

CSM为SSL通信启用强加密算法

目录

[问题](#)

[解决方案](#)

问题

默认情况下，思科安全管理器(CSM)为HTTPS通信提供以下密码：

```
%ASA-7-725011: Cipher[1] : AES128-SHA
%ASA-7-725011: Cipher[2] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[3] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725011: Cipher[5] : EDH-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[6] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[7] : DES-CBC-SHA
%ASA-7-725011: Cipher[8] : EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[9] : EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[10] : EXP-DES-CBC-SHA
%ASA-7-725011: Cipher[11] : EXP-EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[12] : EXP-EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[13] : ECDHE-ECDSA-AES128-SHA256
%ASA-7-725011: Cipher[14] : ECDHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[15] : AES128-SHA256
%ASA-7-725011: Cipher[16] : DHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[17] : DHE-DSS-AES128-SHA256
%ASA-7-725011: Cipher[18] : ECDHE-ECDSA-AES128-SHA
%ASA-7-725011: Cipher[19] : ECDHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[20] : AES128-SHA
%ASA-7-725011: Cipher[21] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[22] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[23] : ECDHE-ECDSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[24] : ECDHE-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[25] : DES-CBC3-SHA
%ASA-7-725011: Cipher[26] : EDH-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[27] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[28] : ADH-AES128-SHA256
%ASA-7-725011: Cipher[29] : ADH-AES128-SHA
%ASA-7-725011: Cipher[30] : ADH-DES-CBC3-SHA
%ASA-7-725011: Cipher[31] : DES-CBC-SHA
%ASA-7-725011: Cipher[32] : EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[33] : EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[34] : ADH-DES-CBC-SHA
%ASA-7-725011: Cipher[35] : EXP-DES-CBC-SHA
%ASA-7-725011: Cipher[36] : EXP-EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[37] : EXP-EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[38] : EXP-ADH-DES-CBC-SHA
%ASA-7-725011: Cipher[39] : NULL-SHA256
%ASA-7-725011: Cipher[40] : ECDHE-ECDSA-NULL-SHA
%ASA-7-725011: Cipher[41] : ECDHE-RSA-NULL-SHA
%ASA-7-725011: Cipher[42] : NULL-SHA
%ASA-7-725011: Cipher[43] : NULL-MD5
```

但是，如果将ASA配置为仅支持强加密算法（如AES256-SHA）：

通信将失败，我们将在ASA上看到以下SYSLOG:

```
%ASA-7-725014: SSL lib error. Function: ssl3_get_client_hello Reason: no shared cipher  
以下登录CSM:
```

```
"Unable to communicate with the Device"  
The Security Manager Server and the device could not negotiate the security level"
```

解决方案

由于某些国家/地区的导入法规，Oracle实施提供了默认加密管辖区策略文件，限制了加密算法的强度。如果需要配置或已在设备上配置更强大的算法（例如，AES有256位密钥，DH组有5,14,24），请执行以下步骤：

1. 从<http://www.oracle.com>下载Java 7无限强度加密策略.jar文件。思科建议在Oracle网站上搜索以下内容：

Java加密扩展(JCE)无限强度管辖策略文件Java 7

<http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>

2. 在CSCOPx\MDC\vm\jre\lib\security文件夹中的安全管理器服务器上替换local_policy.jar和US_export_policy.jar。
3. 重新启动安全管理器服务器。

现在，CSM将显示以下密码：

```
%ASA-7-725011: Cipher[1] : AES128-SHA  
%ASA-7-725011: Cipher[2] : DHE-RSA-AES128-SHA  
%ASA-7-725011: Cipher[3] : DHE-DSS-AES128-SHA  
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA  
%ASA-7-725011: Cipher[5] : EDH-RSA-DES-CBC3-SHA  
%ASA-7-725011: Cipher[6] : EDH-DSS-DES-CBC3-SHA  
%ASA-7-725011: Cipher[7] : DES-CBC-SHA  
%ASA-7-725011: Cipher[8] : EDH-RSA-DES-CBC-SHA  
%ASA-7-725011: Cipher[9] : EDH-DSS-DES-CBC-SHA  
%ASA-7-725011: Cipher[10] : EXP-DES-CBC-SHA  
%ASA-7-725011: Cipher[11] : EXP-EDH-RSA-DES-CBC-SHA  
%ASA-7-725011: Cipher[12] : EXP-EDH-DSS-DES-CBC-SHA  
%ASA-7-725011: Cipher[13] : ECDHE-ECDSA-AES256-SHA384  
%ASA-7-725011: Cipher[14] : ECDHE-RSA-AES256-SHA384  
%ASA-7-725011: Cipher[15] : AES256-SHA256  
%ASA-7-725011: Cipher[16] : DHE-RSA-AES256-SHA256  
%ASA-7-725011: Cipher[17] : DHE-DSS-AES256-SHA256  
%ASA-7-725011: Cipher[18] : ECDHE-ECDSA-AES256-SHA  
%ASA-7-725011: Cipher[19] : ECDHE-RSA-AES256-SHA  
%ASA-7-725011: Cipher[20] : AES256-SHA  
%ASA-7-725011: Cipher[21] : DHE-RSA-AES256-SHA  
%ASA-7-725011: Cipher[22] : DHE-DSS-AES256-SHA  
%ASA-7-725011: Cipher[23] : ECDHE-ECDSA-AES128-SHA256  
%ASA-7-725011: Cipher[24] : ECDHE-RSA-AES128-SHA256  
%ASA-7-725011: Cipher[25] : AES128-SHA256  
%ASA-7-725011: Cipher[26] : DHE-RSA-AES128-SHA256  
%ASA-7-725011: Cipher[27] : DHE-DSS-AES128-SHA256  
%ASA-7-725011: Cipher[28] : ECDHE-ECDSA-AES128-SHA
```

```
%ASA-7-725011: Cipher[29] : ECDHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[30] : AES128-SHA
%ASA-7-725011: Cipher[31] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[32] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[33] : ECDHE-ECDSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[34] : ECDHE-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[35] : DES-CBC3-SHA
%ASA-7-725011: Cipher[36] : EDH-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[37] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[38] : ADH-AES256-SHA256
%ASA-7-725011: Cipher[39] : ADH-AES256-SHA
%ASA-7-725011: Cipher[40] : ADH-AES128-SHA256
%ASA-7-725011: Cipher[41] : ADH-AES128-SHA
%ASA-7-725011: Cipher[42] : ADH-DES-CBC3-SHA
%ASA-7-725011: Cipher[43] : DES-CBC-SHA
%ASA-7-725011: Cipher[44] : EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[45] : EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[46] : ADH-DES-CBC-SHA
%ASA-7-725011: Cipher[47] : EXP-DES-CBC-SHA
%ASA-7-725011: Cipher[48] : EXP-EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[49] : EXP-EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[50] : EXP-ADH-DES-CBC-SHA
%ASA-7-725011: Cipher[51] : NULL-SHA256
%ASA-7-725011: Cipher[52] : ECDHE-ECDSA-NULL-SHA
%ASA-7-725011: Cipher[53] : ECDHE-RSA-NULL-SHA
%ASA-7-725011: Cipher[54] : NULL-SHA
%ASA-7-725011: Cipher[55] : NULL-MD5
```

现在连接将成功：

```
%ASA-7-725012: Device chooses cipher AES256-SHA for the SSL session with client
asa:10.88.243.57/49949 to 10.122.160.233/443
```