

# Video Communications Server (VCS)- Webschnittstelle wiederherstellen - Widerruf des Zertifikats

## Inhalt

[Einführung](#)

[Verwendete Komponenten](#)

[Problem](#)

[Lösung](#)

[SCP-Anwendung \(für z. B.: WinSCP\)](#)

### Einführung

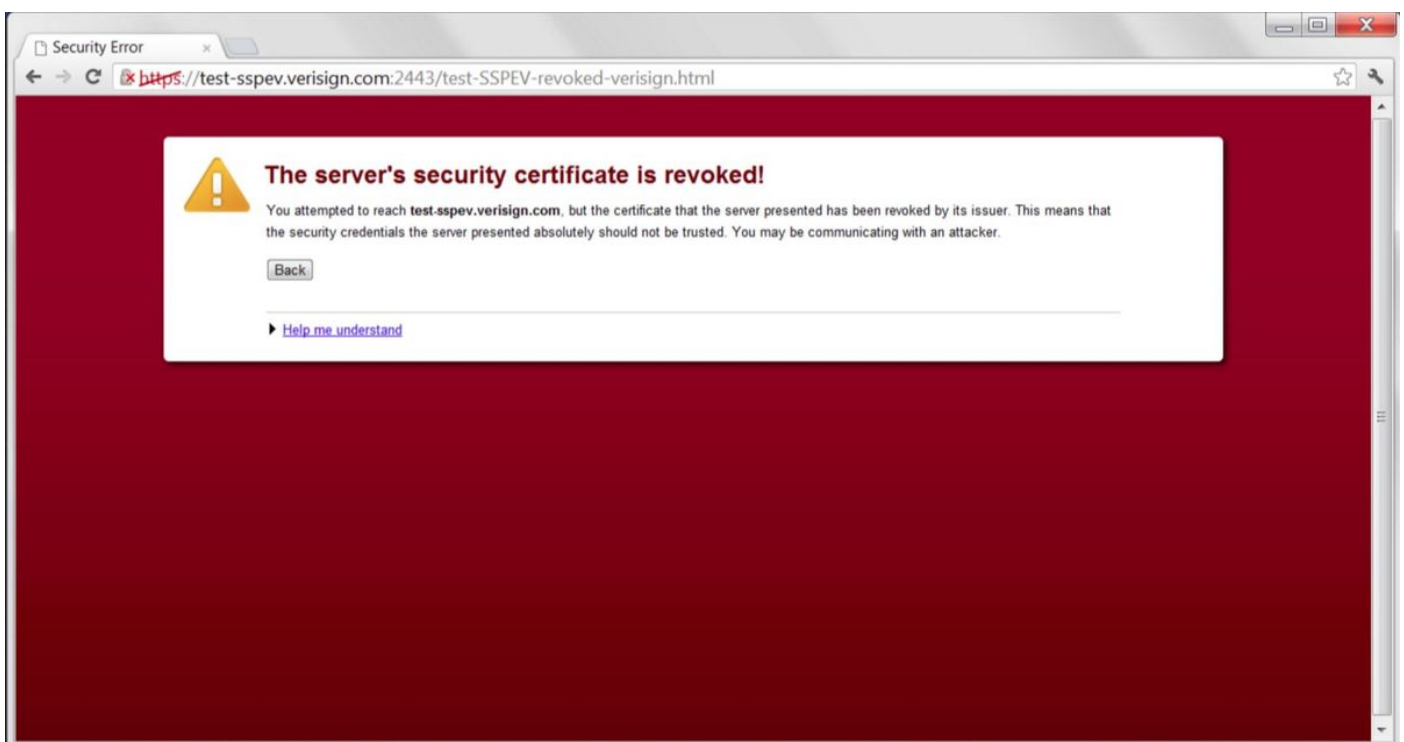
In diesem Dokument wird das Szenario beschrieben, in dem Zertifikate auf VCS-Servern (Video Communications Server) widerrufen wurden und daher nicht auf die grafische Benutzeroberfläche (GUI) zugegriffen werden kann.

