CorreLog®

McAfee ePolicy Orchestrator® (ePO) Adapter Software

Installation And Users Manual

http://www.correlog.com mailto:info@correlog.com

CorreLog, ePO Adapter Users Manual

Table of Contents

Section 1: Introduction

This manual provides a detailed description of the CorreLog McAfee ePolicy Orchestrator (ePO) integration software, including detailed installation and usage. This software is an optional set of files and executables added to the CorreLog Server order to expand the role of the CorreLog to include collection and monitoring of ePO events, and posting of data to the ePO event log.

The manual provides information on specific features and capabilities of this special software, including installation procedures, operating theory, application notes, and certain features not documented elsewhere.

The ePO adapter software consists of several components. The user configures ePO to send events to CorreLog, where they are logged and correlated like any other message. Additionally, the user configures CorreLog (via the "Ticket > Actions" facility) to send ticket information back to ePO, where it is displayed in the ePO event log.

This manual is intended for CorreLog users who will operate the system, as well as system administrators responsible for installing the software components. This information will also be of interest to program developers and administrators who want to extend the range of the CorreLog system's role within an enterprise.

Note: The ePO software is a standard component of the CorreLog system, but must be licensed separately. The option is available during evaluation, but is not enabled as part of the standard CorreLog implementation unless specifically licensed. You should contact your CorreLog account representative to see if you are licensed to execute this product, or to obtain a license to execute.

Overview Of Operation

The ePO adapter software extends the CorreLog system to operate with McAfee ePO within the enterprise. The integration requires ePO Version 4.0, Version 4.5, or Version 4.6 to be installed within the enterprise, and requires the ePO server to be accessible to the CorreLog server. (Note: The ePO adapter supports other versions of ePO also. Contact CorreLog Support for more information.)

At the ePO site, the user configures the system (via the "Registered Executable" function) to forward syslog messages to CorreLog using standard syslog protocol. At CorreLog, the user configures a "Ticket Action" to send ticket information back to ePO when certain (or all) tickets are opened. This configuration enables the following:

- **Correlation of ePO Events**. The software enables CorreLog to monitor event messages, generated by ePO, so that CorreLog can easily correlate security information detected by McAfee with other data on the system. For example, if a Cisco router generates a security event within a few minutes of ePO detecting a virus, then this may indicate a more critical security event.

- **Roll-up of CorreLog Data to ePO.** The software enables CorreLog Server to send ticket information back to ePO, to allow ePO to monitor high-level SIEM events with their dashboards, furnishing a single security console. This information consists of CorreLog "Tickets", and not raw message information, which will reside in CorreLog and not ePO. Note that CorreLog "Tickets" are opened up no faster than once every 10 seconds.

Value Proposition

With the CorreLog ePO adapter software installed, organizations can achieve specific capabilities and value as follows:

1. **Enhanced Security Monitoring For ePO Users.** The adapter software increases the range of ePO to process data from event logs and SNMP traps that may alert the user to security threats that may not otherwise be visible, supporting the ePO role as the central security console for an enterprise.

2. **Enhanced Security Monitoring For CorreLog Users.** The adapter software creases the range of CorreLog to receive important security data from ePO regarding system configuration changes, virus threats, and other anomalies detected by McAfee. This enhances the security monitoring for CorreLog users.

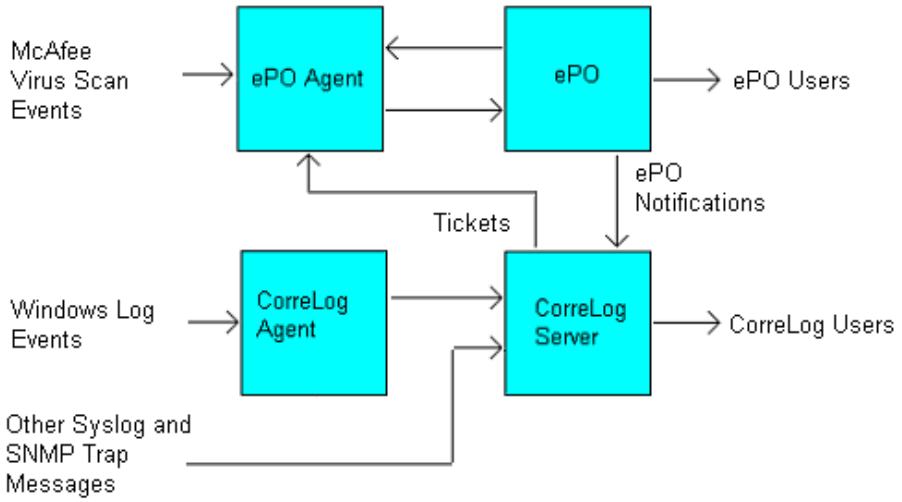
3. **New Abilities to Integrate With A Wider Variety of Devices.** The adapter software increases the types of devices that can be monitored by ePO to include Z/OS mainframe agents, SNMP capable devices, streaming log files, routers and switches, printers, and many other network devices. (CorreLog itself has an extensive API that permits easy integration with a wide variety of devices.)

