alarmAcknowledgeTriggeredAlarm

Mark a triggered alarm as acknowledged

alarmDeleteTriggeredAlarm

Delete a triggered alarm

alarmGetTriggeredAlarms

Retrieves a paged list of alarms that have been triggered

alarmUnacknowledgeTriggeredAlarm

Mark a triggered alarm as unacknowledged

assetGetAssetDetailsObject

Gets asset Details

assetGetAssetThreats

Gets asset threats

caseAddCase

Add a case to the system.

caseAddCaseStatus

Add a case status

caseAddOrganization

Add a case organization

caseDeleteCaseStatus

Delete a case status.

caseEditCase

Edit an existing case.

caseEditCaseStatus

Edit a case status

caseEditOrganization

Edit a case organization

caseGetCaseDetail

Get detail on an existing case.

caseGetCaseEventsDetail

Get case events details

caseGetCaseList

Get a list of cases from the system

caseGetCaseStatusList

Get a list of valid case statuses from the system

caseGetCaseUsers

Get case users

caseGetOrganizationList

Get case organizations

devGetDeviceList

Get a list of all devices defined in the system.

dsAddDataSourceClients

Add client datasources to another datasource

dsAddDataSourceClientsStatus

Get status of adding clients

dsAddDataSources

Add a list of data sources.

dsAddDataSourcesStatus

Get the status of adding datasources

dsDeleteDataSourceClients

Delete client datasource

dsDeleteDataSources

Delete data sources.

dsEditDataSource

Edit a data source's properties.

dsEditDataSourceClient

Edit client datasource properties

dsGetDataSourceClients

Gets a list of clients associated with a datasource

dsGetDataSourceDetail

Get the details for a specifc data sources.

dsGetDataSourceList

Get a list of defined data sources.

dsGetDataSourceTypes

Get all data source types.

dsGetEpoList

Get a list of valid ePO servers for the given target IPs

dsGetUserDefinedDataSources

Get user defined data sources.

dsSetUserDefinedDataSources

Set user defined data sources.

dsWriteThirdpartyConfig

Write out third party config for receiver

essmgtGetBuildStamp

Gets the ESM build Stamp

essmgtGetESSTime

Get the system time of the ESM Device

geoGetGeoLocRegionList

Get the top level geo locations

geoGetGeoLocs

Get geo locations within the given location

getActiveResponseCollectors

Get a list of Active Response Collectors

grpGetDeviceTree

Gets the basic device tree structure with only basic properties loaded. Each entry in the returned list is a root node in the tree.

grpGetDeviceTreeEx

This version of the call returns more detail per device than getDeviceList, wrapped in an esmDeviceList object.

ipsGetAlertData

Gets alert data

ipsGetCorrRawEvents

Get the corr raw events

miscJobStatus

This gets the job status

miscKeepAlive

Keeps the session alive.

notifyGetTriggeredNotificationDetail

Gets the details for the triggered alarm

plcyGetPolicyList

Get the list of all policies defined in the ESM.

plcyGetVariableList

Get all variables defined in the system

plcyRollPolicy

Kicks off policy rollout for datsource ids passed in and returns a list of job ids

qryClose

Closes the query results, must be called after a query's results have been processed. If no exception is thrown, the close operation completed normally.

qryExecute

Execute a query against the database.

qryExecuteDetail

Execute a standard detail (non-grouped) query.

qryExecuteGrouped

Execute a grouped query giving the count and sum

qryGetCorrEventDataForID

Get the source events and flows for a given correlated event ID

qryGetFilterFields

Get all fields that can be used in query filters, with type information for each field.

Get all fields that can be used in query filters, with type information for each field.

qryGetResults

Get the results for a query.

qryGetSelectFields

Get the fields available for selecting in queries. The groupType can be used to filter the fields to only ones that can be used to group results in a particular way. For example, if you want all fields that can be grouped to count the number of events per group, the groupType should be COUNT. If not provided, it is equivalent to passing NO_GROUP which returns all available select fields regardless of whether they can be used in grouped queries. This is useful for getting available fields for detail queries. (qryExecuteDetail)

qryGetStatus

Get the status for a query that has been executed.

runActiveResponseSearch

Execute a ActiveResponse search and return the results

sysAddWatchlist

Add a watchlist to the system.

sysAddWatchlistValues

Add values to a watchlist. This call is not supported for hidden watchlists, for example GTI.

sysEditWatchlist

Edit properties of a watchlist. (Watchlist Type will not be modified) This call is not supported for hidden watchlists, for example GTI.

sysGetWatchlistDetails

Get detailed information about a watchlist.

sysGetWatchlistFields

Get watchlist fields/types.

sysGetWatchlistValues

Read the content of a watchlist value file. Note that the EsmFileData object will contain information on how many bytes were read, as well as the total size of the file. The size of the data returned may be less than count, depending on the amount of file data available. Note that the watchlist file property on EsmWatchlistDetails is used as a parameter to this call. The file will contain the values as they existed when the call to sysGetWatchlistDetails was made. If subsequent changes were made to the watchlist after getting the details, another EsmWatchlistDetails object should be obtained by calling sysGetWatchlistDetails before using its EsmWatchlistFile object to retrieve the updated list of watchlist values. This call is not supported for hidden watchlists, for example GTI.

sysGetWatchlists

Return basic information on all watchlists in the system

sysRemoveWatchlist

Remove watchlist/s from the system. This call is not supported for hidden watchlists, for example GTI.

sysRemoveWatchlistValues

Remove values from a watchlist. This call is not supported for hidden watchlists, for example GTI.

userAddAccessGroup

Add an access group

userAddUser

Add a user to the system.

userCaseList

Get a filtered list of cases from the system

userDeleteAccessGroup

Delete an access group.

userDeleteUser

Delete a user from the system.

userEditAccessGroup

Edit properties of an access group.

userEditUser

Used by the master user to update information about another user.

userGetAccessGroupDetail

Get extended information about an access group.

userGetAccessGroupList

Get all user access groups defined in the system.

userGetRightsList

Get all rights defined in the system.

userGetTimeZones

Get a list of timezones this system recognizes

userGetUserList

Get a list of all users.

userGetUserRights

Get all rights defined for the current user.

zoneAddSubZone

Add a new subzone under a zone

zoneAddZone

Create a new zone.

zoneDeleteSubZone

Delete the sub zone

zoneDeleteZone

Delete the zone

zoneEditSubZone

Edit the given sub zone. Note that ID must be set to an existing sub zone for this to work properly. The ID value will be set if the zone was gotten from zoneGetSubZone().

zoneEditZone

Edit the given zone. Note that ID must be set to an existing zone for this to work properly. The ID value will be set if the zone was gotten from zoneGetZone().

zoneGetSubZone

Get detailed information on a sub zone

zoneGetZone

Get extended detail on a zone.

zoneGetZoneTree

Get the full tree of zones defined in the ESM.

Get the full text of Zenos defined in the ZCM.

alarmAcknowledgeTriggeredAlarm

Description

Mark a triggered alarm as acknowledged

Parameters

triggeredIds

- Type: EsmAlarmIds
- Description: list of triggered alarm ids to be marked acknowledged

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/alarmAcknowledgeTriggeredAlarm

Example JSON Content:

```
{"triggeredIds": {"alarmIdList": ["(alarmIdList)"]}}
```

Back to Command List

alarmDeleteTriggeredAlarm

Description

Delete a triggered alarm

Parameters

triggeredIds

- Type: EsmAlarmIds
- Description: list of triggered alarm ids to be deleted

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/alarmDeleteTriggeredAlarm

Example JSON Content:

```
{"triggeredIds": {"alarmIdList": ["(alarmIdList)"]}}
```

Back to Command List

alarmGetTriggeredAlarms

Description

Retrieves a paged list of alarms that have been triggered

Parameters

assignedUser

- Type: EsmUser
- Description: the userid assigned to handle this triggered alarm (default is current user)

triggeredTimeRange

- Type: EsmTimeRange
- Description: filter the list of alarms by those that where triggered in this time range
- Accepted Values:
  - CUSTOM
  - LAST_MINUTE
  - LAST_10_MINUTES
  - LAST_30_MINUTES
  - LAST_HOUR
  - CURRENT_DAY
  - PREVIOUS_DAY
  - LAST_24_HOURS
  - LAST_2_DAYS
  - LAST_3_DAYS
  - CURRENT_WEEK
  - PREVIOUS_WEEK
  - CURRENT_MONTH
  - PREVIOUS_MONTH
  - CURRENT_QUARTER
  - PREVIOUS_QUARTER
  - CURRENT_YEAR
  - PREVIOUS_YEAR

customStart

- Type: DATETIME
- Description: if triggeredTimeRange is CUSTOM, start time for the time range (ignored if triggeredTimeRange is not CUSTOM)

customEnd

- Type: DATETIME
- Description: if triggeredTimeRange is CUSTOM, end time for the time range (ignored if triggeredTimeRange is not CUSTOM)

status

- Type: STRING
- Description: can be (case sensitive) 'acknowledged', 'unacknowledged', "" or null -> all (default is null)

pageSize

- Type: STRING
- Description: the number of alarms to return per page (default is 1000, max is 5000)

pageNumber

- Type: STRING
- Description: which page of alarms we want to return (default is 1)

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmTriggeredAlarm
- Description: list of alarms that have been triggered

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/alarmGetTriggeredAlarms?triggeredTimeRange=CUSTOM&customStart=2020-03-11T11:30:12.546Z&customEnd=2020-03-11T11:30:12.546Z&status=(status)&pageSize=(pageSize)&pageNumber=(pageNumber)

Example JSON Content:


```
{"assignedUser": {
    "username": "(username)",
    "id": 0,
    "locked": false,
    "loggedInCount": 0,
    "email": "(email)",
    "emailId": 0,
    "sms": "(sms)",
    "smsId": 0,
    "master": false,
    "admin": false,
    "alias": "(alias)",
    "type": "POWER",
    "groups": [0]
}}
```


Back to Command List

alarmUnacknowledgeTriggeredAlarm

Description

Mark a triggered alarm as unacknowledged

Parameters

triggeredIds

- Type: EsmAlarmIds
- Description: list of triggered alarm ids to be marked unacknowledged

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/alarmUnacknowledgeTriggeredAlarm

Example JSON Content:

```
{"triggeredIds": {"alarmIdList": ["(alarmIdList)"]}}
```

Back to Command List

assetGetAssetDetailsObject

Description

Gets asset Details

Parameters

assetId

- Type: AssetId
- Description: - Asset ID

Return Value ("return" JSON root element is NOT returned)

- Type: AssetDetailsObject
- Description: AssetDetailsObject - Asset Details Object

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/assetGetAssetDetailsObject

Example JSON Content:

```
{"assetId": 0}
```

Back to Command List

assetGetAssetThreats

Description

Gets asset threats

Parameters

assetId

- Type: AssetId
- Description: - Asset ID

Return Value ("return" JSON root element is NOT returned)

- Type: JsonString
- Description: AssetDetailsObject - Asset Details Object

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/assetGetAssetThreats

Example JSON Content:

```
{"assetId": 0}
```

Back to Command List

caseAddCase

Description

Add a case to the system.

Parameters

caseDetail

- Type: EsmCaseDetail
- Description: the details of the case to add to the system

Return Value ("return" JSON root element is NOT returned)

- Type: EsmCaseId
- Description: the id of the case that was added

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseAddCase

Example JSON Content:

```
{"caseDetail": {
    "summary": "(summary)",
    "id": 0,
    "statusId": {"value": 0},
    "severity": 0,
    "openTime": "(openTime)",
    "assignedTo": 0,
    "orgId": 0,
    "closeTime": "(closeTime)",
    "eventList": [{
        "id": "(value)",
        "message": "(message)",
        "lastTime": "(lastTime)"
    }],
    "deviceList": ["123456789000"],
    "dataSourceList": ["(value)"],
    "notes": "(notes)",
    "noteAdded": "(noteAdded)",
    "history": "(history)"
}}
```

Back to Command List

caseAddCaseStatus

Description

Add a case status

Parameters

status

- Type: EsmCaseStatus
- Description: the status of the case to add

Return Value ("return" JSON root element is NOT returned)

- Type: EsmCaseStatusId
- Description: status id

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseAddCaseStatus

Example JSON Content:

```
{"status": {
    "name": "(name)",
    "id": 0,
    "default": false,
    "showInCasePane": false
}}
```

Back to Command List

caseAddOrganization

Description

Add a case organization

Parameters

organization

- Type: EsmCaseOrganization
- Description: the organization of the case to add

Return Value ("return" JSON root element is NOT returned)

- Type: EsmOrganizationId
- Description: organization id

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseAddOrganization

Example JSON Content:

```
{"organization": {
    "name": "(name)",
    "id": 0
}}
```

Back to Command List

caseDeleteCaseStatus

Description

Delete a case status.

Parameters

statusId

- Type: EsmCaseStatusId
- Description: the status id of the case to delete

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseDeleteCaseStatus

Example JSON Content:

```
{"statusId": {"value": 0}}
```

Back to Command List

caseEditCase

Description

Edit an existing case.

Parameters

caseDetail

- Type: EsmCaseDetail
- Description: the details of the case to edit

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseEditCase

Example JSON Content:

```
{"caseDetail": {
    "summary": "(summary)",
    "id": 0,
    "statusId": {"value": 0},
    "severity": 0,
    "openTime": "(openTime)",
    "assignedTo": 0,
    "orgId": 0,
    "closeTime": "(closeTime)",
    "eventList": [{
        "id": "(value)",
        "message": "(message)",
        "lastTime": "(lastTime)"
    }],
    "deviceList": ["123456789000"],
    "dataSourceList": ["(value)"],
    "notes": "(notes)",
    "noteAdded": "(noteAdded)",
    "history": "(history)"
}}
```

Back to Command List

caseEditCaseStatus

Description

Edit a case status

Parameters

status

- Type: EsmCaseStatus
- Description: the status of the case to edit

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseEditCaseStatus

Example JSON Content:

```
{"status": {
    "name": "(name)",
    "id": 0,
    "default": false,
    "showInCasePane": false
}}
```

Back to Command List

caseEditOrganization

Description

Edit a case organization

Parameters

organization

- Type: EsmCaseOrganization
- Description: the organization of the case to edit

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseEditOrganization

Example JSON Content:

```
{"organization": {
    "name": "(name)",
    "id": 0
}}
```

Back to Command List

caseGetCaseDetail

Description

Get detail on an existing case.

Parameters

id

- Type: EsmCaseId
- Description: identifier for this case to be retrieved

Return Value ("return" JSON root element is NOT returned)

- Type: EsmCaseDetailExternal
- Description: details of the specified case

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseGetCaseDetail

Example JSON Content:

```
{"id": 0}
```

Back to Command List

caseGetCaseEventsDetail

Description

Get case events details

Parameters

eventIds

- Type: EsmStringList
- Description: the event ids to get the details for

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmCaseEvent
- Description: list of case events

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseGetCaseEventsDetail

Example JSON Content:

```
{"eventIds": {"list": ["(list)"]}}
```

Back to Command List

caseGetCaseList

Description

Get a list of cases from the system

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmCase
- Description: list of cases from the system

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseGetCaseList

Back to Command List

caseGetCaseStatusList

Description

Get a list of valid case statuses from the system

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmCaseStatus
- Description: list of case statuses in the system

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseGetCaseStatusList

Back to Command List

caseGetCaseUsers

Description

Get case users

Return Value ("return" JSON root element is NOT returned)

- Type: EsmCaseUserList
- Description: list of case users

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseGetCaseUsers

Back to Command List

caseGetOrganizationList

Description

Get case organizations

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmCaseOrganization
- Description: list of case organizations

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/caseGetOrganizationList

Back to Command List

devGetDeviceList

Description

Get a list of all devices defined in the system.

Parameters

types

- Type: List of EsmDeviceType
- Description: The types of devices desired

filterByRights

- Type: BOOLEAN
- Description: Whether to filter out devices on which the user doesn't have action rights

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmDevice
- Description: The list of devices

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/devGetDeviceList?filterByRights=false

Example JSON Content:

```
{"types": ["IPS"]}
```

Back to Command List

dsAddDataSourceClients

Description

Add client datasources to another datasource

Parameters

parentId

- Type: IpsId
- Description: ipsid of parent datasource

clients

- Type: List of DataSourceClientAdd
- Description: datasources to add as client

Return Value ("return" JSON root element is NOT returned)

- Type: EsmJobId
- Description: jobid for adding

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsAddDataSourceClients

Example JSON Content:

```
{
    "parentId": "(value)",
    "clients": [null]
}
```

Back to Command List

dsAddDataSourceClientsStatus

Description

Get status of adding clients

Parameters

jobId

- Type: EsmJobId
- Description: job id from dsAddDataSourceClients

Return Value ("return" JSON root element is NOT returned)

- Type: AddDatasourceClientResponse
- Description: status of add clients

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsAddDataSourceClientsStatus

Example JSON Content:

```
{"jobId": 0}
```

Back to Command List

dsAddDataSources

Description

Add a list of data sources.

Parameters

receiverId

- Type: IpsId
- Description: receiver to add datasources to

datasources

- Type: List of DataSourceDataAdd
- Description: list of datasources to add

Return Value ("return" JSON root element is NOT returned)

- Type: EsmJobId
- Description: jobid from add

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsAddDataSources

Example JSON Content:

```
{
    "receiverId": "(value)",
    "datasources": [{
        "name": "(name)",
        "ipAddress": "(ipAddress)",
        "typeId": 0,
        "zoneId": 0,
        "enabled": false,
        "url": "(url)",
        "parameters": [{
            "key": "(key)",
            "value": "(value)"
        }]
    }]
}
```

Back to Command List

dsAddDataSourcesStatus

Description

Get the status of adding datasources

Parameters

jobId

- Type: EsmJobId
- Description: id returned from dsAddDataSources

Return Value ("return" JSON root element is NOT returned)

- Type: AddDatasourceResponse
- Description: details from adding datasources

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsAddDataSourcesStatus

Example JSON Content:

```
{"jobId": 0}
```

Back to Command List

dsDeleteDataSourceClients

Description

Delete client datasource

Parameters

parentId

- Type: IpsId
- Description: id of parent datasource to delete

clientIds

- Type: List of IpsId
- Description: id of client datasource to delete

Return Value ("return" JSON root element is NOT returned)

- Type: WriteRollDatasourceResponse
- Description: the jobId of the delete

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsDeleteDataSourceClients

Example JSON Content:

```
{
    "parentId": "(value)",
    "clientIds": ["(value)"]
}
```

Back to Command List

dsDeleteDataSources

Description

Delete data sources.

Parameters

receiverId

- Type: IpsId
- Description: ID of the receiver to delete the datasources from

datasourceIds

- Type: List of IpsId
- Description: ID of the datasources to delete

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsDeleteDataSources

Example JSON Content:

```
{
    "receiverId": "(value)",
    "datasourceIds": ["(value)"]
}
```

Back to Command List

dsEditDataSource

Description

Edit a data source's properties.

Parameters

datasource

- Type: DatasourceDataEdit
- Description: detail of datasource and properties to edit

rollPolicy

- Type: EsmBoolean
- Description: roll policy now

Return Value ("return" JSON root element is NOT returned)

- Type: WriteRollDatasourceResponse
- Description: job id for policy rollout

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsEditDataSource

Example JSON Content:

```
{
    "datasource": {
        "id": "(value)",
        "name": "(name)",
        "ipAddress": "(ipAddress)",
        "typeId": 0,
        "zoneId": 0,
        "enabled": false,
        "url": "(url)",
        "parameters": [{
            "key": "(key)",
            "value": "(value)"
        }]
    },
    "rollPolicy": true
}
```

Back to Command List

dsEditDataSourceClient

Description

Edit client datasource properties

Parameters

clientId

- Type: IpsId
- Description: id of client to edit

client

- Type: EsmDataSourceClient
- Description: datasource to edit as client

rollPolicy

- Type: EsmBoolean
- Description: roll policy now

Return Value ("return" JSON root element is NOT returned)

- Type: WriteRollDatasourceResponse
- Description: job id for policy rollout

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsEditDataSourceClient

Example JSON Content:

```
{
    "clientId": "(value)",
    "client": {
        "id": 123456789000,
        "name": "(name)",
        "enabled": false,
        "ipAddress": "(ipAddress)",
        "host": "(host)",
        "type": "(type)",
        "timezone": "(timezone)",
        "dateOrder": "(dateOrder)",
        "port": "(port)",
        "useTls": false
    },
    "rollPolicy": true
}
```

Back to Command List

dsGetDataSourceClients

Description

Gets a list of clients associated with a datasource

Parameters

datasourceId

- Type: IpsId
- Description: id of datasource whose clients will be returned

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmDataSourceClient
- Description: list of clients associated with the referenced datasource

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsGetDataSourceClients

Example JSON Content:

```
{"datasourceId": "(value)"}
```

Back to Command List

dsGetDataSourceDetail

Description

Get the details for a specifc data sources.

Parameters

datasourceId

- Type: IpsId
- Description: ID of the datasource to be retrieved

Return Value ("return" JSON root element is NOT returned)

- Type: DataSourceData
- Description: Details of datasource specified.

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsGetDataSourceDetail

Example JSON Content:

```
{"datasourceId": "(value)"}
```

Back to Command List

dsGetDataSourceList

Description

Get a list of defined data sources.

Parameters

receiverId

- Type: IpsId
- Description: ID of the receiver to get the datasource list from

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmDataSource
- Description: List of datasource assigned to a given receiver.

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsGetDataSourceList

Example JSON Content:

```
{"receiverId": "(value)"}
```

Back to Command List

dsGetDataSourceTypes

Description

Get all data source types.

Parameters

receiverId

- Type: IpsId
- Description: ID of the receiver to get the datasource types from

Return Value ("return" JSON root element is NOT returned)

- Type: EsmDataSourceType
- Description: type object that contains a list of vendors and their models comprising all vendors and models in the system.

