# MDM Check-in Protocol

在初始化过程中使用MDM签入协议来验证一个设备是否适合MDM登记，并通知服务器一个设备的push令牌已经更新。

如果在MDM payload中提供了签入服务器URL，则使用签入协议与该签入服务器进行通信。如果没有提供签入服务器URL，则使用主MDM server URL。

## Structure of a Check-in Request

安装MDM payload后，设备开始与签入服务器通信。该设备验证服务器的TLS证书，然后使用其MDM payload中指定的身份作为连接的客户端身份验证证书。

成功协商这个安全连接后，设备发送一个HTTP PUT请求，格式如下:

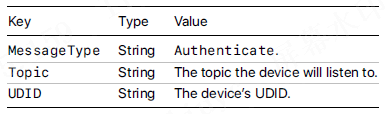


服务器必须发送一个200 (OK)状态码来表示成功，或者发送一个401(未授权)状态码来表示失败。将忽略应答的正文。

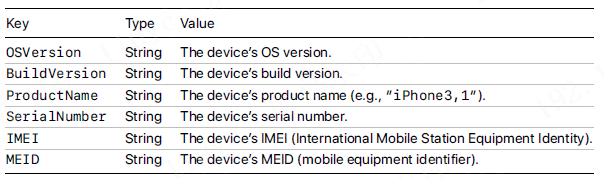
## Supported Check-in Commands

### Authenticate Message

在用户安装MDM payload时，设备发送一条验证消息，该消息的属性列表中至少包含三个键-值对:



如果设备正在运行ios9或更高版本，且具有设备信息访问权限，设备还可以发送以下键值对:



**Server Response**

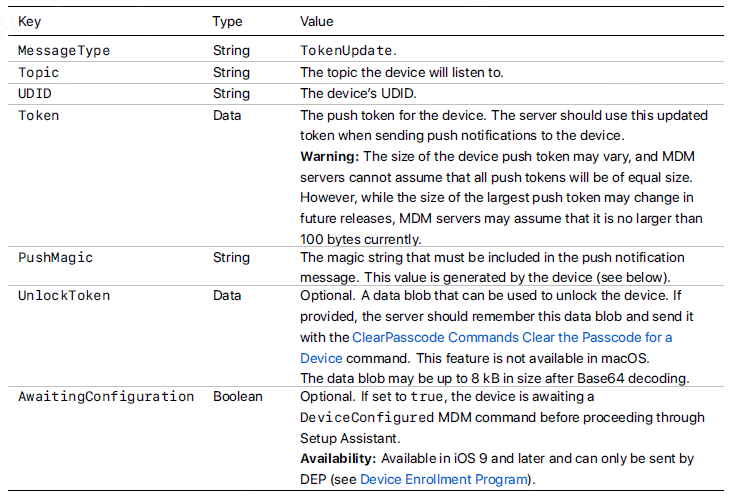
如果成功，服务器必须返回一个200 OK状态。

此时，服务器不应该假设设备已经安装了MDM payload，因为配置文件中的其他 payload可能仍然无法安装。当设备成功安装MDM payload时，它发送一条令牌更新消息。

### TokenUpdate Message

每当设备推送令牌、推送magic或解锁令牌更改时，设备就向签入服务器发送令牌更新消息。服务器需要这些字段来发送设备推送通知或密码重置。

TokenUpdate消息在其属性列表中包含这些键-值对:



在安装了MDM payload之后，设备向服务器发送初始令牌更新消息。服务器应该在收到第一个令牌更新消息后才向设备发送推送消息。如果设备报告正在等待配置，那么MDM server将发送一个deviceconfigure MDM命令，然后才允许用户在Setup Assistant中继续操作。这使MDM server有机会通过MDM命令进行一些设置。

除了发送初始的TokenUpdate消息外，iOS设备现在还可以在拥有有效的MDM登记时随时向签入服务器发送其他的TokenUpdate消息。

PushMagic的使用将设备限制为唯一的MDM关系。当用户删除MDM配置文件时，设备应该不再监听以前的关系，即使用户使用相同的服务器主题重新建立管理关系。注意，在本例中，只有推topic是相同的;服务器地址可能已经更改。这也有助于用户从备份中还原包含旧关系的设备。使用PushMagic还可以确保接收签入消息的服务器与发送推送通知的计算机属于同一家企业。这很重要，因为无法知道推topic是否属于签入服务器的所有者。可以想象，苹果可能会撤销某一方的推送令牌，然后让该方重新招募人员，利用其他正在积极推动的主题。所有的MDM推送主题都位于名称空间com.apple.mgmt.\*中。有助于防止这种情况。

