在思科身份服务引擎 1.2 中自定义访客 Web 门户

安全访问操作指南系列

日期：2014 年 12 月 18 日

作者：Imran Bashir、Jason Kunst、Hsing-Tsu Lai
（思科身份服务引擎技术营销工程师）

目录

简介

本解决方案说明了如何根据访客所在的 AD 组为其显示不同的自定义成功接入页面。

使用案例

在此需求中，我们以某家公司为例。该公司有许多 Apple 承包商和 Microsoft 承包商需要访问其 Web 门户，他们希望为不同类型的承包商提供自定义的身份服务引擎 (ISE) Web 身份验证成功接入页面。

详细信息：

- 有两家不同公司的承包商连接到我的网络。例如：Apple_Contractor 和 Microsoft_Contractor。
- 这些承包商使用其 Active Directory 凭证登录集中式 Web 身份验证（访客）门户，从而连接到网络。
- 在承包商登录 Web 身份验证（访客）门户后，根据他们所登录的组，会为他们提供不同的自定义的成功接入页面：
  - 应为 Apple 承包商提供 Apple 自定义的成功接入页面。
  - 应为 Microsoft 承包商提供 Microsoft 自定义的成功接入页面。

问题

在 ISE 中，成功接入页面是采用硬编码方式写到访客门户中的。因此，如果在承包商登录流程中仅使用一个已配置的门户，则不可能根据其所在 AD 组显示不同的成功接入页面。

解决方案

利用设备注册 Web 身份验证流程，根据 AD 凭证提供自定义的成功接入页面。

注意

- 由于无法通过 purge 命令清除终端组，因此您需要执行手动清除。ISE 1.3 具有自动清除每个终端组的功能。
- 由于门户的变迁和构建方式已发生显著变化，本解决方案可能会在升级到 1.3 版本后出现故障。如果您计划升级，建议您对系统在升级后的运行方式进行验证。
- ISE 1.3 完成自定义工作的方式与之前有所不同，本文档对此不再赘述。

一般情况下，建议在将任何新解决方案投入生产之前，先在实验室中对其进行试验和验证。

配置步骤

此配置文档假定您具有一些配置 ISE 1.2 身份验证和访客接入授权策略的经验。以下将介绍配置过程中出现的相关屏幕以及完成配置所需的基本步骤。

创建终端组

为每个承包商（访客）类型创建必要的终端组。

步骤 1 为承包商终端创建两个终端身份组。MAC 地址会在重定向到 DRW 门户之后被注册。
步骤 2 导航至 **Administration > Groups > Endpoint Identity Groups**。
步骤 3 添加以下终端组。

- **Apple_Contractor**：用于 Apple 承包商的终端身份组。
- **Microsoft_Contractor**：用于 Microsoft 承包商的终端身份组。

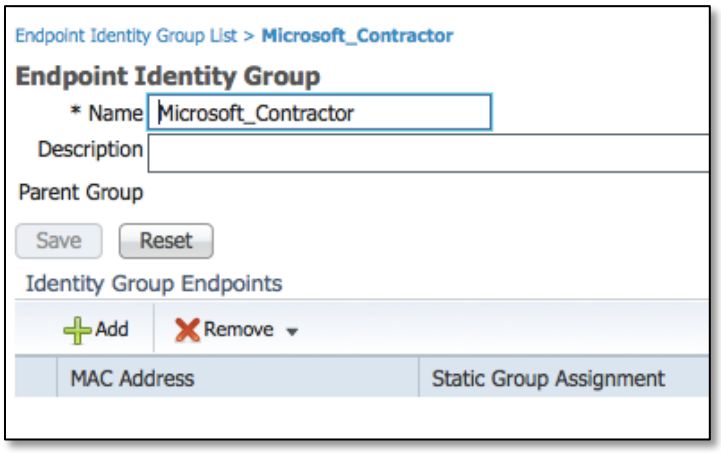

图 1. 终端身份组

步骤 4 创建 3 个自定义的访客门户。

- 具有成功接入页面计时器的自定义 CWA 登录门户，用于触发重定向。
- 2 个 DRW 页面（每个承包商组 1 个），用于将 MAC 地址插入到相应的终端身份组中。