4. **Enhanced ePO Correlation Capabilities.** The adapter software increases the ability of ePO to correlate internal data, external data, or a combination of these. For example, the CorreLog system can correlate the occurrence of multiple threats, logged at ePO, occurring at a short interval of time, and escalate this by posting a new message to ePO, possibly combined with information from devices that only CorreLog is monitoring.

5. **New Self-Monitoring Capabilities.** The adapter software permits CorreLog to monitor ePO, and permits ePO to monitor CorreLog, furnishing a more robust and failsafe operation.

System Block Diagram

The operation of the ePO software system is depicted and explained below:



As indicated in the above diagram, the adapter software permits bi-directional communication between CorreLog and ePO.

1. The ePO site can send notifications to CorreLog (at a rate up to 2500 events per second). These notifications consist of McAfee Virus Scan events (from the ePO agents) and any other events (such as events generated by other McAfee integration partners.

2. CorreLog accepts these notifications, and opens tickets based upon correlation rules. CorreLog provides specific elements needed to prevent McAfee ePO from being flooded with SIEM information.

3. The content of the ticket information is passed to the ePO agent on the local platform, where it is transparently relayed to the ePO console. The ePO agent, executing on the CorreLog platform, is required middleware.

As indicated in the block diagram, CorreLog can correlate the ePO data with Windows events, and other SNMP events. Likewise, CorreLog can receive events from McAfee virus detection programs. Two separate consoles are available; data can be inspected at the CorreLog console, or the ePO console, or both locations depending upon the operator role.

How To Use This Manual

Section 2 of this manual provides the essential information needed to install and configure the CorreLog ePO software for the various versions of ePO systems. For each version of ePO, a similar (but separate) procedure is required for configuration at the CorreLog server, and the ePO server. These procedures will be required upon initial installation, and if the software is upgraded.

Section 3 of this manual provides more detailed application and operating notes on the adapter software, including information that will be useful to further refine communication, or create specialized action scripts for CorreLog, or provide other customization. This information will mainly be useful to developers or administrators responsible for adapting and customizing the system.

Section 4 of this manual provides additional notes and "use cases" that should be reviewed for applicability, including information on how to modify the baseline configuration (described in Section 2 and Section 3) to achieve specific benefits to the organization. This section should be of interest to all operators and administrators, and will be useful for leveraging the existing infrastructure to achieve maximum advantage from the installation.

Section 2: Software Installation

The CorreLog ePO adapter software is incorporated as a standard part of the CorreLog system. It is enabled in all evaluation versions of the program, and is a separately licensed option in purchased versions of the program.

Additionally, the user can obtain separate version upgrades to the ePO software, available from CorreLog to licensees. This permits existing CorreLog ePO integration sites to be upgraded to newer versions and service packs.

This section provides various different installation procedures, depending upon the version of ePO to integrate with, and the particular functions (message directions) to be implemented at the site. The installer should review the particular installation procedures to determine their applicability. Not all procedures will necessarily be executed, depending upon the site requirements.

Administrative logins are required in order to perform the software installation. The detailed steps needed to perform the installation are provided in the sections that follow.

Installation Requirements

The ePO software is minimally invasive, and can be installed on a variety of platforms and operating systems.

- **Existing CorreLog Server Installation.** Prior to installing the ePO adapter software, the CorreLog Server system must be installed on a Windows platform, as discussed in the CorreLog User Reference Manual.

- **Disk Space Requirements.** The ePO adapter software requires no significant disk space beyond the normal footprint of the CorreLog Server. There is generally no extra disk space load due to this software.

- **CPU Requirements**. The ePO adapter software requires very little extra CPU requirements. The adapter starts no additional free-running processes, hence there is no special CPU or memory requirements associated with the ePO software

- **McAfee ePO Requirements.** The ePO adapter operates with McAfee ePO versions 4.0, 4.5, 4.6, and other versions. Additionally, a McAfee agent should be installed on the platform that is executing CorreLog.

- **Service Port Requirements.** The ePO adapter does not require any additional service ports to be opened. The user should verify at the main ePO server that communications with this agent has been established (such as issuance of a successful agent "wakeup" command.).

Upgrading ePO Adapter Software

Normally, the ePO software is an embedded part of the CorreLog server. It is enabled for all temporary evaluation versions of CorreLog, but is separately licensed for production.

If the user wishes to upgrade the ePO version separately, new versions of the software can be obtained from CorreLog. In this case, the user installs the software upgrade as follows:

1. The ePO Adapter software is obtained from CorreLog support. This will be a self-extracting WinZip file with the name "co-n-n-n-epo.exe" (where n-n-n represents the specific package version.)

