Integration Guide

Revision A

Mobileiron 1.0

Overview

This guide covers setting up, configuring, and testing the Partner integration of MobileIron with McAfee ePolicy Orchestrator (ePO) along with DXL.

Use Cases

Use Case #1 – Data Exchange

Use the Device Search Field call to retrieve the list of fields that can be searched and returned via queries. You may wish to give an administrator the flexibility to select which device attributes they are interested in. If so, this query will provide the list.
Use the Devices call to return information about one or more devices based on a query criterion. Refer to the query parameters in the sample call for additional information.

Use Case #2 – Enterprise Data Access

The ActiveSync Device Report will return a list of devices accessing ActiveSync via MobileIron Sentry.

The Devices call has been configured to return a list of devices that are not “blocked” via Sentry (e.g. devices that are not blocked from using the Sentry reverse proxy or SSL VPN). Refer to the query parameters for additional detail.

Use Case #3 – Basic Compliance

The Devices call has been configured to return basic compliance attributes. Refer to the query parameters for additional details.

Use Case #4 – Windows 10 Threat Events

The calls are used to create and update custom attributes. In this example, the custom attributes are called com_mcafee_dxl_Win10Threat and com_mcafee_dxl_Win10Threat_Reason. You may name your custom attributes anything you want, but the only special character that is permitted "_". We also recommend that your naming adhere to the loose "Reverse DNS" convention above to avoid collisions with other custom attributes. Refer to the Request Body for details

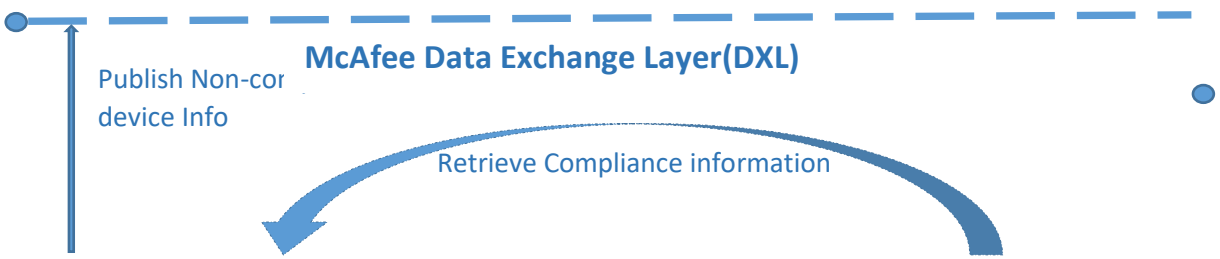
Supported ePO and Product Version

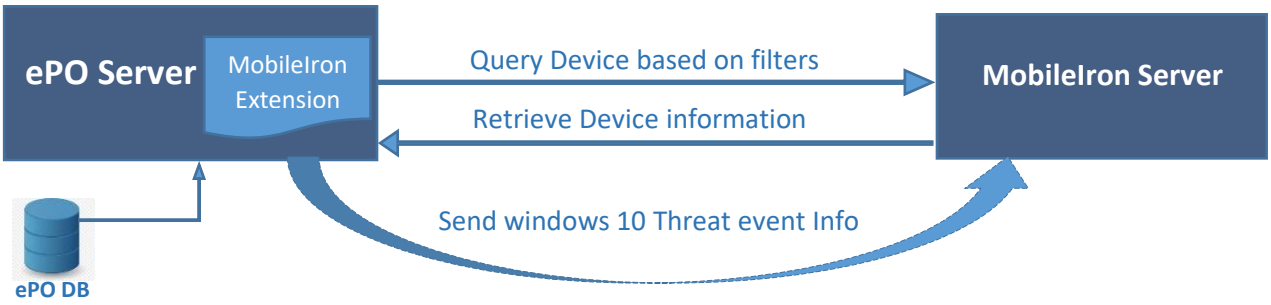
- ePO 5.3.3 and 5.9.1 and MobileIron 1.0.0
- McAfee DXL 3.1.0 and 4.0.0

Approved Product ID and Event ID's

Product ID	Event ID's
S_MOBIRN1000	**204050- 204099**

MobileIron ePO Integration Architecture

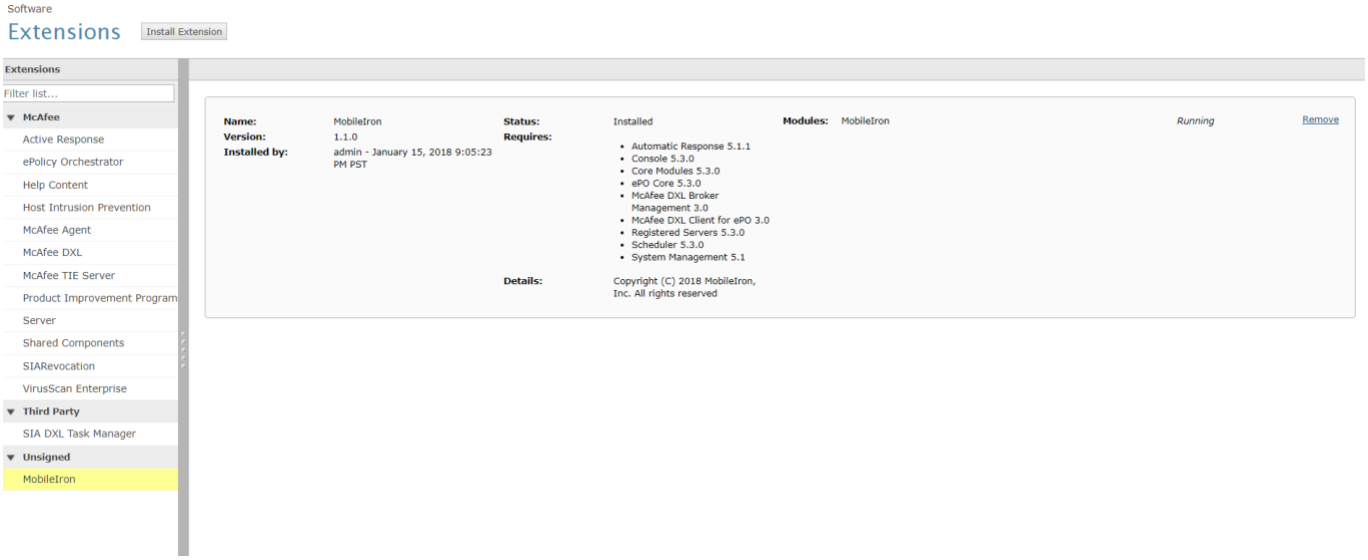




Integration Workflow:

