TREND MICRO™

9.5 Deep Security

SOAP Web Service API

Advanced Protection for Physical, Virtual, and Cloud Servers

Cloud & Data Center

Complete End User

Cyber Threats

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://downloadcenter.trendmicro.com/

Document Part No.: APEM95865_130213

Version 1.0

Release Date: May 2014

The user documentation for Trend Micro Deep Security introduces the main features of the software and installation instructions for your production environment. Read through it before installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Contents

What Is Trend Micro Deep Security 9.5?

Trend Micro™ Deep Security™ 9.5 is a server and application protection software that allows systems to become self-defending. Deep Security Agent is deployed on physical servers and virtual machines to provide comprehensive protection, including:

- Firewall Intrusion Detection and Prevention (IDS/IPS)
- Web Application Protection
- Application Control
- Integrity Monitoring
- Log Inspection

All Deep Security Agents are centrally managed by Deep Security Manager.

What Are Web Services?

To assist in deployment and integration into customer and partner environments, Trend Micro has developed a SOAP Web Service API that is exposed by Deep Security Manager. This allows for an easy, language-neutral method to externally access data and programming configurations.

Audience

This document is targeted at customer and partner system integrators, and customization developers. A typical application of the Web Service API would be to integrate Deep Security into existing configuration and control management systems, or collection of events. It is assumed that the reader is familiar with Trend Micro Deep Security, software development in a recommended language, and the concepts and terminology described in the Terminology section.

Terminology

Term	**Description**
Web Service	Web Services is defined as an application programming interface (API) used to remotely access service-exposed information and functionality that is executed on the remote system hosting the Web service. It is a collection of web methods assembled into a service.
WSDL	Web Service Definition Language (WSDL) is defined by the Web Service as the source for all knowledge of the service-available functionality. Web Service development tools will consume the WSDL and automatically generate the client-side code required to build a Web Service client for that service.
Web Method	A function of the Web Service called from the client that is executed by the service as a remote call.

SOAP

SOAP (Simple Object Access Protocol) is a protocol specification for exchanging structured information in the implementation of Web Services. Its message format is based on XML and relies on other protocols for message communication between client and server.

HTTP

HTTP is a request/response message standard for client/service communication used by Internet browsers and web servers.

HTTPS

HTTPS is a combination of HTTP and the SSL/TLS protocol. This allows for encrypted communication between HTTP client/service partners.

IDE

Integrated Development Environment (IDE) is a development tool used for designing, developing, compiling, and debugging software application.

Getting Started

The basic steps to getting started with the Web Service API are as follows:

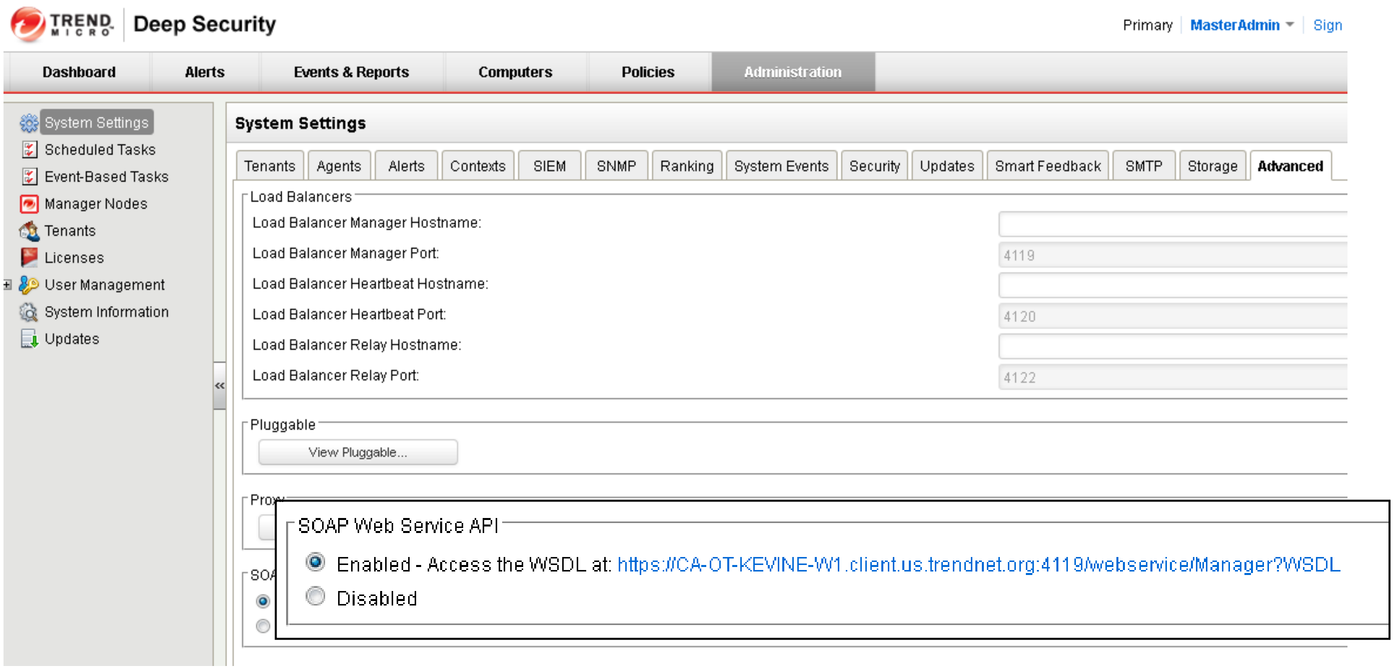
1) Enable the Web Service API.
2) Create an administrator account that an external Web Service client can utilize.
3) Obtain the Web Service WSDL and SSL Certificate.
4) Develop an external Web Service client to communicate with Deep Security Manager.

Enabling the Web Service API

1) Open an Internet browser and connect to the Deep Security Manager:

   https://<hostname/IP>:4119

2) Navigate to **Adminstration-> System Settings**, and select the **Advanced** tab.
3) Select **Enabled** under SOAP Web service API, then click **Save**.



Load Balancers

Load Balancer Manager Hostname:	
Load Balancer Manager Port:	4119
Load Balancer Heartbeat Hostname:	
Load Balancer Heartbeat Port:	4120
Load Balancer Relay Hostname:	
Load Balancer Relay Port:	4122

Pluggable

SOAP Web Service API

● Enabled - Access the WSDL at: https://CA-OT-KEVINE-W1.client.us.trendnet.org:4119/webservice/Manager?WSDL

○ Disabled

Creating a Web Service Administrator Account

Deep Security Manager allows for powerful role-based access, including settings to control if an administrator account may access the Web Service API or Manager user interface. For security reasons, it is recommended that a new administrator account and a new Web Service-specific role be created.

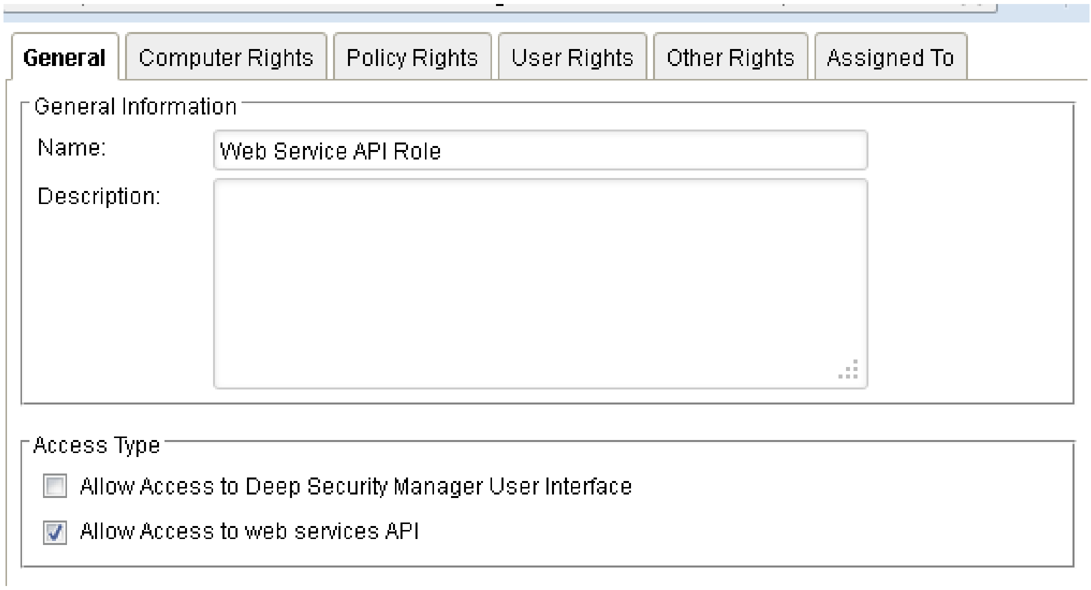
The Web Service API enforces all other Role access controls, such as Computer Rights, Security Profile Rights, and User Rights. If a Role is created for the Web Service API that only permits Computers of a certain Computer Group to be viewable, then a Web Service client using that administrator will only be able to access the specified Computer Group.

To create a new Role for Web Service only access, complete the following steps:

1) Open an Internet browser and connect to the Deep Security Manager:

   https://<hostname/IP>:4119

2) Navigate to **Administration -> User Management -> Roles**, and click **New..**.
3) Create the Role as normal, but de-select "Allow Access to Deep Security Manager User Interface" and select "Allow Access to Web Service API".
4) When all other configuration is complete, click **Save**.



General Information

Name: Web Service API Role

Description:

Access Type

□ Allow Access to Deep Security Manager User Interface

☑ Allow Access to web services API

5) Navigate to **User Management -> Users**, and click **New**.
6) Create a new administrator for use only with the Web Service API. Assign the new Role previously created to this administrator.

Make note of the new administrator account username and password.

Obtaining the Web Service WSDL and SSL Certificate

All Web Service SOAP implementations will require the target Web Service WSDL file. The WSDL is used to automatically generate source code that can be used for developing the Web Service client application. Additionally, the respective SOAP implementation will need to reconcile the fact that HTTPS communication is required between the client application and the Deep Security Manager Web Service. Typically this means that the Deep Security Manager SSL certificate will need to be imported in the trusted X.509 certification used by the SOAP implementation. For example, Microsoft Visual Studio requires that the SSL certificate be imported into the Windows certificate store on each Windows platform that the client application will run on. For Java Axis, the Java Key Store is used and can be easily copied with the client application to each platform that the client application will run on. Alternatively there is the option to develop an alternative certificate validation policy implementation to bypass this default requirement.

To download the Web Service WSDL file, complete the following steps:

1) Open an Internet browser and connect to the Deep Security Manager Web Service URI:

   https://<hostname/IP>:4119/webservice/Manager?WSDL

2) Save the document as Manager.wsdl:

   c:\work\DeepSecurityWebServices\Manager.wsdl

There are many ways to retrieve an installed Deep Security Manager's public certificate. The following is one method using Firefox:

1) Launch Firefox and connect to the Deep Security Manager web page.
2) Double-click on the Lock icon next to the address.
3) Click **More Information**.
4) Click **View Certificate**.
5) Click the **Details** tab.
6) Click **Export...**
7) Export the certificate as "X.509 Certificate (DER)".
8) Save it as Manager.cer.

   c:\work\DeepSecurityWebServices\Manager.cer

Developing a Web Service Client Application

Using a programming language that supports SOAP (http://en.wikipedia.org/wiki/SOAP) over HTTP standard, a client application can be developed to make remote calls to Deep Security Manager. The language chosen should be the conclusion of familiarity, suitability for the task at hand, and language compatibility for the intended integration. Apache Axis works well and is the native implementation of the Web Service itself. The Microsoft .Net Framework's support for Web Services through Visual Studio is a very robust choice. Here is a list of potential SOAP Web Service implementations that can be used:

- C#/VB.NET/Managed C++ using .NET Framework
  http://msdn2.microsoft.com/en-us/netframework/default.aspx

- Java using Apache Axis
  http://ws.apache.org/axis/java/index.html

- C++ using gSOAP
  http://www.cs.fsu.edu/~engelen/soap.html

- C++ using Apache Axis
  http://ws.apache.org/axis/cpp/index.html

- PHP using PEAR
  http://pear.php.net/package/SOAP

- Ruby using soap4r
  http://dev.ctor.org/soap4r

- Perl using SOAP:Lite
  http://www.soaplite.com/

- CORBA using SOAP2CORBA
  http://soap2corba.sourceforge.net/

- Python using Python Web Services
  http://pywebsvcs.sourceforge.net/

Once the selected development environment has been configured, the SOAP implementation will require that the Deep Security Manager WSDL be added and source code generated from it before development can begin. For example, with Microsoft Visual Studio a new Project can be created, and the Manager WSDL file can be added as a new Web Reference, with Apache Axis for Java leverage ANT and the wsdl2java task in order to generate Java code from the WSDL file.

Next, the respective SOAP implementation will have support for HTTPS communication, which requires that the Deep Security Manager SSL certificate be imported into a supported key store container. For Microsoft Windows and Visual Studio, this is the Windows Certificate Store. To import the certificate, it can be double-clicked on the Web Service client application machine, and imported as trusted. For Java and Apache Axis, the SSL certificate will need to be imported into the JDK/JRE “cacerts” key store using the Java keytool command that is included with the JDK/JRE.

For more information on how to import a SSL certificate, or how to use HTTPS support for the respective SOAP implementation, consult the SOAP implementation documentation.

For more examples on how to develop with the Deep Security Manager Web Service API, see the Trend Micro Deep Security Web Service sample package. It can be obtained from a Trend Micro sales or support representative.

Web Service API Capabilities

The Deep Security Manager Web Service API enables customers and partners to:

- Retrieve configuration and event information
- Create, update and delete configuration settings
- Initiate a Manager operation

What Is Possible?

Although the Web Service API endeavors to implement as many Deep Security Manager features as possible, not all functionality that is available in the Deep Security Manager interface is necessarily available through the Web Service API. The following list details the high level functionality, grouped by major category, which is possible with the Web Service API.

Dashboard

- Retrieve counters for dashboard widgets
- Retrieve feature summary for the system
- Retrieve an overall computer and alert status for the system

Computers

- Retrieve Computers
- Add/Update a computer
- Delete a Computer
- Activate a Computer
- Deactivate a Computer
- Lock a Computer
- Unlock a Computer
- Retrieve Computer status
- Initiate Computer "Update Now" operation
- Initiate Computer "Get Events Now" operation
- Initiate Computer Agent software upgrade operation
- Assign Computer to a Security Profile
- Un-assign Computer from a Security Profile
- Get System settings configured at the Computer level
- Set(override) System settings configured at the Computer level
- Clear System settings configured at the Computer level

Groups

- Retrieve Groups
- Add/Update a Group
- Delete a Group
- Move a Computer to a Group

Security Profile

- Retrieve Security Profiles
- Add/Update a Security Profile
- Edit a Security Profile
- Delete a Security Profile
- Set Firewall/DPI/Integrity Monitoring/Log Inspection state at Security Profile level
- Assign Firewall/DPI/Integrity Monitoring/Log Inspection rules at Security Profile level
- Unassign Firewall/DPI/Integrity Monitoring/Log Inspection rules at Security Profile level
- Get System setting configured at the Security Profile level
- Set(override) System settings configured at the Security Profile level
- Clear System settings configured at the Security Profile level

Anti-Malware

- Retrieve Anti-Malware events
- Retrieve Anti-Malware configurations
- Add/Update Anti-Malware configurations
- Delete Anti-Malware configurations
- Add/Update Directory Lists
- Delete Directory Lists
- Add/Update File Lists
- Delete File Lists
- Add/Update File Extension Lists
- Delete File Extension Lists

Web Reputation

- Retrieve Web Reputation events
- Retrieve Web Reputation configurations *
- Add/Update Web Reputation configurations *
- Delete Web Reputation configurations *

These operations are performed with the system setting APIs and not via dedicated APIs.

Firewall

- Retrieve Firewall events
- Retrieve Firewall rules
- Add/Update Firewall rule
- Edit Firewall rule
- Delete Firewall rule
- Retrieve Stateful Configurations
- Add/Update Stateful Configurations
- Edit Stateful Configurations
- Delete Stateful Configurations

Deep Packet Inspection

- Retrieve DPI events
- Retrieve DPI rules
- Add/Update DPI rule
- Edit DPI rule
- Delete DPI rule
- Retrieve Application Types
- Add Application Types
- Edit Application Types
- Delete Application Types
- Retrieve Application Type Overrides
- Add Application Type Overrides
- Edit Application Type Overrides
- Delete Application Type Overrides

Note that only user-created Application Types can be modified or deleted. Application Types issued by Trend Micro are read-only.

Note that Application Type Overrides are only supported at the Security Policy level, not the Computer level.

Integrity Monitoring

- Retrieve Integrity Monitoring events
- Retrieve Integrity Monitoring rules
- Add/Update Integrity Monitoring rules
- Edit Integrity Monitoring rules
- Delete Integrity Monitoring rules
- Initiate Computer "Scan For Integrity Changes" operation
- Initiate Computer "Rebuild Baseline" operation

Log Inspection

- Retrieve Log Inspection events
- Retrieve Log Inspection rules
- Add/Update Log Inspection rules
- Edit Log Inspection rules
- Delete Log Inspection rules
- Retrieve Log Inspection Decoders
- Add/Update Log Inspection Decoder
- Edit Log Inspection Decoder
- Delete Log Inspection Decoder

IP Lists

- Retrieve IP Lists
- Add/Update IP list
- Edit IP lists

- Delete IP lists

MAC Lists

- Retrieve MAC Lists
- Add/Update MAC list
- Edit MAC lists
- Delete MAC lists

Port Lists

- Retrieve Port Lists
- Add/Update Port list
- Edit Port lists
- Delete Port lists

Schedules

- Retrieve Schedules
- Add/Update Schedules
- Edit Schedules
- Delete Schedules

System

- Retrieve System Events
- Get System(global) settings
- Set System(global) settings
- Retrieve System Information

License

- Retrieve License
- Update License

Updates

- Retrieve Security Center customer account
- Set Security Center customer account
- Test Security Center customer account
- Import Security Update from file
- Retrieve stored Security Updates
- Apply stored Security Update
- Export stored Security Update
- Delete stored Security Update
- Retrieve stored Agent/Appliance software
- Export stored software
- Delete stored software

What is Not Possible?

The Deep Security Manager Web Service API is missing capabilities required to provide for the following notable functionality.

Alerts

- Retrieve Alert
- Dismiss Alerts

Reports

- Generate Reports

Computers

- Edit Computer general information
- Initiate “Scan for Recommendations” operation
- Clear Recommendations
- Create Diagnostic Package
- Configure Computer interface settings
- Edit Firewall/DPI/Integrity Monitoring/Log Inspection state at Computer level
- Assign Firewall/DPI/Integrity Monitoring/Log Inspection rules at Computer level
- Override Firewall/DPI/Integrity Monitoring/Log Inspection rule configurations at Computer level
- Override Application Type Properties at Computer level

Groups

- Add vCenter
- Configure Directory/Sync with LDAP

Security Profile

- Select "Real Time" Integrity Monitoring state at Security Profile level
- Override Firewall/DPI/Integrity Monitoring/Log Inspection rule configurations at Security Profile level

Anti-Malware

- Retrieve or operate on quarantined files

Firewall

- Assign Context to a rule

Deep Packet Inspection

- Edit[configuration] of Security Update downloaded DPI rules
- Assign Context to a rule
- Configure SSL certificates
- Modify or delete Application Types issued by Trend Micro.

Integrity Monitoring

- Select "Real Time" Integrity Monitoring state
- Edit [configuration] of downloaded Integrity Monitoring rules
- Assign Context to a Integrity Monitoring rule

Log Inspection

- Edit [configuration] of downloaded Log Inspection rules
- Assign Context to a Log Inspection rule

Contexts

- Retrieve Contexts
- Add/Update/Edit/Delete Context

Tags

- Delete Tags

Scheduled Tasks

- Retrieve Scheduled Tasks
- Add/Edit/Delete Scheduled Tasks

Role

- Retrieve Roles
- Add/Edit/Delete Roles

Users

- Retrieve Users
- Add/Edit/Delete Users

Contacts

- Retrieve Contacts
- Add/Edit/Delete Contacts

Updates

- Download Security Update from Security Center
- Download Software from Security Center

Reference

This section describes all relevant transport and enumeration class objects.

Transport Objects

Transport objects are modeled after Deep Security Manager web interface objects and configuration groups. These transport objects can be constructed as new or retrieved from the Manager by calling the appropriate web method.

A Web Service definition may declare object classes that inherit properties from other base object classes, so only the relevant object classes are covered in this section. If during development, you encounter any WSDL-defined object classes that are not documented, they are likely inherited base object classes or response object classes that are not directly used by any Web Methods and do not have any direct value.

ApplicationTypeTransport

DESCRIPTION Represents an Application Type that reflects some network attributes to which DPI rules are assigned. The DPI engine will determine if a DPI rule should apply to a connection based on the assigned Application Type network attributes.

PROPERTIES

Name	Type	Description
ID	int	ApplicationTypeTransport ID
description	string	ApplicationTypeTransport description
name	string	ApplicationTypeTransport name
TBUID	string	Internal TBUID of a Trend Micro issued Application Type
direction	EnumDirection	The initial direction of the connection which this ApplicationTypeTransport would apply, e.g., INCOMING, OUTGOING Depending on whether the application type is a server or client, the initial direction of the connection to inspect would either be INCOMING for a server, or OUTGOING for a client. E.g. Inspection of “Web Server Common” Application Type for a connection stream on TCP port 80 would be initially an INCOMING direction because incoming Web Server connections should be inspected

ignoreRecommendations	boolean	Whether the Recommendation Engine should ignore this rule
protocolIcmp	ProtocolIcmp	ApplicationTypeTransport protocol ICMP type
protocolPortBased	ProtocolPortBased	ApplicationTypeTransport protocol Port type
protocolType	EnumApplicationTypeProtocolType	ApplicationTypeTransport protocol Application type, e.g., UCMP, TCP, UDP, TCP_UDP
authoritative	boolean	Whether the rule is an internal read only Trend Micro rule

ApplicationTypeOverrideTransport

DESCRIPTION Represents an Override for a specific Application Type and Security Profile. The ports and/or the recommendations flag can be overridden.

