MobileIron and Cisco

Identity Services Engine Configuration Guide

November 2018
Version 1.0

www.mobileiron.com

Copyright Notice

© 2018 MobileIron, Inc. All rights reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies’ trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.

MobileIron, Inc.
401 East Middlefield Road
Mountain View, CA 94043

MobileIron and Cisco ISE Configuration

What is Cisco ISE? 4
Getting MobileIron ready for Cisco ISE 4
Configuring MobileIron to support Cisco ISE calls 4
Core (On-Premise) 4
Step 1: Create an account 5
Step 2: Assign API role 5
Cloud 6
Step 1: Determine the cluster your instance belongs to 6
Step 2: Assign the ISE role to the user 8
Add MDM server to Cisco ISE Admin Portal 10
Cisco ISE API guide 12
Supported API's (triggered from ISE) 12
Examples of API data returned from Cloud to ISE 13
API Call: Retrieve basic information about tenant including version 13
API Call: retrieve information about a device 14
API Call: Retrieve devices that are out of compliance 16
API Call: Lock the device if a device passcode is present 21

What is Cisco ISE?

Cisco Identity Service Engine (ISE) is usually deployed with Cisco WiFi Access Points as a form of NAC (Network Access Control). Based on identity information received from Cisco ISE, decisions are made whether or not to allow a device to join a network

Cisco ISE now integrates with the two major components of MobileIron's Unified Endpoint Management (UEM) platform -- MobileIron Core (on-premise) and MobileIron Cloud -- to receive security posture information about mobile devices and tablets. Supported UEM device actions available from the Cisco ISE portal include Pin Locking, which locks a device but does not impose or set a new PIN, and Full Device Wipe.

Additional ISE-originated commands may be available in future releases. MobileIron Cloud supports Version 2 of Cisco ISE APIs. A silver MobileIron Cloud license is necessary to enable the ISE integration.

Note: the industry naming convention for mobility management software has changed from Mobile Device Management (MDM) to Enterprise Mobility Management (EMM), to its most recent classification in 2018 of Unified Endpoint Management (UEM). Because MobileIron's underlying code still contains references to the original "mdm", we will use MDM throughout this document when referring to MobileIron's solutions.

Getting MobileIron ready for Cisco ISE

First, basic connectivity must be established between the Cisco ISE server and the MobileIron MDM server. In both the on-premise and cloud models, a firewall is typically located between the two servers. The firewall should be configured to allow an HTTPS session from ISE located in the data center to the MDM server located in either the corporate DMZ or public Internet. The session is established outbound from ISE towards the MDM where ISE takes the client role. This is a common direction for Web traffic through corporate firewalls.

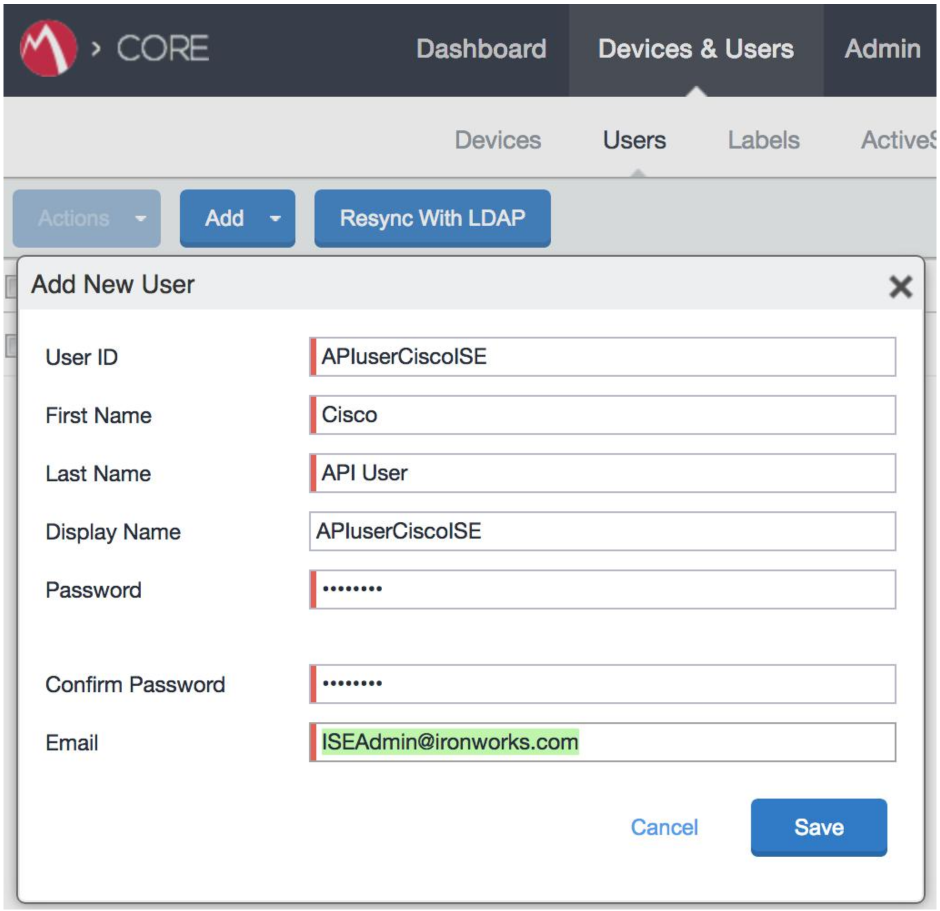
Configuring MobileIron to support Cisco ISE calls

Core (On-Premise)

The MobileIron MDM API is protected by HTTPS and requires a user account that has been granted permission to the API. Ideally, a specific account would be configured for ISE with a very strong password. In addition to this account, only a limited number of administrator accounts should be granted the ability to create new administrators or assign administrator roles.

Step 1: Create an account

Creating local user accounts is accomplished by logging into the Mobileiron Core admin portal >> Devices and Users >> Add >> Add Local Users



Add New User

User ID	APIuserCiscoISE
First Name	Cisco
Last Name	API User
Display Name	APIuserCiscoISE
Password	••••••••
Confirm Password	••••••••
Email	ISEAdmin@ironworks.com

Step 2: Assign API role

Once the account has been created, it is assigned roles to allow ISE access to the API Role. To do this, Mobileiron Core admin portal >> Admin >> Select the user >> Actions >> Edit Roles >> scroll to other roles and select API

