2018

THE IOS MDM PROTOCOL

简单命令参考

《MDM CommandReference.pdf》2012 版翻译及改编版

原作者：David Schuetz

移动互联百科 http://www.baike.net

by 江哥一直在

目录

说明

本文是移动互联技术博客作者（江哥一直在）翻译的由 Intrepidus 公司的 David Schuetz 作者整理的关于 iOS MDM 协议命令参考的 PDF 文档《MDM CommandReference.pdf》，翻译的不足之处，敬请指正，如有任何版权问题，请邮件至 459104018@qq.com。本文档是对 2011 年 Black Hat USA 发布的白皮书的后续。本质上它是更新后的附录 A，其中列出了（以非常简化的形式）Apple iOS MDM 系统使用的各种命令的描述。此更新包含使用 iOS 版本 5.x 实施的更改的说明，其中包括：

1、检出 MDM

2、安装应用程序

3、列出托管应用程序

4、删除托管的应用程序

5、配置设置

请参阅白皮书了解更多详情。 还要注意的是，这个文档并不全面，没有列出所有可能的设备或服务器响应，而且主要是试图公开证明其他未公开的 Apple 私有 API。 因此，准确性无法 100%保证，命令，参数，功能等在未来的 iOS 版本中可能会发生变化。本文仅用于研究和实验/测试。不要使用它来创建实际的商业 MDM 产品。

附录 A - 命令列表

（iOS 5.0 新增的命令以***粗体/斜体/下划线***显示）

Control Commands **（控制类命令）**	• Device Lock（锁屏） • Erase Device（擦除数据） • Clear Passcode （清除密码）

Device Queries **（设备查询类命令）**	• Security Information（设备安全信息） • Installed Application List （安装的 APP） • Device Information（设备信息） • Certificate List（证书数据） • Profile List（描述文件） • Provisioning Profile List（预植描述文件） • Restrictions List （限制信息） • ***List Managed Applications（受管理的 APP）***
Device Configuration **（设备配置）**	• Install Profile（安装描述文件） • Remove Profile（移除描述文件） • Install Provisioning Profile（安装预植描述文件） • Remove Provisioning Profile （移除预植描述文件） • ***Install Application（安装 APP）*** • ***Remove Application（卸载 APP）*** • ***Settings（设置）***
Device to Server Commands **（设备-服务器命令）**	• Authenticate（认证） • Token Update （更新 Token） • ***Check Out（移除管控）***

命令格式

所有命令都以 Apple Property List（.plist）文件的形式发送。 每个包含一个名为“CommandUUID”的顶级密钥，其中包含用于唯一标识命令实例的 UUID 字符串以及包含附

加信息的顶级密钥“Command”。

```
<plist version="1.0">
    <dict>
        <key>Command</key>
        <dict>
            <key>RequestType</key>
            <string>[command name]</string>
            [... additional parameters as needed ...]
        </dict>
        <key>CommandUUID</key>
        <string></string>
    </dict>
</plist>
```

下面列出每条命令的简短描述和所需的参数。

设备响应

设备通过简单的确认来响应许多命令：

```
<plist version="1.0">
    <dict>
        <key>CommandUUID</key>
        <string></string>
        <key>Status</key>
```

```
        <string>Acknowledged</string>
        <key>UDID</key>
        <string>[device UUID]</string>
    </dict>
</plist>
```

“状态”字段可能包含“已确认”，“错误”，“CommandFormatError”或“NotNow”（有关错误字段的详细信息，请参阅下文）。

在命令引发更多扩展响应的地方(比如 DeviceInformation 查询),这些响应的细节在下面给出。通常，这些命令添加一个顶级字段（如 InstalledApplicationList), 该字段的值为扩展数据，存储为字符串，字典或其他元素的数组。 例如：

```
<plist version="1.0">
    <dict>
        <key>CommandUUID</key>
        <string></string>
        <key>SecurityInfo</key>
        <dict>
            <key>HardwareEncryptionCaps</key>
            <integer>3</integer>
            <key>PasscodeCompliant</key>
            <true/>
            <key>PasscodeCompliantWithProfiles</key>
            <true/>
```

```
        <key>PasscodePresent</key>
        <false/>
    </dict>
    <key>Status</key>
    <string>Acknowledged</string>
    <key>UDID</key>
    <string>[device UUID]</string>
</dict>
</plist>
```

