CPPM 对接 AD， 加域终端机器认证失败问题

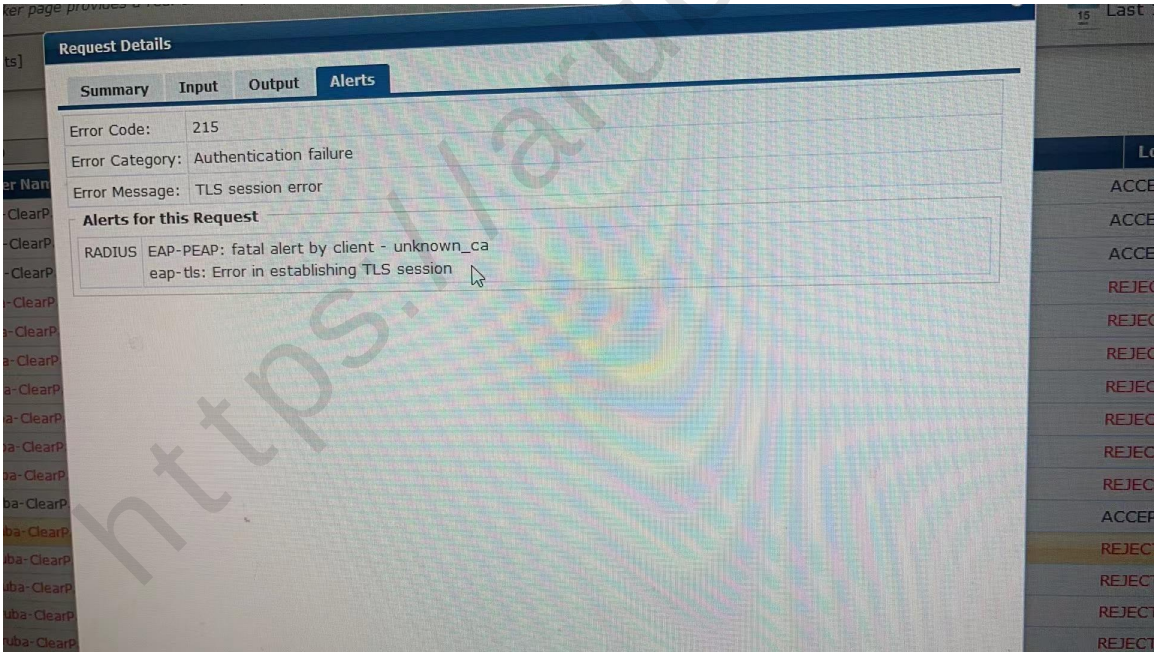
By CCE

现象描述：

CPPM v6.11.1，采用加入 AD 域的方式来实现终端的 802.1x 认证(采用 EAP—PEAP 认证方法)，加域的终端无法完成机器认证。从而导致 CPPM 无法判断加域的公司电脑和非加域的其他电脑的策略决策。

在 Access Tracker 的 Alerts 选项卡中提示 EAP—PEAP：fatal alert by cient — unknown_ca。

错误信息截图如下：



问题原因：

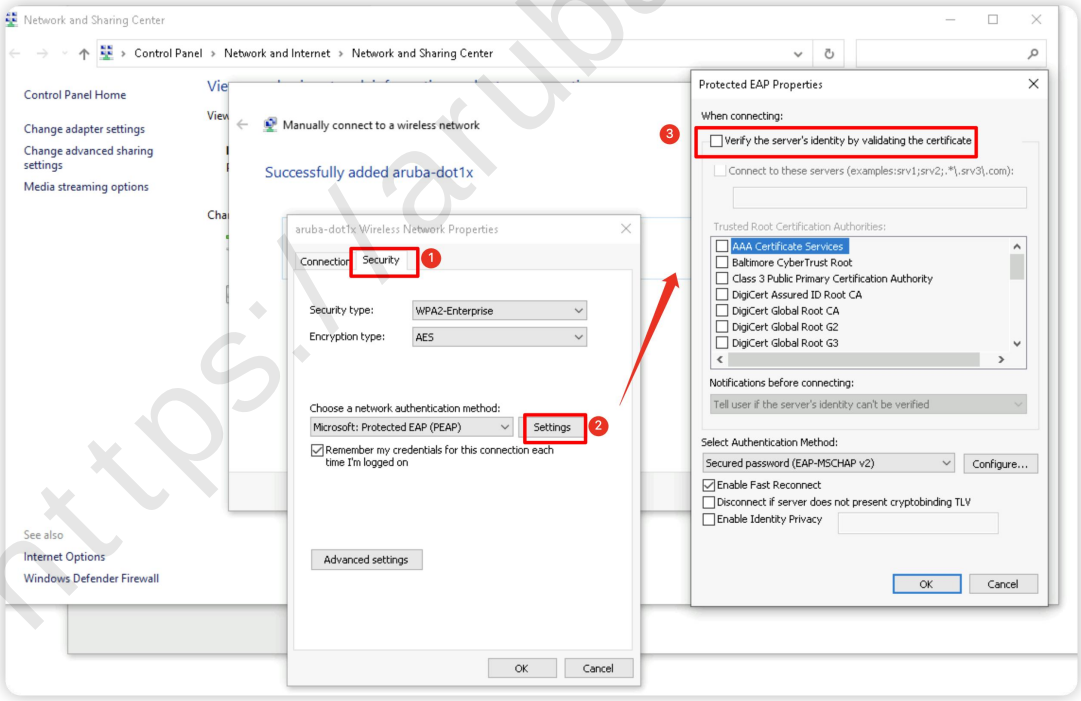
这里报错的根本原因是在 EAP—PEAP 的认证过程中(这里处于机器认证阶段)，终端是需要验证 RADIUS/EAP 服务器证书的，如果终端的机器认证的 Trusted Root Certification Authorities—受信任的根证书颁发机构中没有包含 CPPM RADIUS/EAP 服务器证书的根证书，那就会提示 unknown _ca。

