

瞭解UCCE 12.5安全增強功能

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[驗證下載的ISO](#)

[使用SHA-256和金鑰大小2048位的證書](#)

[SSLUtil工具](#)

[DiagFwCertMgr命令](#)

[資料保護工具](#)

簡介

本檔案介紹整合客服中心企業版(UCCE)12.5新增的最新安全增強功能。

必要條件

- UCCE
- 開放式安全套接字層(SSL)

需求

思科建議您瞭解以下主題：

- UCCE 12.5
- 開啟SSL

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- UCCE 12.5
- Windows版OpenSSL (64位)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

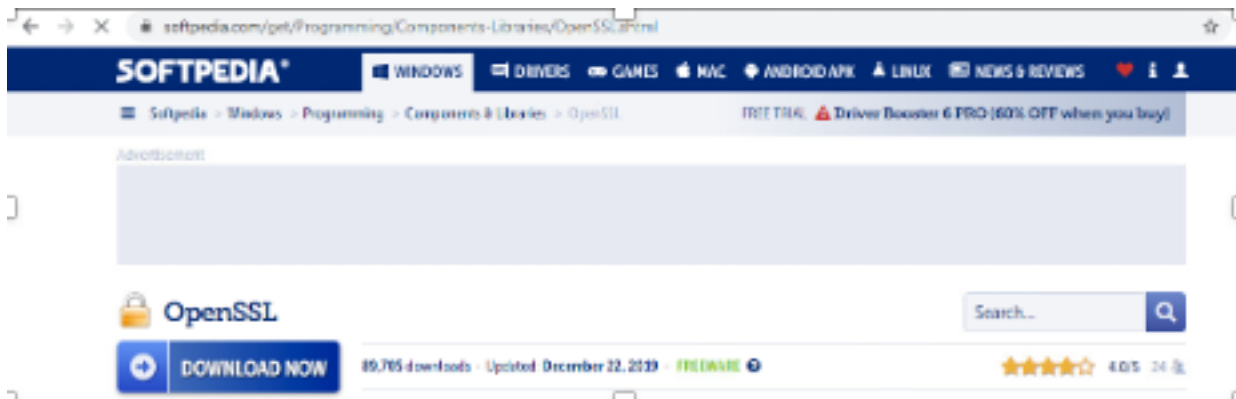
思科安全控制架構(SCF):合作安全控制框架為構建安全可靠的合作基礎設施提供了設計和實施指南。這些基礎設施可抵禦眾所周知和新形式的攻擊。Cisco [Unified ICM/Contact Center Enterprise參考安全指南，版本12.5](#)。

