

Troubleshoot Expressway Upgrade Error

Contents

[Introduction](#)

[Background Information](#)

[Components Used](#)

[What to do Next?](#)

[Procedure](#)

[Additional Information](#)

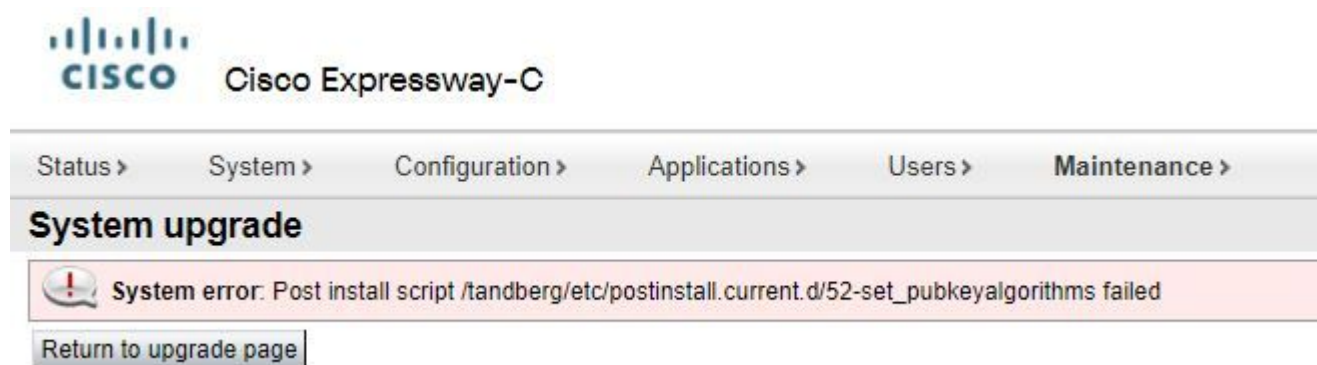
Introduction

This document describes how to fix an Expressway Upgrade Error.

Background Information

On some occasions, while you upgrade the Expressway servers to a higher version, the upgrade fails with the error:

System error: Post install script /tandberg/etc/postinstall.current.d/52-set_pubkeyalgorithms failed



The root cause of this error is the duplicate cipher entries. The main idea in this document is to provide steps needed to remove the duplicate cipher entries in configuration.

Components Used

Expressway on version X12.7.1.

Upgrade firmware on version X14.0.3.

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, ensure that you understand the potential impact of any command.

What to do Next?

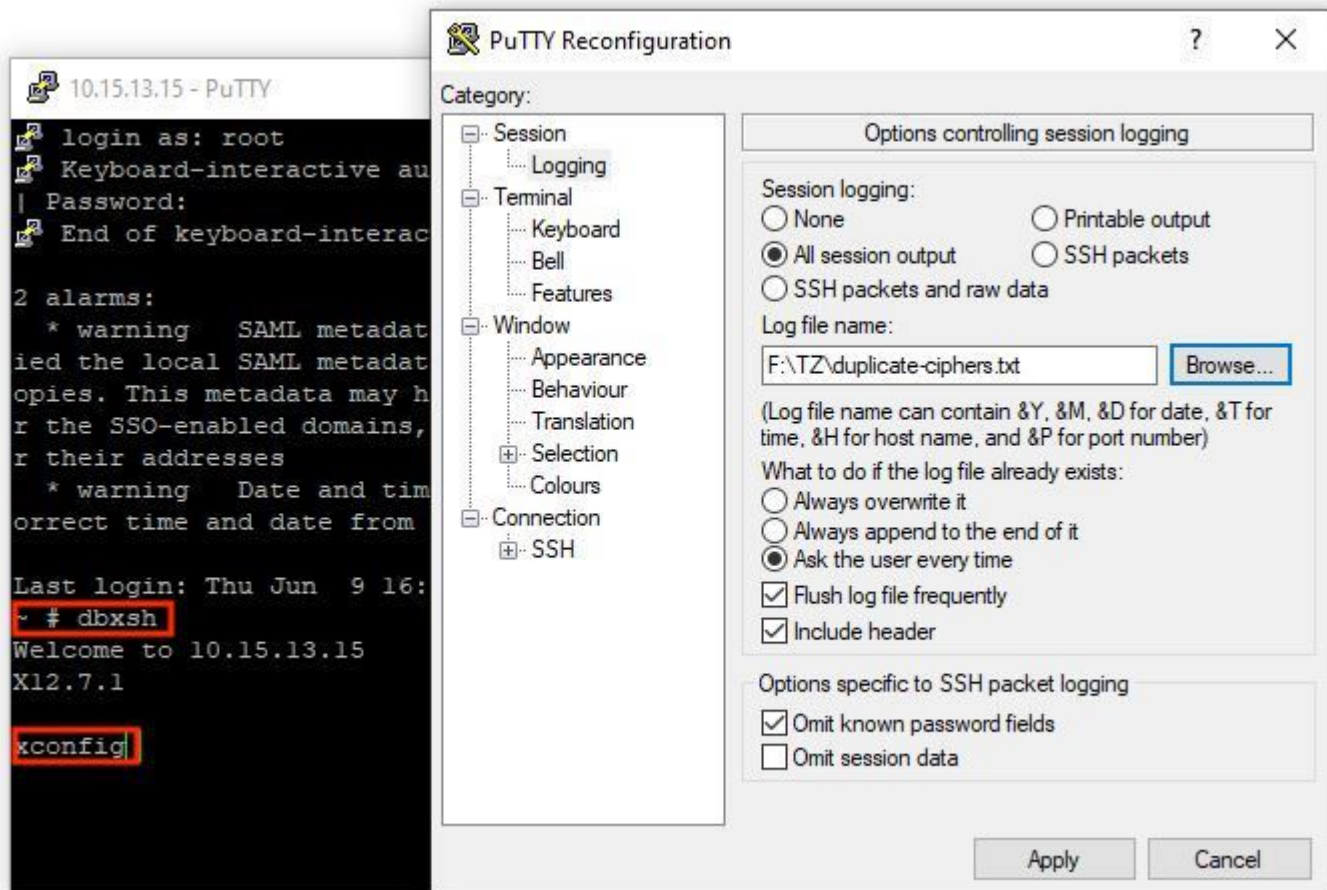
In this scenario, the first step is to take an **xconfig** file from the Expressway. The goal is to confirm which