解决办法：

1） 如果客户环境中 AD 没有启用证书服务模块，我们可以在终端上针对该无线配置， 去掉验证服务器证书的设置。

在终端的无线配置中， 通过验证证书来识别服务器身份选项前面的勾去掉，当然你可以通过 AD 组策略统一下发该无线配置给到加域的所有终端上。

配置截图如下：

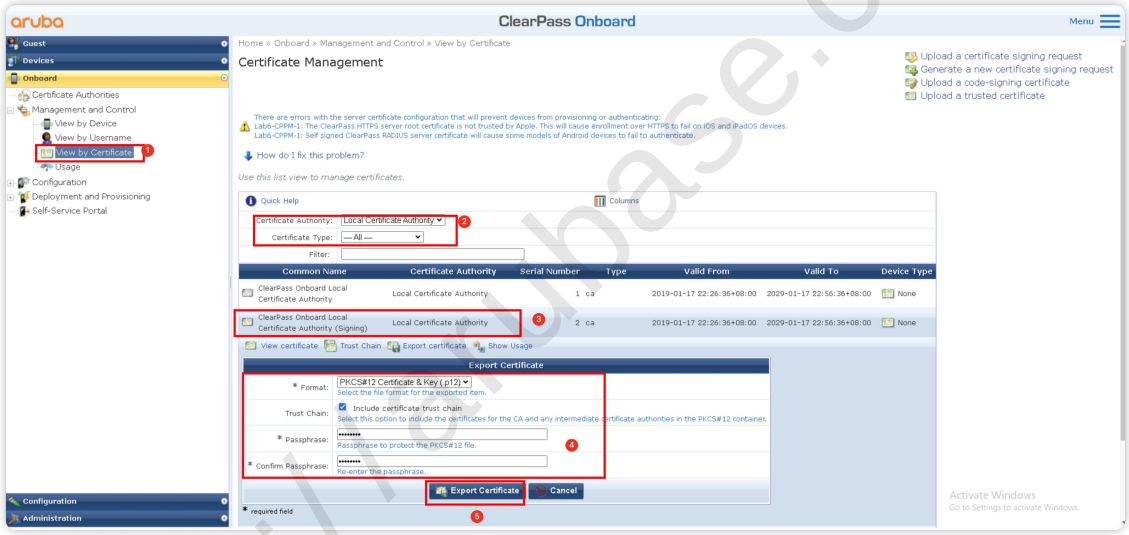


2）如果客户环境中 AD 没有开启证书服务即 ADCS，但是需要终端来验证 RADIUS/EAP 服务器证书，那么在终端机器认证的 Trusted Root Certification Authorities—受

信任的根证书颁发机构中，导入 CPPM 的 RADIUS/EAP 服务器证书的 ROOT CA（此时的 CPPM 的 RADIUS/EAP 服务器证书是采用 Local Onboard CA 做私签证书，需要先将 Onboard Root CA 导出为.P12 格式，设置 Private Key）。

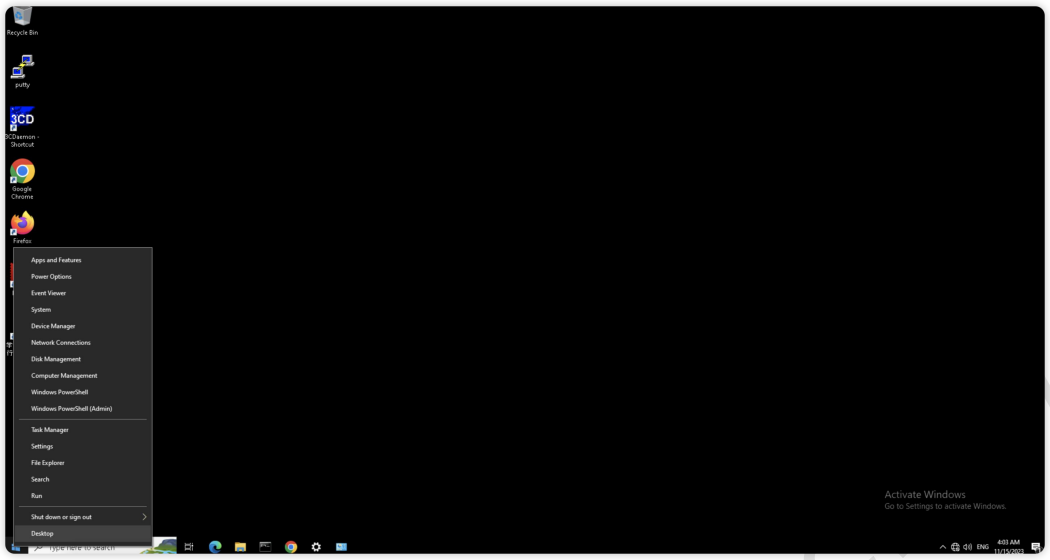
配置截图如下：

i） 在 CPPM Onboard 模块中，将 ClearPass Onboard Local Certificate Authority (Signing)这张根证书导出到 终端本地，格式选择.P12， Trust Chain 勾选，Passphrase 设置 自定义的密码(这个也是导入证书的 Private Key)