作為思科SCF工作的一部分，為UCCE 12.5新增其他安全增強功能。本文檔概述了這些增強功能。

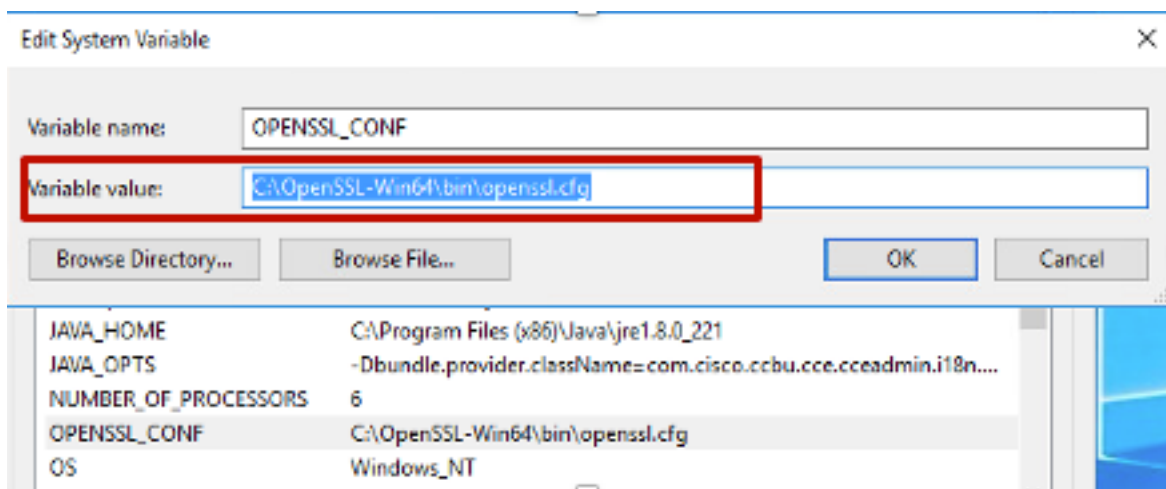
驗證下載的ISO

為了驗證由思科簽署的已下載ISO並確保其獲得授權，請執行以下步驟：

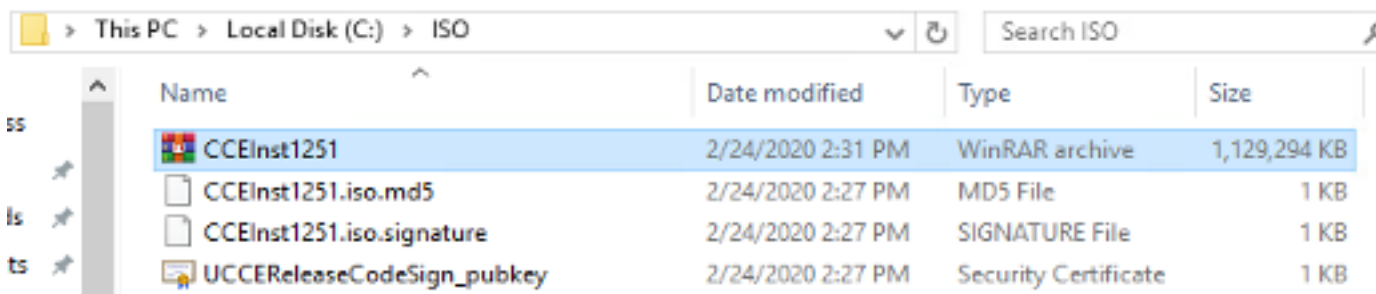
1. 下載並安裝OpenSSL。搜尋軟體「openssl softpedia」。



2. 確認路徑（預設情況下已設定，但仍可用於驗證）。在Windows 10中，轉至「系統屬性」，選擇「環境變數」。



3. ISO驗證所需的檔案



4. 從命令列運行OpenSSL工具。

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

5. 執行命令

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

6. 如果失敗，命令列會顯示錯誤，如下圖所示

```
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>
```

