

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Si usted no tiene las claves preexistentes y Certificados para el Content Services Switch (CSS), usted puede generarlos en el CSS. El CSS incluye una serie de utilidades de administración del certificado y de la clave privada para simplificar el proceso de generar las claves privadas, los pedidos de firma de certificado (CSR), y los Certificados temporales uno mismo-firmados. Este documento describe el proceso para obtener un nuevo certificado de un Certificate Authority (CA) y instalarlo al CSS.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

[Configurar](#)

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para encontrar la información adicional en los comandos usados en este documento, use la [Command Lookup Tool](#) ([clientes registrados solamente](#)).

Configuraciones

Este documento usa las configuraciones detalladas a continuación.

- Genere el Rivest, el Shamir, y el par clave del Adelman (RSA)
- Asocie el archivo del par clave RSA
- Genere el CSR
- Obtenga el certificado de CA
- Importe el archivo de certificado encadenado
- Asocie el archivo de certificado
- Configure la lista del proxy SSL
- Configure el servicio y las reglas de contenido del Secure Socket Layer (SSL)

Genere el Rivest, el Shamir, y el par clave del Adelman (RSA)

Publique el comando **ssl genrsa** de generar un soldado/el par clave público RSA para la encriptación asimétrica. El CSS salva el par clave generado RSA como archivo en el CSS. Por ejemplo, para generar el par clave **myrsakey.pem** RSA, teclee el siguiente:

```
CSS11500(config) # ssl genrsa myrsakey.pem 1024  
?passwd123?Please be patient this could take a few minutes
```

Asociación del archivo del par clave RSA

Publique el comando **ssl associate rsakey** de asociar el nombre del par clave RSA al par clave generado RSA. Por ejemplo, para asociar el nombre de la clave **myrsakey1** RSA al archivo generado **myrsakey.pem** del par clave RSA, teclee el siguiente: `CSS11500(config) # ssl associate rsakey myrsakey1 myrsakey.pem`

Genere el CSR

Publique el comando **ssl gencsr rsakey** de generar un archivo CSR para un archivo asociado del par clave RSA. Este CSR será enviado a CA para firmar. Por ejemplo, para generar un CSR basado en el par clave **myrsakey1** RSA, teclee el siguiente: `CSS11503(config)# ssl gencsr myrsakey1`

```
You are about to be asked to enter  
informationthat will be incorporated into your  
certificaterequest. What you are about to enter is what  
iscalled a Distinguished Name or a DN.For some fields there  
will be a default value,If you enter '.', the field will be  
left blank.Country Name (2 letter code) [US] USState or  
Province (full name) [SomeState] CALocality Name (city)  
[SomeCity] San JoseOrganization Name (company name) [Acme  
Inc]Cisco Systems, Inc.Organizational Unit Name (section)  
[Web Administration] Web AdminCommon Name (your domain name)  
[www.acme.com] www.cisco.comEmail address [webadmin@acme.com]  
webadmin@cisco.com
```

El comando **ssl gencsr** genera el CSR y lo hace salir a la pantalla. La mayoría de los CA importantes tienen aplicaciones basadas en Web que le

requieran cortar y pegar el pedido de certificado a la pantalla. `CSS11503(config)# ssl gensr myrsakey1` You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [US] **US** State or Province (full name) [SomeState] **CA** Locality Name (city) [SomeCity] **San Jose** Organization Name (company name) [Acme Inc] **Cisco Systems, Inc.** Organizational Unit Name (section) [Web Administration] **Web Admin** Common Name (your domain name) [www.acme.com] **www.cisco.com** Email address [webadmin@acme.com] **webadmin@cisco.com** CA firma el CSR y le lo vuelve, típicamente usando la dirección de correo electrónico proporcionada dentro del CSR.

Obtenga el certificado de CA

Después de someter su CSR a CA, toma entre un y siete días hábiles para recibir un certificado firmado; los tiempos varían debido a CA. Una vez que CA ha firmado y ha entregado el certificado, puede ser agregado al CSS.

Archivo de certificado encadenado de la importación

Una vez que el CSR ha sido firmado por CA, ahora se llama un certificado. El archivo de certificado se debe importar al CSS. Publique el **comando copy ssl** de facilitar la importación o la exportación de los Certificados y de las claves privadas o al CSS. El CSS salva todos los archivos importados en una ubicación segura en el CSS. Este comando está disponible solamente en el modo de superusuario. Por ejemplo, para importar el certificado del `mychainedrsacert.pem` de un servidor remoto al CSS, teclee el siguiente: `CSS11500# copy ssl sftp ssl_record import mychainedrsacert.pem PEM ?passwd123?Connecting Completed successfully`

Asocie el archivo de certificado

Publique el **comando ssl associate cert** de asociar un nombre del certificado al certificado importado. Por ejemplo, para asociar el nombre `mychainedrsacert1` del certificado al `mychainedrsacert.pem` importado del archivo de certificado, teclee el siguiente:
`CSS11500(config)# ssl associate cert mychainedrsacert1 mychainedrsacert.pem`

Configure la lista del proxy SSL

Publique el **comando ssl-proxy-list** de crear una lista del proxy SSL. Una lista del proxy SSL es un grupo de servidores SSL virtuales o backend relacionados que se asocian a un servicio SSL. La lista del proxy SSL contiene toda la información de la configuración para cada servidor SSL virtual. Esto incluye el par clave SSL de la creación de servidor SSL, de los Certificados y de la correspondencia, IP virtual el direccionamiento (VIP) y puerto, las cifras SSL soportadas, y otras opciones de