在创建您自己的自定义门户页面时，请使用此链接作为参考：[如何自定义 ISE12 Web 门户]。

创建默认门户和承包商门户

第一个门户为 Default_Custom

步骤 1 导航至 **Administration > Settings > Guest > Multi-Portal Configurations**。

第一个门户为 Default_Custom。

这是默认门户，所有连接到开放式 SSID (MAB) 的终端都将在该门户作为 CWA 的结果被重定向。成功接入页面被设置为在 3 秒后由您的重定向 ACL 重定向到被阻止的 URL。

此代码的示例：

步骤 2 将以下 HTML 重定向代码放在 HTML 代码的 <HEAD> 和 </HEAD> 标签之间。

```
<meta HTTP-EQUIV="REFRESH" content="3" url=" http://www.yahoo.com">

The above HTML redirect code will redirect your visitors to another web page instantly.
The content="3" is the time in seconds before redirection takes place. Don't set it lower then
this value as this is required to be longer than the COA time.
```

步骤 3 映射所要使用的已上传文件。您至少需要映射登录页面、成功接入页面和错误页面。

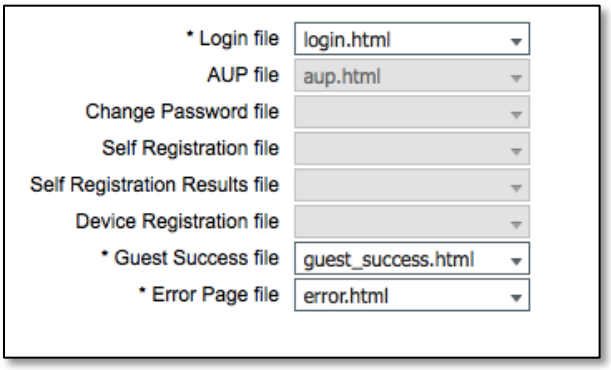

图 2. 登录文件

第二个门户为 APPLE_DRW

步骤 4 为每个承包商类型创建一个门户。对于每个承包商类型，步骤都是相同的。

这是自定义 DRW 门户。此门户将 Apple 承包商的设备 MAC 地址放入 Apple_Contractor 终端身份组中。

此页面应使用面向 Apple 承包商的信息进行自定义。

