TIBCO LogLogic® Security Event Management (SEM)

Release Notes

Software Release 3.6.0

Two-Second Advantage®

Important Information

Release Notes for TIBCO LogLogic® Security Event Management, v3.6.0 GA

TIBCO LogLogic® Security Event Management (SEM) offers scalable and comprehensive data security assistance monitoring for organizations challenged by the complexity of modern IT infrastructures. It is designed to continuously protect the most valuable business assets: core systems and the intellectual property they hold.

This document lists functionality changes and bug fixes in TIBCO LogLogic® Security Event Management **version 3.6.0**.

Note: For changes to the Release Notes after the initial release, see https://download.tibco.com/tibco/

New Features

4th generation of SEM appliances

SEM 3.6 supports the last generation of SEM appliances

4th Generation Appliances (H4)	*SEM 1065*	*SEM 3065*	*SEM 4065*
Rack Format	1U	2U	1U
Processor(s) Type	Xeon E5	Xeon E5	Xeon E5
Total Core #	6	6	8
RAM (GB)	12	24	32
Max. EPS (remote Log Collector)	1700	5000	7000
Max. Instances	1	1	2
Archive Storage (GB)	33	66	100
Online Storage (GB)	350	700	950

Appliance Mapping

The following table provides information per generation:

SEM appliances	
3th Gen (2009-2013)	**4th Gen (2013)**
SEM 1060	SEM 1065
SEM 3060	SEM 3065
SEM 4060	SEM 4065

Log Source Packages for SEM

SEM 3.6 allows the installation of additional log sources though Log Source Packages.

Requirements

Supported Security Event Manager Platforms

TIBCO LogLogic® Security Event Management can be installed on the following appliances:

- TIBCO LogLogic® Security Event Manager 1060
- TIBCO LogLogic® Security Event Manager 3060
- TIBCO LogLogic® Security Event Manager 4060

- TIBCO LogLogic® Security Event Manager 1065
- TIBCO LogLogic® Security Event Manager 3065
- TIBCO LogLogic® Security Event Manager 4065

Web Console Requirements

The Web Console can be used with the following web browsers:

Web browser	Version
Microsoft Internet Explorer	8, 9
Mozilla Firefox	18

Hosts running the Web Console must have at least:

  - 1 GB of RAM.
  - 1024x768 resolutions.
  - 1 GHz 32-bit (x86) or 64-bit (x64) processor.

Supported Log Sources

Vendor	Product
Anti virus/spyware/spam	
Apache	Spamassassin
Blue Coat	Blue Coat ProxyAV
Cisco	Ironport Mail Security
ClamAV	ClamAV
Clearswift	Mimesweeper For SMTP DB
Clearswift	Mimesweeper For SMTP Log
Clearswift	Mimesweeper For WEB
F-Secure	Policy Manager
Sophos	Puremessage
Symantec	Norton Antivirus
Symantec	Symantec Antivirus
TrendMicro	Interscan Viruswall
TrendMicro	Trend Micro SPS system
Authentication server	
ActivIdentity	Activpack v4
ActivIdentity	Activpack v6.3
ActivIdentity	Activpack v6.5
Cisco	Cisco ACS Csv
Cisco	Cisco ACS Syslog
Cistron	Radius
EMC	Rsa Ace server
EMC	Rsa Ace WMI
EMC	Rsa Securid linux
Microsoft	Internet Authentication Service
Novell	Novell eDirectory
Utimaco	Safeguard
Business application	
-	-
Centralized management	
-	Ntsyslog
Arkoon	Arkoon DB
Arkoon	Arkoon DB v3
Arkoon	Arkoon DB v4
Arkoon	Arkoon Syslog
Intrusion.com	Securenet Provider
ISS	SiteProtector SP4
ISS	SiteProtector SP5
ISS	SiteProtector SP6
ISS	SiteProtector SP7
Juniper	Netscreen Security Manager v2004
LogLogic	Security Change Manager
McAfee	Epolicy Orchestrator
Microsoft	Microsoft Operation Management
Nagios	Nagios
TrendMicro	Trend Micro Control Manager
Webmin	Webmin
Database services	
Microsoft	Ms sql
Microsoft	Ms sql Operational
Loglogic	Database Security Manager (DSM)
Oracle	Oracle DB
Sourcefire	Sourcefire3D
Directory services	
-	-

Vendor	Product
Domain Name System (DNS)	
isc.org	Bind
File server	
-	Vsftpd
NetApp	Netapp
ProFTPD	ProFTPD
Wu-ftpd	Wuftpd
Honeypot	
honeyd.org	Honeyd
Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)	
3Com	TippingPoint
Cisco	Cisco CSA v45
Cisco	Cisco CSA v52
Cisco	Cisco CSA v60
Cisco	Cisco IPS (SDEE)
Enterasys	Dragon IDS v7_0
Enterasys	Dragon IDS v7_1
Enterasys	Dragon IDS v7_2
ForeScout	Activescout
Intrusion.com	Securenet Sensor
ISS	Realsecure wgm
Juniper	Netscreen IDP
McAfee	Entercept
McAfee	Intrushield
Niksun	Netdetector
Samhain	Samhain
Sentry Tools	Portsentry
Snort	Snort
Snort	Snort DB
Snort	Winsnort
Symantec	Symantec Client Security
Symantec	Symantec Endpoint Protection
Symantec	Symantec Network Security
Tripwire	Tripwire
Tripwire	Tripwire Entreprise
Log management	
LogLogic	LMI
LogLogic	SMP
LogLogic	SMP Relay
Messaging services	
-	Imapd
Ciphertrust	IronMail
courier-mta.org	Courier MTA
Eudora	Qpopper
GNU	Exim
Inter7	Vpopmail
Lotus	Lotus Domino
Microsoft	Exchange
Postfix	Postfix
sendmail.org	Sendmail
TrendMicro	Interscan Messaging Security Suite

