

Recover Video Communications Server (VCS) Web interface - revoked Certificate

Contents

[Introduction](#)

[Components used](#)

[Problem](#)

[Solution](#)

[SCP Application \(for eg: WinSCP\)](#)

Introduction

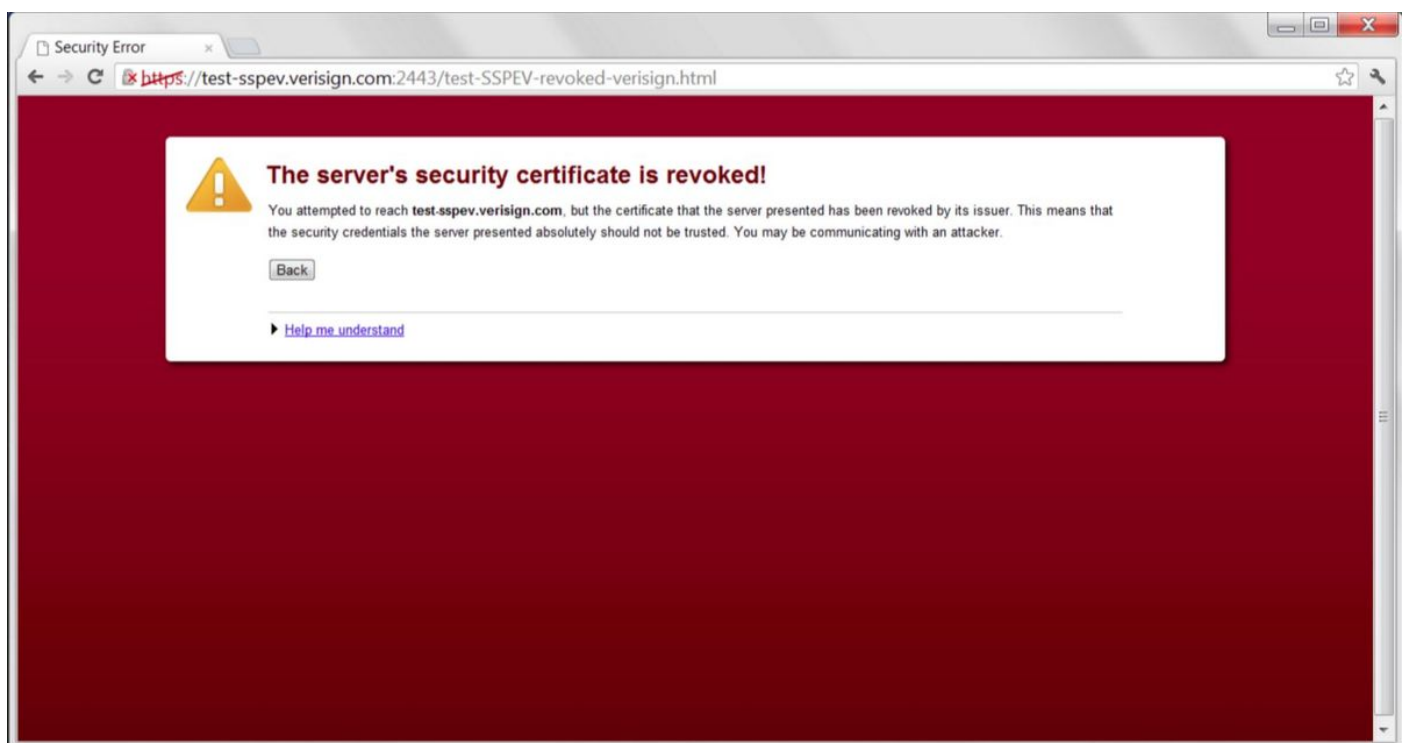
This document describes the scenario where certificate on Video Communications Server (VCS) servers has been revoked and as a result the Graphical User Interface (GUI) is not accessible.

Components used

VCS with expired server certificate

Problem

In this scenario you would not have access to VCS GUI and an attempt to access the VCS through GUI will give you an error that the certificate of the VCS server has been revoked



