解决常见ISE访客访问问题

目录

简介

本文档介绍如何解决部署中的常见访客问题、如何隔离和检查问题以及要尝试的简单解决方法。

前提条件

要求

Cisco 建议您了解以下主题：

- ISE访客配置
- 网络接入设备(NAD)上的CoA配置
- 需要工作站上的捕获工具。

使用的组件

本文档中的信息基于 思科ISE版本2.6和：

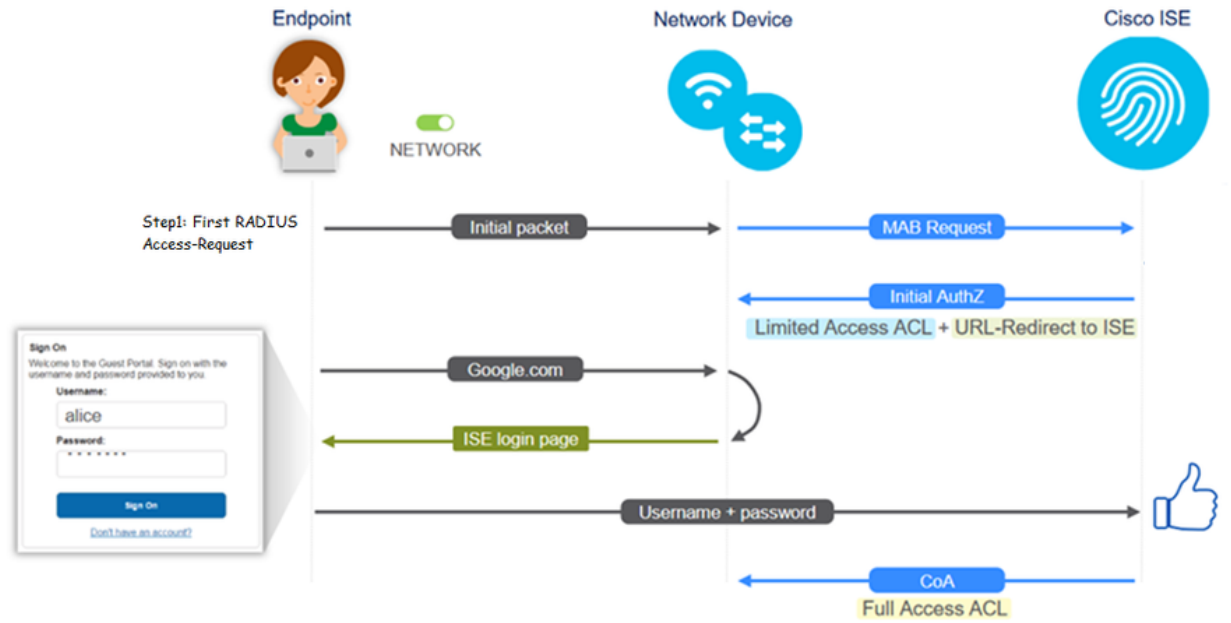
- WLC 5500
- Catalyst交换机3850 15.x版本
- Windows 10工作站

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

访客流

访客流概述类似于有线或无线设置。此流程图图像可供整个文档参考。它有助于直观地显示步骤和

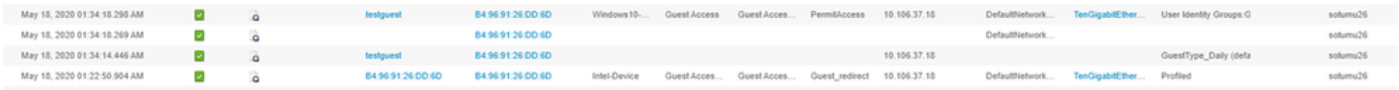
实体。



通过过滤终端ID，还可以在ISE实时日志[Operations > RADIUS Live Logs]上跟踪该流：

- MAB身份验证成功 — 用户名字段具有MAC地址 — URL被推送到NAD — 用户获取门户
- Guest Authentication successful - username字段具有访客用户名，已标识为GuestType_Daily（或访客用户的已配置类型）
- CoA initiated — 用户名字段为空，详细报告显示动态授权成功
- 提供访客接入