错误消息

错误消息的一般格式与确认相同，“状态”更改为“错误”，并添加一个附加的数组作为“ErrorChain”：

ErrorCode	(integer) A unique identifying error code
ErrorDomain	(string) Category of error
LocalizedDescription	(string) Error message, translated to a localized language
USEnglishDescription	(string) Standardized version of error message

一个特殊的错误信息是“NotNow”，当一个命令由于设备被密码锁定而不能被请求时（例如请求安全信息或安装配置文件），就会看到该信息。 发生这种情况时，只要设备解锁，设备就会尝试重新与 MDM 服务器连接，以便重试该命令。

用无效或缺少参数发送的命令将返回“CommandFormatError”状态。

设备锁定

立即锁定设备。 如果存在密码，则需要该密码才能解锁设备。

RequestType	DeviceLock

擦除设备

立即擦除设备内存并将其重置为“从工厂清理”状态。 需要连接 iTunes 才能从备份中恢复或配置为新的。

RequestType	EraseDevice

清除密码

如果设备上存在密码，该命令将清除该密码。 如果其他配置控件需要密码，则会为用户设置一个宽限期，以设置新的密码。

RequestType	ClearPasscode
UnlockToken	(data) UnlockToken data, base-64 encoded

安全信息

列出设备的指定安全相关设置，包括硬件加密功能，以及是否存在密码（如果是，则是否符合配置）。 如果存在密码，则必须解锁该设备才能执行该命令。

RequestType	SecurityInfo
Queries	(array of strings): “HardwareEncryptionCaps”，

	“PasscodePresent”， “PasscodeCompliant”， “PasscodeCompliantWithProfiles”

响应基于通用确认响应，并附带一个名为“SecurityInfo”的附加字典：

HardwareEncryptionCaps	integer
PasscodePresent	boolean
PasscodeCompliant	boolean
PasscodeCompliantWithProfiles	boolean

安装的应用程序列表

列出设备上当前安装的所有应用程序。 包括应用程序使用的总体持久性存储，以字节表示，以及应用程序的名称，版本和软件包标识符。 不列出通过越狱方法安装的应用程序。

RequestType	InstalledApplicationList

在“InstalledApplicationList”关键字中的其他响应信息是一个字典项目数组：

BundleSize	integer
DynamicSize	integer
Identifier	string
Name	string
Version	string

设备信息

检索有关设备的指定一般信息，包括 MAC 地址，IMEI，电话号码，软件版本，型号名称和编号，

序列号。

RequestType	DeviceInformation
Queries	(array of strings): "AvailableDeviceCapacity", "BluetoothMAC", "BuildVersion", "CarrierSettingsVersion", "CurrentCarrierNetwork", "CurrentMCC", "CurrentMNC", "DataRoamingEnabled", "DeviceCapacity", "DeviceName", "ICCID", "IMEI", "IsRoaming", "Model", "ModelName", "ModemFirmwareVersion", "OSVersion", "PhoneNumber", "Product", "ProductName", "SIMCarrierNetwork", "SIMMCC", "SIMMNC", "SerialNumber", "UDID", "WiFiMAC", "UDID"

响应是一个名为“QueryResponses”的字典，其中包括上述项目作为键。 将会被忽略的响应（例如，来自 iPod Touch 的 PhoneNumber 字段）将被忽略。 AvailableDeviceCapacity 和 DeviceCapacity 是实数字段，而 DataRomingEnabled 和 IsRoaming 是布尔值。 其余的都以字符串形式返回。

证书列表

列出设备上当前安装的所有证书。

RequestType	CertificateList

响应包含一个“CertificateList”字典值数组：

CommonName	string
Data	base-64 cert information
IsIdentity	boolean

描述文件列表

列出安装在设备上的配置文件。 包括通用名称，是否需要删除密码，是否禁止删除，唯一标识符以及其他类似信息。

RequestType	ProfileList

响应键“ProfileList”包含一个字典项目数组：

HasRemovalPasscode	boolean
IsEncrypted	boolean
PayloadDisplayName	string
PayloadIdentifier	string
PayloadRemovalDisallowed	boolean
PayloadUUID	string
PayloadVersion	integer
SignerCertificates	array of data items, each with base-64 cert info
PayloadContent	array of dicts, each with PayloadDisplayName, PayloadIdentifier,

	PayloadType, and PayloadVersion keys.