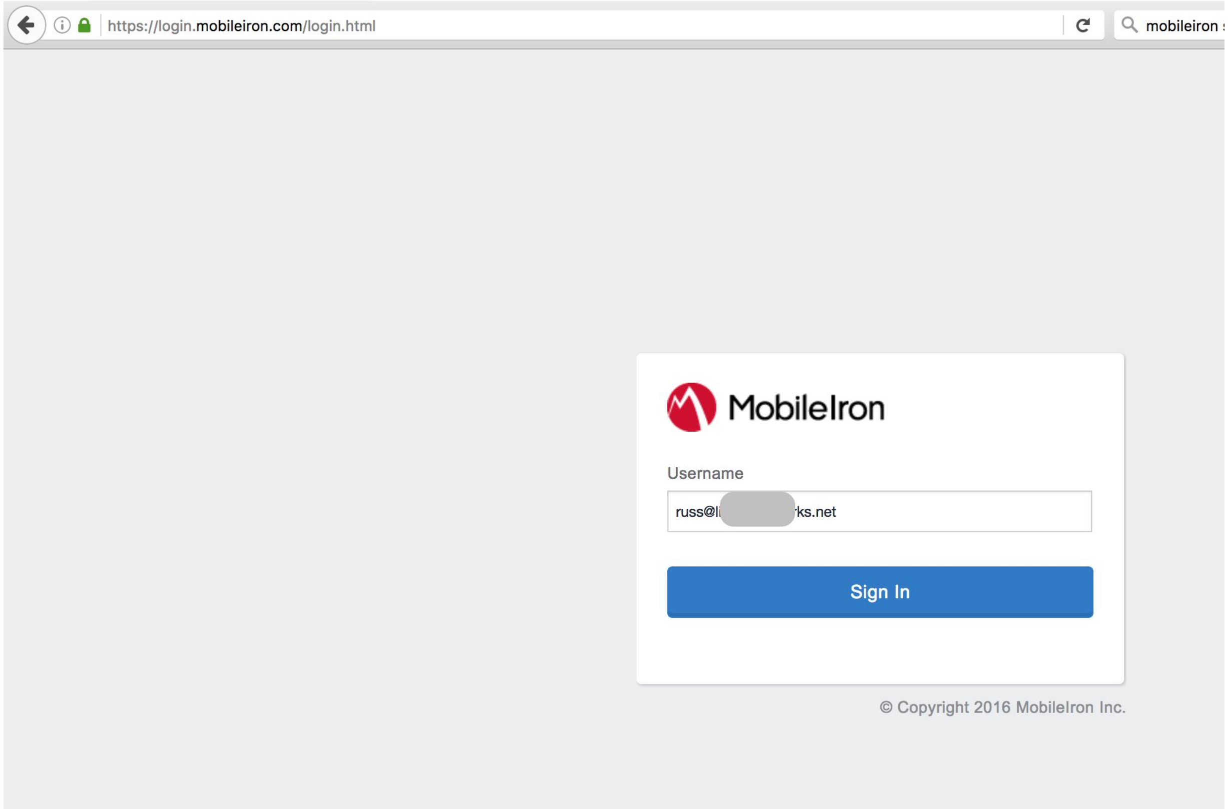
Note: Ensure the local user is in the delegated admin space that will allow the privilege to get the API Role

Cloud

First, you will need to determine which cluster you belong to. You will need to enter this information in the **Hostname or IP Address field** on the Cisco ISE platform later.

Step 1: Determine the cluster your instance belongs to

From Chrome, Firefox, or Safari, log onto your instance from the URL https://login.mobileiron.com



https://login.mobileiron.com/login.html

Username: russ@l[redacted]ks.net

Your Cluster will be displayed in the URL bar after your username is entered. Valid options include:

na1.mobileiron.com

na2.mobileiron.com

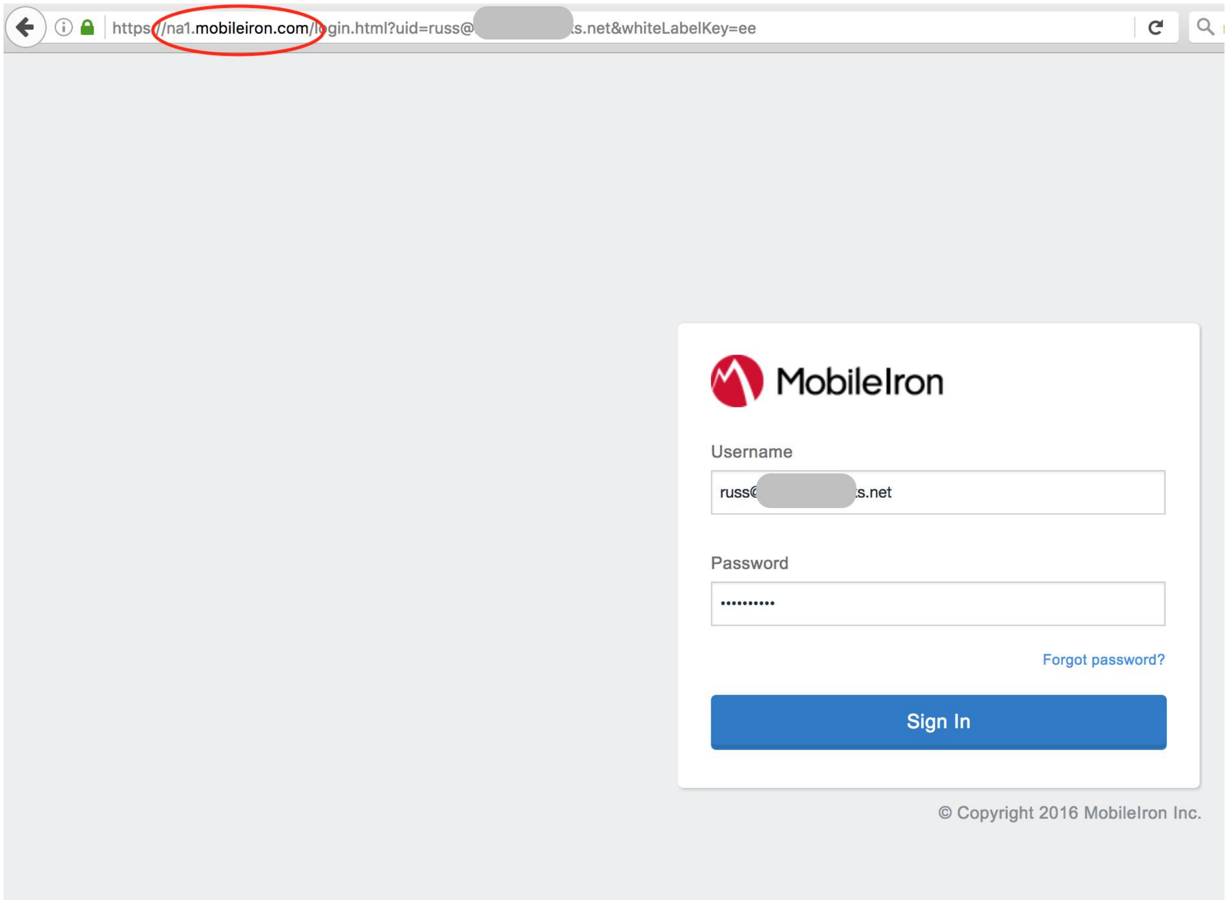
na3.mobileiron.com

eu1.mobileiron.com

ap1.mobileiron.com

ap2.mobileiron.com

sandbox.mobileiron.com (internal testing only)



