# Problema de certificado del servidor de Unified Mobility Advantage con ASA

## Contenido



## Introducción

Este documento describe cómo intercambiar certificados autofirmados entre el dispositivo de seguridad adaptable (ASA) y el servidor de Cisco Unified Mobility Advantage (CUMA) y viceversa. También explica cómo resolver los problemas comunes que se producen al importar los certificados.

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ASA 5500 series
- Servidor Cisco Unified Mobility Advantage 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.

### Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

## Escenarios de implementación

Hay dos escenarios de implementación para el **proxy TLS** utilizado por la **solución Cisco Mobility Advantage**.

**Nota:** En ambos escenarios, los clientes se conectan desde Internet.

1. El dispositivo de seguridad adaptable funciona como firewall y proxy TLS.
2. El dispositivo de seguridad adaptable funciona como proxy TLS solamente.

En ambos escenarios, debe exportar el **certificado de servidor Cisco UMA** y el **par de llaves** en el formato **PKCS-12** e importarlo al dispositivo de seguridad adaptable. El certificado se utiliza durante el intercambio de señales con los clientes de Cisco UMA.

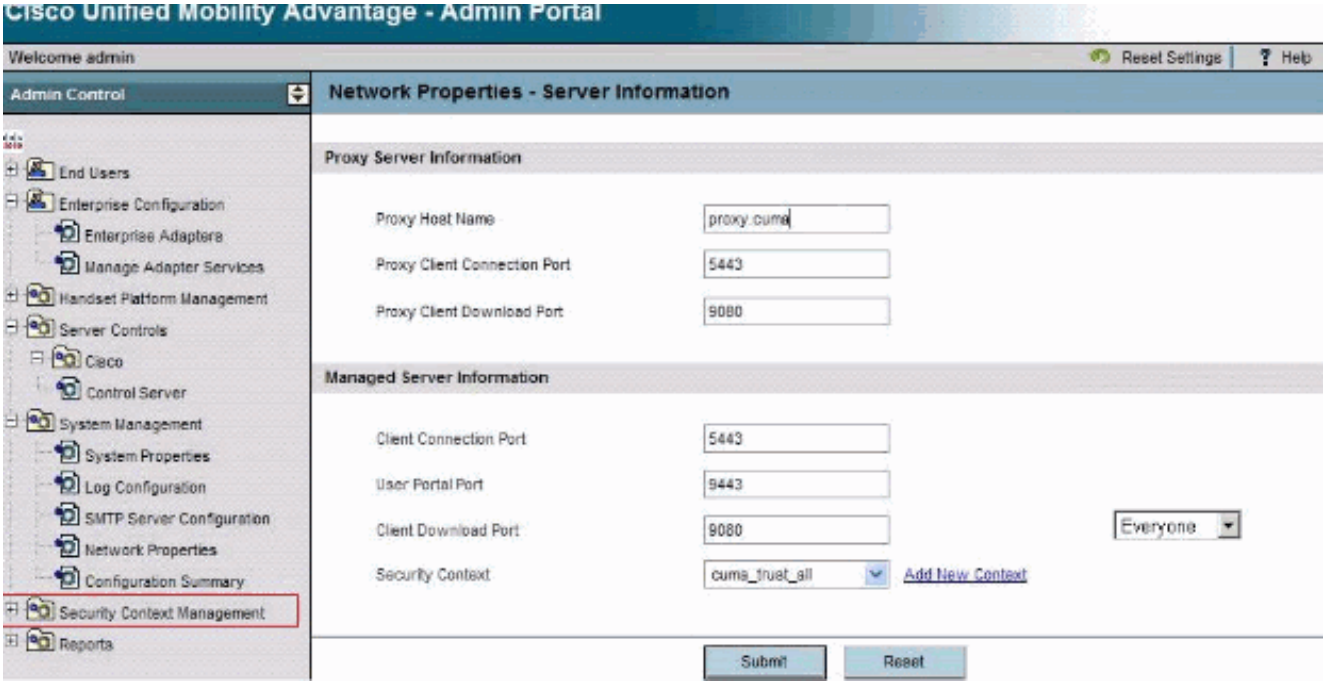
La instalación del certificado autofirmado del servidor Cisco UMA en el almacén de confianza del dispositivo de seguridad adaptable es necesaria para que el dispositivo de seguridad adaptable autentique el servidor Cisco UMA durante el intercambio de señales entre el proxy del dispositivo de seguridad adaptable y el servidor Cisco UMA.