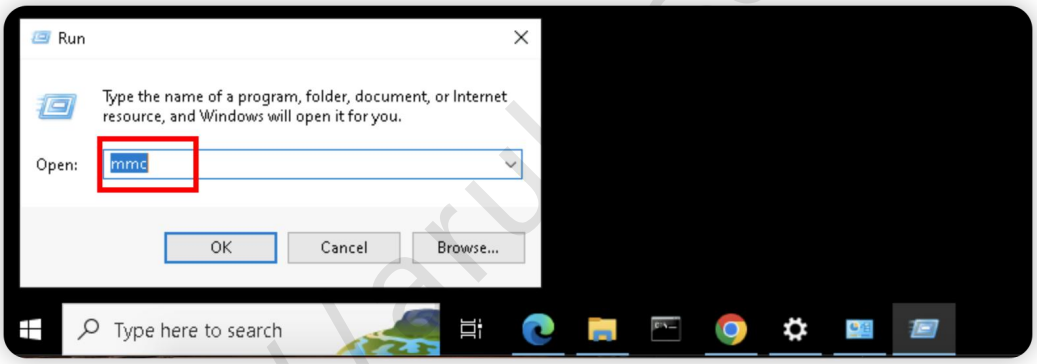


ii）B：在 Windows 终端上导入根证书到 Trusted Root Certification Authorities—受信任的根证书颁发机构中。 由于我们是在机器认证阶段出现问题，所以需要将该根证书导入到 机器证书的受信任的根证书颁发机构中。