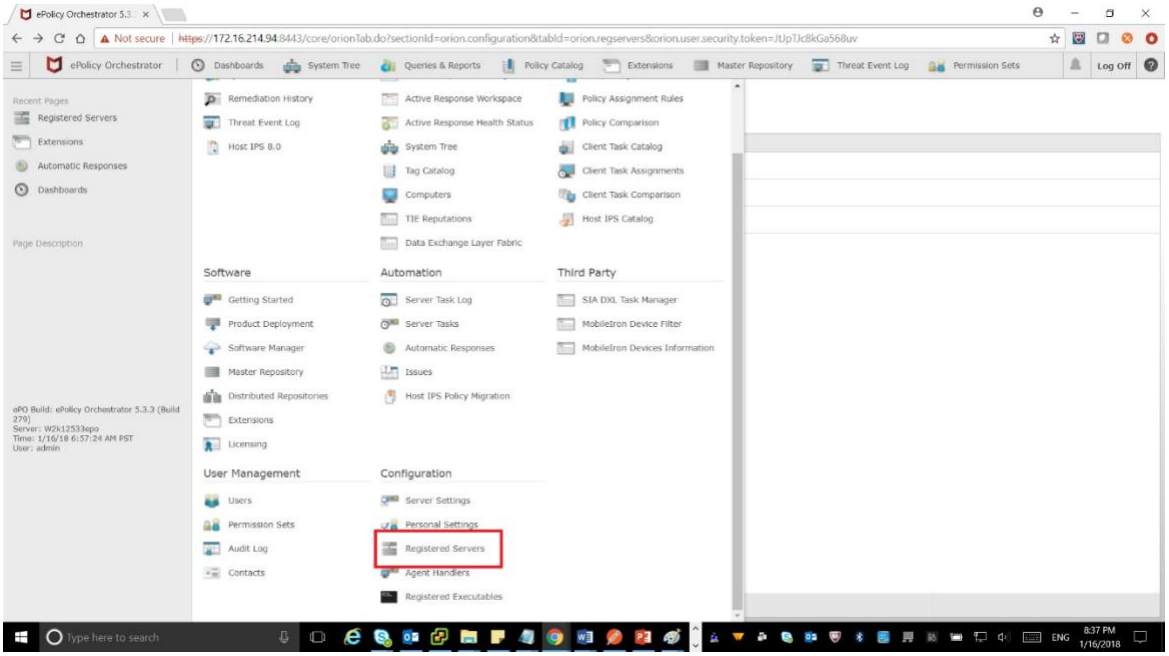
Install the MobileIron Extension by following these steps:

1. Navigate to Menu->Software->Extensions
2. Select Install Extension button at the top of the page
3. In the pop up, select Choose File
4. Navigate to the location of MobileIron Extension
5. Select OK on the summary page
6. A new listing under signed Third Party will display “MobileIron.”
7. Selecting “MobileIron” will display an item Name: MobileIron Version: 1.0.0, as seen below

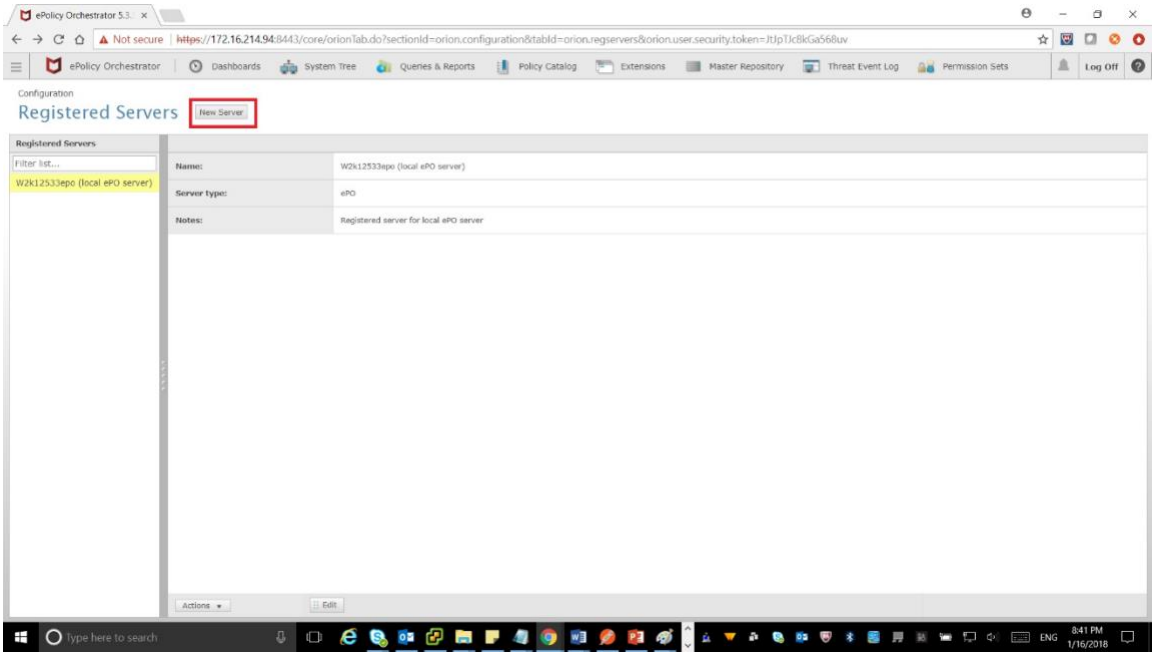


Configure Registered Server: -

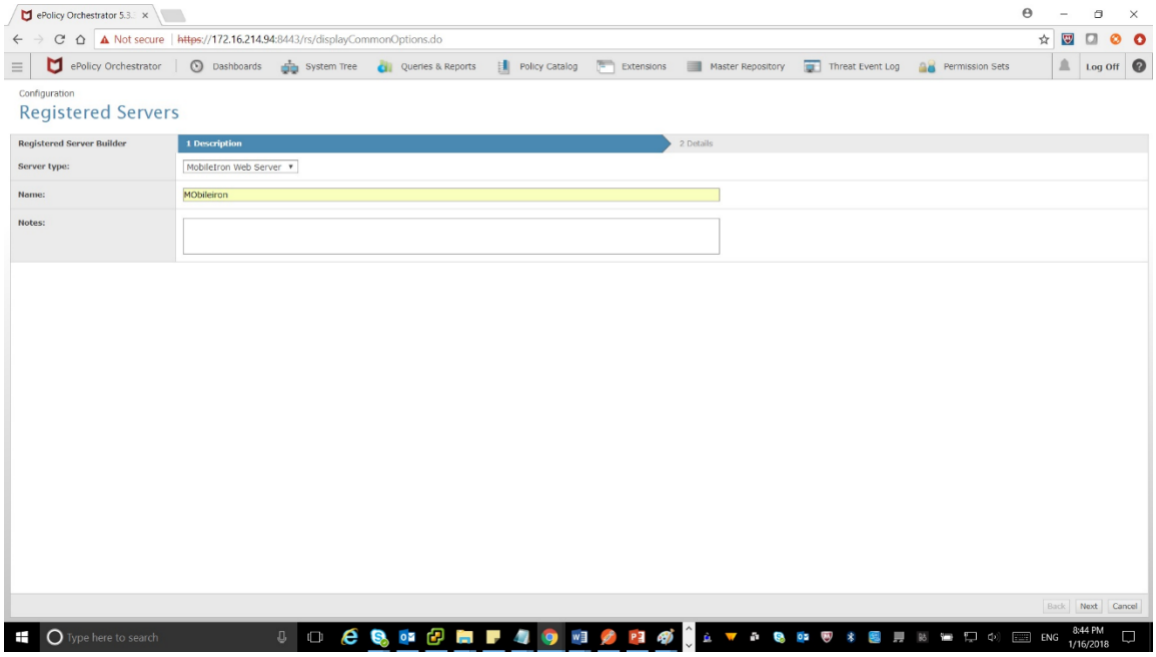
After installation of MobileIron extension on ePO server we should configure the Registered server on ePO.