2. The user executes the ePO adapter software, and extracts files to the CorreLog root directory (by default the path C:\CorreLog). This upgrades all needed files, including documentation (and this manual.)

After extracting files the administrator should consult the latest documentation for any specific additional steps necessary after installing the software.

Configuring The CorreLog to ePO Interface

The configuration of the CorreLog to ePO message interface is independent of the particular ePO version. This configuration procedure can be performed for all licensed CorreLog sites in order to send ePO tickets to CorreLog. The basic steps consist of configuring the "Ticket Actions" facility to send ePO notifications when tickets are opened and optionally modified and closed. At ePO, the ticket data appears in the "Reporting > Event Log" screen of the system.

Specific configuration steps are as follows:

1. Login to the CorreLog server with an administrative login.

2. Click the "Ticket > Actions" screen. This screen displays the list of actions that are executed when a ticket is opened (or optionally, when closed or modified.)

3. Click the "Wizard" button to run the "Add New Ticket Action" wizard. This wizard guides the operator through the process of adding a new action program to the CorreLog system.

4. On the first screen of the wizard, select the "SEND_EPO" action via the "Action Type" drop down, and click the "Next" button.

   Note: If an error message is displayed when the user clicks the "Next" button, indicating that the site is not licensed to execute the SEND_EPO action, contact CorreLog support for assistance. The SEND_EPO command functions in all evaluation versions of the program, but requires a license for production implementations of the system.

5. Finish the wizard, supplying any additional information. (The operator can elect to use default values in order to send messages to ePO for all tickets opened by the system.

6. When the Wizard is finished, the action will be displayed in the list of ticket actions on the main screen.

Configuring the CorreLog ePO Event Handler

Once the operator has installed the SEND_EPO action, as described in the previous procedure, the user must install the registered extension at ePO to correctly decode CorreLog tickets.

Details of the procedure depends upon whether the operator is working with ePO 4.0, 4.5, or 4.6 (as discussed below.) Specific configuration steps are as follows.

1. Log into the CorreLog server, and download the CorreLog ePO extension software to your current desktop. The software can be accessed via the "More > Extensions" menu in the upper right of each CorreLog screen. The extension will be identified with an "epo" extension and a "zip" suffix, such as "correlog-epo-extension.zip".

   Comment: As an alternative to downloading the ".zip" extension package, the software can also be copied from the "CorreLog/s-doc/EXT" directory of the CorreLog installation. Both techniques for acquiring the extension file are equivalent.

2. Log into the ePO server and upload the extension to the system (which was downloaded to your desktop during the previous installation step.) Click the ePO "Configuration" tab, and then click "Install Extension" to upload and install the extension. The precise ePO screen depends upon the version number of the ePO system. The extension works with ePO Version 4.0, Version 4.5, and Version 4.6. (Other versions may also be supported. Contact CorreLog Support for more information.)

Testing the CorreLog to ePO Interface

After the above configuration steps have been executed, the operator can test the CorreLog to ePO interface rather easily as follows:

1. At the CorreLog site, click on the "Tickets > Open" tab, and then click "AddNew" to manually open a new ticket. Provide an arbitrary message as the content of the ticket (under 128 characters.)

2. At the ePO site, click on the "Reporting" tab, and then click the "Event Log" tab. The ticket text, entered in step 1 above, will appear in ePO within a few minutes (depending upon the reporting rate of the system, configured in the ePO "System" tab.)

   Comment: To expedite reception of the event, the user can click the "Wakeup Agents" menu item under the "More Actions" menu of the ePO "System" screen. This will send a wakeup call to the agent, which will relay the ticket event information to the ePO event log.

Note that a common mistake is to forget to install the McAfee agent on the CorreLog server. CorreLog communicates directly with the McAfee agent (not directly with ePO.) Hence, if no agent is installed on the server, no communication will be possible. The user should verify that the McAfee agent is installed and proper communication between the McAfee agent and ePO exist.

Configuring the ePO to CorreLog Interface

In addition to configuring ePO to receive and decode CorreLog messages, the user can also configure ePO to send messages to CorreLog for logging and correlation. This requires installation of the CorreLog Windows Tool Set at the ePO site, registering of the "sendlog" executable, and configuration of notification rules. The specific steps needed to accomplish this activity are dependent on the particular ePO version. The steps to accomplish this are as follows:

1. Install the Windows Tool Set on the ePO server. (This is accomplished via the same technique as installation on any other server. The user can obtain the Windows Tool Set software from the "Home" screen of CorreLog, and from a variety of other locations on the web.)

2. Register the CorreLog "sendlog" external command via the ePO "Automation" tab. By default, the pathname to the CorreLog "sendlog.exe" program (which is a standard program of the CorreLog Windows Tool Set) is as follows:

   ```
   C:\correlog\wintools\sendlog.exe
   ```

   Comment: You can register an ePO executable ONLY if you are browsing ePO directly from the ePO server. Check ePO documentation for specific usage details.

