

# 目录

[简介](#)

[前提条件](#)

[步骤](#)

## 简介

您能配置FireSIGHT管理中心允许外部活动目录LDAP用户验证对网页用户界面和CLI的访问。此条款讨论如何配置，测试，排除故障Microsoft AD验证的验证对象在SSL/TLS。

## 前提条件

思科建议您有在用户管理和外部验证系统的知识在FireSIGHT管理中心。

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.配置验证对象，不用SSL/TLS加密。

1. 配置验证对象，您通常会。已加密和未加密的认证的基本配置步骤是相同的。
2. 确认验证对象工作，并且AD LDAP用户能验证未加密。

步骤2.测试在SSL和TLS的验证对象，不用CA证书。

测试在SSL和TLS的验证对象，不用CA cert。如果遇到问题，请咨询以您的系统管理员解决在AD LDS服务器的此问题。如果证书以前上传对验证对象，请选择"Certificate has been loaded (Select to clear loaded certificate)"清除cert和再测试AO。

如果验证对象发生故障，请参见您的系统管理员验证AD LDS SSL/TLS配置，在您继续前进向下一步前。然而，请继续到以下步骤进一步测试验证对象与CA证书。

步骤3.下载Base64 CA Cert。

1. AD LDS的洛金。
2. 打开Web浏览器并且连接对<http://localhost/certsrv>
3. 点击“下载CA证书、证书链或者CRL”
4. 从“CA证书”列表和“Base64”选择CA cert从“编码方法”
5. 点击“下载CA证书”链路下载certnew.cer文件。

步骤4.验证在cert的附属的值。

1. 用鼠标右键单击在certnew.cer并且选择开放。

2. 点击**详细信息选项卡**并且选择从**显示**下拉式选项的**<All>**

3. 验证每个字段的值。特别是，请验证**附属**的值匹配验证对象的**主服务器主机名**。

步骤5.测试在Microsoft Windows计算机的Cert。您可执行在工作组或域加入的Windows机器的此测验。

**提示：**此步骤可以用于在创建在FireSIGHT管理中心的验证对象前测试在windows系统的CA证书。

1. 复制CA cert对C:\Certificate或所有首选的目录。

2. Run窗口line命令，cmd.exe**管理员**

3. 测试CA证书用Certutil命令

```
cd c:\Certificate
```

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

如果Windows机器已经加入域，CA证书应该在证书存储，并且不应该有在cacert.test.txt错误。然而，如果Windows机器在工作组，您可以根据CA发现两个消息之一cert的存在委托CA列表的。

a. CA委托，但是CRL没有为CA:查找

```
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没有委托：

```
Verifies against UNTRUSTED root
```

```
Cert is a CA certificate
```

```
Cannot check leaf certificate revocation status
```

```
CertUtil: -verify command completed successfully.
```

如果收到任何其他错误消息，如下面，请咨询以您的系统管理员解决在AD LDS和中间CA的问题。这些错误消息是在CA cert的预示不正确Cert，主题，缺少证书链等等。

```
Verifies against UNTRUSTED root
```

```
Cert is a CA certificate
```

```
Cannot check leaf certificate revocation status
```

```
CertUtil: -verify command completed successfully.
```

第六步：一旦确认CA cert有效和通过在步骤5的测验，上传cert对验证对象并且运行测验。

步骤7.保存验证对象并且重新应用系统策略。