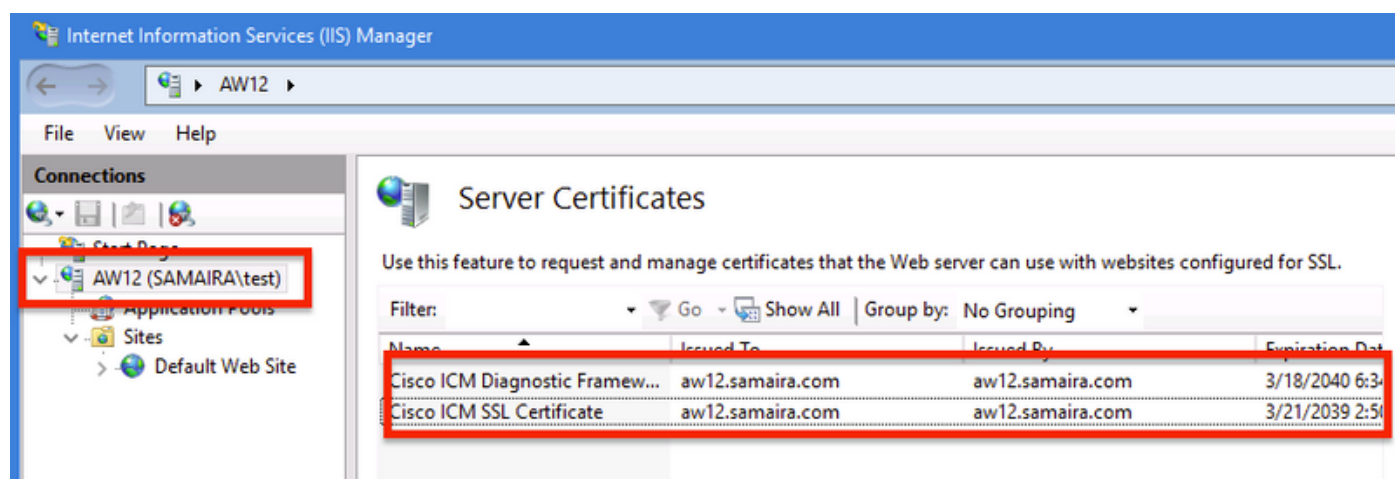
使用SHA-256和金鑰大小2048位的證書

日誌會報告識別非投訴證書時的錯誤（即不符合SHA-256和/或keysize 2048位的要求）。

從UCCE的角度來看，有兩個重要證書：

- Cisco ICM診斷框架服務證書
- Cisco ICM SSL憑證

可以在Windows伺服器的Internet資訊服務(IIS)管理器選項中檢視證書。



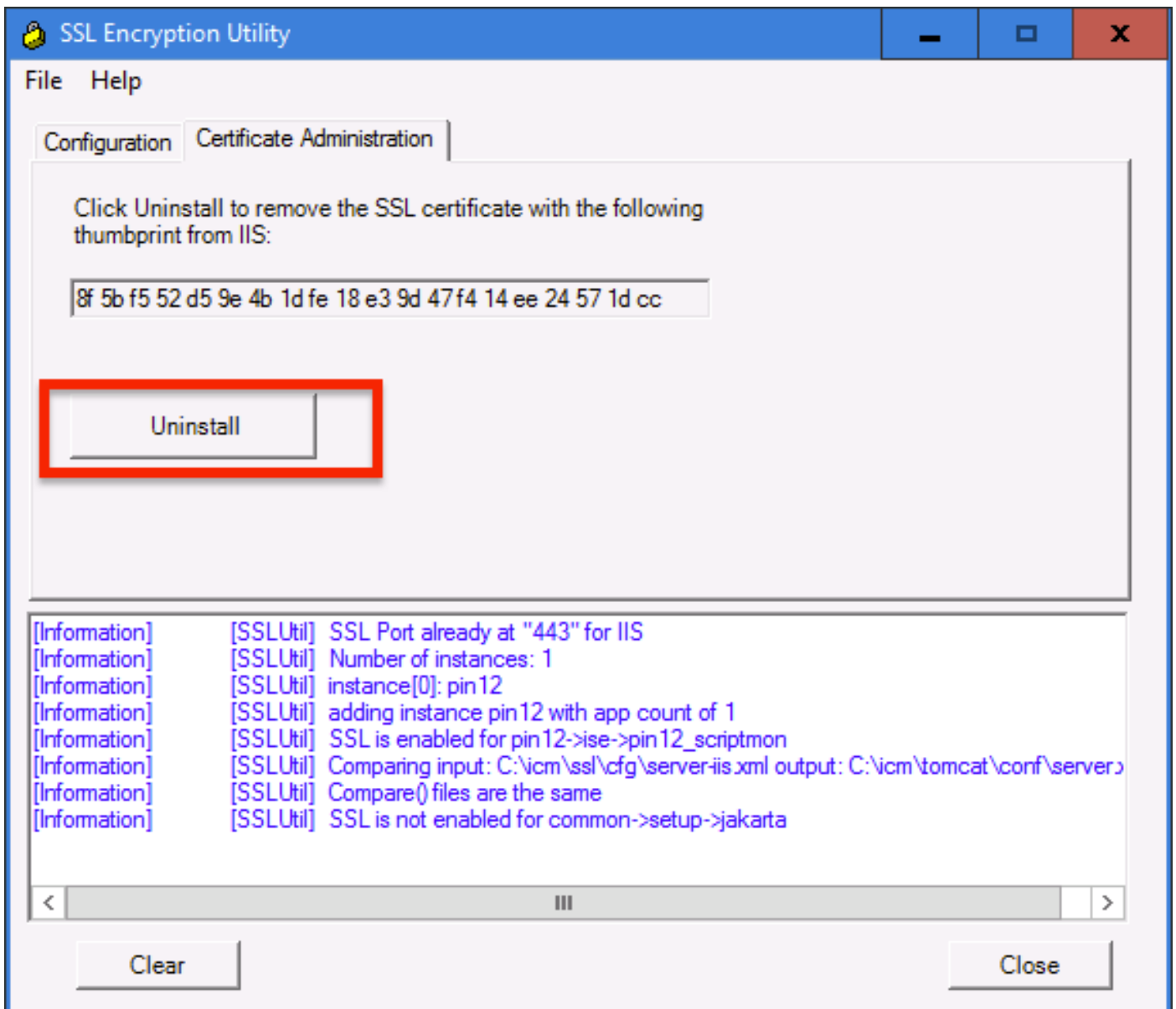
對於自簽名證書（用於診斷門戶或Web設定），報告的錯誤行為：

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

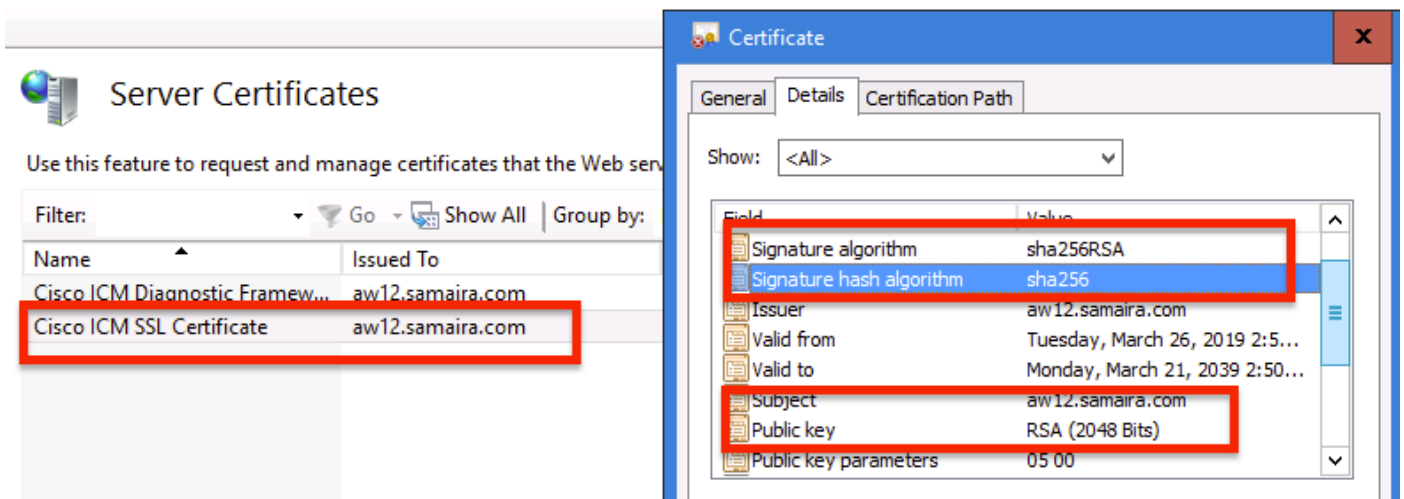
SSLUtil工具

a. 若要重新生成自簽名證書（對於WebSetup/CCEAdmin頁），請使用SSLUtil工具（從位置C:\icm\bin獲取）。

b.選擇Uninstall刪除當前的「Cisco ICM SSL Certificate」。