3. Define an external command that references the external executable above. This is accomplished via the ePO "Automation" tab. The user should place as the first argument the IP address of the CorreLog server. Other arguments can be inserted (placed in double quote marks) that will contain information sent to CorreLog when an ePO event is logged. (See Section 3 for additional notes.)

   A typical example of command line arguments, appropriate for ePO 4.0 installations, is as follows:

   ```
   (correlog-ip-address)
   "ipaddr://{AffectedComputerIPs}
   ePO: {ReceivedThreatNames} {NotificationRuleName}"
   ```

   For ePO Versioins 4.5 and 4.6 a typical command is similar, but uses different "insert" arguments, as follows:

   ```
   (correlog-ip-address)
   "ipaddr://{listOfTargetIPV4}
   ePO: {listOfThreatSeverity} {listOfThreatName}"
   ```

Comment: The value of "(correlog-ip-address)" above will be the IP address where the CorreLog server is currently executing on the network. The above arguments are described in more detail within Section 3 of this manual. The arguments will be constructed by a combination of editing, and inserting variables on the ePO "External Command" screen. The arguments will exist on one line within the notification rule.

4. Add a new ePO "Notification Rule" to the system that executes the external command (defined above) based upon user-selected criteria. As part of the configuration, click the "Test" button to send a test message to CorreLog, and verify that data was properly received.

Note that a common mistake occurs in Step 3 of the above procedure, where the IP address argument of the "sendlog" command is omitted, or the text of the argument message is not enclosed in double quote marks. The standard syntax of the CorreLog "sendlog.exe" utility is as follows:

```
Sendlog.exe (to-addr) "(message)" (priority) (facility)
```

The user can execute the "sendlog.exe program at a command line prompt to see the brief help. The optional "(priority)" and "(facility)" for messages can be included in the command. The user can define multiple notification commands (such as "correlog-info" and "correlog-warning") that affect the particular priority of the message sent to CorreLog.

If communication fails between the sendlog.exe program and the CorreLog server, the command should be checked at a command prompt, and any issues associated with sending UDP messages to 514 should be resolved. The "sendlog" program communicates with CorreLog on the standard UDP service port of 514, which should not be blocked by firewalls on either machine.

Configuring the ePO SNMP Trap Interface

As an alternative to the above procedure, the operator can configure the SNMP Trap interface of ePO to send SNMP traps to CorreLog. This provides the same basic information as the "sendlog" registered executable described above, but sacrifices the flexibility of the "sendlog" command for simplicity of setup. The particular steps needed to send an SNMP trap to CorreLog is defined in the ePO help documentation. Note that CorreLog receives standard SNMP traps, and by default accepts any trap community. (SNMP traps, although in a different format from Syslog messages, are handled precisely the same as Syslog messages in every way within CorreLog.) The resulting message will contain all the user defined text arguments as regular variable bindings to the trap message, in a format suitable for correlation and reporting.

Section 3: Software Operation

This section provides a description of these optional software elements, their usage, and other considerations. Once the ePO software is configured as described in Section 2, the user will be able to collect ePO events as regular event data, and will be able to send event data to ePO in the form of correlated events.

The software adapter can be viewed as having two complimentary but separate functions:

1. **Data Reception of ePO Events.** CorreLog will collect the ePO data, which provides status information on all the McAfee agents on the network. This will provide substantial visibility into the virus protection of the enterprise, as well as useful status information regarding each managed node.

2. **Correlating and Transmitting Events To ePO.** CorreLog can transmit data into the ePO event log, providing a marker of significant events on all the collected data (including any data collected from McAfee, as well as data from other devices.) This provides a way of annotating the ePO event log with information, leveraging the notification facilities of ePO.

The narrative of this section reflects this dual functionality. The operator can use either (or both) of these functions to provide extra security management for the enterprise. The CorreLog ePO adapter software is flexible, and can be configured to perform a variety of special functions as described in this section.

Reception of ePO Events By CorreLog

McAfee ePO sends events using the standard CorreLog "sendlog.exe" program, which is installed on the ePO server via the CorreLog Windows Tool Set (as documented in Section 2.) When ePO sends events to CorreLog, they are handled in a fashion identical to any other event.

Within ePO, the user configures the "sendlog.exe" program by first creating a registered executable program, then creating and external command, and then assigning the external command to a notification rule.

The user configures arguments to the sendlog.exe-registered executable via the ePO "Insert Variable" function, when defining the external command. The variables are substituted with event and ePO data before the "sendlog" command is executed, furnishing the ability to precisely define the data items that appear as part of the CorreLog message. Various variables are possible, as listed listed below.