https://na1.mobileiron.com/login.html?uid=russ@[redacted]s.net&whiteLabelKey=ee

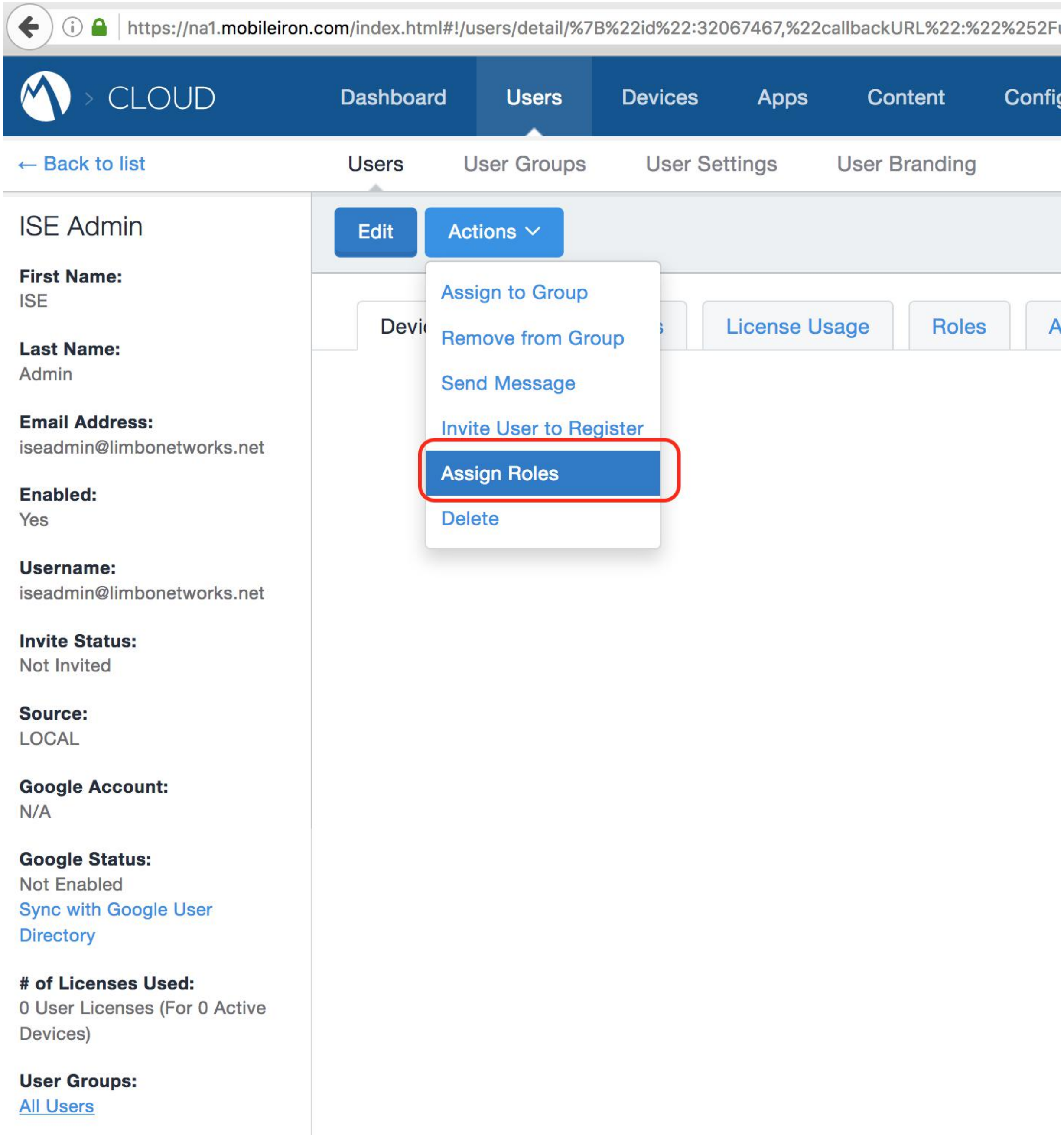
Username: russ@[redacted]s.net

Password: ••••••••••

Step 2: Assign the ISE role to the user

Next, create a user on MobileIron Cloud and assign the ISE role to them.

Navigate to Users and select the user you would like to assign the **Cisco ISE Operations** role to. This user's credentials will be configured on the Cisco ISE Admin portal. You do not need to select all of the roles for the Cisco ISE user, only the **Cisco ISE Operations** role is necessary.



ISE Admin

First Name:
ISE

Last Name:
Admin

Email Address:
iseadmin@limbonetworks.net

Enabled:
Yes

Username:
iseadmin@limbonetworks.net

Invite Status:
Not Invited

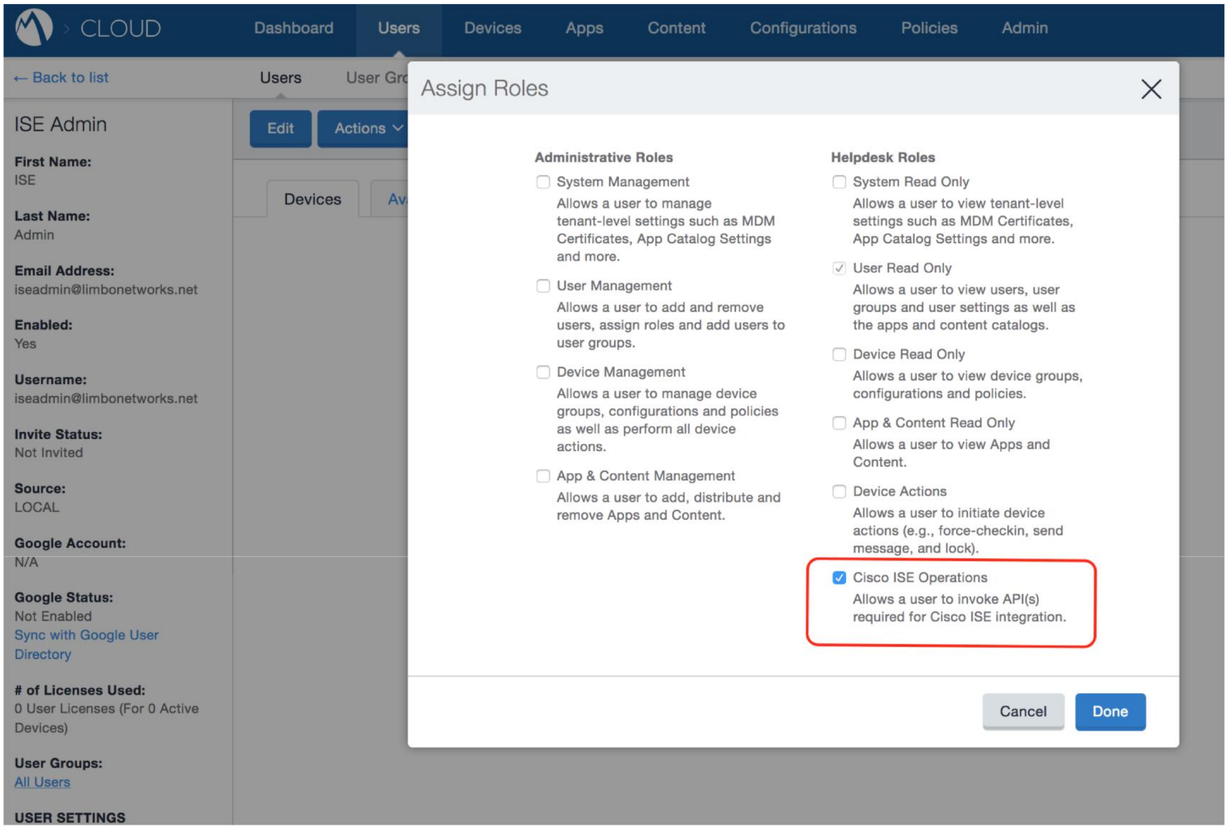
Source:
LOCAL

Google Account:
N/A

Google Status:
Not Enabled
Sync with Google User Directory

# of Licenses Used:
0 User Licenses (For 0 Active Devices)

User Groups:
All Users



ISE Admin

First Name: ISE

Last Name: Admin

Email Address: iseadmin@limbonetworks.net

Enabled: Yes

Username: iseadmin@limbonetworks.net

Invite Status: Not Invited

Source: LOCAL

Google Account: N/A

Google Status: Not Enabled
Sync with Google User Directory

# of Licenses Used: 0 User Licenses (For 0 Active Devices)

User Groups: All Users

USER SETTINGS

Assign Roles

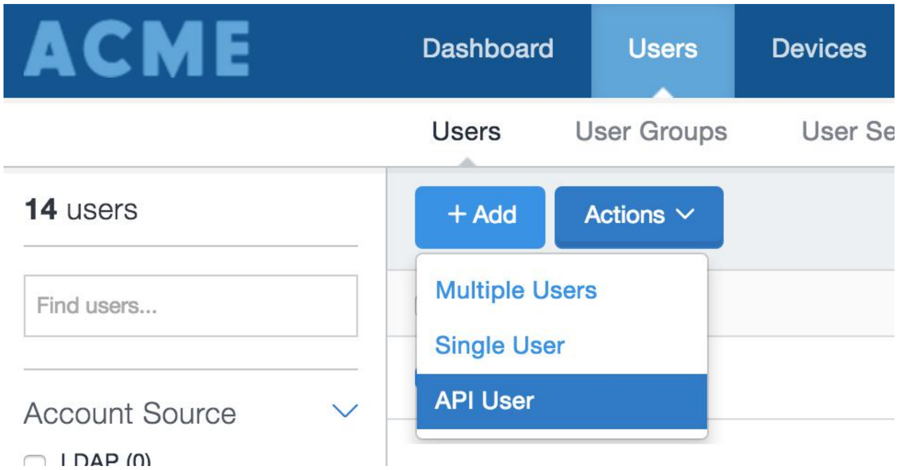
Administrative Roles

- □ System Management
  Allows a user to manage tenant-level settings such as MDM Certificates, App Catalog Settings and more.
- □ User Management
  Allows a user to add and remove users, assign roles and add users to user groups.
- □ Device Management
  Allows a user to manage device groups, configurations and policies as well as perform all device actions.
- □ App & Content Management
  Allows a user to add, distribute and remove Apps and Content.

