

# Fehlerbehebung: Expressway-Upgrade-Fehler

## Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Verwendete Komponenten](#)

[Nächste Schritte](#)

[Vorgehensweise](#)

[Zusätzliche Informationen](#)

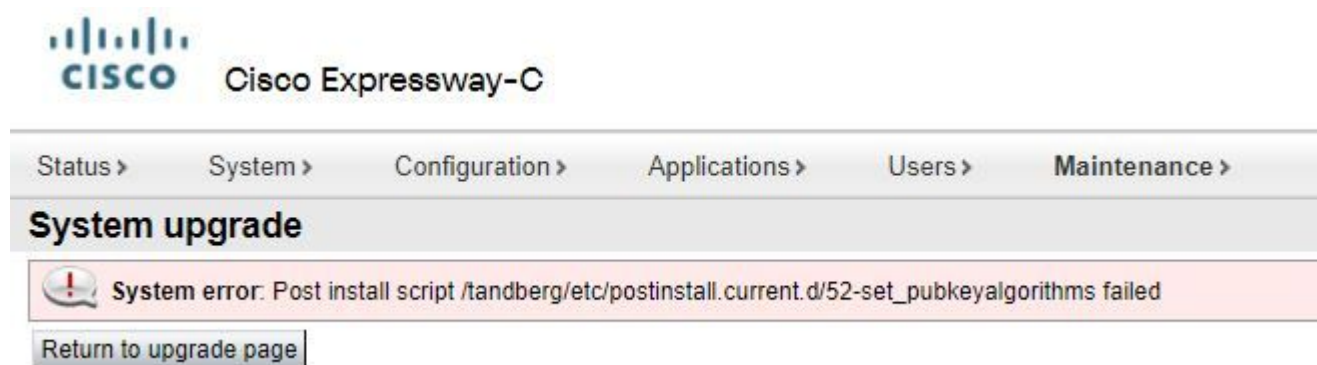
## Einleitung

In diesem Dokument wird beschrieben, wie Sie einen Expressway-Upgrade-Fehler beheben.

## Hintergrundinformationen

In einigen Fällen schlägt das Upgrade fehl, während Sie die Expressway-Server auf eine höhere Version aktualisieren:

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



Die Ursache dieses Fehlers liegt in den doppelten Verschlüsselungseinträgen. Der Hauptidee in diesem Dokument besteht darin, die erforderlichen Schritte zum Entfernen der doppelten Verschlüsselungseinträge in der Konfiguration bereitzustellen.

## Verwendete Komponenten

Expressway auf Version X12.7.1.

Aktualisieren der Firmware auf Version X14.0.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Nächste Schritte

In diesem Szenario besteht der erste Schritt darin, eine **xconfig**-Datei vom Expressway zu übernehmen. Das Ziel ist es, zu bestätigen, welche Chiffren Duplikate sind.