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsGetDataSourceTypes

Example JSON Content:

```
{"receiverId": "(value)"}
```

Back to Command List

dsGetEpoList

Description

Get a list of valid ePO servers for the given target IPs

Parameters

targetIPs

- Type: EPOListRequest
- Description: A comma separated list of IP to investigate

Return Value ("return" JSON root element is NOT returned)

- Type: EPOList
- Description: An object containing info about the available ePO servers

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsGetEpoList

Example JSON Content:

```
{"targetIPs": {"targetIPs": "(targetIPs)"}}
```

Back to Command List

dsGetUserDefinedDataSources

Description

Get user defined data sources.

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmUserDefinedDataSource
- Description: List of user defined datasources

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsGetUserDefinedDataSources

Back to Command List

dsSetUserDefinedDataSources

Description

Set user defined data sources.

Parameters

list

- Type: List of EsmUserDefinedDataSource
- Description: The list of user defined datasources to rename

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsSetUserDefinedDataSources

Example JSON Content:

```
{"list": [{
    "name": "(name)",
    "id": 0
}]}
```

Back to Command List

dsWriteThirdpartyConfig

Description

Write out third party config for receiver

Parameters

receiverId

- Type: IpsId
- Description: ipsid of receiver to writeout

Return Value ("return" JSON root element is NOT returned)

- Type: EsmJobId
- Description: job id for witeout

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/dsWriteThirdpartyConfig

Example JSON Content:

```
{"receiverId": "(value)"}
```

Back to Command List

essmgtGetBuildStamp

Description

Gets the ESM build Stamp

Return Value ("return" JSON root element is NOT returned)

- Type: EsmBuildStamp
- Description: buildStamp

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/essmgtGetBuildStamp

Back to Command List

essmgtGetESSTime

Description

Get the system time of the ESM Device

Return Value ("return" JSON root element is NOT returned)

- Type: EsmRestCalendar
- Description: the system time of the ESM Device

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/essmgtGetESSTime

Back to Command List

geoGetGeoLocRegionList

Description

Get the top level geo locations

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmGeoLoc
- Description: The top level geo locations

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/geoGetGeoLocRegionList

Back to Command List

geoGetGeoLocs

Description

Get geo locations within the given location

Parameters

location

- Type: EsmGeoLoc
- Description: The location whose more specific geo locations are needed

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmGeoLoc
- Description: The list of geo locations within the location passed in

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/geoGetGeoLocs

Example JSON Content:

```
{"location": {
    "id": "123456789000",
    "name": "(name)"
}}
```

Back to Command List

getActiveResponseCollectors

Description

Get a list of Active Response Collectors

Return Value ("return" JSON root element is NOT returned)

- Type: STRING
- Description: The list of active response collectors.

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/getActiveResponseCollectors

Back to Command List

grpGetDeviceTree

Description

Gets the basic device tree structure with only basic properties loaded. Each entry in the returned list is a root node in the tree.

Parameters

hideDisabledDevices

- Type: BOOLEAN
- Description: Whether disabled devices should be returned

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmTreeNode
- Description: The list of root nodes in the device tree

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/grpGetDeviceTree?hideDisabledDevices=false

Back to Command List

grpGetDeviceTreeEx

Description

This version of the call returns more detail per device than getDeviceList, wrapped in an esmDeviceList object.

Parameters

displayID

- Type: UINT32
- Description: The ID of the display, zero is the default

hideDisabledDevices

- Type: BOOLEAN
- Description: Whether to hide disabled devices on the tree

Return Value ("return" JSON root element is NOT returned)

- Type: EsmDeviceTreeEx
- Description: A detailed EsmDeviceTreeEx object

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/grpGetDeviceTreeEx?displayID=0&hideDisabledDevices=false

Back to Command List

ipsGetAlertData

Description

Gets alert data

Parameters

id

- Type: EsmAlertId
- Description: The IPSIDAlertID of the event

Return Value ("return" JSON root element is NOT returned)

- Type: EsmAlertData
- Description: The data for the alert

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/ipsGetAlertData

Example JSON Content:

```
{"id": "(value)"}
```

Back to Command List

ipsGetCorrRawEvents

Description

Get the corr raw events

Parameters

id

- Type: EsmAlertId
- Description: - the event to get the events for

Return Value ("return" JSON root element is NOT returned)

- Type: EsmSourceEvents
- Description: the events

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/ipsGetCorrRawEvents

Example JSON Content:

```
{"id": "(value)"}
```

Back to Command List

miscJobStatus

Description

This gets the job status

Parameters

jobId

- Type: UINT16
- Description: the id of the job

Return Value ("return" JSON root element is NOT returned)

- Type: EsmJobStatus
- Description: the JobStatus

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/miscJobStatus?jobId=0

Back to Command List

miscKeepAlive

Description

Keeps the session alive.

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/miscKeepAlive

Back to Command List

notifyGetTriggeredNotificationDetail

Description

Gets the details for the triggered alarm

Parameters

id

- Type: EsmAlarmId
- Description: - the alarm to get the details for

Return Value ("return" JSON root element is NOT returned)

- Type: EsmTriggeredAlarmDetail
- Description: alarm details

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/notifyGetTriggeredNotificationDetail

Example JSON Content:

```
{"id": 0}
```

Back to Command List

plcyGetPolicyList

Description

Get the list of all policies defined in the ESM.

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmPolicy
- Description: The list of policies defined in the system

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/plcyGetPolicyList

Back to Command List

plcyGetVariableList

Description

Get all variables defined in the system

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmVariable
- Description: The list of variable

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/plcyGetVariableList

Back to Command List

plcyRollPolicy

Description

Kicks off policy rollout for datsource ids passed in and returns a list of job ids

Parameters

ids

- Type: List of IpsId
- Description: ipsids for datasources you wish to rollout

Return Value ("return" JSON root element is NOT returned)

- Type: PolicyRolloutResponse
- Description: list of job ids for policy rolled out

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/plcyRollPolicy

Example JSON Content:

```
{"ids": ["(value)"]}
```

Back to Command List

qryClose

Description

Closes the query results, must be called after a query's results have been processed. If no exception is thrown, the close operation completed normally.

Parameters

resultID

- Type: EsmQueryResultID
- Description: The results being closed

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/qryClose

Example JSON Content:

```
{"resultID": "123456789000"}
```

Back to Command List

qryExecute

Description

Execute a query against the database.

Parameters

qid

- Type: EsmQueryId
- Description: - The type of the query that you want to run. Events = 6, Flows = 10, etc.

filter

- Type: STRING
- Description: - A string representation of the query filters needed to obtain the desired results.

background

- Type: STRING
- Description: - If the query should be run asynchronous or non-asynchronous. "T" or "F".

reverse

- Type: STRING
- Description: - If the results should come in reverse order nor not. "T" or "F".

getTotal

- Type: STRING
- Description: - Return the total rows. "T" or "F".

Return Value ("return" JSON root element is NOT returned)

- Type: EsmRunningQuery
- Description: EsmRunningQuery - The overall results of the query.

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/qryExecute?filter=(filter)&background=(background)&reverse=(reverse)&getTotal=(getTotal)

Example JSON Content:

```
{"qid": 0}
```

Back to Command List

qryExecuteDetail

Description

Execute a standard detail (non-grouped) query.

Parameters

type

- Type: EsmQueryType
- Description: The type of query to execute, either EVENT or FLOW
- Accepted Values:
  - EVENT
  - FLOW
  - IPS_QUERY
  - ASSET
  - CASE_QUERY
  - FILTER_QUERY
  - TRIGGERED_ALARMS_QUERY
  - EPO_REALTIME_QUERY
  - MISC_QUERY
  - IOC_QUERY
  - RISK
  - AGG1
  - AGG2
  - AGG3
  - CORRELATION
  - WATCHLIST

config

- Type: EsmQueryConfig
- Description: The parameters to apply to the query including filters, ordering, fields, etc

reverse

- Type: BOOLEAN
- Description: Whether to reverse the order of the results

Return Value ("return" JSON root element is NOT returned)

- Type: EsmRunningQuery
- Description: The active query information, created as a result of executing the query successfully.

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/qryExecuteDetail?type=EVENT&reverse=false

Example JSON Content:

```
{"config": {
    "timeRange": "CUSTOM",
    "customStart": "2020-03-11T11:30:12.583Z",
    "customEnd": "2020-03-11T11:30:12.584Z",
    "order": [{
        "direction": "ASCENDING",
        "field": {
            "name": "(name)",
            "typeBits": 0,
            "id": "(id)"
        }
    }],
    "includeTotal": false,
    "fields": [{
        "name": "(name)",
        "typeBits": 0,
        "id": "(id)"
    }],
    "filters": [{
        "type": "EsmFieldFilter",
        "field": {"name": "(name)"},
        "operator": "IN",
        "values": [{
            "type": "EsmWatchlistValue",
            "watchlist": 0
```

```
            }]
        }],
        "limit": 0,
        "offset": 0,
        "netmask": "(netmask)"
    }}
```

Back to Command List

qryExecuteGrouped

Description

Execute a grouped query giving the count and sum

Parameters

queryType

- Type: EsmGroupedQueryType
- Description: Query type
- Accepted Values:
  - EVENT
  - FLOW

config

- Type: EsmGroupedQueryConfig
- Description: The parameters to apply to the query including filters, time range, field, etc

Return Value ("return" JSON root element is NOT returned)

- Type: EsmRunningQuery
- Description: The active query information, created as a result of executing the query successfully.

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/qryExecuteGrouped?queryType=EVENT

Example JSON Content:

```
{"config": {
    "filters": [{
        "type": "EsmFieldFilter",
        "field": {"name": "(name)"},
        "operator": "IN",
        "values": [{
            "type": "EsmWatchlistValue",
            "watchlist": 0
        }]
    }],
    "field": {"name": "(name)"},
    "timeRange": "CUSTOM",
    "customStart": "2020-03-11T11:30:12.597Z",
    "customEnd": "2020-03-11T11:30:12.598Z"
}}
```

Back to Command List

qryGetCorrEventDataForID

Description

Get the source events and flows for a given correlated event ID

Parameters

queryType

- Type: EsmQueryType
- Description: Either EVENT or FLOW depending on the events needed
- Accepted Values:
  - EVENT
  - FLOW
  - IPS_QUERY
  - ASSET
  - CASE_QUERY
  - FILTER_QUERY
  - TRIGGERED_ALARMS_QUERY
  - EPO_REALTIME_QUERY
  - MISC_QUERY
  - IOC_QUERY
  - RISK
  - AGG1
  - AGG2
  - AGG3
  - CORRELATION
  - WATCHLIST

eventId

- Type: EsmAlertId
- Description: The event ID whose source events are needed

fields

- Type: List of EsmSelectField
- Description: The list of fields to provide in the returned rows

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmQueryRow
- Description: The list of rows from the database describing the source events.

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/qryGetCorrEventDataForID?queryType=EVENT

Example JSON Content:

```
{
    "eventId": "(value)",
    "fields": [{
        "name": "(name)",
        "typeBits": 0,
        "id": "(id)"
    }]
}
```

Back to Command List

qryGetFilterFields

Description

Get all fields that can be used in query filters, with type information for each field.

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmFilterField
- Description: The list of available fields to filter on

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/qryGetFilterFields

Back to Command List

qryGetResults

Description

Get the results for a query.

Parameters

resultID

- Type: EsmQueryResultID
- Description: The result ID whose data is being requested

startPos

- Type: UINT32
- Description: The start position of the requested data

numRows

- Type: UINT32
- Description: The number of rows requested

Return Value ("return" JSON root element is NOT returned)

- Type: EsmQueryResults
- Description: The data requested

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/qryGetResults?startPos=0&numRows=0

Example JSON Content:

```
{"resultID": "123456789000"}
```

Back to Command List

qryGetSelectFields

Description

Get the fields available for selecting in queries. The groupType can be used to filter the fields to only ones that can be used to group results in a particular way. For example, if you want all fields that can be grouped to count the number of events per group, the groupType should be COUNT. If not provided, it is equivalent to passing NO_GROUP which returns all available select fields regardless of whether they can be used in grouped queries. This is useful for getting available fields for detail queries. (qryExecuteDetail)

Parameters

type

- Type: EsmQueryType
- Description: The type of query being executed
- Accepted Values:
  - EVENT
  - FLOW
  - IPS_QUERY
  - ASSET
  - CASE_QUERY
  - FILTER_QUERY
  - TRIGGERED_ALARMS_QUERY
  - EPO_REALTIME_QUERY
  - MISC_QUERY
  - IOC_QUERY
  - RISK
  - AGG1
  - AGG2
  - AGG3
  - CORRELATION
  - WATCHLIST

groupType

- Type: EsmQueryGroupType
- Description: If the intention is to execute a grouped query, provide the type of grouping desired (meaning what numeric value are we grouping for, count, risk, etc) - leave empty or set to NO_GROUP for all select fields
- Accepted Values:
  - NO_GROUP
  - COUNT
  - SEVERITY
  - RISK
  - AVERAGE
  - SUM

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmSelectField
- Description: The list of fields that can be selected for this type of query

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/qryGetSelectFields?type=EVENT&groupType=NO_GROUP

Back to Command List

qryGetStatus

Description

Get the status for a query that has been executed.

Parameters

resultID

- Type: EsmQueryResultID
- Description: The ID of the results, gotten from the EsmActiveQuery returned from qryExecuteQuery()

Return Value ("return" JSON root element is NOT returned)

- Type: EsmQueryStatus
- Description: The status of the running query, including things like percent complete

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/qryGetStatus

Example JSON Content:

```
{"resultID": "123456789000"}
```

Back to Command List

runActiveResponseSearch

Description

Execute a ActiveResponse search and return the results

Parameters

params

- Type: MActiveResponseParams
- Description: search parameters for ActiveResponse search api

Return Value ("return" JSON root element is NOT returned)

- Type: STRING
- Description: The search results

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/runActiveResponseSearch

Example JSON Content:

```
{"params": {
    "select": {"fields": ["(fields)"]},
    "filters": {"or": [{"and": [{
        "name": "(name)",
        "op": "(op)",
        "value": "(value)",
        "output": "(output)",
        "group": "(group)"
    }]}]}
}}
```

Back to Command List

sysAddWatchlist

Description

Add a watchlist to the system.

Parameters

watchlist

- Type: EsmWatchlistDetails
- Description: The watchlist to be added

Return Value ("return" JSON root element is NOT returned)

- Type: STRING
- Description: The id of the watchlist that was created

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/sysAddWatchlist

Example JSON Content:

```
{"watchlist": {
    "name": "(name)",
    "type": {
        "name": "(name)",
        "id": 0
    },
    "customType": {
        "name": "(name)",
        "id": 0
    },
    "dynamic": false,
    "source": 0,
    "id": 0,
    "search": "(search)",
    "updateType": "EVERY_SO_MANY_MINUTES",
    "updateDay": 0,
    "updateMin": 0,
    "ipsid": "(ipsid)",
    "valueFile": {"fileToken": "(fileToken)"},
    "dbUrl": "(dbUrl)",
    "mountPoint": "(mountPoint)",
    "path": "(path)",
    "port": "(port)",
    "username": "(username)",
    "password": "(password)",
    "query": "(query)",
    "lookup": "(lookup)",
    "enabled": false,
    "jobTrackerURL": "(jobTrackerURL)",
    "jobTrackerPort": "(jobTrackerPort)",
    "postArgs": "(postArgs)",
    "sSLCheck": "(sSLCheck)",
    "ignoreRegex": "(ignoreRegex)",
    "method": 0,
    "matchRegex": "(matchRegex)",
    "lineSkip": 0,
    "delimitRegex": "(delimitRegex)",
    "groups": "(groups)",
    "values": ["(values)"]
}}
```

Back to Command List

sysAddWatchlistValues

Description

Add values to a watchlist. This call is not supported for hidden watchlists, for example GTI.

Parameters

watchlist

- Type: EsmWatchlistId
- Description: ID of the watchlist

values

- Type: List of STRING
- Description: List of string values to be added to a watchlist

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/sysAddWatchlistValues

Example JSON Content:

```
{
    "watchlist": 0,
    "values": ["(values)"]
}
```

Back to Command List

sysEditWatchlist

Description

Edit properties of a watchlist. (Watchlist Type will not be modified) This call is not supported for hidden watchlists, for example GTI.

Parameters

watchlist

- Type: EsmWatchlistDetails
- Description: The watchlist to be edited

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/sysEditWatchlist

Example JSON Content:

```
{"watchlist": {
    "name": "(name)",
    "type": {
        "name": "(name)",
        "id": 0
    },
    "customType": {
        "name": "(name)",
        "id": 0
    },
    "dynamic": false,
    "source": 0,
    "id": 0,
    "search": "(search)",
    "updateType": "EVERY_SO_MANY_MINUTES",
    "updateDay": 0,
    "updateMin": 0,
    "ipsid": "(ipsid)",
    "valueFile": {"fileToken": "(fileToken)"},
    "dbUrl": "(dbUrl)",
    "mountPoint": "(mountPoint)",
    "path": "(path)",
    "port": "(port)",
    "username": "(username)",
    "password": "(password)",
    "query": "(query)",
    "lookup": "(lookup)",
    "enabled": false,
    "jobTrackerURL": "(jobTrackerURL)",
    "jobTrackerPort": "(jobTrackerPort)",
    "postArgs": "(postArgs)",
    "sSLCheck": "(sSLCheck)",
    "ignoreRegex": "(ignoreRegex)",
    "method": 0,
    "matchRegex": "(matchRegex)",
    "lineSkip": 0,
    "delimitRegex": "(delimitRegex)",
    "groups": "(groups)",
    "values": ["(values)"]
}}
```

Back to Command List

sysGetWatchlistDetails

Description

Get detailed information about a watchlist.

Parameters

id

- Type: EsmWatchlistId
- Description: ID of the watchlist

Return Value ("return" JSON root element is NOT returned)

- Type: EsmWatchlistDetails
- Description: details of the watchlist specified

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/sysGetWatchlistDetails

Example JSON Content:

```
{"id": 0}
```

Back to Command List

sysGetWatchlistFields

Description

Get watchlist fields/types.

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmWatchlistField
- Description: The list of watchlist fields/types defined in the system

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/sysGetWatchlistFields

Back to Command List

sysGetWatchlistValues

Description

Read the content of a watchlist value file. Note that the EsmFileData object will contain information on how many bytes were read, as well as the total size of the file. The size of the data returned may be less than count, depending on the amount of file data available. Note that the watchlist file property on EsmWatchlistDetails is used as a parameter to this call. The file will contain the values as they existed when the call to sysGetWatchlistDetails was made. If subsequent changes were made to the watchlist after getting the details, another EsmWatchlistDetails object should be obtained by calling sysGetWatchlistDetails before using its EsmWatchlistFile object to retrieve the updated list of watchlist values. This call is not supported for hidden watchlists, for example GTI.

Parameters

file

- Type: EsmWatchlistFile
- Description: The watchlist file whose data is being requested

pos

- Type: UINT16
- Description: The starting byte position to read from

count

- Type: UINT16
- Description: The number of bytes to read

Return Value ("return" JSON root element is NOT returned)

- Type: EsmFileData
- Description: The file data

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/sysGetWatchlistValues?pos=0&count=0

Example JSON Content:

```
{"file": {"id": "(id)"}}
```

Back to Command List

sysGetWatchlists

Description

Return basic information on all watchlists in the system

Parameters

filters

- Type: List of EsmWatchlistField
- Description: List of fields/types used to filter the list of watchlists returned

hidden

- Type: BOOLEAN
- Description: Whether to show hidden watchlists

dynamic

- Type: BOOLEAN
- Description: Whether to show dynamic watchlists

writeOnly

- Type: BOOLEAN
- Description: Whether to only show modifiable watchlists

indexedOnly

- Type: BOOLEAN
- Description: Whether to show indexed watchlists

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmWatchlist
- Description: The watchlists defined in the system

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/sysGetWatchlists?hidden=false&dynamic=false&writeOnly=false&indexedOnly=false

Example JSON Content:

```
{"filters": [{
    "name": "(name)",
    "id": 0
}]}
```

Back to Command List

sysRemoveWatchlist

Description

Remove watchlist/s from the system. This call is not supported for hidden watchlists, for example GTI.

Parameters

ids

- Type: EsmWatchlistIds
- Description: - list of watchlist ids to be deleted

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/sysRemoveWatchlist

Example JSON Content:

```
{"ids": {"watchlistIdList": ["(watchlistIdList)"]}}
```

Back to Command List

sysRemoveWatchlistValues

Description

Remove values from a watchlist. This call is not supported for hidden watchlists, for example GTI.

Parameters

watchlist

- Type: EsmWatchlistId
- Description: ID of the watchlist

values

- Type: List of STRING
- Description: List of string values to be removed from a watchlist

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/sysRemoveWatchlistValues

Example JSON Content:

```
{
    "watchlist": 0,
    "values": ["(values)"]
}
```

Back to Command List

userAddAccessGroup

Description

Add an access group

Parameters

accessGroup

- Type: EsmAccessGroupDetail
- Description: The new access group to add

authPW

- Type: EsmPassword
- Description: Password for Authorization of the current user

Return Value ("return" JSON root element is NOT returned)

- Type: EsmAccessGroupId
- Description: The ID of the new access group.

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userAddAccessGroup

Example JSON Content:

```
{
    "accessGroup": {
        "id": 0,
        "name": "(name)",
        "description": "(description)",
        "users": [0],
        "rights": [{"value": 0}],
        "devices": ["123456789000"],
        "policies": ["123456789000"],
        "zones": [0],
        "addresses": [{
            "type": "EsmCidr",
            "address": "(address)"
        }],
        "events": ["(value)"],
        "loginTimeEnabled": false,
        "loginStartTime": "(loginStartTime)",
        "loginEndTime": "(loginEndTime)",
        "loginDays": "(loginDays)",
        "loginTimeZone": {"value": 0},
        "limitedAccess": false
    },
    "authPW": {"value": "(value)"}
}
```

Back to Command List

userAddUser

Description

Add a user to the system.