Pull-down Name	Inserted Variable Name	Description
Actual categories	ReceivedEventCategories	This argument contains the official category of the ePO event.
Actual number of events	ReceivedNumEvents	This argument indicates the number of received events (typically the value "1").
Actual number of systems	ReceivedNumComputers	This argument indicates the number of computers participating in the event (typical the value "1").
Actual products	ReceivedProductFamilies	This argument indicates the product that generated the event.
Actual threat or rule names	ReceivedThreatNames	This is the threat name, useful for identifying the nature of the event message. This value is typically passed to the registered executable.

Additional information	AdditionalInformation	This argument contains any additional information associated with the event (typically "Not Available").
Affected objects	AffectedObjects	This argument contains the name of the affected objects (typically "Not Available").
Affected systems IP addresses	AffectedComputerIPs	This argument contains the IP address of the originating machine. This argument is often passed with the "ipaddr://" prefix. (See additional notes below).
Affected systems names	AffectedComputerNames	This argument contains the official hostname of the originating machine, corresponding to the IP address (above)
Event descriptions	EventDescriptions	This contains an event description, if available.
Event IDs	EventIDs	This argument contains the numeric event ID for the event (if available).
First event time	FirstEventTime	This argument contains the date and time of the event.
Notification rule name	NotificationRuleName	This argument contains the name of the notification rule that was triggered.
Rule defined at	BranchNodePath	This argument contains where the rule is defined within ePO.
Rule group	SiteNodeName	This argument contains the name of the group where the rule is defined (such as "My Organization").

Selected categories	ConfiguredEventCategories	This argument contains the matching event categories (typically "Any")
Selected products	ConfiguredProductFamilies	This argument contains the selected product families (typically "Any")
Selected threat or rule name	ConfiguredThreatName	This argument contains the selected thread or rule name (typically "Any")
Source systems	SourceComputers	This argument contains the source systems for the event (typically "Not Available").
Time notification sent	TimeNotificationSent	This argument contains the date and time when the notification was actually sent, which may be slightly delayed from the event time.

Comment: The arguments documented in the above table are for ePO Version 4.0, and also related to Version 4.5 and 4.6. The above information is not intended to be authoritative information, but only to clarify the discussion. The operator should consult McAfee documentation for information specific to the ePO version and patch level currently being used at the installed site.

Note that the name of the insert variable within the pull-down menu (i.e. the first column of the above table) may not precisely match the name of the inserted variable (i.e. the second column of the above table). Also note that not all inserted values are useful.

Basic ePO External Command Arguments

To get started, the user can configure the command line option such as the following (which are typical of ePO implementations):

```
(correlog-ip-address)
"ipaddr://{AffectedComputerIPs}
ePO: {ReceivedThreatNames} {NotificationRuleName}"
```

The above command line argument, including the (correlog-ip-address) is entered on a single line using a combination of manual editing and inserting of variables. The construction of the message is explained as follows:

1. The first argument is the IP address of the CorreLog Server, and indicates to the "sendlog.exe" program where messages are to be sent. This value is hardcoded in this location, but will generally never change. This value must be followed by a single blank space.

2. The second argument (enclosed in double-quote marks) is the message to send. It contains an "ipaddr://" prefix, which causes CorreLog to list the message as coming from the Affected Computer IP address. The message contains the "ePO:" keyword (useful for correlation), the name of the threat, and the notification rule that is activated by the event.

The "ipaddr://" prefix is a simple operator that works with CorreLog to identify the IP address of the event device. The prefix must be immediately followed by the {AffectedComputerIPs} variable, with no space. Following the prefix and IP address should be a single space to delimit the start of the message that is actually displayed by CorreLog.

If the "ipaddr://" prefix is omitted, the messages will be listed in CorreLog as coming from the ePO server, and not the actual affected device. This does not necessarily degrade the correlation capabilities, but the user will not be able to catalog messages automatically by the IP addresses of the affected devices.

Creating Threads, Tickets, and Alerts

The basic method for correlating ePO messages is no different that the techniques discussed elsewhere. The basic steps are provided below.

1. The operator creates a thread to tabulate the messages sent by the ePO using the "Correlation > Threads > Add New" screen. This screen is used to collect all the messages of a particular type or characteristic. For example, the user may wish to create a single "All EPO Messages" thread, which keys off the keyword "ePO" (which is incorporated into the external command line arguments.)

2. The operator creates an Alert for the thread counter using the "Correlation > Alerts > Add New" screen. This alert will send a Syslog message back to the main list of messages when one or more messages are received during an interval of time. As is always the case, when an alert is triggered, a single message is sent back to CorreLog, and a single ticket is opened while the alert is set. (See additional notes below.)

3. The operator optionally identifies an "Assignee" for the alert via the "Correlation > Alerts > Add New" screen. This causes a ticket to be opened on the system, and assigned to a particular user or a ticket group. The user can assign a ticket to any existing user, or ticket group.

