

# Introducción a las mejoras de seguridad de UCCE 12.5

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Verificación de ISO descargado](#)

[Utilizar certificados con bits SHA-256 y tamaño de clave 2048](#)

[Herramienta SSLUtil](#)

[Comando DiagFwCertMgr](#)

[Herramienta de protección de datos](#)

## Introducción

Este documento describe las últimas mejoras de seguridad añadidas con Unified Contact Center Enterprise (UCCE) 12.5.

## Prerequisites

- UCCE
- Capa de sockets seguros abierta (SSL)

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCCE 12.5
- Open SSL

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- UCCE 12.5
- OpenSSL (64 bits) para 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Antecedentes

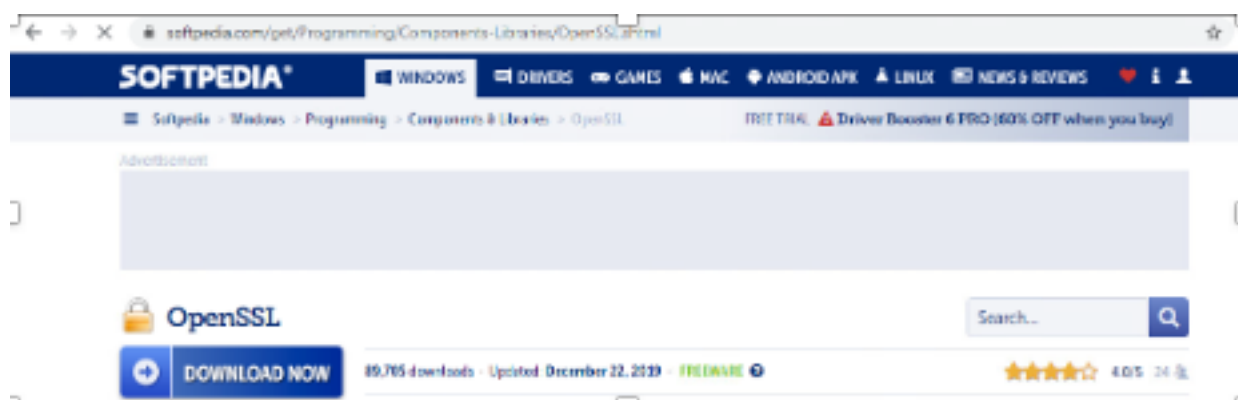
Marco de control de seguridad de Cisco (SCF): El marco de control de seguridad de colaboración proporciona las directrices de diseño e implementación para crear infraestructuras de colaboración seguras y fiables. Estas infraestructuras son resistentes a las formas de ataque conocidas y nuevas. [Guía de seguridad de referencia para Cisco Unified ICM/Contact Center Enterprise, versión 12.5](#).

Como parte del esfuerzo de SCF de Cisco, se añaden mejoras de seguridad adicionales para UCCE 12.5. Este documento describe estas mejoras.

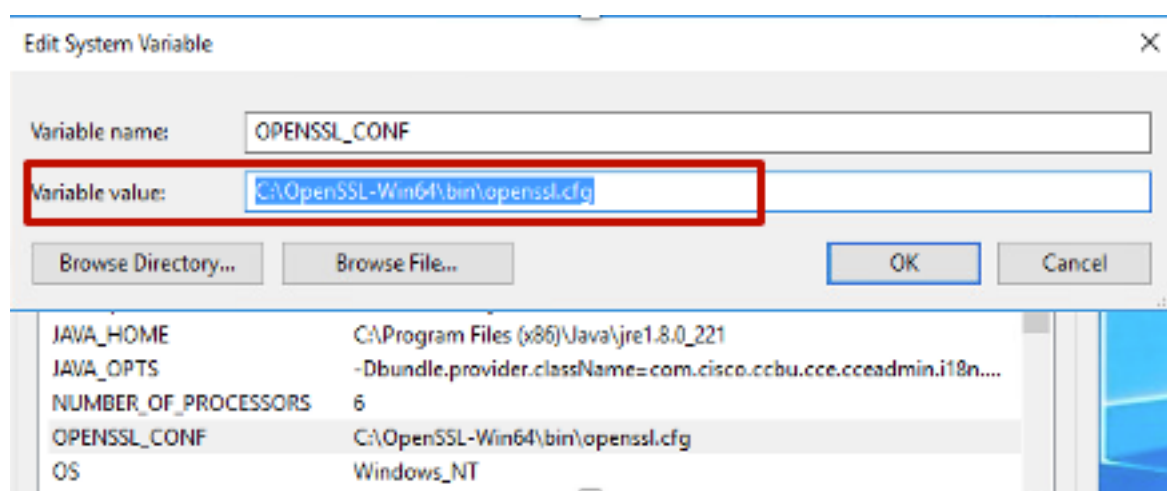
## Verificación de ISO descargado

Para validar la ISO descargada firmada por Cisco y asegurarse de que está autorizada, los pasos son:

1. Descargue e instale OpenSSL. Busque software "openssl softpedia".



2. Confirme la ruta (se establece de forma predeterminada, pero sigue siendo buena para verificar). En Windows 10, vaya a Propiedades del sistema, seleccione Variables de entorno.



3. Archivos necesarios para la verificación 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. Ejecute la herramienta OpenSSL desde la línea de comandos.

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

5. Ejecute el comando

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

6. En caso de error, la línea de comandos muestra el error como se muestra en la imagen

```
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>
```

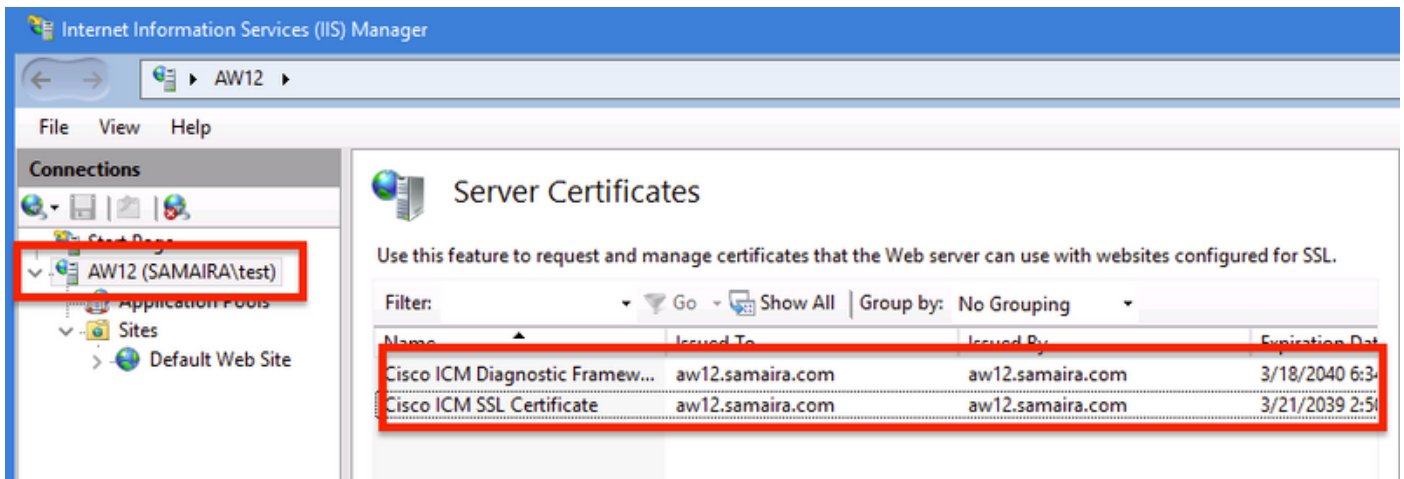
## Utilizar certificados con bits SHA-256 y tamaño de clave 2048

Los registros informan de un error en el caso de identificar certificados que no son de queja (es decir, no cumplen con el requisito SHA-256 y/o tamaño de clave 2048 bits).

Hay dos certificados importantes desde la perspectiva de UCCE:

- Certificado de servicio de Cisco ICM Diagnostic Framework
- Certificado Cisco ICM SSL

Los certificados se pueden revisar en la opción Administrador de Internet Information Services (IIS) del servidor de Windows.