PROPERTIES

Name	**Type**	**Description**
ID	int	ApplicationTypeOverrideTransport ID
ApplicationTypeID	int	ApplicationTypeTransportID this override applies to
SecurityProfileID	int	SecurityProfileTransportID this override applies to
portType	EnumPortType	Assigned EnumPortType, e.g., ANY, PORTS, DEFINED_LIST
ports	String	Comma delimited list of ports and ranges if portType is PORTS
portListID	Integer	PortListTransport ID assigned if portType is DEFINED_LIST
ignoreRecommendations	boolean	Whether the Recommendation Engine should ignore this rule

ApplierInformationTransport

DESCRIPTION Represents the response information regarding the application of a software update using the securityUpdateApply web method.

PROPERTIES

Name	**Type**	**Description**

DPIRulesAdded	int	Number of DPI rules added
DPIRulesAddedAndAssigned	int	Number of DPI rules added and assigned
DPIRulesDeleted	int	Number of DPI rules removed
DPIRulesUpdated	int	Number of DPI rules updated
applicationTypesAdded	int	Number of Application Types added
applicationTypesDeleted	int	Number of Application Types removed
applicationTypesUpdated	int	Number of Application Types updated
detailedSummary	string	Detailed string summary of the update operation
integrityMonitoringRulesAdded	int	Number of Integrity Monitoring rules added
integrityMonitoringRulesDeleted	int	Number of Integrity Monitoring rules removed
integrityMonitoringRulesUpdated	int	Number of Integrity Monitoring rules updated
logInspectionDecodersAdded	int	Number of Log Inspection Decoders added
logInspectionDecodersDeleted	int	Number of Log Inspection Decoders deleted
logInspectionDecodersUpdated	int	Number of Log Inspection Decoders updated
logInspectionRulesAdded	int	Number of Log Inspection rules added
logInspectionRulesDeleted	int	Number of Log Inspection rules deleted
logInspectionRulesUpdated	int	Number of Log Inspection rules updated

portListsAdded	int	Number of Port Lists added
portListsUpdated	int	Number of Port Lists updated

AttributeTransport

DESCRIPTION Represents an Integrity Monitoring entity object attribute that the parent rule should be monitoring.

PROPERTIES

Name	Type	Description
friendlyValue	string	Human readable version of the value property
name	string	Attribute name
value	string	Attribute raw value which may be encoded depending on the attribute type

DPIEventListTransport

DESCRIPTION Represents a returned list of DPI events.

PROPERTIES

Name	Type	Description
truncated	boolean	Whether the event list was truncated or not
DPIEvents	ArrayOfDPIEventTransport	ArrayOfDPIEventTransport which contains a list of DPIEventTransport objects

DPIEventTransport

DESCRIPTION Represents a DPI event and contains all properties that belong to the event.

PROPERTIES

Name	Type	Description
DPIEventID	int	DPIEventTransport ID
DPIRuleID	int	DPIRuleTransport ID that triggered this event
action	string	Resulting action of the triggered event, e.g., log or deny
data	base64Binary	Any captured packet data in Base64 encoded format
dataFlags	int	A binary indication of xor'd flags from the network

		engine which are used to indicate conditions of the engine and data capture, e.g., TRUNCATED 0x01, OVERFLOW 0x02, SUPRESSED 0x04, HAVE DATA 0x08, REF DATA 0x10
dataIndex	int	Index of the final character in the data which triggered the event
destinationIP	string	Destination IP Address
destinationMAC	string	Destination MAC Address
destinationPort	string	Destination Port
direction	string	Direction of the event, e.g., incoming, or outgoing
driverTime	long	Epoch time the Agent driver recorded at the time of the event
endTime	dateTime	End time of the event if repeated multiple times, e.g., Internet browsers will resend a request multiple times if the connection is dropped and the exact same event would be repeated multiple times
eventOrigin	EnumEventOrigin	Origin of the event, e.g., AGENT, GUESTAGENT, APPLIANCEAGENT
flags	string	Data packet flags, e.g., ACK FIN
flow	string	Flow of the packet the log was recorded for in relation to the connection direction, e.g., 0 = FORWARD, 1 = BACKWARD
hostID	int	HostTransport ID of the computer where the event was triggered
hostName	string	HostTransport Name of the computer where the event was triggered
iface	string	Name of the physical network interface where the event was triggered
note	string	Internal note property that the engine may set for use by the Manager, e.g., Drop_data
packetSize	int	Size of the packet which triggered the event
protocol	string	Protocol of the connection
rank	int	Calculated Rank value (Computer Asset Value * IPS Filter Ranking)
reason	string	Name of the DPI filter which triggered the event
repeatCount	int	Repeat count of the event if repeated multiple times, e.g., Internet browsers will resend a request multiple times if the connection is dropped and the exact same event would be repeated multiple times

sourceIP	string	Source IP Address
sourceMAC	string	Source MAC Address
sourcePort	string	Source Port
startTime	dateTime	Start time of the event if repeated multiple times, e.g., Internet browsers will resend a request multiple times if the connection is dropped and the exact same event would be repeated multiple times
status	int	Error status code which will be 0 if no abnormal conditions were found
tags	string	Name of any event tags assigned to this event

DPIRuleTransport

DESCRIPTION

Represents a DPI Rule that can be accessed to read, update, or when creating new DPI Rules. Creating and updating DPI Rules is considered advanced and not a routine or repetitive operation. Changing some configuration options, such as includePacketData or raiseAlert are reasonable; however, creating a new DPI rule from scratch programmatically should only be done if full testing of the ruleXML content has been performed prior.

When creating a new rule, if possible it is recommended that an existing base rule is retrieved first, then modified to reflect the new rule, and saved as the new rule.

Once a new rule has been created and saved, the returned transport object from the save rule method should be used for all subsequent configuration operations for the life of the object. The reason for this is that the Manager will populate some fields during the save operation, such as rule ID, and these fields will not be present if you do not use the returned version after saving.

PROPERTIES

Name	**Type**	**Description**
ID	int	ID
name	string	Name
description	string	Description
TBUID	string	Internal TBUID of a Trend Micro issued DPI Rule
applicationTypeID	int	ApplicationTypeTransport ID this rule is assigned to
authoritative	boolean	Whether the rule is an internal read only Trend Micro rule

cveNumbers	string	A comma separated listing of the CVE Numbers from the vulnerability information
cvssScore	double	Final calculated CVSS score of the vulnerability information. A rule may resolve multiple vulnerabilities, so this will always be the highest CVSS score.
detectOnly	boolean	Whether the rule is detect only
disableEvent	boolean	Whether the rule is disabled
eventOnPacketDrop	boolean	Whether the rule should trigger an event when the connection is dropped
eventOnPacketModify	boolean	Whether the rule should trigger an event when a packet is modified by a rule (uncommon)
identifier	string	Public identifier of the filter used by Trend Micro to track filters
ignoreRecommendations	boolean	Whether the Recommendation Engine should ignore this rule
includePacketData	boolean	Whether this rule events should include packet data
issued	dateTime	Date this rule was issued
msNumbers	string	A comma separated listing of the Microsoft ID from the vulnerability information
patternAction	EnumDPIRuleAction	Action for START_END_PATTERNS type rule, e.g., DROP_CLOSE, LOG_ONLY
patternCaseSensitive	boolean	Whether a START_END_PATTERNS type rule should consider case sensitivity
patternEnd	string	End pattern
patternIf	EnumDPIRuleIf	Trigger if a START_END_PATTERNS type rule meets the criteria, e.g., ALL_PATTERNS_FOUND, ANY_PATTERNS_FOUND, NO_PATTERNS_FOUND
patternPatterns	string	A newline separated list of strings which will be used by a START_END_PATTERNS type rule
patternStart	string	Start pattern
priority	EnumDPIRulePriority	Rule priority, e.g., HIGHEST, NORMAL, LOWEST
raiseAlert	boolean	Whether an alert should be raised when the rule triggers

ruleXML	string	Rule XML of a CUSTOM_XML type rule. This may not be available for rules that have thirdBrigade set to TRUE
scheduleID	int	ScheduleTransport ID assigned to this rule
severity	EnumDPIRuleSeverity	Severity, e.g., CRITICAL, LOW
signatureAction	EnumDPIRuleAction	Action for SIGNATURE type rule, e.g., DROP_CLOSE, LOG_ONLY
signatureCaseSensitive	boolean	Whether a SIGNATURE type rule should consider case sensitivity
signatureSignature	string	Signature string which will be used by a SIGNATURE type rule
templateType	EnumDPIRuleTemplateType	Rule Type, e.g., CUSTOM_XML, SIGNATURE, START_END PATTERNS

EditableSettingStoredTransport

DESCRIPTION Represents existing Manager settings that can apply to a computer, Security Profile, or System. For example, the DPI engine can be configured to be in Detect at the System scope (top level) and the Security Profile scope can be configured to Prevent.

PROPERTIES

Name	**Type**	**Description**
settingKey	EnumEditableSettingKey	Existing setting key, e.g., CONFIGURATION_LOGGINGOVERRIDE
settingUnit	EnumEditableSettingUnit	Setting unit, e.g., MINUTES, EMAIL, IPLIST_ID
settingValue	string	Setting value
settingScope	EnumEditableSettingStoredScope	Scope of the setting, e.g., HOST, PROFILE, SYSTEM

EntityTransport

DESCRIPTION Represents an Integrity Monitoring entity object that references the attributes the parent rule should be monitoring.

PROPERTIES

Name	**Type**	**Description**
attributes	ArrayOfAttributeTransport	ArrayOfAttributeTransport array of AttributeTransport objects which reflect the entity attributes being monitored
key	string	Entity key
type	string	Entity type

FirewallEventTransport

DESCRIPTION Represents a Firewall event and contains all properties that belong to the event.

PROPERTIES

Name	Type	Description
firewallEventID	int	FirewallEventTransport ID
action	string	Resulting action of the triggered event, e.g., log or deny
data	base64Binary	Any captured packet data in Base64 encoded format
dataFlags	int	A binary indication of xor'd flags from the network engine which are used to indicate conditions of the engine and data capture, e.g., TRUNCATED 0x01, OVERFLOW 0x02, SUPRESSED 0x04, HAVE DATA 0x08, REF DATA 0x10
dataIndex	int	Index of the final character in the data which triggered the event
destinationIP	string	Destination IP Address
destinationMAC	string	Destination MAC Address
destinationPort	string	Destination Port
direction	string	Direction of the event, e.g., incoming, or outgoing
driverTime	long	Epoch time the Agent driver recorded at the time of the event
endTime	dateTime	End time of the event if repeated multiple times, e.g., Internet browsers will resend a request multiple times if the connection is dropped and the exact same event would be repeated multiple times
eventOrigin	EnumEventOrigin	Origin of the event, e.g., AGENT, GUESTAGENT, APPLIANCEAGENT
flags	string	Data packet flags, e.g., ACK FIN
flow	string	Flow of the packet the log was recorded for in relation to the connection direction, e.g., 0 = FORWARD, 1 = BACKWARD
frameType	string	Connection frame type, e.g., IP, ARP

hostID	int	HostTransport ID of the computer where the event was triggered

hostName	string	HostTransport Name of the computer where the event was triggered
iface	string	Name of the physical network interface where the event was triggered
note	string	Internal note property that the engine may set for use by the Manager, e.g., Drop_data
packetSize	int	Size of the packet which triggered the event
protocol	string	Protocol of the connection
rank	int	Calculated Rank value (Computer Asset Value * IPS Filter Ranking)
reason	string	Name of the Firewall rule which triggered the event
repeatCount	int	Repeat count of the event if repeated multiple times, e.g., Internet browsers will resend a request multiple times if the connection is dropped and the exact same event would be repeated multiple times
sourceIP	string	Source IP Address
sourceMAC	string	Source MAC Address
sourcePort	string	Source Port
startTime	dateTime	Start time of the event if repeated multiple times, e.g., Internet browsers will resend a request multiple times if the connection is dropped and the exact same event would be repeated multiple times
status	int	Error status code which will be 0 if no abnormal conditions were found
tags	string	Name of any event tags assigned to this event

FirewallRuleTransport

DESCRIPTION Represents a Firewall Rule that can be accessed to create, read, or update. Note that some fields are dynamically required. For example, if destinationIPType is set to RANGE, then destinationIPRangeFrom and destinationIPRangeTo are required fields, but destinationIPListID and destinationIPMask are not. The Web Service validation of these transport object properties is the same as what is validated in the Manager web interface itself. For an initial idea on how to configure a new rule transport object, see the Manager interface itself and the configurable fields you would like to attempt programmatically through the Web Service API.

When creating new rule, if possible it is recommended that an existing base rule be retrieved first, then modified to reflect the new rule, and then saved as the new rule.

Once a new rule has been created and saved, the returned transport object from the save rule method should be used for all subsequent configuration operations for the life of the object. The reason for this is the Manager will populate some fields during the save operation, such as rule ID, and these fields will not be present if you do not use the returned version after saving.

Note that there is some complex property validation that is generally implemented by the Manager web interface. For example, if the destinationIPType DEFINED_LIST is set, then the destinationIPListID will be required. If the destinationIPType RANGE is set, then destinationIPRangeFrom and destinationIPRangeTo will be required. This validation will be reported in the form of an exception when trying to save the object.

PROPERTIES

Name	**Type**	**Description**
ID	int	ID
name	string	Name
description	string	Description
action	EnumFirewallRuleAction	Resulting action of the triggered event, e.g., log or deny
anyFlags	boolean	Overriding packet flag criteria that includes any packet flags
destinationIP	string	Destination IP Address
destinationIPListID	int	IPListTransport ID of the assigned IP List
destinationIPMask	string	Destination IP Mask
destinationIPNot	boolean	Whether the destination IP criteria should be negative
destinationIPRangeFrom	string	Destination IP range from value
destinationIPRangeTo	string	Destination IP range to value
destinationIPType	EnumFirewallRuleIPType	Assigned EnumFirewallRuleIPType, e.g., ANY, MASKED_IP, RANGE, DEFINED_LIST
destinationMAC	string	Destination MAC
destinationMACListID	int	Assigned MACListTransport ID
destinationMACNot	boolean	Whether the destination MAC criteria should be negative
destinationMACType	EnumMACType	Assigned EnumMACType, e.g., ANY, MAC, DEFINED_LIST
destinationPortListID	int	Assigned PortListTransport ID

destinationPortNot	boolean	Whether the destination Port criteria should be negative
destinationPortType	EnumPortType	Assigned EnumPortType, e.g., ANY, PORTS, DEFINED_LIST
destinationPorts	string	Destination Ports
destinationSingleIP	string	Destination single IP
disabledLog	boolean	Disable logging of events triggered by this rule
frameNot	boolean	Whether the assigned frameType criteria should be negative
frameNumber	string	If frameType is OTHER, then use this value
frameType	EnumFirewallRuleFrameType	Assigned EnumFirewallRuleFrameType, e.g., ANY, IP, ARP, REARP, OTHER
icmpCode	int	If protocolType is ICMP, and anyFlags set to false, then include this ICMP code for the specified icmpType
icmpNot	boolean	Whether the icmpType flags should be negative
icmpType	int	If protocolType is ICMP, and anyFlags set to false, then include this ICMP type code, e.g., 30 = Traceroute, 37 = Domain Name Request
packetDirection	EnumDirection	Direction of the event, e.g., incoming, or outgoing
priority	EnumFirewallRulePriority	Assigned EnumFirewallRulePriority, e.g., HIGHEST, NORMAL, LOW
protocolNot	boolean	Whether the destination Protocol criteria should be negative
protocolNumber	int	If protocolType is set to OTHER, use this value
protocolType	EnumFirewallRuleProtocolType	Assigned EnumFirewallRuleProtocolType, e.g., ANY, ICMP, ICMPV6, TCP, UDP, TCP_UDP, OTHER
raiseAlert	boolean	Whether an alert should be raised when the rule triggers
scheduleID	int	ScheduleTransport ID assigned to this rule
sourceIP	string	Source IP Address
sourceIPListID	int	IPListTransport ID of the assigned IP List
sourceIPMask	string	Source IP Mask
sourceIPNot	boolean	Whether the source IP criteria should be

		negative
sourceIPRangeFrom	string	Source IP range from value
sourceIPRangeTo	string	Source IP range to value
sourceIPType	EnumFirewallRuleIPType	Assigned EnumFirewallRuleIPType, e.g., ANY, MASKED_IP, RANGE, DEFINED_LIST
sourceMAC	string	Source MAC
sourceMACListID	int	Assigned MACListTransport ID
sourceMACNot	boolean	Whether the source MAC criteria should be negative
sourceMACType	EnumMACType	Assigned EnumMACType, e.g., ANY, MAC, DEFINED_LIST
sourcePortListID	int	Assigned PortListTransport ID
sourcePortNot	boolean	Whether the source Port criteria should be negative
sourcePortType	EnumPortType	Assigned EnumPortType, e.g., ANY, PORTS, DEFINED_LIST
sourcePorts	string	Source Ports
sourceSingleIP	string	Source single IP
tcpFlagACK	boolean	If protocolType includes TCP, and anyFlags set to false, then include TCP packets with the ACK flag
tcpFlagFIN	boolean	If protocolType includes TCP, and anyFlags set to false, then include TCP packets with the FIN flag
tcpFlagPSH	boolean	If protocolType includes TCP, and anyFlags set to false, then include TCP packets with the PSH flag
tcpFlagRST	boolean	If protocolType includes TCP, and anyFlags set to false, then include TCP packets with the RST flag
tcpFlagSYN	boolean	If protocolType includes TCP, and anyFlags set to false, then include TCP packets with the SYN flag
tcpFlagURG	boolean	If protocolType includes TCP, and anyFlags set to false, then include TCP packets with the URG flag
tcpNot	boolean	Whether the TCP Flag criterion should be negative

HostFilterTransport

DESCRIPTION Used as search criteria to limit the scope of objects returned by computer-related attributes, such as by a Group, a Security Profile, or a specific computer. The event retrieval-related methods will require a HostFilterTransport that is empty to search for all events, or with specific properties populated to limit the scope of the search. For example, setting the HostFilterTransport securityProfileID property to the ID of a Security Profile will limit any event retrieval method calls to events that pertain to computers with the specific Security Profile assigned.

PROPERTIES

Name	**Type**	**Description**
hostGroupID	int	HostGroupTransport ID to filter computers by
hostID	int	HostTransport ID to filter computers by
securityProfileID	int	SecurityProfileTransport ID to filter computers by
type	EnumHostFilterType	EnumHostFilterType to filter computers by

HostGroupTransport

DESCRIPTION Represents a computer group folder that computers can be assigned to for organizational purposes.

PROPERTIES

Name	**Type**	**Description**
ID	int	ID
name	string	Name
description	string	Description
external	boolean	Administrative external boolean for integration purposes
externalID	string	Administrative external ID for integration purposes
parentGroupID	int	If the group belongs to a parent group, then this ID will be set and used to retrieve the parent group

HostStatusTransport

DESCRIPTION Contains the overall status information of a computer, VMWare ESX server, or Deep Security Virtual Appliance. Physical computers, virtual machines, ESX servers, and Deep Security Virtual Appliances are all represented as HostTransport objects. The requested computer HostStatusTransport object can contain optional information about the ESX a virtual machine belongs to, or information about an ESX server.

PROPERTIES

Name	Type	Description
applianceID	int	The HostTransport ID of any protecting Deep Security Virtual Appliance
applianceName	string	The name of any protecting Deep Security Virtual Appliance
esxServerFastPathDriverVersion	string	The fast path driver version a of virtual machine protected by a Deep Security Virtual Appliance
esxServerID	string	The HostTransport ID of a virtual machine hosting ESX server
esxServerName	string	The name of a virtual machine hosting ESX server
esxServerVersion	string	The version of a virtual machine hosting ESX server
locked	boolean	If the computer is locked
overallAntiMalwareStatus	string	Overall Anti Malware status
overallDpiStatus	string	Overall DPI protection status
overallFirewallStatus	string	Overall Firewall protection status
overallIntegrityMonitoringStatus	string	Overall Integrity Monitoring protection status
overallLastSuccessfulCommunication	DateTime	Overall last successful communication date and time.
overallLastSuccessfulUpdate	DateTime	Overall last successful update date and time.
overallLogInspectionStatus	string	Overall Log Inspection protection status.
overallStatus	string	Overall status.
protectionStatusTransports	ProtectionStatusTransport[]	The specific ProtectionStatusTransport objects assigned to the HostTransport object
overallWebReputationStatus	string	Overall Web Reputation Status.

HostTransport

DESCRIPTION

The primary computer transport object that represents the computer systems Deep Security is aware of. Physical computers, virtual machines, ESX servers, and Deep Security Virtual Appliances are all represented as HostTransport objects.

To determine a HostTransport status (e.g., Activated, Offline, Installed, etc.) the computer HostStatusTransport should be retrieved and the assigned ProtectionStatusTransport objects should be inspected. The HostTransportStatus will reflect the overall protection status of a computer. If protection is applied by both an in-guest Agent and Virtual Appliance, then two ProtectionStatusTransport objects will be assigned. Agent and Virtual Appliance protection may have different protection capabilities enabled, so inspection of all assigned ProtectionStatusTransport objects should considered. Note that this is only necessary where a Virtual Appliance is deployed. Computers and virtual machines that only use Agent protection may only use the HostTransportStatus.

PROPERTIES

Name	Type	Description
displayName	string	Computer display name
external	boolean	Administrative external boolean for integration purposes.
externalID	string	Administrative external ID for integration purposes.
hostGroupID	int	Assigned HostGroupTransport ID
hostType	EnumHostType	Assigned host type
platform	string	Computer platform
securityProfileID	int	Assigned SecurityProfileTransport ID

IDFilterTransport

DESCRIPTION Used as a search criteria to limit the scope of objects returned by event transport object ID. Each event transport object, such as IntegrityEventTransport, includes an ID property that is assigned as the primary key of an event when it is generated by a computer agent. Using IDFilterTransport, it is possible to filter event retrieval by this event ID in order to retrieve a specific event by ID, or events that are greater or less than a specified ID. For example, a utility that is designed to retrieve all new events on an interval can use the event ID property to uniquely identify which events have already been retrieved. This way retrieval of duplicate events can be avoided.

PROPERTIES

Name	Type	Description
id	int	Event transport objects ID to filter b.
operator	EnumOperator	EnumOperator to used to apply the id property, e.g., greater than, less than, and equal

IntegrityEventTransport

DESCRIPTION Represents an Integrity monitoring event and contains all properties that belong to the event. Depending on the triggering rule and the target entity types and attributes monitoring, key, process, and user may contain information about the changed service, file, or user account. The isEntity and wasEntity properties may be used to inspect the changes made to the attribute that triggered the event; however, the description will contain a verbose explanation of the changes.

