

Understand UCCE 12.5 Security Enhancements

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Verification of Downloaded ISO](#)

[Use Certificates with SHA-256 and Key Size 2048 Bits](#)

[SSLUtil Tool](#)

[DiagFwCertMgr Command](#)

[Data Protection Tool](#)

Introduction

This document describes about the latest Security enhancements added with Unified Contact Center Enterprise (UCCE) 12.5.

Prerequisites

- UCCE
- Open Secure Sockets Layer (SSL)

Requirements

Cisco recommends that you have knowledge of these topics:

- UCCE 12.5
- Open SSL

Components Used

The information in this document is based on these software and hardware versions:

- UCCE 12.5
- OpenSSL (64 bit) for windows

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

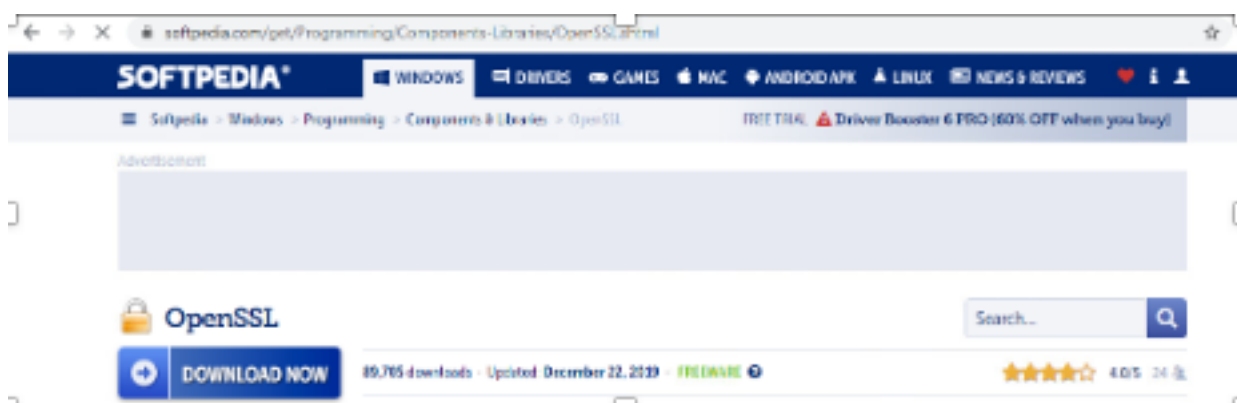
Cisco Security Control Framework (SCF) : The Collaboration Security Control Framework provides the design and implementation guidelines for building secure and reliable collaboration infrastructures. These infrastructures are resilient to both well-known and new forms of attacks. Reference [Security Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.5](#) .

As part of Cisco's SCF effort additional security enhancements are added for UCCE 12.5. This document outlines these enhancements.

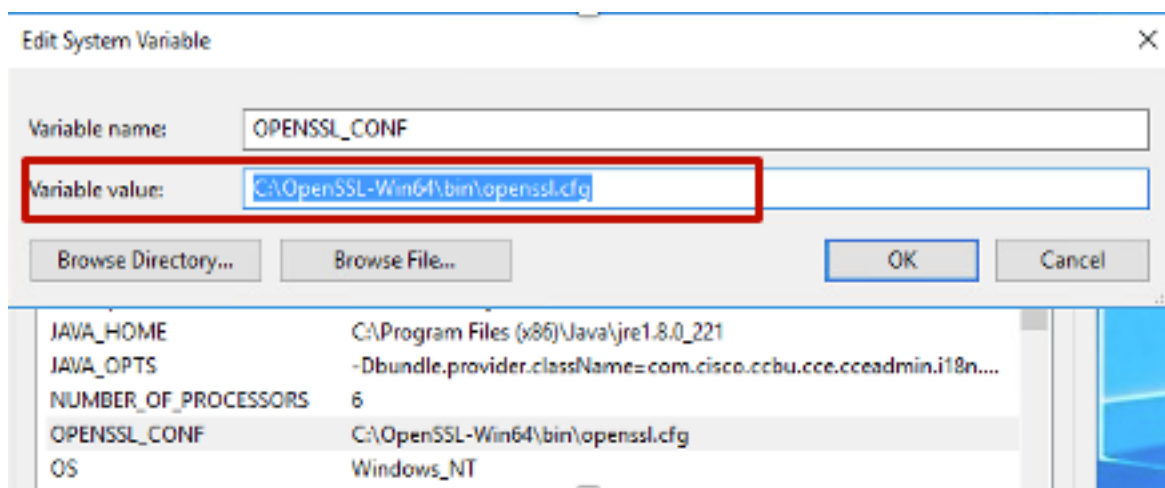
Verification of Downloaded ISO

In order to validate the downloaded ISO signed by Cisco as well as ensure that it is authorized, steps are:

1. Download and Install the OpenSSL. Search for software "openssl softpedia".



2. Confirm the path (this is set by default , but still good to verify). In Windows 10, goto System Properties, select Environment Variables.



