

Troubleshoot PCCE 12.0 SPOG File Transfer Failure

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Problem](#)

[Solution](#)

Introduction

This document describes how to troubleshoot Cisco Packaged Contact Center Enterprise (PCCE) 12.0 Single Pane Of Glass (SPOG) File Transfer Failure.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- PCCE
- Customer Voice Port (CVP)

Components Used

The information in this document is based on PCCE 12.0.1.

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.

Problem

In PCCE SPOG, for file transfer, navigate to **SPOG > OverView > Call Settings > IVR Settings > File Transfers**. At times, the transfer fails as shown in the image:



Job ID	State	Creation Time	Description
<input type="checkbox"/> 5004	● Failed		

Solution

1. Navigate to **Job** and select the **Log File** as shown in the image.

IVR Settings

View Job ID 5004

State ● Failed


Description


Host

Creation Time

Start Time

Total Time 0 min, 6 sec

Job Details 

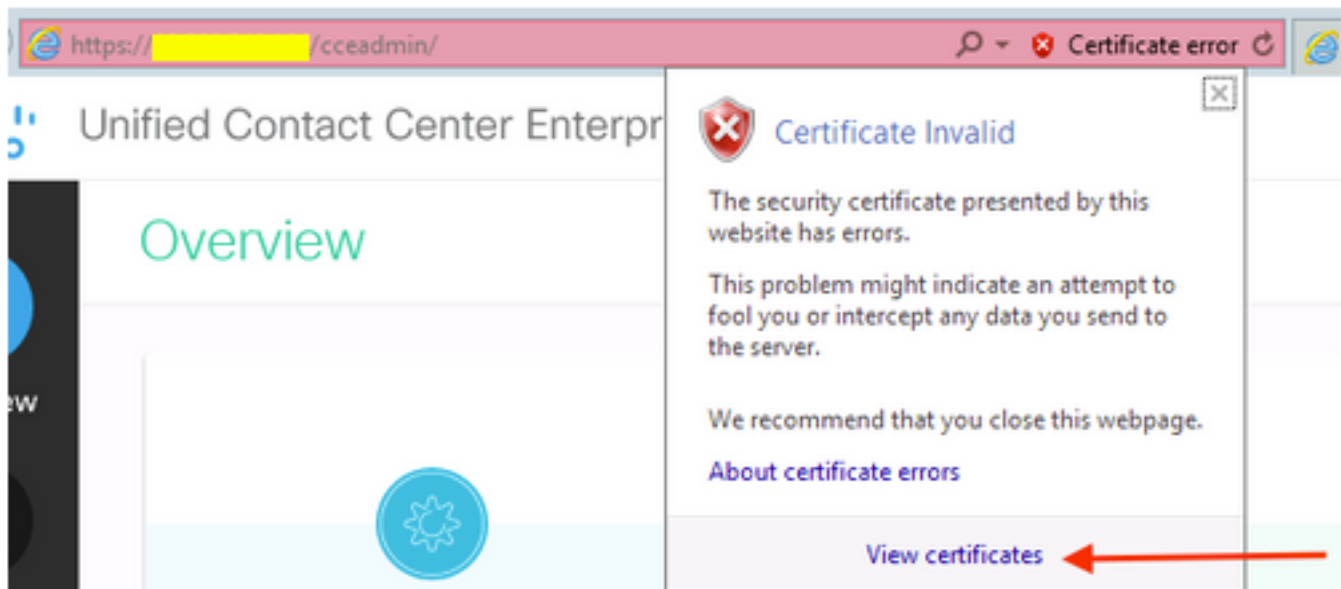
Log File 

Notice for the error message

```
"Deployment of https://<FQDN of AW node>:443/unifiedconfig/config/downloadablefiles/ivrapplication/<FileName>.zip completed on <CVP FQDN> with status as sun.security.validator.ValidatorException: No trusted certificate found."
```

This error implies that there is an issue here due to AW certificate not being trusted by CVP. Steps that can fix this situation are:

2. Copy the certificate file from SPOG URL, as shown in the image.



3. Copy this certificate file to CVP node where the original ZIP file has to be transferred to a directory:

```
C:\cisco\cvp\conf\security
```

4. Next, copy the keystore password from the location:

```
keystore password from : %CVP_HOME%\conf\ and open the security.properties
```

5. In the same way, where the AW certificate was copied to; open Command Prompt as an Administrator, and run the command:

```
cd %CVP_HOME%\jre\bin
```

6. Use this command in order to import the AW certificates to the CVP server.

```
keytool -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -  
alias  
<FQDN of AW Node> -file C:\Cisco\CVP\conf\security\<Name of the AW SPOG certificate>.cer
```

7. At the password prompt, paste the password copied from the **security.properties**.

8. Type **Yes** in order to trust the certificate and ensure you get the result that Certificate was added to keystore.

There is a warning prompted along with the successful import. This is due to proprietary format Keystore and can be ignored.

9. Restart cvpcallservice, vxmlserver and wsm service on CVP nodes.