示例：欢迎您，Apple 用户！以下是有关 Apple 的信息。

您可以使用以前用过的相同操作文档来创建上述页面。这些页面的类型是相同的。

步骤 5 **禁用 AUP**（取消选中“Guest users should agree to an acceptable use policy”复选框）。

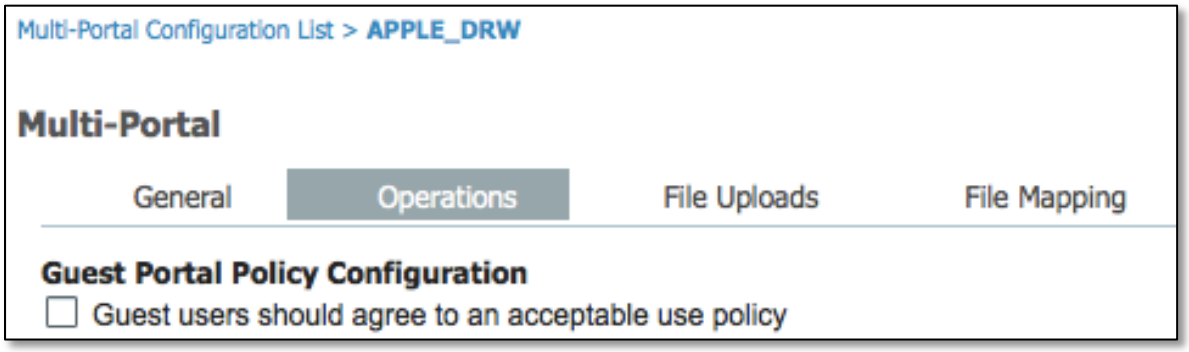

图 3. Multi-Portal Configuration List > Apple_DRW

步骤 6 您必须自定义和映射需要进行自定义和映射的成功接入页面和错误页面。

步骤 7 **映射**已上传的文件。

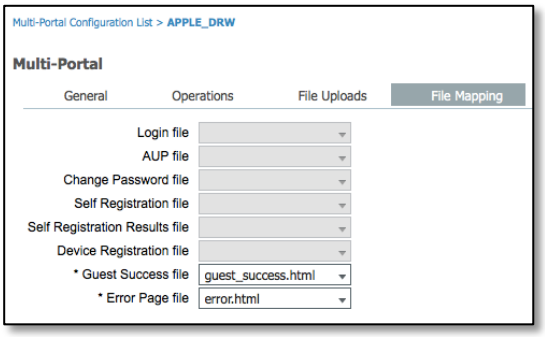

图 4. Multi-Portal Configuration List> Apple_DRW - 错误页面

使用与上面相同的步骤为另一个承包商类型创建一个门户：

第三个门户为 MICROSOFT_DRW。

创建身份验证策略

创建身份验证策略，以作为 MAC 身份验证绕行 (MAB) 的结果进行重定向

步骤 1 导航至 **Policy > Authentication**。
步骤 2 创建要匹配的 **MAB** 规则。

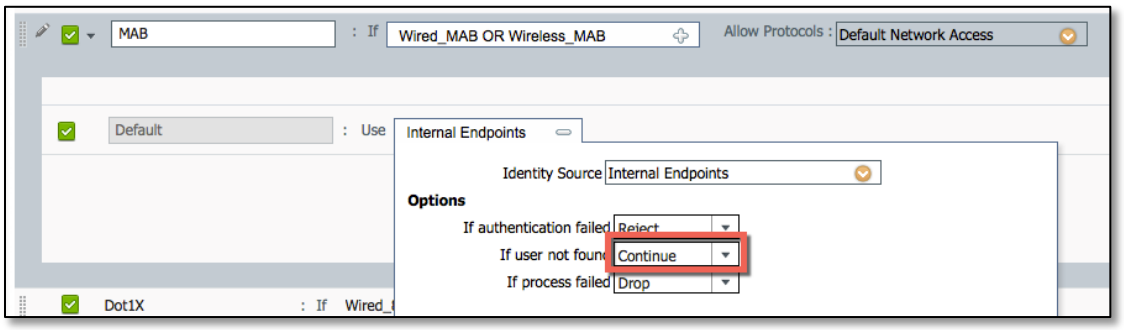

图 5. MAB 规则

步骤 3 更改 **Guest Portal Sequence** 以包括您的 Active Directory 实例。
步骤 4 导航至 **Administration > Identity Source Sequence > Guest_Portal_Sequence**。
步骤 5 将您的 AD 实例移至右侧。

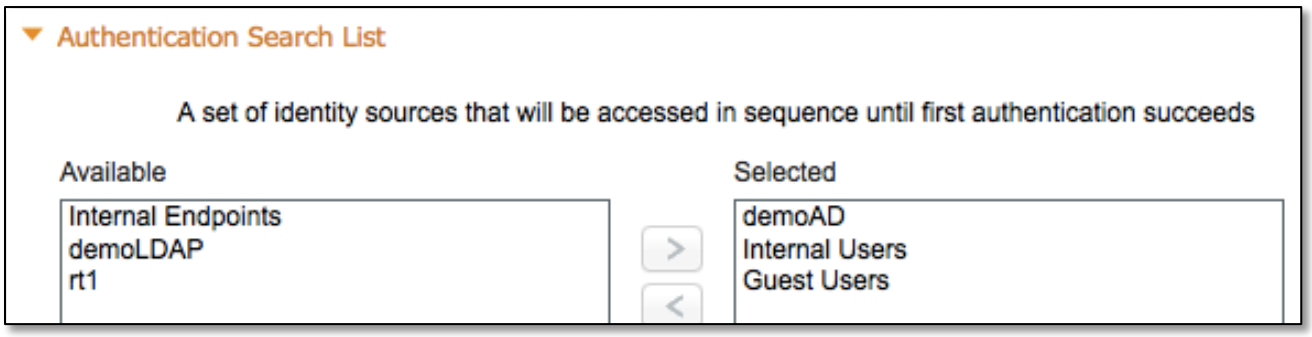

图 6. 身份验证搜索列表

创建授权配置文件

步骤 1 为三个不同的门户分别创建**授权配置文件**。
步骤 2 导航至 **Policy > Results > Authorization > Authorization Profiles**。