图像中的事件顺序（从下到上）



通用部署指南

以下是一些配置帮助链接。对于任何特定使用案例故障排除，了解理想或预期配置都有帮助。

- 有线访客配置
- 无线访客配置
- 无线访客CWA，带FlexAuth AP

常见问题

本文档主要解决以下问题：

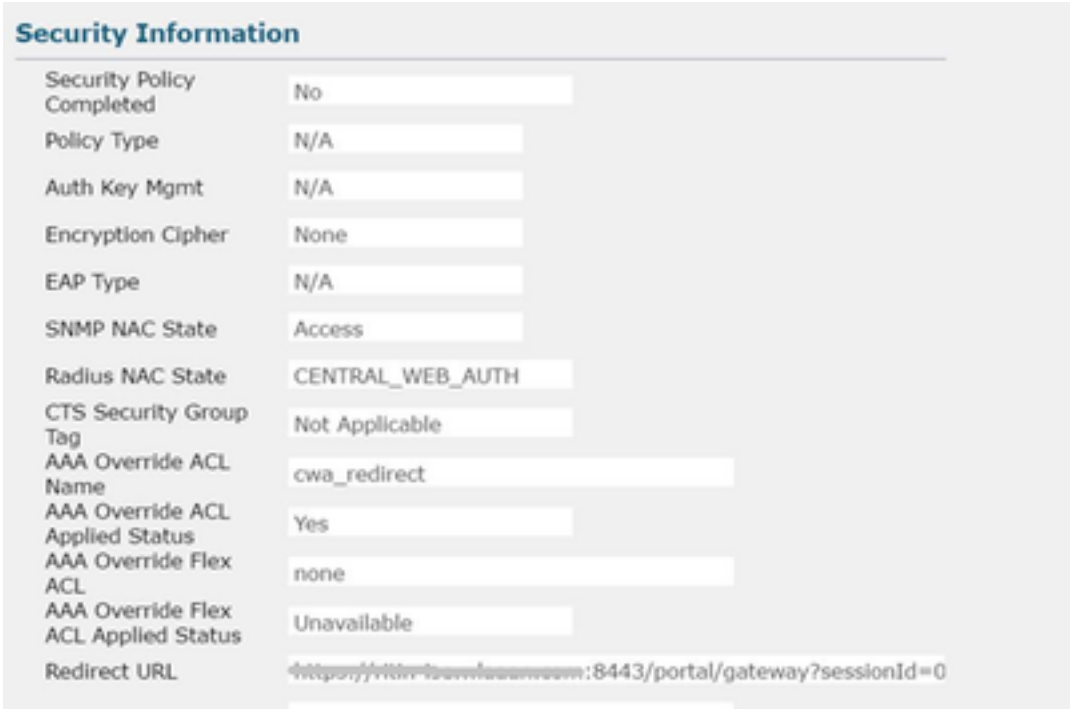
重定向至访客门户不起作用

从ISE推送重定向URL和ACL后，请检查以下项：

1.使用命令**show authentication session int <interface> details**显示交换机上的客户端状态（如果有线访客接入）：

```
guestlab#sh auth sess int T1/0/48 de
           Interface:  TenGigabitEthernet1/0/48
              IIF-ID:  0x1096380000001DC
         MAC Address:  b496.9126.dd6d
        IPv6 Address:  Unknown
        IPv4 Address:  10.106.37.18
           User-Name:  B4-96-91-26-DD-6D
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
     Restart timeout:  N/A
   Common Session ID:  0A6A25110000012652C64B014
     Acct Session ID:  0x0000124F
              Handle:  0x5E00014D
      Current Policy:  POLICY_Te1/0/48

Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:

        URL Redirect:  https://10.127.197.212:8443/portal/gateway?sessionId=0A6
A25110000012652C64B014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&tok
en=66bbfce930a43142fe26b9d9577971de
    URL Redirect ACL:  REDIRECT_ACL

Method status list:
      Method           State
      mab              Authc Success
```