4. The operator optionally adds a "Ticket Action" to the system, which sends e-mail (or performs some other action) when a new ticket is opened on the system, providing a real-time indication that a timeout threshold of the Ping Monitor software has been violated. This message will typically contain the descriptive text entered by the operator when the alert was created, which may be slightly (or totally) different than the originating Ping Monitor message.

As a special note, the "Auto-Learn" function for the alert should probably be disabled to prevent the message threshold and alert interval from changing automatically.

Sending CorreLog Ticket Messages To ePO

Just as McAfee ePO can send events to CorreLog, the CorreLog server can send events to McAfee, which will annotate the ePO Event Log. This provides a method of annotating the ePO event data with information that contains a wider selection of data from devices that are not necessarily managed directly by ePO. In particular, this allows ePO to serve as the end-point collector for high-level Security Information and Event Management (SIEM) data.

Messages are sent from CorreLog to McAfee using the CorreLog "Tickets" facility, which creates actionable data items from correlated data results. Tickets are actually the highest-level of correlation provided by CorreLog, associating a group of correlated messages to an assignee. The architecture of the Tickets facility prevents CorreLog from posting data to ePO at a high rate; typically CorreLog opens a ticket every few minutes (as opposed to receiving thousands of messages per second.) Therefore, the event messages that CorreLog posts to ePO can be very pertinent to network security.

The software needed to send events to ePO is built into each copy of CorreLog, is available with evaluation licenses and separate production licenses.

CorreLog Ticket to ePO Field Mapping

When sending Ticket data to ePO, all mapping between CorreLog and McAfee is performed in the SEND_EPO.bat file, residing in the "t-actions" directory of the CorreLog root folder. Like other ticket action folders, the system executes the ticket action file, first instantiating a series of environmental variables with CorreLog data. The SEND_EPO.bat file passes these variables to the McAfee agent running on the platform (via the "send_to_ePO.exe" program, residing in the "Correlog\system" directory.)

The SEND_EPO.bat file does not require user modification, and is preconfigured for reasonable and useful event data. However, the mapping can be changed to

modify the mapping using a standard text editor. The specific mapping between fields is documented in the Appendix of this document.

Note that the operator can implement multiple instances of SEND_EPO, and can create modified versions of the SEND_EPO.bat file, each of which contains mappings appropriate to a particular message type. Refer to the Appendix of this manual for more information.

Sending Other CorreLog Messages To ePO

The normal function for CorreLog is to send ticket information to ePO. This prevents CorreLog from flooding ePO with more messages than it can conveniently handle. (The McAfee specification requires no more than five events per minute, on average, to be posted.) The ticket action facility specifically supports these McAfee requirements.

It is possible for users to adapt the "SEND_EPO.bat" file to send messages when specific messages are received, without passing through the ticket facility. This is a straightforward adaptation of the "t-actions\SEND_EPO.bat" file, to create an "actions\SEND_EPO.bat" file. The new action (residing in the CorreLog "actions" directory) can then be added to the system via the "Correlation > Actions" screen as a user-defined program. If the user adds this value, caution should be taken to select match patterns that prevent the ePO system from being flooded with event messages..

The "CorreLog > System > Scheduler" screen can also send messages to ePO, such as on CorreLog system startup and shutdown, or at periodic intervals (such as to create a heartbeat function to indicate that CorreLog is still alive.) The user simply creates a batch file that launches the "system\send_to_ePO.exe" program, and then configures the scheduler to launch this program. This will notify ePO when CorreLog is available, or not.

The "send_to_ePO.exe" program, which performs the actual relaying of information to the ePO server, resides in the "system" directory, and accepts a single argument that points to a file containing the field names and values, where the field names are documented in the previous table. The syntax of this command is as follows:

```
Send_to_ePO.exe –f (filepath)
```

The user can construct a batch file that dynamically creates (filepath) with directives, and then launches the send_to_ePO.exe executable. The file is read, processed, and the information is sent to the McAfee agent running on the CorreLog platform. Within a few minutes (or after an agent "wakeup") the information will appear on the McAfee ePO "Event Log" screen of the system.

Section 4: Application Notes

The integration of the CorreLog server with ePO creates a single unified system that monitors both the Virus protection functions of the network, as well as tracking users to enhance the overall network security.

CorreLog is highly compatible with McAfee ePO, and provides an easy way of significantly enhancing an organization's existing software investment. As indicated in previous sections, CorreLog provides multiple integration points with ePO and supports a variety of easy-to-implement integration strategies.

CorreLog can immediately contribute to the management of an ePO site, furnishing a robust and unique technology offering to enhance security monitoring, permit long life-cycle, and provide pro-active defense and information assurance, needed to support compliance standards such as PCI/DSS, HIPAA, FISMA, and other security standards.