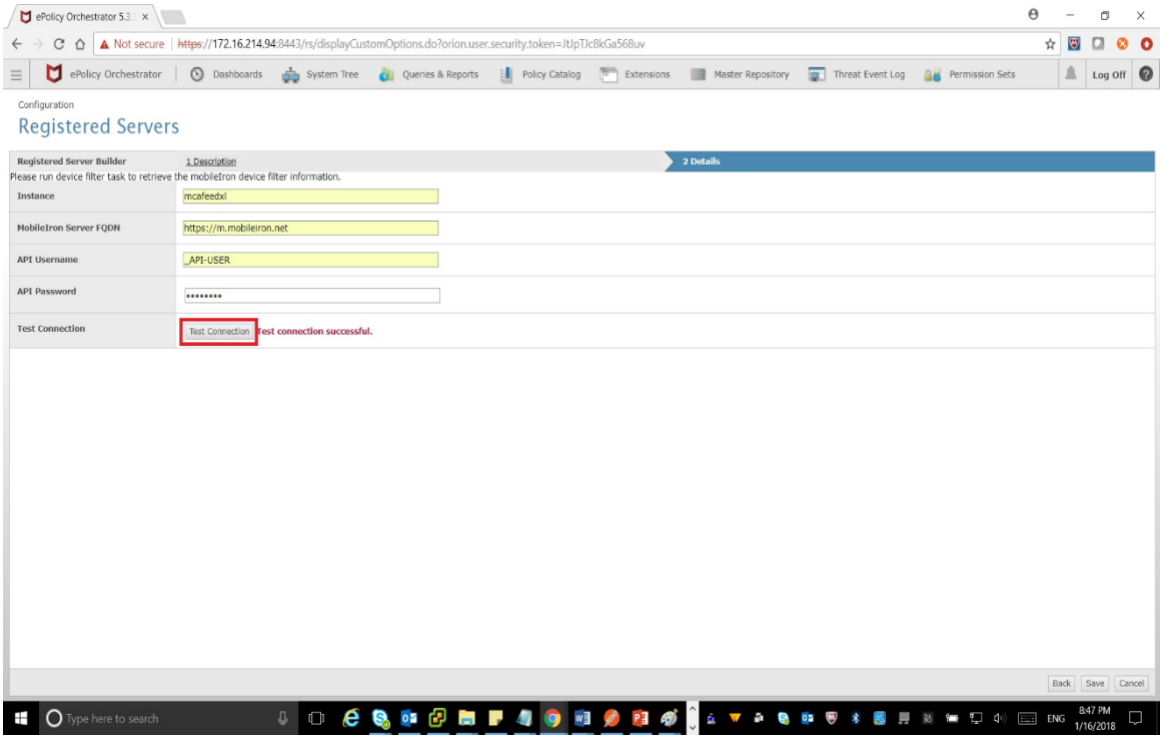
1. Click on Register servers tab
2. And then click new server button



3. Select MobileIron webserver from the server type list, and click next button



4. MobileIron Server configuration information can be provided in this section. User needs to fill in the Server URL and the authentication parameters like username and password. User can test the connection before saving the configuration.



Configure and Schedule Server Tasks: -

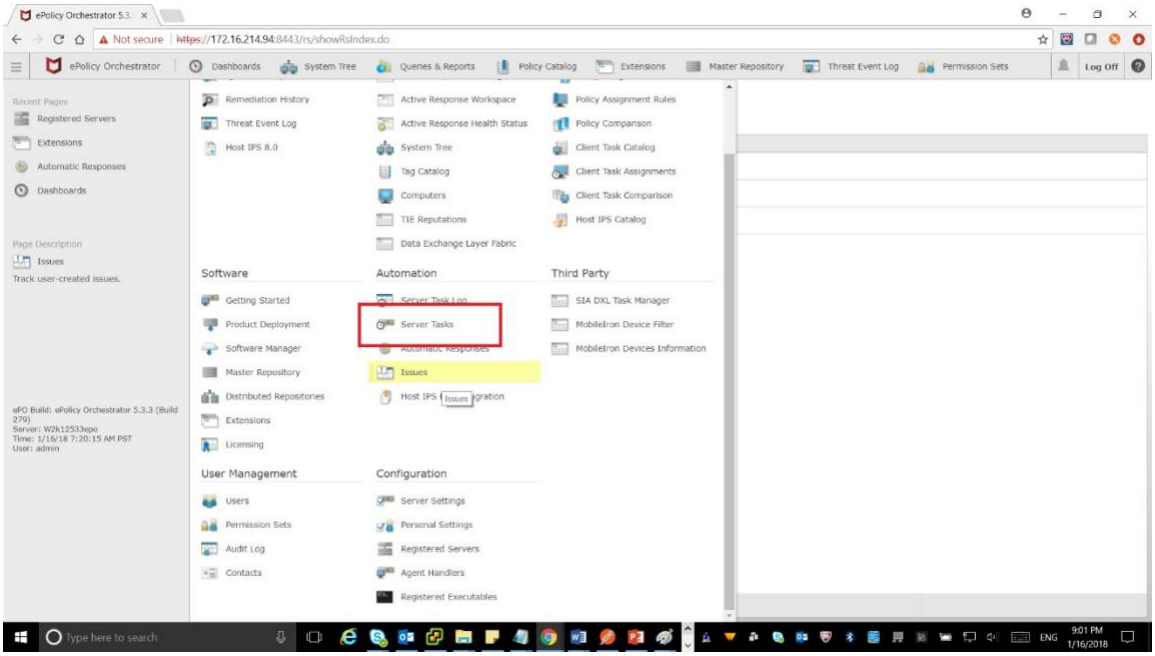
There are three default tasks which are created on installation of MobileIron extension on ePO: -

1. MobileIron: Device Filters Update Task
2. MobileIron: Device Information Update Task
3. MobileIron: Post Windows 10 Events Task

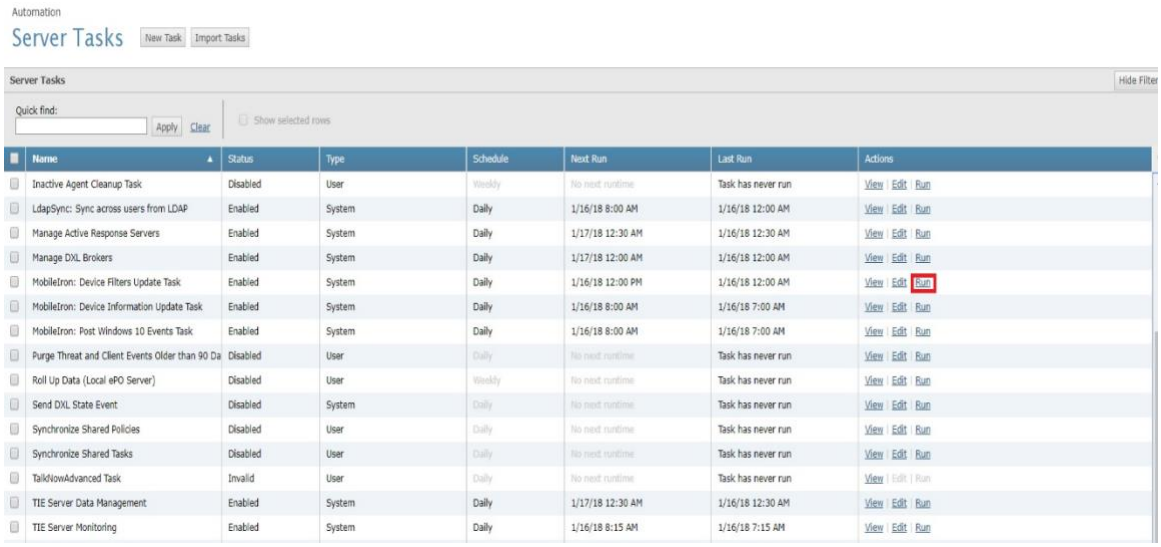
MobileIron: Device Filters Update server task

Please make sure to have saved the MobileIron Rest configuration in the Registered server page created for MobileIron.