Solution

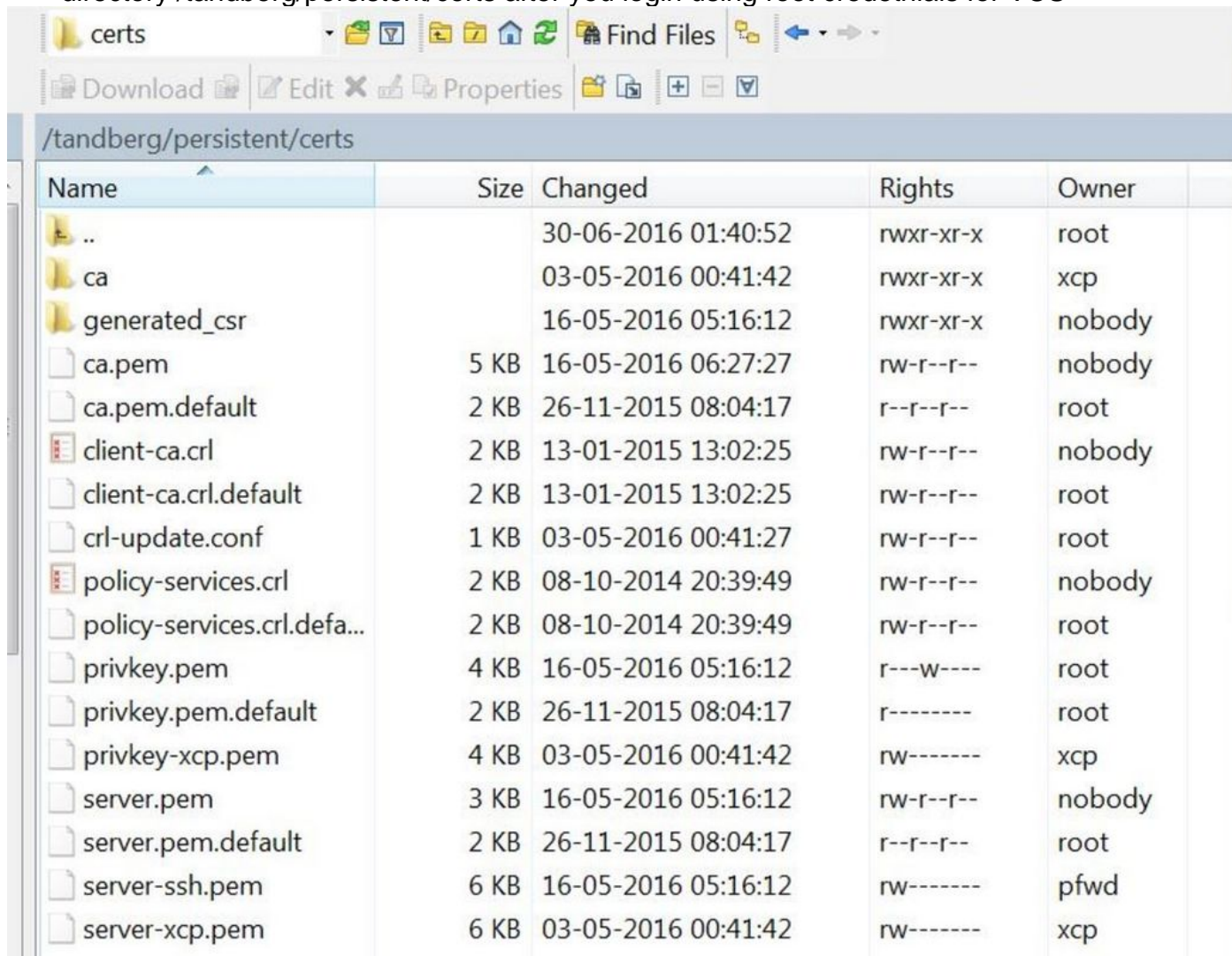
To mitigate the issue you would need to revert to default certificates on the VCS. This will enable GUI access and then certificates will need to be re-generated.

You can achieve the above task in either of the two ways:

1. Using an Secure Copy Protocol (SCP) software (for eg: WinSCP)
2. Using root Command Line Interface (CLI)

SCP Application (for eg: WinSCP)

- Using Secure File Transfer Protocol (SFTP) application (for eg: WinSCP), navigate to the directory /tandberg/persistent/certs after you login using root credetnials for VCS



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 (KEEP BACKUP) server.pem, privkey.pem, ca.pem, client-ca.crl, policy-services.crl
- Restart HTTP service from root (/etc/init.d/S80httpd restart)

ROOT CLI

Use any SSH client and ssh to VCS using root credetials.

For versions prior to VCS 12.5(all 8.x versions), replace the existing certificates with the default certificates using the following commands:

```
~ # 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
```

For version 12.5 the the defaults certificates dont exist anymore under:

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

```
~ # ls
```

You will not see the .default certs here.

You need to delete the server.pem and reboot the VCS which will revert the VCS to default certificates.

```
~ # rm server.pem
```

```
~ # reboot
```