后续TokenUpdate消息的PushMagic或UnlockToken字段可能与前面的消息相同，也可能不同(大小可能与前面的值不同)。如果不同，服务器应该将其设备记录更新为消息提供的新值。如果不这样做，将导致服务器无法发送推送通知或执行密码重置。

虽然设备可以多次发送UnlockToken消息，但如果PushMagic或UnlockToken值发生变化，则可能只发送一次。实现不应该依赖于重复的消息来更新丢失的服务器端数据或从失败中恢复来处理以前的TokenUpdate消息。

### CheckOut

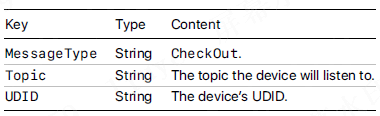
在iOS 5.0及更高版本和macOS v10.9中，如果将MDM payload中的checkoutwhenremove键设置为true，那么在删除MDM配置文件时，设备将尝试发送一条CheckOut消息。

在macOS v10.8中，当删除MDM配置文件时，无论这个键的值是多少(或者是否没有这个键)，设备都会尝试发送一条签出消息。

如果网络条件不允许成功传递消息，设备将不再尝试发送消息。

服务器对该消息的响应将被忽略。

CheckOut消息包含以下关键字:



# Mobile Device Management Protocol

在安装过程中:

•用户或管理员告诉设备安装MDM payload。MDM payload的结构描述了这个 payload的结构。

•设备连接到签到服务器。该设备提供了uthentication的身份证书，以及UDID和推送通知主题。

虽然UDIDs是由MDM使用的，但是不建议在iOS应用程序中使用UDIDs。

而且，在未来，UDID将不会总是41个字符—它可以更长或更短。它也可能包含其他字符，比如破折号。不要在你的产品中硬编码假设。如果你这样做了，注册可能会失败的未来。

如果服务器接受该设备，则该设备向服务器提供其推送通知设备令牌。服务器应该使用这个令牌向设备发送推送消息。此签入消息还包含一个PushMagic字符串。服务器必须记住这个字符串，并将它包含在发送给设备的任何推送消息中。

在正常操作:

•服务器(在将来的某个时候)向设备发送推送通知。

•设备轮询服务器以获得响应推送通知的命令。

•设备执行命令。

•设备与服务器联系，报告上一个命令的结果并请求下一个命令。

设备令牌可能会不时更改。当检测到更改时，设备会自动检入MDM server，报告新的推送通知令牌。

设备仅在响应推送通知时轮询;它不会在安装后立即轮询服务器。

服务器必须向设备发送推送通知来开始事务。

通过建立到MDM server URL的TLS连接，设备启动与MDM server的通信，以响应推送通知。设备验证服务器的证书，然后使用其MDM payload中指定的身份作为连接的客户端身份验证证书。

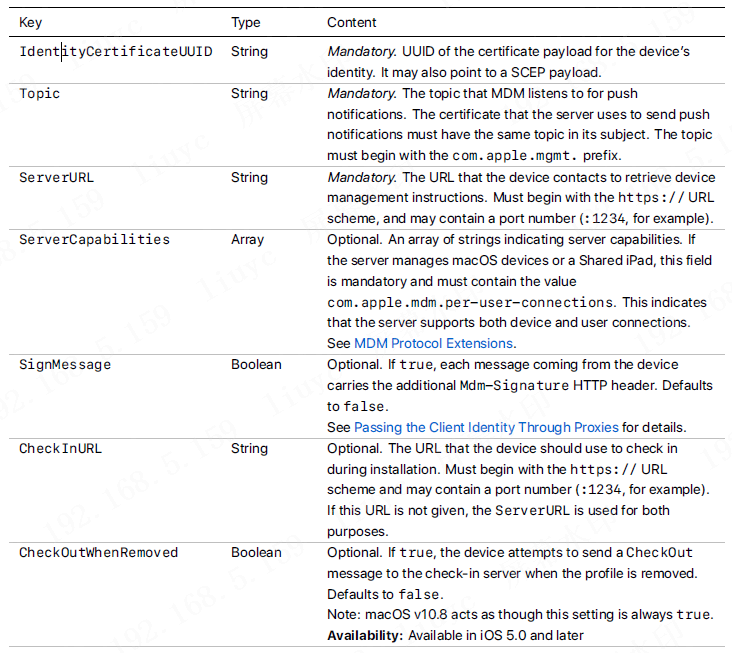
MDM遵循HTTP 3xx重定向，不需要用户交互。但是，它不记得HTTP 301(永久移动)重定向提供的URL。每个事务都从MDM payload中指定的URL开始。

