examine the SenSage AP Retriever log file for errors. The default location is:**

```
<SenSage AP Home>/var/log/collector/windowretrievers.log
```

CHAPTER 52

oracle_fga_xml_batch

SUMMARY INFORMATION

Log Adapter Component	Details
Name	oracle_fga_xml_batch
Version	1.0.0
Source Vendor	Oracle
Source Product	Database
Source Component	Sys Audit (xml files) FGA Sys Audit (xml files)
Source Version	9, 10, 11, 12
Source Host OS	Linux/Windows
Transport Mechanism	SFTP
PTL Filename	oracle_fga_xml_batch.ptl
Parsing Rule	N/A
Alerting Rule	N/A
Connector Views	<ul style="list-style-type: none">• database_ddl__oracle_fga_xml_batch• database_dml__oracle_fga_xml_batch• investigation__oracle_fga_xml_batch• parsedData__oracle_fga_xml_batch• unparsedData__oracle_fga_xml_batch
Look-up file	Not required
Scripts	oracle_fga_xml_batch.preproc
Source-Specific Reports	N/A
Event Types	<ul style="list-style-type: none">• database_ddl• database_dml• investigation• parsedData• unparsedData

SETTING UP ORACLE_FGA_XML_BATCH LOG ADAPTER

This section describes how to configure the oracle_fga_xml_batch log adapter. The following steps are required to set up the Source System.

[“Source System Setup”, next](#)

[“Sample Configuration Files”, on page 629](#)

Source System Setup

Sys Audit

1 Connect to Oracle as SYS.

2 execute SHOW parameter audit.

3 Make sure that following parameters are set as below:

```
audit_trail=OS
audit_syslog_level=''
audit_sys_operations=TRUE (if you also want to audit actions performed by SYS
user)
```

4 Modify settings if needed as described above by executing:

```
ALTER system SET audit_trail=os scope=spfile;
ALTER system SET audit_syslog_level='' scope=spfile;
ALTER system SET audit_sys_operations=TRUE scope=spfile;
```

5 Shut down database.

```
shutdown immediate
```

6 Start up database.

```
startup
```

FGA Sys Audit

1. Connect to Oracle as SYS.

2. Create audit Policy.

```
begin
  dbms_fga.add_policy(
    object_schema  => 'sensage',
    object_name    => 'test_xml',
    policy_name   => 'test_xml',
    handler_schema => null,
    audit_trail    => DBMS_FGA.XML + DBMS_FGA.EXTENDED,
    handler module => null
    enable => true
  );
end
/
```

where

- object_schema - the user name you want to be audited
- object_name - the table name you want to be audited

- policy_name - the desired policy name

Sample Configuration Files

The following section contains these sample configuration files:

- Collector configuration (config.xml)

Collector Configuration (config.xml)

```

<Retriever type='sftp' enabled='1' name='r_oracle_fga_xml_batch'
deleteOriginal='1' method='copy'>
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_oracle_fga_xml_batch</LogQueue>
    <SourceHost>oracle.host.com</SourceHost>
    <SourceUser>user</SourceUser>
    <SourceDir>/location/where/xml/files/are/stored/</SourceDir>
    <Preprocess type='file' id='1' match='.*'>/opt/hexis/hawkeye-ap/
analytics/adapters/oracle_fga_xml_batch/oracle_fga_xml_batch.preproc</
Preprocess>
    <Plugin name='Default'>
        <File ai='ignore' id='1'>.*</File>
        <File ai='accept' id='2'>.*\aud$</File>
    </Plugin>
</Retriever>

<LogQueue path='queue/oracle_fga_xml_batch' minMBFree='100'
name='q_oracle_fga_xml_batch' encoding='UTF-8'>

<Loader enabled='1' name='l_oracle_fga_xml_batch'>
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_oracle_fga_xml_batch</LogQueue>
    <SLSInstance>sls.host.com:8072</SLSInstance>
    <SLSUser>administrator</SLSUser>
    <SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/my_sls_8072/
shared_secret.asc</SLSSharedKey>
    <PTL table='oracle_fga_xml_batch' namespace='analytics' type='file'>
        <Location>/opt/hexis/hawkeye-ap/analytics/adapters/
oracle_fga_xml_batch/oracle_fga_xml_batch.ptl</Location>
        <LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
    </PTL>
</Loader>
```


CHAPTER 53

sap_aud_sftp

SYSTEM INFORMATION

Log Adapter Component	Details
Name	sap_aud_sftp
Log Adapter Version	1.0.0
Source Vendor	SAP
Source Product	AUD
Source Component	None
Source Version	7.2
Source Host OS	None
Transport Mechanism	SFTP
PTL Filename	sap_aud_sftp.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none">investigation_sap_aud_sftp
Look-up file	Not required
Scripts	<ul style="list-style-type: none">sap_aud_sftp.preproc (preprocessor)
Source-Specific Reports	<ul style="list-style-type: none">"SAP Security Audit - Program Summary", on page 441"SAP Security Audit - Terminal Summary", on page 442"SAP Security Audit - Top 10 Records", on page 443"SAP Security Audit - User Summary", on page 444
Event Types	<ul style="list-style-type: none">"Audit Event", on page 109

SETTING UP THE SAP_AUD_SFTP LOG ADAPTER

This document describe how to configure the sap_aud_sftp log adapter. The following steps are required:

- "Configure Source System", on page 632
- "SenSage AP Collector Setup", on page 632

CONFIGURE SOURCE SYSTEM

Configure your SAP system to write event information to the local file system using the SM-20 screen. Files must then be transported to the SenSage AP Collector. If you need additional assistance configuring your source device please contact Professional Services.

SEN SAGE AP COLLECTOR SETUP

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Configure the SenSage AP Collector to pull the file from the target host using SFTP.
- 2 Open the Collector config file <HawkEye AP Home>/etc/collector/adapters/sap_aud_sftp/config.xml, find the `r_sap_aud_sftp` retriever section, and specify **SourceHost**, **SourceUser**, and **SourceDir** for the target system.
- 3 Configure the SenSage AP Collector to delete te log file after loading by setting the `deleteOriginal` attribute to `#1#` inside the `<retriever>` tab. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.
- 4 Restart the Collector.

CHAPTER 54

sun_bsm_sftp

SYSTEM INFORMATION

Log Adapter Component	Details
Name	sun_bsm_sftp
Version	1.1.5
Source Vendor	Sun Microsystems
Source Product	Solaris Basic Security Module
Source Component	None
Source Version	8 - 10
Source Host OS	<ul style="list-style-type: none">• SunOS_5_8;• SunOS_5_9;• SunOS_5_10
Transport Mechanism	sftp
PTL Filename	sun_bsm_sftp.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none">• investigation_sun_bsm_sftp.sql• privilegedCommand_bsm_sun_bsm_sftp.sql• startStop_bsm_sun_bsm_sftp.sql
Look-up file	None
Scripts	None
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none">• “Audit Event”, on page 109• “Privileged Commands”, on page 129• “Privileged Commands: BSM”, on page 130• “System Startup and Shutdown”, on page 136• “Startup and Shutdown: BSM”, on page 138

SETTING UP THE SUN_BSM_SFTP LOG ADAPTER

This document describe how to configure the sun_bsm_sftp log adapter. The following steps are required:

- “Source System syslog Setup”, next
- “SenSage AP Collector Setup”, on page 634

SOURCE SYSTEM SYSLOG SETUP

To configure the source system, make the following configuration changes on your log source host(s):

1 Extract the `ss_bsmextract` korn shell script from the tar file containing your `sun_bsm_sftp` log adapter and copy it to each source system host. The `ss_bsmextract` script converts the native, binary format of BSM log files into a text file.