PROPERTIES

Name	Type	Description
integrityEventID	int	IntegrityEventTransport ID
integrityRuleID	int	IntegrityRuleTransport ID which triggered this event
change	string	Change applied to the target key, e.g., Created, Updated, Deleted, Renamed
description	string	Description of the monitored attributes and what changed
hostID	int	HostTransport ID of the computer where the event was triggered
hostName	string	HostTransport Name of the computer where the event was triggered
isEntity	EntityTransport	EntityTransport of the monitored entity after the change which triggered the event
key	string	Name of file or registry key which the Integrity rule triggered on during a scan (if available)
logTime	dateTime	Time the triggered event was logged
process	string	Name of process or service which the Integrity rule triggered on during a scan (if available)
rank	int	Calculated Rank value (Computer Asset Value * IPS Filter Ranking)
reason	string	Name of the Integrity rule which triggered the event
severity	EnumIntegrityRuleSeverity	EnumIntegrityRuleSeverity severity level of the triggered event, e.g., CRITICAL, HIGH, MEDIUM, LOW
tags	string	Name of any event tags assigned to this event
type	string	Key type, e.g., Directory, File, Group, Installed Software, Service, User
user	string	Name of the user which the Integrity rule triggered on during a scan (if available)
wasEntity	EntityTransport	EntityTransport of the monitored entity before the change which triggered the event

IntegrityRuleTransport

DESCRIPTION

Represents an Integrity Monitoring Rule that can be accessed to create, read, or update.

When creating new rule, if possible it is recommended that an existing base rule be retrieved first, then modified to reflect the new rule, and then saved as the new rule.

Once a new rule has been created and saved, the returned transport object from the save rule method should be used for all subsequent configuration operations for the life of the object. The reason for this is the Manager will populate some fields during the save operation, such as rule ID, and these fields will not be present if you do not use the returned version after saving.

PROPERTIES

Name	**Type**	**Description**
ID	int	ID
name	string	Name
description	string	Description
TBUID	string	Internal TBUID of a Trend Micro issued Integrity Monitoring rule
allowOnChange	boolean	Whether on change detection is enabled
authoritative	boolean	Whether the rule is an internal read only Trend Micro rule
content	string	XML content of the rule
identifier	string	Public identifier of the filter used by Trend Micro to track rules
ignoreRecommendations	boolean	Whether the Recommendation Engine should ignore this rule
issued	dateTime	Date this rule was issued
minAgentVersion	string	Minimum Agent version which can support this rule
minManagerVersion	string	Minimum Manager version which can support this rule
raiseAlert	boolean	Whether an alert should be raised when the rule triggers
severity	EnumIntegrityRuleSeverity	EnumDPIRuleSeverity Severity, e.g., CRITICAL, LOW

IPListTransport

DESCRIPTION Represents an IP Address List which can be assigned to other objects, such as Firewall rules.

PROPERTIES

Name	Type	Description
ID	int	IPListTransport ID
description	string	IPListTransport description
name	string	IPListTransport name
items	string	A newline separated list of IP Addresses

LogInspectionDecoderTransport

DESCRIPTION Represents a Log Inspection log file decoder. Log Inspection rules are applied after a log file has been first decoded. Some log files require special decoding because of the format the log data is contained in.

PROPERTIES

Name	Type	Description
ID	int	IPListTransport ID
description	string	IPListTransport description
name	string	IPListTransport name
TBUID	string	Internal TBUID of a Trend Micro issued Integrity Monitoring rule
authoritative	boolean	Whether the rule is an internal read only Trend Micro rule
content	string	XML content of the decoder
identifier	string	Public identifier of the filter used by Trend Micro to track rules
issued	dateTime	Date this rule was issued
minAgentVersion	string	Minimum Agent version which can support this rule
minManagerVersion	string	Minimum Manager version which can support this rule

LogInspectionEventTransport

DESCRIPTION	Represents a Log Inspection event and contains all properties that belong to the event. Due to the dynamic nature of monitoring many different kinds of application log file, few or many of the properties may be populated. For example, some inspected log files can contain information about a remote computer and so the sourceIP and sourceUser may be populated, while other log files may only contain application related entries like programName. Do not rely on a descriptive property to be always present. Instead perform proper null value checking before utilizing the property.

PROPERTIES

Name	Type	Description
logInspectionEventID	int	LogInspectionEventTransport ID
logInspectionRuleID	string	LogInspectionRuleTransport ID
action	string	Resulting action of the triggered event
command	string	
data	string	Source log file data type, e.g., Windows Events = Crypt32, Security, Application
description	string	Name of the triggered LogInspectionRuleTransport sub-rule
destinationIP	string	Destination IP Address if available
destinationUser	string	Destination User if available
destinationPort	string	Destination Port if available
fullEvent	string	Copy of the triggered full log entry
groups	string	Groups of the LogInspectionRuleTransport triggered sub-rule
hostID	int	HostTransport ID of the computer where the event was triggered
hostName	string	HostTransport Name of the computer where the event was triggered
location	string	Location of the inspected log file
logTime	dateTime	Time of the triggered event
message	string	
programName	string	Name of the monitored log file application
rank	string	Calculated Rank value (Computer Asset Value * IPS Filter Ranking)
reason	string	Name of the Log Inspection rule that triggered the event
ruleID	int	LogInspectionRuleTransport sub-rule ID as defined

		in the rule syntax
severity	string	Severity of the triggered sub-rule, e.g., Lowest = 1, Critical = 15
sourceHostName	string	Source hostname if available
sourceID	string	Source ID if available
sourceIP	string	Source IP Address if available
sourcePort	string	Source Port if available
sourceUser	string	Source User if available
status	string	
systemName	string	System name of the computer the event triggered on
tags	string	Name of any event tags assigned to this event
url	string	URL attribute of the log event if available

LogInspectionRuleTransport

DESCRIPTION Represents a Log Inspection Rule that can be accessed to create, read, or update.

When creating new rule, if possible it is recommended that an existing base rule is retrieved first, and then modified to reflect the new rule, then saved as the new rule.

Once a new rule has been created and saved, the returned transport object from the save rule method should be used for all subsequent configuration operations for the life of the object. The reason for this is the Manager will populate some fields during the save operation, such as rule ID, and these fields will not be present if you do not use the returned version after saving.

PROPERTIES

Name	**Type**	**Description**
ID	int	ID
name	string	Name
description	string	Description
TBUID	string	Internal TBUID of a Trend Micro issued Log Inspection rule
alertMinSeverity	int	Minimum severity at which a sub-rule event will trigger a rule Alert
authoritative	boolean	Whether the rule is an internal read only Trend Micro rule
content	string	XML content of the rule

files	string	XML content that reflects the log file and format to inspect This should contain one or more <localfile> node elements that require <location> and <log_format> elements where location is a path to the log file and format is one of the following pre-defined log handlers: • single-line-text-log • syslog • snort-full • snort-fast • apache • iis • squid • nmapg • mysql_log • postgresql_log • djb-multilog • eventlog Windows Event Log example: <localfile> <location>Application</location> <log_format>eventlog</log_format> </localfile> Multiple single line log files example: <localfile> <location>c:\application\error.log</location> <log_format>single-line-text-log</log_format> </localfile> <localfile> <location>c:\application\debug.log</location> <log_format>single-line-text-log</log_format> </localfile>

		NOTE: LogInspectionRuleTransport objects with the thirdBrigade property set to TRUE will return JIT (Just-In-Time) output logic from the Log Inspection engine and can include internal engine logic fragments. Do not attempt to reuse this internal logic when updating or creating custom Log Inspection rules Please consult the Deep Security User Guide for more information on supported log file formats
identifier	string	Public identifier of the filter used by Trend Micro to track filters
ignoreRecommendations	boolean	Whether the Recommendation Engine should ignore this rule
issued	dateTime	Date this rule was issued
minAgentVersion	string	Minimum Agent version that can support this rule
minManagerVersion	string	Minimum Manager version that can support this rule
raiseAlert	boolean	Whether an alert should be raised when the rule triggers

MACListTransport

DESCRIPTION Represents a MAC Address List that can be assigned to other objects, such as Firewall rules.

PROPERTIES

Name	Type	Description
ID	int	MACListTransport ID
description	string	MACListTransport description
name	string	MACListTransport name
items	string	A newline separated list of MAC Addresses

PortListTransport

DESCRIPTION Represents a Port List that can be assigned to other objects, such as Firewall rules.

PROPERTIES

Name	Type	Description
ID	int	PortListTransport ID
description	string	PortListTransport description
name	string	PortListTransport name
items	string	A newline separated list of Ports
TBUID	string	Internal TBUID

ProtectionStatusTransport

DESCRIPTION Represents the protection status of a host that is provided by and Agent or Virtual Appliance. A HostTransport object may have up to two ProtectionStatusTransport objects assigned if the computer is a Virtual Machine protected by an in-guest Agent.

PROPERTIES

Name	Type	Description
dpiStatus	**string**	DPI protection status
fingerprint	**string**	Fingerprint of the certificate issued to the protection type applied. This will be different between Agent and Appliance protection types, but may be used to determine if the Agent issued certificate has been changed due to legitimate re-activation or illegal tampering
firewallStatus	**string**	Firewall protection status
integrityMonitoringStatus	**string**	Integrity Monitoring protection status
lastSuccessfulCommunication	**dateTime**	Last successful communication
lastSuccessfulUpdate	**dateTime**	Last successful update
logInspectionStatus	**string**	Log Inspection protection status
protectionType	**EnumProtectionType**	Protection type provided, e.g., AGENT, APPLIANCE, NONE
state	**EnumState**	State of the protection type being applied, e.g., VM_STOPPED, VM_PAUSED, STANDBY, ACTIVATED, OFFLINE, INSTALLED, etc…
stateDescription	**string**	Description of the protection type state. Use this property when attempting to communicate to the user the state property assigned
status	**string**	Status of the protection type applied
version	**string**	Version of the protection type being applied, e.g., Agent or Virtual Appliance version
componentInfoTransports	**ArrayOfComponentInfoTransport**	Component Info Transports
webReputationStatus	**string**	Web reputation protection status

ProtocolIcmp

DESCRIPTION Represents a basic ICMP protocol type container.

PROPERTIES

Name	Type	Description
type	EnumProtocolIcmpType	Assigned EnumProtocolIcmpType, e.g., ICMP_ECHO, ICMP_ADDRESS_MASK

ProtocolPortBased

DESCRIPTION Represents an Application Type port protocol container.

PROPERTIES

Name	Type	Description
portListID	int	PortListTransport ID assigned if portType is DEFINED_LIST
portType	EnumPortType	Port type, e.g., ANY, PORTS, DEFINED_LIST
ports	string	Comma delimited list of ports and ranges if portType is PORTS

ScheduleTransport

DESCRIPTION Represents a Schedule container.

PROPERTIES

Name	Type	Description
ID	int	ScheduleTransport ID
description	string	ScheduleTransport description
name	string	ScheduleTransport name
hourOfWeek	String	A custom format that represents each hour of a week. The format is a single line sequence of 168 one and zero characters where a one represents an hour of the week that the assigned schedule should execute beginning Sunday morning. For example,

the following truncated sample would execute Monday at 4am:

00000000000000000000000000001000000…

SecurityProfileTransport

DESCRIPTION Represents a Security Profile container that can be assigned to other Computers by ID using their HostTransport object.

PROPERTIES

Name	**Type**	**Description**
ID	int	SecurityProfileTransport ID
description	string	SecurityProfileTransport description
name	string	SecurityProfileTransport name
DPIRuleIDs	int[]	Array of assigned DPIRuleTransport IDs
DPIState	EnumSecurityProfileDPIState	Assigned EnumSecurityProfileDPIState, e.g., ON, OFF, PASSIVE, INHERITED
antiMalwareManualID	int	Anti Malware Manual ID
antiMalwareManualInherit	boolean	Anti Malware Manual Inherit
antiMalwareRealTimeID	int	Anti Malware Real Time ID
antiMalwareRealTimeInherit	boolean	Anti Malware Real Time Inherit
antiMalwareRealTimeScheduleID	int	Anti Malware Real Time Schedule ID
antiMalwareScheduledID	int	Anti Malware Scheduled ID
antiMalwareScheduledInherit	boolean	Anti Malware Scheduled Inherit
antiMalwareState	EnumSecurityProfileAntiMalwareState	Assigned EnumSecurityProfileAntiMalwareState, e.g., ON, OFF, INHERITED
applicationTypeIDs	int[]	Array of assigned ApplicationTypeTransport IDs
firewallRuleIDs	int[]	Array of assigned FirewallRuleTransport IDs
firewallState	EnumSecurityProfileFirewallState	Assigned EnumSecurityProfileFirewallState, e.g., ON, OFF, INHERITED
integrityRuleIDs	int[]	Array of assigned IntegrityMonitoringRuleTransport IDs

integrityState	EnumSecurityProfileIntegrityState	Assigned EnumSecurityProfileIntegrityState, e.g., ON, OFF, INHERITIED
logInspectionRuleIDs	int[]	Array of assigned LogInspectionRuleTransport IDs
logInspectionState	EnumSecurityProfileLogInspectionState	Assigned EnumSecurityProfileLogInspectionState, e.g., ON, OFF, INHERITED
parentSecurityProfileID	int	Assigned Security Profile ID
recommendationState	EnumSecurityProfileRecommendationState	Assigned EnumSecurityProfileRecommendationState, e.g., OFF, ONGOING
scheduleID	int	Assigned ScheduleTransport ID
statefulConfigurationID	int	Assigned StatefulConfigurationTransport ID

SecurityUpdateTransport

DESCRIPTION Represents a downloaded Security Update that can be applied. Once applied, all updates to rules and recommendations in the Security Update will be available to Deep Security. Deep Security Manager can download and keep multiple Security Updates, but only one can be applied at a time. The currently applied Security Update is indicated by the appliedState property EnumSecurityUpdateAppliedState APPLIED_CURRENT value.

PROPERTIES

Name	Type	Description
ID	int	SecurityUpdateTransport ID
appliedState	EnumSecurityUpdateAppliedState	Applied state, e.g., APPLIED, APPLIED_CURRENT, NOT_APPLIED
contentSummary	string	Summary of the Security Update
detectOnly	boolean	Used to indicate whether new Security Update rules should be applied as Detect Only. This can be used to limit risk associated with automatic assignment of untested new rules in a new Security Update This property should be set before calling the securityUpdateApply() method for it to be effective
downloaded	dateTime	Download date
name	string	Simple friendly name
released	dateTime	Trend Micro release date

SoftwareTransport

DESCRIPTION Represents a downloaded Software update that can be applied to the target type. Generally Software updates are Agent software updates. However Deep Security Virtual Appliances can also be considered a Software package.

PROPERTIES

Name	Type	Description
ID	int	SecurityUpdateTransport ID
fingerprint	string	Hashed fingerprint of the software file
imported	dateTime	Download or import date
name	string	Simple friendly name
notes	string	Release notes
platform	string	Target platform
released	dateTime	Trend Micro release date
version	string	Software version

StatefulConfigurationTransport

DESCRIPTION Represents a Stateful Inspection configuration container.

PROPERTIES

Name	Type	Description
ID	int	StatefulConfigurationTransport ID
description	string	StatefulConfigurationTransport description
name	string	StatefulConfigurationTransport name
ackStormDropConnection	boolean	Enable ACK Storm protection connection drops when detected
ackStormProtection	boolean	Enable ACK Storm protection
ackStormProtectionThreshold	int	The number of acknowledged packets before enforcing ACK Stork protection
allowIncomingActiveFTP	boolean	Allow Active FTP when assigned computer acts as a server
allowIncomingPassiveFTP	boolean	Allow Passive FTP when assigned computer acts as a server

allowOutgoingActiveFTP	boolean	Allow Active FTP when assigned computer acts as a client

allowOutgoingPassiveFTP	boolean	Allow Passive FTP when assigned computer acts as a client
denyFragmentedPackets	boolean	Deny incoming fragmented packets
denyTcpCwrEceFlags	boolean	Deny TCP packets containing CWR, EXE flags when there is network congestion (See RFC 3168 for ECN field definitions)
enableICMPStatefulInspection	boolean	Enable stateful inspection of packets at the ICMP level
enableICMPStatefulLogging	boolean	Enable logging of ICMP stateful inspection
enableTCPStatefulInspection	boolean	Enable stateful inspection of packets at the TCP level
enableTCPStatefulLogging	boolean	Enable logging of TCP stateful inspection
enableUDPStatefulInspection	boolean	Enable stateful inspection of packets at the UDP level
enableUDPStatefulLogging	boolean	Enable logging of UDP stateful inspection
limitHalfOpenConnections	boolean	Enable limiting of the number of half open TCP connections
limitHalfOpenConnectionsTo	int	The number of limited half open TCP connections
limitIncomingConnections	boolean	Enable limiting of incoming connections from a single computer
limitIncomingConnectionsTo	int	The number of limited incoming connection from a single computer
limitOutgoingConnections	boolean	Enable limiting of outgoing connections from a single computer
limitOutgoingConnectionsTo	int	The number of limited outgoing connection from a single computer
synFloodProtection	boolean	Enable SYN flood protection
synFloodProtectionThreshold	int	The number of half open TCP connections allowed before SYN flood protection is enforced

SystemEventTransport

DESCRIPTION Represents a Deep Security Manager System event. A System event can target many different aspects of Deep Security, such as a configuration change to a Security Profile or Computer setting, or applying a Security Update to a Computer.

PROPERTIES

Name	Type	Description
actionPerformedBy	string	Name of the administrator who performed the action that generated the event
description	string	SystemEventTransport Description
event	string	SystemEventTransport Summary
eventID	int	Common Event ID that can be used uniquely identify the event cause (see Deep Security Manager for a list of Event IDs and the action type)
eventOrigin	EnumEventOrigin	Originating source of the event, e.g., UNKNOWN, AGENT, MANAGER
managerHostname	string	Hostname of the Manager
systemEventID	int	SystemEventTransport ID
tags	string	Name of any event tags assigned to this event
target	string	Summary name of the target of the event action
targetID	int	Transport object ID of the target
targetType	string	Type of the target such as an administrator, computer or schedule.
time	dateTime	Time of the event
type	string	Event level type, e.g., Error, Info, Warning

SystemInformationTransport

DESCRIPTION Represents a Deep Security Manager system information container.

PROPERTIES

Name	Type	Description
key	string	System information key
name	string	System information name
value	string	System information value

TimeFilterTransport

DESCRIPTION Used as search criteria limit the scope of objects returned by time related attributes, such as from, to, or a specific time. If the type is set to EnumTimeFilterType CUSTOM_RANGE, then the rangeFrom and rangeTo property will be required. If the EnumTimeFilterType SPECIFIC_TIME type is set, then the specifiicTime property will be required.

PROPERTIES

Name	Type	Description
rangeFrom	dateTime	HostGroupTransport ID to filter computers by.
rangeTo	dateTime	HostTransport ID to filter computers by.
specificTime	dateTime	SecurityProfileTransport ID to filter computers by.
type	EnumTimeFilterType	EnumTimeFilterType to filter computers by.

UserTransport

DESCRIPTION Represents User Transport.

PROPERTIES

Name	Type	Description
ID	int	
country	string	
description	string	
emailAddress	string	
fullName	string	
language	string	
lockedOut	boolean	
mobileNumber	string	
pagerNumber	string	
password	string	
passwordNeverExpires	boolean	
phoneNumber	string	
receiveNotifications	boolean	

TagFilterTransport

DESCRIPTION Used as a search criteria to specify the criteria of tags for the search

PROPERTIES

Name	Type	Description
tags	string	The requested tags, depending on the type field
type	EnumTagFilterType	ALL returns an unbounded set, UNTAGGED returns only events that have no tags. Otherwise the tags field is a freeform field that takes comma delimited tag names (with the not '!' character indicated where not tagged).

CounterTransport

DESCRIPTION This object represents an abstraction of data that is represented on the dashboard.

PROPERTIES

Name	Type	Description
description	string	Blank, for future use
percentOfTotal	float	Percentage of the data in this counter in relation to all data for the given time period.
percentOfTotalString	string	Same as percentOfTotal, but as a string
text	string	Counter dependant
value	long	The actual number of events that triggered that match this counter
valueString	string	Same as value, but as a string
previousValue	long	The previous value of the same counter, but in the previous time period. Useful for trend calculation.

CounterHostTransport

DESCRIPTION A counter object specific from a host. This extends from CounterTransport, so all fields of that class apply here.

PROPERTIES

Name	Type	Description
hostID	Int	The hostID this counter applies to
icon	string	The icon URL that should be used for this host.

CounterWithIDTransport

DESCRIPTION A counter object specific for a specific item, typically a rule. This extends from CounterTransport, so all fields of that class apply here.

PROPERTIES

Name	Type	Description
itemID	Int	The ID of the item this counter corresponds to.

CounterAlertTypeTransport

DESCRIPTION A counter object that aggregates alert information. This extends from CounterTransport, so all fields of that class apply here.

PROPERTIES

Name	Type	Description
severity	int	The severity of the alert.
percentOpen	string	
averageTimeOpen	string	

FeatureSummaryDetailTransport

DESCRIPTION An object that represents the status summary of a protection module.

PROPERTIES

Name	Type	Description
featureName	string	The name of the module
protectedComputerNum	long	Number of computers that currently have this module activated.

totalEventNum	long	Total number of events
preventedEventNum	long	Number of events that were prevented
detectedEventNum	long	Number of events that were detected
previousTotalEventNum	long	Total event count for the previous time period
previousPreventedEventNum	long	Prevent count for the previous time period
previousDetectedEventNum	long	Detect count for the previous time period

HostStatusSummaryTransport

DESCRIPTION An object that represents the high level computer summary for the system.

PROPERTIES

Name	Type	Description
criticalHosts	Int	Number of hosts in critical state
lockedHosts	int	Number of hosts in locked state
onlineHosts	int	Number of managed, online hosts
unmanageHosts	int	Number of unmanaged hosts
warningHosts	int	Number of hosts in warning state

StatusSummaryTransport

DESCRIPTION An collection of objects that represent the high level status for the system

PROPERTIES

Name	Type	Description
alertErrorNum	int	Number of current error alerts
alertWarningNum	int	Number of current warning alerts
hostStatusSummary	HostStatusSummaryTransport	Computer status summary

ComponentInfoTransport

DESCRIPTION Represents the information for an individual component in the system. Components are patterns, rule updates, manifests, etc.., typically items that are visible on the System->Updates page.