预植描述文件列表

列出安装在设备上的配置文件（类似于配置文件列表）。

RequestType	ProvisioningProfileList

响应包括一个“ProvisioningProfileList”键，其中包含一个字典值数组：

ExpiryDate	date
Name	string
UUID	string

限制列表

列出当前对设备有效的限制。 例如，列出禁用的应用程序，是否强制启用备份加密等。

RequestType	RestrictionsList

响应包括“GlobalRestrictions”，它是一个包含限制的详细列表的字典，大部分呈现为布尔值。

确切的内容和结构取决于设备上的限制。

受管理的 APP 列表

列出当前对设备有效的限制。 例如，列出禁用的应用程序，是否强制启用备份加密等。

RequestType	ManagedApplicationList

在关键的“ManagedApplicationList”中，额外的响应信息是一个字典项目数组，每个应用程序（每个字典都有应用程序的捆绑 ID 作为其关键字）：

Status	“Managed”

ManagementFlags	integer

示例响应（采用 JSON 格式）：

```
{'Status': 'Acknowledged',
        'CommandUUID': 'd3a8ac67-6662-4f43-8f28-27b1ce1ab7d5',
        'UDID': '-- redacted --',
        'ManagedApplicationList':
                {'com.apple.movietrailers':
                        {'Status': 'Managed',
                        'ManagementFlags': 1}
                }
}
```

ManagementFlags 设置控制从 MDM 控制中删除设备时发生的情况：

如果设置值为 1，则应用程序及其数据可以通过 MDM 控制删除。 如果该位未设置，则该应用程序不会被删除。

安装配置文件

如果给定.mobileconfig 配置文件（由 IPCU 或其他工具创建）的 base-64 编码，则将配置文件安装到设备上。

RequestType	InstallProfile
Payload	(data) IPCU .mobileconfig file, base-64 encoded

删除配置文件

给定一个有效载荷标识符(通常显示为反向 DNS 标识符 ,如“com.example.cfg.restrictions”) ,

从设备中删除该配置文件。

RequestType	RemoveProfile
Identifier	(string) Profile identifier

安装预植描述文件

给定.mobileprovision 配置文件（由 IPCU 或其他工具创建）的 base-64 编码，将配置文件安

装到设备上。

RequestType	InstallProvisioningProfile
Payload	(data) IPCU .mobileprovision file, base-64 encoded

删除预植描述文件

根据配置文件的 UUID，该命令将从设备中删除配置文件。

RequestType	RemoveProvisioningProfile
UUID	(string) Provisioning profile UUID

安装 APP

支持此命令的两种不同形式：一种用于从 App Store 安装应用程序，另一种用于 plist 安装定制

应用程序。

第一种形式将 iTunesStoreID 作为参数，并使设备提示用户输入其 AppleID 和密码。 该 ID 与

基于 Web 的 App Store 页面中显示的相同（例如：

http://itunes.apple.com/us/app/apple-store/id471966214?mt=8）,其中 471966214 即为

iTunesStoreID 值。

RequestType	InstallApplication
ManagementFlags	integer (see List Managed Applications)
iTunesStoreID	integer

另一种形式安装一个苹果$299 账号打包的企业应用程序。ManifestURL 键指向 Manifest.plist

文件（详述如下）。

RequestType	InstallApplication
ManagementFlags	integer (see List Managed Applications)
ManifestURL	url

Manifest.plist 文件提供有关应用程序的信息，以及指向下载应用程序的 Xcode .ipa 文件的链

接，其中的 URL 应该是 https（SSL）安全模式。

```
<plist version="1.0">
        <dict>
          <key>items</key>
          <array>
            <dict>
              <key>assets</key>
              <array>
                <dict>
```

```
            <key>kind</key>
            <string>software-package</string>
            <key>url</key>
            <string>https://*** SERVER_IP ***:port/MyApp</string>
          </dict>
        </array>
        <key>metadata</key>
        <dict>
          <key>bundle-identifier</key>
          <string>*** BUNDLE ID (com.example.myapp) ***</string>
          <key>bundle-version</key>
          <string>1.0.0</string>
          <key>kind</key>
          <string>software</string>
          <key>subtitle</key>
          <string></string>
          <key>title</key>
          <string>*** APP NAME ***</string>
        </dict>
      </dict>
    </array>
  </dict>
```

```
</plist>
```