This final section provides additional notes and use cases for the ePO adapter software. This information will be useful for administrators looking to leverage their investment in McAfee ePO, as well as CorreLog administrators seeking to add new data sources and capabilities to the program.

Use Cases

The results of this implementation provide new functionality to both CorreLog and ePO users, expanding the role of these systems to efficiently manage the security of an enterprise in a simplified and robust manner. This is accomplished by creating a tightly coupled software system that presents a homogeneous view of a possibly heterogeneous environment.

Typical "use cases" for the integration, based upon the value propositions given in Section 1, are as follows:

1. **Enhanced Security Monitoring For ePO Users.** A CorreLog managed device experiences a security event, which opens a ticket in CorreLog. (CorreLog is monitoring the mainframe via the CMA adapter.) At ePO, the user can see the ticket opened in the event log, and can obtain details about the ticket and original message via a reporting screen or the dashboard.

2. **Enhanced Security Monitoring For CorreLog Users.** McAfee ePO indicates multiple instances of policy changes, virus detection, or other built-in events. These events are sent to CorreLog, which opens a ticket, possibly correlating this data with other data on the system. (The ticket indication can optionally be sent back to McAfee, to annotate the ePO event log.)

3. **New Abilities to Integrate With A Wider Variety of Devices**. CorreLog monitors the security of Cisco routers, UNIX Platforms, Mainframes, Firewalls, Cisco MARS, and other devices through the various adapters, including the SNMP adapter, Ping Adapter, and POP3 Adapter. As security threats are detected, CorreLog opens tickets and sends this indication to McAfee, where it is displayed on a dashboard. Likewise, any device or application that is managed by McAfee is available to CorreLog.

4. **Enhanced ePO Correlation Capabilities.** Several SIA partner send and event indications to ePO during a short interval of time, related to various managed device that only that SIA partner has visibility to. CorreLog receives the various event indications, provides correlation functions across the various SIA partners, and opens a ticket for the CorreLog administrator indicating this relates to some other network problem detected by CorreLog. (The ticket indication can optionally be sent back to McAfee, to annotate the ePO event log.)

5. **New Self-Monitoring Capabilities.** CorreLog monitors the ePO status, opens a ticket to the CorreLog administrator should ePO fail or begin generating errors. Likewise, ePO monitors the status of CorreLog, and

sends notifications to the ePO administrator should CorreLog experience problems or be compromised.

CorreLog Severity Mapping

CorreLog generates severities from 0 (Emergency) to 7 (Debug). McAfee CreateEventElement requires severities from 0 (Informational) to 4 (Critical). The precise mapping between these two severity types, when generating the XML data, is automatically mapped for the user, and cannot be modified.

XML Data Files

Basic operation of the McAfee SDK is as follows: The "send_to_ePO.exe" program generates an XML data file, which is queued to the McAfee Agent program running on the platform in the following directory:

```
C:\Documents and Settings\All Users\Application Data\
McAfee\Common Framework\AgentEvents
```

When a ticket is opened, the operator can inspect the above directory to see the XML file that contains the ticket information. When the XML data file is read by the McAfee agent, the XML file is deleted.

The agent sends the data contained in the XML file to the McAfee ePO server, where it is parsed using an event parser, and placed in the McAfee event database. The resulting event appears in the "Reports > Event Log" screen of the ePO web interface.

1. All CorreLog-defined XML tags begin with the keyword "CorreLog", for example, CorreLogDateTime. XML tag name constants, in both the agent and the DLL, will be named with the tag prepended with "xml", for example, const char xmlCorreLogDateTime[] = “CorreLogDateTime”;.

2. Variable XML data will be passed in a file named on the "send_to_epo.exe" command line following the –f flag, for example, -f ..\to_ePO.txt. The file will consist of pairs of the format *value_name*: *“value*”, for example DATE_TIME: “2011-03-25 19:55:25”.

3. The name: “value” pairs may be separated by one or more white space characters such as blanks, tabs, and newlines; and/or commas. Note that all variables must be quoted, and may not contain embedded quotes.

4. The constants, in both the Agent and the DLL, will have names beginning with key…, dropping the _’s, and in CamelCase, for example, const char keyDateTime[] = “DATE_TIME”;

Appendix: Event Field Mapping

When CorreLog data is sent to ePO, the CorreLog data items are mapped to ePO data in the SEND_EPO.bat file, found in the "t-actions" folder of the CorreLog installation. Generally, this file does not need to be modified and is appropriate for all installations.

For advanced users, who want to enhance or tailor the actions of the SEND_EPO.bat file, a description of how data items are mapped is provided in the table that follows. Further assistance is available from CorreLog support.