PROPERTIES

Name	Type	Description
type	int	An internal type of the component
id	int	An ID representing the component
name	string	The friendly name of the component
shortName	string	The short name for the component
currentVersion	string	The current version of the component
lastUpdate	dateTime	The last time this component was updated
nameKey	string	An internal key for the component
deployed	int	Number of endpoints on which this component is deployed
needDeployed	int	Number of endpoints on which this component is out of date

JobProgressTransport

DESCRIPTION Collects the progress for a given system job, i.e., " Update Security Configuration on N computers"

PROPERTIES

Name	Type	Description
complete	Int	Number jobs that have completed in the time period
error	int	Number that have failed in error
pending	int	Number that are still outstanding
unable	int	Number of jobs that were unable to start

ConfigurationTransport

DESCRIPTION The superclass for many configuration transport objects.

PROPERTIES

Name	Type	Description
ID	int	The ID of the transport object
description	string	Description of the object
name	string	Name of the object

ProtectionStatusTransport

DESCRIPTION An object representing the current module protection status for a given computer.

PROPERTIES

Name	Type	Description
dpiStatus	string	The status of the DPI module for the computer
fingerprint	string	The certificate fingerprint
firewallStatus	string	The status of the Firewall module for the computer
integrityMonitoringStatus	string	The status of the Integrity Monitoring module for the computer
lastSuccessfulCommunication	dateTime	Last successful communication time
lastSuccessfulUpdate	dateTime	Last configuration update time
logInspectionStatus	string	The status of the Log Inspection module for the computer
protectionType	EnumProtectionType	Type of protection this object represents (i.e., Agent, Appliance)
state	EnumState	Computer state
stateDescription	string	Description of the state
status	string	Overall status of the computer
version	string	Version of agent/appliance software
componentInfoTransports	ArrayOfComponentInfoTransport	Component information for this computer
webReputationStatus	string	The status of the Web Reputation module for the computer

SystemEventListTransport

DESCRIPTION A collection of system events

PROPERTIES

Name	Type	Description
systemEvents	ArrayOfSystemEventTransport	The collection of system events

IntegrityEventListTransport

DESCRIPTION A collection of integrity events

PROPERTIES

Name	Type	Description
integrityEvents	ArrayOfIntegrityEventTransport	The collection of integrity events

LogInspectionEventListTransport

DESCRIPTION A collection of log inspection events

PROPERTIES

Name	Type	Description
logInspectionEvents	ArrayOfLogInspectionEventTransport	The collection of log inspection events

ScanFileListTransport

DESCRIPTION Extends ItemsTransport, this is a collection of File Lists.

PROPERTIES

Name	Type	Description

ScanFileExtListTransport

DESCRIPTION Extends ItemsTransport, this is a collection of File Extension Lists.

PROPERTIES

Name	Type	Description

ScanDirectoryListTransport

DESCRIPTION Extends ItemsTransport, this is a collection of Directory Lists.

PROPERTIES

Name	Type	Description

AntiMalwareTransport

DESCRIPTION An object that represents an anti malware configuration object.

PROPERTIES

Name	Type	Description
alert	boolean	Indicates if alerts should be created when events get triggered based on this configuration object
excludeScanDirectoryListID	int	The directory list ID to exclude from scans
excludeScanFileExtListID	int	The File Extension List ID to exclude from scans
excludeScanFileListID	int	The File List ID to exclude from scans
fileToScan	EnumAntiMalwareFilesToScan	What types of files to scan
firstScanAction	EnumAntiMalwareScanCustomAction	The specific custom action to perform
folderToScan	EnumAntiMalwareFoldersToScan	The enum that specifies how to scan folders
scanAction	EnumAntiMalwareScanAction	The default action to perform
intelliTrapEnabled	boolean	Is intellitrap enabled

scanCompressed	boolean	Should compressed files be scanned
scanCompressedLayer	int	Maximum Compressed Layers scannable
scanCompressedSmaller	int	Used by Scan Compressed. The size is in MB
scanCompressedNumberOfFiles	int	The maximum number of files to scan in a compressed file
scanDirList	int	The ID of the Directory list to scan, if folderToScan is setup to point at a specific list
scanFilesActivity	EnumAntiMalwareScanFilesActivity	During real time scan, whether to scan files opened for read, write, or read and write
secondScanAction	EnumAntiMalwareScanCustomAction	The second specific customer action to perform
toScanFileExtListID	int	The File Extension list ID to scan
spywareEnabled	boolean	Is spyware enabled
scanCustomActionForGeneric	EnumAntiMalwareScanCustomAction	A specific custom action to perform for malware classified as generic
unScannableFileAction	EnumAntiMalwareScanCustomAction	A specific custom action to perform for malware the is unscannable
configurationType	EnumAntiMalwareConfigType	Type of config, either for Real-Time scan or Manual/Scheduled
scanNetworkFolder	boolean	If network folders should be scanned
cpuUsage	EnumAntiMalwareCpuUsage	Controls CPU Usage Level
scanOLE	boolean	Scan embedded Microsoft Office objects
scanOLEExploit	boolean	Option to detect exploit code in OLE files
scanOLELayer	int	OLE layers to scan
scanActionForVirus	EnumAntiMalwareScanCustomAction	Scan action for Malware of type Virus
scanActionForTrojans	EnumAntiMalwareScanCustomAction	Scan action for Malware of type Trojans
scanActionForPacker	EnumAntiMalwareScanCustomAction	Scan action for Malware of type Packer

scanActionForSpyware	EnumAntiMalwareScanCustomAction	Scan action for Malware of type Spyware
scanActionForOtherThreats	EnumAntiMalwareScanCustomAction	Scan action for Malware of type other threats
scanActionForCookie	EnumAntiMalwareScanCustomAction	Scan action for Malware of type cookie
excludeScanProcessFileListID	int	File list ID of excluded processes

AntiMalwareSpywareItemTransport

DESCRIPTION Represents an Anti-Malware spyware event and contains all properties that belong to the event.

PROPERTIES

Name	Type	Description
antiMalwareQuarantinedFileID	int	If a file was quarantined as a result of the event, this will contain the ID of the quarantined file
antiMalwareSpywareItemID	int	If a this event was the result of spyware, this will point at the ID of the spyware item
hostID	int	The host ID this event corresponds to
objectInfo	string	File-path, registry key, process name...etc
objectType	int	Type identifier for Process, Cookies, File System, System Registry, Shortcut Link, Host File, Other
riskLevel	int	Risk level gauge Very Low (0), Low (25), Medium(50), High(75), Very High(100)
scanAction	int	Scan Action: The action taken upon each spyware items: Pass (1), Delete (2), Quarantined (3), Clean (4), Deny Access (5)
scanResultAction	int	Represent whether the action is successful (0) or failed (Error Code)
spywareType	int	Type identifier for Adware, Cookie, Dialer, Keylogger, Trojan, Worm, Downloader, etc

AntiMalwareEventTransport

DESCRIPTION Represents an Anti-Malware event

PROPERTIES

Name	Type	Description
antiMalwareConfigID	int	The ID of the Anti-Malware configuration this event corresponds to
antiMalwareEventID	int	The ID of the event
endTime	dateTime	Endtime of this event if it was repeated multiple times (not currently used)
errorCode	int	The VSAPI error code indicates the reason of the actions of failure
hostID	int	The host ID this event corresponds to
infectedFilePath	string	The infected file full path
infectionSource	string	The source computer of the infection
logDate	dateTime	The time this event occurred
malwareName	string	The name of the malware
malwareType	EnumMalwareType	The type of the malware
protocol	int	The protocols: Local Files(0), Network shared folder(1), etc. However, currently Agent only support local files.
quarantineRecordID	int	The ID of the quarantined file, if a file was quarantined as a result of this event
scanResultAction1	int	The result of the first scan action: represent whether the action is successful (0) or failed (Error Code)
scanResultAction2	int	The result of the second scan action: represent whether the action is successful (0) or failed (Error Code)
scanAction1	int	The actual first scan action being taken: e.g. Pass (1), Delete (2), Quarantined (3), Clean (4), Deny Access (5)
scanAction2	int	The actual second scan action being taken: e.g. Pass (1), Delete (2), Quarantined (3), Clean (4), Deny Access (5)

scanType	EnumAntiMalwareScanType	Type of scan this event was captured under

spywareItems	ArrayOfAntiMalwareSpywareItemTransport	An array of spyware items associated with this event
startTime	dateTime	Starttime of this event if it was repeated multiple times (not currently used)
tags	string	Any tags associated with this event
summaryScanResult	string	Summary field for the Scan Result: e.g. passed, deleted, quarantined, cleaned, deny access.

AntiMalwareEventListTransport

DESCRIPTION A list of Anti-Malware events

PROPERTIES

Name	Type	Description
antiMalwareEvents	ArrayOfAntiMalwareEventTransport	The events

AlertStatusTransport

DESCRIPTION An object representing summary information for one individual alert

PROPERTIES

Name	Type	Description
alertDate	dateTime	The time of the alert
alertType	string	The type of the alert
severity	int	The severity of the alert as an integer
severityText	string	The severity of the alert as a string

HostDetailTransport

DESCRIPTION An object that holds detailed information about one computer object. All the "overall" fields are fields created by merging states of potentially multiple endpoints (i.e., Agent + Appliance).

PROPERTIES

Name	Type	Description
antiMalwareClassicPatternVersion	string	Current version of the classic Anti-Malware pattern
antiMalwareEngineVersion	string	Current version of the Anti-Malware engine

antiMalwareIntelliTrapExceptionVersion	string	Current version of the IntelliTrap exception pattern
antiMalwareIntelliTrapVersion	string	Current version of the IntelliTrap pattern
antiMalwareSmartScanPatternVersion	string	Current version of the Smart Scan pattern
antiMalwareSpywarePatternVersion	string	Current version of the Spyware pattern
hostGroupName	string	Name of Group this computer belongs to
cloudObjectImageId	string	Cloud Object Image Id
cloudObjectInstanceId	string	Cloud Object Instance Id
cloudObjectInternalUniqueId	string	Cloud Object Internal Unique Id
cloudObjectSecurityGroupIds	string	Cloud Object Security Group Ids
cloudObjectType	EnumCloudObjectType	Cloud Object Type
hostLight	EnumHostLight	Current color that represents the computers status
lastAnitMalwareScheduledScan	dateTime	Last time an Anti-Malware scheduled scan was performed
lastAntiMalwareEvent	dateTime	The time of the most recent Anti-Malware event for this computer
lastAntiMalwareManualScan	dateTime	Last time an Anti-Malware manual scan was performed
lastDpiEvent	dateTime	The time of the most recent DPI Event for this computer
lastFirewallEvent	dateTime	The time of the most recent Firewall Event for this computer
lastIPUsed	string	The last IP that was used for this computer during communication with the manager
lastIntegrityMonitoringEvent	dateTime	The time of the most recent Integrity Monitoring Event for this computer
lastLogInspectionEvent	dateTime	The time of the most recent Log Inspection Event for this computer
light	int	An integer representing the computers status light
locked	boolean	The locked state of the computer
overallAntiMalwareStatus	string	Overall Anti-Malware status of the computer
overallDpiStatus	string	Overall DPI status of the computer
overallFirewallStatus	string	Overall Firewall status of the computer
overallIntegrityMonitoringStatus	string	Overall Integrity Monitoring status of the computer
overallLastRecommendationScan	dateTime	The time of the last recommendation scan

overallLastSuccessfulCommunication	dateTime	The time of the last communication with the Manager
overallLastSuccessfulUpdate	dateTime	The time of the last successful Configuration Update
overallLastUpdateRequired	dateTime	The time the last configuration update was required at the manager
overallLogInspectionStatus	string	Overall Log Inspection status of the computer
overallStatus	string	Overall status of the computer
overallVersion	string	Overall version of the computer
securityProfileName	string	Name of the security profile assigned to the computer
virtualName	string	Internal virtual name (only populated if this is a computer provisioned through vCenter)
virtualUuid	string	Internal virtual UUID (only populated if this is a computer provisioned through vCenter)
componentKlasses	ArrayOf_xsd_int	Array of class ids for components
componentNames	ArrayOf_xsd_string	Array of component names
componentTypes	ArrayOf_xsd_int	Array of component types
componentVersions	ArrayOf_xsd_string	Array of component versions
overallWebReputationStatus	string	Overall Web Reputation status of the computer
lastWebReputationEvent	dateTime	The time of the most recent Web Reputation event for this computer

HostInterfaceTransport

DESCRIPTION The Host's Interface Transport Object.

PROPERTIES

Name	**Type**	**Description**
dhcp	boolean	DHCP On or Off
hostBridgeId	int	The ID of the Host Bridge
interfaceTypeId	int	The ID of the Interface Type
mac	string	Mac Address
notAvailable	boolean	True is the HostInterface isn't available
virtualDeviceKey	int	The Virtual Device Key

ExternalFilterTransport

DESCRIPTION A filter that can be used to filter by the ExternalID field of a host or host group

PROPERTIES

Name	Type	Description
hostExternalID	string	The ID to filter the host by
hostGroupExternalID	string	The ID to filter the host group by
type	EnumExternalFilterType	The type of filter

WebReputationEventTransport

DESCRIPTION An object representing a web reputation event

PROPERTIES

Name	Type	Description
hostID	int	The ID of the host this event corresponds to
hostName	string	The name of the host this event corresponds to
logTime	dateTime	The time this event occurs
rank	int	The rank of the event
risk	EnumWebReputationEventRisk	The risk level of this event
tags	string	Any tags associated with this event
url	string	The URL that triggered this event
webReputationEventID	int	The ID of the event

WebReputationEventListTransport

DESCRIPTION A list of web reputation event objects.

PROPERTIES

Name	Type	Description
webReputationEvents	ArrayOfWebReputationEventTransport	The web reputation events.

Enumeration Objects

EnumApplicationTypeProtocolType

DESCRIPTION Application Type Protocol enumeration.

Values

ICMP

TCP

UDP

TCP_UDP

EnumAntiMalwareFilesToScan

DESCRIPTION Anti Malware Files to Scan enumeration.

Values

ALLFILES

INTELLISCAN

EXTLISTSCAN

EnumAntiMalwareScanCustomAction

DESCRIPTION Anti Malware Scan Custom Action enumeration.

Values

UNSPECIFIED

PASS

DELETE

QUARANTINE

CLEAN

DENY_ACCESS

EnumAntiMalwareFoldersToScan

DESCRIPTION Anti Malware Folders to Scan enumeration.

Values

ALLFOLDERS

SPECIFIEDFOLDERS

EnumAntiMalwareScanAction

DESCRIPTION Value comparison result enumeration.

Values	INTELLIACTION CUSTOMACTION

EnumAntiMalwareScanFilesActivity

DESCRIPTION Anti Malware Scan Files Activity enumeration.

Values	READ_ONLY WRITE_ONLY READ_WRITE

EnumAntiMalwareConfigType

DESCRIPTION Anti Malware Configuration Type enumeration.

Values	CONFIGURATIONTYPE_RTS CONFIGURATIONTYPE_ODS

EnumAntiMalwareCpuUsage

DESCRIPTION Anti Malware CPU Usage enumeration.

Values	CPUUSAGE_LOW CPUUSAGE_MEDIUM CPUUSAGE_HIGH

EnumAntiMalwareScanType

DESCRIPTION Malware scan type enumeration.

Values	REALTIME MANUAL SCHEDULED QUICK

EnumCompareResults

DESCRIPTION Value comparison result enumeration.

Values

LESS_THAN

EQUAL_TO

GREATER_THAN

INCOMPATIBLE

EnumCounterFilter

DESCRIPTION Counter Filter enumeration.

Values

ANTI_MALWARE_COMPUTER_ACTIVITY

INTEGRITY_COMPUTER_ACTIVITY

LOG_INSPECTION_COMPUTER_ACTIVITY

FIREWALL_DETECT_COMPUTER_ACTIVITY

FIREWALL_PREVENT_COMPUTER_ACTIVITY

FIREWALL_ALL_COMPUTER_ACTIVITY

DPI_DETECT_COMPUTER_ACTIVITY

DPI_PREVENT_COMPUTER_ACTIVITY

DPI_ALL_COMPUTER_ACTIVITY

ANTI_MALWARE_ACTIVITY

ANTI_MALWARE_INCOMPLETE_SCAN

FIREWALL_PREVENT_RULES

FIREWALL_DETECT_RULES

FIREWALL_PREVENT_COMMON_EVENTS

FIREWALL_DETECT_COMMON_EVENTS

FIREWALL_PREVENT_ACTIVITY

FIREWALL_DETECT_ACTIVITY

FIREWALL_ALL_ACTIVITY

FIREWALL_PREVENT_IP_ACTIVITY

FIREWALL_DETECT_IP_ACTIVITY

FIREWALL_PREVENT_PORT_ACTIVITY

FIREWALL_DETECT_PORT_ACTIVITY

DPI_PREVENT_RULES

DPI_DETECT_RULES

DPI_ALL_RULES

DPI_PREVENT_COMMON_EVENTS

DPI_DETECT_COMMON_EVENTS

DPI_ALL_COMMON_EVENTS

DPI_PREVENT_ACTIVITY

DPI_DETECT_ACTIVITY

DPI_PREVENT_IP_ACTIVITY

DPI_DETECT_IP_ACTIVITY

DPI_PREVENT_APP_TYPE_ACTIVITY

DPI_DETECT_APP_TYPE_ACTIVITY

INTEGRITY_ACTIVITY

INTEGRITY_KEY_ACTIVITY

LOG_INSPECTION_ACTIVITY

LOG_INSPECTION_DESCRIPTION_ACTIVITY

ALERT_TYPE

RECONNAISSANCE_SCAN_ACTIVITY

SYSTEM_EVENT_SUMMARY

WEB_REPUTATION_COMPUTER_ACTIVITY

WEB_REPUTATION_URL_ACTIVITY

EnumCounterSumFilter

DESCRIPTION Counter Sum Filter enumeration.

Values

FIREWALL_PREVENT_ACTIVITY

FIREWALL_DETECT_ACTIVITY

FIREWALL_PREVENT_RULES

FIREWALL_DETECT_RULES

FIREWALL_PREVENT_COMMON_EVENTS

FIREWALL_DETECT_COMMON_EVENTS

DPI_PREVENT_ACTIVITY

DPI_DETECT_ACTIVITY

DPI_PREVENT_RULES

DPI_DETECT_RULES

DPI_PREVENT_COMMON_EVENTS

DPI_DETECT_COMMON_EVENTS

INTEGRITY_ACTIVITY

ANTI_MALWARE_ACTIVITY

LOG_INSPECTION_ACTIVITY

LOG_INSPECTION_SEVERITY_LOW

LOG_INSPECTION_SEVERITY_MEDIUM

LOG_INSPECTION_SEVERITY_HIGH

LOG_INSPECTION_SEVERITY_CRITICAL

INTEGRITY_SEVERITY_LOW

INTEGRITY_SEVERITY_MEDIUM

INTEGRITY_SEVERITY_HIGH

INTEGRITY_SEVERITY_CRITICAL

ANTI_MALWARE_SCANACTION_PASS

ANTI_MALWARE_SCANACTION_DELETE

ANTI_MALWARE_SCANACTION_QUARANTINE

ANTI_MALWARE_SCANACTION_CLEAN

ANTI_MALWARE_SCANACTION_DENY_ACCESS

ANTI_MALWARE_SCANACTION_FAILED

WEB_REPUTATION_ACTIVITY

WEB_REPUTATION_RISK_UNTESTED

WEB_REPUTATION_RISK_BLOCKED

WEB_REPUTATION_RISK_SAFE

WEB_REPUTATION_RISK_SUSPICIOUS

WEB_REPUTATION_RISK_HIGHLY_SUSPICIOUS

WEB_REPUTATION_RISK_DANGEROUS

EnumCloudObjectType

DESCRIPTION Cloud Object Types.

Values

AMAZON_VM

VCLOUD_VM

EnumDirection

DESCRIPTION Connection direction enumeration.

Values

INCOMING

OUTGOING

EnumDPIRuleAction

DESCRIPTION DPI rule action enumeration.

Values

DROP_CLOSE

LOG_ONLY

EnumDPIRuleIf

DESCRIPTION DPI rule start/end pattern conditional enumeration.

Values

ALL_PATTERNS_FOUND

ANY_PATTERNS_FOUND

NO_PATTERNS_FOUND

EnumDPIRulePriority

DESCRIPTION DPI rule priority enumeration.

Values

HIGHEST

HIGH

NORMAL

LOW

LOWEST

EnumDPIRuleSeverity

DESCRIPTION DPI rule severity enumeration.

Values

CRITICAL

HIGH

MEDIUM

LOW

EnumDPIRuleTemplateType

DESCRIPTION DPI rule template type enumeration.

Values

CUSTOM_XML

SIGNATURE

START_END_PATTERNS

EnumEditableSettingKey

DESCRIPTION Editable system settings enumeration.

