**概述**

IoT平台提供了接口让第三方NA接入与调用，使得第三方NA可通过接入IoT平台来控制各种设备。当前第三方NA接入IoT平台共有两种方式，分为NA主动连接IoT平台和NA接收IoT平台推送消息。下面针对第三方NA对接IoT平台地址、推送消息配置、对接方式、域名校验、TLS版本要求及加密算法套件进行详细描述。

**对接步骤**

**步骤一 获取IoT平台的IP地址和端口**

第三方NA接入首先需要获取到IoT平台对外暴露的IP地址，该地址需要向IoT平台维护人员获取；默认对接端口为8743。

**步骤二 NA接受IoT平台推送消息配置**

IoT平台收到第三方NA的请求消息，经过处理，会主动向第三方NA推送消息。为保证第三方NA能够正确收到推送消息，建议第三方NA不对消息进行白名单过滤；如果第三方NA鉴于安全考虑需要对消息进行过滤，则需要向IoT平台维护人员获取IoT平台推送消息使用的IP地址及端口信息以加入第三方NA的白名单。

**步骤三  选择合适的对接方式**

目前IoT支持HTTP和HTTPS两种接入方式，其中默认为HTTPS接入。

**使用HTTP方式接入**

如果第三方NA需要使用HTTP方式接入，则需要将第三方NA与IoT平台对接的IP提供给IoT平台维护人员，待IoT平台维护人员进行相关配置之后即可使用HTTP方式接入（HTTP接入的默认端口为8740）。

**使用HTTPS方式接入**

如果第三方NA选择HTTPS方式接入，需要考虑认证方式为单向还是双向，IoT平台默认使用双向认证方式。不论第三方NA使用单向还是双向认证，都需要将IoT平台的CA证书添加到第三方NA的信任列表中，该CA证书可向IoT平台维护人员获取，用xshell 登录服务器，输入命令#lsof -i : 8743 查找出进程号2041 8743是你请求要走的端口

然后输入命令#ps -ef|grep 2041 ,然后获取这个文件cat /opt/oss/IoM/apps/loadbalance-1.1.2.1/etc/instance/haproxy\_\_GW\_IN\_\_a6/haproxy\_\_GW\_IN\_\_a6.cfg

找到存在ca.pem的路径/opt/oss/IoM/apps/loadbalance-1.1.2.1/etc/crt/platform/app-gw/ 然后打开传输通道，将文件传到自己电脑；

如果第三方NA需使用双向认证方式，则需要保证第三方NA的设备证书是由权威机构baltimore、digicert、entrust、geotrust、globalsign、thawte、verisign或IoT平台CA颁发；反之，如果不是由上述机构或IoT平台CA颁发的设备证书，那么在与IoT平台进行对接的时候，需要提供第三方NA设备证书的签发CA证书，添加到信任列表

获取到CA证书后，将CA证书追加到/opt/oss/IoM/apps/loadbalance/etc/crt/platform/app-gw/ca.pem



添加到这个文件里面即可

       域名校验：对于HTTPS接入的场景，需考虑是否支持域名校验，如果需要，可以参考附件“TLS对接示例代码说明.docx”进行操作；反之，则无需关注。

TLS版本要求：对于TLS版本，IoT平台只支持TLS1.1和TLS1.2，因此第三方NA在进行对接时需要对TLS版本进行检查，避免由于TLS版本不对造成握手失败。

加密算法要求：出于安全考虑，消息需使用安全的加密算法加密，IoT平台支持的加密算法有：EECDH+ECDSA+SHA384、EECDH+ECDSA+SHA256、EECDH+aRSA+SHA384、EECDH+aRSA+SHA256、EECDH:EDH+aRSA、RSA+AES:HIGH

不支持的算法有：aNULL、eNULL、LOW、3DES、MD5、EXP、PSK、SRP、DSS、R4、RC4，因此第三方NA在选择加密算法时应避免选择IoT平台不支持的加密算法，以免认证不通过。

至此，NA与IoT平台对接已经完成，如有疑问，请联系IoT平台维护人员。