

# Mensaje de Error de Troubleshooting en Unity Connection en Serviceability

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Etapas para solucionar problemas](#)

[Proceso 1](#)

[Proceso 2](#)

[Proceso 3](#)

[Proceso de regeneración:](#)

[Proceso 4](#)

[Solución alternativa 1](#)

[Solución alternativa 2](#)

[Solución alternativa 3](#)

[Proceso 5](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo resolver problemas de un mensaje de error común de Cisco Unity Connection en la página de facilidad de mantenimiento.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unity Connection (CUC)
- Administración de certificados para servidores unificados

### Componentes Utilizados

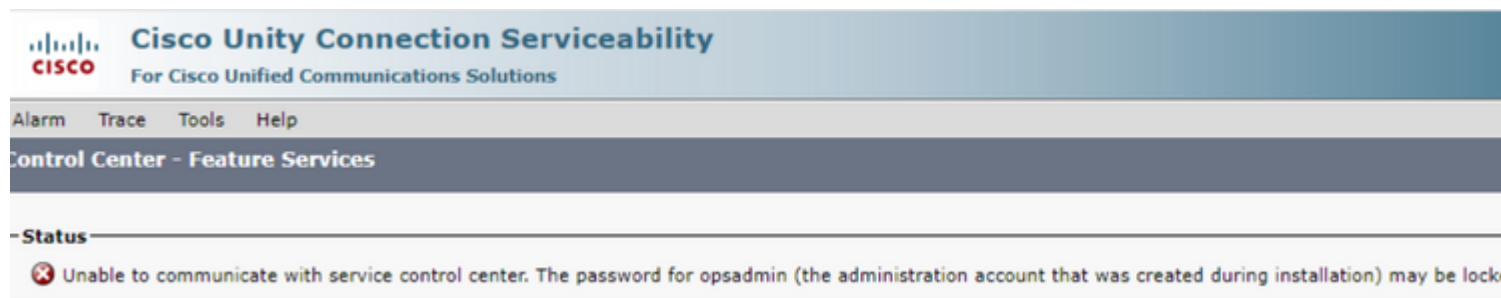
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

En Cisco Unity Connection, cuando se instala un nuevo nodo, se debe asignar un usuario y una contraseña, este usuario se crea y se almacena en la base de datos de Cisco Unity.

Este error aparece por diferentes motivos y hace imposible utilizar la página de nivel de servicio.



## Etapas para solucionar problemas

Para comenzar a solucionar el problema, primero debe ir al usuario administrador que se creó cuando se instaló Unity:

### Proceso 1

Vaya a **Administración de Cisco Unity Connection > Ir > Usuarios > Seleccionar usuario de administración > Editar > Configuración de contraseña**

Desmarque la casilla de verificación **Bloqueado por el administrador** para desbloquear la cuenta de usuario.

Marque la casilla de verificación **No caduca** para evitar que caduque la contraseña.

**Edit Password Settings (Web Application)**

User Edit Refresh Help

**Choose Password**

Web Application ▼

Save

**Web Applications Password Settings**

Locked by Administrator

User Cannot Change

User Must Change at Next Sign-In

Does Not Expire

Authentication Rule Recommended Web Application Authentication Rule ▼

Time Last Changed 7/12/22 10:32 AM

Failed Sign-In Attempts 0

Time of Last Failed Sign-In Attempt 6/14/23 5:49 PM

Time Locked by Administrator

Time Locked Due to Failed Sign-In Attempts

Unlock Password

Save

Haga clic en **Unlock Password** > Save.

Vaya a la página Serviciabilidad de Cisco Unity Connection.

## Proceso 2

Si el problema aún puede replicarse:

Vaya a **Administración de Cisco Unity Connection** > **Ir** > **Usuarios** > **Seleccione el usuario administrador** > **Editar** > **Cambiar contraseña** e ingrese una nueva contraseña.

Navegue hasta la página Serviciabilidad de Cisco Unity Connection y verifique si está accesible.