Vendor	Product
Network device	
Aruba	Aruba Wireless Access Point
Check Point	Check Point Internal Log
Cisco	Cisco CSS
Cisco	Cisco FWSM
Cisco	Cisco Router
Cisco	Cisco Switch
Cisco	Cisco VPN
Cisco	Cisco VPN IOS compat
Cyberguard	Cyberguard
Draytek	Vigor
F5	Bigip
Juniper	Juniper Secure Access
Juniper	Netscreen
Juniper	Netscreen v6
Linksys	Wap11
Lucent	Brick
Nortel	Alteon Web Switch
Nortel	Contivity
Nortel	Nortel Alteon
Nortel	Nortel switch
Nortel	Nortel VPN gateway
StoneSoft	Stonegate
Zyxel	Zywall
Zyxel	Zyxel
Operating System	
-	Ipchains
Breach Security	Modsecurity
FreeBSD	FreeBSD
Grsecurity	Grsecurity
HP	HP UX
HP	Tru64
IBM	Aix
IBM	Tivoli Directory Server
Linux	Linux
Microsoft	Internet Connection Firewall
Microsoft	Windows 2000 server
Microsoft	Windows 2000 workstation
Microsoft	Windows 2003 server - English
Microsoft	Windows 2003 server
Microsoft	Windows 2008 server - English
Microsoft	Windows 2008 server
Microsoft	Windows Vista - English
Microsoft	Windows Vista
Microsoft	Windows XP - English
Microsoft	Windows XP
Netfilter	Netfilter
Nokia	IPSO
Sun	Solaris
Sun	Solaris BSM
Proxy / Reverse proxy	
Beeware	I Sentry
Blue Coat	Blue Coat ProxySG
Deny ALL	Rweb
F5	Appshield
Ingrian	Ingrian
McAfee	WebShield
Microsoft	Internet Security Acceleration v2000 FW
Microsoft	Internet Security Acceleration v2004
Squid	Squid
Squid	Squidguard
Sun	Iplanet
TrendMicro	Interscan Web Security Suite Linux v2
TrendMicro	Interscan Web Security Suite Windows v2
WebSense	Websense v5
WebSense	Websense v6
Remote desktop	
Symantec	PCanywhere
Unified Threat Management (UTM)	
Astaro	Astaro v4
Astaro	Astaro v5
Barracuda	Barracuda
Check Point	Check Point
Check Point	Pointsec Protector
Cisco	Cisco ASA
Cisco	Cisco PIX
Fortinet	Fortigate
PaloAlto Networks	Firewall
NetASQ	Netasq Alarm v6
NetASQ	Netasq Connection v6
NetASQ	Netasq Filter v6
NetASQ	Netasq v5
Sonicwall	Sonicwall
Symantec	Symantec Gateway Security v2
Symantec	Symantec Gateway Security v3
Virtualization	
-	-
Vulnerability scanner	
Criston	Criston VM
ISS	Internet Security Scanner v6
ISS	Internet Security Scanner v7
McAfee	Foundstone
Qualys	QualysGuard
Tenable Security	Nessus
Web server	
Apache	Apache
Microsoft	Internet Information Services NCSA
Microsoft	Internet Information Services W3C
Microsoft	Internet Information Services W3C v3
Other	
APC	APC EMU
APC	APC UPS

Products also supported through LogLogic LMI are highlighted in green.

Upgrade

To upgrade to Security Event Management v3.6.0, please refer to the *User Guide section Updating the SMP Server*.

- Upgrade bundles can be found at:
    - https://support.tibco.com/esupport/loglogic.htm
    - https://download.tibco.com/tibco/

Documentation

You can find the complete set of user documentation gathering all product guides on:

- https://support.tibco.com/esupport/loglogic.htm
- https://download.tibco.com/tibco/

Technical Support

LogLogic is committed to the success of our customers and to ensuring our products improve customers' ability to maintain secure, reliable networks. Although LogLogic products are easy to use and maintain, occasional assistance may be necessary. LogLogic provides timely and comprehensive customer support and technical assistance from highly knowledgeable, experienced engineers who can help you maximize the performance of your LogLogic Appliances.

To reach our experienced support team by telephone:

Toll Free, US—1 800 957 LOGS (5647)

Toll—1 408 834 7480

Toll Free, Canada—1 800 957 LOGS (5647)

Toll—1 408 834 7480

Toll Free, Mexico—1 800 957 LOGS (5647)

Toll—1 408 834 7480

Toll Free, United Kingdom—00 800 0330 4444

Toll—01480 479391

Toll Free, Mainland Europe—00 800 0330 4444

Toll— +44 1480 479391

Toll Free, Japan IDC—0061 800 0330 4444

Toll— Not Available

Toll Free, Japan KDD—0010 800 0330 4444

Toll— Not Available

Toll Free, Brazil—0021 800 0330 4444

Toll— Not Available

Email: ll-support@tibco.com

Support Website: https://support.tibco.com/esupport/loglogic.htm

When contacting the support, be prepared to provide the following information:

- Your name, e-mail address, phone number, and fax number
- Your company name and company address
- Your appliance model and release version
- Serial number located on the back of the Appliance or the eth0 MAC address
- A description of the problem and the content of pertinent error messages (if any)

Documentation Support

Your feedback on the documentation is important to us. If you have questions or comments, send email to DocComments@loglogic.com. In your email message, please indicate the software name and version you are using, as well as the title and document release date of your documentation. Your comments will be reviewed and addressed by LogLogic Technical Publications. The Technical Publications team is eager to receive your feedback to help ensure that the documentation is accurate and useful.