Unified Mobility Advantage Server證書與ASA問題

目錄

簡介

本文說明如何在Adaptive Security Appliance(ASA)和Cisco Unified Mobility Advantage(CUMA)伺服器之間交換自簽名證書，反之亦然。此外，還說明如何排解匯入憑證時發生的常見問題。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASA 5500系列
- Cisco整合行動化優勢伺服器7

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

部署方案

Cisco Mobility Advantage解決方案使用的TLS代理有兩種部署方案。

注意：在這兩種情況下，客戶端都通過Internet進行連線。

1. 自適應安全裝置同時充當防火牆和TLS代理。
2. 自適應安全裝置僅充當TLS代理。

在這兩種情況下，您都需要以PKCS-12格式匯出Cisco UMA伺服器證書和金鑰對，然後將其匯入自適應安全裝置。該證書在與Cisco UMA客戶端握手期間使用。

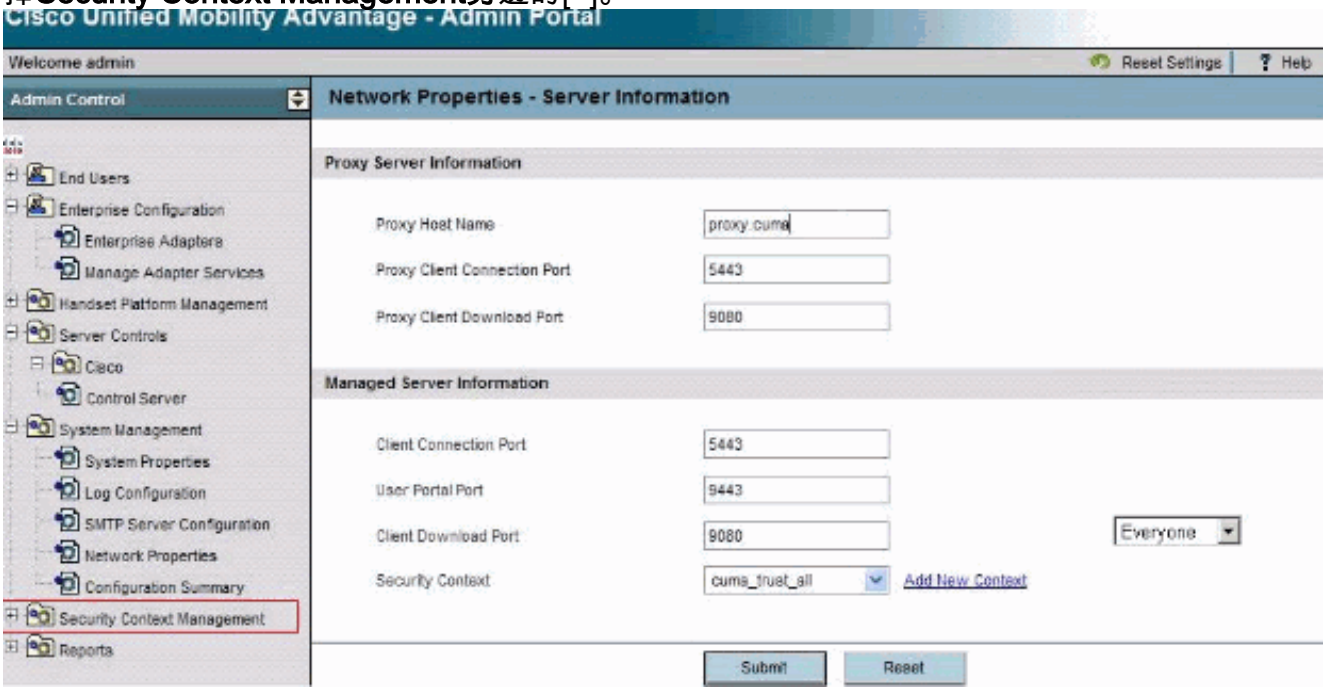
在自適應安全裝置truststore中安裝Cisco UMA伺服器自簽名證書對於自適應安全裝置在自適應安全裝置代理和Cisco UMA伺服器之間的握手期間驗證Cisco UMA伺服器是必需的。