Values

CONFIGURATION_MOTD_TEXT

CONFIGURATION_SPNFB_BANDWIDTHLIMITATION

CONFIGURATION_SPNFB_ENABLEFEEDBACK

CONFIGURATION_SPNFB_ENABLESUSPICIUSFILEFEEDBACK

CONFIGURATION_SPNFB_FEEDBACKINTEVALBYMINUTES

CONFIGURATION_SPNFB_FEEDBACKINTEVALBYTHREATS

CONFIGURATION_SPNFB_INDUSTRYTYPE

CONFIGURATION_AGENTCOMMUNICATIONS

CONFIGURATION_AGENTHARDENING

CONFIGURATION_AGENTHARDENINGPASSWORDFLAG

CONFIGURATION_AGENTHARDENINGPASSWORDVALUE

CONFIGURATION_AGENTINITIATEDACTIVATION

CONFIGURATION_AGENTINITIATEDACTIVATIONACTIVEHOST

CONFIGURATION_AGENTINITIATEDACTIVATIONALLOWHOSTNAME

CONFIGURATION_AGENTINITIATEDACTIVATIONIPLIST

CONFIGURATION_AGENTINITIATEDACTIVATIONSECURITYPROFILE

CONFIGURATION_AGENTLOGFLUSHINTERVAL

CONFIGURATION_ANTIMALWAREGLOBALMANUALSCANCONFIG

CONFIGURATION_ANTIMALWAREGLOBALREALTIMESCANCONFIG

CONFIGURATION_ANTIMALWAREGLOBALREALTIMESCANSCHEDULECONFIG

CONFIGURATION_ANTIMALWAREGLOBALSCHEDULEDSCANCONFIG

CONFIGURATION_ANTIMALWARESTATE

CONFIGURATION_AUTOREQUIRESUPDATE

CONFIGURATION_AUTOUPDATEAPPLIANCECOMPONENTAFTERACTIVATION

CONFIGURATION_AUTOMATICALLYDELETEANTIMALWAREEVENTSOLDERTHANMINUTES

CONFIGURATION_AUTOMATICALLYDELETECOUNTERSOLDERTHANMINUTES

CONFIGURATION_AUTOMATICALLYDELETEDPIEVENTSOLDERTHANMINUTES

CONFIGURATION_AUTOMATICALLYDELETEEVENTSOLDERTHANMINUTES

CONFIGURATION_AUTOMATICALLYDELETEFIREWALLEVENTSOLDERTHANMINUTES

CONFIGURATION_AUTOMATICALLYDELETEINTEGRITYEVENTSOLDERTHANMINUTES

CONFIGURATION_AUTOMATICALLYDELETELOGINSPECTIONEVENTSOLDERTHANMINUTES

CONFIGURATION_AUTOMATICALLYDELETEWEBREPUTATIONEVENTSOLDERTHANMINUTES

CONFIGURATION_AUTOMATICALLYUPDATEIPS

CONFIGURATION_CANHOSTCONTACTGLOBALIAU

CONFIGURATION_CANROAMINGAGENTUPDATECOMPONENT

CONFIGURATION_COLLECTFULLANTIMALWAREEVENTS

CONFIGURATION_COLLECTFULLINTEGRITYEVENTS

CONFIGURATION_COLLECTFULLLOGINSPECTIONEVENTS

CONFIGURATION_CONTEXTS_EXPECTEDCONTENTREGEX

CONFIGURATION_CONTEXTS_TESTINTERVAL

CONFIGURATION_CONTEXTS_TESTURI

CONFIGURATION_DEFAULTALERTEMAIL

CONFIGURATION_DEFAULTFORNEWADMINISTRATORSHIDEUNLICENSEDMODULES

CONFIGURATION_DEFAULTHEARTBEATPERIOD

CONFIGURATION_DETECTIONENGINESTATE

CONFIGURATION_DETECTIONENGINESTATEAUTOAPPLYDPIRULES

CONFIGURATION_DETECTIONENGINESTATEAUTOAPPLYINTEGRITYRULES

CONFIGURATION_DETECTIONENGINESTATEAUTOAPPLYLOGINSPECTIONRULES

CONFIGURATION_DSMGUID

CONFIGURATION_DSRUAUTOAPPLYNEWDSRUS

CONFIGURATION_ENABLEEXCLUSIVEINTERFACES

CONFIGURATION_ENVIRONMENTVARIABLEOVERRIDES

CONFIGURATION_EXCLUSIVEINTERFACEPATTERNS

CONFIGURATION_EXPORTEDFILECHARACTERENCODING

CONFIGURATION_FORWARDLOGS_ANTIMALWARE

CONFIGURATION_FORWARDLOGS_ANTIMALWARE_DIRECT

CONFIGURATION_FORWARDLOGS_INTEGRITY

CONFIGURATION_FORWARDLOGS_INTEGRITY_DIRECT

CONFIGURATION_FORWARDLOGS_LOGINSPECTION

CONFIGURATION_FORWARDLOGS_LOGINSPECTION_DIRECT

CONFIGURATION_FORWARDLOGS_PNP

CONFIGURATION_FORWARDLOGS_PNP_DIRECT

CONFIGURATION_FORWARDLOGS_WRS

CONFIGURATION_FORWARDLOGS_WRS_DIRECT

CONFIGURATION_GENERATEDEVENTSPERMINUTE_ANTIMALWARE

CONFIGURATION_GENERATEDEVENTSPERMINUTE_INTEGRITY

CONFIGURATION_GENERATEDEVENTSPERMINUTE_LOGINSPECTION

CONFIGURATION_GENERATEDEVENTSPERMINUTE_PNP

CONFIGURATION_GENERATEDEVENTSPERMINUTE_WRS

CONFIGURATION_GLOBALSTATEFULCONFIG

CONFIGURATION_INTEGRITYCRITICALRANK

CONFIGURATION_INTEGRITYHIGHRANK

CONFIGURATION_INTEGRITYLOWRANK

CONFIGURATION_INTEGRITYMEDIUMRANK

CONFIGURATION_LOGINSPECTIONAPPLYTAGSTOGROUPS

CONFIGURATION_LOGINSPECTIONCRITICALRANK

CONFIGURATION_LOGINSPECTIONHIGHRANK

CONFIGURATION_LOGINSPECTIONLOWRANK

CONFIGURATION_LOGINSPECTIONMEDIUMRANK

CONFIGURATION_LOGINSPECTIONSTATE

CONFIGURATION_LOGINSPECTIONSTORAGECLIP

CONFIGURATION_LOGINSPECTIONSYSLOGCLIP

CONFIGURATION_LOGGINGOVERRIDE

CONFIGURATION_MAXHOSTCLOCKSHIFT

CONFIGURATION_MAXMISSEDHEARTBEATS

CONFIGURATION_MAXIMUMAGENTINSTALLERSARCHIVED

CONFIGURATION_MAXIMUMSECURITYUPDATESARCHIVED

CONFIGURATION_NETWORKCONTROLSTATE

CONFIGURATION_NETWORKDRIVERMODE

CONFIGURATION_NEWVMSACTIVATIONSECURITYPROFILE

CONFIGURATION_NONNOTIFYINGSYSTEMEVENTS

CONFIGURATION_NONRECORDINGSYSTEMEVENTS

CONFIGURATION_NOTIFICATIONMSGFORAM

CONFIGURATION_NOTIFICATIONMSGFORWP

CONFIGURATION_PACKET_DRIVER_BLOCKIPV6

CONFIGURATION_PACKET_DRIVER_BLOCKIPV6FOR8PLUS

CONFIGURATION_PACKET_DRIVER_BLOCKSAMESRCDSTIP

CONFIGURATION_PACKET_DRIVER_BYPASSWAASCONNECTIONS

CONFIGURATION_PACKET_DRIVER_CONNECTIONEVENTSICMP

CONFIGURATION_PACKET_DRIVER_CONNECTIONEVENTSTCP

CONFIGURATION_PACKET_DRIVER_CONNECTIONEVENTSUDP

CONFIGURATION_PACKET_DRIVER_DEBUGMODE

CONFIGURATION_PACKET_DRIVER_DEBUGPACKETMAX

CONFIGURATION_PACKET_DRIVER_DROP6TO4BOGONS

CONFIGURATION_PACKET_DRIVER_DROPEVASIVERETRANSMIT

CONFIGURATION_PACKET_DRIVER_DROPIPZEROPAYLOAD

CONFIGURATION_PACKET_DRIVER_DROPIPV6BOGONS

CONFIGURATION_PACKET_DRIVER_DROPIPV6MINMTU

CONFIGURATION_PACKET_DRIVER_DROPIPV6RESERVED

CONFIGURATION_PACKET_DRIVER_DROPIPV6SITELOCAL

CONFIGURATION_PACKET_DRIVER_DROPIPV6TYPE0

CONFIGURATION_PACKET_DRIVER_DROPTEREDOANOMALIES

CONFIGURATION_PACKET_DRIVER_DROPTUNNELDEPTHEXCEEDED

CONFIGURATION_PACKET_DRIVER_FILTERIPV4TUNNELS

CONFIGURATION_PACKET_DRIVER_FILTERIPV6TUNNELS

CONFIGURATION_PACKET_DRIVER_FRAGMINOFFSET

CONFIGURATION_PACKET_DRIVER_FRAGMINSIZE

CONFIGURATION_PACKET_DRIVER_IGNORESTATUS0

CONFIGURATION_PACKET_DRIVER_IGNORESTATUS1

CONFIGURATION_PACKET_DRIVER_IGNORESTATUS2

CONFIGURATION_PACKET_DRIVER_LOGRULES

CONFIGURATION_PACKET_DRIVER_LOGSPERSEC

CONFIGURATION_PACKET_DRIVER_MAXCONNECTIONSICMP

CONFIGURATION_PACKET_DRIVER_MAXCONNECTIONSPERIODICCLEANUP

CONFIGURATION_PACKET_DRIVER_MAXCONNECTIONSTCP

CONFIGURATION_PACKET_DRIVER_MAXCONNECTIONSUDP

CONFIGURATION_PACKET_DRIVER_MAXTUNNELDEPTH

CONFIGURATION_PACKET_DRIVER_NODEMAX

CONFIGURATION_PACKET_DRIVER_PASSNULLIP

CONFIGURATION_PACKET_DRIVER_PDUSNAPLENGTH

CONFIGURATION_PACKET_DRIVER_PDUSTATEFUL

CONFIGURATION_PACKET_DRIVER_PDUSTATEFULFIRST

CONFIGURATION_PACKET_DRIVER_PDUSTATEFULPERIOD

CONFIGURATION_PACKET_DRIVER_SETTINGSENABLED

CONFIGURATION_PACKET_DRIVER_SSLSESSIONSIZE

CONFIGURATION_PACKET_DRIVER_SSLSESSIONTIME

CONFIGURATION_PACKET_DRIVER_STRICTTEREDOPORTCHECK

CONFIGURATION_PACKET_DRIVER_TCPMSSLIMIT

CONFIGURATION_PACKET_DRIVER_TCPSILENTRST

CONFIGURATION_PACKET_DRIVER_TIMEOUTACKSTORM

CONFIGURATION_PACKET_DRIVER_TIMEOUTBOOTSTART

CONFIGURATION_PACKET_DRIVER_TIMEOUTCLOSEWAIT

CONFIGURATION_PACKET_DRIVER_TIMEOUTCLOSED

CONFIGURATION_PACKET_DRIVER_TIMEOUTCLOSING

CONFIGURATION_PACKET_DRIVER_TIMEOUTCOLDSTART

CONFIGURATION_PACKET_DRIVER_TIMEOUTCONNCLEANUP

CONFIGURATION_PACKET_DRIVER_TIMEOUTDISCONNECT

CONFIGURATION_PACKET_DRIVER_TIMEOUTERROR

CONFIGURATION_PACKET_DRIVER_TIMEOUTESTAB

CONFIGURATION_PACKET_DRIVER_TIMEOUTFINWAIT

CONFIGURATION_PACKET_DRIVER_TIMEOUTICMP

CONFIGURATION_PACKET_DRIVER_TIMEOUTLASTACK

CONFIGURATION_PACKET_DRIVER_TIMEOUTSYNRCVD

CONFIGURATION_PACKET_DRIVER_TIMEOUTSYNSENT

CONFIGURATION_PACKET_DRIVER_TIMEOUTUDP

CONFIGURATION_PACKET_DRIVER_VERIFYTCPCHECKSUM

CONFIGURATION_PACKETFILTERDENYRANK

CONFIGURATION_PACKETFILTERLOGONLYRANK

CONFIGURATION_PACKETFILTERREJECTIONRANK

CONFIGURATION_PACKETLOG_CACHELIFETIME

CONFIGURATION_PACKETLOG_CACHESIZE

CONFIGURATION_PACKETLOG_CACHESTALETIME

CONFIGURATION_PACKETLOG_IGNORE

CONFIGURATION_PACKETLOG_KEEP

CONFIGURATION_PACKETLOG_LOGOUTOFALLOWEDPOLICY

CONFIGURATION_PACKETLOG_MAXSIZE

CONFIGURATION_PAYLOAD_DRIVER_IPFRAGSENDTIMEEXCEEDED

CONFIGURATION_PAYLOAD_DRIVER_MAXIPFRAG

CONFIGURATION_PAYLOAD_DRIVER_SETTINGSENABLED

CONFIGURATION_PAYLOAD_DRIVER_TIMEOUTFRAGMENT

CONFIGURATION_PAYLOADFILTERCRITICALRANK

CONFIGURATION_PAYLOADFILTERERRORRANK

CONFIGURATION_PAYLOADFILTERHIGHRANK

CONFIGURATION_PAYLOADFILTERLOWRANK

CONFIGURATION_PAYLOADFILTERMEDIUMRANK

CONFIGURATION_PAYLOADLOGFIRSTPDU

CONFIGURATION_PENDINGAGENTUPDATEALERTLIMIT

CONFIGURATION_PORTSTOSCAN

CONFIGURATION_QUARANTINE_MAXFILESIZE

CONFIGURATION_QUARANTINE_MAXGUESTSPACE

CONFIGURATION_QUARANTINE_MAXQUARANTINEDSPACE

CONFIGURATION_RAISEAGENTOFFLINEERRORSFORINACTIVEVMS

CONFIGURATION_RECOMMENDATIONMONITORINTERVAL

CONFIGURATION_RELAYUPDATESOURCE

CONFIGURATION_RELAYUPDATESOURCE_OTHERAU_URL

CONFIGURATION_SCANLIMITATION_MAXFILESCANSIZE

CONFIGURATION_SINGLEEXCLUSIVEINTERFACEENABLED

CONFIGURATION_SMARTPROTECTIONSERVER_PROXYIDFORGLOBALSERVER

CONFIGURATION_SMARTPROTECTIONSERVER_SMARTSCANALLOWFALLBACK

CONFIGURATION_SMARTPROTECTIONSERVER_SMARTSCANLOCALSERVERS

CONFIGURATION_SMARTPROTECTIONSERVER_SMARTSCANUSEGLOBALSERVER

CONFIGURATION_SMARTPROTECTIONSERVER_SMARTSCANUSEPROXYFORGLOBALSERVER

CONFIGURATION_SMARTPROTECTIONSERVER_WEBREPUTATIONALLOWGLOBAL

CONFIGURATION_SMARTPROTECTIONSERVER_WEBREPUTATIONLOCALRATINGSERVER

CONFIGURATION_SMARTPROTECTIONSERVER_WEBREPUTATIONRATINGSERVERPROXYID

CONFIGURATION_SMARTPROTECTIONSERVER_WEBREPUTATIONUSELOCALRATINGSERVER

CONFIGURATION_SMARTPROTECTIONSERVER_WEBREPUTATIONUSEPROXYFORGLOBALSERVER

CONFIGURATION_SMARTSCANSTATE

CONFIGURATION_SPYWAREAPPROVEDLIST

CONFIGURATION_SYSLOGFACILITY_ANTIMALWARE

CONFIGURATION_SYSLOGFACILITY_INTEGRITY

CONFIGURATION_SYSLOGFACILITY_LOGINSPECTION

CONFIGURATION_SYSLOGFACILITY_PNP

CONFIGURATION_SYSLOGFACILITY_WRS

CONFIGURATION_SYSLOGFORMAT_ANTIMALWARE

CONFIGURATION_SYSLOGFORMAT_INTEGRITY

CONFIGURATION_SYSLOGFORMAT_LOGINSPECTION

CONFIGURATION_SYSLOGFORMAT_PNP

CONFIGURATION_SYSLOGFORMAT_WRS

CONFIGURATION_SYSLOGHOST_ANTIMALWARE

CONFIGURATION_SYSLOGHOST_INTEGRITY

CONFIGURATION_SYSLOGHOST_LOGINSPECTION

CONFIGURATION_SYSLOGHOST_PNP

CONFIGURATION_SYSLOGHOST_WRS

CONFIGURATION_SYSLOGOVERRIDE_ANTIMALWARE

CONFIGURATION_SYSLOGOVERRIDE_INTEGRITY

CONFIGURATION_SYSLOGOVERRIDE_LOGINSPECTION

CONFIGURATION_SYSLOGOVERRIDE_PNP

CONFIGURATION_SYSLOGOVERRIDE_WRS

CONFIGURATION_SYSLOGPORT_ANTIMALWARE

CONFIGURATION_SYSLOGPORT_INTEGRITY

CONFIGURATION_SYSLOGPORT_LOGINSPECTION

CONFIGURATION_SYSLOGPORT_PNP

CONFIGURATION_SYSLOGPORT_WRS

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSCRIPTS

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSEXTENDEDDESCRIPTIONS

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSNMPADDRESS

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSNMPCOMMUNITY

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSNMPENABLED

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSNMPPORT

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSNMPRETRIES

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSNMPTIMEOUT

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSYSLOGADDRESS

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSYSLOGENABLED

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSYSLOGFACILITY

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSYSLOGFORMAT

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSYSLOGIDENTIFICATION

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSYSLOGPORT

CONFIGURATION_SYSTEMEVENTNOTIFICATIONSSYSLOGPREPENDTIMESTAMP

CONFIGURATION_SYSTEMINTEGRITYHASH

CONFIGURATION_SYSTEMINTEGRITYSTATE

CONFIGURATION_TRAFFICANALYSIS_FINGERPRINT_BLOCK

CONFIGURATION_TRAFFICANALYSIS_FINGERPRINT_ENABLED

CONFIGURATION_TRAFFICANALYSIS_FINGERPRINT_NOTIFY

CONFIGURATION_TRAFFICANALYSIS_GLOBAL_ANALYZE

CONFIGURATION_TRAFFICANALYSIS_GLOBAL_ENABLED

CONFIGURATION_TRAFFICANALYSIS_GLOBAL_IGNORE

CONFIGURATION_TRAFFICANALYSIS_NULL_BLOCK

CONFIGURATION_TRAFFICANALYSIS_NULL_ENABLED

CONFIGURATION_TRAFFICANALYSIS_NULL_NOTIFY

CONFIGURATION_TRAFFICANALYSIS_SCAN_BLOCK

CONFIGURATION_TRAFFICANALYSIS_SCAN_ENABLED

CONFIGURATION_TRAFFICANALYSIS_SCAN_NOTIFY

CONFIGURATION_TRAFFICANALYSIS_SYNFIN_BLOCK

CONFIGURATION_TRAFFICANALYSIS_SYNFIN_ENABLED

CONFIGURATION_TRAFFICANALYSIS_SYNFIN_NOTIFY

CONFIGURATION_TRAFFICANALYSIS_XMAS_BLOCK

CONFIGURATION_TRAFFICANALYSIS_XMAS_ENABLED

CONFIGURATION_TRAFFICANALYSIS_XMAS_NOTIFY

CONFIGURATION_UPDATEPROXYAUTH

CONFIGURATION_UPDATEPROXYFLAG

CONFIGURATION_UPDATEPROXYHOST

CONFIGURATION_UPDATEPROXYID

CONFIGURATION_UPDATEPROXYPASS

CONFIGURATION_UPDATEPROXYPORT

CONFIGURATION_UPDATEPROXYTYPE

CONFIGURATION_UPDATEPROXYUSER

CONFIGURATION_UPDATESOURCE

CONFIGURATION_UPDATESOURCE_INTRANET_UNC

CONFIGURATION_UPDATESOURCE_INTRANET_PASSWORD

CONFIGURATION_UPDATESOURCE_INTRANET_USER

CONFIGURATION_UPDATESOURCE_OTHERAU_URL

CONFIGURATION_VSUAUTOASSIGN

CONFIGURATION_VULNERABILITYSHIELDSTATE

CONFIGURATION_WEBREPUTATIONALERTINGON

CONFIGURATION_WEBREPUTATIONALLOWEDDOMAINURLS

CONFIGURATION_WEBREPUTATIONALLOWEDPAGEURLS

CONFIGURATION_WEBREPUTATIONBLOCKUNTESTEDPAGES

CONFIGURATION_WEBREPUTATIONBLOCKEDBYADMINISTRATORRANK

CONFIGURATION_WEBREPUTATIONBLOCKEDDOMAINURLS

CONFIGURATION_WEBREPUTATIONBLOCKEDKEYWORDS

CONFIGURATION_WEBREPUTATIONBLOCKEDPAGELINK

CONFIGURATION_WEBREPUTATIONBLOCKEDPAGEURLS

CONFIGURATION_WEBREPUTATIONDANGEROUSRANK

CONFIGURATION_WEBREPUTATIONENABLED

CONFIGURATION_WEBREPUTATIONHIGHLYSUSPICIOUSRANK

CONFIGURATION_WEBREPUTATIONPORTS

CONFIGURATION_WEBREPUTATIONSECURITYLEVEL

CONFIGURATION_WEBREPUTATIONSUSPICIOUSRANK

CONFIGURATION_WEBREPUTATIONUNTESTEDRANK

CONFIGURATION_WEBSERVICEAPIENABLED

LICENSES_HISTORIC

SECURITY_ACTIVESESSIONSALLOWED

SECURITY_ADMINISTRATORPASSWORDEXPIRY

SECURITY_ADMINISTRATORPASSWORDMINIMUMLENGTH

SECURITY_ADMINISTRATORPASSWORDREQUIRECASE

SECURITY_ADMINISTRATORPASSWORDREQUIREMIX

SECURITY_ADMINISTRATORPASSWORDREQUIRESPECIAL

SECURITY_MINUTESTOTIMEOUT

SECURITY_SIGNINATTEMPTSALLOWED

SMTP_BOUNCEEMAIL

SMTP_FROMEMAIL

SMTP_PASSWORD

SMTP_REQUIRESAUTHENTICATION

SMTP_URL

SMTP_USERNAME

WHOIS_IP

EnumEditableSettingStoredScope

DESCRIPTION Editable setting scope enumeration. This enumeration indicates which level to assign the setting to, such as configuring the Syslog target settings at the Computer/Host level, or at the Security Profile level.

Values

HOST

PROFILE

SYSTEM

EnumEditableSettingUnit

DESCRIPTION Editable setting unit enumeration. This enumeration indicates a system settings unit or type.

Values

IPLIST_ID

PORTLIST_ID

NONE

SECONDS

MINUTES

HOURS

DAYS

WEEKS

MONTHS

YEARS

KBYTES

PERCENT

PORT

HOST

EMAIL

EnumEventOrigin

DESCRIPTION The origin of an event enumeration.

Values

UNKNOWN

AGENT

GUESTAGENT

APPLIANCEAGENT

MANAGER

EnumExternalFilterType

DESCRIPTION The action a Firewall rule should result in once applied enumeration.

Values

ALL_EXT_HOSTS

HOSTS_IN_EXT_GROUP

HOSTS_IN_EXT_GROUP_AND_ALL_SUBGROUPS

SPECIFIC_EXT_HOST

EnumFirewallRuleAction

DESCRIPTION The action a Firewall rule should result in once applied enumeration.

Values

LOG_ONLY

ALLOW

DENY

FORCE_ALLOW

BYPASS

EnumFirewallRuleFrameType

DESCRIPTION A Firewall rule frame type enumeration.

Values

ANY

IP

ARP

REVARP

OTHER

EnumFirewallRuleIPType

DESCRIPTION A Firewall rule IP type enumeration.

Values

ANY

MASKED_IP

RANGE

DEFINED_LIST

SINGLE_IP

EnumFirewallRulePriority

DESCRIPTION A Firewall rule Priority enumeration.