Parameters

user

- Type: EsmUser
- Description: The user to add to the system

authPW

- Type: EsmPassword
- Description: Password for Authorization of the current user

Return Value ("return" JSON root element is NOT returned)

- Type: EsmUserId
- Description: The user id for the new user

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userAddUser

Example JSON Content:

```
{
    "user": {
        "username": "(username)",
        "id": 0,
        "locked": false,
        "loggedInCount": 0,
        "email": "(email)",
        "emailId": 0,
        "sms": "(sms)",
        "smsId": 0,
        "master": false,
        "admin": false,
        "alias": "(alias)",
        "type": "POWER",
        "groups": [0]
    },
    "authPW": {"value": "(value)"}
}
```

Back to Command List

userCaseList

Description

Get a filtered list of cases from the system

Parameters

statusId

- Type: UINT16
- Description: the status id to filter with.

from

- Type: STRING
- Description: the date to begin filtering. Accepted format is mm/dd/yyyy hh:mm:ss

to

- Type: STRING
- Description: the date to end filtering. Accepted format is mm/dd/yyyy hh:mm:ss

limit

- Type: UINT16
- Description: the number of records to retrieve. Use value 0 to retrieve all available records.

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmCase
- Description: list of cases from the system

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userCaseList?statusId=0&from=(from)&to=(to)&limit=0

Back to Command List

userDeleteAccessGroup

Description

Delete an access group.

Parameters

groupId

- Type: EsmAccessGroupId
- Description: id of access group to be deleted

authPW

- Type: EsmPassword
- Description: Password for Authorization of the current user

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userDeleteAccessGroup

Example JSON Content:

```
{
    "groupId": 0,
    "authPW": {"value": "(value)"}
}
```

Back to Command List

userDeleteUser

Description

Delete a user from the system.

Parameters

id

- Type: EsmUserId
- Description: The id for the user to be deleted

authPW

- Type: EsmPassword
- Description: Password for Authorization of the current user

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userDeleteUser

Example JSON Content:

```
{
    "id": 0,
    "authPW": {"value": "(value)"}
}
```

Back to Command List

userEditAccessGroup

Description

Edit properties of an access group.

Parameters

group

- Type: EsmAccessGroupDetail
- Description: details of group to be edited

authPW

- Type: EsmPassword
- Description: Password for Authorization of the current user

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userEditAccessGroup

Example JSON Content:

```
{
    "group": {
        "id": 0,
        "name": "(name)",
        "description": "(description)",
        "users": [0],
        "rights": [{"value": 0}],
        "devices": ["123456789000"],
        "policies": ["123456789000"],
        "zones": [0],
        "addresses": [{
            "type": "EsmCidr",
            "address": "(address)"
        }],
        "events": ["(value)"],
        "loginTimeEnabled": false,
        "loginStartTime": "(loginStartTime)",
        "loginEndTime": "(loginEndTime)",
        "loginDays": "(loginDays)",
        "loginTimeZone": {"value": 0},
        "limitedAccess": false
    },
    "authPW": {"value": "(value)"}
}
```

Back to Command List

userEditUser

Description

Used by the master user to update information about another user.

Parameters

user

- Type: EsmUser
- Description: THe user to edit on the system

authPW

- Type: EsmPassword
- Description: Password for Authorization of the current user

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userEditUser

Example JSON Content:

```
{
    "user": {
        "username": "(username)",
        "id": 0,
        "locked": false,
        "loggedInCount": 0,
        "email": "(email)",
        "emailId": 0,
        "sms": "(sms)",
        "smsId": 0,
        "master": false,
        "admin": false,
        "alias": "(alias)",
        "type": "POWER",
        "groups": [0]
    },
    "authPW": {"value": "(value)"}
}
```

Back to Command List

userGetAccessGroupDetail

Description

Get extended information about an access group.

Parameters

group

- Type: EsmAccessGroup
- Description: The group that represents the group details to be returned

authPW

- Type: EsmPassword
- Description: Password for Authorization of the current user

Return Value ("return" JSON root element is NOT returned)

- Type: EsmAccessGroupDetail
- Description: access group detailed information

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userGetAccessGroupDetail

Example JSON Content:

```
{
    "group": {
        "id": 0,
        "name": "(name)",
        "description": "(description)",
        "limited": false
    },
    "authPW": {"value": "(value)"}
}
```

Back to Command List

userGetAccessGroupList

Description

Get all user access groups defined in the system.

Parameters

restrictToUsersGroup

- Type: BOOLEAN
- Description: Whether to restrict the results to the logged in user's group

authPW

- Type: EsmPassword
- Description: Password for Authorization of the current user

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmAccessGroup
- Description: A list of all access groups defined in the system.

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userGetAccessGroupList?restrictToUsersGroup=false

Example JSON Content:

```
{"authPW": {"value": "(value)"}}
```

Back to Command List

userGetRightsList

Description

Get all rights defined in the system.

Parameters

includeFipsRights

- Type: BOOLEAN
- Description: Whether FIPS rights should be included in the list

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmRight
- Description: A list of all user rights defined in the system

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userGetRightsList?includeFipsRights=false

Back to Command List

userGetTimeZones

Description

Get a list of timezones this system recognizes

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmTimeZone
- Description: list of timezones recoginized by the system

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userGetTimeZones

Back to Command List

userGetUserList

Description

Get a list of all users.

Parameters

authPW

- Type: EsmPassword
- Description: Password for Authorization of the current user

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmUser
- Description: The list of users

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userGetUserList

Example JSON Content:

```
{"authPW": {"value": "(value)"}}
```

Back to Command List

userGetUserRights

Description

Get all rights defined for the current user.

Return Value ("return" JSON root element is NOT returned)

- Type: EsmUserRights
- Description: A list of all user rights defined for the current user

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/userGetUserRights

Back to Command List

zoneAddSubZone

Description

Add a new subzone under a zone

Parameters

parentZone

- Type: EsmZoneId
- Description: The id of the parent zone to which this sub zone belongs

newSubZone

- Type: EsmSubZoneInfo
- Description: The new subzone to add

Return Value ("return" JSON root element is NOT returned)

- Type: STRING
- Description: The id of the newly create subzone

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/zoneAddSubZone

Example JSON Content:

```
{
    "parentZone": 0,
    "newSubZone": {
        "id": 0,
        "name": "(name)",
        "description": "(description)",
        "ranges": [{
            "firstIp": "(firstIp)",
            "lastIp": "(lastIp)",
            "geoLoc": {
                "id": "123456789000",
                "name": "(name)"
            },
            "asnId": 123456789000
        }]
    }
}
```

Back to Command List

zoneAddZone

Description

Create a new zone.

Parameters

info

- Type: EsmZoneInfoIn
- Description: The info being created. The ID property will be ignored on this zone object passed in.
- Accepted Values:
  - EsmZoneInfo

Return Value ("return" JSON root element is NOT returned)

- Type: STRING
- Description: The id of the new zone that was created

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/zoneAddZone

Example JSON Content:

```
{"info": {
    "type": "EsmZoneInfo",
    "id": 0,
    "name": "(name)",
    "description": "(description)",
    "default": false,
    "geoLoc": {
        "id": "123456789000",
        "name": "(name)"
    },
    "asnId": 123456789000,
    "devices": ["123456789000"]
}}
```

Back to Command List

zoneDeleteSubZone

Description

Delete the sub zone

Parameters

id

- Type: EsmSubZoneId
- Description: The ID of the sub zone to delete

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/zoneDeleteSubZone

Example JSON Content:

```
{"id": 0}
```

Back to Command List

zoneDeleteZone

Description

Delete the zone

Parameters

id

- Type: EsmZoneId
- Description: The ID of the zone to delete

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/zoneDeleteZone

Example JSON Content:

```
{"id": 0}
```

Back to Command List

zoneEditSubZone

Description

Edit the given sub zone. Note that ID must be set to an existing sub zone for this to work properly. The ID value will be set if the zone was gotten from zoneGetSubZone().

Parameters

subZone

- Type: EsmSubZoneInfo
- Description: The new sub zone information along with its existing ID

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/zoneEditSubZone

Example JSON Content:

```
{"subZone": {
    "id": 0,
    "name": "(name)",
    "description": "(description)",
    "ranges": [{
        "firstIp": "(firstIp)",
        "lastIp": "(lastIp)",
        "geoLoc": {
            "id": "123456789000",
            "name": "(name)"
        },
        "asnId": 123456789000
    }]
}}
```

Back to Command List

zoneEditZone

Description

Edit the given zone. Note that ID must be set to an existing zone for this to work properly. The ID value will be set if the zone was gotten from zoneGetZone().

Parameters

zone

- Type: EsmZoneInfoIn
- Description: The new zone information along with its existing ID
- Accepted Values:
  - EsmZoneInfo

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/zoneEditZone

Example JSON Content:

```
{"zone": {
    "type": "EsmZoneInfo",
    "id": 0,
    "name": "(name)",
    "description": "(description)",
    "default": false,
    "geoLoc": {
        "id": "123456789000",
        "name": "(name)"
    },
    "asnId": 123456789000,
    "devices": ["123456789000"]
}}
```

Back to Command List

zoneGetSubZone

Description

Get detailed information on a sub zone

Parameters

id

- Type: EsmSubZoneId
- Description: The ID of the sub zone whose details are being requested

Return Value ("return" JSON root element is NOT returned)

- Type: EsmSubZoneInfo
- Description: The sub zone information

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/zoneGetSubZone

Example JSON Content:

```
{"id": 0}
```

Back to Command List

zoneGetZone

Description

Get extended detail on a zone.

Parameters

id

- Type: EsmZoneId
- Description: The zone ID whose extended info is needed

Return Value ("return" JSON root element is NOT returned)

- Type: EsmZoneInfoOut
- Description: The extended zone detail, given the zone ID

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/zoneGetZone

Example JSON Content:

```
{"id": 0}
```

Back to Command List

zoneGetZoneTree

Description

Get the full tree of zones defined in the ESM.

Return Value ("return" JSON root element is NOT returned)

- Type: List of EsmZone
- Description: The zone tree

Example REST Call (with JSON if applicable)

https://ESM_URL/rs/esm/v2/zoneGetZoneTree

Back to Command List

AddDatasourceClientResponse

Description

Add clients response

Properties

successfulClients

- Type: List of IpsId
- Description: ipsid for clients added

jobStatus

- Type: JobStatusValue
- Description: status of job
- Accepted Values:
  - READY
  - RUNNING
  - COMPLETE

Returned By

- dsAddDataSourceClientsStatus

Back to Command List

AddDatasourceResponse

Description

Holds information about added datasources

Properties

successfulDatasources

- Type: List of IpsId
- Description: list of datasource ipsid that were successfuly added

unsuccessfulDatasources

- Type: List of NameError
- Description: list of datasources that were not added

jobStatus

- Type: JobStatusValue
- Description: status of job
- Accepted Values:
  - READY
  - RUNNING
  - COMPLETE

Returned By

- dsAddDataSourcesStatus

Back to Command List

AssetDetailsObject

Description

AssetDetailsObject

Properties

hostName

- Type: STRING
- Description: hostName

lastTime

- Type: STRING
- Description: lastTime

ipAddress

- Type: STRING
- Description: ipAddress

mask

- Type: UINT8
- Description: mask

zoneId

- Type: UINT16
- Description: zoneId

mac

- Type: STRING
- Description: mac

ipsid

- Type: STRING
- Description: ipsid

priority

- Type: UINT8
- Description: priority

userSeverity

- Type: UINT8
- Description: userSeverity

calcSeverity

- Type: UINT8
- Description: calcSeverity

severity

- Type: UINT8
- Description: severity

useCalcSev

- Type: STRING
- Description: useCalcSev

guid

- Type: STRING
- Description: guid

os

- Type: STRING
- Description: os

osName

- Type: STRING
- Description: osName

riskDisabled

- Type: UINT8
- Description: riskDisabled

groups

- Type: List of AssetGroup
- Description: groups

tags

- Type: List of TagGroup
- Description: tags

Returned By

- assetGetAssetDetailsObject

Back to Command List

AssetGroup

Description

AssetGroup

Properties

id

- Type: EsmGroupID
- Description: id

name

- Type: STRING
- Description: name

Returned By

- assetGetAssetDetailsObject

Back to Command List

AssetId

Description

AssetId

Back to Command List

DataSourceClientAdd

Description

Details for a datsource client to be added

Back to Command List

DataSourceData

Description

Details for the requested datasource

Returned By

- dsGetDataSourceDetail

Back to Command List

DataSourceDataAdd

Description

Details for a datasource to be added

Properties

name

- Type: STRING
- Description: datasource name

ipAddress

- Type: STRING
- Description: datasource ipaddress

typeId

- Type: EsmDataSourceTypeId
- Description: datasource type

zoneId

- Type: UINT16
- Description: datasource zone id

enabled

- Type: BOOLEAN
- Description: is the datasource enabled

url

- Type: STRING
- Description: datasource url

parameters

- Type: List of EsmDataSourceParameter
- Description: datasource paramaters

Back to Command List

DatasourceDataEdit

Description

Details for a datasource to be edited

Properties

id

- Type: IpsId
- Description: ipsid of datasource

name

- Type: STRING
- Description: name of datasource

ipAddress

- Type: STRING
- Description: ip address of datasource

typeId

- Type: EsmDataSourceTypeId
- Description: type id

zoneId

- Type: UINT16
- Description: zone id

enabled

- Type: BOOLEAN
- Description: enable datasource

url

- Type: STRING
- Description: url of datasource

parameters

- Type: List of EsmDataSourceParameter
- Description: datasource paramaters

Back to Command List

EPOList

Description

An object returned from MiddleWare containing a list of ePo servers and their attibutes. It also contains a boolean of whether or not MVM was found.

Properties

ePOServers

- Type: List of EPOServer
- Description: The ePOServers for this user

foundIPs

- Type: STRING
- Description: The foundIPs for this user

foundMVM

- Type: BOOLEAN
- Description: The foundMVM for this user

Returned By

- dsGetEpoList

Back to Command List

EPOListRequest

Description

A request object for the getEPOList API

Properties

targetIPs

- Type: STRING
- Description: The targetIPs for this user

Back to Command List

EPOServer

Description

Contains the attributes of a representation of an ePO server

Properties

receiverName

- Type: STRING
- Description: The receiverName for this user

ePOName

- Type: STRING
- Description: The ePOName for this user

ePOIPAddr

- Type: STRING
- Description: The ePOIPAddr for this user

ePOPort

- Type: STRING
- Description: The ePOPort for this user

Returned By

- dsGetEpoList

Back to Command List

EsmAccessGroup

Description

Users belong to access groups, which contain various information about what a user has access to.

Properties

id

- Type: EsmAccessGroupId
- Description: The access group's ID

name

- Type: STRING
- Description: The name of the access group

description

- Type: STRING
- Description: The description of the access group

limited

- Type: BOOLEAN
- Description: Whether this group has limited access on the system

Returned By

- userGetAccessGroupList

Back to Command List

EsmAccessGroupDetail

Description

Extended detail on an access group

Properties

id

- Type: EsmAccessGroupId
- Description: The id of this access group

name

- Type: STRING
- Description: The name of this access group

description

- Type: STRING
- Description: The description of this access group

users

- Type: List of EsmUserId
- Description: Userids that belong to this group

rights

- Type: List of EsmRightId
- Description: The rights given to members of this group

devices

- Type: List of EsmDeviceId
- Description: The devices that apply to this group

policies

- Type: List of EsmPolicyId
- Description: The policies associated with this access group

zones

- Type: List of EsmZoneId
- Description: The zones accessible to this access group

addresses

- Type: List of EsmNetworkAddress
- Description: The network addresses visible to this access group

events

- Type: List of EsmEventId
- Description: The events associated with this access group

loginTimeEnabled

- Type: BOOLEAN
- Description: Whether the Login Time Rescription has been enabled for this user group

loginStartTime

- Type: STRING
- Description: The start time when this user group can login

loginEndTime

- Type: STRING
- Description: The end time when this user group can no longer login

loginDays

- Type: STRING
- Description: The days the time restriction on this group applys. Format is string of T/F, one per day of the week starting with Sunday.

loginTimeZone

- Type: EsmTimeZoneId
- Description: The time zone the time restriction will be displayed in

limitedAccess

- Type: BOOLEAN
- Description: Whether this user group has limited access

Returned By

- userGetAccessGroupDetail

Back to Command List

EsmAccessGroupId

Description

An ID for an access group

Properties

value

- Type: UINT32
- Description: The raw 32 bit value for this access group id object

Returned By

- userAddAccessGroup
- userGetAccessGroupDetail
- userGetAccessGroupList
- userGetUserList

Back to Command List

EsmAlarmId

Description

An id for an alarm.

Properties

value

- Type: UINT32
- Description: The numeric ID value, 32 bit unsigned

Returned By

- alarmGetTriggeredAlarms
- notifyGetTriggeredNotificationDetail

Back to Command List

EsmAlarmIds

Description

/** Alarm ID list wrapper

Properties

alarmIdList

- Type: List of STRING
- Description: Getter for alarmIdList

Back to Command List

EsmAlertData

Description

Basic information on a datasource.

Properties

destIp

- Type: STRING
- Description: The destination ip of the alert

destMac

- Type: STRING
- Description: The destination mac of the alert

destPort

- Type: STRING
- Description: The destination port of the alert

eventCount

- Type: UINT32
- Description: The event count for the alert

firstTime

- Type: STRING
- Description: The first time for the alert

flowSessionId

- Type: UINT8
- Description: The first time for the alert

ipsId

- Type: EsmDeviceId
- Description: The ipsid for the alert

lastTime

- Type: STRING
- Description: The last time for the alert

note

- Type: STRING
- Description: The note for the alert

protocol

- Type: STRING
- Description: The protocol for the alert

reviewed

- Type: STRING
- Description: Whether the alert was reviewed

srcIp

- Type: STRING
- Description: The source ip for the alert

srcMac

- Type: STRING
- Description: The source mac for the alert

srcPort

- Type: STRING
- Description: The source port for the alert

subtype

- Type: STRING
- Description: The subtype for the alert

vLAN

- Type: UINT32
- Description: The vlan for the alert

sigId

- Type: STRING
- Description: The signature id for the alert

sigDesc

- Type: STRING
- Description: The signature description for the alert

sigText

- Type: STRING
- Description: The signature text for the alert

ruleName

- Type: STRING
- Description: The rule name for the alert

duration

- Type: STRING
- Description: The duration for the alert

deviceName

- Type: STRING
- Description: The device name for the alert

severity

- Type: UINT32
- Description: The severity for the alert

normId

- Type: UINT32
- Description: The normalization id for the alert

app

- Type: STRING
- Description: The app for the alert

host

- Type: STRING
- Description: The host for the alert

domain

- Type: STRING
- Description: The domain for the alert

srcUser

- Type: STRING
- Description: The user source for the alert

destUser

- Type: STRING
- Description: The user destination for the alert

remedyCaseId

- Type: UINT64
- Description: The remedy case id for the alert

remedyTicketTime

- Type: STRING
- Description: The remote open ticket time for the alert

deviceTime

- Type: STRING
- Description: The remote open ticket time for the alert

remedyAnalyst

- Type: STRING
- Description: The remote user for the alert

command

- Type: STRING
- Description: The command for the alert

object

- Type: STRING
- Description: The object for the alert

sequence

- Type: UINT32
- Description: The sequence for the alert

trusted

- Type: UINT32
- Description: Trusted for the alert

sessionId

- Type: UINT64
- Description: The session id for the alert

asnGeoSrcId

- Type: STRING
- Description: The geo source id for the alert

srcAsnGeo

- Type: STRING
- Description: The geo source message for the alert

asnGeoDestId

- Type: STRING
- Description: The geo destination id for the alert

destAsnGeo

- Type: STRING
- Description: The geo destination message for the alert

normMessage

- Type: STRING
- Description: The normalization message for the alert

normDesc

- Type: STRING
- Description: The normalization description for the alert

archiveId

- Type: STRING
- Description: The archive id for the alert

srcZone

- Type: STRING
- Description: The zone source for the alert

destZone

- Type: STRING
- Description: The zone destination for the alert

flowId

- Type: UINT64
- Description: The flow id for the alert

alertId

- Type: UINT64
- Description: The alert id for the alert

srcGuid

- Type: STRING
- Description: The guid source for the alert

destGuid

- Type: STRING
- Description: The guid destination for the alert

agg1Name

- Type: STRING
- Description: The agg 1 name for the alert

agg1Value

- Type: STRING
- Description: The agg 1 value for the alert

agg2Name

- Type: STRING
- Description: The agg 2 name for the alert

agg2Value

- Type: STRING

- Description: The agg 2 value for the alert

agg3Name

- Type: STRING
- Description: The agg 3 name for the alert

agg3Value

- Type: STRING
- Description: The agg 3 value for the alert

iocName

- Type: STRING
- Description: The ioc name for the alert

iocId

- Type: UINT32
- Description: The ioc id for the alert

cases

- Type: List of EsmCase
- Description: The ioc id for the alert

customTypes

- Type: List of EsmCustomType
- Description: The Custom Type Data

Returned By

- ipsGetAlertData

Back to Command List

EsmAlertId

Description

The ID of a alert defined in the ESM.

Properties

value

- Type: STRING
- Description: The numeric 64 bit unsigned ID for this alert

Back to Command List

EsmBasicValue

Description

A value for any field that has a single type.