创建以下三个配置文件：WLC-CWA、DRW_Apple、DRW_Microsoft。

WLC-CWA 即为自定义访客门户重定向基本配置文件

这是承包商在接入网络时首先看到的门户。

- 对于“Web Redirection”，选择“Centralized Web Auth”。
- ACL“WLC-ACL_ISE-RESTRICTED”将作为您的重定向 ACL 被传递到控制器。
- Default_Custom 即为您创建的门户。

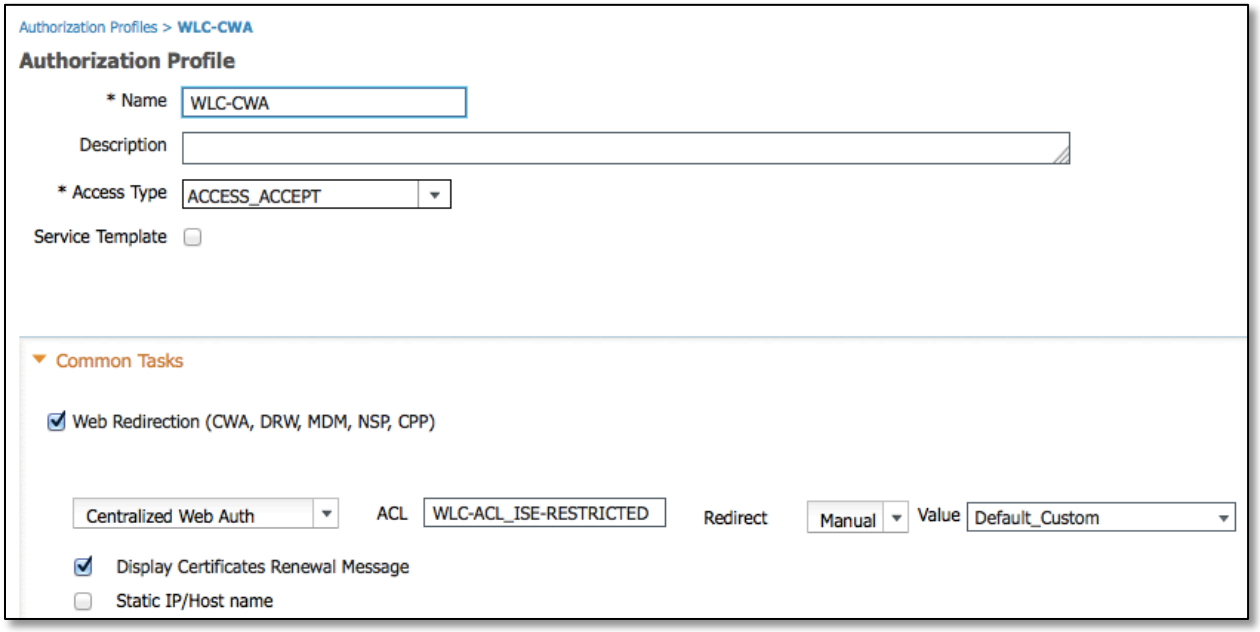

图 7. 授权配置文件 - WLC-CWA

DRW_Apple：用于 Apple 承包商的 DRW 策略

这是 Apple 承包商在基于 CWA 门户进行身份验证之后重定向的目标门户。

- 对于“Web Redirection”，选择“Device Registration Web Auth”。
- ACL“WLC-ACL_ISE-RESTRICTED”将作为您的重定向 ACL 被传递到控制器。
- APPLE_DRW 是您为确保 Apple 承包商的 DRW 成功创建的门户。