Heading on ePO Detail Panel	**Format and Maximum Length**	**.BAT File Key (Keys are *not* case-sensitive)**	**Suggested or Default CorreLog Environment Variable or Value**	**Notes**
Event Generated Time (UTC):	2011/04/26 15:05:34	CorreLog LocalTime	x_DATE_TIME	Converted to UTC by send_to_ePO. Defaults to current date and time. Caution: event will not display in ePO console unless this time is within the range indicated by “Filter:”
Detecting Product Version:	Char 20	Analyzer Version	Currently “3.5.0”	

Heading on ePO Detail Panel	Format and Maximum Length	.BAT File Key (Keys are *not* case-sensitive)	Suggested or Default CorreLog Environment Variable or Value	Notes
Detecting Product Host Name:	Char 128	Analyzer HostName		
Detecting Product MAC Address:	Char 16	Analyzer MAC		
DAT Version:	Char 20	Analyzer DATVersion		
Engine Version:	Char 20	Analyzer Engine Version		
Threat Source Host Name:	Char 128	Source HostName		
Threat Source IPv4 Address:	127.0.0.1	SourceIPV4		If supplied, must be a valid dotted address.
Threat Source MAC Address:	Char 16	SourceMAC		
Threat Source User Name:	Char 128	SourceUser Name	x_ASSIGNED_ TO	
Threat Source Process Name:	Char 128	Source ProcessName		
Threat Source URL:	Char 1024	SourceURL	x_EXTURL	Need not be an actual URL
Threat Target Host Name:	Char 266	Target HostName		
Threat Target IPv4 Address:	127.0.0.1	TargetIPV4	x_RELATED_ ADDRESS	If supplied, must be a valid dotted address.
Threat Target MAC Address:	Char 16	TargetMAC		
Threat Target User Name:	Char 128	TargetUser Name	x_RELATED_ DEVNAME	
Threat Target Port Number:	Numeric	TargetPort		
Threat Target Network Protocol:	Char 16	Target Protocol		
Threat Target Process Name:	Char 128	Target ProcessName	x_COMMENT	
Threat Target File Path:	Char 266	Target FileName	x_MESSAGE	

<table>
<tr><th>Heading on ePO Detail Panel</th><th>Format and Maximum Length</th><th>.BAT File Key (Keys are not case-sensitive)</th><th>Suggested or Default CorreLog Environment Variable or Value</th><th>Notes</th></tr>
<tr><td>Event Category:</td><td>Char 128</td><td>Threat Category</td><td>x_FACILITY</td><td>ePO displaysfield in parentheses. Defaults to “n/a”</td></tr>
<tr><td>Event ID:</td><td>See notes at right.</td><td>CorreLog EventType</td><td></td><td>Maps to Event ID as follows:
<table><tr><th>CorreLog Event Type</th><th>Event ID</th></tr><tr><td>TICKET</td><td>201451</td></tr><tr><td>MESSAGE</td><td>201452</td></tr><tr><td>INTERNAL</td><td>201453</td></tr><tr><td>USER</td><td>201454</td></tr><tr><td>Any other</td><td>201450</td></tr></table></td></tr>
<tr><td>Threat Severity:</td><td>Numeric</td><td>Threat Severity</td><td>x_SEVERITY_ NUMBER</td><td>Must be in range 0 to 7.</td></tr>
<tr><td>Threat Name:</td><td>Char 128</td><td>ThreatName</td><td>x_SUMMARY</td><td>Defaults to “n/a”</td></tr>
<tr><td>Threat Type:</td><td>Char 32</td><td>ThreatType</td><td>"CorreLog Ticket" or "CorreLog Message"</td><td>Defaults to “n/a”</td></tr>
<tr><td>Action Taken:</td><td>Char 24</td><td>ThreatAction Taken</td><td>x_STATUS</td><td>Defaults to “n/a”</td></tr>
<tr><td>Threat Handled:</td><td>Char 20</td><td>CorreLog State</td><td>x_STATE</td><td>If equal to “closed” (case-insensitive) sets ThreatHandled to true; else sets to false</td></tr>
<tr><td>Analyzer Detection Method:</td><td>Char 128</td><td>Analyzer Detection Method</td><td></td><td>Available for test.</td></tr>
</table>

For Additional Help And Information…

Detailed specifications regarding the CorreLog Server, add-on components, and resources are available from our corporate website. Test software may be downloaded for immediate evaluation. Additionally, CorreLog is pleased to support proof-of-concepts, and provide technology proposals and demonstrations on request.

CorreLog, Inc., a privately held corporation, has produced software and framework components used successfully by hundreds of government and private operations worldwide. We deliver security information and event management (SIEM) software, combined with deep correlation functions, and advanced security solutions. CorreLog markets its solutions directly and through partners.

We are committed to advancing and redefining the state-of-art of system management, using open and standards-based protocols and methods. Visit our website today for more information.

CorreLog, Inc.
http://www.CorreLog.com
mailto:support@CorreLog.com

Alphabetical Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X

CorreLog, Inc.
http://www.correlog.com