Properties

value

- Type: STRING
- Description: A single filter value for a field

Back to Command List

EsmBoolean

Description

boolean values true/false for use with external API

Back to Command List

EsmBuildStamp

Description

EsmBuildStamp

Properties

buildStamp

- Type: STRING
- Description: The ESM buildstamp

Returned By

- essmgtGetBuildStamp

Back to Command List

EsmCase

Description

Basic information for a case

Properties

summary

- Type: STRING
- Description: The summary (name) of the case

id

- Type: EsmCaseId
- Description: The id of the case

statusId

- Type: EsmCaseStatusId
- Description: The status of the case

severity

- Type: UINT8
- Description: The severity of the case

openTime

- Type: STRING
- Description: The time the case was opened

Returned By

- caseGetCaseList
- ipsGetAlertData
- userCaseList

Back to Command List

EsmCaseDetail

Description

Detail information for a specific Case

Properties

summary

- Type: STRING
- Description: The summary (name) of the case

id

- Type: EsmCaseId
- Description: The id of the case

statusId

- Type: EsmCaseStatusId
- Description: The status of the case

severity

- Type: UINT8
- Description: The severity of the case

openTime

- Type: STRING
- Description: The time the case was opened

assignedTo

- Type: UINT32
- Description: Unsigned 32 bit ID describing who the case is assigned to

orgId

- Type: UINT16
- Description: Unsigned 16 bit value representing the organization assigned this case

closeTime

- Type: STRING
- Description: The close time for this case

eventList

- Type: List of EsmCaseEvent
- Description: The list (comma separated) of event ids tied to this case

deviceList

- Type: List of EsmDeviceId
- Description: The list (comma separated) of devices tied to this case

dataSourceList

- Type: List of EsmDataSourceId
- Description: The list (comma separated) of datasources tied to this case

notes

- Type: STRING
- Description: Notes associated with this case

`noteAdded`

- Type: STRING
- Description: Note added associated with this case

`history`

- Type: STRING
- Description: History associated with this case

Back to Command List

EsmCaseDetailExternal

Description

Detail information for a specific case

Properties

id

- Type: EsmCaseId
- Description: case id

summary

- Type: STRING
- Description: The summary (name) of the case

assignedTo

- Type: UINT32
- Description: ID describing who the case is assigned to

severity

- Type: UINT8
- Description: The severity of the case

orgId

- Type: UINT16
- Description: ID representing the organization assigned this case - see API caseGetOrganizationList for more detail

statusId

- Type: UINT32
- Description: The status of the case - see API caseGetCaseStatusList for more details

openTime

- Type: STRING
- Description: The time the case was opened

closeTime

- Type: STRING
- Description: The close time for this case

deviceList

- Type: List of EsmDeviceId
- Description: List of devices tied to this case

dataSourceList

- Type: List of EsmDataSourceId
- Description: List of datasources tied to this case

eventList

- Type: List of EsmCaseEvent
- Description: List of event ids tied to this case

notes

- Type: STRING
- Description: Notes associated with this case

history

- Type: STRING
- Description: History associated with this cases

Returned By

- caseGetCaseDetail

Back to Command List

EsmCaseEvent

Description

Case event details

Properties

id

- Type: EsmEventId
- Description: The event id tied to this case

message

- Type: STRING
- Description: The message of the event

lastTime

- Type: STRING
- Description: The time of the event

Returned By

- caseGetCaseDetail
- caseGetCaseEventsDetail

Back to Command List

EsmCaseId

Description

Unique identifier for a case in the system

Properties

value

- Type: UINT32
- Description: Unsigned 32 bit ID

Returned By

- caseAddCase
- caseGetCaseDetail
- caseGetCaseList
- ipsGetAlertData
- userCaseList

Back to Command List

EsmCaseOrganization

Description

Case Organization representation

Properties

name

- Type: STRING
- Description: The name of the case status

id

- Type: UINT16
- Description: The id of the case status

Returned By

- caseGetOrganizationList

Back to Command List

EsmCaseStatus

Description

A valid Case Status

Properties

name

- Type: STRING
- Description: The name of the case status

id

- Type: UINT16
- Description: The id of the case status

default

- Type: BOOLEAN
- Description: Whether the status is default or not

showInCasePane

- Type: BOOLEAN
- Description: The task for this user

Returned By

- caseGetCaseStatusList

Back to Command List

EsmCaseStatusId

Description

Unique identifier for a case status in the system

Properties

value

- Type: UINT32
- Description: Unsigned 16 bit ID

Returned By

- caseAddCaseStatus
- caseGetCaseList
- ipsGetAlertData
- userCaseList

Back to Command List

EsmCaseUser

Description

Esm Case User

Properties

name

- Type: STRING
- Description: The name of the case user

id

- Type: UINT32
- Description: The id of the case user

Returned By

- caseGetCaseUsers

Back to Command List

EsmCaseUserList

Description

This class holds a list of ESM user groups along with Email information of the user that is querying this information.

Properties

caseUserList

- Type: List of EsmCaseUser
- Description: List<EsmCaseUser>

emailServerConfigured

- Type: BOOLEAN
- Description: Email Server Configured (T/F)

usersEmailAddress

- Type: STRING
- Description: Current users Email Address

Returned By

- caseGetCaseUsers

Back to Command List

EsmCidr

Description

A CIDR used in the ESM

Properties

address

- Type: STRING
- Description: The ip address string

prefix

- Type: UINT16
- Description: The prefix for this CIDR; the number of static bits

Back to Command List

EsmCompoundValue

Description

A filter value for a field with multiple subtypes. Only custom fields can have multiple subtypes.

Properties

values

- Type: List of STRING
- Description: The filter values for the multiple subtypes on a field - can be less than the number of subtypes but not more. If less, then fields are filled with values from the first subtype to the last, in order, until we run out of values.

Back to Command List

EsmCustomType

Description

This is used to hold the custom types from the ESM data

Properties

fieldId

- Type: UINT32
- Description: The Field id

fieldName

- Type: STRING
- Description: The Field name

definedFieldNumber

- Type: UINT8
- Description: The Defined field number

formatedValue

- Type: STRING
- Description: the Formatted value

unformattedValue

- Type: STRING
- Description: The unformatted Value

Returned By

- ipsGetAlertData

Back to Command List

EsmDataSource

Description

Basic information on a datasource.

Properties

name

- Type: STRING
- Description: The name of the datasource

id

- Type: EsmDataSourceId
- Description: The id of the datasource

typeId

- Type: EsmDataSourceTypeId
- Description: The datasource type

typeName

- Type: STRING
- Description: The datasource type name

parsing

- Type: BOOLEAN
- Description: Whether this datasource is set for parsing or not

inSync

- Type: BOOLEAN
- Description: Whether this datasource is in sync

elmLogging

- Type: STRING
- Description: Elm logging settings for this datasource

elsLogging

- Type: STRING
- Description: Els logging settings for this datasource

Returned By

- dsGetDataSourceList

Back to Command List

EsmDataSourceClient

Description

Basic information on a datasource client

Properties

id

- Type: UINT64
- Description: The ID of the client or parent

name

- Type: STRING
- Description: The name of the client

enabled

- Type: BOOLEAN
- Description: Whether the client is enabled or not

ipAddress

- Type: STRING
- Description: The ipaddress of the client

host

- Type: STRING
- Description: The hostname for the client

type

- Type: STRING
- Description: 0 matches parent. If type is different than parent see dsGetDataSourceTypes

timezone

- Type: STRING
- Description: The timezone designation for this client: see userGetTimeZones API for values

dateOrder

- Type: STRING
- Description: The date order for this client

port

- Type: STRING
- Description: The port for the client

useTls

- Type: BOOLEAN
- Description: Should the client use tls

Returned By

- dsGetDataSourceClients

Back to Command List

EsmDataSourceId

Description

The ID of a datasource defined in the ESM.

Properties

id

- Type: STRING
- Description: Unsigned 16 bit ID

Returned By

- caseGetCaseDetail
- dsGetDataSourceList
- grpGetDeviceTree
- grpGetDeviceTreeEx

Back to Command List

EsmDataSourceModel

Description

Basic information on a datasource model/type defined in the ESM.

Properties

id

- Type: EsmDataSourceTypeId
- Description: The id of the datasource model/type

name

- Type: STRING
- Description: The datasource model name

protocol

- Type: STRING
- Description: The datasource thirdparty type protocol

flags

- Type: UINT32
- Description: The internal flags for this datsource model

parser

- Type: STRING
- Description: Parser for this datasource

collector

- Type: STRING
- Description: Collector for this datasource

extraParams

- Type: STRING
- Description: ExtraParams for this datasource

Returned By

- dsGetDataSourceTypes

Back to Command List

EsmDataSourceParameter

Description

Represents a key/value parameter for a datasource definition

Properties

key

- Type: STRING
- Description: Key for this datasource parameter

value

- Type: STRING
- Description: Value for this datasource parametere

Back to Command List

EsmDataSourceType

Description

Basic information on a datasource type defined in the ESM.

Properties

idmId

- Type: UINT64
- Description: ID for the autoritative identiy manager

vendors

- Type: List of EsmDataSourceVendor
- Description: The vendors of datasources found in the system

Returned By

- dsGetDataSourceTypes

Back to Command List

EsmDataSourceTypeId

Description

The Type ID describing a datasource type that is defined in the ESM.

Properties

id

- Type: UINT16
- Description: Unsigned 16 bit ID

Returned By

- dsGetDataSourceList
- dsGetDataSourceTypes

Back to Command List

EsmDataSourceVendor

Description

Basic information on a datasource vendor defined in the ESM.

Properties

name

- Type: STRING
- Description: The name of the vendor of this datasource

models

- Type: List of EsmDataSourceModel
- Description: The list of models associated with this vendor

Returned By

- dsGetDataSourceTypes

Back to Command List

EsmDevice

Description

A device defined in the system.

Properties

name

- Type: STRING
- Description: The name of the device

type

- Type: EsmDeviceType
- Description: The device type information for this device
- Accepted Values:
  - IPS
  - POLICY
  - RECEIVER
  - THIRD_PARTY
  - DBM
  - DBM_DB
  - DBM_AGENT
  - VA
  - IPSVIPS
  - ESM
  - APM
  - APMVIPS
  - ELM
  - ELMREC
  - LOCALESM
  - RISK
  - ASSET
  - RISKMANAGER
  - RISKAGENT
  - EPO
  - EPO_APP
  - NSM
  - NSM_SENSOR
  - NSM_INTERFACE
  - MVM
  - SEARCH_ELASTIC
  - KID_CLUSTER
  - KID_NODE
  - SYSTEM
  - BUCKET
  - UNKNOWN

id

- Type: EsmDeviceId
- Description: The id of the device

Returned By

- devGetDeviceList

Back to Command List

EsmDeviceId

Description

The ID of a device defined in the ESM.

Properties

id

- Type: UINT64
- Description: Unsigned 16 bit ID

Returned By

- caseGetCaseDetail
- devGetDeviceList
- ipsGetAlertData
- userGetAccessGroupDetail

Back to Command List

EsmDeviceTreeEx

Description

Defines all response information related to a device list request using the API.

Properties

displayName

- Type: STRING
- Description: The name of the device tree

ACnt

- Type: UINT16
- Description: The alert count

afSet

- Type: STRING
- Description: Whether the alert flag is set

FCnt

- Type: UINT16
- Description: The number of flows

FFSet

- Type: STRING
- Description: Whether the flow flag is set

LCnt

- Type: UINT16
- Description: Number of logs

lfSet

- Type: STRING
- Description: Whether the log flag is set

esmFlags

- Type: UINT32
- Description: Internal use flags

devices

- Type: List of EsmTreeNodeEx
- Description: The devices in the tree

Returned By

- grpGetDeviceTreeEx

Back to Command List

EsmDeviceType

Description

All supported device types in the system

Accepted Values

- IPS
- POLICY
- RECEIVER
- THIRD_PARTY
- DBM
- DBM_DB
- DBM_AGENT
- VA
- IPSVIPS
- ESM
- APM
- APMVIPS
- ELM
- ELMREC
- LOCALESM
- RISK
- ASSET
- RISKMANAGER
- RISKAGENT
- EPO
- EPO_APP
- NSM
- NSM_SENSOR
- NSM_INTERFACE
- MVM
- SEARCH_ELASTIC
- KID_CLUSTER
- KID_NODE
- SYSTEM
- BUCKET
- UNKNOWN

Back to Command List

EsmEmailId

Description

An ID for an email in the ESM.

Properties

value

- Type: UINT32
- Description: The raw 32 bit id for this email ID object

Returned By

- userGetUserList

Back to Command List

EsmEventId

Description

An ID for an event in the ESM.

Properties

value

- Type: STRING
- Description: The id for this event ID object

Returned By

- caseGetCaseDetail
- caseGetCaseEventsDetail
- userGetAccessGroupDetail

Back to Command List

EsmField

Description

A field that can be used to create a filter when querying for data in the ESM.

Properties

name

- Type: STRING
- Description: The name of the field

types

- **Read only**
- Type: List of EsmFieldType
- Description: The field type for this filter field. Most fields only have one type, but some custom fields can have multiple subtypes. In this case, multiple values need to be set for the field.

Back to Command List

EsmFieldFilter

Description

A filter on a specific field

Properties

field

- Type: EsmField
- Description: The field this filter applies to

operator

- Type: EsmFilterOperator
- Description: The operator for this filter, defaults to IN
- Accepted Values:
  - IN
  - NOT_IN
  - GREATER_THAN
  - LESS_THAN
  - GREATER_OR_EQUALS_THAN
  - LESS_OR_EQUALS_THAN
  - NUMERIC_EQUALS
  - NUMERIC_NOT_EQUALS
  - DOES_NOT_EQUAL
  - EQUALS
  - CONTAINS
  - DOES_NOT_CONTAIN
  - REGEX

values

- Type: List of EsmFilterValue
- Description: One or more values for the filter

Back to Command List

EsmFieldType

Description

Indicated what type of data is stored in a given field

Accepted Values

- BOOLEAN
- STRING
- CUSTOM
- INT2
- INT4
- INT8
- INT32
- INT64
- UINT8
- UINT16
- UINT32
- UINT64
- IPV4
- FLOAT
- SIGID
- SSTRING
- IPTYPE
- IP
- GUID
- MAC_ADDRESS
- LONG_CUSTOM
- HSTRING
- STRLIT
- AGG
- TIME4
- TIME8

Back to Command List

EsmFileData

Description

Data from a file read on the server.

Properties

fileSize

- Type: UINT32
- Description: The size of the file in bytes

bytesRead

- Type: UINT32
- Description: The number of bytes read from the file

data

- Type: STRING
- Description: The text data read from the file

Returned By

- sysGetWatchlistValues

Back to Command List

EsmFileToken

Description

Created by sherd on 9/30/16.

Properties

fileToken

- Type: STRING
- Description: The fileToken for this user

Returned By

- sysGetWatchlistDetails

Back to Command List

EsmFilter

Description

A base for all filter types in the querying interface. Due to restrictions in how inheritance works in XML schema, there is currently no common functionality across all filter objects.

Properties

type

- Type: TYPE
- Description: Must be set to one of the accepted type string values. Note the properties for the type must appear alongside this property.
- Accepted Values:
  - EsmFieldFilter
  - EsmFilterGroup

Back to Command List

EsmFilterField

Description

Fields used in filtering

Properties

name

- Type: STRING
- Description: The name of the field

types

- **Read only**
- Type: List of EsmFieldType
- Description: The field type for this filter field. Most fields only have one type, but some custom fields can have multiple subtypes. In this case, multiple values need to be set for the field.

Returned By

- qryGetFilterFields

Back to Command List

EsmFilterGroup

Description

A group of other filters, always ANDed together

Properties

filters

- Type: List of EsmFilter
- Description: The filters in this group

logic

- Type: EsmFilterGroupLogic
- Description: What type of logic to apply to the group (AND, OR, etc)
- Accepted Values:
  - AND
  - OR

Back to Command List

EsmFilterGroupLogic

Description

Defines the available types of filter group logic

Accepted Values

- AND
- OR

Back to Command List

EsmFilterOperator

Description

Defines all possible operators used in field filters.

Accepted Values

- IN
- NOT_IN
- GREATER_THAN
- LESS_THAN
- GREATER_OR_EQUALS_THAN
- LESS_OR_EQUALS_THAN
- NUMERIC_EQUALS
- NUMERIC_NOT_EQUALS
- DOES_NOT_EQUAL
- EQUALS
- CONTAINS
- DOES_NOT_CONTAIN
- REGEX

Back to Command List

EsmFilterValue

Description

Base type for filter values passed into a query

Properties

type

- Type: TYPE
- Description: Must be set to one of the accepted type string values. Note the properties for the type must appear alongside this property.
- Accepted Values:
  - EsmWatchlistValue
  - EsmVariableValue
  - EsmBasicValue
  - EsmCompoundValue

Back to Command List

EsmGeoLoc

Description

A geo location defined in the ESM.

Properties

id

- Type: EsmGeoLocId
- Description: The ID of this geo location

name

- Type: STRING
- Description: The readable name of the geo location

Returned By

- geoGetGeoLocRegionList
- geoGetGeoLocs
- zoneGetSubZone
- zoneGetZone

Back to Command List

EsmGeoLocId

Description

A geographic location ID, commonly just referred to as a geo.

Properties

value

- Type: UINT64
- Description: The unsigned 64 bit ID for this geo location

Returned By

- geoGetGeoLocRegionList
- geoGetGeoLocs
- zoneGetSubZone
- zoneGetZone

Back to Command List

EsmGroupID

Description

A group id

Properties

iD

- Type: UINT32
- Description: The id of the group

Returned By

- assetGetAssetDetailsObject

Back to Command List

EsmGroupedQueryConfig

Description

When a query is executed, various settings can change what is returned in the results. This object stores all customizations for a query.

Properties

filters

- Type: List of EsmFilter
- Description: Query filters can be considered similar to WHERE clauses in SQL. If none are specified, no filters will be applied to the query.

field

- Type: EsmField
- Description: The field that will be selected when this query is executed.

timeRange

- Type: EsmTimeRange
- Description: If set, the results will be limited to the time specified by this time filter.
- Accepted Values:
  - CUSTOM
  - LAST_MINUTE
  - LAST_10_MINUTES
  - LAST_30_MINUTES
  - LAST_HOUR
  - CURRENT_DAY
  - PREVIOUS_DAY
  - LAST_24_HOURS
  - LAST_2_DAYS
  - LAST_3_DAYS
  - CURRENT_WEEK
  - PREVIOUS_WEEK
  - CURRENT_MONTH
  - PREVIOUS_MONTH
  - CURRENT_QUARTER
  - PREVIOUS_QUARTER
  - CURRENT_YEAR
  - PREVIOUS_YEAR

customStart

- Type: DATETIME
- Description: The custom start time for the query, if the timeRange property is set to CUSTOM

customEnd

- Type: DATETIME
- Description: The custom end time for the query, if the timeRange property is set to CUSTOM

Back to Command List

EsmGroupedQueryType

Description

Query Type

Accepted Values

- EVENT
- FLOW

Back to Command List

EsmJobId

Description

An ID for a job in the ESM.

Properties

value

- Type: UINT32
- Description: Unsigned 32 bit ID

Returned By

- dsAddDataSourceClients
- dsAddDataSources
- dsDeleteDataSourceClients
- dsEditDataSource
- dsEditDataSourceClient
- dsWriteThirdpartyConfig
- plcyRollPolicy

Back to Command List

EsmJobStatus

Description

The Status of the job

Properties

jobId

- Type: UINT32
- Description: The jobId for this user

jobErrorCode

- Type: UINT8
- Description: The jobErrorCode for this user

jobStatus

- Type: JobStatusValue
- Description: The jobStatus for this user
- Accepted Values:
  - READY
  - RUNNING
  - COMPLETE

response

- Type: STRING
- Description: The response for this user

action

- Type: UINT32
- Description: The action for this user

Returned By

- miscJobStatus

Back to Command List

EsmNetworkAddress

Description

An IP address in the ESM.

Properties

type

- Type: TYPE
- Description: Must be set to one of the accepted type string values. Note the properties for the type must appear alongside this property.
- Accepted Values:
  - EsmCidr

address

- Type: STRING
- Description: The ip address string

Returned By

- userGetAccessGroupDetail

Back to Command List

EsmOrganizationId

Description

Created by sherd on 9/16/16.

Properties

value

- Type: UINT32
- Description: Unsigned 16 bit ID

Returned By

- caseAddOrganization

Back to Command List

EsmPassword

Description

An ID for an event in the ESM.

Properties

value

- Type: STRING
- Description: The raw 32 bit id for this event ID object

Back to Command List

EsmPolicy

Description

Represents a policy: some type of configuration data that tells the system how to handle incoming events - often referred to as a "rule". (TODO: determine if the above description is accurate/complete)

Properties

deviceName

- Type: STRING
- Description: Name of the device this policy applies to

id

- Type: EsmPolicyId
- Description: The id of this policy

parentId

- Type: EsmPolicyId
- Description: Parent policy id

policyType

- Type: EsmPolicyType
- Description: Type of policy
- Accepted Values:
  - DEVICE
  - POLICY

deviceType

- Type: EsmDeviceType
- Description: Type of device this policy applies to
- Accepted Values:
  - IPS
  - POLICY
  - RECEIVER
  - THIRD_PARTY
  - DBM
  - DBM_DB
  - DBM_AGENT
  - VA
  - IPSVIPS
  - ESM
  - APM
  - APMVIPS
  - ELM
  - ELMREC
  - LOCALESM
  - RISK
  - ASSET
  - RISKMANAGER
  - RISKAGENT
  - EPO
  - EPO_APP
  - NSM
  - NSM_SENSOR
  - NSM_INTERFACE
  - MVM
  - SEARCH_ELASTIC
  - KID_CLUSTER
  - KID_NODE
  - SYSTEM
  - BUCKET
  - UNKNOWN

vipsEnabled

- Type: BOOLEAN
- Description: Whether VIPS is enabled

policyRight

- Type: BOOLEAN
- Description: Whether the policy requires policy rights (??) TODO: is this right?

addDeleteRight

- Type: BOOLEAN
- Description: TODO: is this the right to add/delete rights to this policy or whether the user has add/delete rights for this policy?

customRuleRight

- Type: BOOLEAN
- Description: TODO: what is this?

synced

- Type: BOOLEAN
- Description: Whether this policy is synced to the device

stagedTime

- Type: STRING
- Description: The time this policy was synced to the device TODO: is this right?

applyRulesAllowed

- Type: BOOLEAN
- Description: Whether the user can apply this policy TODO: is this right?

rollbackAllowed

- Type: BOOLEAN
- Description: Whether the user can rollback this policy TODO: is this right?

dataSourceProtocol

- Type: STRING
- Description: The protocol associated with this policy's data source

dataSourceParser

- Type: STRING
- Description: The parser associated with this policy's data source

hierarchicalName

- Type: STRING
- Description: The hierarchical name of this policy

parentVersion

- Type: UINT32
- Description: The parent's version TODO: more information here?

thirdPartyType

- Type: UINT16
- Description: The third party type ID associated with this policy TODO: more information here?