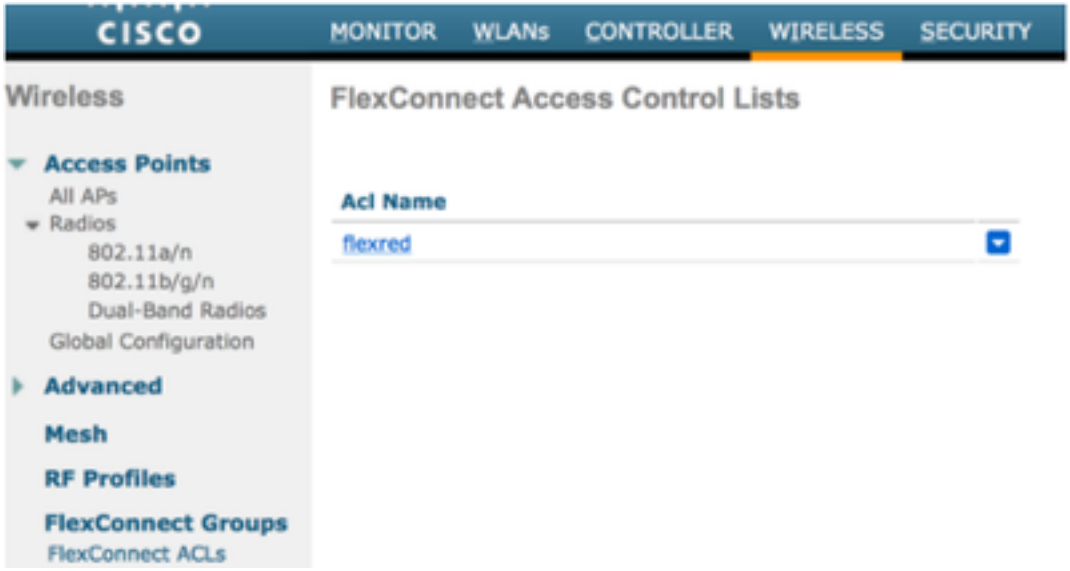
2.无线局域网控制器上的客户端状态（如果无线访客接入）：**Monitor > Client > MAC address**



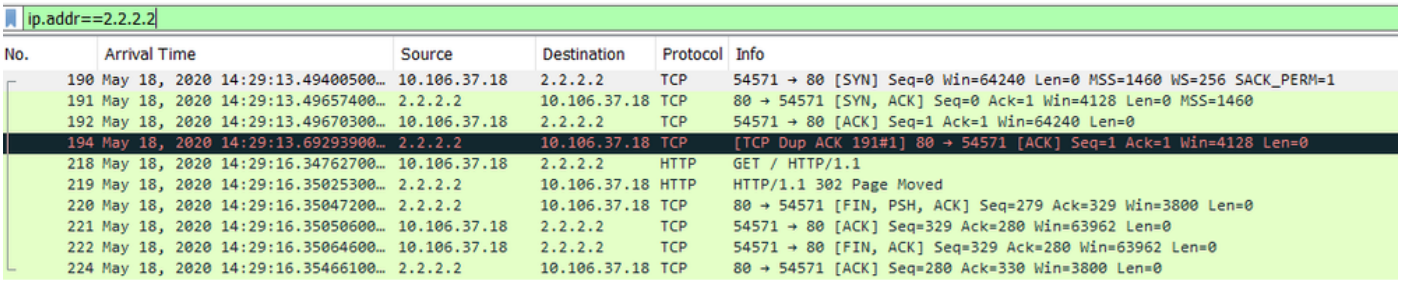
3.借助命令提示符，从终端到TCP端口8443上ISE的可达性： **C:\Users\user>telnet <ISE-IP> 8443**

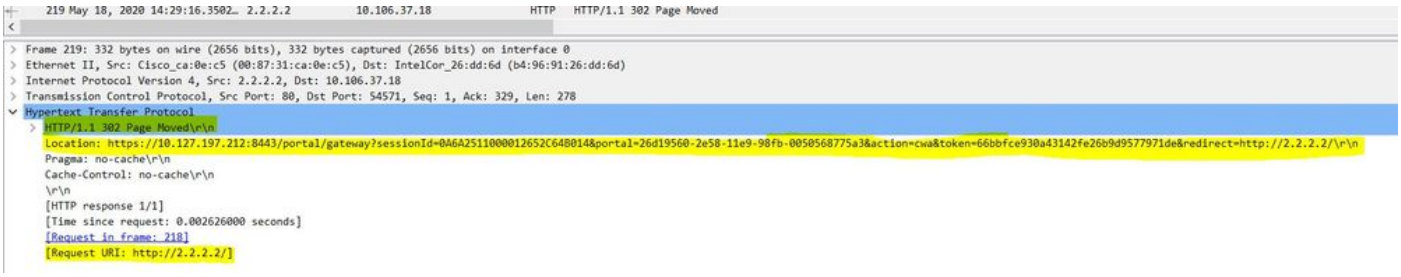
4.如果门户重定向URL具有FQDN，则检查客户端能否通过命令提示符进行解析：**C:\Users\user>nslookup guest.ise.com**