### Verwendete Komponenten

VCS mit abgelaufenem Serverzertifikat

### Problem

In diesem Szenario hätten Sie keinen Zugriff auf die VCS-GUI. Wenn Sie versuchen, über die Benutzeroberfläche auf das VCS zuzugreifen, erhalten Sie einen Fehler, dass das Zertifikat des VCS-Servers widerrufen wurde.



## Lösung

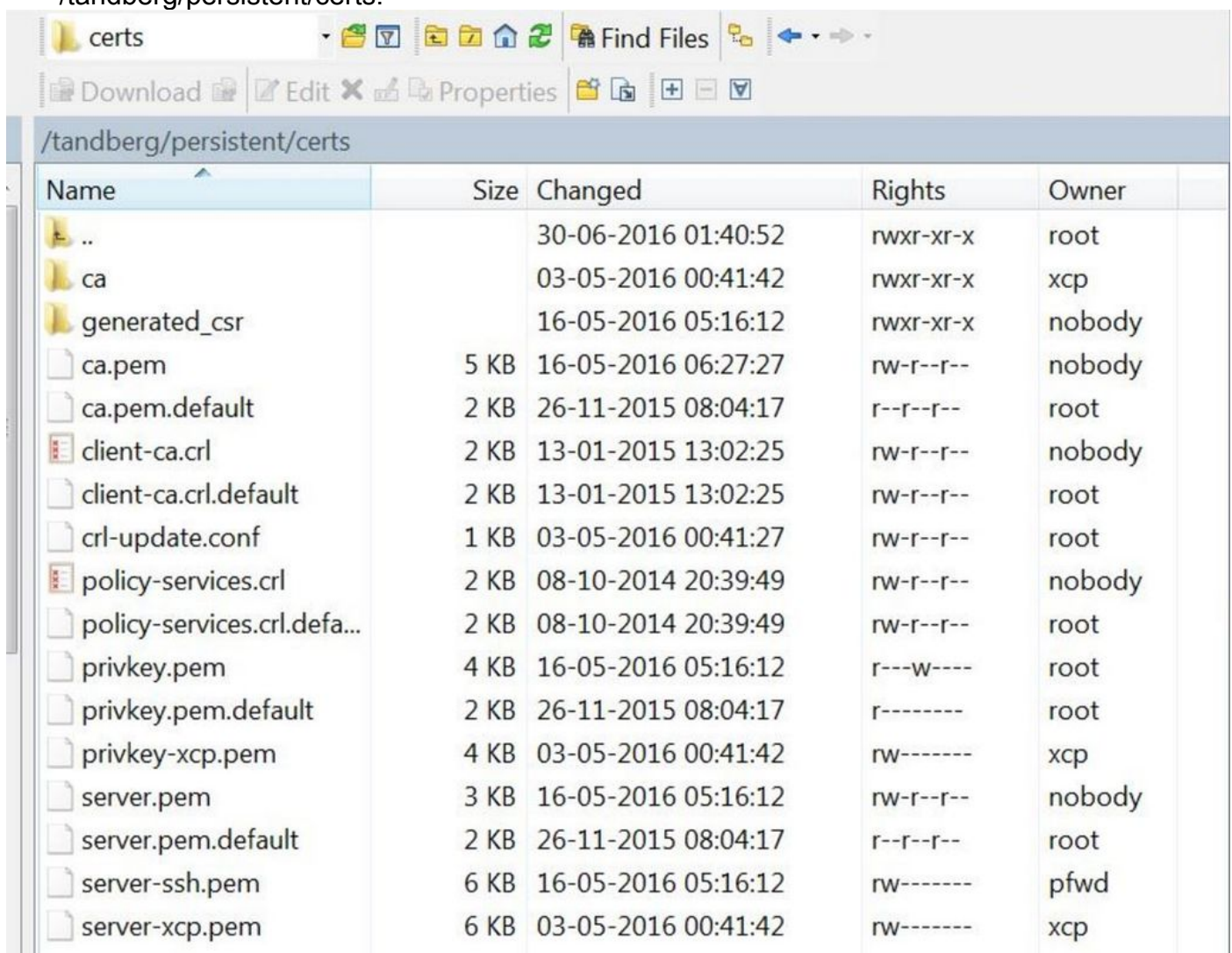
Um das Problem zu beheben, müssen Sie auf die Standard-Zertifikate im VCS zurücksetzen. Dadurch wird der GUI-Zugriff aktiviert, und dann müssen Zertifikate neu generiert werden.