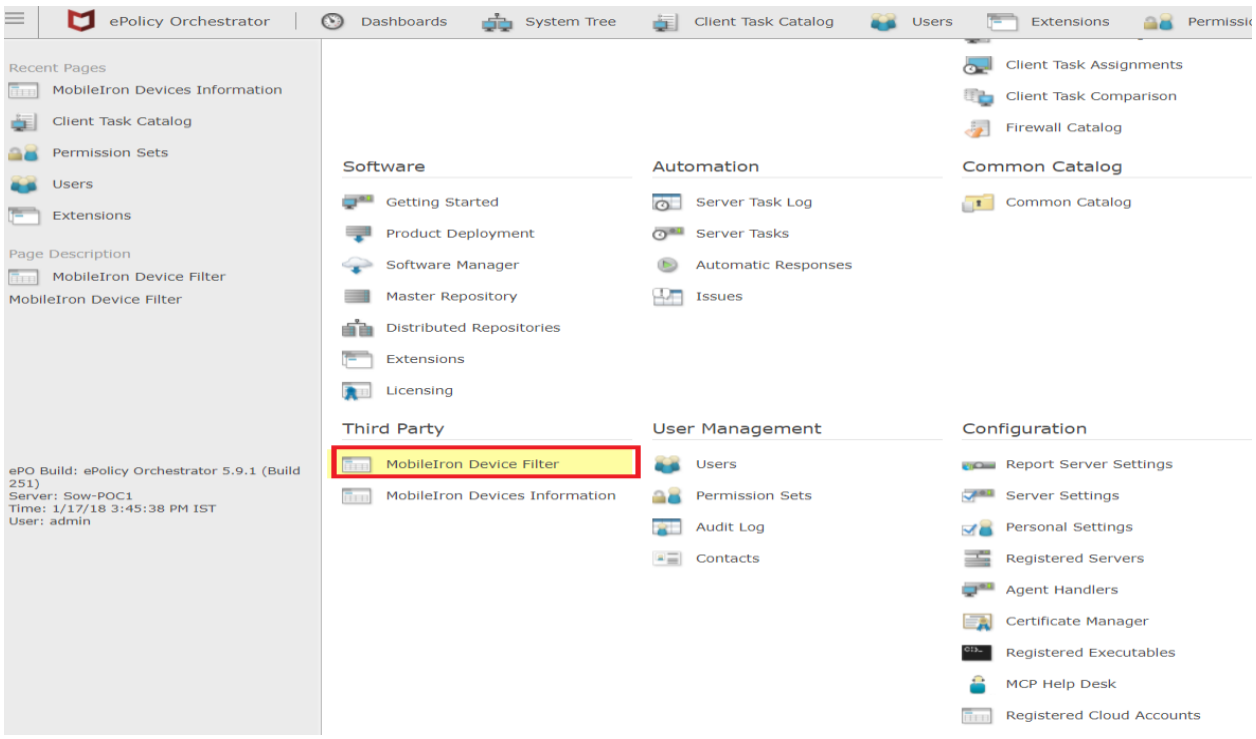
1. Navigate to ePO menu->Automation->Server Tasks

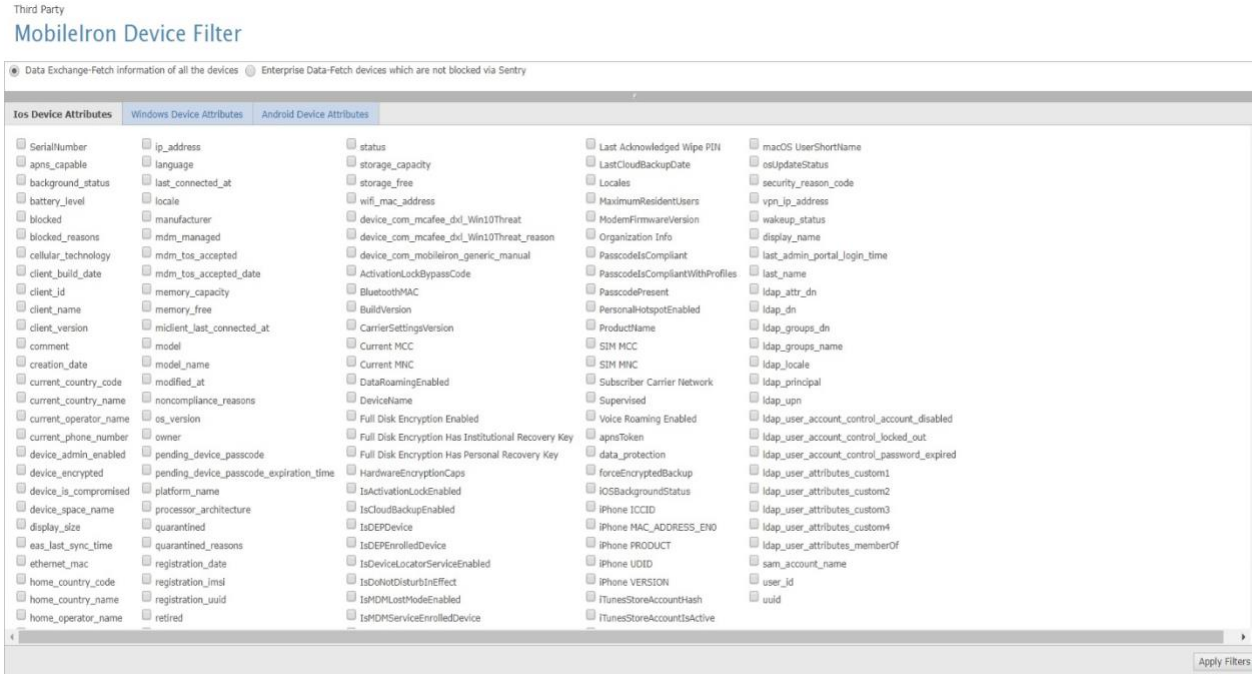


2. Select MobileIron device filter server task and click on run button.



3. Once the MobileIron device filter update task is completed successfully, user can view the list of device filters on MobileIron device filter tab on third party page.


ePolicy Orchestrator
Dashboards
System Tree
Client Task Catalog
Users
Extensions
Recent Pages
MobileIron Devices Information
Client Task Catalog
Permission Sets
Users
Extensions
Page Description
MobileIron Device Filter
MobileIron Device Filter
ePO Build: ePolicy Orchestrator 5.9.1 (Build 251)
Server: Sow-POC1
Time: 1/17/18 3:45:38 PM IST
User: admin
Client Task Assignments
Client Task Comparison
Firewall Catalog
Software
Getting Started
Product Deployment
Software Manager
Master Repository
Distributed Repositories
Extensions
Licensing
Automation
Server Task Log
Server Tasks
Automatic Responses
Issues
Common Catalog
Common Catalog
Third Party
MobileIron Device Filter
MobileIron Devices Information
User Management
Users
Permission Sets
Audit Log
Contacts
Configuration
Report Server Settings
Server Settings
Personal Settings
Registered Servers
Agent Handlers
Certificate Manager
Registered Executables
MCP Help Desk
Registered Cloud Accounts