Values

HIGHEST

HIGH

NORMAL

LOW

LOWEST

EnumFirewallRuleProtocolType

DESCRIPTION A Firewall rule Protocol type enumeration.

Values

ANY

ICMP

ICMPV6

IGMP

GGP

TCP

PUP

UDP

IDP

ND

RAW

TCP_UDP

OTHER

EnumHostDetailLevel

DESCRIPTION	Host/Computer detail level enumeration.
Values	LOW MEDIUM HIGH

EnumHostFilterType

DESCRIPTION	Host/Computer filter type used when filtering retrieved events by Host, Group, Security Profile or specific Hosts.
Values	ALL_HOSTS HOSTS_IN_GROUP HOSTS_USING_SECURITY_PROFILE HOSTS_IN_GROUP_AND_ALL_SUBGROUPS SPECIFIC_HOST MY_HOSTS

EnumHostLight

DESCRIPTION	Host/Computer Light color enumeration.
Values	GREEN YELLOW RED GREY BLUE

EnumHostType

DESCRIPTION	Host/Computer type enumeration. Used to determine if the retrieve HostTransport object is a VM, standard physical computer, ESX server, or Virtual Appliance.
Values	STANDARD ESX APPLIANCE VM

EnumIntegrityRuleSeverity

DESCRIPTION	Integrity Monitoring rule severity enumeration.
Values	CRITICAL HIGH MEDIUM LOW

EnumJobType

DESCRIPTION	Job Type enumeration.
Values	UPDATE

EnumMalwareType

DESCRIPTION	Malware type enumeration.
Values	GENERAL SPYWARE

EnumMACType

DESCRIPTION	MAC List type enumeration.
Values	ANY MAC DEFINED_LIST

EnumOperator

DESCRIPTION	General filter operator enumeration. Used when filtering retrieved events by event ID that are greater than, less than, or equal to.
Values	GREATER_THAN LESS_THAN EQUAL

EnumPortType

DESCRIPTION Port List type enumeration.

Values

ANY

MAC

DEFINED_LIST

EnumProtectionType

DESCRIPTION Computer protection type enumeration. Protection for a computer can be applied by an installed Agent or by the Deep Security Virtual Appliance.

Values

NONE

AGENT

APPLIANCE

EnumProtocolIcmpType

DESCRIPTION ICMP protocol type enumeration.

Values

ICMP_ECHO

ICMP_TIMESTAMP

ICMP_INFORMATION

ICMP_ADDRESS_MASK

ICMP_MOBILE_REGISTRATION

EnumSecurityProfileDPIState

DESCRIPTION Security Profile DPI configured state enumeration.

Values

ON

OFF

PASSIVE

INHERITED

EnumSecurityProfileFirewallState

DESCRIPTION Security Profile Firewall configured state enumeration.

Values

- ON
- OFF
- INHERITED

EnumSecurityProfileAntiMalwareState

DESCRIPTION Security Profile Anti Malware configured state enumeration.

Values

- ON
- OFF
- INHERITED

EnumSecurityProfileIntegrityState

DESCRIPTION Security Profile Integrity Monitoring configured state enumeration.

Values

- ON
- OFF
- INHERITED

EnumSecurityProfileLogInspectionState

DESCRIPTION Security Profile Log Inspection configured state enumeration.

Values

- ON
- OFF
- INHERITED

EnumSecurityProfileRecommendationState

DESCRIPTION Security Profile Recommendation Engine configured state enumeration.

Values

- OFF
- ONGOING

EnumWebReputationEventRisk

DESCRIPTION Web Reputation Event Risk enumeration.

Values

SAFE

SUSPICIOUS

HIGHLYSUSPICIOUS

DANGEROUS

UNTESTED

BLOCKEDBYADMINISTRATOR

EnumSecurityUpdateAppliedState

DESCRIPTION Security Update applied state. Can be used to determine if a retrieved or applied Security Update has been applied and is currently active.

Values

APPLIED

APPLIED_CURRENT

NOT_APPLIED

EnumState

DESCRIPTION Computer HostTransport state enumeration that can be used to determine what state a computer is currently in.

Values

NEUTRAL

VM_STOPPED

VM_PAUSED

STANDBY

UNKNOWN

NONE

INSTALLED

HAS_DSM_CERT

ACTIVATED

OTHER_DSM_AGENT

OFFLINE

EnumTagFilterType

DESCRIPTION	Tag Filters Type enumeration.
Values	ALL UNTAGGED TAGS

EnumTimeFilterType

DESCRIPTION	Time based filter enumeration. Used when filtering retrieved events by event time.
Values	LAST_HOUR LAST_24_HOURS LAST_7_DAYS CUSTOM_RANGE SPECIFIC_TIME

EnumRuleType

DESCRIPTION	Rule Type enumeration.
Values	APPLICATIONTYPE PAYLOADFILTER FIREWALLRULE INTEGRITYRULE LOGINSPECTIONRULE

Web Methods

softwareRetrieveForHost()

DESCRIPTION Retrieves the software for a provided host id.

SYNTAX

```
SoftwareTransport[] softwareRetrieveForHost(int hostID, String sID)
```

PARAMETERS

hostID	Identifying Host ID.
sID	Authentication session token ID.

RETURNS SoftwareTransport object array.

softwareVersionStringsCompare()

DESCRIPTION Compares two software version strings.

SYNTAX

```
EnumCompareResults softwareVersionStringsCompare(String version1, String version2, String sID)
```

PARAMETERS

version1	First version to compare.
version2	Second version to compare.
sID	Authentication session token ID.

RETURNS -1 if version1 < version2
0 if version1 = version2
1 if version1 > version2
2 if version1 and version2 are incompatible version types.

systemInformationRetrieve()

DESCRIPTION Retrieves system information.

SYNTAX

```
SystemInformationTransport[] systemInformationRetrieve(String sID)
```

PARAMETERS

sID Authentication session token ID.

RETURNS SystemInformationTransport object array.

hostGroupRetrieve()

DESCRIPTION Retrieves a Host Group by ID.

SYNTAX

```
HostGroupTransport hostGroupRetrieve(int ID, String sID)
```

PARAMETERS

ID Identifying Host Group ID.

sID Authentication session identifier ID.

RETURNS HostGroupTransport object.

hostGroupRetrieveByName()

DESCRIPTION Retrieves a Host Group by name.

SYNTAX

```
HostGroupTransport hostGroupRetrieveByName(String Name, String sID)
```

PARAMETERS

Name Identifying Host Group name.

sID Authentication session identifier ID.

RETURNS HostGroupTransport object.

hostGroupRetrieveAll()

DESCRIPTION Retrieves all Host Groups.

SYNTAX

```
HostGroupTransport[] hostGroupRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS HostGroupTransport object array.

hostGroupDelete()

DESCRIPTION Deletes a Host Group by ID.

SYNTAX

```
void hostGroupDelete(int ID, String sID)
```

PARAMETERS

ID	Identifying Host Group ID.
sID	Authentication session identifier ID.

hostGroupCreate()

DESCRIPTION Creates a new Host Group.

SYNTAX

```
HostGroupTransport hostGroupCreate(HostGroupTransport hostGroup, String sID)
```

PARAMETERS

hostGroup	HostGroupTransport object to create.
sID	Authentication session identifier ID.

RETURNS Newly created HostGroupTransport object.

softwareApplyToHosts()

DESCRIPTION Apply an Agent software install to hosts by IDs.

SYNTAX

```
void softwareApplyToHosts(int[] hostIDs, String installerVersion, String sID)
```

PARAMETERS

hostIDs	Array of host IDs to apply software to.
installerVersion	The version of the software install to apply.
sID	Authentication session identifier ID.

RETURNS Security Center customer account username.

softwareStore()

DESCRIPTION Uploads and stores an Agent software installer on the Manager.

SYNTAX

```
SoftwareTransport softwareStore(byte[] software, String fileName, String notes, String sID)
```

PARAMETERS

software	Byte array representation of the software to upload and store.
fileName	The filename of the software.
notes	Any notes to associate with the software file.
sID	Authentication session identifier ID.

RETURNS The resulting uploaded SoftwareTransport object.

softwareRetrieve()

DESCRIPTION Retrieves Agent install file SoftwareTransport object by ID.

SYNTAX

```
SoftwareTransport softwareRetrieve(int ID, String sID)
```

PARAMETERS

ID SoftwareTransport ID.

sID Authentication session identifier ID.

RETURNS The resulting uploaded SoftwareTransport object.

softwareRetrieveAll()

DESCRIPTION Retrieves all Agent install file SoftwareTransport objects.

SYNTAX

```
SoftwareTransport[] softwareRetrieveAll(String sID)
```

PARAMETERS

sID Authentication session identifier ID.

RETURNS SoftwareTransport object array.

softwareExport()

DESCRIPTION Retrieves byte array representation of Agent install file object by ID.

SYNTAX

```
byte[] softwareExport(int id, String sID)
```

PARAMETERS

ID SoftwareTransport ID.

sID Authentication session identifier ID.

RETURNS Byte array representation of the retrieved software file.

softwareDelete()

DESCRIPTION	Deletes Agent install file by ID.

SYNTAX

```
void softwareDelete(int[] ids, String sID)
```

PARAMETERS

ids	The list of agent installers to delete
sID	Authentication session identifier ID.

securityUpdateStore()

DESCRIPTION	Stores the provided Security Update on the Manager.

SYNTAX

```
SecurityUpdateTransport securityUpdateStore(byte[] securityUpdate, String fileName, String sID)
```

PARAMETERS

securityUpdate	The raw Security Update as provided by Security Center
fileName	The name of the Security Update
sID	Authentication session identifier ID.
RETURNS	SecurityUpdateTransport object

securityUpdateGetApplierInformation()

DESCRIPTION	Retrieves Security Update information on what would be applied.

SYNTAX

```
ApplierInformationTransport securityUpdateGetApplierInformation(int ID, String sID)
```

PARAMETERS

ID	Security Update ID.
sID	Authentication session identifier ID.
RETURNS	ApplierInformationTransport object.

securityUpdateApply()

DESCRIPTION Applies a Security Update.

SYNTAX

```
ApplierInformationTransport securityUpdateApply(int ID, boolean detectOnly, String sID)
```

PARAMETERS

ID Security Update ID.

detectOnly Apply in detect only mode.

sID Authentication session identifier ID.

RETURNS ApplierInformationTransport object of the applied Security Update.

securityUpdateRetrieve()

DESCRIPTION Retrieves Security Update.

SYNTAX

```
SecurityUpdateTransport securityUpdateRetrieve(int ID, String sID)
```

PARAMETERS

ID Security Update ID.

sID Authentication session identifier ID.

RETURNS SecurityUpdateTransport object.

securityUpdateRetrieveAll()

DESCRIPTION Retrieves all Security Updates.

SYNTAX

```
SecurityUpdateTransport[] securityUpdateRetrieveAll(String sID)
```

PARAMETERS

sID Authentication session identifier ID.

RETURNS SecurityUpdateTransport object array.

securityUpdateExport()

DESCRIPTION Retrieves byte array representation of a Security Update.

SYNTAX

```
byte[] securityUpdateExport(int ID, String sID)
```

PARAMETERS

ID	Security Update ID.
sID	Authentication session identifier ID.

RETURNS Byte array representation of the exported Security Update file.

securityUpdateDelete()

DESCRIPTION Deletes a Security Update.

SYNTAX

```
void securityUpdateDelete(int[] ids, String sID)
```

PARAMETERS

ids	Array of Security Update IDs to delete.
sID	Authentication session identifier ID.

getApiVersion()

DESCRIPTION Retrieves the Manager Web Service API version. Not the same as the Manager version.

SYNTAX

```
int getApiVersion()
```

PARAMETERS

RETURNS The Web Service API version.

getManagerTime()

DESCRIPTION Retrieve the Manager Web Service API version. Not the same as the Manager version.

SYNTAX

```
Date getManagerTime()
```

PARAMETERS

RETURNS Manager time as a language localized object. For example, a Java client would return a Calendar object, and a C# client would return a DataTime object.

authenticate()

DESCRIPTION Authenticates a user for and returns a session ID for use when calling other Web Service methods.

SYNTAX

```
String authenticate(String username, String password)
```

PARAMETERS

username Account username.

password Account password.

RETURNS Authenticated user session ID.

authenticateTenant ()

DESCRIPTION Authenticates a user within the given tenant, and returns a session ID for use when calling other methods of Manager. When no longer required, the session should be terminated by calling endSession.

SYNTAX

```
String authenticateTenant(String tenantName, String username, String password)
```

PARAMETERS

tenantName Tenant Name.

username Account username.

password Account password.

RETURNS Authenticated user session ID.

endSession()

DESCRIPTION Ends an authenticated user session. The Web Service client should end the authentication session in all exit cases.

SYNTAX

```
void endSession(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS

portListDelete()

DESCRIPTION Deletes Port Lists by ID.

SYNTAX

```
void portListDelete(int[] ids, String sID)
```

PARAMETERS

ids	Port List IDs to delete.
sID	Authentication session identifier ID.

RETURNS

portListSave()

DESCRIPTION Saves a new or existing Port List.

SYNTAX

```
PortListTransport portListSave(PortListTransport pl, String sID)
```

PARAMETERS

pl	PortListTransport object to create.
sID	Authentication session identifier ID.

RETURNS Newly created PortListTransport object.

portListRetrieve()

DESCRIPTION Retrieves a Port List by ID.

SYNTAX

```
PortListTransport portListRetrieve(int ID, String sID)
```

PARAMETERS

ID	Port List ID.
sID	Authentication session identifier ID.

RETURNS PortListTransport object.

portListRetrieveByName()

DESCRIPTION Retrieves a Port List by name.

SYNTAX

```
PortListTransport portListRetrieveByName(String name, String sID)
```

PARAMETERS

name	Port List name.
sID	Authentication session identifier ID.

RETURNS PortListTransport object.

portListRetrieveAll()

DESCRIPTION Retrieves all Port Lists.

SYNTAX

```
PortListTransport[] portListRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS PortListTransport object array.

MACListDelete()

DESCRIPTION Deletes MAC Lists by ID.

SYNTAX

void MACListDelete(int[] IDs, String sID)

PARAMETERS

IDs	MAC List IDs to delete.
sID	Authentication session identifier ID.

MACListSave()

DESCRIPTION Saves a new or existing MAC List.

SYNTAX

MACListTransport MACListSave(MACListTransport ml, String sID)

PARAMETERS

ml	MACListTransport object to create.
sID	Authentication session identifier ID.

RETURNS Newly created MACListTransport object.

MACListRetrieve()

DESCRIPTION Retrieves a MAC List by ID.

SYNTAX

MACListTransport MACListRetrieve(int ID, String sID)

PARAMETERS

ID	MAC List ID.
sID	Authentication session identifier ID.

RETURNS MACListTransport object.

MACListRetrieveByName()

DESCRIPTION Retrieves a MAC List by name.

SYNTAX

```
MACListTransport MACListRetrieveByName(String name, String sID)
```

PARAMETERS

name	MAC List name.
sID	Authentication session identifier ID.

RETURNS MACListTransport object.

MACListRetrieveAll()

DESCRIPTION Retrieves all MAC Lists.

SYNTAX

```
MACListTransport[]MACListRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS MACListTransport object array.

IPListDelete()

DESCRIPTION Deletes IP Lists by ID.

SYNTAX

```
void IPListDelete(int[] ids, String sID)
```

PARAMETERS

ids	IP List IDs to delete.
sID	Authentication session identifier ID.

IPListSave()

DESCRIPTION Saves a new or existing IP List.

SYNTAX

IPListTransport IPListSave(MACListTransport ipl, String sID)

PARAMETERS

ipl	IPListTransport object to create.
sID	Authentication session identifier ID.

RETURNS Newly created IPListTransport object.

IPListRetrieve()

DESCRIPTION Retrieves an IP List by ID.

SYNTAX

IPListTransport IPListRetrieve(int ID, String sID)

PARAMETERS

ID	IP List ID.
sID	Authentication session identifier ID.

RETURNS IPListTransport object.

IPListRetrieveByName()

DESCRIPTION Retrieves an IP List by name.

SYNTAX

IPListTransport IPListRetrieveByName(String name, String sID)

PARAMETERS

name	IP List name.
sID	Authentication session identifier ID.

RETURNS IPListTransport object.

IPListRetrieveAll()

DESCRIPTION Retrieves all IP Lists.

SYNTAX

```
IPListTransport[] IPListRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS IPListTransport object array.

applicationTypeDelete()

DESCRIPTION Deletes Application Type by ID. Note that Application Types issued by Trend Micro cannot be deleted.

SYNTAX

```
void applicationTypeDelete(int[] ids, String sID)
```

PARAMETERS

ids	Application Type IDs to delete.
sID	Authentication session identifier ID.

RETURNS

applicationTypeSave()

DESCRIPTION Saves a new or existing Application Type. Note that Application Types issued by Trend Micro cannot be saved.

SYNTAX

```
ApplicationTypeTransport applicationTypeSave(ApplicationTypeTransport at, String sID)
```

PARAMETERS

at	ApplicationTypeTransport object to create.
sID	Authentication session identifier ID.

RETURNS Newly created ApplicationTypeTransport object.

applicationTypeRetrieve()

DESCRIPTION Retrieves an Application Type by ID.

SYNTAX

```
ApplicationTypeTransport applicationTypeRetrieve (int ID, String sID)
```

PARAMETERS

ID	Application Type ID.
sID	Authentication session identifier ID.

RETURNS ApplicationTypeTransport object.

applicationTypeRetrieveByName()

DESCRIPTION Retrieves an Application Type by name.

SYNTAX

```
ApplicationTypeTransport applicationTypeRetrieveByName(String name, String sID)
```

PARAMETERS

name	Application Type name.
sID	Authentication session identifier ID.

RETURNS ApplicationTypeTransport object.

applicationTypeRetrieveAll()

DESCRIPTION Retrieves all Application Types.

SYNTAX

```
ApplicationTypeTransport[] applicationTypeRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS ApplicationTypeTransport object array.

applicationTypeOverrideDelete()

DESCRIPTION Deletes Application Type Override by ID.

SYNTAX

void applicationTypeOverrideDelete(int[] ids, String sID)

PARAMETERS

ids	Application Type Override IDs to delete.
sID	Authentication session identifier ID.

RETURNS

applicationTypeOverrideSave()

DESCRIPTION Saves a new or existing Application Type Override.

SYNTAX

ApplicationTypeOverrideTransport applicationTypeOverrideSave(ApplicationTypeOverrideTransport at, String sID)

PARAMETERS

at	ApplicationTypeOverrideTransport object to save.
sID	Authentication session identifier ID.

RETURNS Newly created or updated ApplicationTypeOverrideTransport object.

applicationTypeOverrideRetrieve()

DESCRIPTION Retrieves an Application Type Override by ID.

SYNTAX

ApplicationTypeOverrideTransport applicationTypeOverrideRetrieve (int ID, String sID)

PARAMETERS

ID	Application Type Override ID.
sID	Authentication session identifier ID.

RETURNS ApplicationTypeOverrideTransport object.

applicationTypeOverrideRetrieveAll()

DESCRIPTION Retrieves all Application Type Overrides.

SYNTAX

```
ApplicationTypeOverrideTransport[] applicationTypeOverrideRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS ApplicationTypeOverrideTransport object array.

firewallRuleDelete()

DESCRIPTION Deletes Firewall Rules by ID.

SYNTAX

```
void firewallRuleDelete(int[] ids, String sID)
```

PARAMETERS

ids	Firewall Rule IDs to delete.
sID	Authentication session identifier ID.

firewallRuleSave()

DESCRIPTION Saves a new or existing Firewall Rule.

SYNTAX

```
FirewallRuleTransport firewallRuleSave(FirewallRuleTransport fr, String sID)
```

PARAMETERS

fr	FirewallRuleTransport object to create.
sID	Authentication session identifier ID.

RETURNS Newly created FirewallRuleTransport object.

firewallRuleRetrieve()

DESCRIPTION Retrieves a Firewall Rule by ID.

SYNTAX

```
FirewallRuleTransport firewallRuleRetrieve(int ID, String sID)
```

PARAMETERS

ID	Firewall Rule ID.
sID	Authentication session identifier ID.

RETURNS FirewallRuleTransport object.

firewallRuleRetrieveByName()

DESCRIPTION Retrieves a Firewall Rule by name.

SYNTAX

```
FirewallRuleTransport firewallRuleRetrieveByName(String name, String sID)
```

PARAMETERS

name	Firewall Rule name.
sID	Authentication session identifier ID.

RETURNS FirewallRuleTransport object.

firewallRuleRetrieveAll()

DESCRIPTION Retrieves all Firewall Rule.

SYNTAX

```
FirewallRuleTransport[] firewallRuleRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS FirewallRuleTransport object array.

DPIRuleDelete()

DESCRIPTION Deletes DPI Rules by ID.

SYNTAX

void DPIRuleDelete(int[] ids, String sID)

PARAMETERS

ids	DPI Rule IDs to delete.
sID	Authentication session identifier ID.

DPIRuleSave()

DESCRIPTION Saves a new or existing DPI Rule.

SYNTAX

DPIRuleTransport DPIRuleSave(DPIRuleTransport ipsf, String sID)

PARAMETERS

ipsf	The DPIRuleTransport to save.
sID	Authentication session identifier ID.

RETURNS Newly created DPIRuleTransport object.

DPIRuleRetrieve()

DESCRIPTION Retrieves a DPI Rule by ID.

SYNTAX

DPIRuleTransport DPIRuleRetrieve(int ID, String sID)

PARAMETERS

ID	DPI Rule ID.
sID	Authentication session identifier ID.

RETURNS DPIRuleTransport object.

DPIRuleRetrieveByName()

DESCRIPTION Retrieves a DPI Rule by name.

SYNTAX

```
DPIRuleTransport DPIRuleRetrieveByName(String name, String sID)
```

PARAMETERS

name	DPI Rule name.
sID	Authentication session identifier ID.

RETURNS DPIRuleTransport object.

DPIRuleRetrieveAll()

DESCRIPTION Retrieves all DPI Rule.