Returned By

- plcyGetPolicyList

Back to Command List

EsmPolicyId

Description

The ID for a single policy in the system. This is a unique ID across all policies.

Properties

value

- Type: UINT64
- Description: The raw numeric ID for the policy

Returned By

- plcyGetPolicyList
- userGetAccessGroupDetail

Back to Command List

EsmPolicyType

Description

The types of policies defined in the system

Accepted Values

- DEVICE
- POLICY

Back to Command List

EsmPrivileges

Description

Created by blongmor on 4/9/2015.

Properties

master

- Type: BOOLEAN
- Description: whether the user is the master user.

admin

- Type: BOOLEAN
- Description: whether the user is an Admin user.

power

- Type: BOOLEAN
- Description: whether the user is an admin user.

audit

- Type: BOOLEAN
- Description: whether the user is an audit user.

crypto

- Type: BOOLEAN
- Description: whether the user is an crypto user.

systemSettings

- Type: Privilege
- Description: whether the user can read and write system settings.

dashboards

- Type: Privilege
- Description: whether the user can read and write dashboards

policyConfig

- Type: Privilege
- Description: whether the user can read and write policy configurations.

eventManagement

- Type: Privilege
- Description: whether the user can read and write event management

deviceCreation

- Type: Privilege
- Description: whether the user can read and write device Creation

customRules

- Type: Privilege
- Description: whether the user can read and write custom rules

reports

- Type: Privilege
- Description: whether the user can read and write reports

systemSecuritySettings

- Type: Privilege
- Description: whether the user can read and write system security settings

networkDiscovery

- Type: Privilege
- Description: whether the user can read and write network discovery

networkPortControl

- Type: Privilege
- Description: whether the user can read and write network port control

fipsTest

- Type: Privilege
- Description: whether the user can read and write fips test.

userManagement

- Type: Privilege
- Description: whether the user can read and write user management

cases

- Type: Privilege
- Description: whether the user can read and write cases

assets

- Type: Privilege
- Description: whether the user can read and write assets

zones

- Type: Privilege
- Description: whether the user can read and write zones

eventForwarding

- Type: Privilege
- Description: whether the user can read and write event forwarding

globalBlacklisting

- Type: Privilege
- Description: whether the user can read and write global blacklisting

alarms

- Type: Privilege
- Description: whether the user can read and write alarms

cyberThreatDetails

- Type: Privilege
- Description: whether the user can read and write cyber threat details

watchlists

- Type: Privilege
- Description: whether the user can read and write cyber threat details

elmSftp

- Type: Privilege
- Description: whether the user can read and write cyber threat details

elmStorage

- Type: Privilege
- Description: whether the user can read and write cyber threat details

`ipsManagement`

- Type: Privilege
- Description: whether the user can read and write ips

`deviceAction`

- Type: BOOLEAN
- Description: whether the user can perform device action

Returned By

- userGetUserRights

Back to Command List

EsmQueryColumn

Description

A field in a query result

Properties

name

- Type: STRING
- Description: The field name

Returned By

- qryGetResults

Back to Command List

EsmQueryColumnInfo

Description

Details which column indexes have special meaning.

Properties

countColumn

- Type: UINT16
- Description: The column containing the count in a grouped query

labelColumn

- Type: UINT16
- Description: The column containing text labels

attributeColumn

- Type: UINT16
- Description: The column containing an attribute if applicable

drilldownColumn

- Type: UINT16
- Description: The drilldown column for the query if applicable

Back to Command List

EsmQueryConfig

Description

When a query is executed, various settings can change what is returned in the results. This object stores all customizations for a query.

Properties

timeRange

- Type: EsmTimeRange
- Description: If set, the results will be limited to the time specified by this time filter.
- Accepted Values:
  - CUSTOM
  - LAST_MINUTE
  - LAST_10_MINUTES
  - LAST_30_MINUTES
  - LAST_HOUR
  - CURRENT_DAY
  - PREVIOUS_DAY
  - LAST_24_HOURS
  - LAST_2_DAYS
  - LAST_3_DAYS
  - CURRENT_WEEK
  - PREVIOUS_WEEK
  - CURRENT_MONTH
  - PREVIOUS_MONTH
  - CURRENT_QUARTER
  - PREVIOUS_QUARTER
  - CURRENT_YEAR
  - PREVIOUS_YEAR

customStart

- Type: DATETIME
- Description: The custom start time for the query, if the timeRange property is set to CUSTOM

customEnd

- Type: DATETIME
- Description: The custom end time for the query, if the timeRange property is set to CUSTOM

order

- Type: List of EsmRowOrder
- Description: Query results can be sorted on a column, either ascending or descending. This can be left empty.

includeTotal

- Type: BOOLEAN
- Description: Whether to include total sum for query

locked

- **Read only**
- Type: BOOLEAN
- Description: Whether this query config is currently locked

userLocked

- **Read only**
- Type: STRING
- Description: If locked, the username that has locked the query

fields

- Type: List of EsmSelectField
- Description: The fields that will be selected when this query is executed.

filters

- Type: List of EsmFilter
- Description: Query filters can be considered similar to WHERE clauses in SQL. If none are specified, no filters will be applied to the query.

`limit`

- Type: UINT16
- Description: Query results can be limited to a maximum row count. The default value is 0. If this value is left, no limit will be placed on the resulting row count.

`offset`

- Type: UINT16
- Description: Query results can start at an offset.

`netmask`

- Type: STRING
- Description: Query netmask CIDR.

Back to Command List

EsmQueryGroupType

Description

Defines the available types of grouped queries.

Accepted Values

- NO_GROUP
- COUNT
- SEVERITY
- RISK
- AVERAGE
- SUM

Back to Command List

EsmQueryId

Description

An ID for a query, used to execute queries. Gotten by listing available queries in the system with qryGetQueryList.

Properties

value

- Type: UINT32
- Description: The raw 32 bit unsigned value for this query ID object

Back to Command List

EsmQueryResultID

Description

An ID used to reference query results, gotten from an EsmRunningQuery.

Properties

value

- Type: UINT64
- Description: The raw 64 bit unsigned value for this query result ID

Returned By

- qryExecute
- qryExecuteDetail
- qryExecuteGrouped

Back to Command List

EsmQueryResults

Description

The result data from a query that has completed.

Properties

columns

- Type: List of EsmQueryColumn
- Description: The column information for the query results

rows

- Type: List of EsmQueryRow
- Description: The row data in the results

Returned By

- qryGetResults

Back to Command List

EsmQueryRow

Description

A single row of data in ESM query results.

Properties

values

- Type: List of STRING
- Description: The values in the query result

Returned By

- qryGetCorrEventDataForID
- qryGetResults

Back to Command List

EsmQueryStatus

Description

The progress associated with a running query

Properties

complete

- Type: BOOLEAN
- Description: Whether the query is complete

percentComplete

- Type: UINT16
- Description: The percent complete for the query between 0 and 100

milliseconds

- Type: UINT16
- Description: The milliseconds this query has been running

Returned By

- qryGetStatus

Back to Command List

EsmQueryType

Description

The type of information returned by a query

Accepted Values

- EVENT
- FLOW
- IPS_QUERY
- ASSET
- CASE_QUERY
- FILTER_QUERY
- TRIGGERED_ALARMS_QUERY
- EPO_REALTIME_QUERY
- MISC_QUERY
- IOC_QUERY
- RISK
- AGG1
- AGG2
- AGG3
- CORRELATION
- WATCHLIST

Back to Command List

EsmRestCalendar

Description

Calendar Formatter

Returned By

- essmgtGetESSTime

Back to Command List

EsmRight

Description

An ESM right.

Properties

name

- Type: STRING
- Description: The name of this right

description

- Type: STRING
- Description: The description of this right

id

- Type: EsmRightId
- Description: The ID of this right, used to reference this right in other calls

Returned By

- userGetRightsList

Back to Command List

EsmRightId

Description

An id for an ESM right.

Properties

value

- Type: UINT32
- Description: The raw numeric right ID

Returned By

- userGetAccessGroupDetail
- userGetRightsList

Back to Command List

EsmRowOrder

Description

A configuration option for queries, a column index can be sorted ascending or descending.

Properties

direction

- Type: EsmSortDirection
- Description: The direction associated with this order object
- Accepted Values:
  - ASCENDING
  - DESCENDING

field

- Type: EsmSelectField
- Description: The field that will be ordered in the query results

Back to Command List

EsmRunningQuery

Description

Represents a running query in the system.

Properties

type

- Type: TYPE
- Description: Must be set to one of the accepted type string values. Note the properties for the type must appear alongside this property.
- Accepted Values:
  - EsmQueryColumnInfo

countColumn

- Type: UINT16
- Description: The column containing the count in a grouped query

labelColumn

- Type: UINT16
- Description: The column containing text labels

attributeColumn

- Type: UINT16
- Description: The column containing an attribute if applicable

drilldownColumn

- Type: UINT16
- Description: The drilldown column for the query if applicable

totalRows

- Type: UINT32
- Description: The total rows in the query result

resultID

- Type: EsmQueryResultID
- Description: The result ID used to get the results for this running query

startTime

- Type: STRING
- Description: The time this query started running

stopTime

- Type: STRING
- Description: The time this query stopped running

totalResultID

- Type: EsmQueryResultID
- Description: The result to get the total rows for the query

groupByString

- Type: STRING
- Description: The group by string for the query if applicable

Returned By

- qryExecute

- qryExecuteDetail
- qryExecuteGrouped

Back to Command List

EsmSelectField

Description

Fields that can be selected in queries.

Properties

name

- Type: STRING
- Description: The name of the field

types

- **Read only**
- Type: List of EsmFieldType
- Description: The field type for this filter field. Most fields only have one type, but some custom fields can have multiple subtypes. In this case, multiple values need to be set for the field.

table

- **Read only**
- Type: STRING
- Description: If not the base table for the query, this will store the table name

alertField

- **Read only**
- Type: UINT8
- Description: The internal event table index for this custom field

flowField

- **Read only**
- Type: UINT8
- Description: The internal flow table index for this custom field

filterFlag

- **Read only**
- Type: UINT16
- Description: The filter flags telling us which type of query this field applies to

typeBits

- Type: UINT16
- Description: The bits telling us which query type this field is relevant for

id

- Type: STRING
- Description: ID of the field

Returned By

- qryGetSelectFields

Back to Command List

EsmSmsId

Description

An ID representing an SMS number in the ESM.

Properties

value

- Type: UINT32
- Description: The raw 32 bit SMS id value

Returned By

- userGetUserList

Back to Command List

EsmSortDirection

Description

The sort direction for a single column in a query

Accepted Values

- ASCENDING
- DESCENDING

Back to Command List

EsmSourceEvent

Description

Created by sherd on 9/22/16.

Properties

id

- Type: STRING
- Description: The id

severity

- Type: UINT32
- Description: The severity

ruleMessage

- Type: STRING
- Description: The rule message

eventCount

- Type: UINT32
- Description: The event count

sourceIp

- Type: STRING
- Description: The sourceIp

destIp

- Type: STRING
- Description: The destIp

protocol

- Type: STRING
- Description: The protocol

lastTime

- Type: STRING
- Description: The lastTime

usage

- Type: STRING
- Description: The usage

Returned By

- ipsGetCorrRawEvents

Back to Command List

EsmSourceEvents

Description

Created by sherd on 9/22/16.

Properties

sourceEvents

- Type: List of EsmSourceEvent
- Description: The source events

sourceFlows

- Type: List of EsmSourceFlow
- Description: The source flows

deviations

- Type: List of STRING
- Description: The deviations

text

- Type: STRING
- Description: The text

Returned By

- ipsGetCorrRawEvents

Back to Command List

EsmSourceFlow

Description

Created by sherd on 9/22/16.

Properties

flowId

- Type: STRING
- Description: The flowId

sourceIp

- Type: STRING
- Description: The sourceIp

destIp

- Type: STRING
- Description: The destIp

destPort

- Type: STRING
- Description: The destPort

protocol

- Type: STRING
- Description: The protocol

eventCount

- Type: UINT32
- Description: The eventCount

lastTime

- Type: STRING
- Description: The lastTime

Returned By

- ipsGetCorrRawEvents

Back to Command List

EsmStringList

Description

This class is used for passing a generic string list to the java from the javascript through the rest calls. Created by sherd on 8/19/16.

Properties

list

- Type: List of STRING
- Description: Gets the list of strings

Back to Command List

EsmSubZone

Description

A sub zone is a child of a zone.

Properties

name

- Type: STRING
- Description: The name of the sub zone

id

- Type: EsmSubZoneId
- Description: The ID of the sub zone, used to reference this sub zone in the API

Returned By

- zoneGetZoneTree

Back to Command List

EsmSubZoneId

Description

A sub zone ID

Properties

value

- Type: UINT16
- Description: The unsigned 16 bit id for this sub zone

Returned By

- zoneGetSubZone
- zoneGetZoneTree

Back to Command List

EsmSubZoneInfo

Description

Extended detail on a sub zone

Properties

id

- Type: EsmSubZoneId
- Description: The ID of the subZone

name

- Type: STRING
- Description: The name of the sub zone

description

- Type: STRING
- Description: The description for ths sub zone

ranges

- Type: List of EsmZoneRange
- Description: The ranges that make up this sub zone

Returned By

- zoneGetSubZone

Back to Command List

EsmTimeRange

Description

All available time ranges available for queries

Accepted Values

- CUSTOM
- LAST_MINUTE
- LAST_10_MINUTES
- LAST_30_MINUTES
- LAST_HOUR
- CURRENT_DAY
- PREVIOUS_DAY
- LAST_24_HOURS
- LAST_2_DAYS
- LAST_3_DAYS
- CURRENT_WEEK
- PREVIOUS_WEEK
- CURRENT_MONTH
- PREVIOUS_MONTH
- CURRENT_QUARTER
- PREVIOUS_QUARTER
- CURRENT_YEAR
- PREVIOUS_YEAR

Back to Command List

EsmTimeZone

Description

A timezone defined in the system

Properties

id

- Type: EsmTimeZoneId
- Description: The ID of this timezone

name

- Type: STRING
- Description: The name of this timezone

offset

- Type: STRING
- Description: The offset for this timezone

Returned By

- userGetTimeZones

Back to Command List

EsmTimeZoneId

Description

The ID object for a specific timezone

Properties

value

- Type: UINT32
- Description: The raw timezone id for this timezone id object

Returned By

- userGetAccessGroupDetail
- userGetTimeZones

Back to Command List

EsmTreeNode

Description

Describes a node in the device tree.

Properties

type

- Type: EsmDeviceType
- Description: The type of the device
- Accepted Values:
  - IPS
  - POLICY
  - RECEIVER
  - THIRD_PARTY
  - DBM
  - DBM_DB
  - DBM_AGENT
  - VA
  - IPSVIPS
  - ESM
  - APM
  - APMVIPS
  - ELM
  - ELMREC
  - LOCALESM
  - RISK
  - ASSET
  - RISKMANAGER
  - RISKAGENT
  - EPO
  - EPO_APP
  - NSM
  - NSM_SENSOR
  - NSM_INTERFACE
  - MVM
  - SEARCH_ELASTIC
  - KID_CLUSTER
  - KID_NODE
  - SYSTEM
  - BUCKET
  - UNKNOWN

name

- Type: STRING
- Description: The name of the device

id

- Type: EsmDataSourceId
- Description: The ID of the tree node

addDeleteRight

- Type: BOOLEAN
- Description: Whether the user has the right to add/delete to/from this node

children

- Type: List of EsmTreeNodeEx
- Description: Devices defined under this device in the tree

Returned By

- grpGetDeviceTree

Back to Command List

EsmTreeNodeEx

Description

Extended device record, usually only used internally

Properties

type

- Type: EsmDeviceType
- Description: The type of the device
- Accepted Values:
  - IPS
  - POLICY
  - RECEIVER
  - THIRD_PARTY
  - DBM
  - DBM_DB
  - DBM_AGENT
  - VA
  - IPSVIPS
  - ESM
  - APM
  - APMVIPS
  - ELM
  - ELMREC
  - LOCALESM
  - RISK
  - ASSET
  - RISKMANAGER
  - RISKAGENT
  - EPO
  - EPO_APP
  - NSM
  - NSM_SENSOR
  - NSM_INTERFACE
  - MVM
  - SEARCH_ELASTIC
  - KID_CLUSTER
  - KID_NODE
  - SYSTEM
  - BUCKET
  - UNKNOWN

name

- Type: STRING
- Description: The name of the device

id

- Type: EsmDataSourceId
- Description: The ID of the tree node

addDeleteRight

- Type: BOOLEAN
- Description: Whether the user has the right to add/delete to/from this node

children

- Type: EsmTreeNodeEx
- Description: Devices defined under this device in the tree

vipsID

- Type: STRING
- Description: The VIPS ID associated with this entity

adRight

- Type: BOOLEAN
- Description: Group add/delete right flag

eventRight

- Type: STRING
- Description: Whether the user has event management rights for this entity

ipsRight

- Type: BOOLEAN
- Description: Whether the user has IPS management rights for this entity

reportRight

- Type: STRING
- Description: Whether the user has reporting rights for this entity

polRight

- Type: BOOLEAN
- Description: Whether the user has policy admin rights for this entity

viewRight

- Type: STRING
- Description: Whether the user has view management rights for this entity

CRuleRight

- Type: BOOLEAN
- Description: Whether the user has custom rule rights for this entity

FTestRight

- Type: BOOLEAN
- Description: Whether the user has FIPS test rights for this entity

vipsInSync

- Type: BOOLEAN
- Description: Whether the VIPS represented by this tree node is in sync

status

- Type: STRING
- Description: A status string for this node

statusAck

- Type: STRING
- Description: Status acknowledgement code

vipsEnabled

- Type: BOOLEAN
- Description: Whether VIPS is enabled

tpcType

- Type: STRING
- Description: Internal use value (third party config)

protocol

- Type: STRING
- Description: The data source protocol for this entity

hasParent

- Type: BOOLEAN
- Description: Whether this tree node has a parent node

elmHasSAN

- Type: BOOLEAN
- Description: Whether the ELM is using a SAN

elmFile

- Type: BOOLEAN
- Description: TODO: add description

clientVipsInSync

- Type: BOOLEAN
- Description: Whether the client VIPS is in sync

clientStatus

- Type: STRING
- Description: Client status string related to this entity

tpcCollector

- Type: STRING
- Description: Internal use value (third party config)

clientCount

- Type: UINT32
- Description: Number of clients associated with this entity

deviceActionRight

- Type: BOOLEAN
- Description: Whether the user has device action rights for this entity

deviceDisabled

- Type: BOOLEAN
- Description: Whether this device is disabled

ipAddress

- Type: STRING
- Description: The ip address of the node, if any

hostname

- Type: STRING
- Description: The hostname of the node, if any

deviceMask

- Type: STRING
- Description: The device mask

Returned By

- grpGetDeviceTree
- grpGetDeviceTreeEx

Back to Command List

EsmTriggeredAlarm

Description

An alarm that has been triggered in the system

Properties

id

- Type: EsmAlarmId
- Description: The ID of the triggered alarm

summary

- Type: STRING
- Description: The summary of the triggered alarm

assignee

- Type: STRING
- Description: The assignee for this triggered alarm

severity

- Type: UINT32
- Description: The severity for this triggered alarm

triggeredDate

- Type: STRING
- Description: The date this alarm was triggered

acknowledgedDate

- Type: STRING
- Description: The date this triggered alarm was acknowledged

acknowledgedUsername

- Type: STRING
- Description: The user that acknowledged this triggered alarm

alarmName

- Type: STRING
- Description: The name of the alarm that was triggered

conditionType

- Type: UINT32
- Description: The condition type of the alarm

Returned By

- alarmGetTriggeredAlarms

Back to Command List

EsmTriggeredAlarmDetail

Description

Created by sherd on 9/7/16.

Properties

id

- Type: EsmAlarmId
- Description: The ID of the triggered alarm

summary

- Type: STRING
- Description: The summary of the triggered alarm

assignee

- Type: STRING
- Description: The assignee for this triggered alarm

severity

- Type: UINT32
- Description: The severity for this triggered alarm

triggeredDate

- Type: STRING
- Description: The date this alarm was triggered

acknowledgedDate

- Type: STRING
- Description: The date this triggered alarm was acknowledged

acknowledgedUsername

- Type: STRING
- Description: The user that acknowledged this triggered alarm

alarmName

- Type: STRING
- Description: The name of the alarm that was triggered

conditionType

- Type: UINT32
- Description: The condition type of the alarm

filters

- Type: STRING
- Description: The filters for this user

queryId

- Type: UINT32
- Description: The queryId for this user

alretRateMin

- Type: UINT32
- Description: The alretRateMin for this user

alertRateCount

- Type: UINT32
- Description: The alertRateCount for this user

percentAbove

- Type: UINT8
- Description: The percentAbove for this user

percentBelow

- Type: UINT8
- Description: The percentBelow for this user

offsetMinutes

- Type: UINT32
- Description: The offsetMinutes for this user

timeFilter

- Type: STRING
- Description: The timeFilter for this user

maximumConditionTriggerFrequency

- Type: UINT32
- Description: The maximumConditionTriggerFrequency for this user

useWatchlist

- Type: STRING
- Description: The useWatchlist for this user

matchField

- Type: STRING
- Description: The matchField for this user

matchValue

- Type: STRING
- Description: The matchValue for this user

healthMonStatus

- Type: STRING
- Description: The healthMonStatus for this user

assigneeId

- Type: UINT32
- Description: The assigneeId for this user

escalatedDate

- Type: STRING
- Description: The escalatedDate for this user

caseId

- Type: UINT32
- Description: The caseId for this user

caseName

- Type: STRING
- Description: The caseName for this user

iocName

- Type: STRING
- Description: The iocName for this user

`iocId`

- Type: UINT32
- Description: The iocId for this user

`description`

- Type: STRING
- Description: The description for this user

`actions`

- Type: STRING
- Description: The actions for this user

`events`

- Type: List of EsmTriggeredAlarmEvent
- Description: The events for this user

Returned By

- notifyGetTriggeredNotificationDetail

Back to Command List

EsmTriggeredAlarmEvent

Description

Created by sherd on 9/7/16.