3. Files needed for ISO verification

This PC > Local Disk (C:) > ISO

Name	Date modified	Type	Size
CCEInst1251	2/24/2020 2:31 PM	WinRAR archive	1,129,294 KB
CCEInst1251.iso.md5	2/24/2020 2:27 PM	MD5 File	1 KB
CCEInst1251.iso.signature	2/24/2020 2:27 PM	SIGNATURE File	1 KB
UCCEReleaseCodeSign_pubkey	2/24/2020 2:27 PM	Security Certificate	1 KB

4. Run the OpenSSL tool from command line.

```
C:\OpenSSL-Win64\bin>openssl
OpenSSL>
```

5. Run the command

```
dgst -sha512 -keyform der -verify <public Key.der> -signature <ISO image.iso.signature> <ISO Image>
```

6. In the event of failure, command line shows error as shown in the image

```
OpenSSL> dgst -sha512 -keyform der -verify c:\iso\UCCEReleaseCodeSign_pubkey.der -signature c:\iso\CCEInst1251.iso.signature c:\iso\CCEInst1251.iso
Verification Failure
error in dgst
OpenSSL>
```

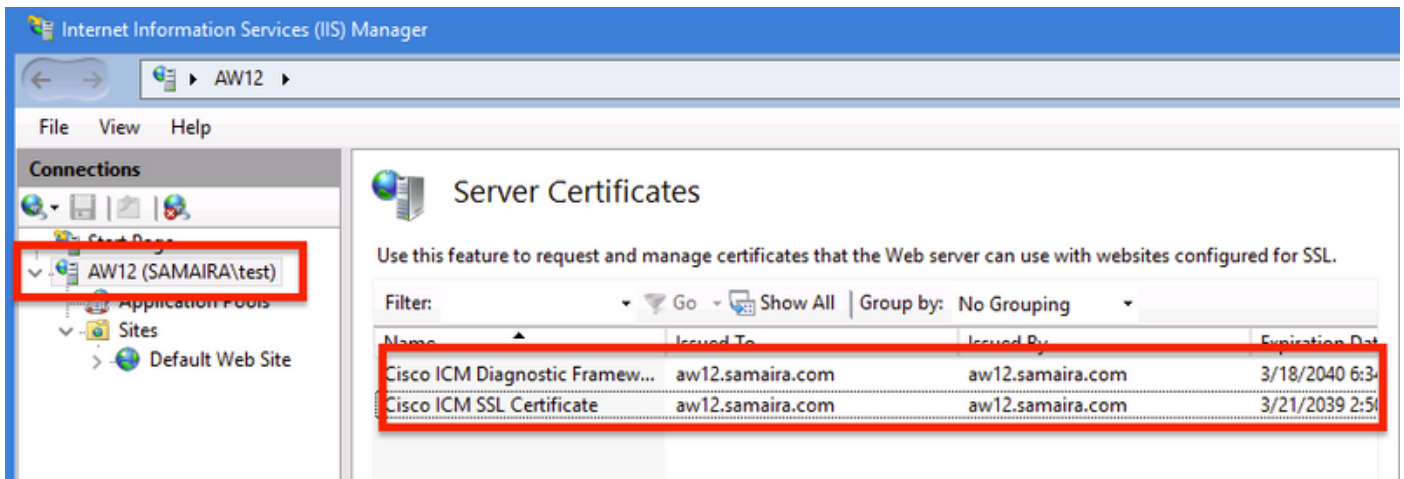
Use Certificates with SHA-256 and Key Size 2048 Bits

Logs report error in the event of identifying non-complaint certificates (i.e not meeting the SHA-256 and/or keysize 2048 bits requirement.)