Sie können diese Aufgabe auf zwei Arten durchführen:

1. Verwenden einer Secure Copy Protocol (SCP)-Software (z. B.: WinSCP)
2. Verwenden der CLI (Root Command Line Interface)

## SCP-Anwendung (für z. B.: WinSCP)

- Verwenden der SFTP-Anwendung (Secure File Transfer Protocol) (z. B.: WinSCP), navigieren Sie nach der Anmeldung mit Root Credetals für VCS zum Verzeichnis `/tandberg/persistent/certs`.



Name	Size	Changed	Rights	Owner
..		30-06-2016 01:40:52	rwxr-xr-x	root
ca		03-05-2016 00:41:42	rwxr-xr-x	xcp
generated_csr		16-05-2016 05:16:12	rwxr-xr-x	nobody
ca.pem	5 KB	16-05-2016 06:27:27	rw-r--r--	nobody
ca.pem.default	2 KB	26-11-2015 08:04:17	r--r--r--	root
client-ca.crl	2 KB	13-01-2015 13:02:25	rw-r--r--	nobody
client-ca.crl.default	2 KB	13-01-2015 13:02:25	rw-r--r--	root
crl-update.conf	1 KB	03-05-2016 00:41:27	rw-r--r--	root
policy-services.crl	2 KB	08-10-2014 20:39:49	rw-r--r--	nobody
policy-services.crl.defa...	2 KB	08-10-2014 20:39:49	rw-r--r--	root
privkey.pem	4 KB	16-05-2016 05:16:12	r---w----	root
privkey.pem.default	2 KB	26-11-2015 08:04:17	r-----	root
privkey-xcp.pem	4 KB	03-05-2016 00:41:42	rw-----	xcp
server.pem	3 KB	16-05-2016 05:16:12	rw-r--r--	nobody
server.pem.default	2 KB	26-11-2015 08:04:17	r--r--r--	root
server-ssh.pem	6 KB	16-05-2016 05:16:12	rw-----	pfwd
server-xcp.pem	6 KB	03-05-2016 00:41:42	rw-----	xcp

- Remove (BACKUP ERHALTEN) server.pem, privkey.pem, ca.pem, client-ca.crl, policy-services.crl
- Starten Sie den HTTP-Dienst vom Root neu (`/etc/init.d/S80httpd restart`)

## ROOT-CLI

Verwenden Sie einen beliebigen SSH-Client und SSH für VCS mithilfe von Root Credetals.

Bei Versionen vor VCS 12.5 (alle 8.x-Versionen) müssen die vorhandenen Zertifikate durch die Standardzertifikate ersetzt werden, indem die folgenden Befehle verwendet werden:

```
~ # cp /tandberg/persistent/certs/server.pem.default /tandberg/persistent/certs/server.pem
```

```
~ # cp /tandberg/persistent/certs/privkey.pem.default /tandberg/persistent/certs/privkey.pem
```

```
~ # cp /tandberg/persistent/certs/ca.pem.default /tandberg/persistent/certs/ca.pem
```

```
~ # cp /tandberg/persistent/certs/client-ca.crl.default /tandberg/persistent/certs/client-ca.crl
```

```
~ # cp /tandberg/persistent/certs/policy-services.crl.default /tandberg/persistent/certs/policy-services.crl
```

```
~ /etc/init.d/S80httpd restart
```

Für Version 12.5 existieren die Standardzertifikate nicht mehr unter:

```
~ cd /tandberg/persistent/certs
```

```
~ #
```

Die ".default"-Zertifikate werden hier nicht angezeigt.

Sie müssen server.pem löschen und den VCS neu starten, um das VCS auf die Standard-Zertifikate zurückzusetzen.

```
~ rm server.pem
```

```
~ # Neustart
```