SYNTAX

```
DPIRuleTransport[] DPIRuleRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS DPIRuleTransport object array.

logInspectionRuleDelete()

DESCRIPTION Deletes Log Inspection Rules by ID.

SYNTAX

```
void logInspectionRuleDelete(int[] ids, String sID)
```

PARAMETERS

ids	Log Inspection Rule IDs to delete.
sID	Authentication session identifier ID.

logInspectionRuleSave()

DESCRIPTION Saves a new or existing Log Inspection Rule.

SYNTAX

```
LogInspectionRuleTransport logInspectionRuleSave(LogInspectionRuleTransport irt, String sID)
```

PARAMETERS

irt	LogInspectionRuleTransport object to create.
sID	Authentication session identifier ID.

RETURNS Newly created LogInspectionRuleTransport object.

logInspectionRuleRetrieve()

DESCRIPTION Retrieves a Log Inspection Rule by ID.

SYNTAX

```
LogInspectionRuleTransport logInspectionRuleRetrieve(int id, String sID)
```

PARAMETERS

id	Log Inspection Rule ID.
sID	Authentication session identifier ID.

RETURNS LogInspectionRuleTransport object.

logInspectionRuleRetrieveByName()

DESCRIPTION Retrieves a Log Inspection Rule by name.

SYNTAX

```
LogInspectionRuleTransport logInspectionRuleRetrieveByName(String name, String sID)
```

PARAMETERS

name	Log Inspection Rule name.
sID	Authentication session identifier ID.

RETURNS LogInspectionRuleTransport object.

logInspectionRuleRetrieveAll()

DESCRIPTION Retrieves all Log Inspection Rule.

SYNTAX

LogInspectionRuleTransport[] logInspectionRuleRetrieveAll(String sID)

PARAMETERS

sID	Authentication session identifier ID.

RETURNS LogInspectionRuleTransport object array.

logInspectionDecoderDelete()

DESCRIPTION Deletes Log Inspection Decoder by ID.

SYNTAX

void logInspectionDecoderDelete(int[] ids, String sID)

PARAMETERS

ids	Log Inspection Decoder IDs to delete.
sID	Authentication session identifier ID.

logInspectionDecoderSave()

DESCRIPTION Saves a new or existing Log Inspection Decoder.

SYNTAX

LogInspectionDecoderTransport logInspectionDecoderSave(LogInspectionDecoderTransport irt, String sID)

PARAMETERS

irt	LogInspectionDecoderTransport object to create.
sID	Authentication session identifier ID.

RETURNS Newly created LogInspectionDecoderTransport object.

logInspectionDecoderRetrieve()

DESCRIPTION Retrieves a Log Inspection Decoder by ID.

SYNTAX

```
LogInspectionDecoderTransport logInspectionDecoderRetrieve(int ID, String sID)
```

PARAMETERS

ID	Log Inspection Decoder ID.
sID	Authentication session identifier ID.

RETURNS LogInspectionDecoderTransport object.

logInspectionDecoderRetrieveByName()

DESCRIPTION Retrieves a Log Inspection Decoder by name.

SYNTAX

```
LogInspectionDecoderTransport logInspectionDecoderRetrieveByName(String Name, String sID)
```

PARAMETERS

Name	Log Inspection Decoder name.
sID	Authentication session identifier ID.

RETURNS LogInspectionDecoderTransport object.

logInspectionDecoderRetrieveAll()

DESCRIPTION Retrieves all Log Inspection Decoder.

SYNTAX

```
LogInspectionDecoderTransport[] logInspectionDecoderRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS LogInspectionDecoderTransport object array.

integrityRuleDelete()

DESCRIPTION Deletes Integrity Rules by ID.

SYNTAX

```
void integrityRuleDelete(int[] ids, String sID)
```

PARAMETERS

ids	Integrity Rule IDs to delete.
sID	Authentication session identifier ID.

integrityRuleSave()

DESCRIPTION Saves a new or existing Integrity Rule.

SYNTAX

```
IntegrityRuleTransport integrityRuleSave(IntegrityRuleTransport irt, String sID)
```

PARAMETERS

irt	IntegrityRuleTransport object to create.
sID	Authentication session identifier ID.

RETURNS Newly created IntegrityRuleTransport object.

integrityRuleRetrieve()

DESCRIPTION Retrieves an Integrity Rule by ID.

SYNTAX

```
IntegrityRuleTransport integrityRuleRetrieve(int ID, String sID)
```

PARAMETERS

ID	Integrity Rule ID.
sID	Authentication session identifier ID.

RETURNS IntegrityRuleTransport object.

integrityRuleRetrieveByName()

DESCRIPTION Retrieves an Integrity Rule by name.

SYNTAX

```
IntegrityRuleTransport integrityRuleRetrieveByName(String name, String sID)
```

PARAMETERS

name	Integrity Rule name.
sID	Authentication session identifier ID.

RETURNS IntegrityRuleTransport object.

integrityRuleRetrieveAll()

DESCRIPTION Retrieves all Integrity Rules.

SYNTAX

```
IntegrityRuleTransport[] integrityRuleRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS IntegrityRuleTransport object array.

scheduleDelete()

DESCRIPTION Deletes Schedule by ID.

SYNTAX

```
void scheduleDelete (int[] IDs, String sID)
```

PARAMETERS

ids	Schedule IDs to delete.
sID	Authentication session identifier ID.

scheduleSave()

DESCRIPTION Saves a new or existing Schedule.

SYNTAX

```
ScheduleTransport scheduleSave(ScheduleTransport s, String sID)
```

PARAMETERS

s	ScheduleTransport object to create.
sID	Authentication session identifier ID.

RETURNS Newly created ScheduleTransport object.

scheduleRetrieve()

DESCRIPTION Retrieves a Schedule by ID.

SYNTAX

```
ScheduleTransport scheduleRetrieve(int id, String sID)
```

PARAMETERS

id	Schedule ID.
sID	Authentication session identifier ID.

RETURNS ScheduleTransport object.

scheduleRetrieveByName()

DESCRIPTION Retrieves a Schedule by name.

SYNTAX

```
ScheduleTransport scheduleRetrieveByName(String name, String sID)
```

PARAMETERS

name	Schedule name.
sID	Authentication session identifier ID.

RETURNS ScheduleTransport object.

scheduleRetrieveAll()

DESCRIPTION Retrieves all Schedules.

SYNTAX

```
ScheduleTransport[] scheduleRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS ScheduleTransport object array.

statefulConfigurationDelete()

DESCRIPTION Deletes Stateful Configuration by ID.

SYNTAX

```
void statefulConfigurationDelete(int[] ids, String sID)
```

PARAMETERS

ids	Stateful Configuration IDs to delete.
sID	Authentication session identifier ID.

statefulConfigurationSave()

DESCRIPTION Saves a new or existing Stateful Configuration.

SYNTAX

```
StatefulConfigurationTransport statefulConfigurationSave(StatefulConfigurationTransport s, String sID)
```

PARAMETERS

s	StatefulConfigurationTransport object to create.
sID	Authentication session identifier ID.

RETURNS Newly created StatefulConfigurationTransport object.

statefulConfigurationRetrieve()

DESCRIPTION Retrieves a Stateful Configuration by ID.

SYNTAX

```
StatefulConfigurationTransport statefulConfigurationRetrieve(int id, String sID)
```

PARAMETERS

id	Stateful Configuration ID.
sID	Authentication session identifier ID.

RETURNS StatefulConfigurationTransport object.

statefulConfigurationRetrieveByName()

DESCRIPTION Retrieves a Stateful Configuration by name.

SYNTAX

```
StatefulConfigurationTransport statefulConfigurationRetrieveByName(String Name, String sID)
```

PARAMETERS

name	Stateful Configuration name.
sID	Authentication session identifier ID.

RETURNS StatefulConfigurationTransport object.

statefulConfigurationRetrieveAll()

DESCRIPTION Retrieves all Stateful Configuration.

SYNTAX

```
StatefulConfigurationTransport[] statefulConfigurationRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS StatefulConfigurationTransport object array.

securityProfileDelete()

DESCRIPTION Deletes Security Profile by ID.

SYNTAX

```
void securityProfileDelete(int[] IDs, String sID)
```

PARAMETERS

ids Security Profile IDs to delete.

sID Authentication session identifier ID.

RETURNS

securityProfileSave()

DESCRIPTION Saves a new or existing Security Profile.

SYNTAX

```
SecurityProfileTransport securityProfileSave(SecurityProfileTransport sp, String sID)
```

PARAMETERS

sp SecurityProfileTransport object to create.

sID Authentication session identifier ID.

RETURNS Newly created SecurityProfileTransport object.

securityProfileAssignToHost()

DESCRIPTION Assigns a Security Profile to a Host.

SYNTAX

```
void securityProfileAssignToHost(int securityProfileID, int[] hostIDs, String sID)
```

PARAMETERS

securityProfileID Security Profile ID to assign.

hostIDs Host IDs to assign to Security Profile.

sID Authentication session identifier ID.

RETURNS

hostSecurityProfileClear()

DESCRIPTION Un-assigns a Host from a Security Profile.

SYNTAX

```
void hostSecurityProfileClear(int[] hostIDs, String sID)
```

PARAMETERS

hostIDs	Host IDs to assign to Security Profile.
sID	Authentication session identifier ID.

hostMoveToHostGroup()

DESCRIPTION Assigns a Host Group to a Host.

SYNTAX

```
void hostMoveToHostGroup(int[] hostIDs, int hostGroupID, String sID)
```

PARAMETERS

hostIDs	Host IDs to assign to Host Group.
hostGroupID	Host Group ID.
sID	Authentication session identifier ID.

RETURNS

hostCreate()

DESCRIPTION Creates a new Host object.

SYNTAX

```
HostTransport hostCreate(HostTransport host, String sID)
```

PARAMETERS

host	HostTransport object to create.
sID	Authentication session identifier ID.

RETURNS Newly created HostTransport object.

hostDelete()

DESCRIPTION	Deletes Hosts from the Manager.

SYNTAX

```
void hostDelete(int[] IDs, String sID)
```

PARAMETERS

ids	Host IDs to delete.
sID	Authentication session identifier ID.

hostRetrieve()

DESCRIPTION	Retrieves a Host by ID.

SYNTAX

```
HostTransport hostRetrieve(int ID, String sID)
```

PARAMETERS

ID	Host ID.
sID	Authentication session identifier ID.
RETURNS	HostTransport object.

hostRetrieveByName()

DESCRIPTION	Retrieves a Host by name.

SYNTAX

```
HostTransport hostRetrieveByName(String hostname, String sID)
```

PARAMETERS

hostname	Host name.
sID	Authentication session identifier ID.
RETURNS	HostTransport object.

hostRetrieveByHostGroup()

DESCRIPTION Retrieves Hosts by Host Group.

SYNTAX

```
HostTransport[] hostRetrieveByHostGroup(int hostGroupID, String sID)
```

PARAMETERS

hostGroupID	Host Group ID.
sID	Authentication session identifier ID.

RETURNS HostTransport object array.

hostGetStatus()

DESCRIPTION Retrieves a Host status.

SYNTAX

```
HostStatusTransport hostGetStatus(int id, String sID)
```

PARAMETERS

id	Host ID to retrieve.
sID	Authentication session identifier ID.

RETURNS HostStatusTransport object.

hostAgentActivate()

DESCRIPTION Activates the agents on the set of hosts identified by IDs.

SYNTAX

```
public void hostAgentActivate(int[] hostIDs , String sID)
```

PARAMETERS

hostIDs	Array of host IDs to activate.
sID	Authentication session identifier ID.

hostAgentDeactivate()

DESCRIPTION Deactivates the agents on the set of hosts identified by IDs.

SYNTAX

```
public void hostAgentDeactivate(int[] hostIDs, String sID)
```

PARAMETERS

hostIDs	Array of host IDs to deactivate.
sID	Authentication session identifier ID.

hostUpdateNow()

DESCRIPTION Immediately initiates the update of hosts identified by IDs.

SYNTAX

```
public void hostUpdateNow(int[] hostIDs, String sID)
```

PARAMETERS

hostIDs	Array of host IDs to update.
sID	Authentication session identifier ID.

hostIntegrityScan()

DESCRIPTION Immediately initiates an integrity scan update of hosts identified by IDs.

SYNTAX

```
public void hostIntegrityScan(int[] hostIDs, String sID)
```

PARAMETERS

hostIDs	Array of host IDs to update.
sID	Authentication session identifier ID.

hostRebuildBaseline()

DESCRIPTION Immediately initiates an integrity scan baseline rebuild of hosts identified by IDs.

SYNTAX

```
public void hostRebuildBaseline(int[] hostIDs, String sID)
```

PARAMETERS

hostIDs	Array of host IDs to update.
sID	Authentication session identifier ID.

hostGetEventsNow()

DESCRIPTION Immediately initiates the fetch of events from hosts identified by IDs. The completion of this method is not synchronized with the event retrieval.

SYNTAX

```
public void hostGetEventsNow(int[] IDs, String sID)
```

PARAMETERS

IDs	Array of host IDs to update.
sID	Authentication session identifier ID.

hostGetEventsNowSync()

DESCRIPTION Immediately initiates the fetch of events from hosts identified by IDs and will block until the events are successfully retrieved or the Manager fails to communicate with the computers requested. There is a maximum timeout of 60 seconds.

SYNTAX

```
void hostGetEventsNowSync(int hostID, String sID)
```

PARAMETERS

hostID	The host on which to perform the action.
sID	Authentication session identifier ID.

securityProfileRetrieve()

DESCRIPTION Retrieves a Security Profile by ID.

SYNTAX

```
public SecurityProfileTransport securityProfileRetrieve(int ID, String sID)
```

PARAMETERS

ID Identifying Security Profile ID.

sID Authentication session identifier ID.

RETURNS SecurityProfileTransport object.

securityProfileRetrieveByName()

DESCRIPTION Retrieves a Security Profile by name.

SYNTAX

```
public SecurityProfileTransport securityProfileRetrieveByName(String name, String sID)
```

PARAMETERS

name Identifying Security Profile name.

sID Authentication session identifier ID.

RETURNS SecurityProfileTransport object.

securityProfileRetrieveAll()

DESCRIPTION Retrieves all Security Profiles.

SYNTAX

```
public SecurityProfileTransport[] securityProfileRetrieveAll(String sID)
```

PARAMETERS

sID Authentication session identifier ID.

RETURNS SecurityProfileTransport object array.

systemSettingSet()

DESCRIPTION Sets the set of system setting key value pairs identified in the EditableSettingTransport array.

SYNTAX

```
public void systemSettingSet(EditableSettingTransport[] EditableSettings, String sID)
```

PARAMETERS

EditableSettings	Array of EditableSettingTransport to set.
sID	Authentication session identifier ID.

securityProfileSettingGet()

DESCRIPTION Retrieves the set of setting identified by the EnumEditableSettingKey array.

SYNTAX

```
EditableSettingStoredTransport[] securityProfileSettingGet(int securityProfileID, EnumEditableSettingKey[] keys,  String sID)
```

PARAMETERS

securityProfileID	Identifying Security Profile ID.
keys	Array of EnumEditableSettingKey to get.
sID	Authentication session identifier ID.

RETURNS EditableSettingStoredTransport object array.

securityProfileSettingSet()

DESCRIPTION Sets a set of Security Profile setting key value pairs identified in the EditableSettingTransport array.

SYNTAX

```
void securityProfileSettingSet(int securityProfileID, EditableSettingTransport[] editableSettings, String sID)
```

PARAMETERS

securityProfileID	Identifying Security Profile ID.
editableSettings	Array of EditableSettingTransport to set.
sID	Authentication session identifier ID.

securityProfileSettingClear()

DESCRIPTION Clears a set of Security Profile setting key value pairs identified in the EnumEditableSettingKey array.

SYNTAX

```
public void securityProfileSettingClear(int ID, EnumEditableSettingKey[] EditableSettings, String sID)
```

PARAMETERS

ID	Identifying Security Profile ID.
EditableSettings	Array of EditableSettingTransport to clear.
sID	Authentication session identifier ID.

hostSettingGet()

DESCRIPTION Retrieves the set of host settings identified by the EnumEditableSettingKey array.

SYNTAX

```
public EditableSettingStoredTransport[] hostSettingGet(int hostID, EnumEditableSettingKey[] keys, String sID)
```

PARAMETERS

hostID	Identifying host ID.
keys	Array of EnumEditableSettingKey to get.
sID	Authentication session identifier ID.

RETURNS EditableSettingStoredTransport object array.

hostSettingSet()

DESCRIPTION Sets a set of host setting key value pairs identified in the EditableSettingTransport array.

SYNTAX

```
public void hostSettingSet(int hostID, EditableSettingTransport[]editableSettings, String sID)
```

PARAMETERS

hostID	Identifying host ID.
editableSettings	Array of EditableSettingTransport to set.
sID	Authentication session identifier ID.

hostSettingClear()

DESCRIPTION

Clears host overrides for the setting key value pairs identified in the EnumEditableSettingKey array. The host Security Profile or System inherited setting will then apply.

SYNTAX

```
public void hostSettingClear(int hostID, EnumEditableSettingKey[] keys, String sID)
```

PARAMETERS

hostID	Identifying host ID.
keys	Array of EditableSettingTransport to clear.
sID	Authentication session identifier ID.

systemEventRetrieve()

DESCRIPTION

Retrieves the system events specified by the time, host and event ID filters. System events that do not pertain to hosts can be included or excluded.

SYNTAX

```
public SystemEventListTransport systemEventRetrieve(TimeFilterTransport timeFilter, HostFilterTransport
hostFilter, IDFilterTransport eventIdFilter, boolean includeNonHostEvents, String sID)
```

PARAMETERS

timeFilter	TimeFilterTransport to filter by.
hostFilter	HostFilterTransport to filter by.
eventIdFilter	IDFilterTransport to filter by.
includeNonHostEvents	Boolean to specify if non-host events should be retrieved as well.
sID	Authentication session identifier ID.

RETURNS

SystemEventListTransport object array.

DPIEventRetrieve()

DESCRIPTION Retrieves the DPI events specified by the time, host and event ID filters.

SYNTAX

```
public DPIEventListTransport DPIEventRetrieve(TimeFilterTransport timeFilter, HostFilterTransport hostFilter, IDFilterTransport eventIdFilter, String sID)
```

PARAMETERS

timeFilter	TimeFilterTransport to filter by.
hostFilter	HostFilterTransport to filter by.
eventIdFilter	IDFilterTransport to filter by.
sID	Authentication session identifier ID.

RETURNS DPIEventListTransport object array.

integrityEventRetrieve()

DESCRIPTION Retrieves the integrity events specified by the time, host and event ID filters.

SYNTAX

```
public IntegrityEventListTransport integrityEventRetrieve(TimeFilterTransport timeFilter, HostFilterTransport hostFilter, IDFilterTransport eventIdFilter, String sID)
```

PARAMETERS

timeFilter	TimeFilterTransport to filter by.
hostFilter	HostFilterTransport to filter by.
eventIdFilter	IDFilterTransport to filter by.
sID	Authentication session identifier ID.

RETURNS DPIEventListTransport object array.

logInspectionEventRetrieve()

DESCRIPTION Retrieves the Log Inspection events specified by the time, host and event ID filters.

SYNTAX

```
public LogInspectionEventListTransport logInspectionEventRetrieve(TimeFilterTransport timeFilter,
HostFilterTransport hostFilter, IDFilterTransport eventIdFilter, String sID)
```

PARAMETERS

timeFilter	TimeFilterTransport to filter by.
hostFilter	HostFilterTransport to filter by.
eventIdFilter	IDFilterTransport to filter by.
sID	Authentication session identifier ID.

RETURNS LogInspectionEventListTransport object array.

firewallEventRetrieve()

DESCRIPTION Retrieves the firewall events specified by the time, host and event ID filters.

SYNTAX

```
public FirewallEventListTransport firewallEventRetrieve(TimeFilterTransport timeFilter, HostFilterTransport
hostFilter, IDFilterTransport eventIdFilter, String sID)
```

PARAMETERS

timeFilter	TimeFilterTransport to filter by.
hostFilter	HostFilterTransport to filter by.
eventIdFilter	IDFilterTransport to filter by.
sID	Authentication session identifier ID.

RETURNS FirewallEventListTransport object array.

userDelete ()

DESCRIPTION Deletes the set of users defined identified by the provided ids. The user must have rights to delete user.

SYNTAX

public void userDelete(int[] ids, String sID)

PARAMETERS

ids	The list of user ids to delete.
sID	Authentication session identifier ID.

userSave ()

DESCRIPTION Saves the supplied user.

SYNTAX

UserTransport userSave(UserTransport ipl, String sID)

PARAMETERS

ipl	The UserTransport to save
sID	Authentication session identifier ID.

RETURNS UserTransport object.

userRetrieve ()

DESCRIPTION Retrieves the user with the provided ID (password is always blank)

SYNTAX

UserTransport userRetrieve(int id, String sID)

PARAMETERS

id	The id of the user to retrieve
sID	Authentication session identifier ID.

RETURNS UserTransport containing the user with the provided ID

userRetrieveAll ()

DESCRIPTION Retrieves all users (password is always blank).

SYNTAX

```
UserTransport[] userRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS UserTransport object array.

roleGetDefaultID ()

DESCRIPTION Get the full access (read-only) role. This can be used for creating users, especially for 'service users' (user accounts used for API integration).