There are two important certificates from UCCE's perspective:

- Cisco ICM Diagnostic Framework service certificate
- Cisco ICM SSL Certificate

The certificates can be reviewed in the Internet Information Services (IIS) Manager option of windows server.

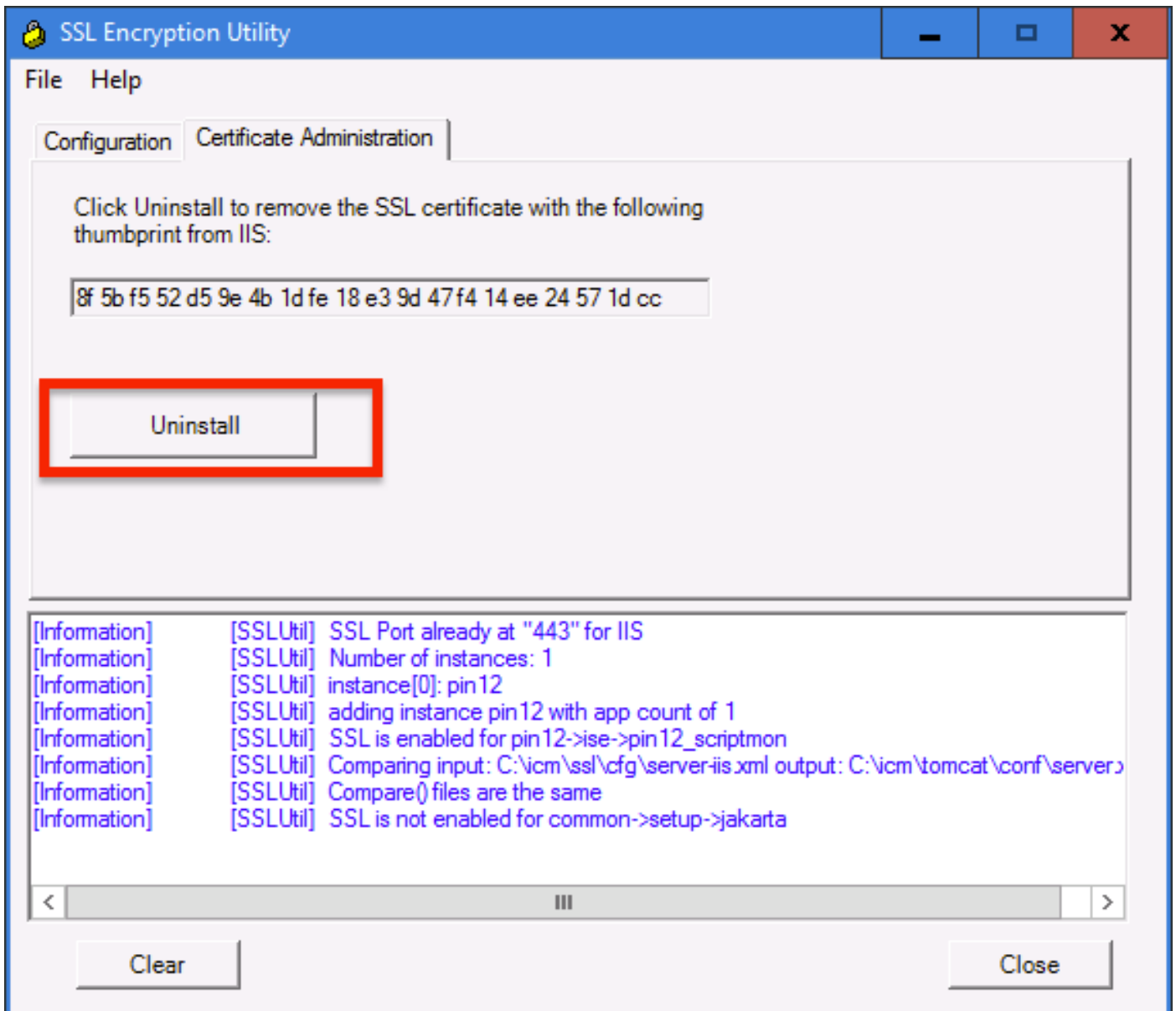


For Self-signed certificates (either for Diagnose Portico or Web Setup) , error line reported is:

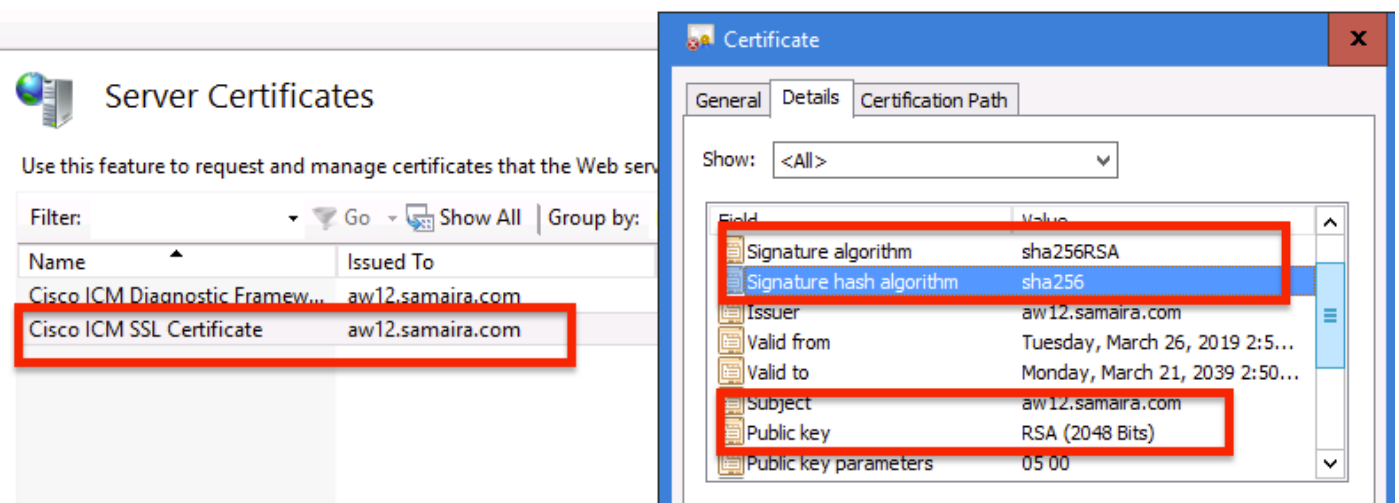
Re-generating Cisco ICM SSL Certificate with SHA-256 and key size '2048' and will be binded with port 443.

SSLUtil Tool

- a. In order to regenerate self-signed certificates (for WebSetup/CCEAdmin page) use SSLUtil tool (from location C:\icm\bin).
- b. Select Uninstall to delete the current "Cisco ICM SSL Certificate".



c. Next select Install in SSLUtil tool and once the process completes , notice the certificate created now include SHA-256 and keysize '2048' bits.



DiagFwCertMgr Command

In order to regenerate a self-signed certificate for Cisco ICM Diagnostic Framework service

certificate, use command line "**DiagFwCertMgr**", as shown in the image:

```
C:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:CreateAndBindCert
*****
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
*****
Executing Task: 'CreateAndBindCert'

Deleted old binding successfully
Binding new certificate with HTTP service completed successfully
Found existing registry key for the service
Hash of certificate used saved in the service registry
ALL TASKS FOR BINDING THE CERTIFICATE WITH HTTP SERVICE COMPLETED SUCCESSFULLY

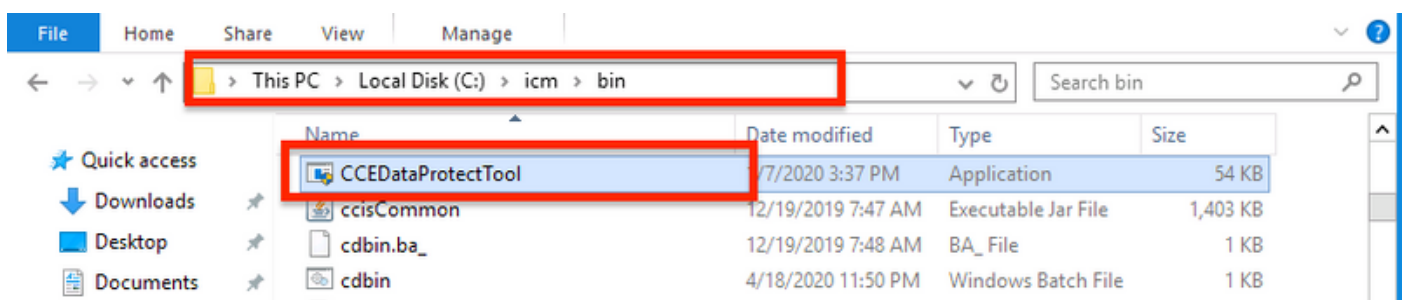
C:\icm\serviceability\diagnostics\bin>_
```