Properties

eventId

- Type: STRING
- Description: The value for this user

severity

- Type: UINT32
- Description: The value for this user

ruleMessage

- Type: STRING
- Description: The value for this user

eventCount

- Type: UINT32
- Description: The value for this user

sourceIp

- Type: STRING
- Description: The value for this user

destIp

- Type: STRING
- Description: The value for this user

protocol

- Type: STRING
- Description: The value for this user

lastTime

- Type: STRING
- Description: The value for this user

eventSubType

- Type: STRING
- Description: The value for this user

Returned By

- notifyGetTriggeredNotificationDetail

Back to Command List

EsmUpdateType

Description

A type of update frequency

Accepted Values

- EVERY_SO_MANY_MINUTES
- HOURLY_AT_SPECIFIED_MINUTE
- DAILY_AT_SPECIFIED_TIME
- WEEKLY_AT_SPECIFIED_DAYTIME
- MONTHLY_AT_SPECIFIED_DAYTIME

Back to Command List

EsmUser

Description

Holds basic information about a user in the ESM

Properties

username

- Type: STRING
- Description: The username for this user

id

- Type: EsmUserId
- Description: The ESM ID representing this user

locked

- Type: BOOLEAN
- Description: Whether this user is locked out

loggedInCount

- Type: UINT32
- Description: The number of times this user is currently logged in

email

- Type: STRING
- Description: The user's email address

emailId

- Type: EsmEmailId
- Description: Internal use

sms

- Type: STRING
- Description: This user's SMS address

smsId

- Type: EsmSmsId
- Description: Internal use

master

- Type: BOOLEAN
- Description: Whether this user is the master user

admin

- Type: BOOLEAN
- Description: Whether this user is an admin

alias

- Type: STRING
- Description: The alias for this user if defined

type

- Type: EsmUserType
- Description: The type of user
- Accepted Values:

- POWER
- AUDIT
- CRYPTO
- USER

`groups`

- Type: List of EsmAccessGroupId
- Description: The access group ids to which this user belongs

Returned By

- userGetUserList

Back to Command List

EsmUserDefinedDataSource

Description

Represents a User Defined Data Source

Properties

name

- Type: STRING
- Description: The name of the user-defined datasource

id

- Type: UINT16
- Description: The id of the user-defined datasource

Returned By

- dsGetUserDefinedDataSources

Back to Command List

EsmUserId

Description

A user id in the ESM.

Properties

value

- Type: UINT32
- Description: The raw 32 bit user id

Returned By

- userAddUser
- userGetAccessGroupDetail
- userGetUserList

Back to Command List

EsmUserRights

Description

The rights assigned to a given user in the system.

Properties

privileges

- Type: EsmPrivileges
- Description: the EsmPrivileges object that stores the users privilege settings.

Returned By

- userGetUserRights

Back to Command List

EsmUserType

Description

User type

Accepted Values

- POWER
- AUDIT
- CRYPTO
- USER

Back to Command List

EsmVariable

Description

A variable defined in the ESM

Properties

name

- Type: STRING
- Description: The name of the variable

id

- Type: EsmVariableId
- Description: The ID of the variable

type

- Type: EsmVariableType
- Description: The type of the variable
- Accepted Values:
  - ACTION
  - DSID
  - IPADDRESS
  - MACADDRESS
  - OTHER
  - PORT
  - PROTOCOL
  - SIGID
  - IPV6
  - USER
  - APP
  - HOST
  - DOMAIN
  - NORMSIGID
  - INTERFACE
  - DEVICE
  - COMMAND
  - OBJECT
  - UNSET
  - REGEX
  - SESSION
  - GEOLOC
  - ASN
  - ZONE
  - STRING
  - BINARY
  - GUID

Returned By

- plcyGetVariableList

Back to Command List

EsmVariableId

Description

An ID representing a variable in the system

Properties

value

- Type: UINT16
- Description: The id of the variable

Returned By

- plcyGetVariableList

Back to Command List

EsmVariableType

Description

The data types for variables defined in the system

Accepted Values

- ACTION
- DSID
- IPADDRESS
- MACADDRESS
- OTHER
- PORT
- PROTOCOL
- SIGID
- IPV6
- USER
- APP
- HOST
- DOMAIN
- NORMSIGID
- INTERFACE
- DEVICE
- COMMAND
- OBJECT
- UNSET
- REGEX
- SESSION
- GEOLOC
- ASN
- ZONE
- STRING
- BINARY
- GUID

Back to Command List

EsmVariableValue

Description

Used to specify a variable as a filter value when executing a query

Properties

variable

- Type: EsmVariableId
- Description: The variable that should be used as the value for this field filter

Back to Command List

EsmWatchlist

Description

Basic information on a watchlist defined in the ESM.

Properties

name

- Type: STRING
- Description: The name of the watchlist

type

- Type: EsmWatchlistField
- Description: The watchlist type

customType

- Type: EsmWatchlistField
- Description: The watchlist custom type (custom field)

dynamic

- Type: BOOLEAN
- Description: Whether this watchlist is dynamic

hidden

- **Read only**
- Type: BOOLEAN
- Description: Whether this watchlist is hidden

scored

- **Read only**
- Type: BOOLEAN
- Description: Whether this watchlist has a scoring component (GTI for example)

valueCount

- **Read only**
- Type: UINT32
- Description: The number of values in this watchlist

active

- **Read only**
- Type: BOOLEAN
- Description: Whether this watchlist is a active

errorMsg

- **Read only**
- Type: STRING
- Description: The error message, if there is one associated with this watchlist

source

- Type: UINT8
- Description: source

id

- Type: UINT16
- Description: The id of the watchlist

Returned By

- sysGetWatchlists

Back to Command List

EsmWatchlistDetails

Description

Detailed information on a watchlist defined in the ESM.

Properties

name

- Type: STRING
- Description: The name of the watchlist

type

- Type: EsmWatchlistField
- Description: The watchlist type

customType

- Type: EsmWatchlistField
- Description: The watchlist custom type (custom field)

dynamic

- Type: BOOLEAN
- Description: Whether this watchlist is dynamic

hidden

- **Read only**
- Type: BOOLEAN
- Description: Whether this watchlist is hidden

scored

- **Read only**
- Type: BOOLEAN
- Description: Whether this watchlist has a scoring component (GTI for example)

valueCount

- **Read only**
- Type: UINT32
- Description: The number of values in this watchlist

active

- **Read only**
- Type: BOOLEAN
- Description: Whether this watchlist is a active

errorMsg

- **Read only**
- Type: STRING
- Description: The error message, if there is one associated with this watchlist

source

- Type: UINT8
- Description: source

id

- Type: UINT8
- Description: The id of the watchlist

search

- Type: STRING
- Description: A regular expression, if applicable to the type of data source

updateType

- Type: EsmUpdateType
- Description: If dynamic is true, the type of update frequency (hourly, weekly, etc)
- Accepted Values:
  - EVERY_SO_MANY_MINUTES
  - HOURLY_AT_SPECIFIED_MINUTE
  - DAILY_AT_SPECIFIED_TIME
  - WEEKLY_AT_SPECIFIED_DAYTIME
  - MONTHLY_AT_SPECIFIED_DAYTIME

updateDay

- Type: UINT8
- Description: The day the watchlist should be updated, if applicable. This value will either be the day of the week (1-7, corresponding to Sunday to Saturday), or the day of the month depending on the update type.

updateMin

- Type: UINT16
- Description: If dynamic is true and a minute field is applicable to the update frequency, this will hold the minute of either the hour or day depending on updateType.

age

- **Read only**
- Type: UINT32
- Description: The age of the watchlist values in milliseconds

ipsid

- Type: STRING
- Description: ipsid

recordCount

- **Read only**
- Type: UINT32
- Description: The number of records in the watchlist

valueFile

- Type: EsmFileToken
- Description: valueFile The file that can be obtained with a call to sysGetWatchlistValues containing all of the watchlist values

dbUrl

- Type: STRING
- Description: If an enrichment source is being set up for the watchlist, this should hold the database URL

mountPoint

- Type: STRING
- Description: If an enrichment source is being set up for the watchlist, this would hold the mount point if applicable. See product documentation on enrichment settings for more details.

path

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment path setting. See the enrichment configuration documentation for more details on this setting.

port

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment port setting. See the enrichment configuration documentation for more details on this setting.

username

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment username setting. See the enrichment configuration documentation for more details on this setting.

password

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment password setting. See the enrichment configuration documentation for more details on this setting.

query

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment query setting. See the enrichment configuration documentation for more details on this setting.

lookup

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment lookup setting. See the enrichment configuration documentation for more details on this setting.

enabled

- Type: BOOLEAN
- Description: Whether the watchlist is enabled

jobTrackerURL

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment Job Tracker URL setting. See the enrichment configuration documentation for more details on this setting.

jobTrackerPort

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment Job Tracker Port setting. See the enrichment configuration documentation for more details on this setting.

postArgs

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment Post Argument setting. See the enrichment configuration documentation for more details on this setting.

sSLCheck

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment SSL Check setting. See the enrichment configuration documentation for more details on this setting.

ignoreRegex

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment Ignore RegEx setting. See the enrichment configuration documentation for more details on this setting.

method

- Type: UINT8
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment method setting. See the enrichment configuration documentation for more details on this setting.

matchRegex

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment match regex setting. See the enrichment configuration documentation for more details on this setting.

lineSkip

- Type: UINT8
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment line skip setting. See the enrichment

configuration documentation for more details on this setting.

`delimitRegex`

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment delimit regex setting. See the enrichment configuration documentation for more details on this setting.

`groups`

- Type: STRING
- Description: If the watchlist is populated from an enrichment source, this will hold the enrichment groups setting. See the enrichment configuration documentation for more details on this setting.

`values`

- Type: List of STRING
- Description: values

Returned By

- sysGetWatchlistDetails

Back to Command List

EsmWatchlistField

Description

Basic information on a watchlist field/type.

Properties

name

- Type: STRING
- Description: The name of the watchlist field

id

- Type: UINT32
- Description: The id of the watchlist field

Returned By

- sysGetWatchlistDetails
- sysGetWatchlistFields
- sysGetWatchlists

Back to Command List

EsmWatchlistFile

Description

Represents a file that holds all of the values for a watchlist. The contents of this file represent the values in the watchlist at the time the call to sysGetWatchlistDetails was made.

Properties

id

- Type: STRING
- Description: The ID of the watchlist file.

Back to Command List

EsmWatchlistId

Description

Represents a watchlist in the system

Properties

value

- Type: UINT16
- Description: Unsigned 16 bit ID

Back to Command List

EsmWatchlistIds

Description

Watchlist ID list wrapper

Properties

watchlistIdList

- Type: List of STRING
- Description: Getter for watchlistIdList

Back to Command List

EsmWatchlistValue

Description

Used to specify a watchlist as a filter value when executing a query.

Properties

watchlist

- Type: EsmWatchlistId
- Description: The ID of the watchlist for this value

Back to Command List

EsmZone

Description

A zone defined in the system

Properties

id

- Type: EsmZoneId
- Description: The ID of this zone

name

- Type: STRING
- Description: The name of this zone

subZones

- Type: List of EsmSubZone
- Description: The sub zones defined in this zone

Returned By

- zoneGetZoneTree

Back to Command List

EsmZoneId

Description

The ID object for a zone, used to reference specific zones throughout the API

Properties

value

- Type: UINT16
- Description: The raw zone id for this zone id object

Returned By

- userGetAccessGroupDetail
- zoneGetZone
- zoneGetZoneTree

Back to Command List

EsmZoneInfo

Description

Full detail on a single zone

Properties

id

- Type: EsmZoneId
- Description: The ID of this zone

name

- Type: STRING
- Description: The name of this zone

description

- Type: STRING
- Description: The description of this zone

default

- Type: BOOLEAN
- Description: Whether this zone is a default zone

geoLoc

- Type: EsmGeoLoc
- Description: The GEO location associated with this zone

asnId

- Type: UINT64
- Description: An ASN ID associated with this zone

Back to Command List

EsmZoneInfoIn

Description

Full detail on a single zone

Properties

type

- Type: TYPE
- Description: Must be set to one of the accepted type string values. Note the properties for the type must appear alongside this property.
- Accepted Values:
  - EsmZoneInfo

id

- Type: EsmZoneId
- Description: The ID of this zone

name

- Type: STRING
- Description: The name of this zone

description

- Type: STRING
- Description: The description of this zone

default

- Type: BOOLEAN
- Description: Whether this zone is a default zone

geoLoc

- Type: EsmGeoLoc
- Description: The GEO location associated with this zone

asnId

- Type: UINT64
- Description: An ASN ID associated with this zone

devices

- Type: List of EsmDeviceId
- Description: The devices associated with this zone

Back to Command List

EsmZoneInfoOut

Description

Full detail on a single zone

Properties

type

- Type: TYPE
- Description: Must be set to one of the accepted type string values. Note the properties for the type must appear alongside this property.
- Accepted Values:
  - EsmZoneInfo

id

- Type: EsmZoneId
- Description: The ID of this zone

name

- Type: STRING
- Description: The name of this zone

description

- Type: STRING
- Description: The description of this zone

default

- Type: BOOLEAN
- Description: Whether this zone is a default zone

geoLoc

- Type: EsmGeoLoc
- Description: The GEO location associated with this zone

asnId

- Type: UINT64
- Description: An ASN ID associated with this zone

devices

- Type: List of UINT64
- Description: The devices associated with this zone

Returned By

- zoneGetZone

Back to Command List

EsmZoneRange

Description

A range of IPs associated with a geo location and ASN id within a sub zone.

Properties

firstIp

- Type: STRING
- Description: The first IP in this zone, inclusive

lastIp

- Type: STRING
- Description: The last IP in this zone, inclusive

geoLoc

- Type: EsmGeoLoc
- Description: The geo location associated with this zone if any

asnId

- Type: UINT64
- Description: The autonomous system number for this zone range TODO: is this right?

Returned By

- zoneGetSubZone

Back to Command List

IpsId

Description

ipsid

Properties

value

- Type: STRING
- Description: the string representation of the IpsId

Returned By

- dsAddDataSourceClientsStatus
- dsAddDataSourcesStatus

Back to Command List

JobStatusValue

Description

Job Status values

Accepted Values

- READY
- RUNNING
- COMPLETE

Back to Command List

JsonString

Description

AssetThreats

Properties

json

- Type: STRING
- Description: json

Returned By

- assetGetAssetThreats

Back to Command List

MActiveResponseAndFilter

Description

Basic information on a ActiveResponse Filter.

Properties

and

- Type: List of MActiveResponseFilterElement
- Description: The ActiveResponse Search Filters

Back to Command List

MActiveResponseFilter

Description

Basic information on a ActiveResponse Filter.

Properties

or

- Type: List of MActiveResponseAndFilter
- Description: The ActiveResponse Filter

Back to Command List

MActiveResponseFilterElement

Description

Basic information on a ActiveResponse Filter.

Properties

name

- Type: STRING
- Description: The ActiveResponse Filter Collector

op

- Type: STRING
- Description: The ActiveResponse Filter Operation

value

- Type: STRING
- Description: The ActiveResponse Filter Value

output

- Type: STRING
- Description: The ActiveResponse Filter Element

group

- Type: STRING
- Description: The ActiveResponse Filter Group

Back to Command List

MActiveResponseParams

Description

Basic information on a ActiveResponse Search Params.

Properties

select

- Type: MActiveResponseSelect
- Description: The ActiveResponse Search Output Fields

filters

- Type: MActiveResponseFilter
- Description: The ActiveResponse Search Filters

Back to Command List

MActiveResponseSelect

Description

Basic information on a ActiveResponse Select Params.

Properties

fields

- Type: List of STRING
- Description: The ActiveResponse Collector Fields that we want results from

Back to Command List

NameError

Description

Contains the name and error explaining why a client datasource was not added

Properties

name

- Type: STRING
- Description: Name of the datasoruce

error

- Type: STRING
- Description: error message

Returned By

- dsAddDataSourcesStatus

Back to Command List

PolicyRolloutError

Description

policy rollout errors

Returned By

- plcyRollPolicy

Back to Command List

PolicyRolloutResponse

Description

Policy roll out response

Properties

policyJobIds

- Type: List of EsmJobId
- Description: list of job ids for rollout

errors

- Type: List of PolicyRolloutError
- Description: list of errors from submitting policy rollout

Returned By

- plcyRollPolicy

Back to Command List

Privilege

Description

Created by blongmor on 4/9/2015.

Properties

read

- Type: BOOLEAN
- Description: whether this privilege can be read.

write

- Type: BOOLEAN
- Description: whether the privilege allows writing.

Returned By

- userGetUserRights

Back to Command List

TagGroup

Description

TagGroup

Properties

id

- Type: UINT32
- Description: id

name

- Type: STRING
- Description: name

Returned By

- assetGetAssetDetailsObject

Back to Command List

WriteRollDatasourceResponse

Description

Write and roll response

Properties

writeoutErrorCode

- Type: EsmErrorCode
- Description: error code related to the write out
- Accepted Values:
  - ERROR_SchemaNotFoundInHash
  - ERROR_SchemaHashFull
  - ERROR_BadSchema
  - ERROR_CouldNotStopDBMFTasksOnChildESM
  - ERROR_CouldNotReadUserIPSRecord
  - ERROR_ShuttingDown
  - ERROR_NotInitialized
  - ERROR_CouldNotReadIPSRecord
  - ERROR_InvalidOpCode
  - ERROR_TempDirectoryDoesNotExist
  - ERROR_CouldNotReadJobRecord
  - ERROR_CouldNotCreateJobRecord
  - ERROR_ScheduleJobFailure
  - ERROR_JobThreadInitFailure
  - ERROR_CouldNotOpenDatabase
  - ERROR_InvalidPriorityBoundry
  - ERROR_InvalidPriorityThreadCount
  - ERROR_InvalidJobThreadCount
  - ERROR_AlreadyInitialized
  - ERROR_libESSInternal
  - ERROR_libESSDBInternal
  - ERROR_Internal
  - ERROR_Ok
  - ERROR_INVALID_SESSION
  - ERROR_MaxSessionsHit
  - ERROR_SessionTimeout
  - ERROR_SchemaCreate
  - ERROR_Session_SQLResultNotAvailable
  - ERROR_INVALID_SESSION_NETWORK
  - ERROR_InsufficientDeviceRights
  - ERROR_InvalidUser
  - ERROR_Login_UserName
  - ERROR_Login_Password
  - ERROR_Login_Locked
  - ERROR_PasswordMatch
  - ERROR_InsufficientRights
  - ERROR_RadiusConnection
  - ERROR_InvalidClientVersion
  - ERROR_ActDirLogin
  - ERROR_InvalidLDAPLogin
  - ERROR_ReadRecord
  - ERROR_ClearRecordFields
  - ERROR_DeleteRecord
  - ERROR_WriteRecord
  - ERROR_DuplicatePrimaryKey
  - ERROR_RecordNotFound
  - ERROR_UnableToCreate
  - ERROR_BadData
  - ERROR_BadQuery
  - ERROR_RecordLocked
  - ERROR_WriteLock
  - ERROR_CannotUnlock
  - ERROR_CustomOnly
  - ERROR_OneOrMoreMembersNotAdded
  - ERROR_NotEmpty
  - ERROR_CantCopyRuleToCustFW
  - ERROR_CantCopyFWRuleToCustRule
  - ERROR_UnknownGroup
  - ERROR_UnknownList
  - ERROR_MAX_FILTER_SIZE
  - ERROR_CannotDeleteUsedByOthers
  - ERROR_AutoProcessActive
  - ERROR_UnknownReceiver
  - ERROR_UknownDataSourceType
  - ERROR_IndexCacheFailed
  - ERROR_ReadField
  - ERROR_SetMaxDaysFailed
  - ERROR_InvalidMapListValue