2 Execute the file as follows:

```
ss_bsmextract INPUT_FILE [OUTPUT_DIR]
```

Where `INPUT_FILE`: is the name of the binary bsm data file contained in `/var/audit` and `OUTPUT_DIR` is the name of the directory where you want to place the converted file.

IMPORTANT: If the `/var/audit` directory fills, the system may halt.

SENSAGE AP COLLECTOR SETUP

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Configure the SenSage AP Collector to pull the file from the Solaris host using SFTP.
- 2 Configure the SenSage AP Collector to delete the log file after loading by setting the `delete Original` attribute to "1" inside the `<retriever>` tag. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

symantec_endpoint_syslogng

SUMMARY INFORMATION

Log Adapter Component	Details
Name	symantec_endpoint_syslogng
Version	1.0.2
Source Vendor	Symantec
Source Product	Symantec Endpoint Protection
Source Component	N/A
Source Version	12.x
Source Host OS	Cross-platform
Transport Mechanism	syslog-ng
PTL Filename	symantec_endpoint_syslogng.ptl
Parsing Rule	symantec_endpoint_syslogng.rule
Alerting Rule	SymantecEventMatch.template.rule.xml
Connector Views	<ul style="list-style-type: none"> • alert_symantec_endpoint_syslogng • malware_symantec_endpoint_syslogng • parsedData_symantec_endpoint_syslogng • unparsedData_symantec_endpoint_syslogng.sql • vulnerability_symantec_endpoint_syslogng.sql
Look-up file	Not required
Scripts	Not required
Source-Specific Reports	None
Event Types	None

SETTING UP SYMANTEC_ENDPOINT_SYSLOGNG LOG ADAPTER

This section describes how to configure the symantec_endpoint_syslogng log adapter. The following steps are required:

- “Source System Setup”, next
- “HawkEye Collector Configuration”, on page 590

Source System Setup

Refer to the documentation for the Source Product.

SenSage AP Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open the syslog-ng configuration file <SenSage AP Home>/etc/syslog-ng/syslog-ng.conf on the host running the SenSage AP Collector.
- 2 Make sure the following destination filter and log statement are configured as shown below:

```
destination d_symantec_endpoint_syslogng {  
    file("<SenSage AP Home>/incoming/syslog-ng/symantec_endpoint_syslogng/  
symantec_endpoint_syslogng.log"  
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST  
$MSGHDR$MSG\n")  
        template_escape(no) );  
};  
  
filter f_symantec_endpoint_syslogng {  
    message(" SymantecServer ");  
};  
  
log {  
    source(s_network_std); source(s_network_tls);  
    filter(f_symantec_endpoint_syslogng);  
    destination(d_symantec_endpoint_syslogng);  
    flags(final);  
};
```

- 3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```
- 4 Edit the SenSage AP Collector **config.xml** with sections for logqueue, retriever, and loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guidee*.
- 5 (Optional). Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

SAMPLE CONFIGURATION FILES

The following section contains these sample configuration files:

- Collector configuration (**config.xml**)
- Syslog-NG Configuration Entries (**syslog-ng.conf**)

Collector Configuration (**config.xml**)

```
<LogQueue encoding="UTF-8" minMBFree="100" name="q_symantec_endpoint_syslogng"  
path="queue/symantec_endpoint_syslogng"/>
```

```

<Retriever deleteOriginal="1" enabled="1" method="copy"
name="r_symantec_endpoint_syslogng" type="filesystem">
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_symantec_endpoint_syslogng</LogQueue>
    <SourceDir>/opt/hexis/incoming/syslog-ng/symantec_endpoint_syslogng</
SourceDir>
    <Plugin name="Default">
        <File ai="ignore" id="1">.*</File>
        <File ai="accept" id="2">.*\.loadme$</File>
    </Plugin>
</Retriever>

<Loader enabled="1" name="l_symantec_endpoint_syslogng">
    <RunOnHost>localhost</RunOnHost>
    <LogQueue>q_symantec_endpoint_syslogng</LogQueue>
    <SLSInstance>analytics.example.com:8072</SLSInstance>
    <SLSUser>administrator</SLSUser>
    <SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>
    <PTL namespace="analytics" table="symantec_endpoint_syslogng" type="file">
        <Location>/opt/hexis/hawkeye-ap/analytics/adapters/
symantec_endpoint_syslogng/symantec_endpoint_syslogng.ptl</Location>
        <LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
    </PTL>
</Loader>
```

Syslog-NG Configuration Entries (syslog-NG.conf)

```

destination d_symantec_endpoint_syslogng {
    file("/opt/hexis/incoming/syslog-ng/symantec_endpoint_syslogng/
symantec_endpoint_syslogng.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};

filter f_symantec_endpoint_syslogng {
    message(" SymantecServer ");
};

log {
    source(s_network_std); source(s_network_tls);
    filter(f_symantec_endpoint_syslogng);
    destination(d_symantec_endpoint_syslogng);
    flags(final);
};
```


CHAPTER 56

syslogng_catchall_syslogng

SYSTEM INFORMATION

Log Adapter Component	Details
Name	syslogng_catchall_syslogng
Version	1.0
Source Vendor	n/a
Source Product	n/a
Source Component	n/a
Source Version	n/a
Source Host OS	<ul style="list-style-type: none">• AIX_5.1-5.3• HPUX_11• Suse_ES10• RedHat_ES3.0• Solaris_2.6-9
Transport Mechanism	syslog- <i>ng</i>
PTL Filename	syslogng_catchall_syslogng.ptl
Parsing Rule	syslogng_catchall_syslogng.rule
Alerting Rule	SyslogSourceHealth.alert.rule.xml
Connector Views	<ul style="list-style-type: none">• investigation__syslogng_catchall_syslogng
Look-up file	None
Scripts	None
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none">• “Audit Event”, on page 109

SETTING UP THE SYSLOGNG_CATCHALL_SYSLOGNG LOG ADAPTER

The syslogng_catchall_syslogng log adapter is a “catch all” log adapter that processes messages not processed by the syslog-*ng* filter statement of other log adapters. Because the type of data collected by this adapter is different for each message, there are no reports provided.

This document describes how to configure the syslogng_catchall_syslogng log adapter. The following steps are required:

- “[Source System syslog Setup](#)”, next

SOURCE SYSTEM SYSLOG SETUP

This section describes configurations you make on your log source host. Instructions are provided for the following Unix-based operating systems:

- “[Linux](#)”, next
- “[HP-UX](#)”, on page 640

Linux

To configure your source system, make the following configuration changes on your log source host:

- 1 Log in to the Linux server using a privileged account.
- 2 Open the file `/etc/syslog.conf` in a text editor.
- 3 Add the following line:

```
*.debug @###.###.###.###
```

where `###.###.###.###` is the IP address of the host running the Sensage AP collector.