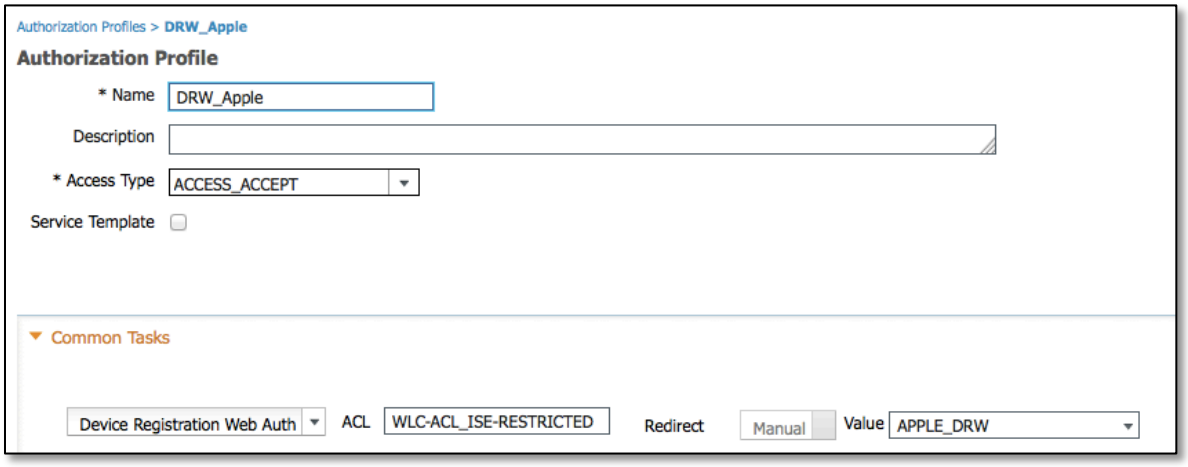

图 8. 授权配置文件 - DRW_Apple

DRW_Microsoft：用于 Microsoft 承包商的 DRW 策略

这是 Microsoft 承包商在基于 CWA 门户进行身份验证之后重定向的目标门户。

- 对于“Web Redirection”，选择“Device Registration Web Auth”。
- ACL“WLC-ACL_ISE-RESTRICTED”将作为您的重定向 ACL 被传递到控制器。
- MICROSOFT_DRW 是您为确保 Microsoft 承包商的 DRW 成功创建的门户。