5.在flex connect设置中，确保在ACL和flex ACL下配置相同的ACL名称。此外，验证ACL是否已映射到AP。有关详细信息，请参阅上一节中的配置指南 — 步骤7 b和c。



6.从客户端捕获数据包，并检查重定向。数据包HTTP/1.1 302 Page Moved用于指示WLC/Switch将访问站点重定向到ISE访客门户（重定向URL）：





7.在网络访问设备上启用HTTP(s)引擎：

在交换机上：

```
guestlab#sh run | in ip http
ip http server
ip http secure-server
```

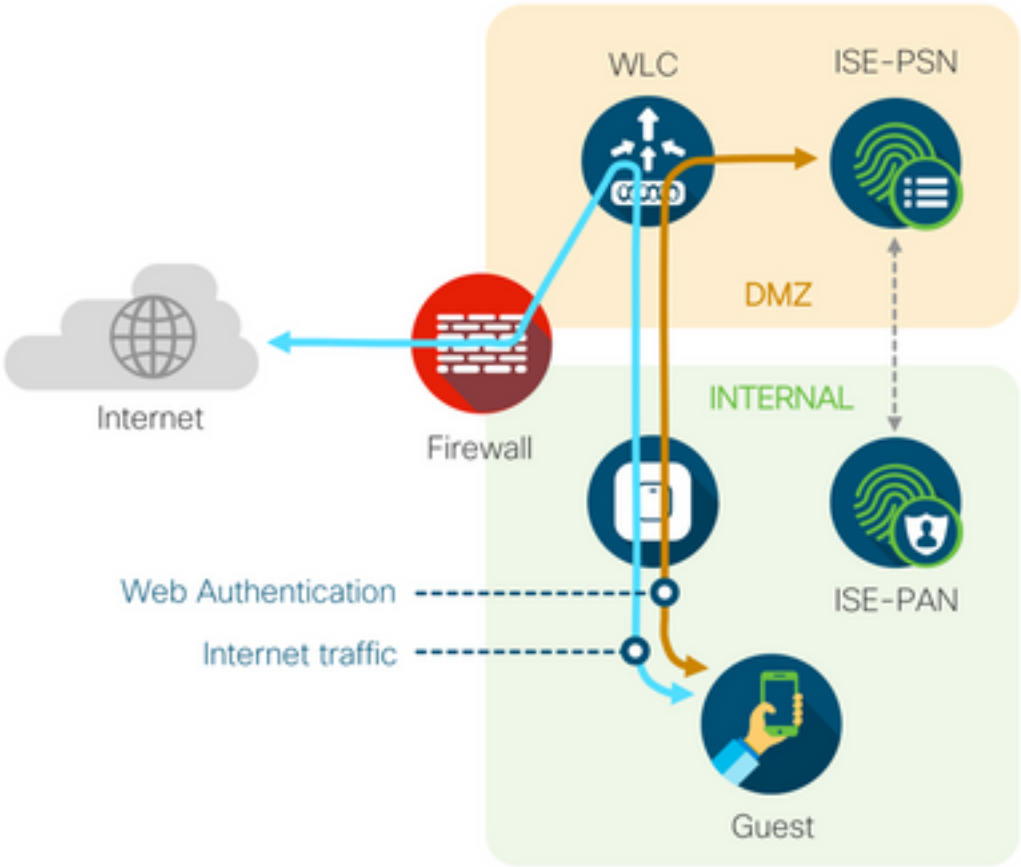