- 4 Save and close the file.
- 5 Restart the syslog daemon:

```
kill -HUP `cat /var/run/syslogd.pid`
```

HP-UX

To configure your source system, make the following configuration changes on your log source host:

- 1 Log in to the HP-UX server using a privileged account.
- 2 Open the file `/etc/syslog.conf` in a text editor.
- 3 Add the following lines:

```
*.info @###.###.###.###  
*.alert;*.emerg @###.###.###.###  
*.crit;*.err;*.notice @###.###.###.###
```

Where `###.###.###.###` is the IP address of the host running the Sensage AP collector.

- 4 Save and close the file.

5 Restart the syslog daemon:

```
kill -HUP `cat /var/run/syslog.pid`
```

SENSAGE AP COLLECTOR SYSLOG-NG SETUP

To configure your log adapter, make the following configuration change on the host running the Sensage AP Collector:

- 1 Edit `/etc/syslog-nginx.conf` on the host running the Sensage AP Collector, configuring a destination statement and a log statement as shown below:

■ Destination statement:

```
destination d_nix_ftpd {
    file("<HawkEye AP Home>/incoming/syslog-nginx/syslogng_catchall_syslogng/
syslogng_catchall_syslogng.log"
    template
    ("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST $MSG\n")
    template_escape(no) );
};
```

NOTE: Change the path and file name of the “file” argument to match the location of your log file. This argument must match the location of your retriever as specified in the Collector config.xml.

■ Log statement:

```
log {
    source(s_network_std);
    filter(f_nix_ftpd);
    destination(d_nix_ftpd);
    flags(fallback);
};
```

- 2 Restart the syslog-nginx daemon.

3 Edit the Sensage AP Collector config.xml with sections for logqueue, retriever, loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

4 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

tipping_point_syslogng

SYSTEM INFORMATION

Log Adapter Component	Details
Name	tipping_point_syslogng
Version	1.0
Source Vendor	Tipping Point
Source Product	Tipping Point
Source Component	IPS 1200 IPS 2400E
Source Version	2.5.4
Source Host OS	n/s
Transport Mechanism	syslog-ng
PTL Filename	tipping_point_syslogng.ptl
Parsing Rule	tipping_point_syslogng.rule
Alerting Rule Template	HP Tipping Point IPS Global Substring Match Rule
Connector Views	<ul style="list-style-type: none"> • investigation_tipping_point_syslogng.sql
Look-up file	None
Scripts	None
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none"> • “Audit Event”, on page 109

CHAPTER 54

unix_ftpd_syslogng

SYSTEM INFORMATION

Log Adapter Component	Details
Name	unix_ftpd_syslogng
Version	1.1.1
Source Vendor	Unix
Source Product	FTPD Daemon
Source Component	None
Source Version	None
Source Host OS	<ul style="list-style-type: none">• AIX_5.1-5.3• HPUX_11• Suse_ES10• RedHat_ES3.0• Solaris_2.6-9
Transport Mechanism	syslog- <i>ng</i>
PTL Filename	unix_ftpd_syslogng.ptl
Parsing Rule	unix_login_syslogng.rule
Alerting Rule Template	Unix ftpd Substring Match Rule
Connector Views	<ul style="list-style-type: none">• investigation_unix_ftpd_syslogng.sql• userLogin_unix_unix_ftpd_syslogng.sql
Look-up file	None
Scripts	None
Source-Specific Reports	<ul style="list-style-type: none">• "Unix or Linux Login Details", on page 254
Event Types	<ul style="list-style-type: none">• "Audit Event", on page 109• "Unparsed Data", on page 139• "User Logins: Linux/Unix", on page 147

SETTING UP THE UNIX_FTPD_SYSLOGNG LOG ADAPTER

This document describe how to configure the log adapter for unix_ftpd_syslogng. The following steps are required:

- “Source System syslog Setup”, next
- “SenSage AP Collector syslog-ng Setup”, on page 647

SOURCE SYSTEM SYSLOG SETUP

This section describes configurations you make on your log source host. Instructions are provided for the following Unix-based operating systems:

- “Linux”, next
- “HP-UX”, on page 646

Linux

To configure your source system, make the following configuration changes on your log source host:

1 Log in to the Linux server using a privileged account.

2 Open the file `/etc/syslog.conf` in a text editor.

3 Add the following line:

```
*.debug @###.###.###.###
```

where `###.###.###.###` is the IP address of the host running the SenSage AP collector.

4 Save and close the file.

5 Restart the syslog daemon:

```
kill -HUP `cat /var/run/syslogd.pid`
```

HP-UX

To configure your source system, make the following configuration changes on your log source host:

1 Log in to the HP-UX server using a privileged account.

2 Open the file `/etc/syslog.conf` in a text editor.

3 Add the following lines:

```
*.info @###.###.###.###  
*.alert;*.emerg @###.###.###.###  
*.crit;*.err;*.notice @###.###.###.###
```

Where `###.###.###.###` is the IP address of the host running the SenSage AP Collector.

4 Save and close the file.

5 Restart the syslog daemon:

```
kill -HUP `cat /var/run/syslog.pid`
```

SEN\$AGE AP COLLECTOR SYSLOG-NG SETUP

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Edit `/etc/syslog-ng.conf` on the host running the SenSage AP Collector, configuring a filter statement, a destination statement, and a log statement as shown below:

- Filter statement:

```
filter f_nix_ftpd {facility(daemon) and program(ftpd);};
```

- Destination statement:

```
destination d_nix_ftpd {
    file("CLW Event Processing Language/incoming/syslog-ng/unix_ftpd_syslogng/
        unix_ftpd_syslogng.log"
    template
        ("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST $MSG\n")
    template_escape(no) );
};
```

NOTE: Change the path and file name of the “file” argument to match the location of your log file. This argument must match the location of your retriever as specified in the Collector config.xml.

- Log statement:

```
log {
    source(s_network_std);
    filter(f_nix_ftpd);
    destination(d_nix_ftpd);
    flags(final);
};
```

- 2 Restart the syslog-ng daemon.

- 3 Edit the SenSage AP Collector config.xml with sections for logqueue, retriever, loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

- 4 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

CHAPTER 55

unix_login_syslogng

SYSTEM INFORMATION

Log Adapter Component	Details
Name	unix_login_syslogng
Version	1.0.0
Source Vendor	Unix
Source Product	Login Daemon
Source Component	None
Source Version	None
Source Host OS	<ul style="list-style-type: none">• AIX_5.1-5.3• HPUX_11• Suse_ES10• RedHat_7.3_8.0_ES/AS2.1_3.0• Solaris_2.6-9
Transport Mechanism	syslog- <i>ng</i>
PTL Filename	unix_login_syslogng.ptl
Parsing Rule	unix_login_syslogng.rule
Alerting Rule Template	Unix login Substring Match Rule
Connector Views	<ul style="list-style-type: none">• investigation_unix_login_syslogng.sql• userLogin_unix_unix_login_syslogng.sql
Look-up file	None
Scripts	None
Source-Specific Reports	<ul style="list-style-type: none">• "Unix or Linux Login Details", on page 254
Event Types	<ul style="list-style-type: none">• "Audit Event", on page 109• "Unparsed Data", on page 139• "User Logins: Linux/Unix", on page 147

SETTING UP THE UNIX_LOGIN_SYSLOGNG LOG ADAPTER

This document describe how to configure the unix_login_syslogng log adapter. The following steps are required:

- “[Source System syslog Setup](#)”, on page 650
- “[HawkEye Collector syslog-ng Setup](#)”, on page 651

SOURCE SYSTEM SYSLOG SETUP

This section describes configurations you make on your log source host. Instructions are provided for the following Unix-based operating systems:

- “[Linux](#)”, next
- “[HP-UX](#)”, on page 650

Linux

To configure your source system, make the following configuration changes on your log source host:

1 Log in to the Linux server using a privileged account.

2 Open the the file `/etc/syslog.conf` in a text editor.

3 Add the following line:

```
*.debug @###.###.###.###
```

where `###.###.###.###` is the IP address of the host running the HawkEye Collector.