- ERROR_CouldNotCopyRecord
- ERROR_IndexNotTurnedOn
- ERROR_ETagMismatch
- ERROR_DeleteAlreadyRunning
- ERROR_ArraySizeTooSmall
- ERROR_BadRequest
- ERROR_InvalidValue
- ERROR_NoData
- ERROR_ActionNotAllowed
- ERROR_BadQueryID
- ERROR_NoTimeSpecified
- ERROR_RequestTooLarge
- ERROR_MustBeMasterUser
- ERROR_CommandTimeout
- ERROR_BadCommand
- ERROR_AccessDenied
- ERROR_INVALID_PARAMS
- ERROR_Port22
- ERROR_MaxVIPS
- ERROR_WrongDeviceType
- ERROR_ReceiverPermissionDenied
- ERROR_MaxIPS
- ERROR_FlowsNotAllowed
- ERROR_Cancelled
- ERROR_MaxVMsHit
- ERROR_NoVMsAllowed
- ERROR_MaxDataEnrichHit
- ERROR_VMStorageNotAllowed
- ERROR_InvalidCustTypeName
- ERROR_APINotImplemented
- ERROR_AlreadyClustered
- ERROR_ClusterQueryResultNotAvailable
- ERROR_InvalidQueryGroups
- ERROR_JobExists
- ERROR_InvalidJob
- ERROR_JobStarted
- ERROR_JobNotAllowedBeforeUpgrade
- ERROR_NoJobsExist
- ERROR_UnknownJobError
- ERROR_JobCouldNotBeFound
- ERROR_InSizeMismatch
- ERROR_OutSizeMismatch
- ERROR_BadDirectory
- ERROR_UnableToBackup
- ERROR_UnableToRestore
- ERROR_BadFileName
- ERROR_FileSystemError
- ERROR_FileDoesNotExist
- ERROR_NoMoreData
- ERROR_RequestBytesTooLarge
- ERROR_CouldNotCopy_Move
- ERROR_BadFile
- ERROR_UnableToMount
- ERROR_DiskSpaceNotAvailable
- ERROR_DiskSpaceLow
- ERROR_SharingViolation
- ERROR_CouldNotCreateLogFile
- ERROR_BackupFileCountMismatch
- ERROR_BackupFilesNotFound
- ERROR_BackupOkRedundFailed
- ERROR_CouldNotDecompressFile
- ERROR_CouldNotConnectToIPS
- ERROR_CouldNotExecuteIPSCommand
- ERROR_CouldNotGetFileFromIPS
- ERROR_InvalidIPSResponse
- ERROR_CouldNotCompressFile
- ERROR_CouldNotPutFileToIPS
- ERROR_ErrorProcNotAssigned
- ERROR_CouldNotGetIPSVersion
- ERROR_NotManagementInterface
- ERROR_IncompatibleIPSVersion
- ERROR_TcpDumpBusy
- ERROR_FIPSFailed
- ERROR_MaxAudioFileSizeExceeded
- ERROR_UnableToUnMount
- ERROR_CouldNotGetMachineID
- ERROR_NeedKey
- ERROR_NoActivationKey
- ERROR_CannotRekey
- ERROR_KeyExpired
- ERROR_KeyWrongDeviceType
- ERROR_DeviceAlreadyKeyed
- ERROR_NotValidated
- ERROR_InvalidCustomerID
- ERROR_InvalidCustomerPassword
- ERROR_InvalidCustomer
- ERROR_CouldNotSendEmail

- ERROR_NoViewNotifications
- ERROR_WrongReportFormat
- ERROR_CouldNotCreateReportQuery
- ERROR_ViewNotFound
- ERROR_DeleteDefaultView
- ERROR_REPORT_NoFileCreated
- ERROR_BadPolicyAction
- ERROR_CouldNotLockPolicy
- ERROR_CouldNotSendRules
- ERROR_CouldNotSendFWRules
- ERROR_CouldNotSendSnortRules
- ERROR_OneOrMoreUndoOpsFailed
- ERROR_CannotUseExportMethod
- ERROR_CannotImportPolicy
- ERROR_PolicyElementNotFound
- ERROR_CouldNotSendDSRules
- ERROR_CouldNotSendASPRules
- ERROR_CouldNotSendSyslogRules
- ERROR_CouldNotSendRCSRules
- ERROR_InvalidParentPolicy
- ERROR_MaximumRuleLengthExceeded
- ERROR_KeyOrCertFileNotFound
- ERROR_EncryptedKeyFileNotAllowed
- ERROR_CreatingSSLBackup
- ERROR_KeyAndCertMatch
- ERROR_Unrecoverable
- ERROR_ApplyingSSLKeyCert
- ERROR_BadCertificateChain
- ERROR_DuplicateSubTypeName
- ERROR_UnableToDelete
- ERROR_DuplicateName
- ERROR_NoNitroSecurityConnection
- ERROR_LookupFailed
- ERROR_NotInUpgradePath
- ERROR_InvalidMachineID
- ERROR_DuplicateIPAddress
- ERROR_NameRequired
- ERROR_FieldDelimiterNotFound
- ERROR_InvalidVariableName
- ERROR_InvalidCategoryName
- ERROR_InvalidDescription
- ERROR_ValueRequired
- ERROR_NameTruncated
- ERROR_ValueTruncated
- ERROR_CategoryTruncated
- ERROR_DescriptionTruncated
- ERROR_TooManyDuplicateNames
- ERROR_MaxCharLimit
- ERROR_DupMaxCharLimit
- ERROR_CannotRename
- ERROR_MaxAttributes
- ERROR_InvalidFolder
- ERROR_ZoneDoesNotExist
- ERROR_ManualRuleUpdateFailed
- ERROR_UnableToSyncClock
- ERROR_InvalidAccess
- ERROR_InvalidFilter
- ERROR_NoParams
- ERROR_InvalidManualRuleFileVersion
- ERROR_EmailHostNotSet
- ERROR_EmailAlreadySent
- ERROR_CaseIDExists
- ERROR_UnableToExecuteCommand
- ERROR_NotSentToRemedy
- ERROR_CannotSyncDataSources
- ERROR_ValueInUseByOtherDataSources
- ERROR_QueryResultNotAvailable
- ERROR_InvalidIPAddress
- ERROR_DuplicateHostName
- ERROR_InvalidEncryptValue
- ERROR_InvalidName
- ERROR_InvalidOrganization
- ERROR_InvalidStatus
- ERROR_InvalidSeverity
- ERROR_InvalidParent
- ERROR_PortRequired
- ERROR_InvalidQueryType
- ERROR_InvalidTime
- ERROR_UnableToStartDiscovery
- ERROR_PortControlValuesDifferent
- ERROR_DeviceInUse
- ERROR_UnknownOperation
- ERROR_SQLiFilterItem
- ERROR_MaxItemsExceeded
- ERROR_DeviceDisabled
- ERROR_InvalidTimeRange
- ERROR_LoginTimeRestricted

- ERROR_DayRestrictionRequired
- ERROR_PasswordTimeRestricted
- ERROR_InvalidHeader
- ERROR_OperatingInCloudNotAllowed
- ERROR_ServiceUnavailable
- ERROR_InvalidCredentials
- ERROR_DevicesInCloudExceeded
- ERROR_InvalidTimeRangeGetData
- ERROR_CloudFeatureFlagIsSet
- ERROR_CouldNotReadFilterSet
- ERROR_XMLParseError
- ERROR_XMLRecursion
- ERROR_CorPasteNotAllowed
- ERROR_CorrelationExists
- ERROR_CannotAddCorrelationType
- ERROR_HistoricalNotSet
- ERROR_JSONParsingError
- ERROR_DXLCommandFailed
- ERROR_ActiveResponseSearchFailed
- ERROR_PacketLengthExceeded
- ERROR_CorrelationRuleNotFound
- ERROR_RecursionLevelExceeded
- ERROR_Wakeup_Port_Conflict
- ERROR_DeviceVersionMismatch
- ERROR_CPInvalidESMVersion
- ERROR_InvalidImportVersion
- ERROR_BadCredentials
- ERROR_DBMFTaskFail
- ERROR_InvalidFeedID
- ERROR_CannotDeleteIOCTriggeredAlarm
- ERROR_ATDDataSourceInUseByAnotherFeed
- ERROR_InvalidSTIXFormat
- ERROR_NoSupportedIOCsFound
- ERROR_CyberThreatFileBeingParsed
- ERROR_UnableToCreateKey
- ERROR_UnableToGetKeyFile
- ERROR_UnableToReadKey
- ERROR_UnableToSaveKey
- ERROR_SSHCommandFailed
- ERROR_PrimaryRedundantDiffTypes
- ERROR_CertGenFailed
- ERROR_CertUpdateFailed
- ERROR_CertRestoreFailed
- ERROR_UnableToRemoveKey
- ERROR_SSHConnectionFailed
- ERROR_SSHAuthFailed
- ERROR_RedundantVersionMismatch
- ERROR_InvalidRedundantESMCommand
- ERROR_CannotUpdatePrimaryESM
- ERROR_UpdateRedundantESMFailed
- ERROR_UnableToResetRedundSettings
- ERROR_UnableToStartDBLogging
- ERROR_UnableToStopDBLogging
- ERROR_CannotUpgradeRedundantESM
- ERROR_WaitedTooLongToFinalize
- ERROR_NotReadyToFinalize
- ERROR_NoRedundantsAreSyncing
- ERROR_RedundantIPOrPortInvalid
- ERROR_UnknownDBM
- ERROR_UnknownValueInConfFile
- ERROR_FileFailedValidation
- ERROR_UnknownDatabaseSource
- ERROR_MaxCustomActions
- ERROR_UnknownAgent
- ERROR_MaxDatabaseSources
- ERROR_MaxAgents
- ERROR_LicenseExpired
- ERROR_ValueNotFound
- ERROR_NoAttributesFound
- ERROR_FiltersRequired
- ERROR_DistribCouldNotConnectToDevice
- ERROR_DistribDetailsUnavailable
- ERROR_ChildDSBNotFound
- ERROR_DistribNotApproved
- ERROR_NoDistribFiltersFound
- ERROR_NoDistribDSBBrokersFound
- ERROR_NoDistribCertFound
- ERROR_PasswordExpired
- ERROR_PasswordUsed
- ERROR_PasswordCriteriaFailed
- ERROR_No_Credentials
- ERROR_NoUsersWithCaseMgtRights
- ERROR_SNMPTrapDuplicateIPAddress
- ERROR_NoKeysToExport
- ERROR_SC_Invalid_Filter
- ERROR_SC_Invalid_Query
- ERROR_SC_Invalid_Executive_View_Type

- ERROR_SC_Benchmark_Group_Not_Found
- ERROR_SC_Asset_Group_Not_Found
- ERROR_SC_Invalid_Executive_View_Serialization
- ERROR_SC_Invalid_Range_Data
- ERROR_SC_Get_Operating_System_Error
- ERROR_SC_Get_Operating_System_Empty
- ERROR_SC_Settings_Function_Not_Found
- ERROR_SC_Export_Could_not_translate_to_SQL_statement
- ERROR_SC_BenchmarkGroups_InvalidGroupName
- ERROR_SC_BenchmarkGroups_DuplicatedGroupName
- ERROR_SC_BenchmarkGroups_CannotDeleteGroupName
- ERROR_UnknownType
- ERROR_InvalidTableHandle
- ERROR_UnableToAttachPartition
- ERROR_UnableToDetachPartition
- ERROR_NoSpaceAllocatedForEvents
- ERROR_NoSpaceAllocatedForFlows
- ERROR_InvalidCfgHandle
- ERROR_UnableToGetPartitionInfo
- ERROR_ArchiveNotEnabled
- ERROR_CouldNotConnectToRemote
- ERROR_RemoteLoginFailed
- ERROR_RemotePathFailed
- ERROR_ArchiveRatiosInvalid
- ERROR_KID_BadStrategyName
- ERROR_KID_BadMethodName
- ERROR_KID_CannotParseInputData
- ERROR_KID_CannotValidateData
- ERROR_KID_CannotAddNode
- ERROR_KID_MissingConfiguration
- ERROR_SettingsFile_NoSuchMethod
- ERROR_SettingsFile_IllegalAccess
- ERROR_InterruptedException
- ERROR_KID_BadOpCodeRequested
- ERROR_KID_CanNotDeleteCluster
- ERROR_CannotReassignDeviceELM
- ERROR_InvalidArchiveID
- ERROR_DeviceNotAssociatedWithELM
- ERROR_CannotSetELMPoolName
- ERROR_UnableToRetrieveLog
- ERROR_NotSANCapable
- ERROR_MirrorOutOfSync
- ERROR_UnableToStoreELMConfig
- ERROR_UnableToRetrieveELMConfig
- ERROR_InvalidMirrorConfiguration
- ERROR_UnableToRetrieveStorageConf
- ERROR_UnableToRetrieveAllocConf
- ERROR_UnableToRetrieveMgtDBConf
- ERROR_UnableToStoreStorageConf
- ERROR_UnableToStoreAllocConf
- ERROR_UnableToStoreMgtDBConf
- ERROR_NoDevicesAssociatedWithELM
- ERROR_AllocationNotFound
- ERROR_ELMCannotSearchItself
- ERROR_ELMCouldNotTrimStorehouse
- ERROR_ELMInvalidAllocationSize
- ERROR_ELMTrimInProgress
- ERROR_RELMInvalidDevice
- ERROR_RELMAlreadyEnabled
- ERROR_RELMDisabled
- ERROR_RELMInvalidOperation
- ERROR_RELMTPCError
- ERROR_RELMSuspended
- ERROR_RELMLocked
- ERROR_RELMCouldNotUnlock
- ERROR_RELMRunSetup
- ERROR_RELMSecondMirrorOutOfSync
- ERROR_RELMVersionMismatch
- ERROR_RELMRestoreRELMFailed
- ERROR_RELMSwitchoverRECFail
- ERROR_RELMDiskSpaceNotAvailable
- ERROR_UnableToMoveMgtDB
- ERROR_UnableToObtainLock
- ERROR_NotAllAllocsDeleted
- ERROR_SharedPathExists
- ERROR_InvalidDefault
- ERROR_Expired
- ERROR_PublicAPIServiceDown
- ERROR_ApplicationError
- ERROR_ElasticServiceDown
- ERROR_InvalidPrimaryName
- ERROR_InvalidAlias
- ERROR_AliasNotInGroup
- ERROR_PrimaryIsAnAlias
- ERROR_SomeAliasesUnassigned
- ERROR_AliasIsAPrimary
- ERROR_HADisabled

- ERROR_HAModeUnknown
- ERROR_HAModeChanged
- ERROR_NotHACapable
- ERROR_HADevicesNotCompatible
- ERROR_HANotConfigured
- ERROR_HAStartingUp
- ERROR_ImportError
- ERROR_UnknownModel
- ERROR_InvalidClientMatchBy
- ERROR_NoDataToImport
- ERROR_UnknownDataSourceParent
- ERROR_IPAddrOrNameRequired
- ERROR_MatchByTypeNotAllowed
- ERROR_ExportError
- ERROR_CannotAddAgent
- ERROR_CannotAddClient
- ERROR_EditClientFailed
- ERROR_DuplicateClientType
- ERROR_NoValidDataSourcesToExport
- ERROR_CantChangeParentOfChild
- ERROR_DBNameRequired
- ERROR_TenantNotUnique
- ERROR_CannotCreateTempFile
- ERROR_InvalidCacCert
- ERROR_ModifyFolderNotAllowed
- ERROR_DeleteFolderNotAllowed
- ERROR_CantFindFolder
- ERROR_CantFindThirdPartyType
- ERROR_CantWriteFolderRecord
- ERROR_TooManyValues
- ERROR_OneOrMoreValuesNotAdded
- ERROR_TooManyWatchlists
- ERROR_WatchlistAgeInvalid
- ERROR_IncompatibleTypes
- ERROR_OneOrMoreValuesNotDeleted
- ERROR_InvalidHashedString
- ERROR_WLValuesNotReady
- ERROR_InvalidPackageContents
- ERROR_ModelNodeNotFound
- ERROR_CannotSaveConfData
- ERROR_CannotReadConfData
- ERROR_InvalidUserDefinableField
- ERROR_InvalidRegularExpression
- ERROR_UnknownTaskType
- ERROR_TaskNotFound
- ERROR_TerminateTaskFailed
- ERROR_PermissionDenied
- ERROR_NoAssociatedReceiver
- ERROR_NSMDeviceNotFound
- ERROR_InvalidSensor
- ERROR_InactiveSensor
- ERROR_IPAlreadyBlacklisted
- ERROR_InvalidDuration
- ERROR_IPNotBlacklisted
- ERROR_IPPermamentlyBlacklisted
- ERROR_DuplicateEPOAPIIP
- ERROR_DuplicateEPODatabase
- ERROR_NoSavedQuestions
- ERROR_RealTimeNotInstalled
- ERROR_InvalidEpoQuery
- ERROR_ReadAccessDenied
- ERROR_WriteAccessDenied
- ERROR_ReadWriteAccessDenied
- ERROR_DeleteMTOriginDenied
- ERROR_DeleteMTDefaultDenied
- ERROR_EditMTOriginDenied
- ERROR_DeleteMTUsedByAlarmDenied
- ERROR_RepeatBlockBadlyFormed
- ERROR_GroupAssignmentNotAllowed
- ERROR_RightAssignmentNotAllowed
- ERROR_DASAlreadyAllocated
- ERROR_ESMAlreadyHasDAS
- ERROR_CannotRunScriptOnDevice
- ERROR_DatabusFailure
- ERROR_DEEPOQuery
- ERROR_QuestionNotFound
- ERROR_InvalidEPOIPSIDS
- ERROR_ListActionCmdFailed
- ERROR_Result_File_Not_Found
- ERROR_DuplicateUsernameUrl
- ERROR_TestConnectFailed
- ERROR_TestConnectDoesNotApply
- ERROR_WatchListSyncVerifyFailed
- ERROR_EPOQueryNotAvailable
- ERROR_EPOSessionRecordNotFound
- ERROR_Login_Error
- ERROR_Message_Forwarding_Not_Found

- ERROR_ELS_BadQuery
- ERROR_ELS_OnlyLike
- ERROR_FIRST_LOOK_FEATURE_NOT_FOUND
- ERROR_JobEngine_ExecuteQuery_CouldNotCreateStatment
- ERROR_JobEngine_ExecuteQuery_CouldNotExecuteQuery
- ERROR_JobEngine_JSONParsingError
- ERROR_JobEngine_GetQueryStatus_QueryNotFound_Unrecoverable
- ERROR_JobEngine_CouldNotConnectToSnowflex
- ERROR_JobEngine_GetQueryStatus_StatusNotFound
- ERROR_JobEngine_GetQueryResults_QueryNotFound_Unrecoverable
- ERROR_JobEngine_GetQueryResults_StatusNotFound
- ERROR_JobEngine_GetQueryResults_ReportedCompleteButNot
- ERROR_JobEngine_GetQueryResults_InvalidStartIndex
- ERROR_JobEngine_GetQueryResults_InvalidMaxRows
- ERROR_JobEngine_GetQueryResults
- ERROR_JobEngine_ExecuteUpdate
- ERROR_JobEngine_ExecuteUpdate_ReportedCompleteButNot
- ERROR_JobEngine_CannotConnectToJobEngine
- ERROR_JobEngine_GetUpdateResultsJob_QueryNotFound_Unrecoverable
- ERROR_JobEngine_GetUpdateResultsJob_SnowflexResult
- ERROR_JobEngine_GetUpdateResultsJob_ReportedCompleteButNot
- ERROR_JobEngine_GetUpdateResultsJob
- ERROR_JobEngine_TimeoutToShort
- ERROR_JobEngine_QueryTimedOut
- ERROR_JEC_JobEngineErrorNotFound
- ERROR_JEC_JobResultNotAvailable
- ERROR_JEC_ResponseNotAvailable
- ERROR_JEC_EmptyRequest
- ERROR_JEC_ErrorSendingRequest
- ERROR_JEC_SocketConnectionError
- ERROR_JEQ_BG_JobResultsNotAvailable
- ERROR_JEQ_BG_InvalidUUID
- ERROR_JEQ_GetRecords_ResultsNotAvailable
- ERROR_JEQ_PutRecord_ResultsNotAvailable
- ERROR_CP_UnmetDependency
- ERROR_CP_IncompatibleESMversion
- ERROR_CP_GetComponentFailed
- ERROR_UA_Invalid_input_json_file
- ERROR_UA_Fail_reading_config_params
- ERROR_UA_Fail_collecting_upgrade_info
- ERROR_UA_Version_to_upgrade_not_chosen
- ERROR_UA_Cannot_upgrade_to_version_choose
- ERROR_UA_Cannot_gather_appliances_info
- ERROR_UA_Cannot_find_advisory_checkers
- ERROR_UA_Executing_advisor_command
- ERROR_UA_Non_existent_check_id
- ERROR_UA_Retreiving_history_checks
- ERROR_UA_Reading_configuration_file
- ERROR_UA_Writing_input_checker_file
- ERROR_UA_Reading_upgrade_info_file
- ERROR_UA_Writing_upgrade_info_file
- ERROR_FILTER_SET_Alarm_Not_Found

`policyRolloutJobId`

- Type: EsmJobId
- Description: The job id for policy roll out. Will be null if the API failed before rollout

`policyRolloutErrorCode`

- Type: EsmErrorCode
- Description: An error code for policy roll out. null indicates failure before policy roll out
- Accepted Values:
  - ERROR_SchemaNotFoundInHash
  - ERROR_SchemaHashFull
  - ERROR_BadSchema
  - ERROR_CouldNotStopDBMFTasksOnChildESM
  - ERROR_CouldNotReadUserIPSRecord
  - ERROR_ShuttingDown
  - ERROR_NotInitialized
  - ERROR_CouldNotReadIPSRecord
  - ERROR_InvalidOpCode
  - ERROR_TempDirectoryDoesNotExist
  - ERROR_CouldNotReadJobRecord
  - ERROR_CouldNotCreateJobRecord
  - ERROR_ScheduleJobFailure
  - ERROR_JobThreadInitFailure
  - ERROR_CouldNotOpenDatabase
  - ERROR_InvalidPriorityBoundry
  - ERROR_InvalidPriorityThreadCount
  - ERROR_InvalidJobThreadCount
  - ERROR_AlreadyInitialized
  - ERROR_libESSInternal
  - ERROR_libESSDBInternal