在WLC上：

8.如果WLC处于外部锚点设置中，请检查以下项：

步骤1:两个WLC上的客户端状态必须相同。

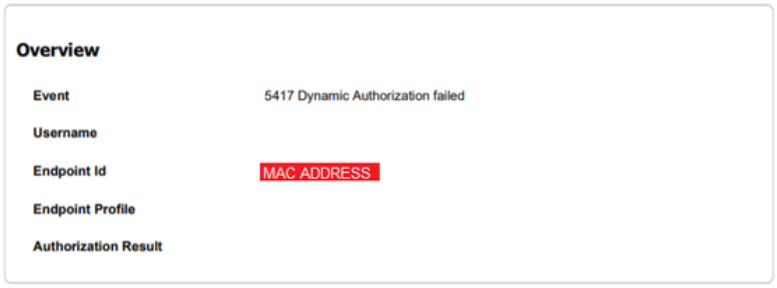
第二步：必须在两个WLC上看到重定向URL。

第三步：必须在锚点WLC上禁用RADIUS记帐。



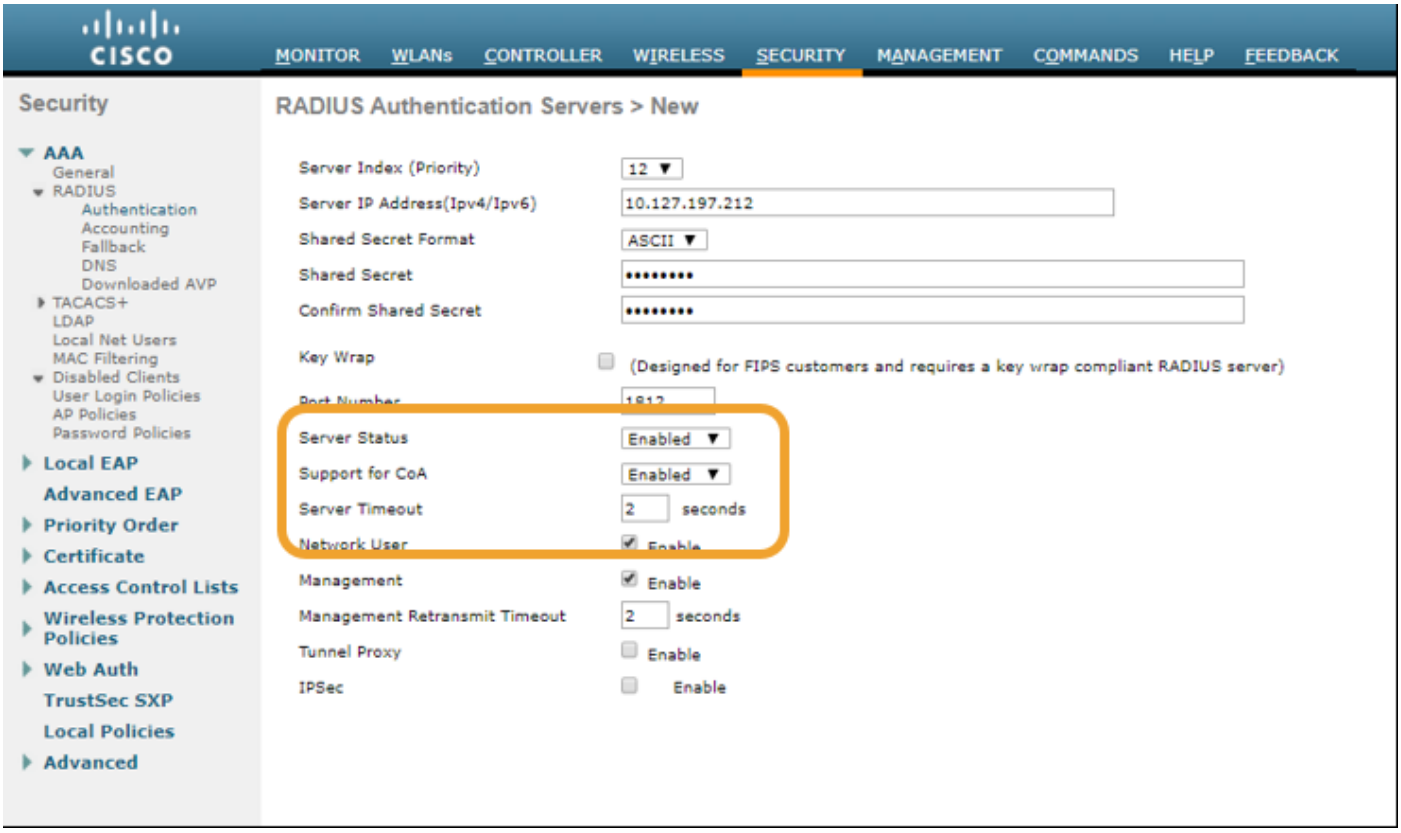
动态授权失败

如果最终用户能够访问访客门户并成功登录，则下一步是更改授权，为用户提供完全的访客访问权限。如果这不起作用，您会看到ISE Radius实时日志上的动态授权故障。要修复此问题，请检查以下项：