ciphers are duplicates.

Note: Make sure to use `root` instead of `admin` account to get the `xconfig` file.

Procedure

Log in with `root` account into the Expressway server by SSH, type `dbxsh`, then run the `xconfig` command. Save the output in a `.txt` file.



Open the `xconfig` file, search for the duplicated cipher entries. You are recommended to take note of which entries are duplicates. By the use of Notepad++ (Windows) or Sublime Text (Mac), it is possible to filter for the words `cipher uuid`, then look for duplicates, as shown in this example:

```

*new 1 - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
xconfig-cipher.txt new 1
1 xconfiguration cipher uuid 0276f859-fb9e-4e47-92fd-ea7f42cea988 uuid: "0276f859-fb9e-4e47-92fd-ea7f42cea988"
2 xconfiguration cipher uuid 0276f859-fb9e-4e47-92fd-ea7f42cea988 name: "RemoteSyslog1TLSProtocol"
3 xconfiguration cipher uuid 0276f859-fb9e-4e47-92fd-ea7f42cea988 value: "minTLSv1.0"
4 xconfiguration cipher uuid 085bcc06-46e8-4d4f-9a43-d6e9ebff7a67 uuid: "085bcc06-46e8-4d4f-9a43-d6e9ebff7a67"
5 xconfiguration cipher uuid 085bcc06-46e8-4d4f-9a43-d6e9ebff7a67 name: "UcClientTLSProtocol"
6 xconfiguration cipher uuid 085bcc06-46e8-4d4f-9a43-d6e9ebff7a67 value: "minTLSv1.0"
7 xconfiguration cipher uuid 1cb8a665-2d5e-4c72-b6aa-6bc4a6770cf0 uuid: "1cb8a665-2d5e-4c72-b6aa-6bc4a6770cf0"
8 xconfiguration cipher uuid 1cb8a665-2d5e-4c72-b6aa-6bc4a6770cf0 name: "RemoteSyslog3TLSCiphers"
9 xconfiguration cipher uuid 1cb8a665-2d5e-4c72-b6aa-6bc4a6770cf0 value: "ALL"
10 xconfiguration cipher uuid 1e768381-fc76-4713-94da-7f48484ba861 uuid: "1e768381-fc76-4713-94da-7f48484ba861"
11 xconfiguration cipher uuid 1e768381-fc76-4713-94da-7f48484ba861 name: "sshd_pfw_d_pubkeyalgorithms"
12 xconfiguration cipher uuid 1e768381-fc76-4713-94da-7f48484ba861 value: "x509v3-sign-rsa"
13 xconfiguration cipher uuid 1f803c71-6442-487e-86d1-202af7457b31 uuid: "1f803c71-6442-487e-86d1-202af7457b31"
14 xconfiguration cipher uuid 1f803c71-6442-487e-86d1-202af7457b31 name: "RemoteSyslog4TLSProtocol"
15 xconfiguration cipher uuid 1f803c71-6442-487e-86d1-202af7457b31 value: "minTLSv1.0"
16 xconfiguration cipher uuid 26afb85f-80ae-4569-9d48-cf30bf741430 uuid: "26afb85f-80ae-4569-9d48-cf30bf741430"
17 xconfiguration cipher uuid 26afb85f-80ae-4569-9d48-cf30bf741430 name: "sshd_pfw_d_pubkeyalgorithms"
18 xconfiguration cipher uuid 26afb85f-80ae-4569-9d48-cf30bf741430 value: "x509v3-sign-rsa"
19 xconfiguration cipher uuid 329946c9-d80a-42ee-b2cd-43bfc02998a7 uuid: "329946c9-d80a-42ee-b2cd-43bfc02998a7"
20 xconfiguration cipher uuid 329946c9-d80a-42ee-b2cd-43bfc02998a7 name: "sshd_pfw_d_kexalgorithms"
21 xconfiguration cipher uuid 329946c9-d80a-42ee-b2cd-43bfc02998a7 value: "ecdh-sha2-nistp384"
22 xconfiguration cipher uuid 45064c81-2e0c-42bd-a5dc-49a3ff2b0614 uuid: "45064c81-2e0c-42bd-a5dc-49a3ff2b0614"