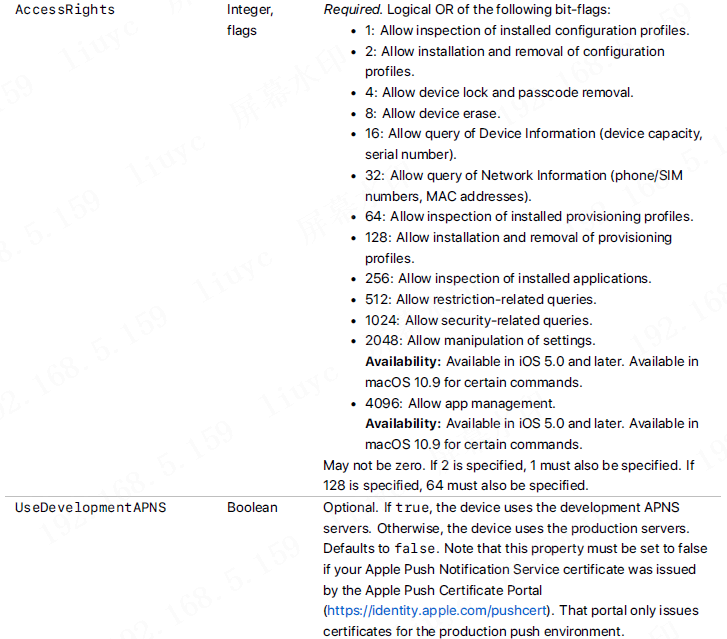
移动设备管理，顾名思义，最初是为嵌入式系统开发的。支持环境中计算机绑定到一个开的目录服务器和各种网络用户可以登录,扩展MDM网络协议开发识别和验证用户登录,这样任何网络用户也由MDM server(通过他们的用户配置文件)。对MDM协议的扩展在MDM协议扩展中进行了描述。

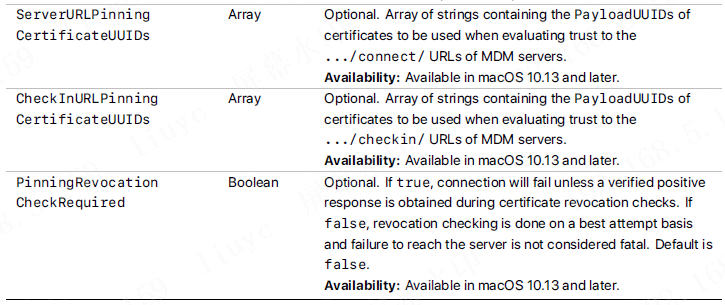
在联系MDM server进行最新设置时，可能会暂时阻止登录。设备登记也可以在计算机连接到Internet之后进行。

## Structure of MDM Payloads

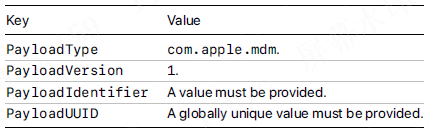
移动设备管理(MDM) payload是一个简单的属性列表，由com.apple.mdm指定在PayloadType字段中。这个 payload为MDM payloads定义了以下键:







此外，必须定义四个标准的payload键:



这些键被记录在配置文件参考中的“所有有效载荷通用的有效载荷字典键”中。

有关负载的一般结构和示例，请参阅配置配置文件参考中的“配置配置文件键引用”。

以“payload”为前缀的配置文件 payload字典键是保留的键名，绝不能被视为托管首选项。 payload字典中的任何其他键可视为该首选项域的托管首选项。

## Structure of MDM Messages

安装MDM payload后，设备侦听推送通知。MDM监听的主题与推送通知客户端证书的Subject字段中的用户ID参数的内容相对应。

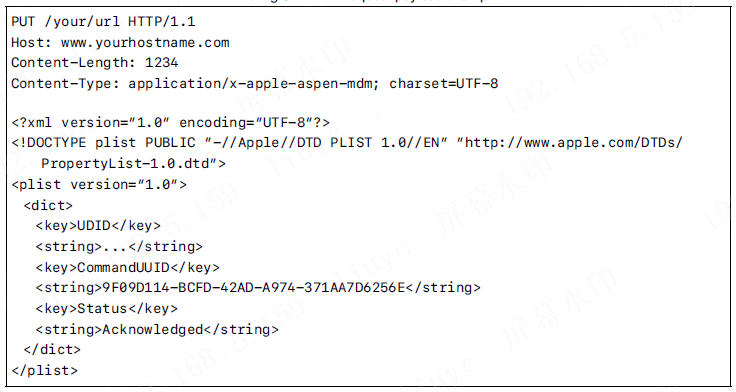
为了使设备轮询MDM server以获得命令，MDM server通过APNS网关向设备发送通知。与推送通知一起发送的消息是json格式的，必须包含PushMagic字符串作为mdm密钥的值。例如:



代替上面的PushMagicValue，在TokenUpdate消息中替换设备发送给MDM server的实际PushMagic字符串。这应该就是全部信息。不应该有aps密钥。(aps密钥仅用于第三方应用程序推送通知。)

设备通过使用HTTP PUT over TLS (SSL)联系MDM server来响应这个推送通知。此消息可能包含空闲状态，也可能包含前一个操作的结果。如果连接在设备执行任务时被切断，设备将尝试在网络恢复后再次报告其结果。

MDM请求 payload示例展示了一个MDM请求 payload示例。



服务器通过发送设备应该执行的下一个命令来响应，并将其封装在HTTP应答中。MDM服务器的响应负载的例子显示了一个示例ʼ响应负载。



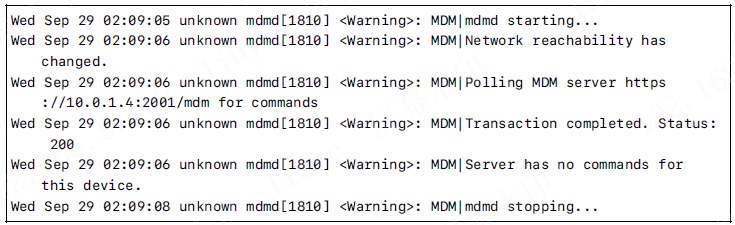
设备执行该命令，并以另一个HTTP PUT请求向MDM server发送应答。然后，MDM server可以使用下一个命令进行应答，或者通过发送200个状态(OK)和一个空的响应主体来结束连接。

空的响应体长度必须为零字节，而不是空的属性列表。

如果连接在设备执行命令时中断，设备将缓存该命令的结果并重新尝试连接到服务器，直到发送状态为止。

向设备发送几个推送通知是安全的。APNS合并多个通知，只向设备发送最后一个通知。

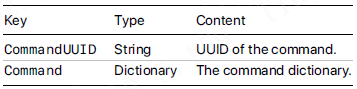
可以使用Xcode或Apple Configurator 2监视设备控制台中的MDM活动。一个健康的(但空的)推活动应该是这样的:



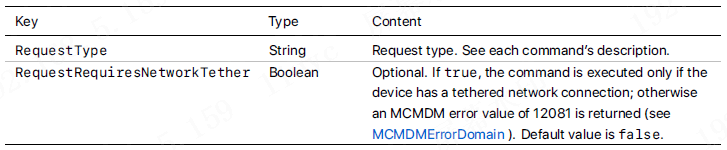
## MDM Command Payloads

主机可以通过发送包含以下必需内容的plist编码的字典向设备发送命令

密钥:

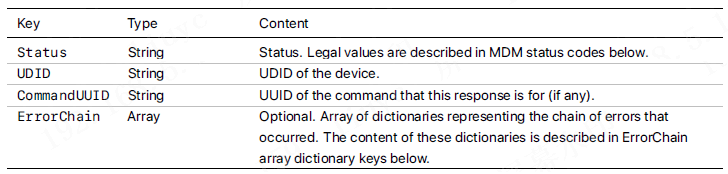


命令字典的内容必须包括以下必需的键，以及每个命令定义的其他键。

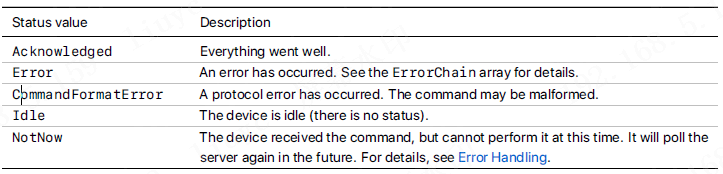


## MDM Result Payloads

设备通过发送一个包含以下密钥的plist编码的字典以及每个命令返回的其他密钥来应答主机。

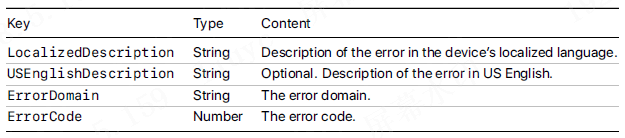


状态键包含以下字符串之一:



ErrorChain键包含一个数组。第一项是顶级错误。数组中的后续项是导致顶级错误的基础错误。

ErrorChain数组中的每个条目都包含以下字典:



ErrorDomain和ErrorCode密钥包含Apple使用的内部代码，这些代码可能对诊断有用。

您的主机不应该依赖于这些值，因为它们可能在不同的软件版本之间变化。但是，作为参考，目前的代码是在错误代码中列出的。