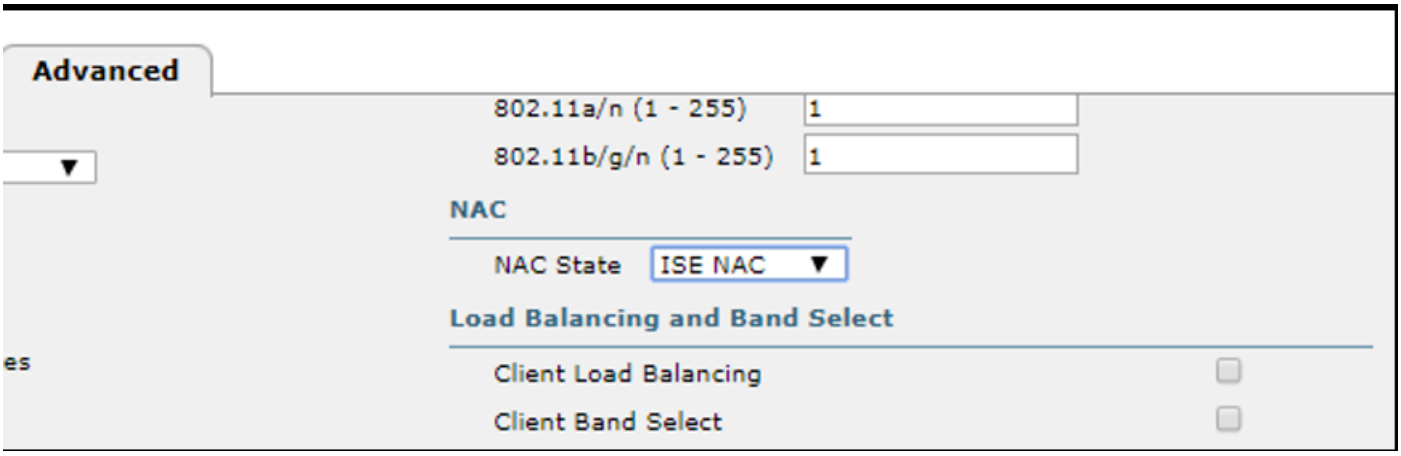
1.必须在NAD上启用/配置授权更改(CoA):

```
!
aaa server radius dynamic-author
 client 10.127.197.209 server-key cisco123
 client 10.127.197.212 server-key cisco123
!
```