## Proceso 3

Si el problema continúa:

Vaya a **Administración de Cisco Unified OS** > **Ir** > **Seguridad** > **Administración de certificados** y verifique si los certificados Ipsec y Tomcat no han caducado.

Si los certificados han caducado, se deben volver a generar.

### Proceso de regeneración:

- Autofirmado:[proceso de regeneración de certificados autofirmados](#)
- CA -signed:[proceso de regeneración de certificado firmado por CA](#)

## Proceso 4

Si los certificados están firmados por CA, debe verificar si Cisco Unity Connection no coincide con el ID de bug de Cisco [CSCvp31528](#).

En caso de que Unity coincida, realice las siguientes soluciones alternativas:

### **Solución alternativa 1**

Pida a la CA que firme el certificado del servidor sin la extensión crítica del nombre alternativo del sujeto X509v3 y deje que otras extensiones permanezcan tal cual.

### **Solución alternativa 2**

Pida a la CA que firme el certificado de servidor y agregue la extensión especificada junto a para que funcione.

Restricciones básicas de X509v3: críticas

### **Solución alternativa 3**

Utilice certificados autofirmados; no siempre es la solución adecuada para todos.

### **Solución alternativa 4**

Como una de las últimas soluciones alternativas disponibles, actualice a la versión que contiene la solución del defecto y genere la CSR en la versión fija y consígala firmada por CA como se conoce con el proceso normal.

### **Proceso 5**

En CLI de CUC:

1. Recupere el objectID del usuario administrador de aplicaciones predeterminado de la base de datos de Unity Connection.

```
run cuc dbquery unitydirdb select name, value from vw_configuration where name='DefaultAdministrator'
```

### **Resultado del Comando:**

name	value
------	-------

```
-----
DefaultAdministrator XXXX-XXXX-XXXXX-XXXX
```

2. Recupere el alias asociado al objectID del administrador de aplicaciones predeterminado. En la consulta, reemplace el campo objectid='XXXX-XXXX-XXXXX-XXXX' por el valor del resultado anterior.

```
run cuc dbquery unitydirdb select alias,objectid from vw_user where objectid='XXXX-XXXX-XXXXX-XXXX'
```

### Resultado del Comando:

```
alias  objectid
-----
admin  XXXX-XXXX-XXXXX-XXXX
```

3. Confirme que el tipo de cifrado sea 4 para la autenticación Web del usuario administrador de aplicaciones predeterminado (el tipo de credencial 3 es para la contraseña de la aplicación Web).

```
run cuc dbquery unitydirdb select objectid, userobjectid, credentialtype, encryptiontype from tbl_creden
```

### Resultado del Comando:

objectid	userobjectid	credentialtype	encryptiontype
ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ	XXXX-XXXX-XXXXX-XXXX	3	4
TTTTT-TTTTT-TTTTT-TTTTT	XXXX-XXXX-XXXXX-XXXX	4	3

Si el tipo de encriptación = 3, cambie a 4.

```
run cuc dbquery unitydirdb update tbl_credential set encryptiontype = "4" where objectid = "ZZZZZ-ZZZZZ-
```

5. Se debe cambiar la contraseña porque la contraseña antigua tenía al usuario cifrado con el tipo 3

```
utils cuc reset password <accountalias>
```

6. Reinicie Tomcat mediante CLI

```
utils service restart Cisco Tomcat
```

Verifique si se puede acceder a la página de mantenimiento.

Si el problema es persistente, recopile los registros de Tomcat de CUC de RTMT.

Para ello:

1. Abra RTMT.
2. Inserte el nombre de host/IP de Cisco Unity Connection.
3. Inserte el usuario y la contraseña.
4. Haga doble **clic en Recopilar archivos**. Se abre la ventana Recopilar de archivos para seleccionar servicios/aplicaciones de UCM.
5. En Seleccionar servicios/aplicaciones de UCM, haga clic en la casilla de verificación en la columna Todos los servidores para:
  - Tomcat de Cisco

## Información Relacionada

- [Asistencia técnica y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).