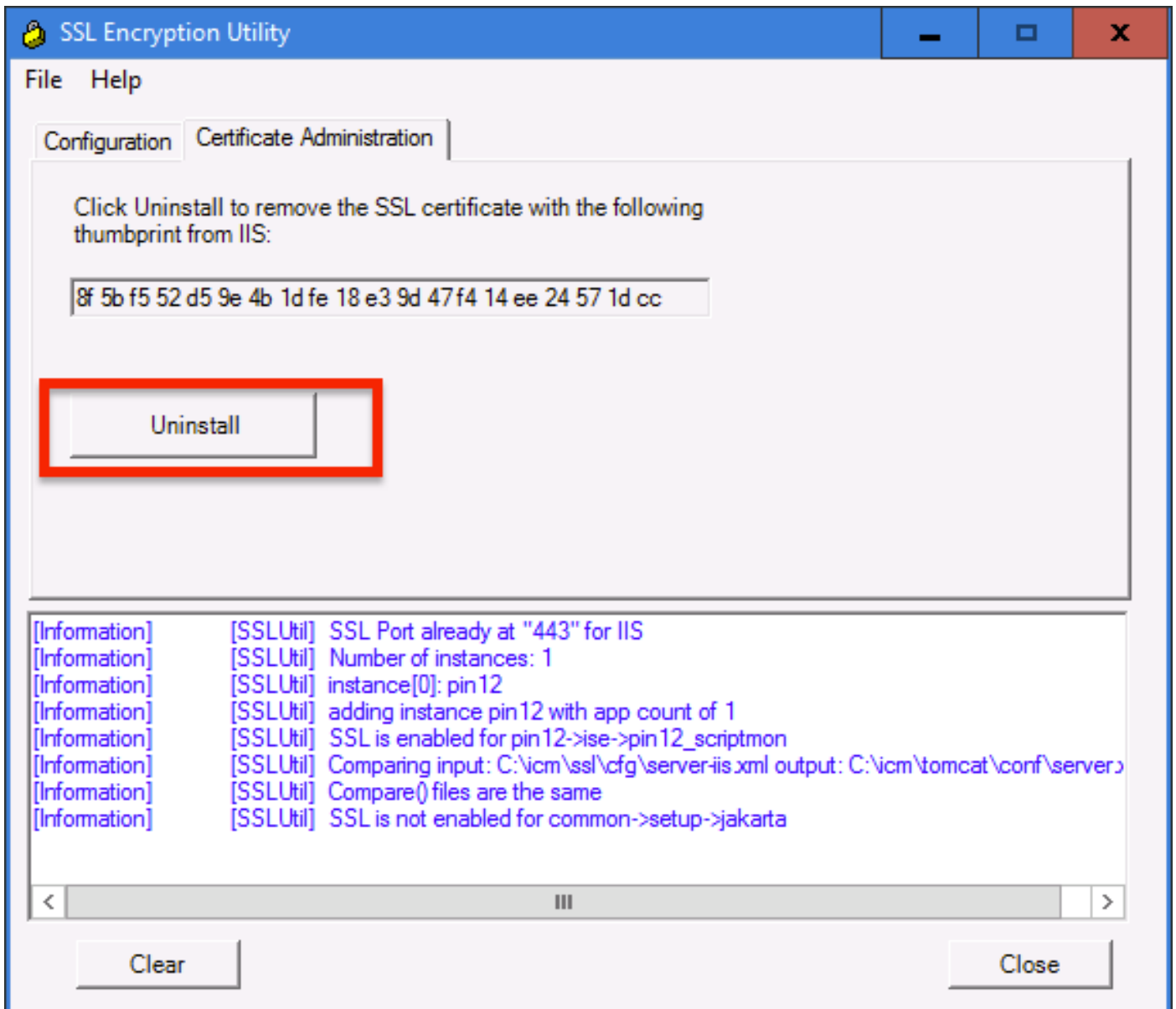


Para los certificados autofirmados (ya sea para Diagnose Portico o Web Setup) , la línea de error informada es:

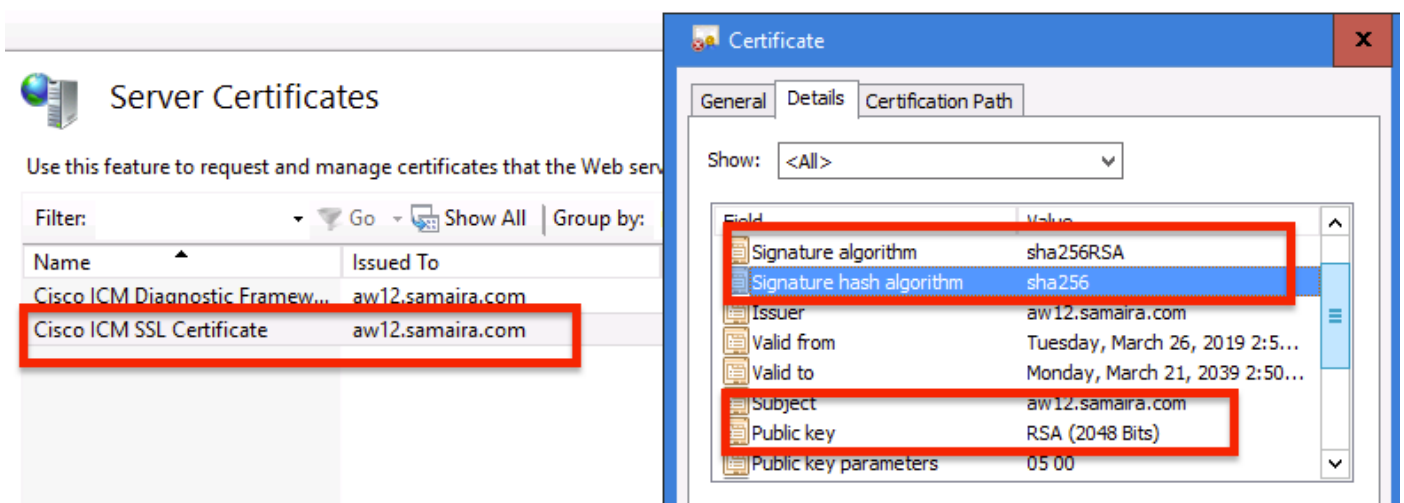
Re-generating Cisco ICM SSL Certificate with SHA-256 and key size '2048' and will be binded with port 443.

