

ASA的Unified Mobility Advantage服务器证书问题

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[部署方案](#)

[安装Cisco UMA服务器自签名证书](#)

[要在CUMA服务器上完成的任务](#)

[将CUMA证书请求添加到其他证书颁发机构时出现问题](#)

[问题 1](#)

[Error:无法连接](#)

[解决方案](#)

[CUMA管理员门户中的某些页面无法访问](#)

[解决方案](#)

[相关信息](#)

简介

本文档介绍如何在自适应安全设备(ASA)和思科统一移动优势(CUMA)服务器之间交换自签名证书，反之亦然。它还说明如何排除导入证书时出现的常见问题。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ASA 5500 系列
- 思科统一移动优势服务器7

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。

规则

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

部署方案

Cisco Mobility Advantage解决方案使用的TLS代理有两种部署方案。

注意：在这两种情况下，客户端都从Internet连接。

1. 自适应安全设备同时用作防火墙和TLS代理。
2. 自适应安全设备仅用作TLS代理。

在这两种情况下，您都需要以PKCS-12格式导出Cisco UMA服务器证书和密钥对，并将其导入自适应安全设备。证书在与Cisco UMA客户端握手期间使用。

在自适应安全设备信任库中安装Cisco UMA服务器自签名证书是自适应安全设备在自适应安全设备代理与Cisco UMA服务器握手期间对Cisco UMA服务器进行身份验证的必要条件。

安装Cisco UMA服务器自签名证书

要在CUMA服务器上完成的任务

这些步骤需要在CUMA服务器上完成。通过这些步骤，您可以在CUMA上创建自签名证书，以与CN=portal.aipc.com的ASA交换。这需要安装在ASA信任库中。请完成以下步骤：

1. 在CUMA服务器上创建自签名证书。登录Cisco Unified Mobility Advantage管理员门户。选择“安全情景管理”旁边的[+]。

Cisco Unified Mobility Advantage - Admin Portal

Welcome admin Reset Settings Help

Admin Control **Network Properties - Server Information**

Proxy Server Information

Proxy Host Name	<input type="text" value="proxy.cuma"/>
Proxy Client Connection Port	<input type="text" value="5443"/>
Proxy Client Download Port	<input type="text" value="9080"/>

Managed Server Information

Client Connection Port	<input type="text" value="5443"/>
User Portal Port	<input type="text" value="9443"/>
Client Download Port	<input type="text" value="9080"/>
Security Context	<input type="text" value="cuma_trust_all"/> Add New Context

选择Security Contexts。选择“添加上下文”。输入此信息：

Do you want to create/upload a new certificate? create

Context Name "cuma"

Description "cuma"

Trust Policy "Trusted Certificates"

Client Authentication Policy "none"

```
Client Password "changeme"
Server Name cuma.ciscodom.com
Department Name "vsec"
Company Name "cisco"
City "san jose"
State "ca"
Country "US"
```

2. 从Cisco Unified Mobility Advantage下载自签名证书。要完成任务，请完成以下步骤：选择“安全情景管理”旁边的[+]。选择**Security Contexts**。选择保存要下载的证书的安全上下文旁的**Manage Context**。选择“**Download Certificate**”。注：如果证书是链，且具有关联的根或中间证书，则仅下载链中的第一个证书。这足以用于自签名证书。保存文件。
3. 下一步是将Cisco Unified Mobility Advantage的自签名证书添加到ASA。在ASA上完成以下步骤：在文本编辑器中打开Cisco Unified Mobility Advantage的自签名证书。将证书导入思科自适应安全设备信任库：

```
cuma-asa(config)# crypto ca trustpoint cuma-server-id-cert
cuma-asa(config-ca-trustpoint)# enrollment terminal
cuma-asa(config-ca-trustpoint)# crypto ca authenticate
cuma-server-id-cert
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
----BEGIN CERTIFICATE----
** paste the contents from wordpad **
----END CERTIFICATE----
```