4 Save and close the file.

5 Restart the syslog daemon:

```
kill -HUP `cat /var/run/syslogd.pid`
```

HP-UX

To configure your source system, make the following configuration changes on your log source host:

1 Log in to the HP-UX server using a privileged account.

2 Open the the file `/etc/syslog.conf` in a text editor.

3 Add the following lines:

```
*.info @###.###.###.###  
*.alert;*.emerg @###.###.###.###  
*.crit;*.err;*.notice @###.###.###.###
```

Where `###.###.###.###` is the IP address of the host running the HawkEye Collector.

4 Save and close the file.

5 Restart the syslog daemon:

```
kill -HUP `cat /var/run/syslog.pid`
```

HAWKEYE COLLECTOR SYSLOG-NG SETUP

To configure your log adapter, make the following configuration change on the host running the HawkEye Collector:

- 1 Edit `/etc/syslog-ng.conf` on the host running the HawkEye Collector, configuring a filter statement, a destination statement, and a log statement as shown below:

- Filter statement:

```
filter f_nix_login
{ facility(auth, authpriv) and (program(login) or match(login)); };
```

- Destination statement:

```
destination d_nix_login {
file("<HawkEye AP Home>/incoming/syslog-ng/unix_login_syslogng/
unix_login_syslogng.log"
template
("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST $MSG\n")
template_escape(no) );
};
```

NOTE: Change the path and file name of the “file” argument to match the location of your log file.

- Log statement:

```
log {
source(s_network_std);
filter(f_nix_login);
destination(d_nix_login);
flags(final);
};
```

- 2 Restart the syslog-ng daemon.

- 3 Edit the HawkEye Collector `config.xml` with sections for `logqueue`, `retriever`, `loader`. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

- 4 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

CHAPTER 56

unix_sshd2_syslogng

SYSTEM INFORMATION

Log Adapter Component	Details
Name	unix_sshd2_syslogng
Version	1.1.0
Source Vendor	Unix
Source Product	SSHD Daemon
Source Component	None
Source Version	<ul style="list-style-type: none">• OpenSSH_3.9p1• OpenSSL 0.9.7a
Source Host OS	<ul style="list-style-type: none">• AIX_5.1-5.3• HPUX_11• Suse_EL9• RedHat_7.3_8.0_ES/AS2.1_3.0• Solaris_2.9
Transport Mechanism	syslog- <i>ng</i>
PTL Filename	unix_sshd2_syslogng.ptl
Parsing Rule	unix_sshd2_syslogng.rule
Alerting Rule Template	Unix sshd Substring Match Rule
Connector Views	<ul style="list-style-type: none">• investigation__unix_sshd2_syslogng.sql• userLogin__unix_unix_sshd2_syslogng.sql
Look-up file	None
Scripts	None
Source-Specific Reports	<ul style="list-style-type: none">• “Unix or Linux Login Details”, on page 254
Event Types	<ul style="list-style-type: none">• “Audit Event”, on page 109• “Unparsed Data”, on page 139• “User Logins: Linux/Unix”, on page 147

SETTING UP THE UNIX_SSHD2_SYSLOGNG LOG ADAPTER

This document describe how to configure the unix_sshd2_syslogng log adapter. The following steps are required:

- “Source System syslog Setup”, on page 654
- “SenSage AP Collector syslog-*ng* Setup”, on page 655

SOURCE SYSTEM SYSLOG SETUP

This section describes configurations you make on your log source host. Instructions are provided for the following Unix-based operating systems:

- “Linux”, next
- “HP-UX”, on page 654

Linux

To configure your source system, make the following configuration changes on your log source host:

1 Log in to the Linux server using a privileged account.

2 Open the file `/etc/syslog.conf` in a text editor.

3 Add the following line:

```
*.debug @###.###.###.###
```

where `###.###.###.###` is the IP address of the host running the Sensage collector.

4 Save and close the file.

5 Restart the syslog daemon:

```
kill -HUP `cat /var/run/syslogd.pid`
```

HP-UX

To configure your source system, make the following configuration changes on your log source host:

1 Log in to the HP-UX server using a privileged account.

2 Open the the file `/etc/syslog.conf` in a text editor.

3 Add the following lines:

```
*.info @###.###.###.###  
*.alert;*.emerg @###.###.###.###  
*.crit;*.err;*.notice @###.###.###.###
```

Where `###.###.###.###` is the IP address of the host running the SenSage AP Collector.

4 Save and close the file.

5 Restart the syslog daemon:

```
kill -HUP `cat /var/run/syslog.pid`
```

SEN SAGE AP COLLECTOR SYSLOG-NG SETUP

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Edit `/etc/syslog-ng.conf` on the host running the SenSage AP Collector, configuring a filter statement, a destination statement, and a log statement as shown below:

- Filter statement:

```
filter f_nix_sshd2 { program(sshd); };
```

- Destination statement:

```
destination d_nix_sshd2 {
    file("<HawkEye AP Home>/incoming/syslog-ng/unix_login_syslogng/
        unix_login_syslogng.log"
    template
        ("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST $MSG\n")
    template_escape(no) );
};
```

NOTE: Change the path and file name of the “file” argument to match the location of your log file.

- Log statement:

```
log {
    source(s_network_std);
    filter(f_nix_sshd2);
    destination(d_nix_sshd2);
    flags(final);
};
```

- 2 Restart the syslog-ng daemon.

- 3 Edit the `SenSage AP Collector config.xml` with sections for `logqueue`, `retriever`, `loader`. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

- 4 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

CHAPTER 57

unix_su_syslogng

SYSTEM INFORMATION

Log Adapter Component	Details
Name	unix_su_syslogng
Version	1.2.0
Source Vendor	Unix
Source Product	SU
Source Component	None
Source Version	5.2.1
Source Host OS	<ul style="list-style-type: none">• AIX_5.1-5.3• HPUX_11• Suse_ES10• RedHat_7.3_8.0_ES/AS2.1_3.0• Solaris_2.6-9
Transport Mechanism	syslog- <i>ng</i>
PTL Filename	unix_su_syslogng
Parsing Rule	unix_su_syslogng.rule
Alerting Rule	Unix su Substring Match Rule
Connector Views	<ul style="list-style-type: none">• investigation_unix_su_syslogng.sql• privilegedCommand_unix_unix_su_syslog.sql
Look-up file	None
Scripts	None
Source-Specific Reports	<ul style="list-style-type: none">• “Unix or Linux Privileged Commands Details”, on page 262
Event Types	<ul style="list-style-type: none">• “Audit Event”, on page 109• “Privileged Commands”, on page 129• “Privileged Commands: Linux/Unix”, on page 131

SETTING UP THE UNIX_SU_SYSLOGNG LOG ADAPTER

This document describe how to configure the microsoft_windows_securityEvent_snare log adapter. The following steps are required:

- “[Source System syslog Setup](#)”, next

- “SenSage AP Collector syslog-ng Setup”, on page 659

SOURCE SYSTEM SYSLOG SETUP

This section describes configurations you make on your log source host. Instructions are provided for the following Unix-based operating systems:

- “Linux”, next
- “HP-UX”, on page 658

Linux

To configure your source system, make the following configuration changes on your log source host:

- 1 Log in to the Linux server using a privileged account.
- 2 Open the file `/etc/syslog.conf` in a text editor.
- 3 Add the following line:

```
*.debug @###.###.###.###
```

where `###.###.###.###` is the IP address of the host running the SenSage AP collector.