## Herramienta SSLUtil

- a. Para regenerar certificados autofirmados (para la página WebSetup/CCEAdmin), utilice la herramienta SSLUtil (desde la ubicación C:\icm\bin).
- b. Seleccione Uninstall (Desinstalar) para eliminar el "Cisco ICM SSL Certificate" actual.



c. A continuación, seleccione Install in SSLUtil tool y, una vez que el proceso haya finalizado, observe que el certificado creado ahora incluye los bits SHA-256 y el tamaño de clave '2048'.



## Comando DiagFwCertMgr

Para regenerar un certificado autofirmado para el certificado de servicio de Cisco ICM Diagnostic

Framework, utilice la línea de comandos "DiagFwCertMgr", como se muestra en la imagen:

```
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>_
```

## Herramienta de protección de datos

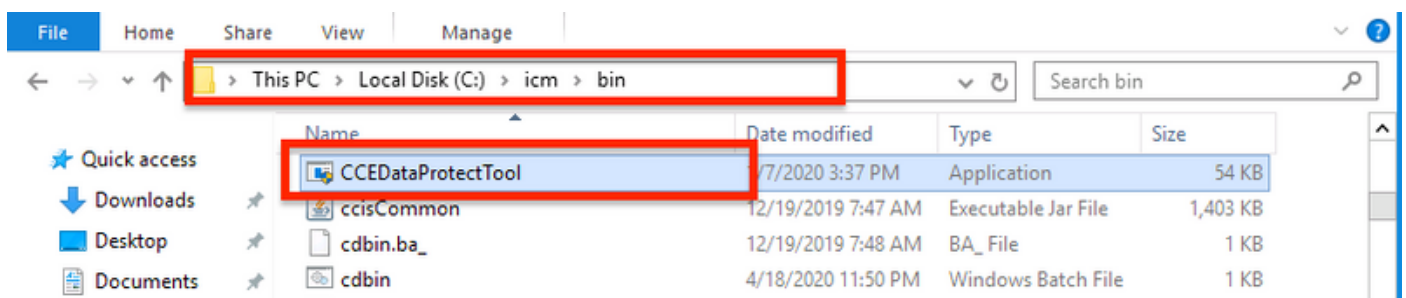
1. CCEDDataProtectTool se utiliza para cifrar y descifrar la información confidencial que almacena el Registro de Windows en él. Después de actualizar a SQL 12.5 , el almacén de valores en el registro **SQLLogin** debe reconfigurarse con CCEDDataProtectTool. Sólo el administrador, el usuario de dominio con derechos administrativos o un administrador local pueden ejecutar esta herramienta.

2. Esta herramienta se puede utilizar para ver, configurar, editar, eliminar el almacén de valores cifrado en el registro **SQLLogin**.