Helpdesk Roles

- □ System Read Only
  Allows a user to view tenant-level settings such as MDM Certificates, App Catalog Settings and more.
- ☑ User Read Only
  Allows a user to view users, user groups and user settings as well as the apps and content catalogs.
- □ Device Read Only
  Allows a user to view device groups, configurations and policies.
- □ App & Content Read Only
  Allows a user to view Apps and Content.
- □ Device Actions
  Allows a user to initiate device actions (e.g., force-checkin, send message, and lock).
- ☑ Cisco ISE Operations
  Allows a user to invoke API(s) required for Cisco ISE integration.

Alternate method: You may also navigate to **Users**and select **Add+.** You will have the option to add an API User that does not have **access to the admin portal.**

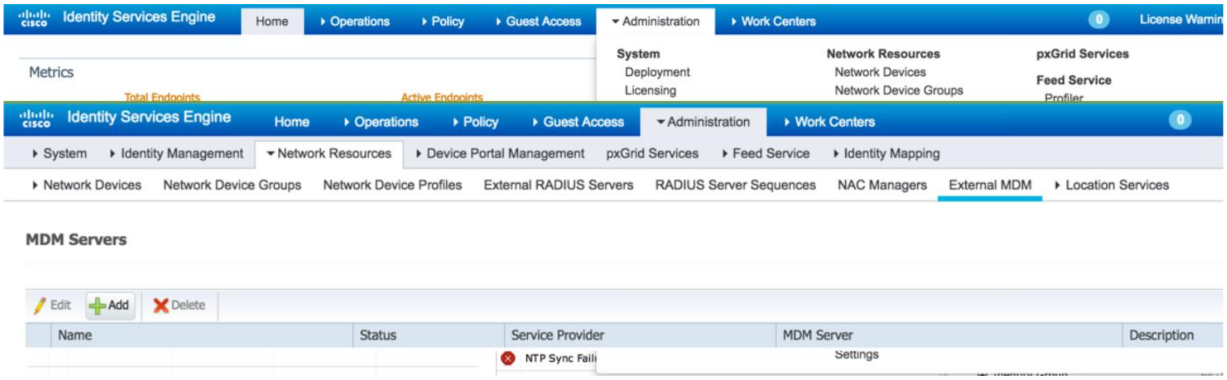


You can now log into the Cisco ISE portal to continue the configuration.

Add MDM server to Cisco ISE Admin Portal

Once the account has been defined on the MobileIron MDM server with the proper roles, ISE can be configured to use this account when querying the MDM for device information. ISE will contact the MDM to gather posture information about devices or to issue device commands, such as corporate wipe or lock. The session is initiated from ISE towards the MDM server

Log into the Cisco ISE Admin portal. Navigate to **Administration >> Network Resources >> External MDM**



Select **Add**

Configure the connection by giving a friendly name to your configuration. In the **Hostname or IP Address** field, enter the cluster you determined your MI Cloud tenant is located as determined from the earlier section and

if you are using Core, then key in the IP address or the hostname of Core that ISE can reach and establish connection. It is not necessary to enter http://or https://before the hostname.

Configuration fields

Name: Name your configuration, this can be whatever you like.

Hostname or IP Address: *na1.mobileiron.com*OR *core.mobileiron.com*(example only)

Portfield: 443 (*default port for admin portal on Core*; *if a* custom *port is configured to access admin portal of Core, then specify that here.*)

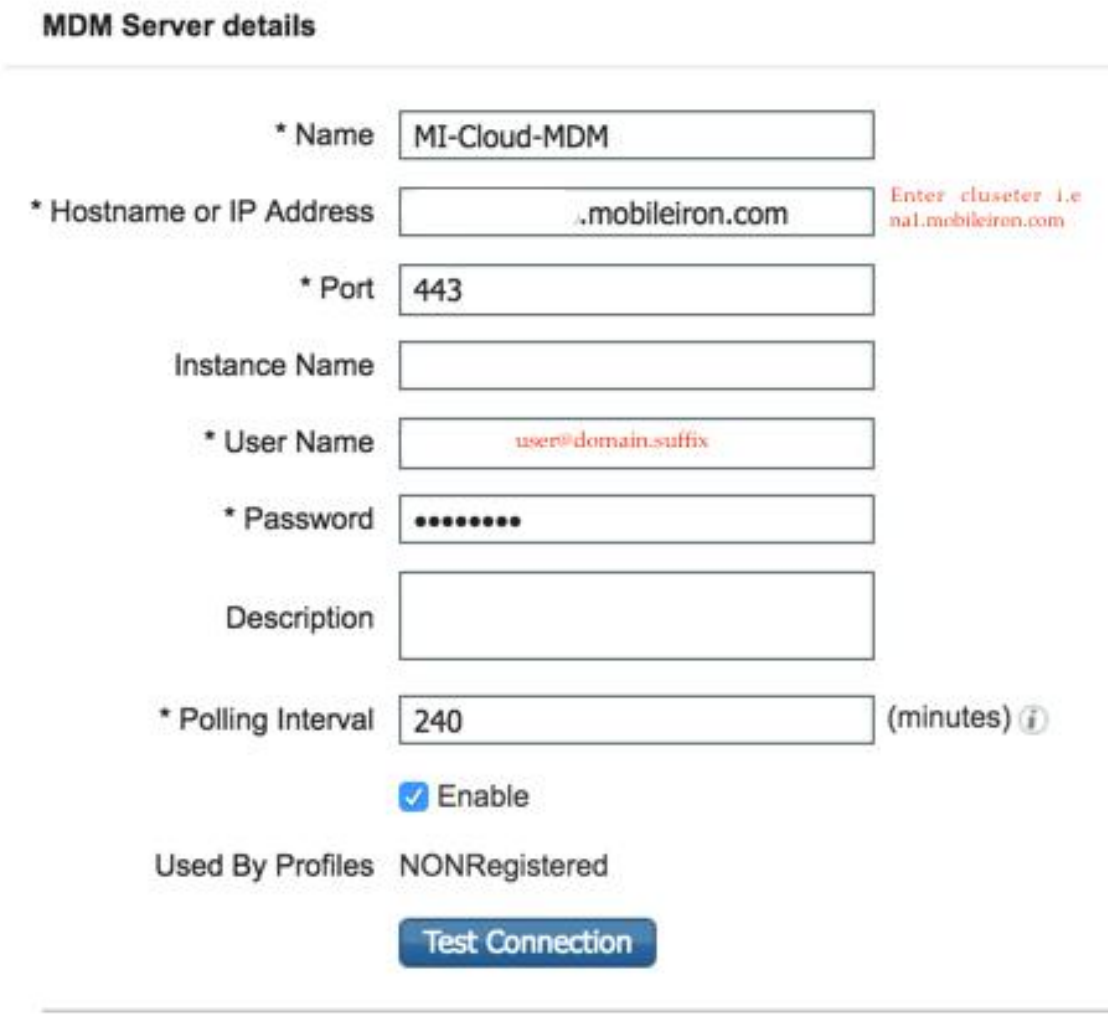
Instance Name: Leave this blank

Username: this is the full format of the user that the **Cisco ISE Operations** role was assigned to.

Password: The password for the user that the **Cisco ISE Operations** role was assigned to.

Polling Interval: This is a value in minutes. ISE will obtain new information from MobileIron Core / Cloud when the polling interval expires. Setting the value to zero will disable polling. Polling is used to periodically check the MDM compliance posture of an end station. The polling interval is a global setting and cannot be set for specific users or asset classes. If the polling interval is set, then it should match the device check-in period defined on the MDM

For example, if the MDM is configured such that devices will report their status every four hours, then ISE should be set to the same value and no less than half of this value. Oversampling, the device posture will create unnecessary loads on the MDM server and reduced battery life on the mobile devices. There are other considerations with respect to scan intervals. Changing MDM timers should be done only after consulting with MobileIron's best practices.