鼠标右击下左下角的 Start 图标，弹出菜单，选择 Run。



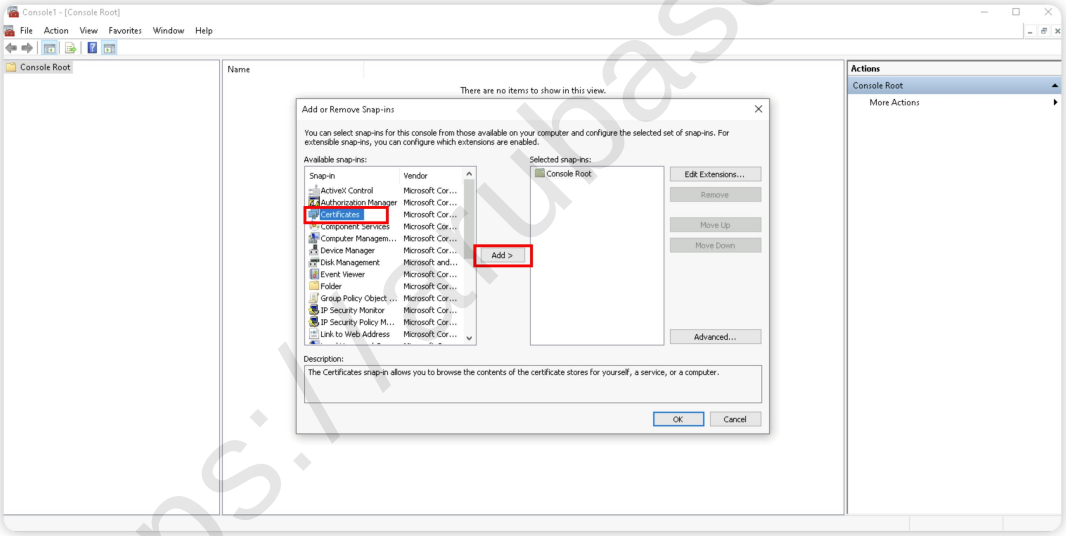
在 Run 窗口输入 mmc



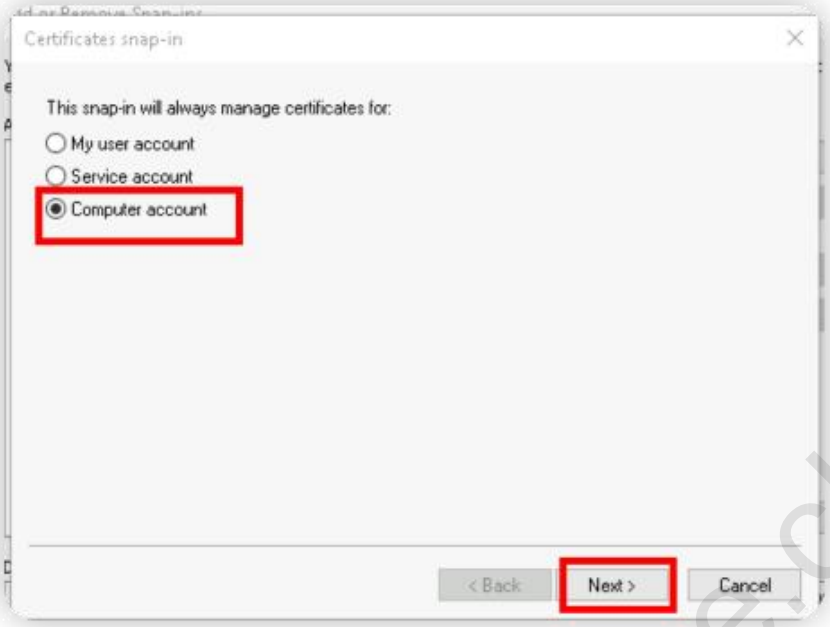
进入到 Microsoft Management Console 界面，

点击 File→Add/Remove Snap-ins

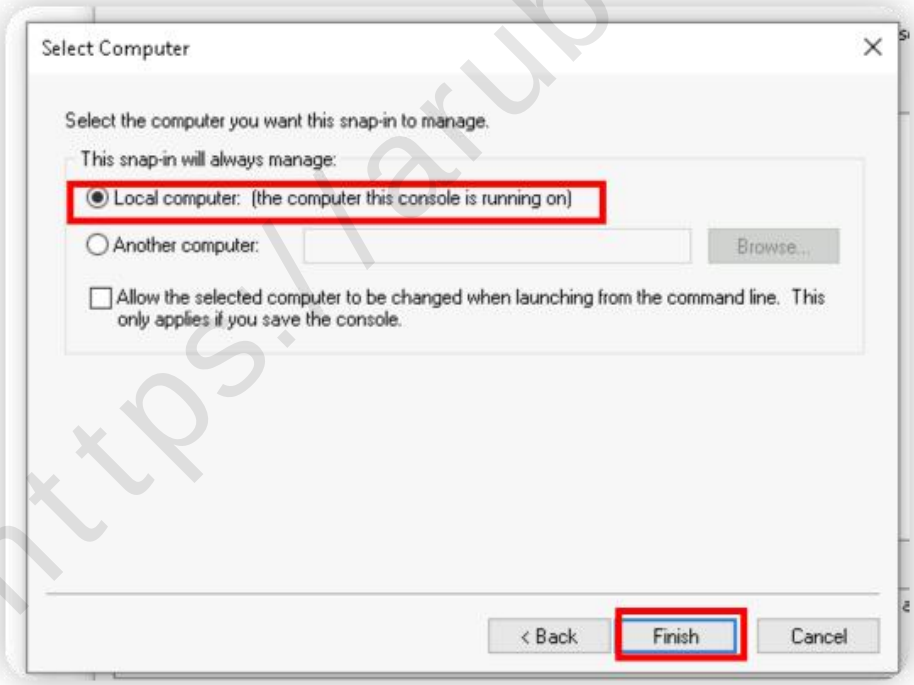
在 Available snap—ins 中选择 Certificates， 然后点击中间的 Add 按钮