## Instalación del certificado autofirmado del servidor Cisco UMA

### Tareas que deben realizarse en el servidor CUMA

Estos pasos deben realizarse en el servidor CUMA. Con estos pasos, crea un certificado autofirmado en CUMA para intercambiar con ASA con CN=portal.aipc.com. Esto debe instalarse en el almacén de confianza de ASA. Complete estos pasos:

1. Cree un certificado autofirmado en el servidor CUMA.Inicie sesión en el portal de administración de Cisco Unified Mobility Advantage.Elija **[+]** junto a Administración del Contexto de
   Seguridad.




Elija **Contextos de Seguridad**.Elija **Add Context**.Ingresar esta información

```
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. Descargue los certificados autofirmados de Cisco Unified Mobility Advantage. Complete estos pasos para realizar la tarea:Elija **[+]** junto a Administración del Contexto de Seguridad.Elija **Contextos de Seguridad**.Elija **Administrar contexto** junto al contexto de seguridad que contiene el certificado para descargar.Elija **Descargar certificado**.**Nota:** Si el certificado es una cadena y tiene certificados raíz o intermedios asociados, sólo se descarga el primer certificado de la cadena. Esto es suficiente para los certificados autofirmados.Guarde el archivo.
3. El siguiente paso es agregar el certificado autofirmado de Cisco Unified Mobility Advantage al ASA. Complete estos pasos en el ASA:Abra el certificado autofirmado de Cisco Unified Mobility Advantage en un editor de texto.Importe el certificado en el almacén de confianza de Cisco Adaptive Security Appliance:

```
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. Exportar el certificado autofirmado de ASA en el servidor CUMA. Debe configurar Cisco Unified Mobility Advantage para solicitar un certificado del Cisco Adaptive Security Appliance. Complete estos pasos para proporcionar el certificado autofirmado requerido.

Estos pasos deben realizarse en el ASA.Generar un nuevo par de claves:

```
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...
```

Agregue un nuevo punto de confianza:

```
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
```

Inscriba el punto de confianza:

```
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
```

Exportar el certificado a un archivo de texto.

```
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. Copie el resultado anterior en un archivo de texto y agréguelo al almacén de confianza del servidor CUMA y utilice este procedimiento:Elija **[+]** junto a Administración del Contexto de Seguridad.Elija **Contextos de Seguridad**.Elija **Administrar contexto** junto al Contexto de Seguridad en el que importa el certificado firmado.Elija **Importar** en la barra Certificados de confianza.Pegue el texto del certificado.Nombre el certificado.Elija **Importar**.**Nota:** Para la configuración de destino remoto, llame al teléfono de escritorio para determinar si el teléfono móvil suena al mismo tiempo. Esto confirmaría que la conexión móvil funciona y que no hay problema con la configuración de destino remoto.

## Problema al agregar la solicitud de certificado CUMA a otras autoridades certificadoras

### Problema 1

Muchas instalaciones de demostración/prototipo donde ayuda si la solución CUMC/CUMA funciona con certificados de confianza son autofirmadas u obtenidas de *otras autoridades certificadoras*. Los certificados de verificación son caros y la obtención de estos certificados lleva mucho tiempo. Es bueno si la solución admite certificados autofirmados y certificados de otras CA.

Los certificados actuales admitidos son GeoTrust y Verisign. Esto se documenta con el ID de bug de Cisco CSCta62971 (sólo clientes registrados)

## Error: No se puede conectar

Cuando intenta acceder a la página del portal de usuarios, por ejemplo, `https://<host>:8443`, aparece el mensaje de error `No se puede conectar`.

### Solución

Este problema se documenta con el ID de bug de Cisco CSCsm26730 (sólo clientes registrados) . Para acceder a la página del portal del usuario, complete esta solución:

La causa de este problema es el carácter en dólares, por lo que escape el carácter en dólares con otro carácter en dólares en el **archivo server.xml** del servidor administrado. Por ejemplo, edite /opt/cuma/jpatrón-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml.

En línea: **keystorePass="pa$word"** maxSpareThread="15"

Reemplace el `$` por `$$`. Parece **keystorePass="pa$$word"** maxSpareThread="15".

## No se puede acceder a algunas páginas del portal de administración de CUMA

Estas páginas no se pueden ver en el **Portal de administración de CUMA**:

- activar/desactivar usuario
- búsqueda/mantenimiento

Si el usuario hace clic en una de las dos páginas anteriores del menú a la izquierda, el explorador parece indicar que está cargando una página, pero no sucede nada (sólo se ve la página anterior que estaba en el explorador).

### Solución

Para resolver este problema relacionado con la página de usuario, cambie el puerto utilizado para Active Directory a **3268** y reinicie el CUMA.

## Información Relacionada

- Configuración paso a paso del proxy ASA-CUMA
- Introducción a ASR5000 v1
- Actualización de Cisco Unified Mobility Advantage
- Soporte de tecnología de voz
- Soporte de Productos de Voice and Unified Communications
- Soporte Técnico y Documentación - Cisco Systems