c.接下來選擇「安裝在SSLUtil工具中」，在過程完成之後，請注意現在建立的證書包括SHA-256和keysize '2048'位。



DiagFwCertMgr命令

若要為Cisco ICM診斷框架服務證書重新生成自簽名證書，請使用命令列「DiagFwCertMgr」，如下圖所示：

```
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

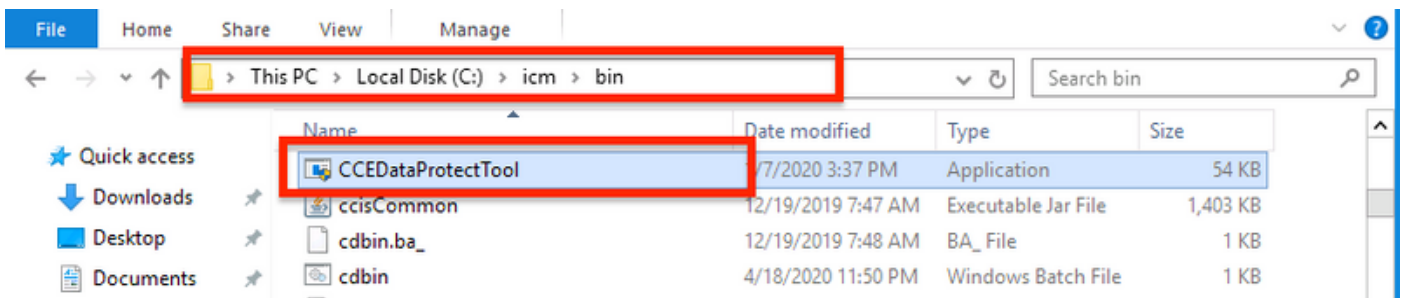
C:\icm\serviceability\diagnostics\bin>
```

資料保護工具

1. CCEDDataProtectTool用於加密和解密Windows登錄檔儲存在其中的敏感資訊。升級到SQL 12.5後，需要使用CCEDDataProtectTool重新配置SQLLogin註冊表中儲存的值。只有管理員、具有管理許可權的域使用者或本地管理員可以運行此工具。
- 2.此工具可用於檢視、配置、編輯、刪除SQLLogin登錄檔中的加密值儲存。
- 3.在位置找到工具；