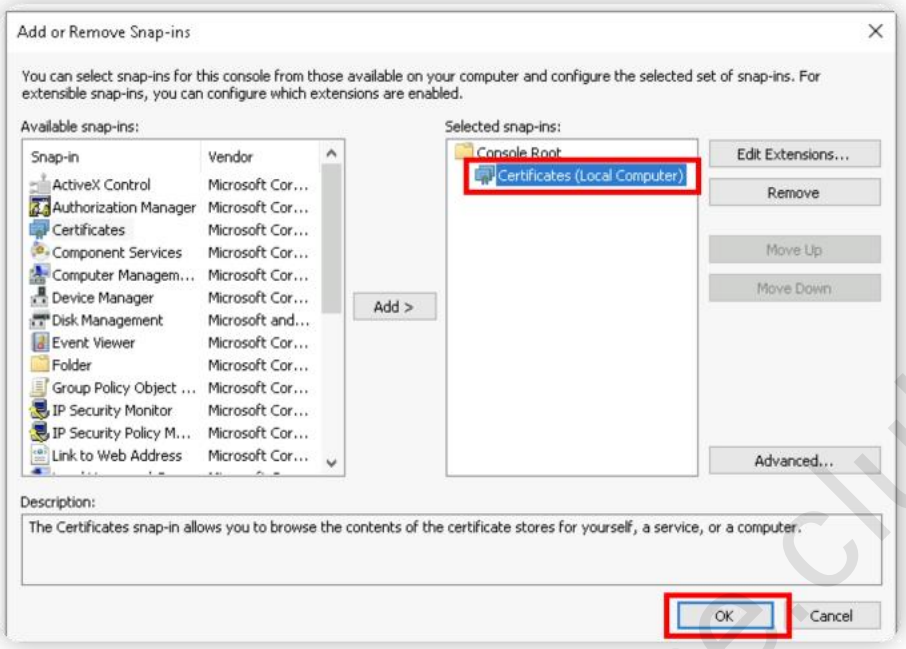
选择 Computer account



选择 Local computer

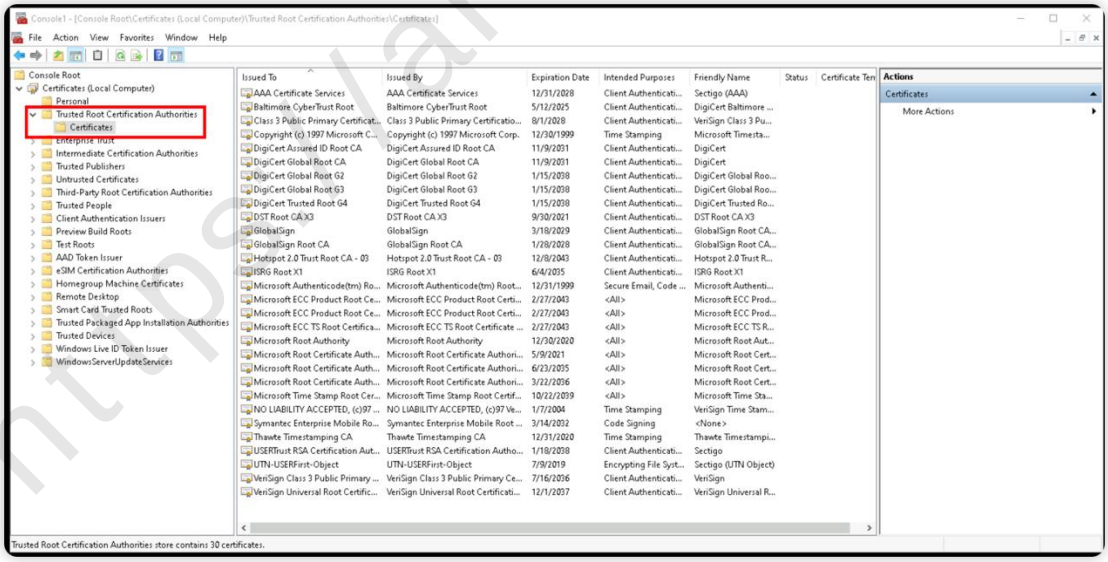


看到 Selected snap-ins 中已经包含了 Certificates(Local Computer)，点击 OK 按钮

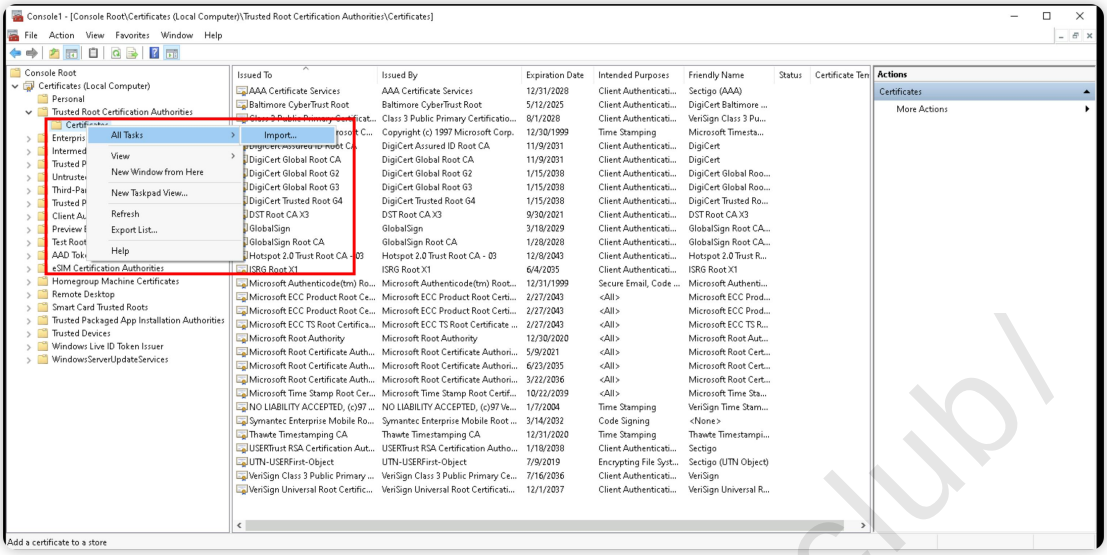


点击 Certificates（Local Computer)前面的箭头，展开配置，

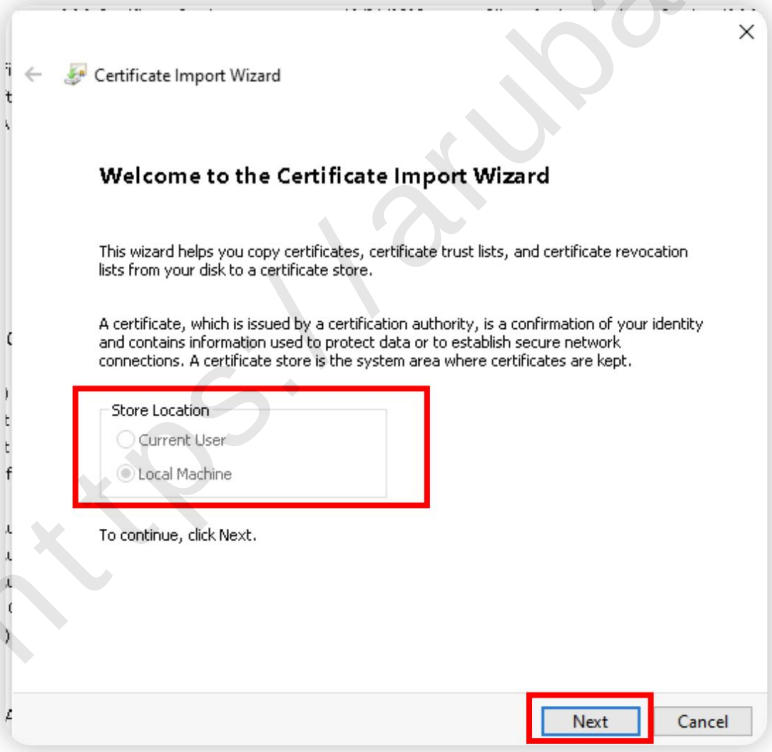
选择 Trusted Root Certification Authorities→Certificates， 查看现有的根证书列表，应该是没有 Clearpass Onboard Local Certificate Authority 的