Third Party
MobileIron Device Filter
Data Exchange-Fetch information of all the devices
Enterprise Data-Fetch devices which are not blocked via Sentry
Ios Device Attributes
Windows Device Attributes
Android Device Attributes
SerialNumber
apns_capable
background_status
battery_level
blocked
blocked_reasons
cellular_technology
client_build_date
client_id
client_name
client_version
comment
creation_date
current_country_code
current_country_name
current_operator_name
current_phone_number
device_admin_enabled
device_encrypted
device_is_compromised
device_space_name
display_size
eas_last_sync_time
ethernet_mac
home_country_code
home_country_name
home_operator_name
ip_address
language
last_connected_at
locale
manufacturer
mdm_managed
mdm_tos_accepted
mdm_tos_accepted_date
memory_capacity
memory_free
miclient_last_connected_at
model
model_name
modified_at
noncompliance_reasons
os_version
owner
pending_device_passcode
pending_device_passcode_expiration_time
platform_name
processor_architecture
quarantined
quarantined_reasons
registration_date
registration_imsi
registration_uuid
retired
status
storage_capacity
storage_free
wifi_mac_address
device_com_mcafee_dxl_Win10Threat
device_com_mcafee_dxl_Win10Threat_reason
device_com_mobileiron_generic_manual
ActivationLockBypassCode
BluetoothMAC
BuildVersion
CarrierSettingsVersion
Current MCC
Current MNC
DataRoamingEnabled
DeviceName
Full Disk Encryption Enabled
Full Disk Encryption Has Institutional Recovery Key
Full Disk Encryption Has Personal Recovery Key
HardwareEncryptionCaps
IsActivationLockEnabled
IsCloudBackupEnabled
IsDEPDevice
IsDEPEnrolledDevice
IsDeviceLocatorServiceEnabled
IsDoNotDisturbInEffect
IsMDMLostModeEnabled
IsMDMServiceEnrolledDevice
Last Acknowledged Wipe PIN
LastCloudBackupDate
Locales
MaximumResidentUsers
ModemFirmwareVersion
Organization Info
PasscodeIsCompliant
PasscodeIsCompliantWithProfiles
PasscodePresent
PersonalHotspotEnabled
ProductName
SIM MCC
SIM MNC
Subscriber Carrier Network
Supervised
Voice Roaming Enabled
apnsToken
data_protection
forceEncryptedBackup
iOSBackgroundStatus
iPhone ICCID
iPhone MAC_ADDRESS_EN0
iPhone PRODUCT
iPhone UDID
iPhone VERSION
iTunesStoreAccountHash
iTunesStoreAccountIsActive
macOS UserShortName
osUpdateStatus
security_reason_code
vpn_ip_address
wakeup_status
display_name
last_admin_portal_login_time
last_name
ldap_attr_dn
ldap_dn
ldap_groups_dn
ldap_groups_name
ldap_locale
ldap_principal
ldap_upn
ldap_user_account_control_account_disabled
ldap_user_account_control_locked_out
ldap_user_account_control_password_expired
ldap_user_attributes_custom1
ldap_user_attributes_custom2
ldap_user_attributes_custom3
ldap_user_attributes_custom4
ldap_user_attributes_memberOf
sam_account_name
user_id
uuid
Apply Filters

Mobileiron Device Filter tab: -

MobileIron Device filters are classified into 4 categories “**Android**”,” **Windows**”,” **IOS**” and “**Common**” based on the user requirement filters can be selected and saved.

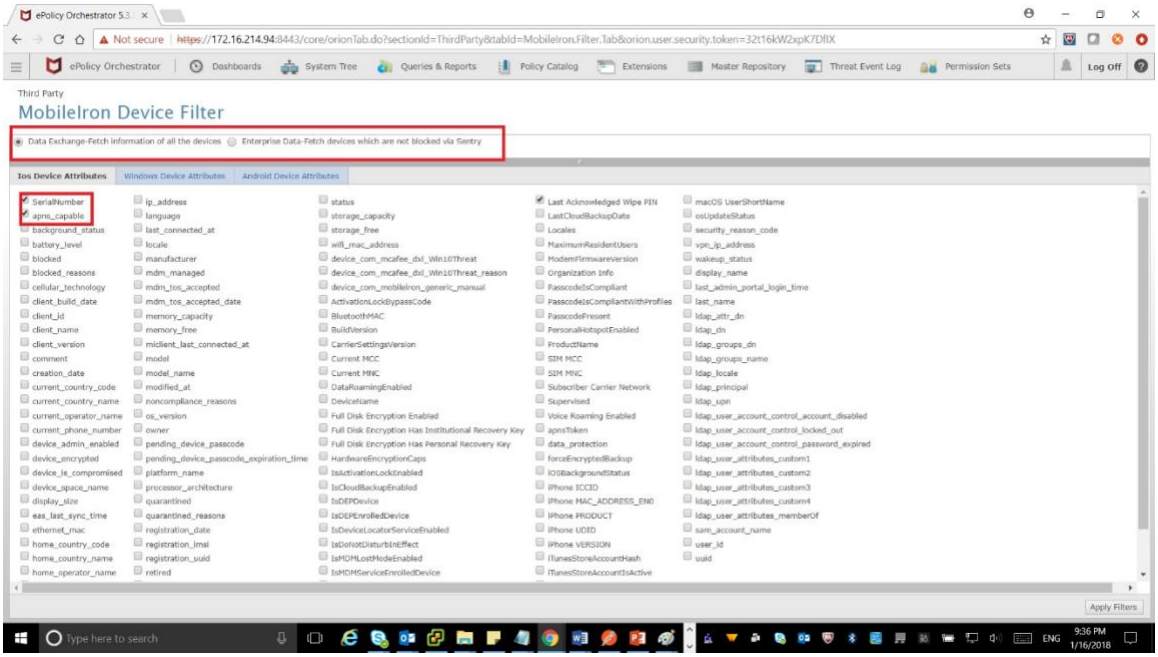
User can also select the type of devices to be fetched from Data Exchange by selecting the radio button

Data Exchange-Fetch information of all the devices: -

- If you select this radio button all the device information will be fetched from MobileIron server.

Data Exchange -Fetch devices which are not blocked via Sentry: -

- If you select this radio button only non-blocked device information will be fetched from MobileIron server.

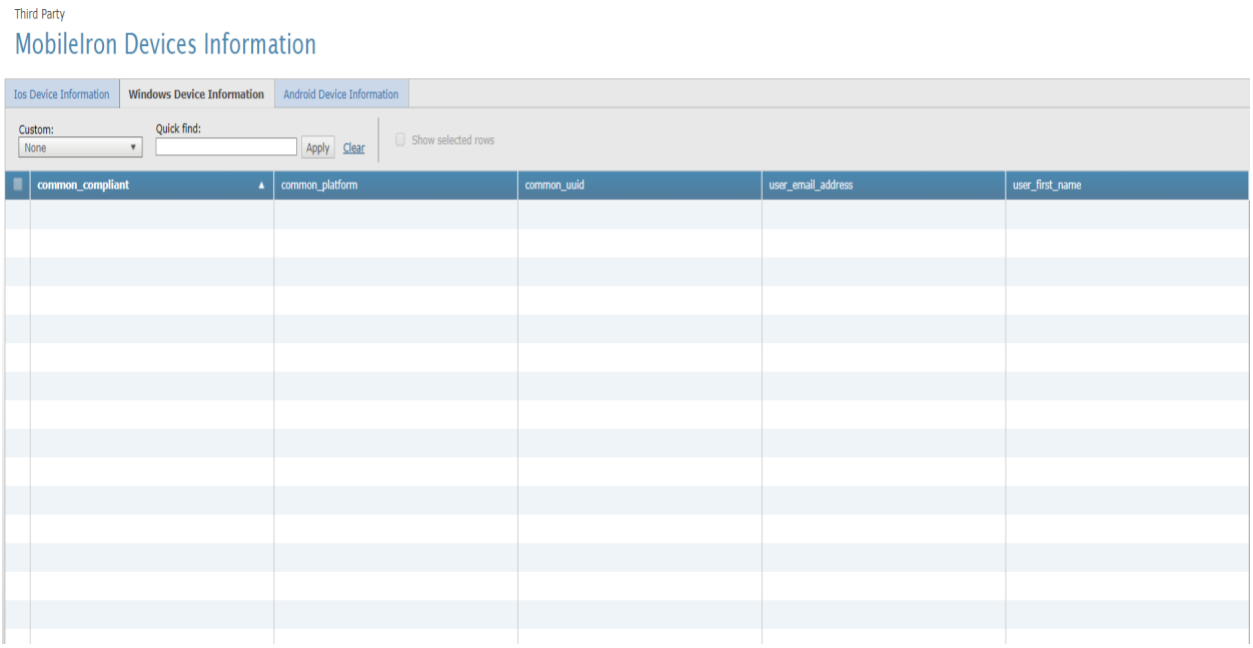


Based on the filters selected we will query the MobileIron Server to get list of devices.