Data Protection Tool

1. CCEDDataProtectTool is used to encrypt and decrypt sensitive information that the Windows registry stores in it. Post upgrade to SQL 12.5 , value store in the **SQLLogin** registry need to be reconfigured with CCEDDataProtectTool. Only administrator, domain user with administrative rights, or a local administrator can run this tool.
2. This tool can be used to view, configure, edit, remove encrypted value store in **SQLLogin** registry.
3. Tool is found in location;

<Install Directory>:\icm\bin\CCEDDataProtectTool.exe

4. Navigate to location and double click CCEDDataProtectTool.exe.



5. In order to encrypt , press 1 for DBLookup, enter Instance Name. Next, press 2 to select "Edit and Encrypt"

```
C:\icm\bin\CCEDDataProtectTool.exe
CCEDDataProtectTool supports Encryption/Decryption of sensitive information in Windows Registry.
Main Menu:
Select one of the below options
1. DBLookup ← 2. Rekey          3. Help          4. Exit
1
Enter Instance Name:
cc125
Select one of the below options for DBLookup Registry
1. Decrypt and View          2. Edit and Encrypt ← 3. Help          4. Exit
2
Fetching / Decryption failed, Refer the C:\temp\CCEDDataProtect.log for more Details
Enter New Registry Value:
[Redacted]
Are you sure you want to Edit the Registry Details [Y/N]
Y
Registry Updated with Encrypted Data Successfully.
Select one of the below options for DBLookup Registry
1. Decrypt and View          2. Edit and Encrypt          3. Help          4. Exit
```

6. Navigate to registry location and review String Value **SQLLogin** looks blank , as shown in the image :

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\pin12\RouterA\Router\CurrentVersion\Configuration\Database

Name	Type	Data
(Default)	REG_SZ	(value not set)
AbandonTimeout	REG_DWORD	0x00001388 (5000)
SQLLogin	REG_SZ	
Threads	REG_DWORD	0x00000005 (5)
Timeout	REG_DWORD	0x0000015e (350)

Edit String dialog box showing Value name: SQLLogin and Value data: [Redacted]

7. In case of need to review the encrypted value; while command line of CCEDDataProtectTool , select press 1 for "Decrypt and View", as shown in the image;

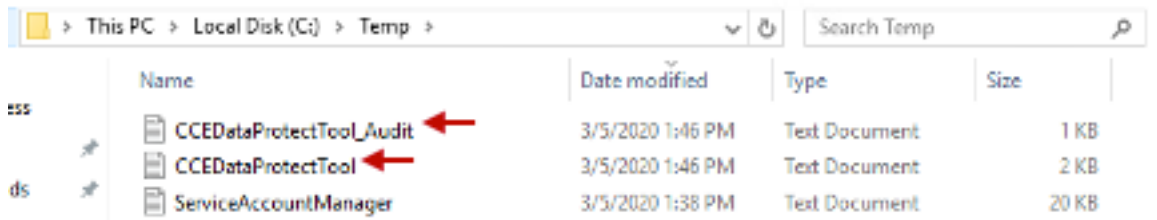
```
Select one of the below options for DBLookup Registry
1. Decrypt and View ← 2. Edit and Encrypt 3. Help 4. Exit
1
████████████████████████████████████████████████████████████████████████████████
```

8. Any logs for this tool can be found in location;

<Install Directory>:\temp

Audit logs filename : CCEDDataProtectTool_Audit

CCEDDataProtectTool logs : CCEDDataProtectTool



The screenshot shows a Windows File Explorer window with the address bar set to 'This PC > Local Disk (C:) > Temp >'. The search bar contains 'Search Temp'. The main area displays a table of files:

Name	Date modified	Type	Size
CCEDDataProtectTool_Audit	3/5/2020 1:46 PM	Text Document	1 KB
CCEDDataProtectTool	3/5/2020 1:46 PM	Text Document	2 KB
ServiceAccountManager	3/5/2020 1:38 PM	Text Document	20 KB

Red arrows point to the 'CCEDDataProtectTool_Audit' and 'CCEDDataProtectTool' files.