鼠标右击下 Trusted Root Certification Authorities→Certificates，弹出菜单，选择 All Tasks—→ Import



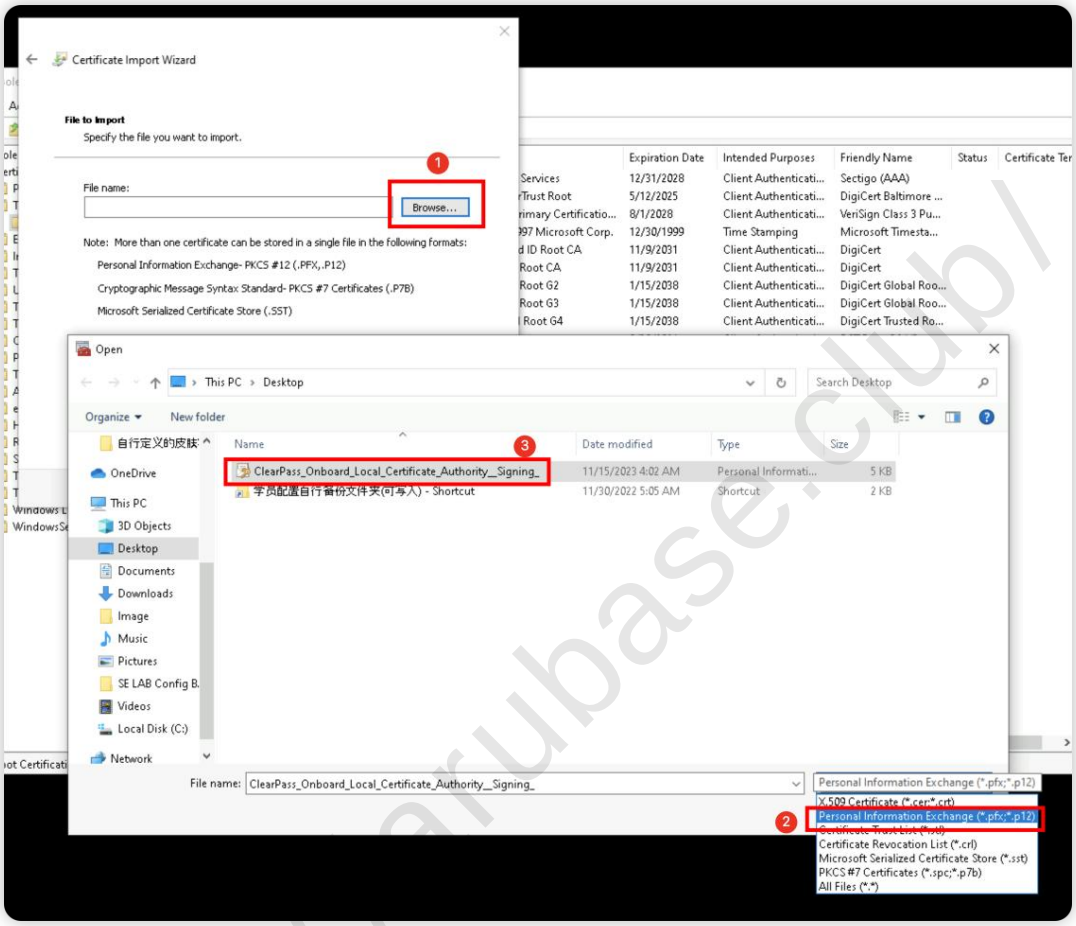
弹出 Import Wizard 的界面， 在 Store Location 中默认选择了 Local Machine(灰色)，点击 Next 按钮



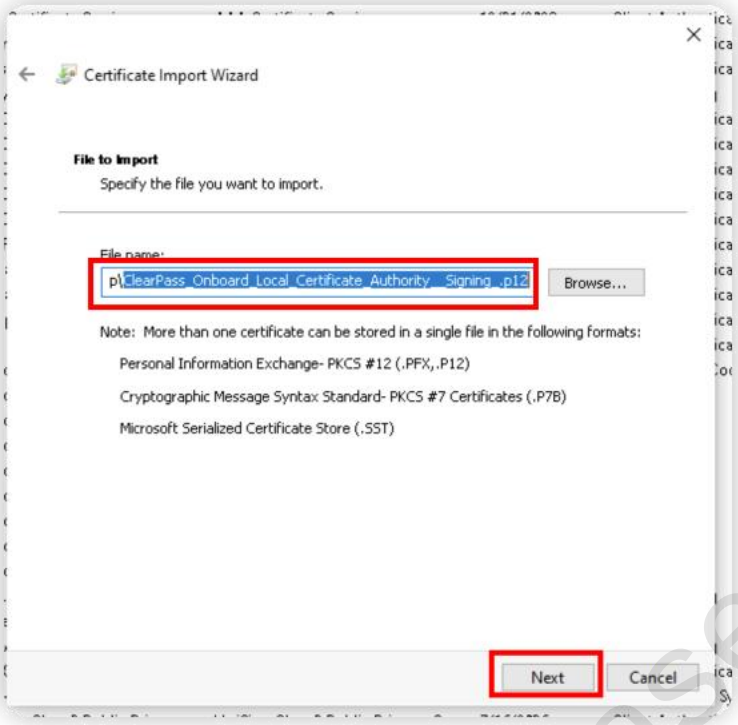
然后鼠标点击 Browse 来选择 Clearpass Onboard Local Certificate Authoriy_signing.p12，