MobileIron Device information tab:

This tab displays MobileIron device information for the selected filters.

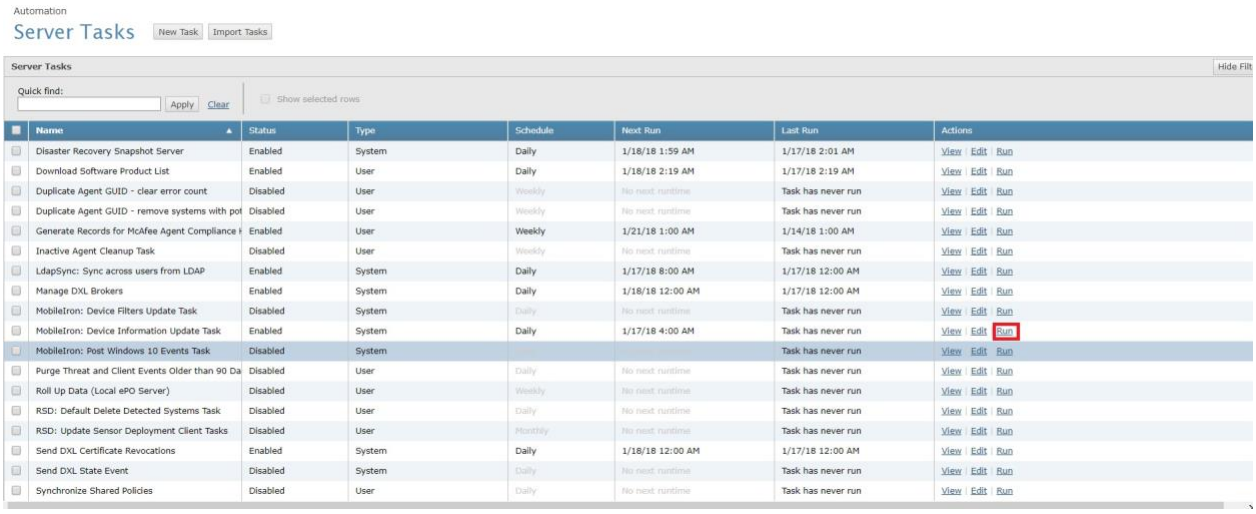
By default, five mandatory filters (i.e. common_complaint, common_platform, common_uuid, user_email_address, user_first_name) will be selected and displayed for all the platforms on the device information table.



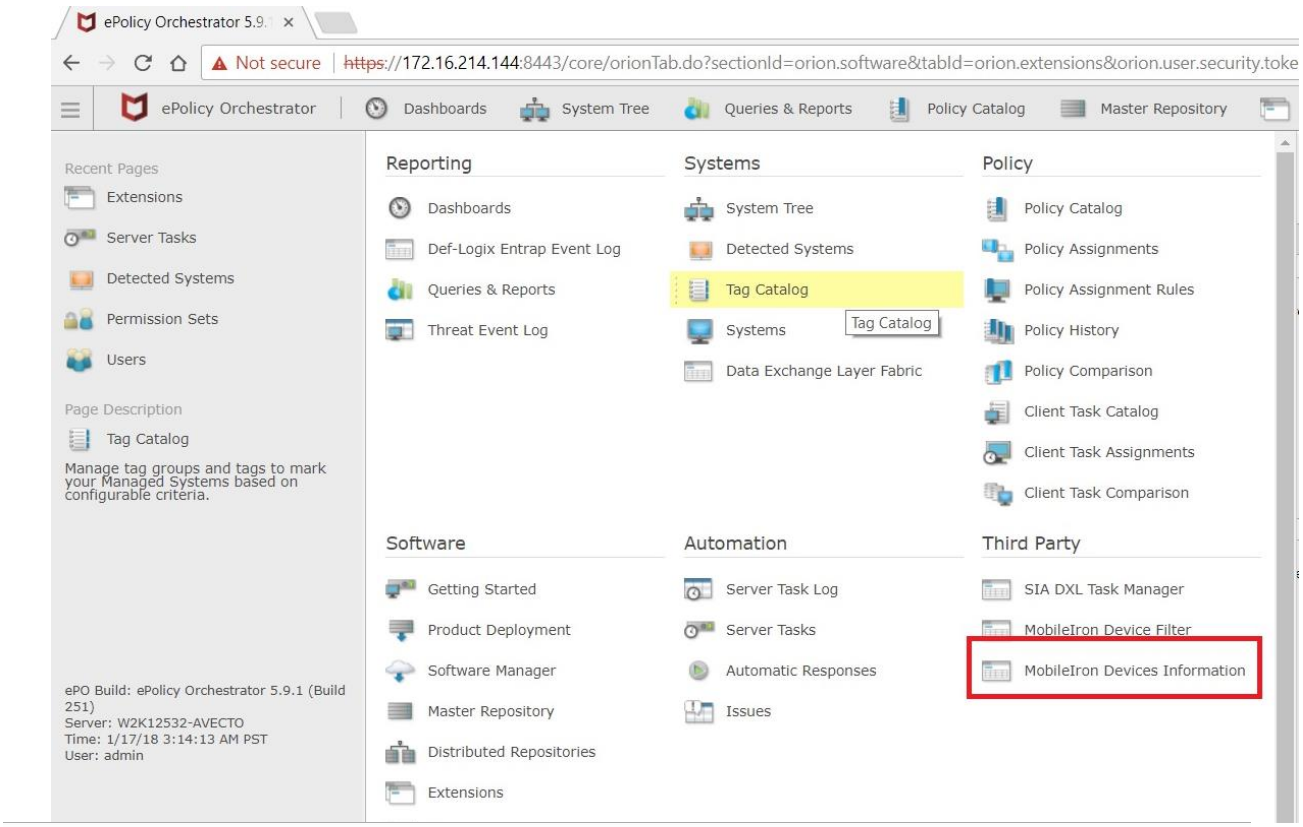
MobileIron: Device Information Update Task: -

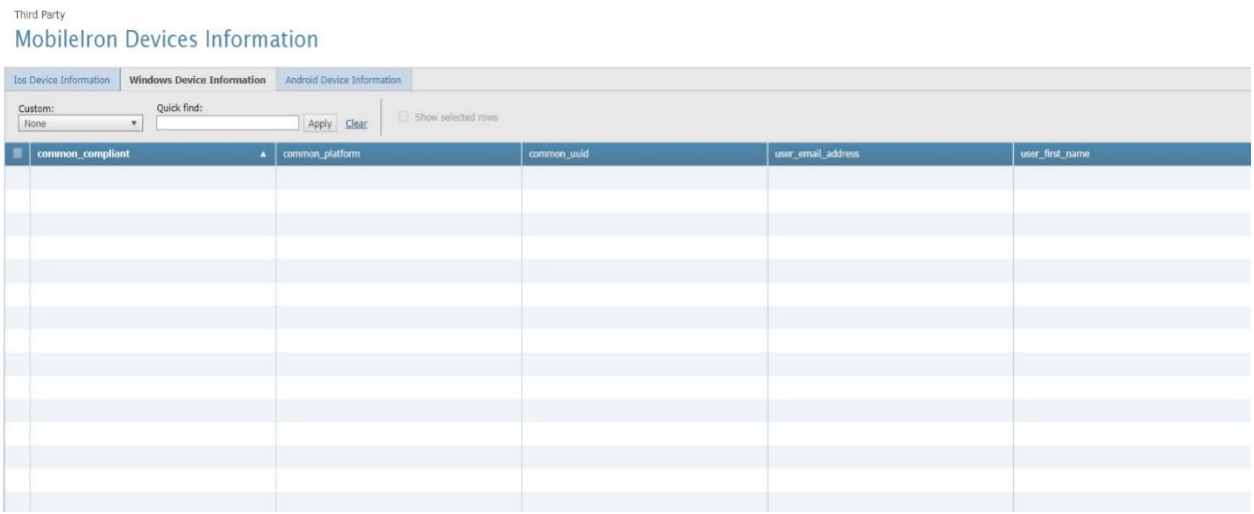
Please make sure to have saved the MobileIron Rest configuration in the Registered server page created for MobileIron.