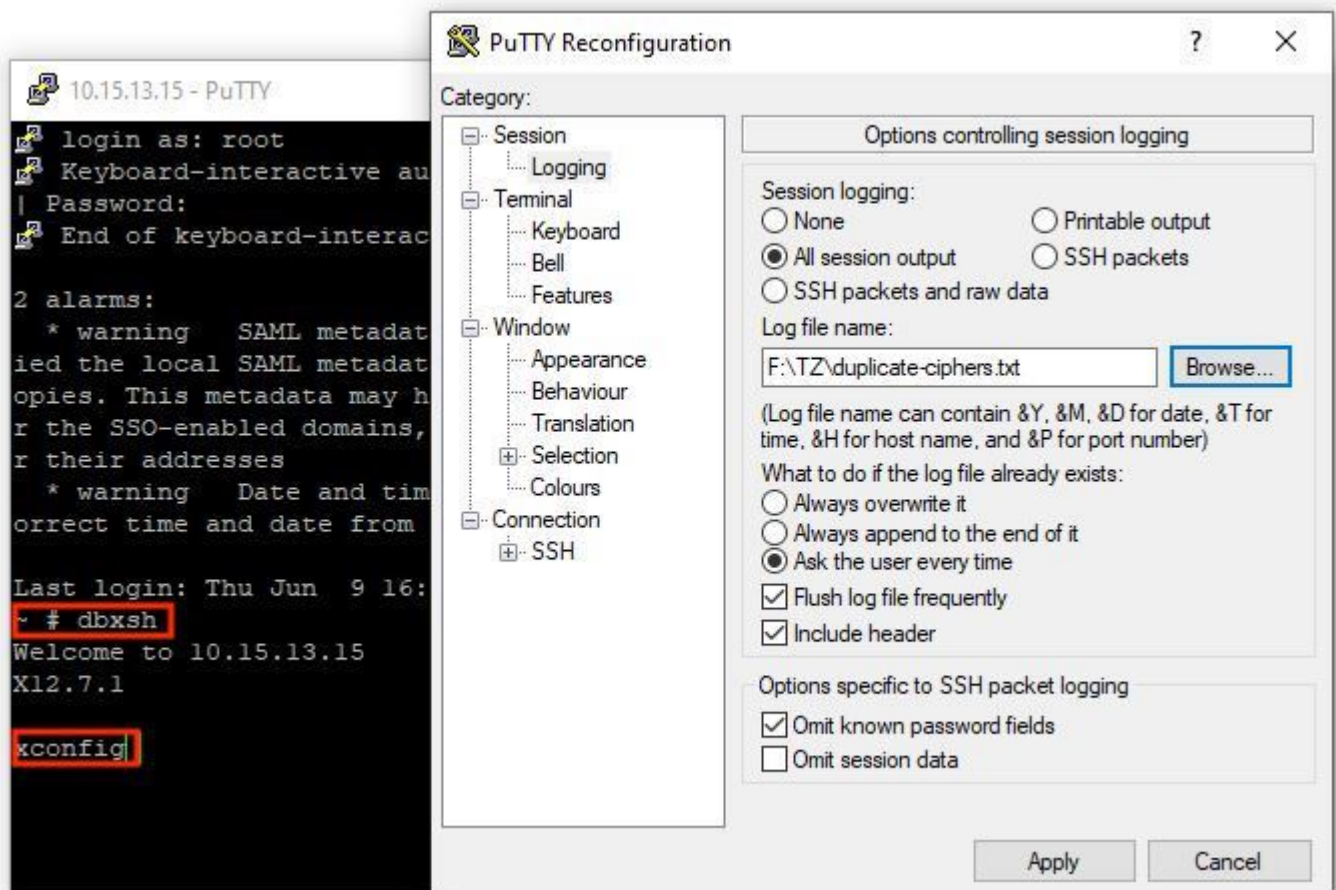
---

**Hinweis:** Achten Sie darauf, **root** statt **admin** um das **xconfig** Datei.

---

## Vorgehensweise

Anmelden mit **root** Konto auf dem Expressway-Server durch SSH, typ **dbxsh**, dann führen Sie das **xconfig** aus. Speichern Sie die Ausgabe in einem **.txt** Datei.



Öffnen Sie **xconfig** nach den doppelten Verschlüsselungseinträgen suchen. Es wird empfohlen, sich die doppelten Einträge anzumerken. Durch die Verwendung von Notepad++ (Windows) Sublime Text (Mac), kann nach den Wörtern gefiltert werden, **cipher uuid**, dann suchen Sie nach Duplikaten, wie in diesem Beispiel gezeigt:

```

*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:

```

Dieses Beispiel zeigt, dass cipher sshd\_pfw\_d\_pubkeyalgorithms verfügt über einen doppelten Verschlüsselungscode mit einem anderen Universal Unique Identifier (UUID).

Sobald alle doppelten Chiffren identifiziert wurden, greifen Sie über die CLI mit Putty über den root Konto, dann löschen Sie nur doppelte Einträge, verwenden Sie die UUID-Informationen unter dbxsh.

Befehlsformat: `xdelete cipher uuid`

Beispiel für in dieser xconfig-Datei gelöschte Chiffren:

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

```

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

```

Wiederholen Sie den gleichen Vorgang, bis alle doppelten Einträge gelöscht wurden.

---

**Hinweis:** Dieser Vorgang kann mehrere Versuche dauern, bis alle doppelten Einträge gelöscht werden. Es wird empfohlen, eine weitere xconfig-Datei zu verwenden, um die Chiffren zu überprüfen.

---

Fahren Sie anschließend mit dem Upgrade fort.

## **Zusätzliche Informationen**

Cisco Bug-ID [CSCvx35891](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.