注意右下角的类型中要先选择*.P12 格式，这样才能看到和选择你的根证书。

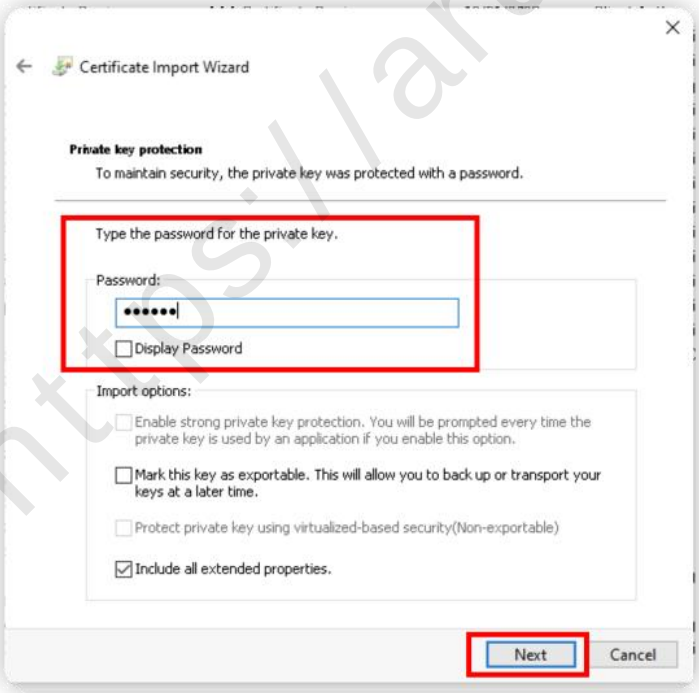
最后鼠标点击 Open 按钮



选择好根证书后，点击 Next 按钮



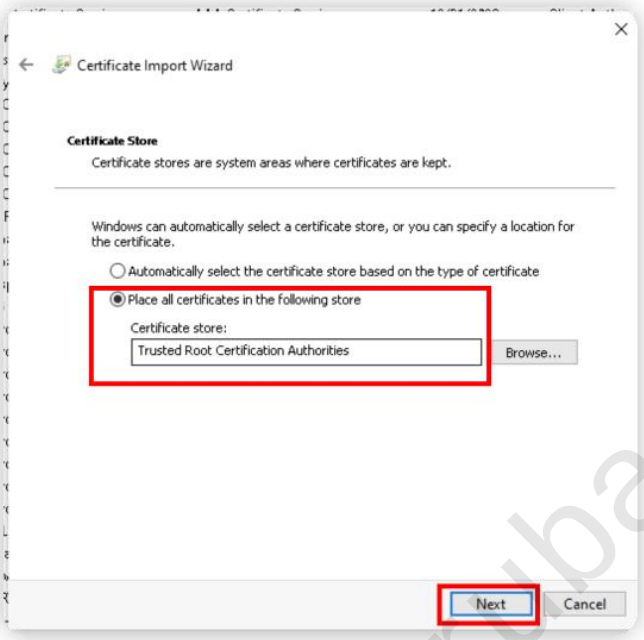
接着需要好输入 Password(就是之前在 CPPM 上导出证书时设置的密码)。点击 Next 按钮



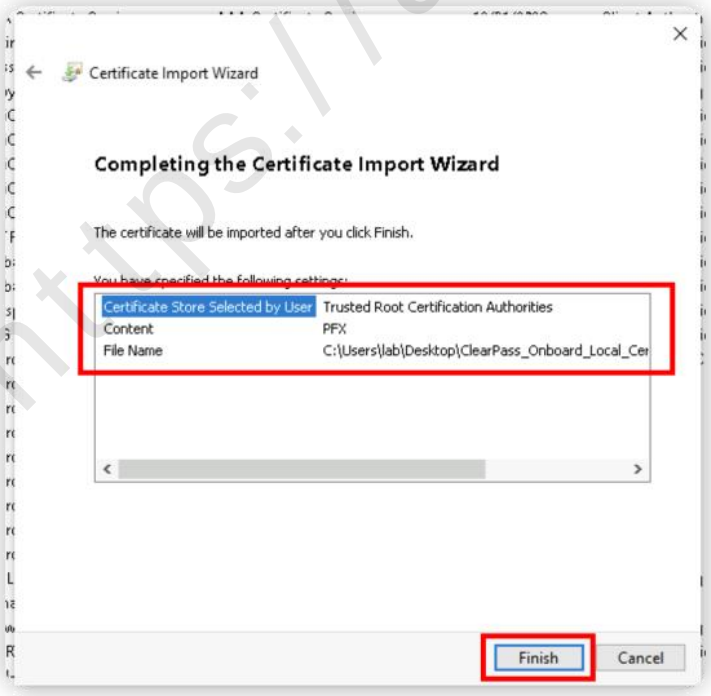
在 Certificate Store 界面中，系统自动设置了 Place all certificates in the following store