MDM Server details

* Name	MI-Cloud-MDM	
* Hostname or IP Address	.mobileiron.com	Enter cluseter i.e na1.mobileiron.com
* Port	443	
Instance Name		
* User Name	user@domain.suffix	
* Password	●●●●●●●●●	
Description		
* Polling Interval	240	(minutes)
	☑ Enable	
Used By Profiles	NONRegistered	

Test Connection: The Test Connection button shown above can be used to isolate and resolve common problems prior to developing MDM-based authorization policy. ISE will attempt to log in to the API and report back the result. Completing the test successfully is required prior to saving the settings. If the test does not complete successfully, the settings can still be saved, but the Enable box will be deselected and the MDM will not be active.

Cisco ISE API guide

You can download the latest version of supported Cisco ISE API's from MobileIron Core Cisco ISE API Guide

Supported API's (triggered from ISE)

These are the API's that Cisco ISE is calling in the background. The configuration of these API's on the CIsco ISE portal is not necessary. The Cluster URL uses the value entered in the **Hostname or IP Address** field in the ISE configuration step. For a full listed of Cisco ISE v2 API's, please see MobileIron Core Cisco ISE API Guide

API Description	API Call
MDM info- retrieves general information about the MobileIron Cloud tenant	**https://<Cluster URL>/ciscoise/mdminfo** • **HTTP GET**
Get devices for the given single value filter criteria	https://<**Cluster URL**>/ciscoise/mdmapi/v1/devices? • **HTTP GET**
Get devices for the given multi value filter criteria	https://<**Cluster URL**>/ciscoise/mdmapi/v1/batchdevices? • **HTTP POST**
Take an action (pin_lock or full_wipe) supported	https://<**Cluster URL**>/ciscoise/mdmapi/v1/action • **HTTP POST**
Send a message to a device	https://<**Cluster URL**>/ciscoise/mdmapi/v1/sendmessage • **HTTP PUT**

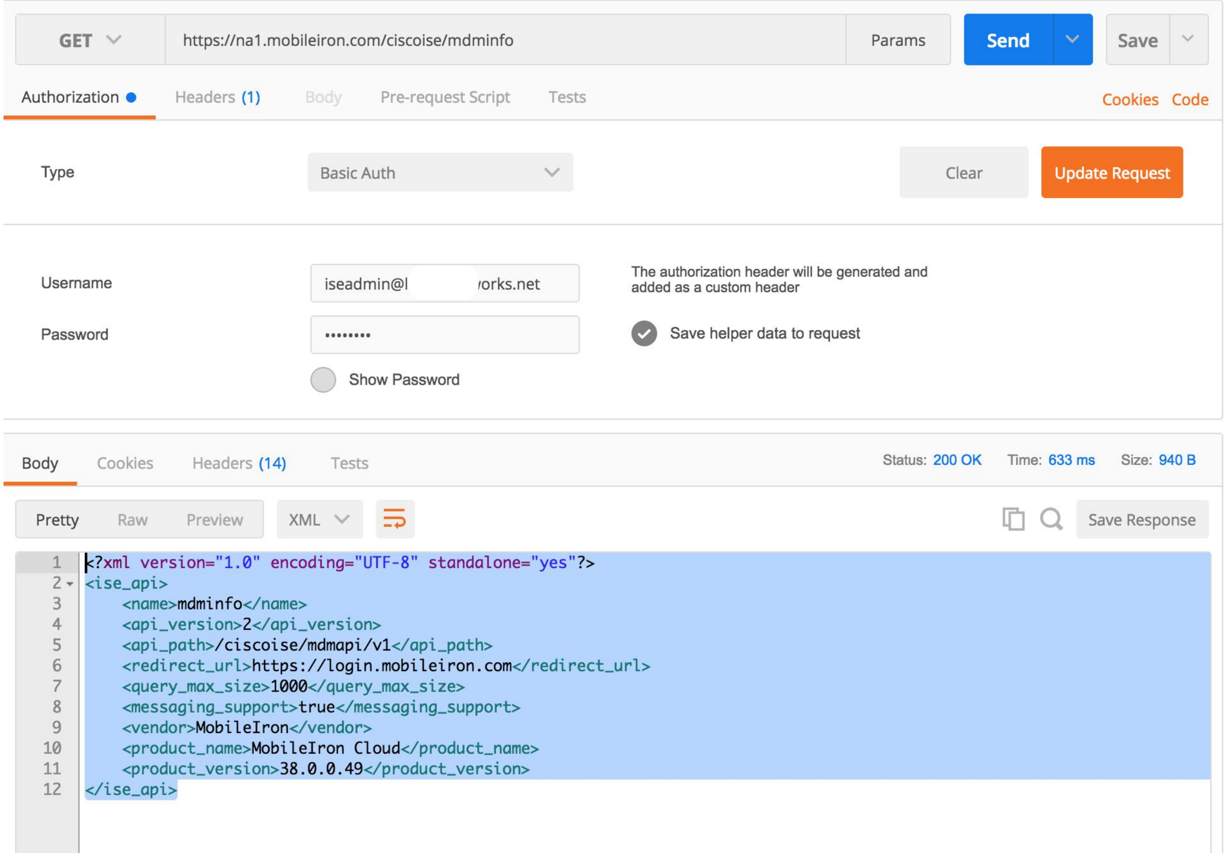
Examples of API data returned from Cloud to ISE

API Call: Retrieve basic information about tenant including version

https://na1.mobileiron.com/ciscoise/mdminfo

Method: GET

```
<?xml version="1.0" encoding="UTF-8"
standalone="yes"?> <ise_api>
  <name>mdminfo</name>
  <api_version>2</api_version>
  <api_path>/ciscoise/mdmapi/v1</api_path>
  <redirect_url>https://login.mobileiron.com</redirect_url>
  <query_max_size>1000</query_max_size>
  <messaging_support>true</messaging_support>
  <vendor>MobileIron</vendor>
  <product_name>MobileIron Cloud</product_name>
  <product_version>38.0.0.49</product_version>
</ise_api>
```