- 4 Save and close the file.
- 5 Restart the syslog daemon:

```
kill -HUP `cat /var/run/syslogd.pid`
```

HP-UX

To configure your source system, make the following configuration changes on your log source host:

- 1 Log in to the HP-UX server using a privileged account.
- 2 Open the file `/etc/syslog.conf` in a text editor.
- 3 Add the following lines:

```
*.info @###.###.###.###  
*.alert;*.emerg @###.###.###.###  
*.crit;*.err;*.notice @###.###.###.###
```

Where `###.###.###.###` is the IP address of the host running the SenSage AP collector.

- 4 Save and close the file.
- 5 Restart the syslog daemon:

```
kill -HUP `cat /var/run/syslog.pid`
```

SEN\$AGE AP COLLECTOR SYSLOG-NG SETUP

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Edit `/etc/syslog-ng.conf` on the host running the SenSage AP collector, configuring a filter statement, a destination statement, and a log statement as shown below:

- Filter statement:

```
filter f_nix_su {
    facility(auth, authpriv) and program(su) or match(su) and match(pam_unix);
};
```

- Destination statement:

```
destination d_nix_su {
    file("<SenSage AP Home>/incoming/syslog-ng/unix_su_syslogng/
        unix_su_syslogng.log"
        template
        ("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST $MSG\n")
        template_escape(no)
    );
};
```

NOTE: Change the path and file name of the “file” argument to match the location of your log file.

- Log statement:

```
log {
    source(s_network_std);
    filter(f_nix_su);
    destination(d_nix_su);
    flags(final);
};
```

- 2 Restart the syslog-ng daemon.

- 3 Edit the SenSage AP Collector `config.xml` with sections for `logqueue`, `retriever`, `loader`. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

- 4 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.s

unix_sudo_syslogng

SYSTEM INFORMATION

Log Adapter Component	Details
Name	unix_sudo_syslogng
Version	2.1.0
Source Vendor	Unix
Source Product	SUDO
Source Component	None
Source Version	1.6.7
Source Host OS	<ul style="list-style-type: none"> • AIX_5.2 • HPUX_11 • Suse_ES10 • RedHat_7.3_8.0_ES/AS2.1_3.0 • Solaris_2.9
Transport Mechanism	syslog- <i>ng</i>
PTL Filename	unix_sudo_syslogng.ptl
Parsing Rule	unix_sudo_syslogng.rule
Alerting Rule	Unix sudo Substring Match Rule
Connector Views	<ul style="list-style-type: none"> • investigation_unix_sudo_syslogng • privilegedCommand_unix_unix_sudo_syslogng
Look-up file	None
Scripts	None
Source-Specific Reports	<ul style="list-style-type: none"> • “Unix or Linux Privileged Commands Details”, on page 262
Event Types	<ul style="list-style-type: none"> • “Audit Event”, on page 109 • “Privileged Commands”, on page 129 • “Privileged Commands: Linux/Unix”, on page 131

SETTING UP THE UNIX_SUDO_SYSLOGNG LOG ADAPTER

This document describe how to configure the log adapter for microsoft_windows_securityEvent_snare. The following steps are required:

- “Source System syslog Setup”, on page 662
- “SenSage AP Collector syslog-*ng* Setup”, on page 663

SOURCE SYSTEM SYSLOG SETUP

This section describes configurations you make on your log source host. Instructions are provided for the following Unix-based operating systems:

- “Linux”, next
- “HP-UX”, on page 662

Linux

To configure your source system, make the following configuration changes on your log source host:

1 Log in to the Linux server using a privileged account.

2 Open the file `/etc/syslog.conf` in a text editor.

3 Add the following line:

```
*.debug @###.###.###.###
```

where `###.###.###.###` is the IP address of the host running the SenSage AP collector.

4 Save and close the file.

5 Restart the syslog daemon:

```
kill -HUP `cat /var/run/syslogd.pid`
```

HP-UX

To configure your source system, make the following configuration changes on your log source host:

1 Log in to the HP-UX server using a privileged account.

2 Open the the file `/etc/syslog.conf` in a text editor.

3 Add the following lines:

```
*.info @###.###.###.###  
*.alert;*.emerg @###.###.###.###  
*.crit;*.err;*.notice @###.###.###.###
```

Where `###.###.###.###` is the IP address of the host running the SenSage AP Collector.

4 Save and close the file.

5 Restart the syslog daemon:

```
kill -HUP `cat /var/run/syslog.pid`
```

SEN SAGE AP COLLECTOR SYSLOG-NG SETUP

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Edit `/etc/syslog-ng.conf` on the host running the SenSage AP Collector, configuring a filter statement, a destination statement, and a log statement as shown below:

- Filter statement:

```
filter f_nix_sudo { facility(auth, authpriv) and program(sudo); };
```

- Destination statement:

```
destination d_nix_sudo {
    file("<HawkEye AP Home>/incoming/syslog-ng/unix_su_syslogng/
        unix_su_syslogng.log"
    template
        ("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST $MSG\n")
    template_escape(no)
};
```

NOTE: Change the path and file name of the “file” argument to match the location of your log file.

- Log statement:

```
log {
    source(s_network_std);
    filter(f_nix_sudo);
    destination(d_nix_sudo);
    flags(final);
};
```

- 2 Restart the syslog-ng daemon.

- 3 Edit the SenSage AP Collector `config.xml` with sections for `logqueue`, `retriever`, `loader`. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.

- 4 (Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

CHAPTER 59

vmware_esx_500_syslogng

SYSTEM INFORMATION

Log Adapter Component	Details
Name	vmware_esx_500_syslogng
Version	2.0.0
Source Vendor	Vmware
Source Product	ESXi server
Source Component	N/A
Source Version	5.0 or later
Source Host OS	N/A
Transport Mechanism	syslog- <i>ng</i>
PTL Filename	vmware_esx_500_syslogng.ptl
Parsing Rule	None
Alerting Rule	None
Connector Views	<ul style="list-style-type: none">• investigation__vmware_esx_500_syslogng• parsedData__vmware_esx_500_syslogng• unparsedData__vmware_esx_500_syslogng• userLogin__vmware_esx_500_syslogng
Look-up file	Not required
Scripts	Not required
Source-Specific Reports	None
Event Types	<ul style="list-style-type: none">• “Audit Event”, on page 109• “Unparsed Data”, on page 139

SETTING UP VMWARE_ESX_500_SYSLOGNG LOG ADAPTER

This document describes how to configure the vmware_esx_syslogng log adapter. The following steps are required:

- “Source System Setup”, next
- “HawkEye Collector Configuration”, on page 621

SOURCE SYSTEM SETUP

To enable logging to remote the remote host, execute the following commands from the ESXI shell:

- 1 Check the current configuration:

```
# esxcli system syslog config get
```

Example of output:

```
Default Rotation Size: 1024
Default Rotations: 8
Log Output: /scratch/log
Log To Unique Subdirectory: false
Remote Host: <none>
```

- 2 Set the remote host for logging:

```
# esxcli system syslog config set --loghost 10.10.10.10
```

- 3 Restart the syslog service (vmsyslogd):

```
# esxcli system syslog reload
```

- 4 Make sure that the firewall does not block syslog::

```
# esxcli network firewall ruleset list | grep syslog
```

Example of output:

```
syslog      false
```

Allow syslog on firewall:

```
# esxcli network firewall ruleset set --ruleset-id=syslog --enabled=true
# esxcli network firewall refresh
```

- 5 For testing send some message to all logs at the same time:

```
# esxcli system syslog mark -message="syslogng-test-configuration"
```

SenSage AP Collector Configuration

To configure your log adapter, make the following configuration change on the host running the SenSage AP Collector:

- 1 Open the syslog-ng configuration file <SenSage AP Home>/etc/syslog-ng/syslog-ng.conf on the host running the SenSage AP Collector.
- 2 Make sure that the following destination, filter and log statements are configured as shown below:

```
destination d_vmware_esx_500_syslogng {
    file("<SenSage AP Home>/incoming/syslog-ng/vmware_esx_500_syslogng/
vmware_esx_500_syslogng.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MSGHDR$MSG\n")
        template_escape(no) );
};

filter f_vmware_esx_500_syslogng {
    program('Vpxa') or program('Hostd')
    or program('vmkernel') or program('vmkwarning')
    or program('vmkssummary') or program('shell')
    or program('Fdm') or program('esxupdate');
};

log {
    source(s_network_std); source(s_network_tls);
    filter(f_vmware_esx_500_syslogng);
    destination(d_vmware_esx_500_syslogng);
    flags(final);
};
```

- 3 Reload the syslog-ng configuration file using the following command:

```
kill -HUP $(pgrep syslog-ng)
```

- 4 Edit the SenSage AP Collector **config.xml** with sections for logqueue, retriever, loader. For more information, see [Chapter 2: SenSage AP Collector Configuration](#) in the *Collector Guide*.
- 5 Optional) Set up log file rotation. See “[Setting Up Syslog-NG Log Rotation](#)”, on page 677.

SAMPLE CONFIGURATION FILES

This section contains the following sample configuration files:

- Collector Configuration (**config.xml**)
- Syslog-NG Configuration entries (**syslog-ng.conf**)

Collector Configuration (**config.xml**)

```
<LogQueue path='queue/vmware_esx_500_syslogng' minMBFree='100'
name='q_vmware_esx_500_syslogng' encoding='UTF-8' />
```

```

<Retriever type='filesystem' enabled='1' name='r_vmware_esx_500_syslogng'
deleteOriginal='1' method='copy'>
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_vmware_esx_500_syslogng</LogQueue>
<SourceDir>/opt/hexis/incoming/syslog-ng/vmware_esx_500_syslogng</SourceDir>
<Plugin name='Default'>
<File ai='ignore' id='1'>.*</File>
<File ai='accept' id='2'>.*\.loadme$</File>
</Plugin>
</Retriever>

<Loader enabled='1' name='l_vmware_esx_500_syslogng'>
<RunOnHost>localhost</RunOnHost>
<LogQueue>q_vmware_esx_500_syslogng</LogQueue>
<SLSInstance>analytics.example.com:8072</SLSInstance>
<SLSUser>administrator</SLSUser>
<SLSSharedKey>file:/opt/hexis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc</SLSSharedKey>

<PTL table='vmware_esx_500_syslogng' namespace='analytics' type='file'>
<Location>/opt/hexis/hawkeye-ap/analytics/adapters/
vmware_esx_500_syslogng/vmware_esx_500_syslogng.ptl</Location>
<LoadOption>--override=TZ:'America/Los_Angeles'</LoadOption>
</PTL>
</Loader>

```

Syslog -ng Configuration Entries (**syslog-ng.conf**)

```

# VMware ESXi server
destination d_vmware_esx_500_syslogng {
    file("/opt/hexis/incoming/syslog-ng/vmware_esx_500_syslogng/
vmware_esx_500_syslogng.log"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST
$MESSHDR$MESS\n")
        template_escape(no) );
};

# VMware ESXi server
filter f_vmware_esx_500_syslogng {
    program('Vpxa') or
    program('Hostd') or
    program('vmkernel') or
    program('vmkwarning') or
    program('vmkssummary') or
    program('shell') or
    program('Fdm') or
    program('esxupdate');
};

log {
    source(s_network_std);
    source(s_network_tls);
    filter(f_vmware_esx_500_syslogng);
    destination(d_vmware_esx_500_syslogng);
    flags(final);
};

```

APPENDIX A

REPORT LIBRARIES REFERENCE

Report libraries provide functions for common look-up and conversion operations you may wish to perform in your SQL reports.

The following libraries are included with your SenSage AP distribution:

- “Geo IP Utility”, next
- “IP Conversion Utility”, on page 670
- “Internal System Audit Library”, on page 671
- “Microsoft Windows Library”, on page 671

GEO IP UTILITY

The Geo IP Utility library contains functions to look up domain and country of origin from a URL.

domain()

Returns the domain name portion of the URL.

Synopsis

```
domain (<URL>)
```

Arguments

Argument	Description
<URL>	Universal Resource Locator (URL)

Example

```
SELECT
    URL as "URL",
    domain(URL) as "Domain"
FROM
    myTable
DURING ALL
```

Return Value

The domain name portion of the URL. For example, the domain name of the URL “www.foo.com” is “foo.com”

get_country_from_domain()

Returns the country where a domain is located.

Synopsis

```
get_country_from_domain(<domain_name>)
```

Arguments

Argument	Description
<domain_name>	Domain name

Example

```
SELECT
    URL as "URL",
    domain(URL) as "Domain"
    get_country_from_domain(domain(URL)) as "Country of Origin"
FROM
    myTable
DURING ALL
```

Return Value

The Country where the domain is located, displayed as a two-character code using ISO 3166-1-alpha-2 code elements. See [English country names and code elements](#) for a complete list.

IP CONVERSION UTILITY

The IP Conversion Utility library provides the `hex_to_dotted_quad()` function.

[hex_to_dotted_quad\(IP address in Hexadecimal format\)](#)

Converts an IP address stored in hexadecimal format to the standard dotted quad format.

Synopsis

```
hex_to_dotted_quad(<Hex_IP>)
```

Arguments

Argument	Description
<Hex_IP>	IP address in hexadecimal format

Return Value

IP address in dotted quad format. For example, the following IP address is displayed in dotted quad format:

127.0.0.1.

Example

```
SELECT
    hex_to_dotted_quad(SOURCEIPADDR) as "IP Address"
FROM
    myTable
DURING ALL
```

INTERNAL SYSTEM AUDIT LIBRARY

The Internal System Audit library provides a function for use with creating reports on SenSage AP internal auditing tables.

service2Description()

Translates an internal service name to a textual description.

