

很多客户在开机后进行iNode认证后会打开各种应用进行办公，有时候应用过多时会难于寻找，iNode客户端快捷链接功能免去了去找应用的烦恼。该功能可以在运行iNode后自动打开配置好的应用。此次典型配置以远程桌面功能为例进行测试，用户可以根据自己的爱好自行修改相关配置即可。

典型的Portal认证环境

iMC版本信息如下：

iMC PLAT 7.1E030P16

iMC EIA 7.1 E0307

iMC EAD 7.1 E0307

iNode客户端快捷链接典型配置本质上是应用级的单点登录，就是iNode认证成功后可以直接登录Web门户网站，不需要重新输入用户名密码，其实下发可执行程序与单点登录没有关系，本质上可以认为是在iNode上创建一个本地应用的快捷链接并能够使其自动运行。

1、首先进行portal的基本配置，包括添加接入设备、接入策略、接入服务、接入用户、portal接入设备、IP地址组、端口组配置、接入用户。此处不做Portal的重点讲解，只讲其中的配置以截图方式呈现出来。具体portal配置可以参考KMS上的各种案例。

2、点击用户-接入策略管理-业务参数配置-单点登录配置-iNode客户端快捷链接配置-修改iNode客户端快捷链接配置。其中共享秘钥可以随意填写，但只能是8位。具体填写值可以参考后续的配置关键点及注意事项。填写好共享秘钥之后，在“可执行程序”中点击“增加”按钮，此处以mstsc为例，可执行命令中填写“mstsc.exe”即可，运行方式有三种，此处选择“身份认证后运行”，即iNode认证通过后会自动运行该程序。

3、上述配置完成后，打开iNode客户端，输入portal服务器地址，用户名和密码之后点击“连接”按钮，等待认证通过后可以发现iNode自动弹出了远程桌面的连接框。并且在iNode导航栏中增加了一个快捷链接的按钮图标，如下图所示。

## 基本参数

- (1)、配置名：iNode客户端快捷链接配置名称。
- (2)、启用：如果选中则启用iNode客户端快捷链接配置，如果不选中则所有配置项都将灰显。
- (3)、共享秘钥：用于保证iNode客户端与Web应用系统之间交互的安全性。只能包含如下字符：[A, Z]U[a, z]U[0, 9]U{~!@#%&\*()\_+{}|:;<.>./}。

Web应用系统

- (1)、名称：显示在iNode客户端左侧导航栏中的Web应用系统名称。
- (2)、URL：Web应用系统页面的URL。遵循标准URL格式，即“http://XXXXXXXX”。
- (3)、校验方式：iNode客户端安全检查完成后，自动打开Web应用系统URL时需要进行校验。该参数决定了采用密码还是时间戳进行校验。默认为密码校验。
- (4)、运行方式：Web应用系统除了在左侧导航栏中显示快捷链接，还可以在iNode客户端认证过程中自动打开Web应用系统。自动打开的时机由参数“运行方式”决定。可选项为“不运行”、“身份认证后运行”、“安全认证后运行”、“安全认证成功后运行”和“安全认证失败后运行”五种方式。如果选择“不运行”，只有当用户手动触发运行时才会打开Web应用系统。如果选择“身份认证后运行”，当用户通过身份认证后就会立即打开Web应用系统。如果选择“安全认证后运行”，只有当用户使用安全策略且安全认证后（无论成功还是失败）才会打开Web应用系统。如果选择“安全认证成功后运行”，只有当用户使用安全策略且安全认证成功后才会打开Web应用系统。如果选择“安全认证失败后运行”，只有当用户使用安全策略且安全认证失败后才会打开Web应用系统。后三个选项只有部署了EAD组件后才会显示。

可执行程序

- (1)、名称：显示在iNode客户端左侧导航栏中的可执行程序名称。
- (2)、可执行命令：打开程序的命令行。
- (3)、运行方式：可执行程序除了在左侧导航栏中显示快捷链接，还可以在iNode客户端认证过程中自动执行程序。自动执行的时机由参数“运行方式”决定。可选项为“不运行”、“身份认证后运行”和“安全认证后运行”三种方式。如果选择“不运行”，只有当用户手动触发运行时才会执行该任务。如果选择“身份认证后运行”，当用户通过身份认证后就会立即执行该任务。如果选择“安全认证后运行”，只有当用户使用安全策略且安全认证后（无论成功还是失败）才会执行该任务。最后一个选项只有在EAD组件已经部署的情况下才可见。

用户选择方式

- (1)、可以选择按用户、按用户分组或所有用户分别配置。

注意事项

- (1) Web应用系统和可执行程序分别只能增加32条。

(2) 选择所有用户和选择按用户或按用户分组互斥。