移除 APP

给定应用程序包 ID，从应用程序中删除应用程序及其数据。 如果请求移除的应用程序不受 MDM 管理，则返回错误（并且不会删除应用程序）。

MessageType	RemoveApplication
Identifier	(string) Bundle identifier

```
<plist version="1.0">
    <dict>
      <key>items</key>
      <array>
        <dict>
          <key>assets</key>
          <array>
            <dict>
              <key>kind</key>
              <string>software-package</string>
              <key>url</key>
              <string>https://*** SERVER_IP ***:port/MyApp</string>
            </dict>
          </array>
```

```
            <key>metadata</key>
            <dict>
              <key>bundle-identifier</key>
              <string>*** BUNDLE ID (com.example.myapp) ***</string>
              <key>bundle-version</key>
              <string>1.0.0</string>
              <key>kind</key>
              <string>software</string>
              <key>subtitle</key>
              <string></string>
              <key>title</key>
              <string>*** APP NAME ***</string>
            </dict>
          </dict>
        </array>
      </dict>
</plist>
```

设置

用于配置设备上的某些设置。 目前支持更改 DataRoaming 和 VoiceRoaming。 代码中的提示表明某些形式的 Wallpaper 控件也可能存在。

RequestType	Settings

Settings	(array of dicts)

“设置”键是一组字符串，每个字符表示要更改的设置：

Item	(string) (“DataRoaming” or “VoiceRoaming”)
Enabled	(boolean)

完整命令的示例：

```
{'CommandUUID': 'ce0c8b34-9ac5-44f6-a25b-1c9cfffce666',
    'Command': {
        'RequestType': 'Settings',
        'Settings': [
            {'Item': 'DataRoaming', 'Enabled': False},
            {'Item': 'VoiceRoaming', 'Enabled': True}]}}
```

当在没有语音服务的设备（如 iPad）上更改“VoiceRoaming”时，仅返回该项目的错误，但其他项目仍可能成功处理。 这种回应的例子：

```
{'Status': 'Acknowledged',
    'CommandUUID': 'ce0c8b34-9ac5-44f6-a25b-1c9cfffce666',
    'UDID': '-- redacted --',
    'Settings': [
        {'Status': 'Acknowledged', 'Item': 'DataRoaming'},
        {'Status': 'CommandFormatError', 'Item': 'VoiceRoaming'}]}
```

设备认证

这是设别发送的用于启动注册的设备命令。可以由服务器使用 ,以允许或拒绝基于设备的 UDID 的注册。 注 - 不遵循与服务器到设备命令相同的格式。 没有 CommandUUID 字段和 Command 字典结构 - 所有参数都是主属性列表字典中的顶级项目。

MessageType	Authenticate
Topic	(string) Subject Name: User ID on APNS push certificate used by server
UDID	(string) Device UDID

令牌更新

这是设备在注册期间发送的设备消息。 向服务器提供用于通过 APNS 与设备联系的令牌，以及通过 Clear Passcode 命令解锁设备的密钥。 注 - 不遵循与服务器到客户端命令相同的格式。没有CommandUUID字段和Command字典结构 - 所有参数都是主属性列表字典中的顶级项目。

MessageType	Token Update
PushMagic	(string) UUID-like string
Token	(data) 32-byte APNS device token, base-64 encoded
Topic	(string) Subject Name: User ID on APNS push certificate used by server
UDID	(string) Device UDID