Synopsis

```
service2Description(<service_name>)
```

Arguments

Argument	Description
<service_name>	Internal SenSage AP service name

Return Value

A textual description of the service name.

Example

```
service2Description(ReportService.createReportDefinition)
```

```
SELECT
    SERVICE_NAME as "Service Name"
    service2Description(SERVICE_NAME) as "Service Description"
FROM
    myTable
DURING ALL
```

MICROSOFT WINDOWS LIBRARY

The Microsoft Windows library provides the following functions for use in processing Windows event data:

- “[loginType2desc\(\)](#)”, on page 672
- “[eventId2desc\(\)](#)”, on page 672

- “rights2desc()”, on page 673
- “k5code2desc()”, on page 673

loginType2desc()

Translates numeric login types to a textual description.

Synopsis

```
loginType2desc (<login_type>)
```

Arguments

Argument	Description
<login_type>	Windows login type code

Return Value

A textual description of the Windows login type code.

Example

```
SELECT
    LOGIN_TYPE as "Login Type Code",
    loginType2desc(LOGIN_TYPE) as "Login Description"
FROM
    myTable
DURING ALL
```

eventId2desc()

Translates numeric event ID codes into a textual description.

Synopsis

```
eventId2desc (<Event_ID_code>)
```

Arguments

Argument	Description
<Event_ID_code>	Windows event ID code

Return Value

A textual description of the Windows event ID code.

Example

```
SELECT
    EVENT_ID as "Event ID Code",
    eventId2desc(EVENT_ID) as "Event Description"
FROM
```

```
myTable
DURING ALL
```

rights2desc()

Translates Windows user rights strings to a textual description.

Synopsis

```
rights2desc (<Windows_user_right>)
```

Arguments

Argument	Description
<Windows_user_right>	A string representing user rights. For example: SeBackupPrivilege.

Return Value

A textual description of the user right.

Example

```
SELECT
    USER_RIGHT as "User Right",
    rights2desc(USER_RIGHT) as "User Right Description"
FROM
    myTable
DURING ALL
```

k5code2desc()

Translates a Kerberos hexadeicmal error code into a textual description.

Synopsis

```
k5code2desc (<hex_code>)
```

Arguments

Argument	Description
<hex_code>	Kerberos error code in hexadecimal format

Return Value

Textual description of the Kerberos error code.

Example

```
SELECT
    KERBEROS_ERROR as "Kerberos Error Code",
```

```
k5code2desc(KERBEROS_ERROR) as "Kerberos Error Description"  
FROM  
    myTable  
DURING ALL
```

APPENDIX B

SYSLOG-NG SETUP

This appendix describes various Syslog-NG setup issues. The following topics are covered:

- “About syslog-ng”, next
- “syslog-*ng.conf* file”, on page 676
- “destination statement: escaped characters”, on page 676
- “Log Statement: flags(final);”, on page 677
- “Log Statement: Order of Processing and String Matching”, on page 677
- “Setting Up Syslog-NG Log Rotation”, on page 677

ABOUT SYSLOG-NG

syslog-*ng* is a replacement for syslog that adds functionality such as multiplexing, TCP, and year data in the time stamp and adds a powerful set of configuration options. For more information on syslog-*ng*, see [BalaBit’s Web site](#). syslog-*ng* allows you to configure handling of messages by forwarding them to other syslog-*ng* instances, forwarding messages to other applications, or by writing the messages to a log file.

In a SenSage AP deployment, you typically configure a syslog-*ng* instance on the host system running the SenSage AP Collector, and, depending on your environment, also on source information systems. Often, the easiest way to collect operating system logs from a variety of Unix hosts is to configure syslog or syslog-*ng* on these host systems. Some applications send data using the syslog protocol and require configuration in the application. The syslog-*ng* instance running on the SenSage AP Collector receives incoming log data from these syslog or syslog-*ng* sources and saves the data as log files that are then loaded into the SenSage AP Event Data Warehouse (EDW) for storage and analysis.

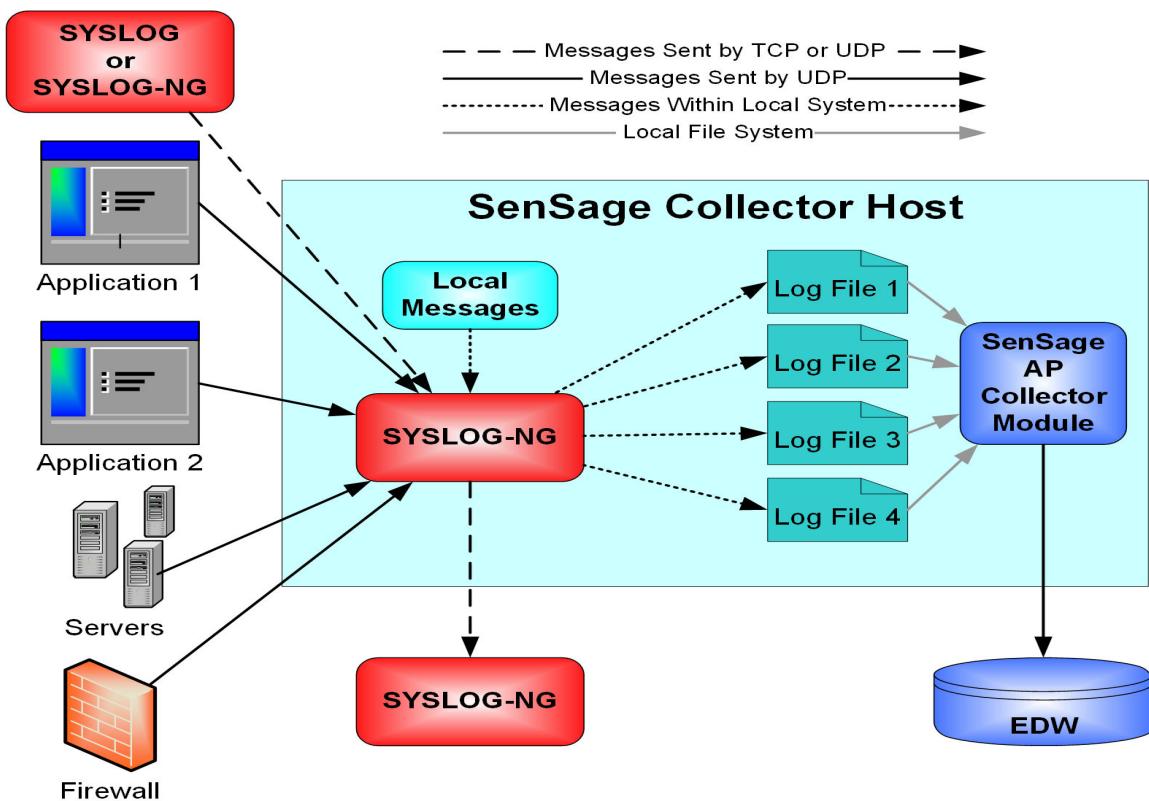
Figure B-1: SenSage AP Collector and syslog-*ng* Architecture

Figure B-1 shows applications, servers, firewalls, another syslog-*ng* instance, and local messages all forwarding their messages to a syslog-*ng* instance running on the SenSage AP Collector. The syslog-*ng* instance running on the collector writes out log files with the received messages on to the local file system. The SenSage AP Collector module then picks up the log files and loads them into the EDW. The collector syslog-*ng* instance also forwards some messages to a remote syslog-*ng* instance for processing outside of the SenSage AP deployment.