安裝Cisco UMA伺服器自簽名證書

在CUMA伺服器上要完成的任務

這些步驟需要在CUMA伺服器上完成。通過這些步驟，您可以在CUMA上建立自簽名證書，以便與CN=portal.aipc.com的ASA進行交換。需要將此項安裝在ASA信任儲存上。請完成以下步驟：

1. 在CUMA伺服器上建立自簽名證書。登入到Cisco Unified Mobility Advantage管理員門戶。選擇Security Context Management旁邊的[+]。



選擇Security Contexts。選擇Add Context。輸入以下資訊：

```
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. 從Cisco Unified Mobility Advantage下載自簽名證書。完成以下步驟即可完成任務：選擇**Security Context Management**旁邊的[+]。選擇**Security Contexts**。選擇儲存要下載的證書的安全上下文旁的**Manage Context**。選擇**Download Certificate**。**注意：**如果憑證是鏈結，且具有關聯的根憑證或中間憑證，則只會下載鏈結中的第一個憑證。這對自簽名證書就足夠了。儲存檔案。
3. 下一步是將來自Cisco Unified Mobility Advantage的自簽名證書新增到ASA中。在ASA上完成以下步驟：在文本編輯器中開啟Cisco Unified Mobility Advantage的自簽名證書。將證書匯入思科自適應安全裝置信任庫：

```
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. 匯出CUMA伺服器上的ASA自簽名證書。您需要配置Cisco Unified Mobility Advantage，以要求從思科自適應安全裝置獲取證書。完成這些步驟，以提供所需的自簽名證書。這些步驟需要在ASA上完成。生成新的金鑰對：

```
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...
```

新增新信任點：

```
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
```

註冊信任點：

```
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
```

將證書匯出到文本檔案。

```
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. 將先前的輸出複製到文本檔案，並將其新增到CUMA伺服器信任儲存中，然後使用以下過程：選擇**Security Context Management**旁邊的[+]。選擇**Security Contexts**。選擇將簽名證書匯

入到的安全上下文旁的**管理上下文**。在Trusted Certificates欄中選擇**Import**。貼上證書文本。為證書命名。選擇**Import**。**注意**：對於「遠端目標」配置，請致電台式電話，以確定行動電話是否同時振鈴。這將確認移動連線工作正常，並且遠端目標配置沒有問題。

向其他證書頒發機構新增CUMA證書請求時出現問題

問題1

許多演示/原型安裝（如果CUMC/CUMA解決方案與受信任證書配合使用，則安裝會有所幫助）都是自簽名或從其他證書頒發機*構處獲得的*。Verisign證書很昂貴，獲取這些證書需要很長時間。如果解決方案支援自簽名證書和來自其他CA的證書，則這是很好的。

當前支援的證書是GeoTrust和Verisign。這一點記錄在Cisco錯誤ID CSCta62971中(僅限註冊客戶)

錯誤：無法連線

當您嘗試訪問使用者門戶頁面(例如`https://<host>:8443`)時，會顯示`Unable to connect`錯誤消息。

解決方案

此問題已記錄在Cisco錯誤ID CSCsm26730(僅限註冊客戶)。 若要存取使用者入口頁面，請完成以下變通方法：

出現此問題的原因是美元字元，因此在受控伺服器的**server.xml檔案中用另一個美元字元轉義**美元字元。例如，編輯/opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml。

內線：**keystorePass="pa$word"** maxSpareThreads="15"

將$字元換為`$$`。看起來**像keystorePass="pa$$word"** maxSpareThreads="15"。

無法訪問CUMA管理門戶中的某些頁面

在**CUMA Admin Portal**中無法檢視**這些頁面：**

- 啟用/停用使用者
- 搜尋/維護

如果使用者按一下左側選單中的上述兩個頁面之一，瀏覽器似乎表示它正在載入頁面，但什麼也沒發生（只能看到瀏覽器中的上一頁）。

解決方案

為了解決與使用者頁面相關的此問題，請將用於Active Directory的埠更改為**3268**，然後重新啟動CUMA。

相關資訊

- ASA-CUMA代理逐步配置
- ASR5000 v1簡介
- 升級Cisco Unified Mobility Advantage
- 語音技術支援
- 語音和整合通訊產品支援
- 技術支援與文件 - Cisco Systems