23 xconfiguration cipher uuid 45064c81-2e0c-42bd-a5dc-49a3ff2b0614 name: "UcClientTLSCiphers"
24 xconfiguration cipher uuid 45064c81-2e0c-42bd-a5dc-49a3ff2b0614 value: "ALL"
25 xconfiguration cipher uuid 4f0bca0b-914a-496c-84cb-2a74bcbe0395 uuid: "4f0bca0b-914a-496c-84cb-2a74bcbe0395"
26 xconfiguration cipher uuid 4f0bca0b-914a-496c-84cb-2a74bcbe0395 name: "LDAPTLSProtocol"
27 xconfiguration cipher uuid 4f0bca0b-914a-496c-84cb-2a74bcbe0395 value: "minTLSv1.2"
28 xconfiguration cipher uuid 4f5ac5ca-2e15-4dc7-9162-5bb684425f7a uuid: "4f5ac5ca-2e15-4dc7-9162-5bb684425f7a"
29 xconfiguration cipher uuid 4f5ac5ca-2e15-4dc7-9162-5bb684425f7a name: "HTTPSProtocol"
30 xconfiguration cipher uuid 4f5ac5ca-2e15-4dc7-9162-5bb684425f7a value: "minTLSv1.0"
31 xconfiguration cipher uuid 588d2093-6bb3-44df-8e91-1a5a09fc303b uuid: "588d2093-6bb3-44df-8e91-1a5a09fc303b"
32 xconfiguration cipher uuid 588d2093-6bb3-44df-8e91-1a5a09fc303b name: "sshd_ciphers"
33 xconfiguration cipher uuid 588d2093-6bb3-44df-8e91-1a5a09fc303b value: "aes256-gcm@openssh.com,aes128-gcm@openssh.com,a"
34 xconfiguration cipher uuid 5cec77c9-3645-4484-980e-139ac6629954 uuid: "5cec77c9-3645-4484-980e-139ac6629954"
35 xconfiguration cipher uuid 5cec77c9-3645-4484-980e-139ac6629954 name: "RemoteSyslog2TLSCiphers"
36 xconfiguration cipher uuid 5cec77c9-3645-4484-980e-139ac6629954 value: "ALL"
37 xconfiguration cipher uuid 5e79851a-2ee9-44a7-9373-5887ba62546c uuid: "5e79851a-2ee9-44a7-9373-5887ba62546c"
38 xconfiguration cipher uuid 5e79851a-2ee9-44a7-9373-5887ba62546c name: "SMTPTLSProtocol"
39 xconfiguration cipher uuid 5e79851a-2ee9-44a7-9373-5887ba62546c value: "minTLSv1.2"
40 xconfiguration cipher uuid 6003cda6-afdc-4dal-9030-bdeafdeb6f43 uuid: "6003cda6-afdc-4dal-9030-bdeafdeb6f43"
41 xconfiguration cipher uuid 6003cda6-afdc-4dal-9030-bdeafdeb6f43 name: "TMSProvisioningTLSProtocol"
42 xconfiguration cipher uuid 6003cda6-afdc-4dal-9030-bdeafdeb6f43 value: "minTLSv1.2"
Normal text file length: 11,287 lines: 112 Ln: 17 Col: 64 Sel:

```

This example shows that cipher `sshd_pfw_d_pubkeyalgorithms` has a duplicate cipher with a different Universal Unique Identifier (UUID).

Once all duplicate ciphers are identified, access the Expressway server by CLI with Putty with the `root` account, then delete only duplicate entries, use the UUID information, under `dbxsh`.

Command format: `xdelete cipher uuid`

Example of ciphers deleted in this xconfig file:

`xdelete cipher uuid 26afb85f-80ae-4569-9d48-cf30bf741430`

```

10.15.13.20 - PuTTY
xdelete cipher uuid 26afb85f-80ae-4569-9d48-cf30bf741430
OK

```

Repeat the same process until all duplicate entries are deleted.

Note: This procedure can take several attempts until all duplicate entries are deleted. It is recommended to take another xconfig file to double check the ciphers.

After this, proceed with the upgrade.

Additional Information

Cisco bug ID [CSCvx35891](#)