UnlockToken	(data) Device unlock key, base-64 encoded

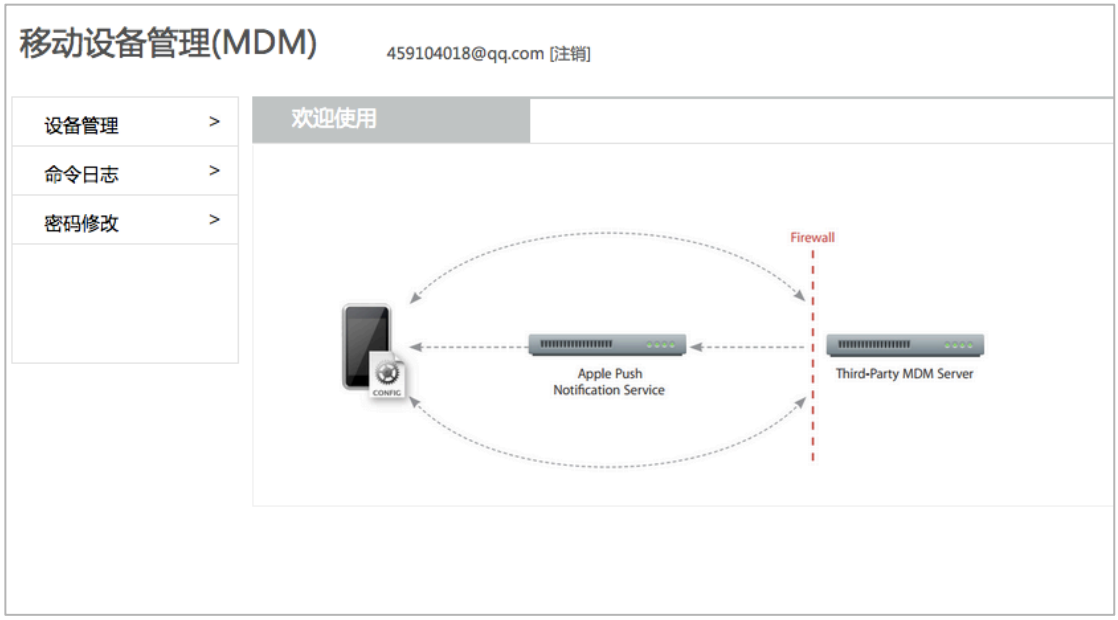
移除管控

这是由设备发送的客户端命令，用于提醒服务器该设备即将从 MDM 控制中移除。 设备不会等待响应，并且服务器不能拒绝移除。 注 - 不遵循与服务器到客户端命令相同的格式。 没有 CommandUUID 字段和 Command 字典结构 - 所有参数都是主属性列表字典中的顶级项目。

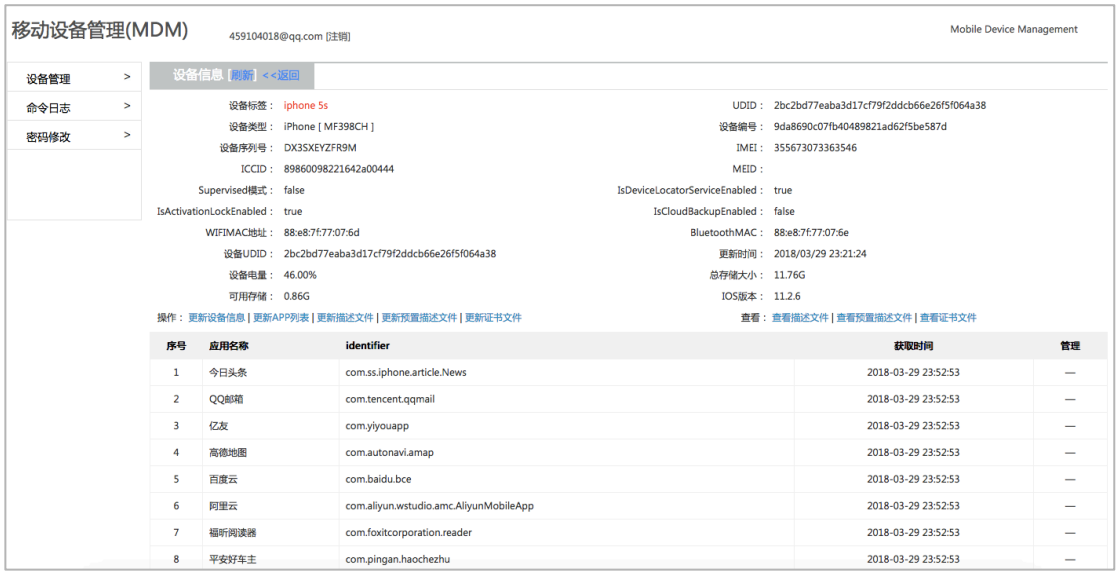
MessageType	CheckOut
Topic	(string) Subject Name: User ID on APNS push certificate used by server
UDID	(string) Device UDID