2.防火墙上必须允许UDP端口1700。

3. WLC上的NAC状态不正确。在**WLC GUI > WLAN上的Advanced settings**下，将NAC状态更改为ISE NAC。

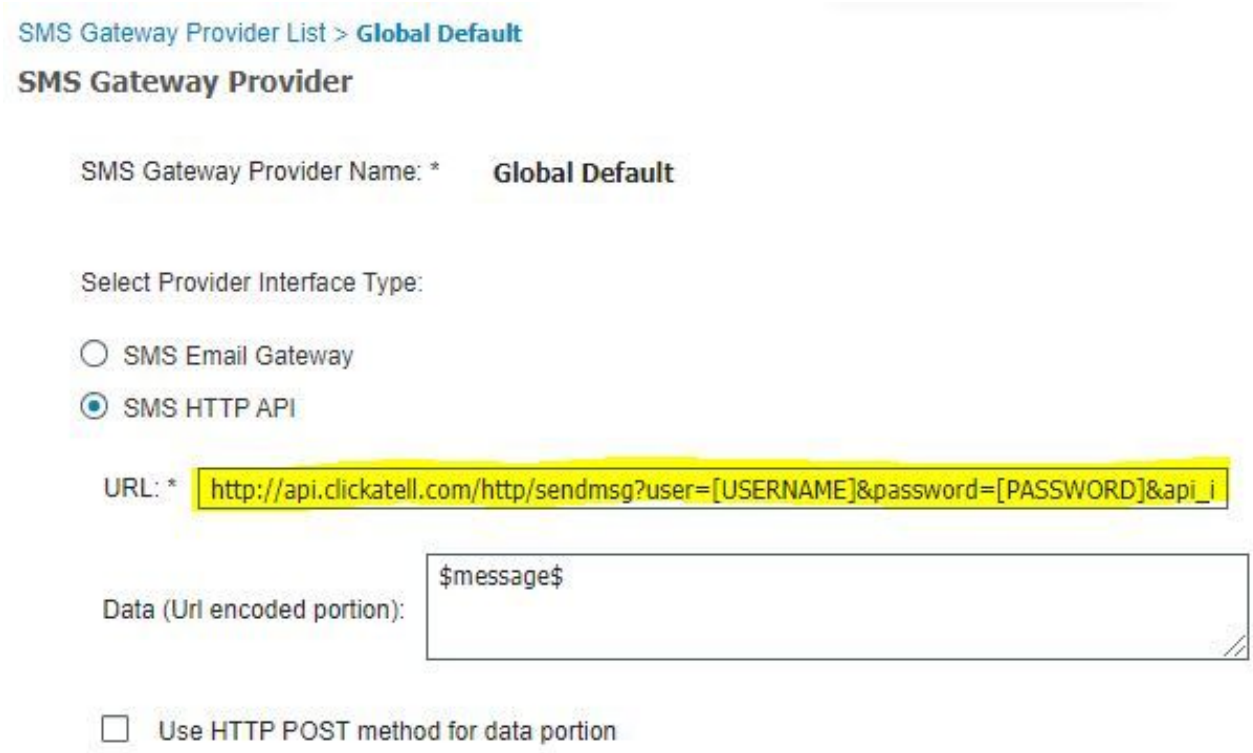


未发送SMS/EMAIL通知

1.检查**管理>系统>设置> SMTP**下的SMTP配置。

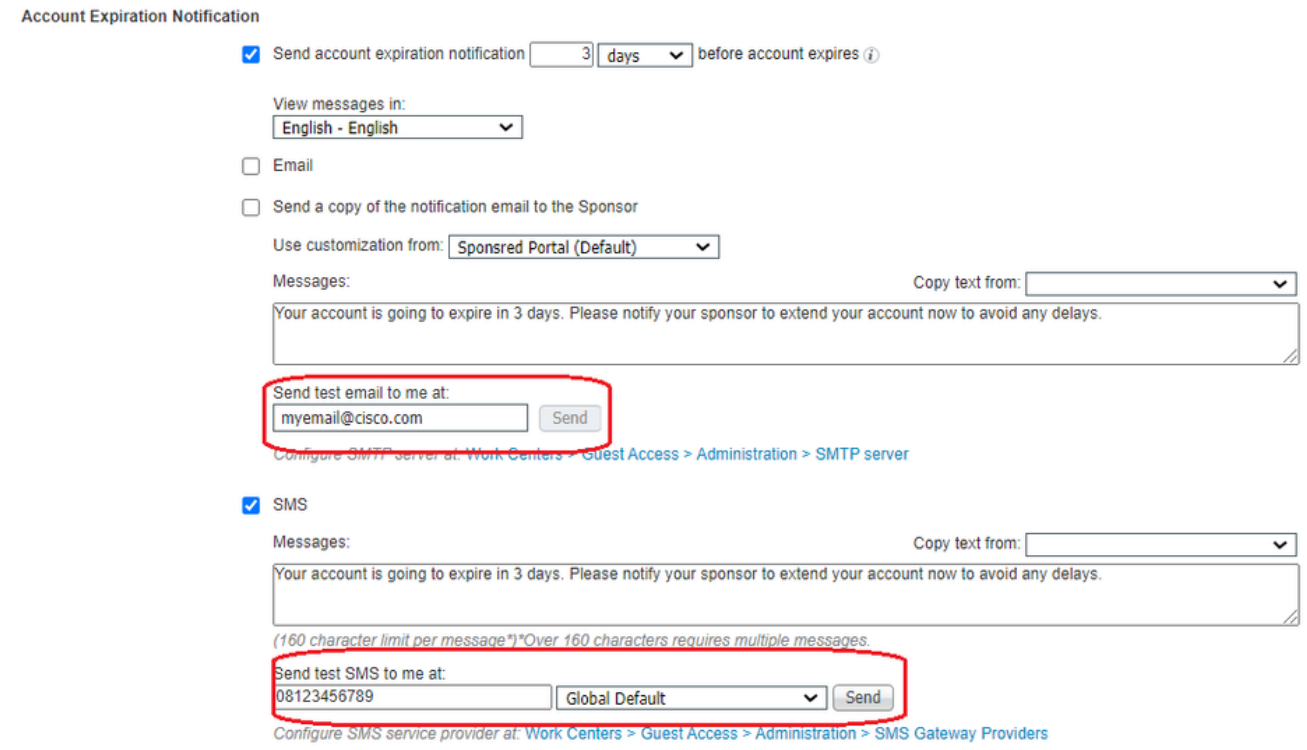
2.检查ISE以外的SMS/邮件网关的API:

测试供应商在API客户端或浏览器上提供的URL，替换用户名、密码、手机号码等变量，并测试可达性。[**Administration > System > Settings > SMS Gateways**]



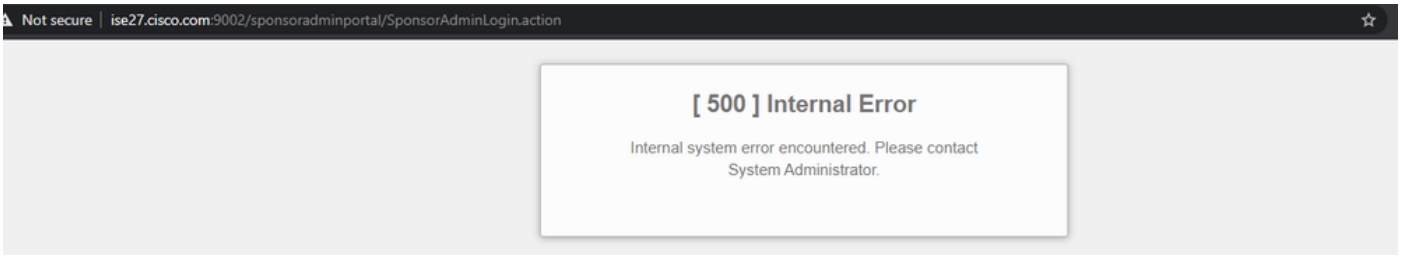
或者，如果从ISE保证人组[**Workcenters > Guest Access > Portals and Components > Guest Types**]进行测试，请在ISE和SMS/SMTP网关上进行数据包捕获以检查是否

1. 请求数据包未经篡改即可到达服务器。
2. ISE服务器具有供应商建议的网关处理此请求的权限/权限。



无法访问“管理帐户”页

1.在**Workcenters > Guest Access > Manage accounts**按钮下，重定向到端口9002上的ISE FQDN，ISE管理员可以访问发起人门户：



2.使用**nslookup <FQDN of ISE PAN>**命令检查发起人门户访问的工作站是否解析了FQDN。

3.使用命令**show ports从ISE的CLI检查ISE TCP端口9002是否打开 | include 9002**。

门户证书最佳实践

- 为获得无缝的用户体验，用于门户和管理员角色的证书必须由众所周知的公共证书颁发机构（例如：GoDaddy、DigiCert、VeriSign等）签署，浏览器通常信任这些证书（例如：Google Chrome、Firefox等）。

- 建议不要使用静态IP进行访客重定向，因为这会使ISE的专用IP对所有用户可见。大多数供应商不为私有IP提供第三方签名的证书。

- 当您从ISE 2.4 p6移至p8或p9时，有一个已知漏洞：Cisco Bug ID CSCvp75207，其中**Trust for authentication within ISE**和**Trust for client authentication**和Syslog框必须在补丁升级后手动选中。这可以确保ISE在访客门户被访问时发出TLS流的完整证书链。

如果这些操作不能解决访客访问问题，请联系TAC使用文档中的说明收集的支持捆绑包：Debugs to

enable on ISE。

相关信息

- **思科技术支持和下载**

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。