Troubleshoot Error Message in Unity Connection in Serviceability

Contents

Introduction

This document describes how to troubleshoot a common Cisco Unity Connection error message on the serviceability page.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unity Connection (CUC)
- Certificate Management for Unified Servers

Components Used

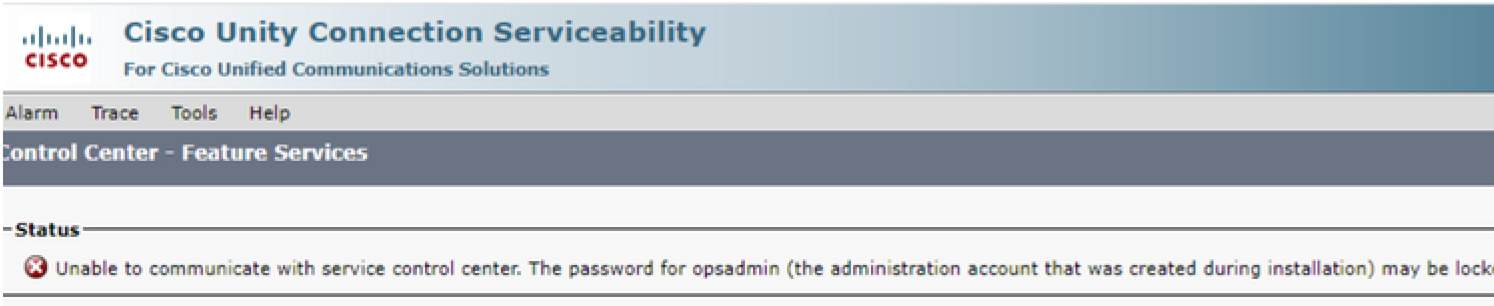
This document is not restricted to specific software and hardware versions.

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.

Background information

In Cisco Unity Connection when a new node is installed, a user and password must be assigned, this user is created and stored in the Cisco Unity database.

This error appears for different reasons, and makes it impossible to use the serviceability page.


Cisco Unity Connection Serviceability
For Cisco Unified Communications Solutions
Alarm
Trace
Tools
Help
Control Center - Feature Services
Status

Unable to communicate with service control center. The password for opsadmin (the administration account that was created during installation) may be lock

Stages to Troubleshoot

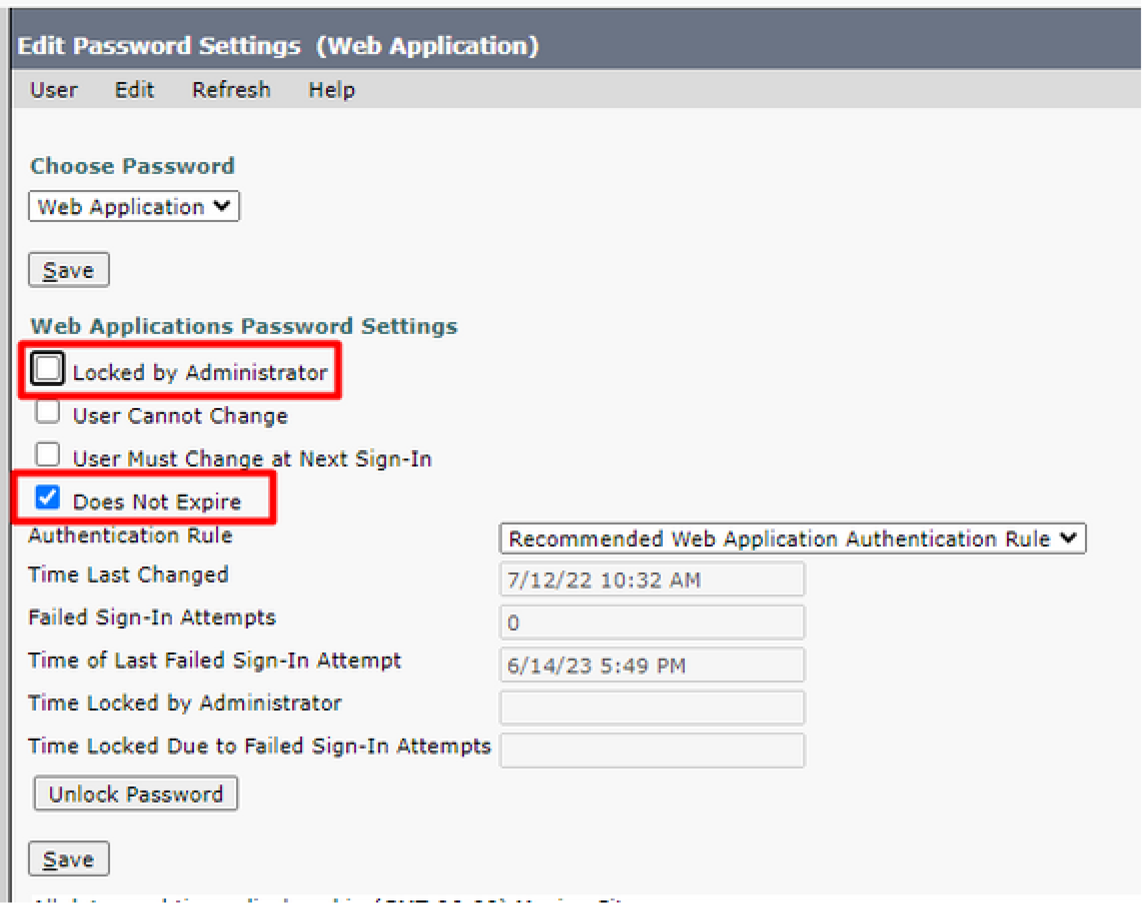
In order to start troubleshooting the issue, you first need to go to the administrator user that was created when Unity was installed:

Process 1

Navigate to **Cisco Unity Connection Administration** > **Go** > **Users** > **Select administration user** > **Edit** > **Password Settings**

Uncheck the **Locked by Administrator** check box to unlock the user account.

Check the **Does Not Expire** check box to avoid the password to expire.



Choose Password: Web Application

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	

Click on the **Unlock Password > Save**.

Navigate to the Cisco Unity Connection Serviceability page.

Process 2

If issue can still be replicated:

Navigate to **Cisco Unity Connection Administration > Go > Users > Select the administrator user > Edit > Change Password** and enter a new password.

Navigate to the Cisco Unity Connection Serviceability page and verify if it is accessible.

Process 3

If issue continues:

Navigate to **Cisco Unified OS Administration > Go > Security > Certificate Management** and verify if Ipsec and Tomcat certificates are not expired.

If certificates are expired, the certificates must be regenerated.

Regeneration process:

- Self-signed:Self signed certificate regeneration process
- CA -signed:CA signed certificate regeneration process

Process 4

If the certificates are CA signed, you need to verify if Cisco Unity Connection does not match with the Cisco bug ID CSCvp31528.

In case Unity matches, perform the next workarounds:

Workaround 1

Ask the CA to sign the server certificate without the critical extension of the X509v3 Subject Alternative Name and Let other extensions remain as it is.

Workaround 2

Ask the CA to sign the server certificate and add the extension specified next to make it work.
X509v3 Basic Constraints: critical

Workaround 3

Use Self Signed Certificates, it is not always the right solution for all.

Workaround 4

As one of the last workarounds available, upgrade to Release that contains the fix of the defect and Generate the CSR on fixed release and get it signed by CA as it is known with the Normal Process.

Process 5

On CUC CLI:

1. Retrieve the objectID of the default application administrator user from the Unity Connection database.

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

Command Output:

```
name                  value
--------------------  ------------------------------------
DefaultAdministrator  XXXX-XXXX-XXXXX-XXXX
```

2. Retrieve the alias associated with the default application administrator objectID. On query replace the field objectid='XXXX-XXXX-XXXXX-XXXX' with the value in the previous output.

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

Command Output:

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

3. Confirm the encryptiontype is 4 for web authentication for the default application administrator user (Credentialtype 3 is for web application password).

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

Command Output:

```
objectid                                userobjectid                        credentialtype encryptiontyp
------------------------------------   ------------------------------------ -------------- -------------
ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ                  XXXX-XXXX-XXXXX-XXXX                      3               4
TTTTT-TTTTT-TTTTT-TTTTT                  XXXX-XXXX-XXXXX-XXXX                      4               3
```

If encryption type = 3, change to 4.

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

5. Password must be changed because old password had the user encrypted with type 3

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

6. Restart Tomcat via CLI

```
utils service restart Cisco Tomcat
```

Verify if serviceability page is accessible.

If issue is persist collect CUC Tomcat logs from RTMT.

To do so:

1. Open RTMT.

2. Insert Cisco Unity Connection IP/Hostname.

3. Insert the user and password.

4. Double-click**Collect Files**. The Collect Files window opens to Select UCM Services/Applications.

5. In Select UCM Services/Applications, click the check box in the All Servers column for:

- Cisco Tomcat

Related Information

- **Cisco Technical Support & Downloads**