# FireSIGHT系统上用于SSL/TLS上Microsoft AD身份验证的身份验证对象验证

## 目录



## 简介

您可以配置FireSIGHT管理中心，以允许外部Active Directory LDAP用户对Web用户界面和CLI的访问进行身份验证。本文讨论如何配置、测试和排除Microsoft AD身份验证对象的故障通过SSL/TLS。

## 先决条件

思科建议您了解FireSIGHT管理中心上的用户管理和外部身份验证系统。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 步骤

步骤1.配置不使用SSL/TLS加密的身份验证对象。

1. 按照通常的方式配置身份验证对象。加密和未加密身份验证的基本配置步骤相同。
2. 确认身份验证对象正在工作，并且AD LDAP用户可以对未加密的身份验证。

步骤2.测试无CA证书的SSL和TLS身份验证对象。

在没有CA证书的情况下，通过SSL和TLS测试身份验证对象。如果遇到问题，请咨询系统管理员以在AD LDS服务器上解决此问题。如果之前已将证书上传到身份验证对象，请选择“**Certificate has been loaded(Select to clear loaded certificate)”以清除证书并再次测试AO。**

如果身份验证对象失败，请咨询您的系统管理员以验证AD LDS SSL/TLS配置，然后继续下一步。但是，请继续执行以下步骤，使用CA证书进一步测试身份验证对象。

步骤3.下载**Base64** CA证书

1. 登录AD LDS。

2. 打开Web浏览器并连接到http://localhost/certsrv
3. 单击“Download a CA certificate， certificate chain， or CRL”
4. 从“CA Certificate”列表中选择CA证书，从“Encoding Method”中选择“Base64”
5. 单击“Download CA certificate”(下载CA证书)链接下载certnew.cer文件。

步骤4.验证证书中的Subject值。

1. 右键单击certnew.cer，然后选择open。
2. 单击“详细信息”选项卡，然后从“显示”下拉选项中选择“<全部>”
3. 检验每个字段的值。特别是，验证主题值是否与身份验证对象的主服务器主机名匹配。

步骤5.在Microsoft Windows计算机上测试证书。您可以在加入工作组或域的Windows计算机上执行此测试。

**提示：**此步骤可用于在FireSIGHT管理中心上创建身份验证对象之前测试Windows系统上的CA证书。

1. 将CA证书复制到C:\Certficate或任何首选目录。
2. 运行Windows命令行cmd.exe。作为管理员
3. 使用Certutil命令测试CA证书

```
cd c:\Certificate

certutil -v -urlfetch -verify certnew.cer >cacert.test.txt
```

如果Windows计算机已加入域，则CA证书应位于证书存储区中，且cacert.test.txt中不应出现错误。但是，如果Windows计算机在工作组中，您可能会看到两条消息之一，具体取决于受信任CA列表中是否存在CA证书。

a.CA受信任，但找不到CA的CRL:

```
ERROR: Verifying leaf certificate revocation status returned The revocation function
was unable to check revocation because the revocation server was offline. 0x80092013
(-2146885613)

CertUtil: The revocation function was unable to check revocation because the
revocation server was offline.
```

b.CA不受信任：

```
Verifies against UNTRUSTED root
Cert is a CA certificate
Cannot check leaf certificate revocation status
CertUtil: -verify command completed successfully.
```

如果您收到以下任何其他错误消息，请咨询您的系统管理员，以解决AD LDS和中间CA上的问题。这些错误消息表示证书不正确、CA证书中的主题、缺少证书链等。

```
Failed "AIA" Time: 0
Failed "CDP" Time: 0
Error retrieving URL: The specified network resource or d evice is no longer available
```

步骤6.确认CA证书有效并在步骤5中通过测试后，将证书上传到身份验证对象并运行测试。

步骤7.保存身份验证对象并重新应用系统策略。