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

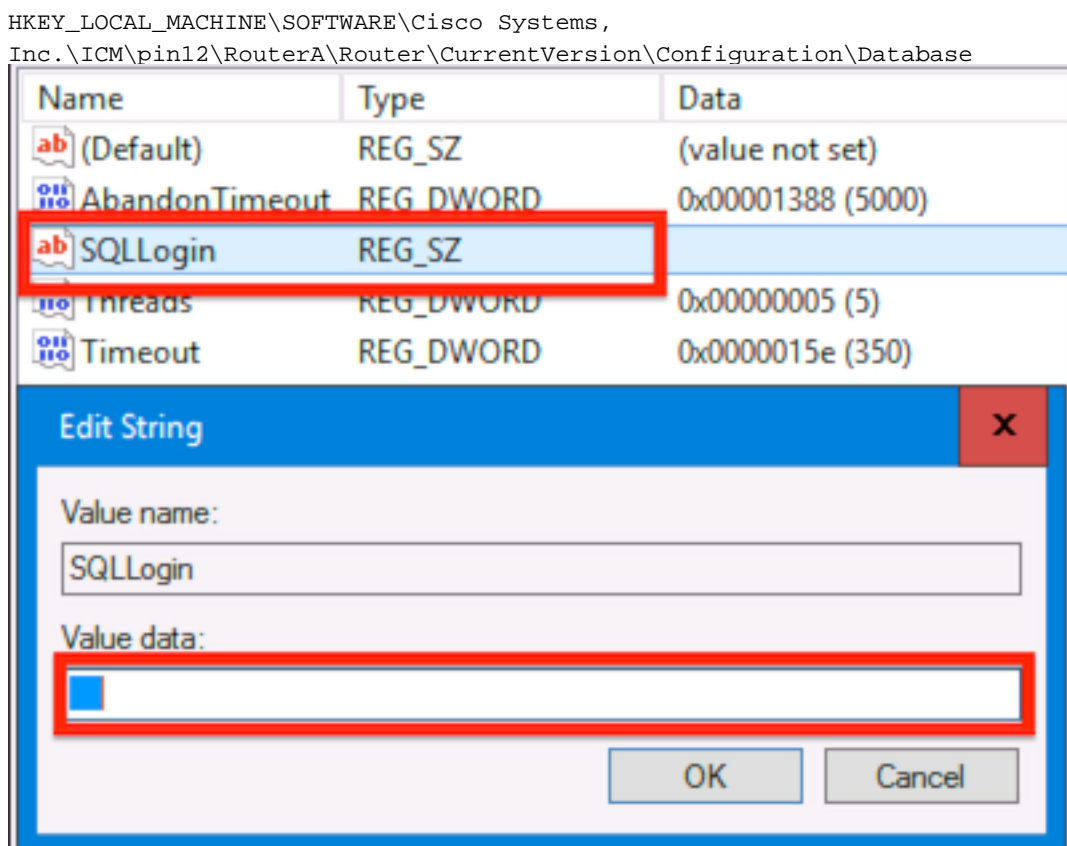
4.導航到位置，然後按兩下CCEDDataProtectTool.exe。



5.若要加密，請按1對DBLookup，請輸入例項名稱。接下來，按2選擇「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. 導航至登錄檔位置並檢視字串值SQLLogin顯示為空白，如下圖所示：



7. 在需要檢查加密值的情況下；在CCEDDataProtectTool的命令列中，選擇「Decrypt and View」（解密和檢視）按1，如下圖所示；

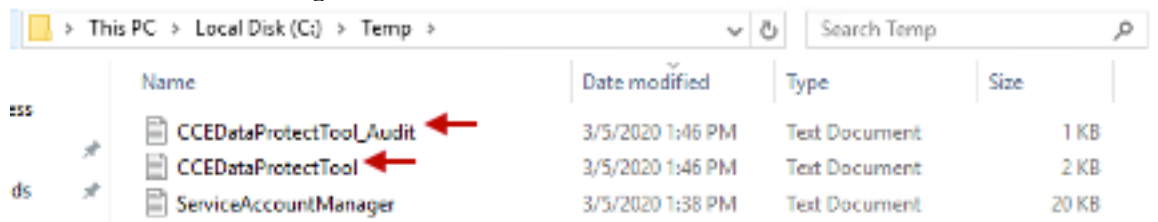
```
Select one of the below options for DBLookup Registry
1. Decrypt and View ← 2. Edit and Encrypt          3. Help          4. Exit
1
[Redacted]
```

8.在位置可以找到此工具的任何日誌;

<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 with columns for Name, Date modified, Type, and Size. Two files are highlighted with red arrows: 'CCEDataProtectTool_Audit' and 'CCEDataProtectTool'.

	Name	Date modified	Type	Size
ESS	CCEDataProtectTool_Audit	3/5/2020 1:46 PM	Text Document	1 KB
ds	CCEDataProtectTool	3/5/2020 1:46 PM	Text Document	2 KB
	ServiceAccountManager	3/5/2020 1:38 PM	Text Document	20 KB