附录 B - 源代码

MDMServer 截图




移动设备管理(MDM)
459104018@qq.com [注销]
Mobile Device Management
设备管理
命令日志
密码修改
设备列表 [刷新]
序号 标签 版本 设备ID 设备类型 设备状态 控制 查看 操作
1 iphone 5s 11.2.6 9da8690c07fb40489821ad62f5be587d iPhone 设备可控 设备锁屏 | 清除密码 | 清除数据 | 安装APP 设备信息 移除
共 1 条数据，页次:1/1 页 首页 上一页 下一页 尾页


移动设备管理(MDM)
459104018@qq.com [注销]
Mobile Device Management
设备管理
命令日志
密码修改
设备信息 [刷新] <<返回
设备标签： iphone 5s
设备类型： iPhone [MF398CH]
设备序列号： DX3SXEYZFR9M
ICCID： 89860098221642a00444
Supervised模式： false
IsActivationLockEnabled： true
WIFIMAC地址： 88:e8:7f:77:07:6d
设备UDID： 2bc2bd77eaba3d17cf79f2ddcb66e26f5f064a38
设备电量： 46.00%
可用存储： 0.86G
UDID： 2bc2bd77eaba3d17cf79f2ddcb66e26f5f064a38
设备编号： 9da8690c07fb40489821ad62f5be587d
IMEI： 355673073363546
MEID：
IsDeviceLocatorServiceEnabled： true
IsCloudBackupEnabled： false
BluetoothMAC： 88:e8:7f:77:07:6e
更新时间： 2018/03/29 23:21:24
总存储大小： 11.76G
IOS版本： 11.2.6
操作： 更新设备信息 | 更新APP列表 | 更新描述文件 | 更新预置描述文件 | 更新证书文件
查看： 查看描述文件 | 查看预置描述文件 | 查看证书文件
序号 应用名称 identifier 获取时间 管理
1 今日头条 com.ss.iphone.article.News 2018-03-29 23:52:53 —
2 QQ邮箱 com.tencent.qqmail 2018-03-29 23:52:53 —
3 亿友 com.yiyouapp 2018-03-29 23:52:53 —
4 高德地图 com.autonavi.amap 2018-03-29 23:52:53 —
5 百度云 com.baidu.bce 2018-03-29 23:52:53 —
6 阿里云 com.aliyun.wstudio.amc.AliyunMobileApp 2018-03-29 23:52:53 —
7 福昕阅读器 com.foxitcorporation.reader 2018-03-29 23:52:53 —
8 平安好车主 com.pingan.haochezhu 2018-03-29 23:52:53 —


移动设备管理(MDM)
459104018@qq.com [注销]
设备管理
命令日志
密码修改
APP信息 [刷新] <<返回
设备类型： iPhone [MF398CH]
设备编号： 9da8690c07fb40489821ad62f5be587d
安装类型： APP ID PList安装
输入值：
提交请求

代码地址

1、演示站：http://mdm.mbaike.net

2、GitHub 开源地址：https://github.com/keaijohnee/OpenMDMServer

3、OSChina 开源地址：http://git.oschina.net/jianggege/OpenMDMServer

技术咨询及服务

咨询 QQ：459104018　　微信：13568933413（电话同号）　　QQ 群：205891305；

附录 C - 参考文献

1、 http://www.mbaike.net/mdm/6.html　基于 IOS 上 MDM 技术相关资料整理及汇总

2、 https://mdm.mbaike.net　Apple iOS 移动设备管理

3、 https://github.com/notnoop/java-apns/　Java APNS 推送

4、 http://www.rootmanager.com/iphone-ota-configuration/iphone-ota-setup-with-signed-mobileconfig.html　mobileconfig 配置文件的签名和认证

5、 https://github.com/keaijohnee/OpenMDMServer　GitHub 开源地址

6、 http://git.oschina.net/jianggege/OpenMDMServer　OSChina 开源地址

2018 年 4 月 03 日

江哥一直在