Cisco Unified Mobility Advantage Server Certificate Issue with ASA

Document ID: 112884

Contents

Introduction

This document describes how to exchange self−signed certificates between the Adaptive Security Appliance (ASA) and the Cisco Unified Mobility Advantage (CUMA) server and vice versa. It also explains how to troubleshoot the common issues that occurs while you import the certificates.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA 5500 series
- Cisco Unified Mobility Advantage Server 7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Deployment Scenarios

There are two deployment scenarios for the **TLS proxy** used by the **Cisco Mobility Advantage** solution.

Note: In both scenarios, the clients connect from the Internet.

1. The adaptive security appliance functions as both the firewall and TLS proxy.
2. The adaptive security appliance functions as the TLS proxy only.

In both scenarios, you need to export the **Cisco UMA server certificate** and **key−pair** in **PKCS−12** format and import it to the adaptive security appliance. The certificate is used during handshake with the Cisco UMA clients.

The installation of the Cisco UMA server self−signed certificate in the adaptive security appliance truststore is necessary for the adaptive security appliance to authenticate the Cisco UMA server during handshake between the adaptive security appliance proxy and Cisco UMA server.

Install the Cisco UMA server Self−signed Certificate

Tasks to be done on the CUMA server

These steps need to be done on the CUMA server. With these steps, you create a self−signed certificate on CUMA to exchange with the ASA with CN=portal.aipc.com. This needs to be installed on the ASA trust store. Complete these steps:

1. Create a self−signed cert on the CUMA server.

    a. Sign in to the Cisco Unified Mobility Advantage Admin portal.
    b. Choose the **[+]** beside Security Context Management.

    c. Choose **Security Contexts**.
    d. Choose **Add Context**.
    e. Enter this information:

```
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. Download the Self−Signed Certificates from Cisco Unified Mobility Advantage. Complete these steps in order to accomplish the task:

    a. Choose the **[+]** beside Security Context Management.
    b. Choose **Security Contexts**.

c. Choose **Manage Context** beside the security context that holds the certificate to download.
d. Choose **Download Certificate**.

Note: If the certificate is a chain, and has associated root or intermediate certificates, only the first certificate in the chain is downloaded. This is sufficient for self−signed certificates.

e. Save the file.

3. The next step is to add the self−signed certificate from Cisco Unified Mobility Advantage onto the ASA. Complete these steps on the ASA:

a. Open the self−signed certificate from Cisco Unified Mobility Advantage in a text editor.
b. Import the certificate into the Cisco Adaptive Security Appliance trust store:

```
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. Export ASA self−signed certificate on CUMA server. You need to configure Cisco Unified Mobility Advantage to require a certificate from the Cisco Adaptive Security Appliance. Complete these steps in order to provide the required self−signed certificate. These steps need to be done on the ASA.

a. Generate a new key pair:

```
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...
```

b. Add a new trustpoint:

```
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
```

c. Enroll the trustpoint:

```
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
```

d. Export the certificate to a text file.

```
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. Copy the previous output to a text file and add it to the CUMA server trust store and use this procedure:

a. Choose the **[+]** beside Security Context Management.
b. Choose **Security Contexts**.
c. Choose **Manage Context** beside the Security Context into which you import the signed certificate.
d. Choose **Import** in the Trusted Certificates bar.
e. Paste the certificate text.
f. Name the certificate.
g. Choose **Import**.

Note: For the Remote Destination configuration, call into the desk phone in order to determine whether the cell phone rings at same time. This would confirm that mobile connect works and that there is no issue with the Remote Destination configuration.

Trouble adding CUMA Certificate request to other certificate authorities

Problem 1

Many demo/prototype installations where it helps if the CUMC/CUMA solution works with trusted certificates are self−signed or obtained from *other certificate authorities*. Verisign certificates are expensive and it takes a long time to get these certificates. It is good if the solution supports self−signed certificates and certificates from other CAs.

The current certificates supported are GeoTrust and Verisign. This is documented in Cisco bug ID CSCta62971 (registered customers only)

Error: Unable to connect

When you try to access the user portal page, for example, `https://<host>:8443`, the `Unable to connect` error message appears.

Solution

This issue is documented in Cisco bug ID CSCsm26730 (registered customers only) . In order to access the user portal page, complete this workaround:

The cause of this issue is the dollar character, so escape the dollar character with another dollar character in the managed server's **server.xml file**. For example, edit /opt/cuma/jboss−4.0.1sp1/server/cuma/deploy/jbossweb−tomcat50.sar/server.xml.

In line: **keystorePass="pa$word"** maxSpareThreads="15"

Replace the $ character with $$. It looks like **keystorePass="pa$$word"** maxSpareThreads="15".

Some pages in CUMA Admin Portal are not accessible

These pages cannot be viewed in the **CUMA Admin Portal**:

- activate/deactivate user
- search/maintenance

If the user clicks on one of the above two pages in the menu to the left, the browser seems to indicate it is loading a page, but nothing happens (only the previous page that was in the browser is visible).

Solution

In order to resolve this issue related to user page, change the port used for Active Directory to **3268** and restart the CUMA.

Related Information

- **ASA−CUMA Proxy step−by−step Configuration**
- **Introduccion al ASR5000 v1**
- **Upgrading Cisco Unified Mobility Advantage**
- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Technical Support & Documentation − Cisco Systems**

Updated: Apr 04, 2011 Document ID: 112884