4. 在CUMA服务器上导出ASA自签名证书。您需要配置Cisco Unified Mobility Advantage，以要求从思科自适应安全设备获得证书。完成以下步骤以提供所需的自签名证书。这些步骤需要在ASA上完成。生成新密钥对：

```
cuma-asa(config)# crypto key generate rsa label asa-id-key mod 1024
```

```
INFO: The name for the keys will be: asa-id-key
```

```
Keypair generation process begin. Please wait...
```

添加新信任点：

```
cuma-asa(config)# crypto ca trustpoint asa-self-signed-id-cert
```

```
cuma-asa(config-ca-trustpoint)# keypair asa-id-key
```

```
cuma-asa(config-ca-trustpoint)# enrollment self
```

注册信任点：

```
cuma-asa(config-ca-trustpoint)# crypto ca enroll asa-self-signed-id-cert
```

```
% The fully-qualified domain name in the certificate will be:
```

```
cuma-asa.cisco.com
```

```
% Include the device serial number in the subject name? [yes/no]: n
```

```
Generate Self-Signed Certificate? [yes/no]: y
```

将证书导出到文本文件。

```
cuma-asa(config)# crypto ca export asa-self-signed-id-cert
identity-certificate
```

```
The PEM encoded identity certificate follows:
```

```
-----BEGIN CERTIFICATE-----
```

```
Certificate data omitted
```

```
-----END CERTIFICATE-----
```

5. 将上一个输出复制到文本文件，并将其添加到CUMA服务器信任库，然后使用以下步骤：选择“安全情景管理”旁边的[+]。选择**Security Contexts**。选择**Manage Context**（在导入签名证书的安全上下文旁）。在“受信任证书”栏中选择导入。粘贴证书文本。为证书命名。选择**Import**。

注意：对于远程目标配置，请呼入台式电话以确定手机是否同时振铃。这将确认移动连接是否工作，以及远程目标配置是否不存在问题。

[将CUMA证书请求添加到其他证书颁发机构时出现问题](#)

[问题 1](#)

许多演示/原型安装，如果CUMC/CUMA解决方案与受信任证书配合使用，这些安装将自签名或从其他证书颁发机构获得。Verisign证书昂贵，获取这些证书需要很长时间。如果解决方案支持来自其他CA的自签名证书和证书，则情况良好。

支持的当前证书是GeoTrust和Verisign。这记录在Cisco Bug ID CSCta62971([仅限注册客户](#))中

[Error:无法连接](#)

当您尝试访问用户门户页面(例如<https://<host>:8443>)，出现“Unable to connect”错误消息。

[解决方案](#)

此问题记录在Cisco Bug ID CSCsm26730(仅[限注册客户](#))中。要访问用户门户页面，请完成以下解决方法：

此问题的原因是美元字符，因此在受控服务器的server.xml文件中用另一个美元字符来转义美元字符。例如，编辑/opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml。

行：`keystorePass="pa$word"maxSpareThreads="15"`

用\$\$换\$。它看起来像`keystorePass="pa$$word"maxSpareThreads="15"`。

[CUMA管理员门户中的某些页面无法访问](#)

在CUMA管理员门户中无法查看这些页：

- 激活/停用用户
- 搜索/维护

如果用户点击左侧菜单中上述两个页面之一，则浏览器似乎指示它正在加载页面，但没有发生任何情况（只有浏览器中的上一页可见）。

[解决方案](#)

要解决与用户页面相关的此问题，请将用于Active Directory的端口更改为**3268**并重新启动CUMA。

[相关信息](#)

- [ASA-CUMA代理分步配置](#)
- [ASR5000 v1简介](#)

- [升级Cisco Unified Mobility Advantage](#)
- [语音技术支持](#)
- [语音和统一通信产品支持](#)
- [技术支持和文档 - Cisco Systems](#)