SYSLOG-NG.CONF FILE

The `syslog-ng.conf` file contains configuration instructions for handling incoming messages. In the `syslog-ng.conf` file you configure four types of statements, a `source` statement, `filter` statement, a `destination` statement, and a `log` statement. Together, these statements define how syslog-*ng* handles incoming messages. The `source` statement specifies where syslog-*ng* listens for messages. The `filter` statement contains logic to identify the log source of an incoming message, the `destination` statement defines where to send the data, and the `log` statement specifies what is done with the messages when a filter statement is matched.

DESTINATION STATEMENT: ESCAPED CHARACTERS

In the following sample destination statement, the final line has the statement `template_escape(no)`, which specifies that syslog-*ng* does not “escape” special characters

(such as tabs) when writing out a log line. Because SenSage AP PTL files are written to expect non-escaped characters, incorrect data may be written to the EDW if this statement is not included.

```
destination d_ios {
    file("/opt/hexis/incoming/cisco_ios/cisco_ios.log"
template
("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST $MSG\n")
template_escape(no) );
};
```

LOG STATEMENT: FLAGS(FINAL):

The following sample `log` statement includes the statement `flags(final);`. When syslog-ng processes log data, it searches sequentially through the `syslog-ng.conf` file for a log statement whose filter matches the log data. The `flags(final);` statement instructs syslog-ng to stop looking for additional matches in subsequent log statements after matching a log statement containing the `flags(final)` statement. If you are sending log data to multiple destination log files, you may need to examine the placement of any `flags(final)` statements.

```
log { source(s_network_ssi); filter(f_ios); destination(d_ios);
flags(final); }
```

LOG STATEMENT: ORDER OF PROCESSING AND STRING MATCHING

Log statements are processed in the order they appear in the `syslog-ng.conf` file. If your filter statement contains string matching logic, note that a match can occur on a substring. For instance, the following filter statements look for the string “sudo” and then “su”. A message containing the string “sudo” will match both filters. If the log statement that references this filter uses the `flags(final);` the message will be written only to the destination referenced in that log statement. The second filter statement will not be evaluated due to the use of the `flags(final);` statement.

```
filter f_nix_sudo          { match(su); };
filter f_nix_su             { match(sudo) };
```

SETTING UP SYSLOG-NG LOG ROTATION

You can configure syslog-ng to perform an implicit log rotation by appending date and/or time information to the filename generated by syslog-ng. For example, if you append year, month, and day information, syslog will create a new log file every day.

Because messages may arrive from various time zones, it is possible that a message will contain a date or time later than the time when the message is processed by syslog-ng, causing a new file to be created, appended with the new time information. For this reason, syslog-ng provides date and time macros that represent the time the message is processed by syslog-ng rather than the timestamp contained in the message. These macros are preceded by “`R_`”.

To configure log rotation, make the following modifications to the `syslog-ng.conf` file on the host running the SenSage AP Collector:

- 1 Change the destination statement by appending any of the following variables to the log file name:

- `$R_YEAR`
- `$R_MONTH`
- `$R_DAY`
- `$R_HOUR`
- `$R_MIN`

The log file will be rotated (that is, saved with a new file name) at the interval specified by the smallest unit of time you specify. For example, if your destination statement looks like the following sample, your log file will rotate daily and the file name will be appended with year, month and date information:

```
destination d_nix_login {  
    file(  
        "/opt/lw/incoming/nix_login/nix_login.log-$R_YEAR-$R_MONTH-$R_DAY"  
        template  
        ("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $FACILITY.$PRIORITY $HOST  
        $MSG\n")  
        template_escape(no) );  
};
```

- 2 Configure a Retriever module in the SenSage AP Collector to collect the log files at the same interval as your log rotation.
- 3 Configure file handling. Depending on how your Retriever is configured, you may need to copy files to the Collector host on an appropriate schedule, and delete them after they are loaded. (You can configure the Retriever to delete the files after loading by setting its `deleteOriginal` parameter to 1.)

For more information, see: “[SenSage AP Collector Configuration](#)”, on page 21 in the *Collector Guide*.

INDEX

A

Access and privileges
IT Model 38

Analytics

- BlueCoat Reports 351
- Compliance Reports 185
- exporting 36
- Foundation Analytics Reports (Windows) 211
- Foundation Reports (UNIX/LINUX) 253
- importing 36
- IntelliSchema 28
- Internal System Reports 298
- overview 27
- Panos Reports 437
- SAP Reports 441
- Systems Analytics Reports 273
- Workbench 28

Analytics Workbench

- Component Input Parameter 41
- working with Sample Models 69

associated reports

- investigation 114

B

backslash

- syntax usage explained 26

BlueCoat Reports

- reference 351

C

Collector Activity Monitoring Reports

- reference 282

Compliance Analytics Reports 34

- reference 185

Component Input Parameter

- Analytics Workbench 41

connector view 29

D

documentation 23

E

Email Name configuration
IT Model 45

event types

- IntelliSchema 32
- Investigation 114
- reference 93

event-type view 29

exporting

- analytics 36

Foundation Analytics Reports 33

Foundation Analytics Reports (UNIX/LINUX) 253

Foundation Analytics Reports (Windows) 211

H

HawkEye AP Analytics Workbench

- IT Model 41

HawkEye G Analytics Reports

- reference 359

I

importing

- analytics 36

Insider Threat Detection Model

- see IT Model 37

IntelliSchema 28

- adding new event sources 165
- and tablematch() function 166
- architecture 31
- Compliance reports 34
- connector view 29
- creating views 36
- event type reference 93
- event types 32
- event-type view 29
- implementation 28
- master view 29
- modifying 36

namespaces 32
naming conventions 167
IntelliSchema Name configuration
 IT Model 44
Internal System Reports
 reference 298
investigation
 event type 114
IT Detection Dashboard 53
IT Model
 access and privileges 38
 Analytics Workbench parameter settings 41
 configuring changes 44
 creating views and functions 39
 Email Name configuration 45
 HawkEye AP Analytics Workbench 41
 Human Resources Table Configuration 46
 IntelliSchema Name configuration 44
 IT detection dashboard 53
 modifying the weighting used in the IT Model 49
 overview 37
 requirements 38, 39
 Time Period settings 48

L

Log Adapters 35
 verification 35

M

master view 29
Models
 also see Sample Models 69
 sample models listing 69

N

namespaces
 and IntelliSchema 32

O

overview
 Analytics 27

P

Panos Reports reference 437

R

reports
 investigation 114

S

Sample model description
 Notification threshold is exceeded in a report 85
Sample Models
 creating a new data table using samples 83
 dashboard 82
 data table descriptions 77
 data table outputs 79
 data table programmable fields 77
 data tables description 76
 expected results of data table samples 82
 implement data tabs 74
 importing sample data table models 75
 Reports 82
 scheduling a data table 80
 setting up the database 75
 using data tables 72
 Working with Analytics Workbench 69
SAP Reports
 reference 441
Systems Analytics Reports
 Collector Activity Monitoring Reports reference 282
 reference 273

T

tablematch() 166
Time Period settings
 IT Model 48

W

Weighting
 IT Model 49
Workbench 28