3. La herramienta se encuentra en la ubicación;

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

4. Desplácese hasta la ubicación y haga doble clic en CCEDDataProtectTool.exe.



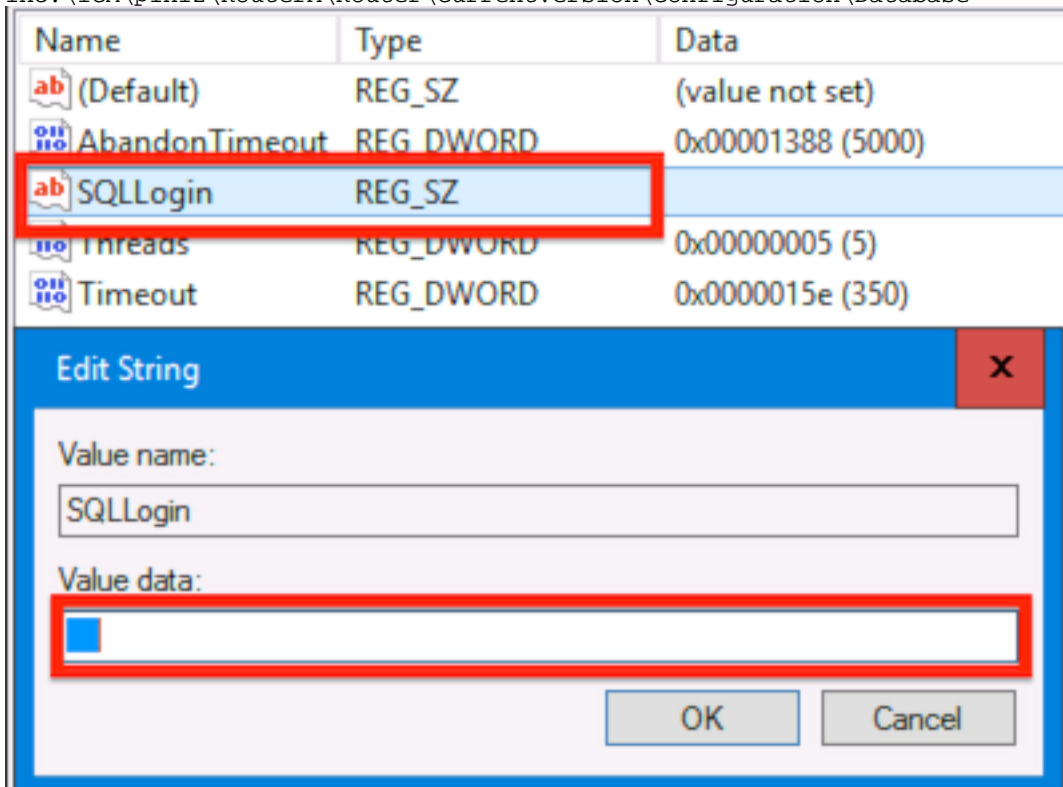
5. Para cifrar , presione 1 para DBLookup, ingrese Instance Name . A continuación, pulse 2 para seleccionar "Editar y cifrar"

```
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. Navegue hasta la ubicación del Registro y revise el aspecto en blanco del valor de cadena SQLLogin , como se muestra en la imagen :

HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\pin12\RouterA\Router\CurrentVersion\Configuration\Database



7. En caso de necesidad de revisar el valor cifrado; mientras que la línea de comandos de CCEDDataProtectTool , seleccione pulsar 1 para "Descifrar y ver", como se muestra en la imagen;

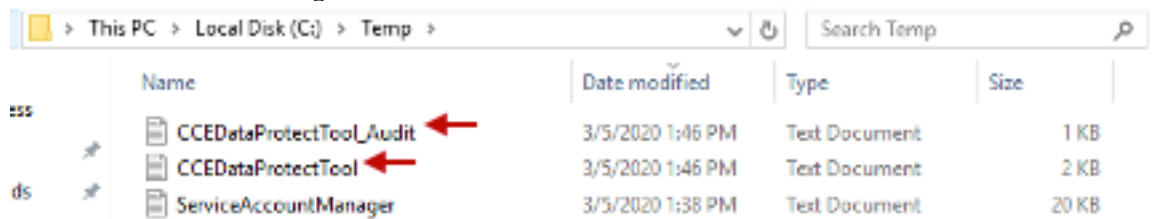
```
Select one of the below options for DBLookup Registry
1. Decrypt and View ← 2. Edit and Encrypt 3. Help 4. Exit
1
████████████████████████████████████████████████████████████████████████████████
```

8. Los registros de esta herramienta se pueden encontrar en la ubicación;

<Install Directory>:\temp

Audit logs filename : CCEDataProtectTool\_Audit

CCEDataProtectTool logs : CCEDataProtectTool



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
sss	CCEDataProtectTool_Audit ←	3/5/2020 1:46 PM	Text Document	1 KB
	CCEDataProtectTool ←	3/5/2020 1:46 PM	Text Document	2 KB
ds	ServiceAccountManager	3/5/2020 1:38 PM	Text Document	20 KB