1. Navigate to ePO menu->Automation->Server Tasks
2. Select MobileIron device information server task and click on run button.



1. Once the task is successfully completed, information pulled by running the task can viewed as part of “MobileIron Device Information” in the third-party page.





Actions: -

Action menu provides list of action which can be performed on the devices retrieved from the MobileIron server

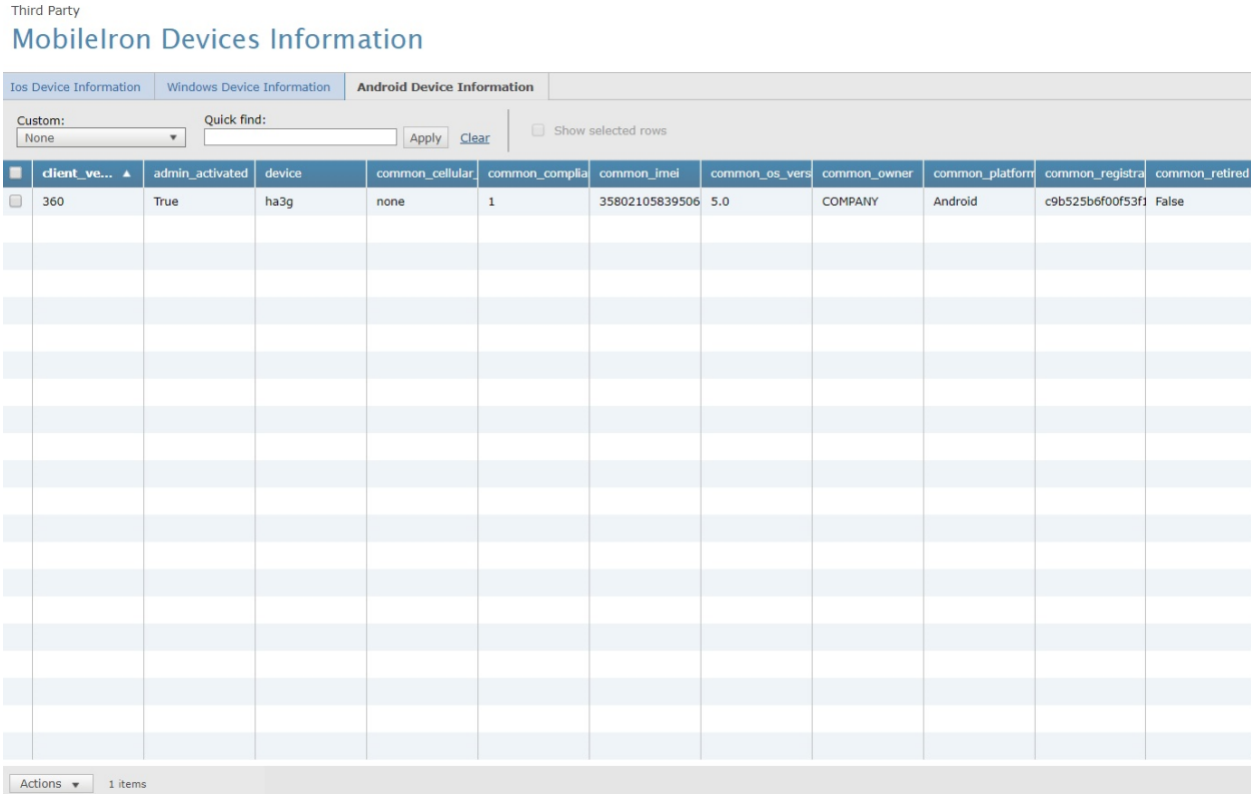
Below is the list of actions: -

- Pull device information
- Lock device
- Retire device
- Unlock device

- Wipe device

Pull device information: -

This action Pulls the information for the selected filters from the MobileIron server and will be displayed on device information tab inside third-party section. This action can also be performed by running the MobileIron device information update server task.



Lock device: -

This action sends lock device request to MobileIron server for the selected device.

Note: - (To complete this action a pop up will be triggered asking for the reason to send the lock request.)

Retire Device: -

This action sends retire device request to MobileIron server for the selected device.

Note: - (To complete this action a pop up will be triggered asking for the confirmation to send the retire request.)

Un-lock device: -

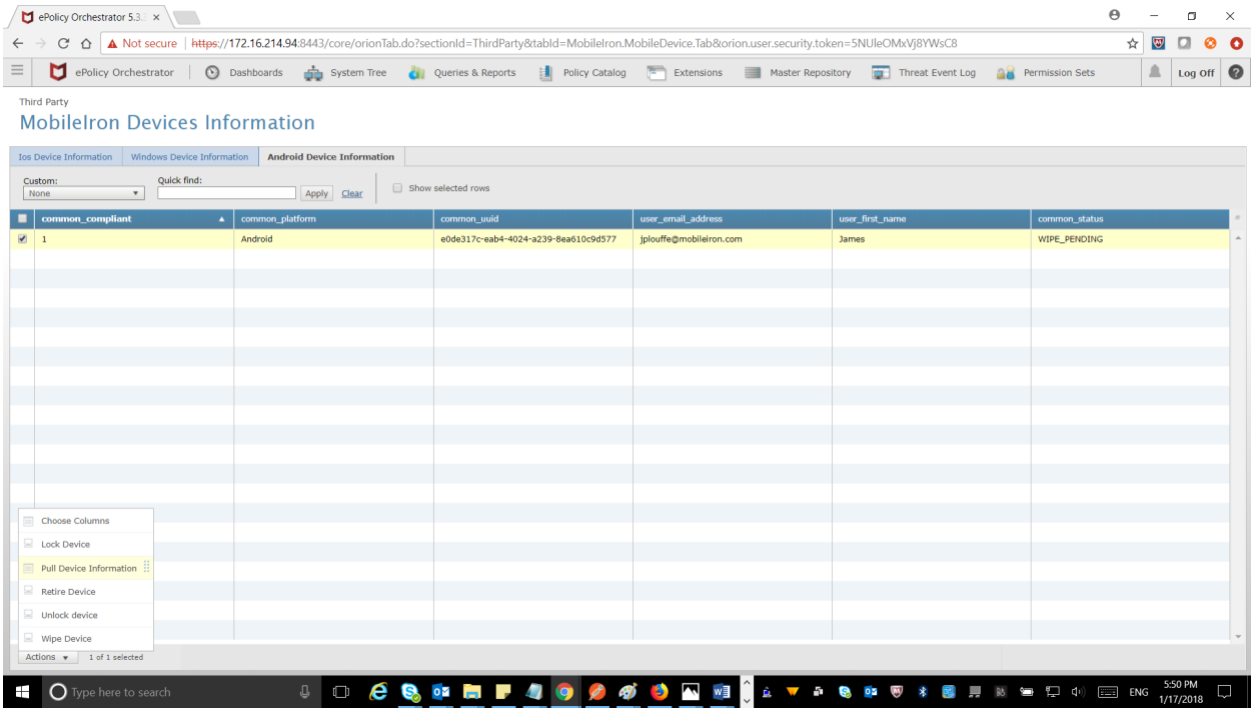
This action sends un-lock device request to MobileIron server for the selected device.