Certificate store：Trusted Root Certification Authorities

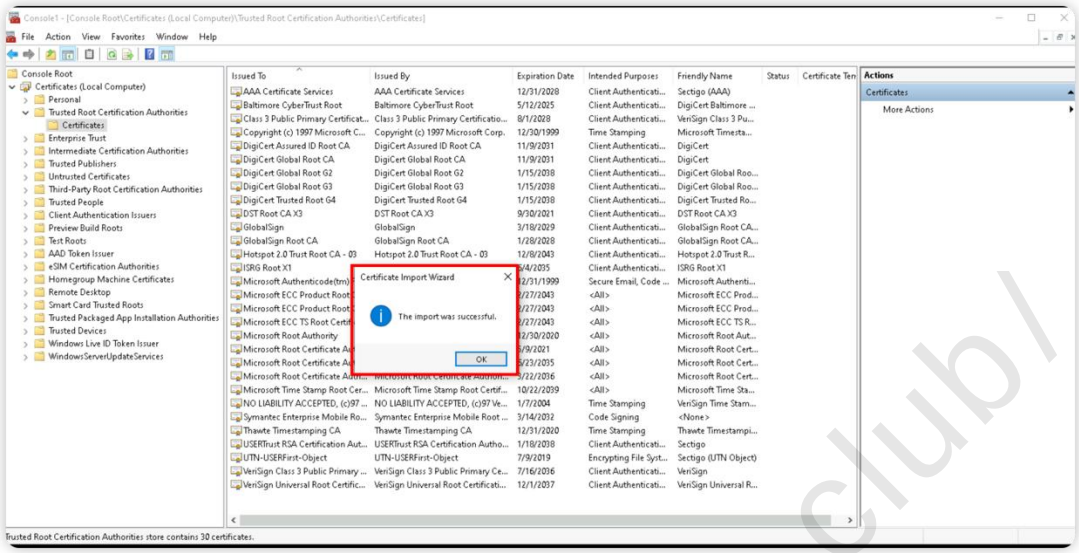
鼠标点击 Next 按钮



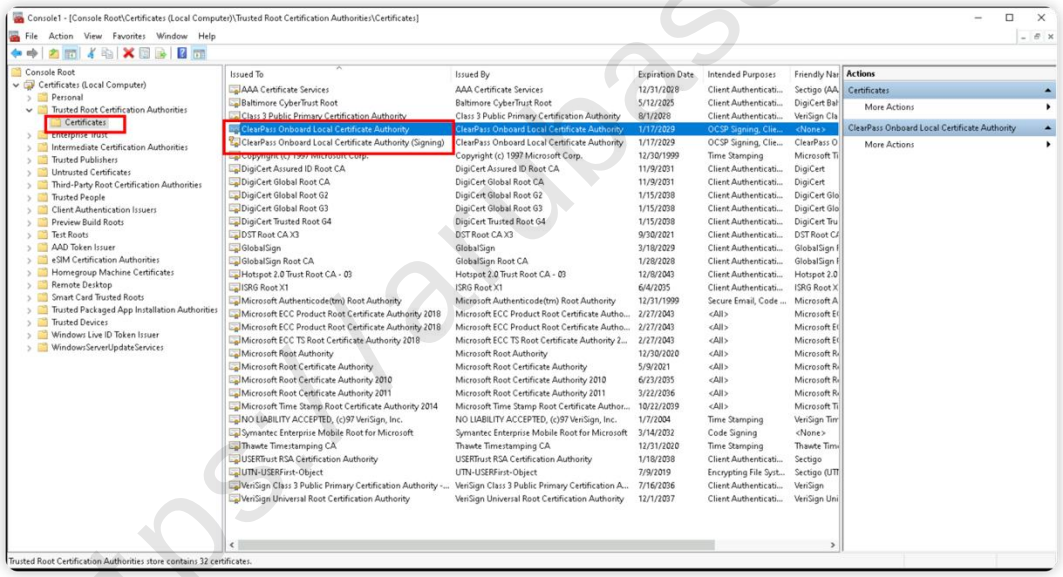
鼠标点击 Finish 按钮



最后系统提示证书导入成功，鼠标点击 ok 按钮



在 证书列表中，可以看到 Clearpass Onboard Local Certificate Authoriy



Note：导入后，也会自动同步到 Current user 证书的根证书颁发机构信任列表中

3）如果客户环境中 AD 开启了证书服务即 ADCS，需要终端验证 RADIUS/EAP 服务器证书，那需要事先在加域的终端上将 ADCS 的根证书导入到机器认证的受信任的根证书颁发机构中，接着还需要由 ADCS 给 CPPM 签发一张 RADIUS/EAP 服务器证书并导入到 CPPM 中(针对 EAP—PEAP 认知方法)。 如果是基于 EAP—TLS 认证方法，由于是双向验证

证书，所以在之前的基础上，另外还需要为终端签发机器认证和用户认证的 TLS 证书，用于无线配置中的使用。

关于如何使用 ADCS 为终端签发和导入 TLS-CIient 和 Root CA 证书的相关配置，请参考：

https://arubase.club/archives/5601
https://arubase.club/archives/6422

关于如何使用 ADCS 给 CPPM 签发一张 RADIUS/EAP 服务器证书的相关配置，请参考：

https://arubase.club/archives/8249

注意：以上方法是采用任何一种即可。 本文介绍的是机器认证失败，如果是用户认证阶段失败提示相同错误，也可以参考上述方法，但是需要注意用户认证的：Trusted Root Certification Authorities 中也需要有 Root CA 存在。