https://na1.mobileiron.com/ciscoise/mdminfo

Type: Basic Auth

Username: iseadmin@l[redacted]ʼorks.net

Password: ••••••••

○ Show Password

The authorization header will be generated and added as a custom header

✓ Save helper data to request

Status: 200 OK Time: 633 ms Size: 940 B

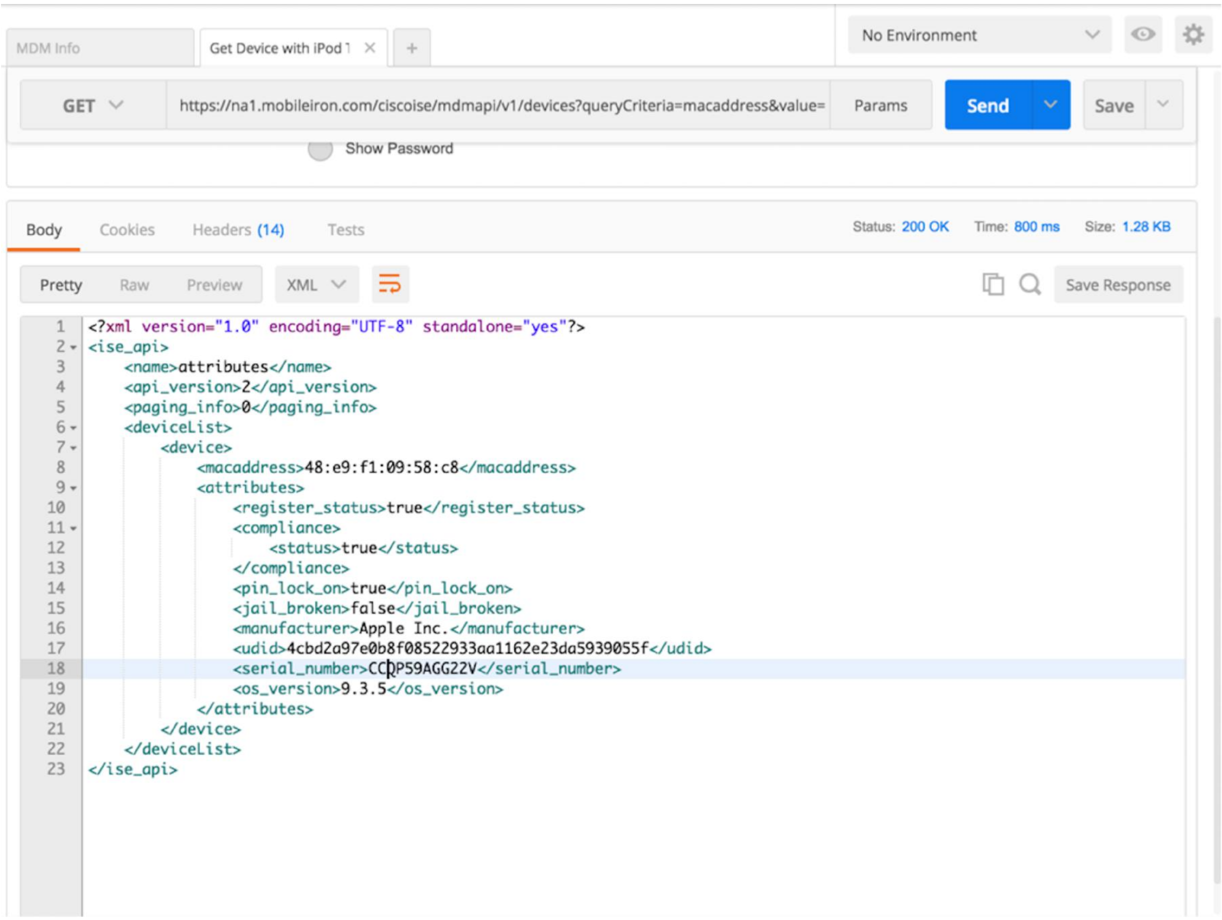
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ise_api>
    <name>mdminfo</name>
    <api_version>2</api_version>
    <api_path>/ciscoise/mdmapi/v1</api_path>
    <redirect_url>https://login.mobileiron.com</redirect_url>
    <query_max_size>1000</query_max_size>
    <messaging_support>true</messaging_support>
    <vendor>MobileIron</vendor>
    <product_name>MobileIron Cloud</product_name>
    <product_version>38.0.0.49</product_version>
</ise_api>
```

API Call: retrieve information about a device

https://na1.mobileiron.com/ciscoise/mdmapi/v1/devices?queryCriteria=macaddress&value= 48:e9:f1:09:58:c8&paging=0

Method: GET
(based on the macaddress as queryCriteria)

```
<?xml version="1.0" encoding="UTF-8"
standalone="yes"?> <ise_api>
  <name>attributes</name>
  <api_version>2</api_version>
  <paging_info>0</paging_info>
  <deviceList>
    <device>
      <macaddress>48:e9:f1:09:58:c8</macaddress>
      <attributes>
        <register_status>true</register_status>
        <compliance>
          <status>true</status>
        </compliance>
        <pin_lock_on>true</pin_lock_on>
        <jail_broken>false</jail_broken> <manufacturer>Apple
        Inc.</manufacturer>
        <udid>4cbd2a97e0b8f08522933aa1162e23da5939055f
        </udid>
        <serial_number>CCQP59AGG22V</serial_number>
        <os_version>9.3.5</os_version>
      </attributes>
    </device>
  </deviceList>
</ise_api>
```



https://na1.mobileiron.com/ciscoise/mdmapi/v1/devices?queryCriteria=macaddress&value=

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ise_api>
    <name>attributes</name>
    <api_version>2</api_version>
    <paging_info>0</paging_info>
    <deviceList>
        <device>
            <macaddress>48:e9:f1:09:58:c8</macaddress>
            <attributes>
                <register_status>true</register_status>
                <compliance>
                    <status>true</status>
                </compliance>
                <pin_lock_on>true</pin_lock_on>
                <jail_broken>false</jail_broken>
                <manufacturer>Apple Inc.</manufacturer>
                <udid>4cbd2a97e0b8f08522933aa1162e23da5939055f</udid>
                <serial_number>CCQP59AGG22V</serial_number>
                <os_version>9.3.5</os_version>
            </attributes>
        </device>
    </deviceList>
</ise_api>
```

API Call: Retrieve devices that are out of compliance

https://na1.mobileiron.com/ciscoise/mdmapi/v1/devices/?paging=0&queryCrietera=compliance&fileter=all&value=false