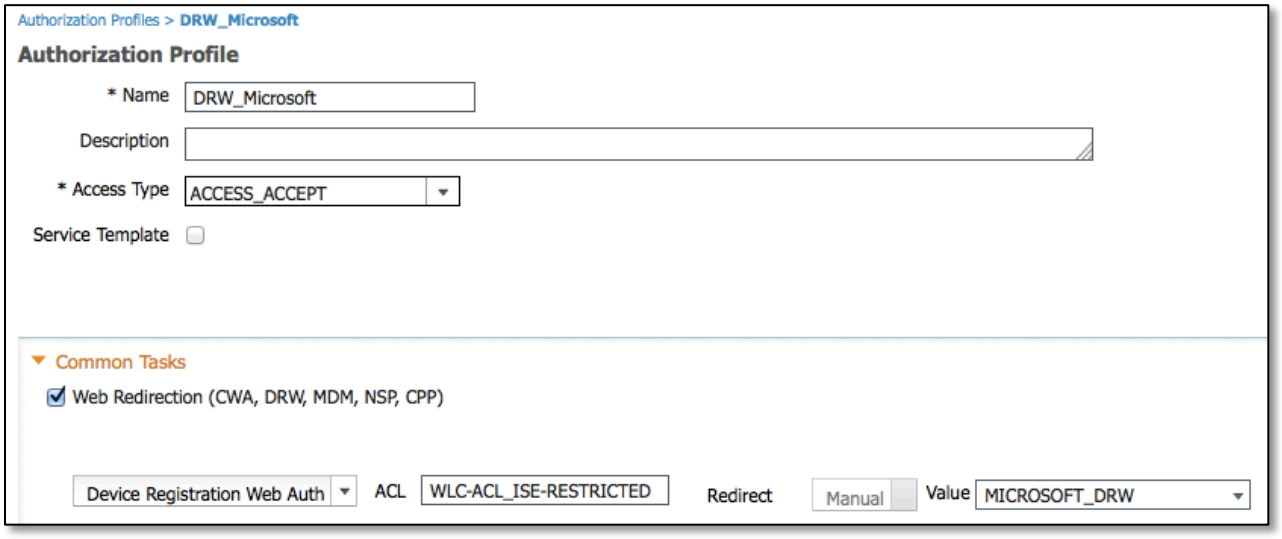

图 9. 授权配置文件 - DRW_Microsoft

创建授权策略

最终根据以下信息和截图创建授权策略。

步骤 1 导航至 **Policy** > **Authorization**。

虽然没有要求，但建议按照与下图相同的顺序输入策略。

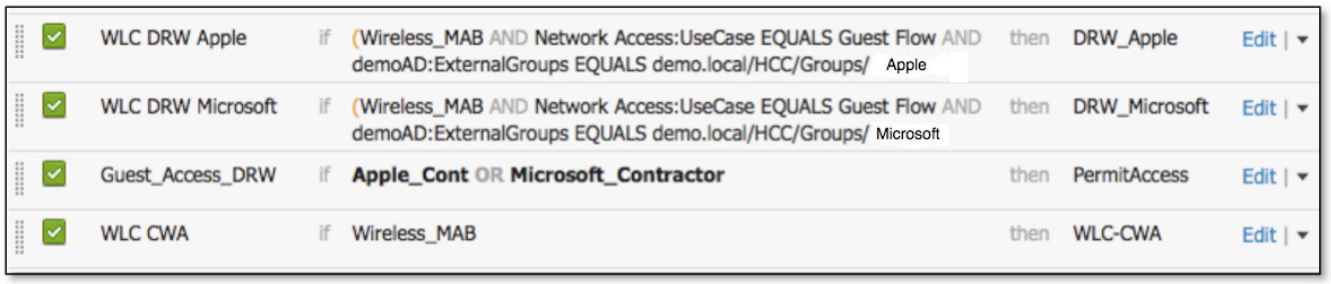

图 10. 授权策略

WLC DRW Apple 即为设备注册的授权策略

Apple 承包商的 Web 身份验证需检查以下事项：

- 设备通过无线连接。
- 设备自之前使用 WLC CWA 策略进行身份验证后仍处于访客流状态。
- 用户属于 Apple AD 组。

结果：获取此 MAC 地址并将其放入 Apple_*Contractor* 终端身份组，*然后发出 COA_Session_Terminate 命令*。

WLC DRW Microsoft 即为设备注册的授权策略

Microsoft 承包商的 Web 身份验证需检查以下事项：

- 设备通过无线连接。
- 设备自之前使用 WLC CWA 策略进行身份验证后仍处于访客流状态。
- 用户属于 Microsoft AD 组。

结果：获取此 MAC 地址并将其放入 Microsoft_Contractor 终端身份组，*然后发出 COA_Session_Terminate 命令*。

Guest_Access_DRW 即为授权策略

如果采用授予 Apple_Contractor 和 Microsoft-Contractor 差异化的接入权限的策略，则根据终端身份组授予员工接入权限的策略还可以拆分为多个策略。

如果终端身份组是 Apple_Contractor 或 Microsoft_Contractor，则允许接入。

注：MAC 地址已按照之前定义的 DRW 策略插入到这些终端身份组中。

WLC CWA 即为承包商要登录的默认自定义门户的重定向

总结

具体应用过程总结如下：

步骤 1 承包商连接到开放式无线网络。
步骤 2 设备重定向到 Web 身份验证门户。
步骤 3 承包商使用其 AD 凭证登录。
步骤 4 当成功接入页面显示时，发送 COA 以重新为会话授权。
步骤 5 成功接入页面将自动尝试访问 yahoo.com，并再次重定向到 DRW 门户。
步骤 6 DRW 门户会自动将终端注册到相应的组中，并提供自定义的成功接入页面。
步骤 7 COA 再次发生，并且设备在终端组授权获得授权。
步骤 8 自此之后，系统将允许连接直接接入（除非终端从相应承包商终端组中清除）。

有关详细信息，请查看我们提供的其他操作指南。