- ERROR_Internal
- ERROR_Ok
- ERROR_INVALID_SESSION
- ERROR_MaxSessionsHit
- ERROR_SessionTimeout
- ERROR_SchemaCreate
- ERROR_Session_SQLResultNotAvailable
- ERROR_INVALID_SESSION_NETWORK
- ERROR_InsufficientDeviceRights
- ERROR_InvalidUser
- ERROR_Login_UserName
- ERROR_Login_Password
- ERROR_Login_Locked
- ERROR_PasswordMatch
- ERROR_InsufficientRights
- ERROR_RadiusConnection
- ERROR_InvalidClientVersion
- ERROR_ActDirLogin
- ERROR_InvalidLDAPLogin
- ERROR_ReadRecord
- ERROR_ClearRecordFields
- ERROR_DeleteRecord
- ERROR_WriteRecord
- ERROR_DuplicatePrimaryKey
- ERROR_RecordNotFound
- ERROR_UnableToCreate
- ERROR_BadData
- ERROR_BadQuery
- ERROR_RecordLocked
- ERROR_WriteLock
- ERROR_CannotUnlock
- ERROR_CustomOnly
- ERROR_OneOrMoreMembersNotAdded
- ERROR_NotEmpty
- ERROR_CantCopyRuleToCustFW
- ERROR_CantCopyFWRuleToCustRule
- ERROR_UnknownGroup
- ERROR_UnknownList
- ERROR_MAX_FILTER_SIZE
- ERROR_CannotDeleteUsedByOthers
- ERROR_AutoProcessActive
- ERROR_UnknownReceiver
- ERROR_UknownDataSourceType
- ERROR_IndexCacheFailed
- ERROR_ReadField
- ERROR_SetMaxDaysFailed
- ERROR_InvalidMapListValue
- ERROR_CouldNotCopyRecord
- ERROR_IndexNotTurnedOn
- ERROR_ETagMismatch
- ERROR_DeleteAlreadyRunning
- ERROR_ArraySizeTooSmall
- ERROR_BadRequest
- ERROR_InvalidValue
- ERROR_NoData
- ERROR_ActionNotAllowed
- ERROR_BadQueryID
- ERROR_NoTimeSpecified
- ERROR_RequestTooLarge
- ERROR_MustBeMasterUser
- ERROR_CommandTimeout
- ERROR_BadCommand
- ERROR_AccessDenied
- ERROR_INVALID_PARAMS
- ERROR_Port22
- ERROR_MaxVIPS
- ERROR_WrongDeviceType
- ERROR_ReceiverPermissionDenied
- ERROR_MaxIPS
- ERROR_FlowsNotAllowed
- ERROR_Cancelled
- ERROR_MaxVMsHit
- ERROR_NoVMsAllowed
- ERROR_MaxDataEnrichHit
- ERROR_VMStorageNotAllowed
- ERROR_InvalidCustTypeName
- ERROR_APINotImplemented
- ERROR_AlreadyClustered
- ERROR_ClusterQueryResultNotAvailable
- ERROR_InvalidQueryGroups
- ERROR_JobExists
- ERROR_InvalidJob
- ERROR_JobStarted
- ERROR_JobNotAllowedBeforeUpgrade
- ERROR_NoJobsExist
- ERROR_UnknownJobError
- ERROR_JobCouldNotBeFound

- ERROR_InSizeMismatch
- ERROR_OutSizeMismatch
- ERROR_BadDirectory
- ERROR_UnableToBackup
- ERROR_UnableToRestore
- ERROR_BadFileName
- ERROR_FileSystemError
- ERROR_FileDoesNotExist
- ERROR_NoMoreData
- ERROR_RequestBytesTooLarge
- ERROR_CouldNotCopy_Move
- ERROR_BadFile
- ERROR_UnableToMount
- ERROR_DiskSpaceNotAvailable
- ERROR_DiskSpaceLow
- ERROR_SharingViolation
- ERROR_CouldNotCreateLogFile
- ERROR_BackupFileCountMismatch
- ERROR_BackupFilesNotFound
- ERROR_BackupOkRedundFailed
- ERROR_CouldNotDecompressFile
- ERROR_CouldNotConnectToIPS
- ERROR_CouldNotExecuteIPSCommand
- ERROR_CouldNotGetFileFromIPS
- ERROR_InvalidIPSResponse
- ERROR_CouldNotCompressFile
- ERROR_CouldNotPutFileToIPS
- ERROR_ErrorProcNotAssigned
- ERROR_CouldNotGetIPSVersion
- ERROR_NotManagementInterface
- ERROR_IncompatibleIPSVersion
- ERROR_TcpDumpBusy
- ERROR_FIPSFailed
- ERROR_MaxAudioFileSizeExceeded
- ERROR_UnableToUnMount
- ERROR_CouldNotGetMachineID
- ERROR_NeedKey
- ERROR_NoActivationKey
- ERROR_CannotRekey
- ERROR_KeyExpired
- ERROR_KeyWrongDeviceType
- ERROR_DeviceAlreadyKeyed
- ERROR_NotValidated
- ERROR_InvalidCustomerID
- ERROR_InvalidCustomerPassword
- ERROR_InvalidCustomer
- ERROR_CouldNotSendEmail
- ERROR_NoViewNotifications
- ERROR_WrongReportFormat
- ERROR_CouldNotCreateReportQuery
- ERROR_ViewNotFound
- ERROR_DeleteDefaultView
- ERROR_REPORT_NoFileCreated
- ERROR_BadPolicyAction
- ERROR_CouldNotLockPolicy
- ERROR_CouldNotSendRules
- ERROR_CouldNotSendFWRules
- ERROR_CouldNotSendSnortRules
- ERROR_OneOrMoreUndoOpsFailed
- ERROR_CannotUseExportMethod
- ERROR_CannotImportPolicy
- ERROR_PolicyElementNotFound
- ERROR_CouldNotSendDSRules
- ERROR_CouldNotSendASPRules
- ERROR_CouldNotSendSyslogRules
- ERROR_CouldNotSendRCSRules
- ERROR_InvalidParentPolicy
- ERROR_MaximumRuleLengthExceeded
- ERROR_KeyOrCertFileNotFound
- ERROR_EncryptedKeyFileNotAllowed
- ERROR_CreatingSSLBackup
- ERROR_KeyAndCertMatch
- ERROR_Unrecoverable
- ERROR_ApplyingSSLKeyCert
- ERROR_BadCertificateChain
- ERROR_DuplicateSubTypeName
- ERROR_UnableToDelete
- ERROR_DuplicateName
- ERROR_NoNitroSecurityConnection
- ERROR_LookupFailed
- ERROR_NotInUpgradePath
- ERROR_InvalidMachineID
- ERROR_DuplicateIPAddress
- ERROR_NameRequired
- ERROR_FieldDelimiterNotFound
- ERROR_InvalidVariableName
- ERROR_InvalidCategoryName

- ERROR_InvalidDescription
- ERROR_ValueRequired
- ERROR_NameTruncated
- ERROR_ValueTruncated
- ERROR_CategoryTruncated
- ERROR_DescriptionTruncated
- ERROR_TooManyDuplicateNames
- ERROR_MaxCharLimit
- ERROR_DupMaxCharLimit
- ERROR_CannotRename
- ERROR_MaxAttributes
- ERROR_InvalidFolder
- ERROR_ZoneDoesNotExist
- ERROR_ManualRuleUpdateFailed
- ERROR_UnableToSyncClock
- ERROR_InvalidAccess
- ERROR_InvalidFilter
- ERROR_NoParams
- ERROR_InvalidManualRuleFileVersion
- ERROR_EmailHostNotSet
- ERROR_EmailAlreadySent
- ERROR_CaseIDExists
- ERROR_UnableToExecuteCommand
- ERROR_NotSentToRemedy
- ERROR_CannotSyncDataSources
- ERROR_ValueInUseByOtherDataSources
- ERROR_QueryResultNotAvailable
- ERROR_InvalidIPAddress
- ERROR_DuplicateHostName
- ERROR_InvalidEncryptValue
- ERROR_InvalidName
- ERROR_InvalidOrganization
- ERROR_InvalidStatus
- ERROR_InvalidSeverity
- ERROR_InvalidParent
- ERROR_PortRequired
- ERROR_InvalidQueryType
- ERROR_InvalidTime
- ERROR_UnableToStartDiscovery
- ERROR_PortControlValuesDifferent
- ERROR_DeviceInUse
- ERROR_UnknownOperation
- ERROR_SQLiFilterItem
- ERROR_MaxItemsExceeded
- ERROR_DeviceDisabled
- ERROR_InvalidTimeRange
- ERROR_LoginTimeRestricted
- ERROR_DayRestrictionRequired
- ERROR_PasswordTimeRestricted
- ERROR_InvalidHeader
- ERROR_OperatingInCloudNotAllowed
- ERROR_ServiceUnavailable
- ERROR_InvalidCredentials
- ERROR_DevicesInCloudExceeded
- ERROR_InvalidTimeRangeGetData
- ERROR_CloudFeatureFlagIsSet
- ERROR_CouldNotReadFilterSet
- ERROR_XMLParseError
- ERROR_XMLRecursion
- ERROR_CorPasteNotAllowed
- ERROR_CorrelationExists
- ERROR_CannotAddCorrelationType
- ERROR_HistoricalNotSet
- ERROR_JSONParsingError
- ERROR_DXLCommandFailed
- ERROR_ActiveResponseSearchFailed
- ERROR_PacketLengthExceeded
- ERROR_CorrelationRuleNotFound
- ERROR_RecursionLevelExceeded
- ERROR_Wakeup_Port_Conflict
- ERROR_DeviceVersionMismatch
- ERROR_CPInvalidESMVersion
- ERROR_InvalidImportVersion
- ERROR_BadCredentials
- ERROR_DBMFTaskFail
- ERROR_InvalidFeedID
- ERROR_CannotDeleteIOCTriggeredAlarm
- ERROR_ATDDataSourceInUseByAnotherFeed
- ERROR_InvalidSTIXFormat
- ERROR_NoSupportedIOCsFound
- ERROR_CyberThreatFileBeingParsed
- ERROR_UnableToCreateKey
- ERROR_UnableToGetKeyFile
- ERROR_UnableToReadKey
- ERROR_UnableToSaveKey
- ERROR_SSHCommandFailed
- ERROR_PrimaryRedundantDiffTypes

- ERROR_CertGenFailed
- ERROR_CertUpdateFailed
- ERROR_CertRestoreFailed
- ERROR_UnableToRemoveKey
- ERROR_SSHConnectionFailed
- ERROR_SSHAuthFailed
- ERROR_RedundantVersionMismatch
- ERROR_InvalidRedundantESMCommand
- ERROR_CannotUpdatePrimaryESM
- ERROR_UpdateRedundantESMFailed
- ERROR_UnableToResetRedundSettings
- ERROR_UnableToStartDBLogging
- ERROR_UnableToStopDBLogging
- ERROR_CannotUpgradeRedundantESM
- ERROR_WaitedTooLongToFinalize
- ERROR_NotReadyToFinalize
- ERROR_NoRedundantsAreSyncing
- ERROR_RedundantIPOrPortInvalid
- ERROR_UnknownDBM
- ERROR_UnknownValueInConfFile
- ERROR_FileFailedValidation
- ERROR_UnknownDatabaseSource
- ERROR_MaxCustomActions
- ERROR_UnknownAgent
- ERROR_MaxDatabaseSources
- ERROR_MaxAgents
- ERROR_LicenseExpired
- ERROR_ValueNotFound
- ERROR_NoAttributesFound
- ERROR_FiltersRequired
- ERROR_DistribCouldNotConnectToDevice
- ERROR_DistribDetailsUnavailable
- ERROR_ChildDSBNotFound
- ERROR_DistribNotApproved
- ERROR_NoDistribFiltersFound
- ERROR_NoDistribDSBBrokersFound
- ERROR_NoDistribCertFound
- ERROR_PasswordExpired
- ERROR_PasswordUsed
- ERROR_PasswordCriteriaFailed
- ERROR_No_Credentials
- ERROR_NoUsersWithCaseMgtRights
- ERROR_SNMPTrapDuplicateIPAddress
- ERROR_NoKeysToExport
- ERROR_SC_Invalid_Filter
- ERROR_SC_Invalid_Query
- ERROR_SC_Invalid_Executive_View_Type
- ERROR_SC_Benchmark_Group_Not_Found
- ERROR_SC_Asset_Group_Not_Found
- ERROR_SC_Invalid_Executive_View_Serialization
- ERROR_SC_Invalid_Range_Data
- ERROR_SC_Get_Operating_System_Error
- ERROR_SC_Get_Operating_System_Empty
- ERROR_SC_Settings_Function_Not_Found
- ERROR_SC_Export_Could_not_translate_to_SQL_statement
- ERROR_SC_BenchmarkGroups_InvalidGroupName
- ERROR_SC_BenchmarkGroups_DuplicatedGroupName
- ERROR_SC_BenchmarkGroups_CannotDeleteGroupName
- ERROR_UnknownType
- ERROR_InvalidTableHandle
- ERROR_UnableToAttachPartition
- ERROR_UnableToDetachPartition
- ERROR_NoSpaceAllocatedForEvents
- ERROR_NoSpaceAllocatedForFlows
- ERROR_InvalidCfgHandle
- ERROR_UnableToGetPartitionInfo
- ERROR_ArchiveNotEnabled
- ERROR_CouldNotConnectToRemote
- ERROR_RemoteLoginFailed
- ERROR_RemotePathFailed
- ERROR_ArchiveRatiosInvalid
- ERROR_KID_BadStrategyName
- ERROR_KID_BadMethodName
- ERROR_KID_CannotParseInputData
- ERROR_KID_CannotValidateData
- ERROR_KID_CannotAddNode
- ERROR_KID_MissingConfiguration
- ERROR_SettingsFile_NoSuchMethod
- ERROR_SettingsFile_IllegalAccess
- ERROR_InterruptedException
- ERROR_KID_BadOpCodeRequested
- ERROR_KID_CanNotDeleteCluster
- ERROR_CannotReassignDeviceELM
- ERROR_InvalidArchiveID
- ERROR_DeviceNotAssociatedWithELM
- ERROR_CannotSetELMPoolName
- ERROR_UnableToRetrieveLog

- ERROR_NotSANCapable
- ERROR_MirrorOutOfSync
- ERROR_UnableToStoreELMConfig
- ERROR_UnableToRetrieveELMConfig
- ERROR_InvalidMirrorConfiguration
- ERROR_UnableToRetrieveStorageConf
- ERROR_UnableToRetrieveAllocConf
- ERROR_UnableToRetrieveMgtDBConf
- ERROR_UnableToStoreStorageConf
- ERROR_UnableToStoreAllocConf
- ERROR_UnableToStoreMgtDBConf
- ERROR_NoDevicesAssociatedWithELM
- ERROR_AllocationNotFound
- ERROR_ELMCannotSearchItself
- ERROR_ELMCouldNotTrimStorehouse
- ERROR_ELMInvalidAllocationSize
- ERROR_ELMTrimInProgress
- ERROR_RELMInvalidDevice
- ERROR_RELMAlreadyEnabled
- ERROR_RELMDisabled
- ERROR_RELMInvalidOperation
- ERROR_RELMTPCError
- ERROR_RELMSuspended
- ERROR_RELMLocked
- ERROR_RELMCouldNotUnlock
- ERROR_RELMRunSetup
- ERROR_RELMSecondMirrorOutOfSync
- ERROR_RELMVersionMismatch
- ERROR_RELMRestoreRELMFailed
- ERROR_RELMSwitchoverRECFail
- ERROR_RELMDiskSpaceNotAvailable
- ERROR_UnableToMoveMgtDB
- ERROR_UnableToObtainLock
- ERROR_NotAllAllocsDeleted
- ERROR_SharedPathExists
- ERROR_InvalidDefault
- ERROR_Expired
- ERROR_PublicAPIServiceDown
- ERROR_ApplicationError
- ERROR_ElasticServiceDown
- ERROR_InvalidPrimaryName
- ERROR_InvalidAlias
- ERROR_AliasNotInGroup
- ERROR_PrimaryIsAnAlias
- ERROR_SomeAliasesUnassigned
- ERROR_AliasIsAPrimary
- ERROR_HADisabled
- ERROR_HAModeUnknown
- ERROR_HAModeChanged
- ERROR_NotHACapable
- ERROR_HADevicesNotCompatible
- ERROR_HANotConfigured
- ERROR_HAStartingUp
- ERROR_ImportError
- ERROR_UnknownModel
- ERROR_InvalidClientMatchBy
- ERROR_NoDataToImport
- ERROR_UnknownDataSourceParent
- ERROR_IPAddrOrNameRequired
- ERROR_MatchByTypeNotAllowed
- ERROR_ExportError
- ERROR_CannotAddAgent
- ERROR_CannotAddClient
- ERROR_EditClientFailed
- ERROR_DuplicateClientType
- ERROR_NoValidDataSourcesToExport
- ERROR_CantChangeParentOfChild
- ERROR_DBNameRequired
- ERROR_TenantNotUnique
- ERROR_CannotCreateTempFile
- ERROR_InvalidCacCert
- ERROR_ModifyFolderNotAllowed
- ERROR_DeleteFolderNotAllowed
- ERROR_CantFindFolder
- ERROR_CantFindThirdPartyType
- ERROR_CantWriteFolderRecord
- ERROR_TooManyValues
- ERROR_OneOrMoreValuesNotAdded
- ERROR_TooManyWatchlists
- ERROR_WatchlistAgeInvalid
- ERROR_IncompatibleTypes
- ERROR_OneOrMoreValuesNotDeleted
- ERROR_InvalidHashedString
- ERROR_WLValuesNotReady
- ERROR_InvalidPackageContents
- ERROR_ModelNodeNotFound
- ERROR_CannotSaveConfData

- ERROR_CannotReadConfData
- ERROR_InvalidUserDefinableField
- ERROR_InvalidRegularExpression
- ERROR_UnknownTaskType
- ERROR_TaskNotFound
- ERROR_TerminateTaskFailed
- ERROR_PermissionDenied
- ERROR_NoAssociatedReceiver
- ERROR_NSMDeviceNotFound
- ERROR_InvalidSensor
- ERROR_InactiveSensor
- ERROR_IPAlreadyBlacklisted
- ERROR_InvalidDuration
- ERROR_IPNotBlacklisted
- ERROR_IPPermamentlyBlacklisted
- ERROR_DuplicateEPOAPIIP
- ERROR_DuplicateEPODatabase
- ERROR_NoSavedQuestions
- ERROR_RealTimeNotInstalled
- ERROR_InvalidEpoQuery
- ERROR_ReadAccessDenied
- ERROR_WriteAccessDenied
- ERROR_ReadWriteAccessDenied
- ERROR_DeleteMTOriginDenied
- ERROR_DeleteMTDefaultDenied
- ERROR_EditMTOriginDenied
- ERROR_DeleteMTUsedByAlarmDenied
- ERROR_RepeatBlockBadlyFormed
- ERROR_GroupAssignmentNotAllowed
- ERROR_RightAssignmentNotAllowed
- ERROR_DASAlreadyAllocated
- ERROR_ESMAlreadyHasDAS
- ERROR_CannotRunScriptOnDevice
- ERROR_DatabusFailure
- ERROR_DEEPOQuery
- ERROR_QuestionNotFound
- ERROR_InvalidEPOIPSIDS
- ERROR_ListActionCmdFailed
- ERROR_Result_File_Not_Found
- ERROR_DuplicateUsernameUrl
- ERROR_TestConnectFailed
- ERROR_TestConnectDoesNotApply
- ERROR_WatchListSyncVerifyFailed
- ERROR_EPOQueryNotAvailable
- ERROR_EPOSessionRecordNotFound
- ERROR_Login_Error
- ERROR_Message_Forwarding_Not_Found
- ERROR_ELS_BadQuery
- ERROR_ELS_OnlyLike
- ERROR_FIRST_LOOK_FEATURE_NOT_FOUND
- ERROR_JobEngine_ExecuteQuery_CouldNotCreateStatment
- ERROR_JobEngine_ExecuteQuery_CouldNotExecuteQuery
- ERROR_JobEngine_JSONParsingError
- ERROR_JobEngine_GetQueryStatus_QueryNotFound_Unrecoverable
- ERROR_JobEngine_CouldNotConnectToSnowflex
- ERROR_JobEngine_GetQueryStatus_StatusNotFound
- ERROR_JobEngine_GetQueryResults_QueryNotFound_Unrecoverable
- ERROR_JobEngine_GetQueryResults_StatusNotFound
- ERROR_JobEngine_GetQueryResults_ReportedCompleteButNot
- ERROR_JobEngine_GetQueryResults_InvalidStartIndex
- ERROR_JobEngine_GetQueryResults_InvalidMaxRows
- ERROR_JobEngine_GetQueryResults
- ERROR_JobEngine_ExecuteUpdate
- ERROR_JobEngine_ExecuteUpdate_ReportedCompleteButNot
- ERROR_JobEngine_CannotConnectToJobEngine
- ERROR_JobEngine_GetUpdateResultsJob_QueryNotFound_Unrecoverable
- ERROR_JobEngine_GetUpdateResultsJob_SnowflexResult
- ERROR_JobEngine_GetUpdateResultsJob_ReportedCompleteButNot
- ERROR_JobEngine_GetUpdateResultsJob
- ERROR_JobEngine_TimeoutToShort
- ERROR_JobEngine_QueryTimedOut
- ERROR_JEC_JobEngineErrorNotFound
- ERROR_JEC_JobResultNotAvailable
- ERROR_JEC_ResponseNotAvailable
- ERROR_JEC_EmptyRequest
- ERROR_JEC_ErrorSendingRequest
- ERROR_JEC_SocketConnectionError
- ERROR_JEQ_BG_JobResultsNotAvailable
- ERROR_JEQ_BG_InvalidUUID
- ERROR_JEQ_GetRecords_ResultsNotAvailable
- ERROR_JEQ_PutRecord_ResultsNotAvailable
- ERROR_CP_UnmetDependency
- ERROR_CP_IncompatibleESMversion
- ERROR_CP_GetComponentFailed
- ERROR_UA_Invalid_input_json_file
- ERROR_UA_Fail_reading_config_params
- ERROR_UA_Fail_collecting_upgrade_info

- ERROR_UA_Version_to_upgrade_not_chosen
- ERROR_UA_Cannot_upgrade_to_version_choose
- ERROR_UA_Cannot_gather_appliances_info
- ERROR_UA_Cannot_find_advisory_checkers
- ERROR_UA_Executing_advisor_command
- ERROR_UA_Non_existent_check_id
- ERROR_UA_Retreiving_history_checks
- ERROR_UA_Reading_configuration_file
- ERROR_UA_Writing_input_checker_file
- ERROR_UA_Reading_upgrade_info_file
- ERROR_UA_Writing_upgrade_info_file
- ERROR_FILTER_SET_Alarm_Not_Found

Returned By

- dsDeleteDataSourceClients
- dsEditDataSource
- dsEditDataSourceClient

Back to Command List