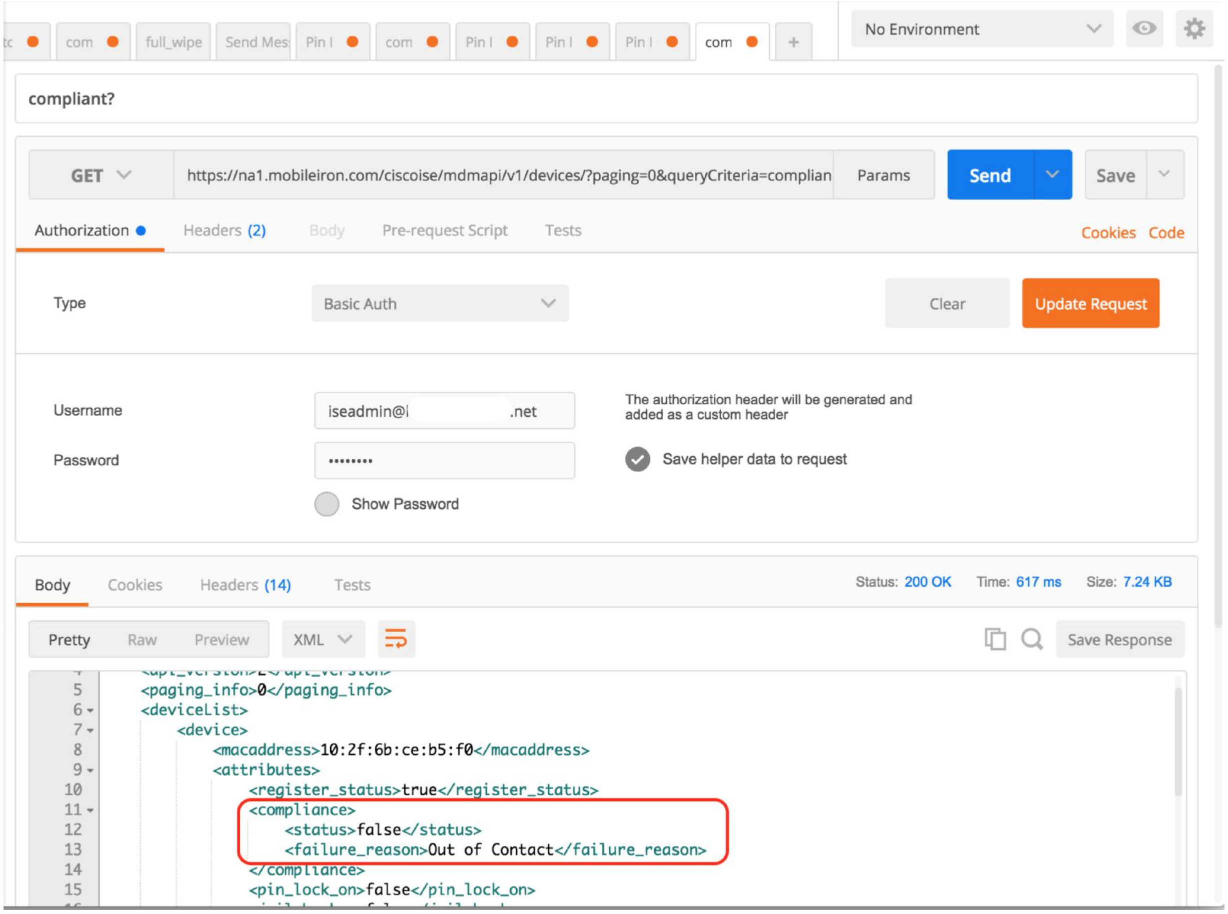
Method: GET

(compliance value is set to false. Setting it to true would retrieve a list of compliant devices)

```
<?xml version="1.0" encoding="UTF-8"
standalone="yes"?> <ise_api>

  <name>attributes</name>

  <api_version>2</api_version>

  <paging_info>0</paging_info>

  <deviceList>
    <device>
      <macaddress>10:2f:6b:ce:b5:f0</macaddress>
      <attributes>
        <register_status>true</register_status>
        <compliance>
          <status>false</status>
          <failure_reason>Out of Contact</failure_reason>
        </compliance>
        <pin_lock_on>false</pin_lock_on>
        <jail_broken>false</jail_broken>
        <manufacturer>NOKIA</manufacturer>
        <imei>353045067066348</imei>
        <udid>urn:uuid:9F3A846F-0D50-51A6-A64C-3829EE5D7D56</udid>
        <os_version>8.1</os_version>
        <phone_number></phone_number>
      </attributes>
    </device>
    <device>
      <macaddress>a4:f1:e8:3c:a9:38</macaddress>
  <attributes>
    <register_status>true</register_status>
    <compliance>
      <status>false</status>
      <failure_reason>Out of Contact</failure_reason>
    </compliance>
    <pin_lock_on>true</pin_lock_on>
    <jail_broken>false</jail_broken>
    <manufacturer>Apple Inc.</manufacturer>
    <udid>042458ff962250dacd0cf3ef0b318b2efa93207d</udid>
    <serial_number>CCQR62AFGGK5</serial_number>
    <os_version>9.3.2</os_version>
  </attributes>
</device>
<device>
  <macaddress>94:d7:71:d2:25:4e</macaddress>
  <attributes>
    <register_status>false</register_status>
    <compliance>
      <status>false</status>
      <failure_reason>Compromised
    Devices</failure_reason> </compliance>
    <pin_lock_on>false</pin_lock_on>
    <jail_broken>true</jail_broken>
    <manufacturer>samsung</manufacturer>
    <imei>357742051405922</imei>
    <meid></meid>
    <udid>7c96043f36477a4ad20d3376faf0011178468799d7435396d03c01f27201de7c</udid>
    <serial_number>R31D8100NXL</serial_number>
    <os_version>4.2.2</os_version>
    <phone_number></phone_number>
    </attributes>
  </device>
  <device>
    <macaddress>a4:f1:e8:a8:f4:b3</macaddress>
    <attributes>
      <register_status>false</register_status>
      <compliance>
        <status>false</status>
        <failure_reason>Out of Contact</failure_reason>
      </compliance>
      <pin_lock_on>true</pin_lock_on>
      <jail_broken>false</jail_broken>
      <manufacturer>Apple Inc.</manufacturer>
      <imei>35 545007 032832 1</imei>
      <meid>35545007032832</meid>
      <udid>1f08f6251d49cc8efb69f8706baf2f08b90ed95a
      </udid>
      <serial_number>DMPR9A42H256</serial_number>
      <os_version>9.3.5</os_version>
      <phone_number></phone_number>
    </attributes>
  </device>
  <device>
    <macaddress>fc:db:b3:09:53:be</macaddress>
    <attributes>
      <register_status>true</register_status>
      <compliance>
        <status>false</status>
        <failure_reason>Out of Contact</failure_reason>
      </compliance>
    <pin_lock_on>false</pin_lock_on>
    <jail_broken>false</jail_broken>
    <manufacturer>samsung</manufacturer>
    <imei>990004872072834</imei>
    <meid></meid>
    <udid>273b5e693f922ca9b88abc73712a5a0e7241e2da3d1a42e564c77c6d037a5089</udid>
    <serial_number>R28G627G92L</serial_number>
    <os_version>5.0.2</os_version>
    <phone_number></phone_number>
  </attributes>
</device>
<device>
  <macaddress>c0:f2:fb:37:56:13</macaddress>
  <attributes>
    <register_status>true</register_status>
    <compliance>
      <status>false</status>
      <failure_reason>Out of Contact</failure_reason>
    </compliance>
    <pin_lock_on>true</pin_lock_on>
    <jail_broken>false</jail_broken>
    <manufacturer>Apple Inc.</manufacturer>
    <udid>63fc6f4d22ded20e17a6317cf864bf0965f218a5</udid>
    <serial_number>F4KN855FG5V1</serial_number>
    <os_version>9.3.2</os_version>
  </attributes>
</device>
<device>
  <macaddress>ac:bc:32:1d:8e:a4</macaddress>
  <attributes>
    <register_status>true</register_status>
```

```
      <compliance>
        <status>false</status>
        <failure_reason>Out of Contact</failure_reason>
      </compliance>
      <pin_lock_on>true</pin_lock_on>
      <jail_broken>false</jail_broken>
      <manufacturer>Apple Inc.</manufacturer>
      <udid>9fc420d031b7b5af737264dbc4f4581fb1d1eb58</udid>
      <serial_number>CCQQN2TTGGK5</serial_number>
      <os_version>9.1</os_version>
    </attributes>
  </device>
  <device>
    <macaddress>a4:31:35:a2:51:72</macaddress>
    <attributes>
      <register_status>true</register_status>
      <compliance>
        <status>false</status>
        <failure_reason>Out of Contact</failure_reason>
      </compliance>
      <pin_lock_on>true</pin_lock_on>
      <jail_broken>false</jail_broken>
      <manufacturer>Apple Inc.</manufacturer>
      <udid>d68b77a59f21c2cdc78772485a936098bcb9837a</udid>
      <serial_number>CCQQ347QGGK5</serial_number>
      <os_version>10.0.2</os_version>
    </attributes>
  </device>
  <device>
    <macaddress>a4:f1:e8:3c:d1:06</macaddress>
    <attributes>
```

```
            <register_status>false</register_status>
            <compliance>
              <status>false</status>
              <failure_reason>Out of Contact</failure_reason>
            </compliance>
            <pin_lock_on>true</pin_lock_on>
            <jail_broken>false</jail_broken>
            <manufacturer>Apple Inc.</manufacturer>
            <udid>5bbff6a5b9c7aab78316798245ff1a3528fcfb04</udid>
            <serial_number>CCQR628MGGK5</serial_number>
            <os_version>10.0.1</os_version>
          </attributes>
        </device>
      </deviceList>
    </ise_api>
```



compliant?