SSL. Por ejemplo, para crear la lista SSL del proxy `ssl_list1`, teclee el siguiente:

```
CSS11500(config)# ssl-proxy-list ssl_list1Create ssl-list <ssl_list1>, [y/n]: y
```

Una vez que usted crea una lista del proxy SSL, el CLI le ingresa en el modo de configuración de la lista SSL del proxy. Configure a su servidor SSL como se muestra abajo.

```
CSS11500(ssl-proxy-list[ssl_list1])# ssl-server  
20CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 vip  
address 192.168.3.6CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 rsacert mychainedrsacert1CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 rsakey myrsa  
key1CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 cipher rsa-export-with-rc4-40-md5  
192.168.11.2 80 5CSS11500(ssl-proxy-list[ssl_list1])# active
```

Configure el servicio y las reglas de contenido del Secure Socket Layer (SSL)

Una vez que se activa la lista del proxy SSL, una necesidad del servicio y de la regla de contenido de ser configurado para permitir que el CSS envíe el tráfico SSL al módulo SSL. Esta tabla proporciona una descripción de los pasos requeridos para crear un servicio SSL para un servidor SSL virtual, incluyendo agregar la lista del proxy SSL al servicio y crear una regla de contenido SSL.

Cree un servicio SSL

```
CSS11500(config)# service ssl_serv1Create service <ssl_serv1>, [y/n]: y  
CSS11500(config-service[ssl_serv1])# type ssl-accel  
CSS11500(config-service[ssl_serv1])# slot 2  
CSS11500(config-service[ssl_serv1])# keepalive type none  
CSS11500(config-service[ssl_serv1])# add ssl-proxy-list ssl_list1  
CSS11500(config-service[ssl_serv1])# active
```

Cree una regla de contenido SSL

```
CSS11500(config)# owner ssl_ownerCreate owner <ssl_owner>, [y/n]: y  
CSS11500(config-owner[ssl_owner])# content ssl_rule1Create content <ssl_rule1>, [y/n]: y  
CSS11500(config-owner-content[ssl_rule1])# vip address 192.168.3.6  
CSS11500(config-owner-content[ssl_rule1])# port 443  
CSS11500(config-owner-content[ssl_rule1])# add service ssl_serv1  
CSS11500(config-owner-content[ssl_rule1])# active
```

Cree una regla de contenido del texto claro

```
CSS11500(config-owner[ssl_owner])# content decrypted_wwwCreate content <decrypted_www>, [y/n]: y  
CSS11500(config-owner-content[decrypted_www])# vip address 192.168.11.2  
CSS11500(config-owner-content[decrypted_www])# port 80  
CSS11500(config-owner-content[decrypted_www])# add service linux_http  
CSS11500(config-owner-content[decrypted_www])# add service win2k_http  
CSS11500(config-owner-content[decrypted_www])# active
```

En este momento, el tráfico del cliente HTTPS se puede enviar al CSS en 192.168.3.6:443. El CSS descripta el tráfico HTTPS, convirtiéndolo al HTTP. El CSS después elige un servicio y envía el tráfico HTTP a un servidor Web HTTP. Lo que sigue es una configuración CSS de trabajo usando los ejemplos anteriores:

```
CSS11501# show runconfigure!***** GLOBAL  
*****ssl associate rsakey myrsa  
key1  
myrsakey.pemssl associate cert mychainedrsacert1  
mychainedrsacert.pemip route 0.0.0.0 0.0.0.0 192.168.3.1
```

```
1ftp-record conf 192.168.11.101 admin des-password
4f2bxansrcehgka /tftpboot!*****
INTERFACE *****interface 1/1bridge vlan
10description "Client Side"interface 1/2bridge vlan
20description "Server Side"!*****
CIRCUIT *****circuit VLAN10description
"Client Segment"ip address 192.168.3.254 255.255.255.0circuit
VLAN20description "Server Segment"ip address 192.168.11.1
255.255.255.0!***** SSL PROXY LIST
*****ssl-proxy-list ssl_list1ssl-server
20ssl-server 20 vip address 192.168.3.6ssl-server 20 rsakey
myrsakey1ssl-server 20 rsacert mycertcert1ssl-server 20
cipher rsa-with-rc4-128-md5 192.168.11.2
80active!***** SERVICE
*****service linux-httpip address
192.168.11.101port 80activeservice win2k-httpip address
192.168.11.102port 80activeservice ssl_serv1type ssl-
accelslot 2keepalive type noneadd ssl-proxy-list
ssl_list1active!***** OWNER
*****owner ssl_ownercontent
ssl_rule1vip address 192.168.3.6protocol tcpport 443add
service ssl_serv1activecontent decrypted_wwwvip address
192.168.11.2add service linux-httpadd service win2k-
httpprotocol tcpport 80active
```

[Verificación](#)

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

[Troubleshooting](#)

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

[Información Relacionada](#)

- [Soporte del hardware de los CSS 11500 Series Content Services Switch](#)
- [Soporte del hardware de los CSS 11000 Series Content Services Switch](#)
- [Descarga del software de Cisco WebNS CSS11500 \(clientes registrados solamente\)](#)
- [Descarga del software de Cisco WebNS CSS11000 \(clientes registrados solamente\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)