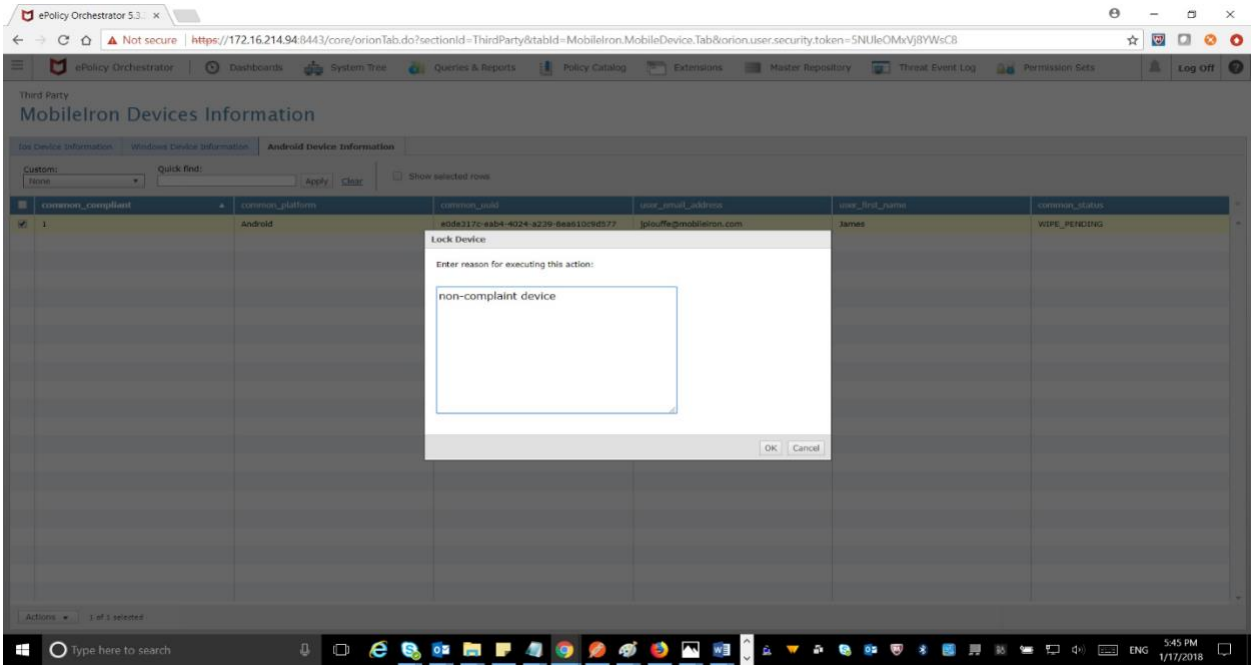
Note: - (To complete this un-action a pop up will be triggered asking for the reason to send the un-lock request.)

Wipe device: -

This action sends wipe device request to MobileIron server for the selected device.

Note: - (To complete this action a pop up will be triggered asking for the reason to send the wipe request.)





Pushing of windows 10 Events to MobileIron server:

This task involves sending windows 10 events at regular intervals. The intervals can be configured as part of the server task designated for the same.

List of attributes provided by McAfee as part of threat events:

- AutoID
- AnalyzerHostName
- SourceMAC
- SourceIPV4
- ThreatName
- ThreatType
- ThreatSeverity
- ThreatEventID
- AnalyzerMAC

As part of this task events generated for windows 10 systems that are managed by both ePO and MobileIron server are queried from the ePO database and sent to the MobileIron server. This task can be scheduled as required.

Publishing DXL Events: -

When retrieving device information from the MobileIron server, information related to non-compliance of the devices will be published to the dxl-fabric.

This information can be consumed by anyone who subscribes to the below mentioned topic

Topic Name:

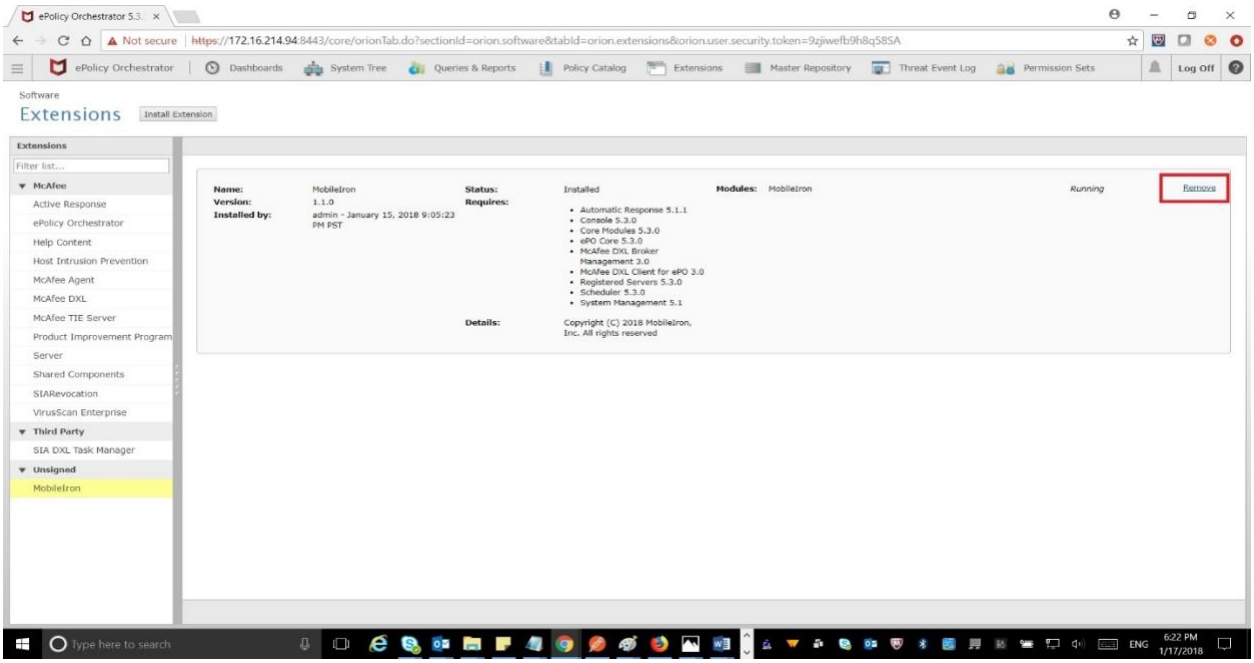
/open/compliance/devices/mobileIron

Payload Details: -


```
{
"msgType":"McAfee Compliance Report",
  "msgVersion":"1.0",
  "compliance":{
    "compliant":false,
    "entity":{
      "id":"e08d135e-7f77-4e52-9dc6-baec2e15acf5",
      "osType":"iPhone OS 10.2.1 (14D27)",
      "osPlatform":"iOS"
      "wifi_mac_address":"5cc30703a1b0"
   },
    "source":{
      "userName":"xxxxx@mobileiron.com"
    },
    "otherData":{
      "lastConnectedAt":"2017-04-21T10:46:01.000Z",
      "miClientLastConnectedAt":"2017-04-21T10:46:01.000Z",
      "status":"ACTIVE",
      "blocked":false
    }
  }
}
```

Uninstalling ePO Integration

To uninstall this integration, go to Extensions and select “MobileIron” extension from the extension list. Click on “Remove” to uninstall this integration.



Reporting

Query Targets

- MobileIron android devices
- MobileIron IOS devices
- MobileIron windows devices
- MobileIron custom devices

<List all the Query Targets (Query targets means registering the custom table with ePO Query builder framework) used by the point product>

Useful Logs

Log files are placed in “C:\Program Files\McAfee\ePolicy orchestrator\Server\Logs\orion.log”

Release Notes

- DXL dependency is made optional so that users who don’t want to publish MobileIron dxl non-complaint events on dxl fabric.