GET https://na1.mobileiron.com/ciscoise/mdmapi/v1/devices/?paging=0&queryCriteria=complian

Type: Basic Auth

Username: iseadmin@l .net

Password: ••••••••

○ Show Password

The authorization header will be generated and added as a custom header

✓ Save helper data to request

Status: 200 OK Time: 617 ms Size: 7.24 KB

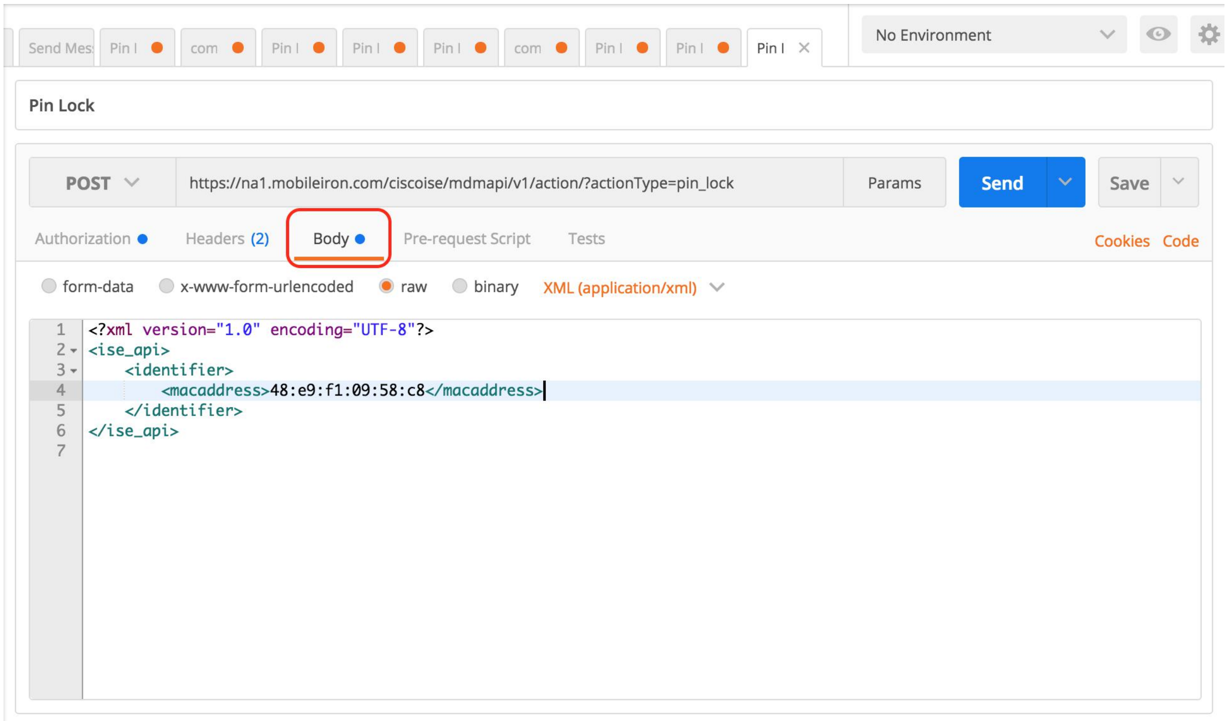
```
<api_version>2</api_version>
<paging_info>0</paging_info>
<deviceList>
    <device>
        <macaddress>10:2f:6b:ce:b5:f0</macaddress>
        <attributes>
            <register_status>true</register_status>
            <compliance>
                <status>false</status>
                <failure_reason>Out of Contact</failure_reason>
            </compliance>
            <pin_lock_on>false</pin_lock_on>
```

API Call: Lock the device if a device passcode is present

https://na1.mobileiron.com/ciscoise/mdmapi/v1/action/?actionType=pin_lock

Method: POST

This command is sent as XML. In the Postman example, the XML is configured in the Bodyfield. Full_Wipeis also supported. The Enterprise_Wipeaction is not currently supported.



https://na1.mobileiron.com/ciscoise/mdmapi/v1/action/?actionType=pin_lock

```
<?xml version="1.0" encoding="UTF-8"?>
<ise_api>
    <identifier>
        <macaddress>48:e9:f1:09:58:c8</macaddress>
    </identifier>
</ise_api>
```

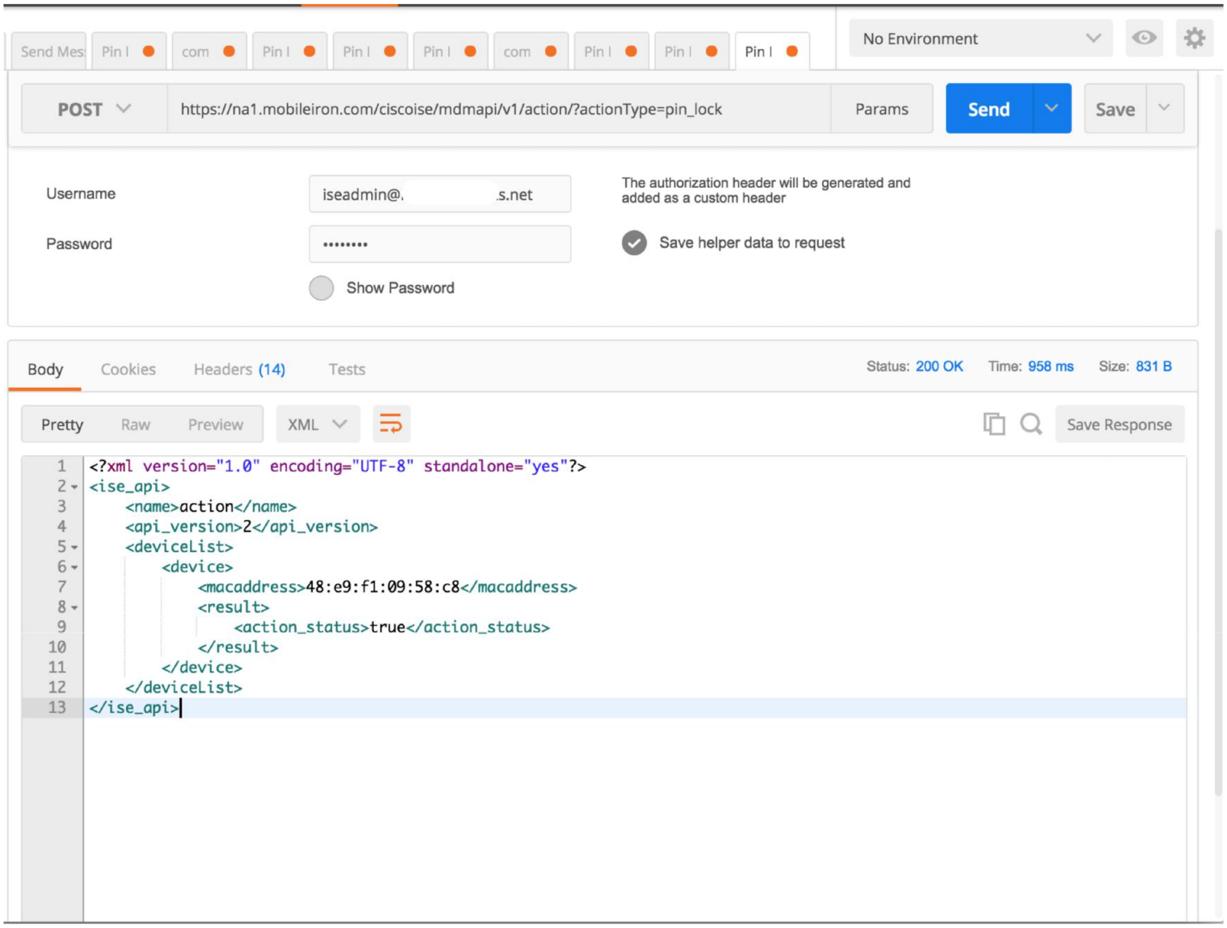
Example XML (Identifier is MAC Address)

```
<?xml version="1.0" encoding="UTF-8"?>
<ise_api>
   <identifier>
      <macaddress>48:e9:f1:f3:58:d8</macaddress>
   </identifier>
</ise_api>
```

Successful call output

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<ise_api>
  <name>action</name>
  <api_version>2</api_version>
  <deviceList>
    <device>
      <macaddress>48:e9:f1:09:58:c8</macaddress>
      <result>
        <action_status>true</action_status>
      </result>
    </device>
  </deviceList>
</ise_api>
```



https://na1.mobileiron.com/ciscoise/mdmapi/v1/action/?actionType=pin_lock

Username iseadmin@. s.net

Password ••••••••

○ Show Password

The authorization header will be generated and added as a custom header

✓ Save helper data to request

Status: 200 OK Time: 958 ms Size: 831 B

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ise_api>
    <name>action</name>
    <api_version>2</api_version>
    <deviceList>
        <device>
            <macaddress>48:e9:f1:09:58:c8</macaddress>
            <result>
                <action_status>true</action_status>
            </result>
        </device>
    </deviceList>
</ise_api>
```