SYNTAX

```
int roleGetDefaultID(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS the role ID.

pluginRequest ()

DESCRIPTION Dispatches a generic message to a plugin. Can be used to 'push' data or events to a plug-in via the WSAPI.

SYNTAX

```
String pluginRequest(String pluginID, String input, String sID)
```

PARAMETERS

pluginID	Plug-in identifier.
input	Input (can be string, XML, Base64, etc).
sID	Authentication session identifier ID.

RETURNS Output (can be string, XML, Base64, etc), blank if PLM shutdown.

counterRetrieve ()

DESCRIPTION

Load a list of counters per host, based on the counter filter type.
This method access the underlying counters that power the dashboard and reports efficiently. The text field of the CounterTransport object is varied by different counters. The description is blank.
Value is the count for the event type (including duplicate rolled events).

SYNTAX

```
CounterTransport[] counterRetrieve(EnumCounterFilter counterFilter, TimeFilterTransport timeFilter,
HostFilterTransport hostFilter, TagFilterTransport tagFilter, String sID)
```

PARAMETERS

counterFilter — Type of counter filter to access. Please refer to EnumCounterFilter for officially supported values.

timeFilter — The time range to pull.

hostFilter — The host filter to constrain the query to. Not all hosts will be listed if they have a value of 0.

tagFilter — The tag filter or all tags. All returns an unbounded set, untagged returns only the untagged events, otherwise the freeform field takes comma delimited tag names (with the not '!' character indicating where not tagged).

sID — Authentication session identifier ID.

RETURNS

CounterTransport object array.

counterHostRetrieve ()

DESCRIPTION

Load a list of counters per host, based on the counter filter type.

SYNTAX

```
public CounterHostTransport[] counterHostRetrieve(EnumCounterFilter counterFilter, TimeFilterTransport
timeFilter, HostFilterTransport hostFilter, TagFilterTransport tagFilter, String sID)
```

PARAMETERS

counterFilter — Type of counter filter to access.

timeFilter — Type of counter filter to access.

hostFilter — The host filter to constrain the query to.

tagFilter — The tag filter or all tags.

sID Authentication session identifier ID.

RETURNS CounterHostTransport object array for the hosts that have a value > 0.

counterWithIDRetrieve ()

DESCRIPTION Load a list of counters per host, based on the counter filter type.

SYNTAX

```
public CounterWithIDTransport[] counterWithIDRetrieve(EnumCounterFilter counterFilter,
TimeFilterTransport timeFilter, HostFilterTransport hostFilter, TagFilterTransport tagFilter, String sID)
```

PARAMETERS

counterFilter Type of counter filter to access. Please refer to EnumCounterFilter for officially supported values

timeFilter The time range to pull.

hostFilter The host filter to constrain the query to. Not all hosts will be listed if they have a value of 0.

tagFilter The tag filter or all tags.

sID Authentication session identifier ID.

RETURNS CounterWithIDTransport object array.

counterAlertTypeRetrieve ()

DESCRIPTION Retrieves the firewall events specified by the time, host and event ID filters.

SYNTAX

```
public CounterAlertTypeTransport[] counterAlertTypeRetrieve(EnumCounterFilter counterFilter,
TimeFilterTransport timeFilter, HostFilterTransport hostFilter, TagFilterTransport tagFilter, String sID)
```

PARAMETERS

counterFilter Type of counter filter to access. Please refer to EnumCounterFilter for officially supported values

timeFilter The time range to pull.

hostFilter The host filter to constrain the query to. Not all hosts will be listed if they have a value of 0.

tagFilter IDFilterTransport to filter by.

sID Authentication session identifier ID.

RETURNS CounterAlertTypeTransport object array.

counterSumRetrieve ()

DESCRIPTION Load a list of counters per host, based on the counter filter type.

SYNTAX

public CounterAlertTypeTransport[] counterAlertTypeRetrieve(EnumCounterFilter counterFilter, TimeFilterTransport timeFilter, HostFilterTransport hostFilter, TagFilterTransport tagFilter, String sID)

PARAMETERS

counterFilter Type of counter filter to access.

timeFilter The time range to pull.

hostFilter The host filter to constrain the query to.

tagFilter The tag filter or all tags.

sID Authentication session identifier ID.

RETURNS CounterAlertTypeTransport object array.

featureSummaryRetrieve ()

DESCRIPTION Get status summary of each protection feature.

SYNTAX

public FeatureSummaryTransport featureSummaryRetrieve(TimeFilterTransport timeFilter, TimeFilterTransport previousTimeFilter, String sID)

PARAMETERS

timeFilter the lookup time range

previousTimeFilter the comparison baseline time range.

sID Authentication session identifier ID.

RETURNS FeatureSummary including summaries of each protection feature.

statusSummaryRetrieve ()

DESCRIPTION Return the status summary of the system.

SYNTAX

```
public StatusSummaryTransport statusSummaryRetrieve(String sID)
```

PARAMETERS

sID Authentication session identifier ID.

RETURNS Status summary including host status summary and alert numbers

componentSummaryRetrieve ()

DESCRIPTION Return component info for each component

SYNTAX

```
public ComponentInfoTransport[] componentSummaryRetrieve(String sID)
```

PARAMETERS

sID Authentication session identifier ID.

RETURNS ComponentInfoTransport object array.

hostStatusSummaryRetrieve ()

DESCRIPTION Retrieves the summary of the hosts status (error, warning, online, locked, unmanaged) as integers for the given hostFilter.

SYNTAX

```
public HostStatusSummaryTransport hostStatusSummaryRetrieve(HostFilterTransport hostFilter, String sID)
```

PARAMETERS

hostFilter HostFilterTransport to filter by.

sID Authentication session identifier ID.

RETURNS HostStatusSummaryTransport object.

hostJobProgress ()

DESCRIPTION	Gets the progress of a given job type since the invocation time.

SYNTAX

```
public JobProgressTransport hostJobProgress(EnumJobType type, java.util.Calendar sinceManagerTime, int[] hostIDs, String sID)
```

PARAMETERS

type	Type of operation (UPDATE, etc)
sinceManagerTime	use getManagerTime before invoking the operation
hostIDs	list of hostIDs to check
sID	Authentication session identifier ID.
RETURNS	JobProgressTransport object.

hostClearWarningsErrors ()

DESCRIPTION	Clear warnings and errors

SYNTAX

```
public void hostClearWarningsErrors(int[] hostIDs, String sID)
```

PARAMETERS

hostIDs	The ids of the hosts to clear the warnings and errors
sID	Authentication session identifier ID.

systemSettingGet ()

DESCRIPTION Retrieves the set of setting identified by the EnumEditableSettingKey[].

SYNTAX

```
public EditableSettingStoredTransport[] systemSettingGet(EnumEditableSettingKey[] keys, String sID)
```

PARAMETERS

keys	The keys of the settings to return
sID	Authentication session identifier ID.

RETURNS EditableSettingStoredTransport object array.

securityProfileSettingClear ()

DESCRIPTION Removes the provided Security Profile's overrides for the settings in keys, returning the values to those inherited from system.

SYNTAX

```
public void securityProfileSettingClear(int securityProfileID,  EnumEditableSettingKey[] keys, String sID)
```

PARAMETERS

securityProfileID	The ID of the security profile that the settings are for.
keys	Transport object containing the required information to store a setting.
sID	Authentication session identifier ID.

hostGetEventsNowSync ()

DESCRIPTION Immediately initiates the fetch of events from the host.

SYNTAX

```
public void hostGetEventsNowSync(int hostID, String sID)
```

PARAMETERS

hostID	The host on which to perform the action
sID	Authentication session identifier ID.

retrieveActivationCode ()

DESCRIPTION Retrieves the current activation code for the specified module

SYNTAX

```
public String retrieveActivationCode(int moduleNumber, String sID)
```

PARAMETERS

moduleNumber The module number on which to perform the action.

sID Authentication session identifier ID.

RETURNS The current activation code for the specified module.

retrieveLicenseProfile ()

DESCRIPTION Retrieves the current license profile code for the specified module

SYNTAX

```
public String retrieveLicenseProfile(int moduleNumber, String sID)
```

PARAMETERS

moduleNumber The module number on which to perform the action.

sID Authentication session identifier ID.

RETURNS The current license profile for the specified module in a String.

addActivationCode ()

DESCRIPTION Adds the activation code for the specified module

SYNTAX

```
public void addActivationCode(int moduleNumber, String activationCode, String sID)
```

PARAMETERS

moduleNumber The module number on which to perform the action. -1 for all modules, 0 for AV, 1 for NET, 2 for IM, 3 for LI

activationCode The activation code to add.

sID Authentication session identifier ID.

logInspectionRuleRetrieveAll ()

DESCRIPTION Retrieves all of the LogInspectionRules

SYNTAX

```
public LogInspectionRuleTransport[] logInspectionRuleRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS LogInspectionRuleTransport object array.

logInspectionDecoderRetrieveByName()

DESCRIPTION Retrieves the logInspectionDecoder with the provided name (Case Sensitive)

SYNTAX

```
public LogInspectionDecoderTransport logInspectionDecoderRetrieveByName(String name, String sID)
```

PARAMETERS

name	The name of the logInspectionDecoder to retrieve
sID	Authentication session identifier ID.

RETURNS LogInspectionDecoderTransport object.

scanFileListDelete()

DESCRIPTION Deletes the set of Scan File lists identified by the provided ids.

SYNTAX

```
public void scanFileListDelete(int[] ids, String sID)
```

PARAMETERS

ids	The list of Scan File list ids to delete.
sID	Authentication session identifier ID.

scanFileListSave()

DESCRIPTION Saves the supplied Scan File list.

SYNTAX

public ScanFileListTransport scanFileListSave(ScanFileListTransport scanFileListTransport, String sID)

PARAMETERS

scanFileListTransport	The ScanFileListTransport to save
sID	Authentication session identifier ID.

RETURNS ScanFileListTransport object.

scanFileListRetrieve()

DESCRIPTION Retrieves the Scan File list with the provided ID

SYNTAX

public ScanFileListTransport scanFileListRetrieve(int id, String sID)

PARAMETERS

id	The id of the Scan File list to retrieve
sID	Authentication session identifier ID.

RETURNS ScanFileListTransport object with the IP list with the provided ID

scanFileListRetrieveByName()

DESCRIPTION Retrieves the Scan File list with the provided name (Case sensitive)

SYNTAX

public ScanFileListTransport scanFileListRetrieveByName(String name, String sID)

PARAMETERS

name	The name id of the Scan File list to retrieve
sID	Authentication session identifier ID.

RETURNS ScanFileListTransport object with the IP list with the provided name.

scanFileListRetrieveAll ()

DESCRIPTION Retrieves all of the Scan File lists

SYNTAX

public ScanFileListTransport[] scanFileListRetrieveAll(String sID)

PARAMETERS

sID	Authentication session identifier ID.

RETURNS ScanFileListTransport object array.

scanFileExtListDelete()

DESCRIPTION Deletes the set of Scan File Extension lists identified by the provided ids

SYNTAX

public void scanFileExtListDelete(int[] ids, String sID)

PARAMETERS

ids	public void scanFileExtListDelete(int[] ids, String sID)
sID	Authentication session identifier ID.

scanFileExtListSave ()

DESCRIPTION Deletes the set of Scan File Extension lists identified by the provided ids.

SYNTAX

public void scanFileExtListDelete(int[] ids, String sID)

PARAMETERS

ids	The list of Scan File Extension list ids to delete
sID	Authentication session identifier ID.

scanFileExtListRetrieve ()

DESCRIPTION Retrieves the Scan File Extension list with the provided ID

SYNTAX

```
public ScanFileExtListTransport scanFileExtListRetrieve(int id, String sID)
```

PARAMETERS

id	The id of the Scan File Extension list to retrieve.
sID	Authentication session identifier ID.

RETURNS ScanFileExtListTransport object with the IP list with the provided ID.

scanFileExtListRetrieveByName ()

DESCRIPTION Retrieves the Scan File Extension list with the provided name (Case sensitive)

SYNTAX

```
public ScanFileExtListTransport scanFileExtListRetrieveByName(String name, String sID)
```

PARAMETERS

name	The name of the Scan File Extension list to retrieve.
sID	Authentication session identifier ID.

RETURNS ScanFileExtListTransport object with the IP list with the provided ID

scanFileExtListRetrieveAll()

DESCRIPTION Retrieves all of the Scan File Extension lists

SYNTAX

```
public ScanFileExtListTransport[] scanFileExtListRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS ScanFileExtListTransport object array.

scanDirectoryListDelete ()

DESCRIPTION Retrieves all of the Scan File Extension lists

SYNTAX

```
public void scanDirectoryListDelete(int[] ids, String sID)
```

PARAMETERS

ids The list of Scan Directory list ids to delete

sID Authentication session identifier ID.

scanDirectoryListSave()

DESCRIPTION Saves the supplied Scan File Extension list

SYNTAX

```
public ScanDirectoryListTransport scanDirectoryListSave(ScanDirectoryListTransport
scanDirectoryListTransport, String sID)
```

PARAMETERS

scanDirectoryListTransport The ScanFileExtListTransport to save

sID Authentication session identifier ID.

RETURNS ScanDirectoryListTransport object.

scanDirectoryListRetrieve()

DESCRIPTION Retrieves the Scan Directory list with the provided ID

SYNTAX

```
public ScanDirectoryListTransport scanDirectoryListRetrieve(int id, String sID)
```

PARAMETERS

id The id of the Scan Directory list to retrieve

sID Authentication session identifier ID.

RETURNS ScanDirectoryListTransport object with the IP list with the provided ID.

scanDirectoryListRetrieveByName()

DESCRIPTION Retrieves the Scan Directory list with the provided name (Case sensitive)

SYNTAX

```
public ScanDirectoryListTransport scanDirectoryListRetrieveByName(String name, String sID)
```

PARAMETERS

name	The name of the Scan Directory list to retrieve
sID	Authentication session identifier ID.

RETURNS ScanDirectoryListTransport object.

scanDirectoryListRetrieveAll()

DESCRIPTION Retrieves all of the Scan Directory lists.

SYNTAX

```
public ScanDirectoryListTransport[] scanDirectoryListRetrieveAll(String sID)
```

PARAMETERS

sID	Authentication session identifier ID.

RETURNS ScanDirectoryListTransport object array.

antiMalwareDelete()

DESCRIPTION Deletes the set of AntiMalware identified by the provided ids

SYNTAX

```
public void antiMalwareDelete(int[] ids, String sID)
```

PARAMETERS

ids	The list of AntiMalware ids to delete
sID	Authentication session identifier ID.

antiMalwareSave()

DESCRIPTION Saves the supplied AntiMalware

SYNTAX

public AntiMalwareTransport antiMalwareSave(AntiMalwareTransport antiMalwareTransport, String sID)

PARAMETERS

antiMalwareTransport	The AntiMalwareTransport to save
sID	Authentication session identifier ID.

RETURNS AntiMalwareTransport object.

antiMalwareRetrieve()

DESCRIPTION Retrieves the AntiMalware with the provided ID

SYNTAX

public AntiMalwareTransport antiMalwareRetrieve(int id, String sID)

PARAMETERS

id	The id of the AntiMalware to retrieve
sID	Authentication session identifier ID.

RETURNS The AntiMalwareTransport object.

antiMalwareRetrieveByName()

DESCRIPTION Retrieves the AntiMalware with the provided name (Case sensitive)

SYNTAX

public AntiMalwareTransport antiMalwareRetrieveByName(String name, String sID)

PARAMETERS

name	The name of the AntiMalware to retrieve
sID	Authentication session identifier ID.

RETURNS AntiMalwareTransport object.

antiMalwareRetrieveAll()

DESCRIPTION Retrieves all of the AntiMalware

SYNTAX

```
public AntiMalwareTransport[] antiMalwareRetrieveAll(String sID)
```

PARAMETERS

sID Authentication session identifier ID.

RETURNS AntiMalwareTransport object array.

antiMalwareEventRetrieve()

DESCRIPTION Retrieves the AntiMalware events specified by the time and host filter.

SYNTAX

```
public AntiMalwareEventListTransport antiMalwareEventRetrieve(TimeFilterTransport timeFilter
HostFilterTransport hostFilter, IDFilterTransport eventIdFilter, String sID)
```

PARAMETERS

timeFilter Restricts the retrieved events by time.

hostFilter Restricts the retrieved events by host, group, or security profile.

eventIdFilter Restricts the retrieved events by event id.

sID Authentication session identifier ID.

RETURNS AntiMalwareEventListTransport object.

updateComponents()

DESCRIPTION Performs a global component update of the system. This will do a full update of all relays, and then the corresponding agent updates

SYNTAX

```
public boolean updateComponents(String sID)
```

PARAMETERS

sID Authentication session identifier ID.

RETURNS AntiMalwareEventListTransport object.

updateComponentFromAU()

DESCRIPTION Performs a global component update of the system. This will do a full update of all relays, and then the corresponding agent updates, and also for legacy purposes, if 7.5 Appliances are in use, we will utilize some of the parameters and attempt to perform specific updates for those legacy Appliances.

SYNTAX

```
public boolean updateComponentFromAU(int type, int id, boolean applyDSRU, String sID)
```

PARAMETERS

type	If in legacy mode, specifies the specific type of component to update
Id	If in legacy mode, specifies the ID of the component to update
applyDSRU	If in legacy mode, indicates if the DSRU should be applied or not
sID	Authentication session identifier ID.

RETURNS True if the update was successful.

hostAntiMalwareScan()

DESCRIPTION Trigger Anti-Malware Manual Scan on specified host.

SYNTAX

```
public void hostAntiMalwareScan(int[] hostIDs, String sID)
```

PARAMETERS

hostIDs	Array of host IDs to apply software to.
sID	Authentication session identifier ID.

hostUpdateComponent()

DESCRIPTION Update Component

SYNTAX

```
public void hostUpdateComponent(int[] hostIDs, int type, int id, String sID)
```

PARAMETERS

hostIDs	Host IDs to update.

type	Component type (ignored)
id	Component id (ignored)
sID	Authentication session identifier ID.

hostRollbackComponent()

DESCRIPTION Rollback Component on DSVA to the previous version

SYNTAX

public void hostRollbackComponent(int[] hostIDs, int type, int id, String sID)

PARAMETERS

hostIDs	All the DSVAs to update.
type	Component type (ignored)
id	Component id (ignored)
sID	Authentication session identifier ID.

alertStatusRetrieve()

DESCRIPTION Retrieves the alerts.

SYNTAX

public AlertStatusTransport[] alertStatusRetrieve(int count, String sID)

PARAMETERS

count	Restricts the retrieved alerts amount
sID	Authentication session identifier ID.

RETURNS The alert list

userRetrieveByName()

DESCRIPTION Retrieves the user with the provided username (Case Sensitive) (password is always blank)

SYNTAX

public UserTransport userRetrieveByName(String name, String sID)

PARAMETERS

name	The username of the user to retrieve
sID	Authentication session identifier ID.
RETURNS	The user with the provided username

counterRetrieve()

DESCRIPTION Load a list of counters per host, based on the counter filter type.

SYNTAX

```
public CounterTransport[] counterRetrieve(EnumCounterFilter counterFilter, TimeFilterTransport timeFilter,
HostFilterTransport hostFilter, TagFilterTransport tagFilter, String sID)
```

PARAMETERS

counterFilter	Type of counter filter to access. Please refer to EnumCounterFilter for officially supported values.
timeFilter	The time range to pull.
hostFilter	The host filter to constrain the query to. Not all hosts will be listed if they have a value of 0.
tagFilter	The tag filter or all tags. All returns an unbounded
sID	Authentication session identifier ID.
RETURNS	CounterTransport object array.

hostDetailRetrieve()

DESCRIPTION Retrieves the detail information of hosts.

SYNTAX

```
public HostDetailTransport[] hostDetailRetrieve(HostFilterTransport hostFilter, EnumHostDetailLevel
hostDetailLevel, String sID)
```

PARAMETERS

hostFilter	Restricts the retrieved hosts by host, group, or security profile
hostDetailLevel	The detail level
sID	Authentication session identifier ID.

RETURNS HostDetailTransport object array.

hostDetailRetrieveByName()

DESCRIPTION Retrieves the detail information of host.

SYNTAX

```
public HostDetailTransport[] hostDetailRetrieveByName(String hostname, EnumHostDetailLevel
hostDetailLevel, String sID)
```

PARAMETERS

hostname	The name of host
hostDetailLevel	The detail level
sID	Authentication session identifier ID.

RETURNS HostDetailTransport object array.

hostDetailRetrieveByExternal()

DESCRIPTION Retrieves the detail information of hosts by External ID (Host/HostGroup).

SYNTAX

```
public HostDetailTransport[] hostDetailRetrieveByExternal(ExternalFilterTransport externalFilter,
EnumHostDetailLevel hostDetailLevel, String sID)
```

PARAMETERS

externalFilter	Restricts the retrieved hosts by hostExternalID, or hostGroupExternalID
hostDetailLevel	The detail level

sID Authentication session identifier ID.

RETURNS HostDetailTransport object array.

hostDetailRetrieveByNameStartsWith()

DESCRIPTION Retrieves the detail information of host by starting with startsWithHostname.

SYNTAX

public HostDetailTransport[] hostDetailRetrieveByNameStartsWith(String startsWithHostname, EnumHostDetailLevel hostDetailLevel, String sID)

PARAMETERS

startsWithHostname The name of host

hostDetailLevel The detail level

sID Authentication session identifier ID.

RETURNS HostDetailTransport object array.

webReputationEventRetrieve()

DESCRIPTION Retrieves the Web Reputation events specified by the time and host filter.

SYNTAX

public WebReputationEventListTransport webReputationEventRetrieve(TimeFilterTransport timeFilter, HostFilterTransport hostFilter, IDFilterTransport eventIdFilter, String sID)

PARAMETERS

timeFilter Restricts the retrieved events by time

hostFilter	Restricts the retrieved events by host, group, or security profile
eventIdFilter	Restricts the retrieved events by event ID.
sID	Authentication session identifier ID.
RETURNS	WebReputationEventListTransport object.

hostRecommendationScan()

DESCRIPTION Initiate a host recommendation scan.

SYNTAX

```
void hostRecommendationScan(int[] hostIDs, String sID)
```

PARAMETERS

hostIDs	Array of host IDs to scan
sID	Authentication session identifier ID.

hostRecommendationsClear()

DESCRIPTION Clear the existing host recommendation.

SYNTAX

```
public void hostRecommendationsClear(int[] hostIDs, String sID)
```

PARAMETERS

hostIDs	Array of host IDs to clear
sID	Authentication session identifier ID.

hostRecommendationsResolve()

DESCRIPTION Manually resolve recommendations on unresolved hosts by type and rules.

SYNTAX

```
void hostRecommendationsResolve(int hostID, int type, int[] ruleIDs, String sID)
```

PARAMETERS

hostID	The host on which to perform the resolution

type	The type of rule
ruleIDs	An array of rule IDs
sID	Authentication session identifier ID.

hostRecommendationRuleIDsRetrieve()

DESCRIPTION Retrieve host recommendation rule IDs.

SYNTAX

```
public int[] hostRecommendationRuleIDsRetrieve(int hostID, int type, boolean onlyunassigned, String sID)
```

PARAMETERS

hostID	The host for which to retrieve the recommendations
type	The type of rule
onlyunassigned	Boolean to specify if the function should only return rules that are recommended, and not assigned at the host.
sID	Authentication session identifier ID.

RETURNS An array of recommended rule IDs.

securityProfileRecommendationRuleIDsRetrieve()

DESCRIPTION Retrieve security profile recommendation rule IDs.

SYNTAX

```
public int[] securityProfileRecommendationRuleIDsRetrieve(int securityProfileID, int type, String sID)
```

PARAMETERS

securityProfileID	The security profile ID for which to retrieve the recommendations
type	The type of rule
sID	Authentication session identifier ID.

RETURNS An array of recommended rule IDs.

hostRecommendationUnresolvedRetrieve()

DESCRIPTION Retrieve hosts with unresolved recommendation rule IDs.

SYNTAX

```
public int[] hostRecommendationUnresolvedRetrieve(String sID)
```

PARAMETERS

sID Authentication session identifier ID.

RETURNS An array of hosts IDs that have unresolved recommendations.

TREND MICRO

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA
Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APEM96340/140306