

UCCE 12.5-Sicherheitsverbesserungen

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Überprüfung heruntergeladener ISO](#)

[Zertifikate mit SHA-256 und Schlüsselgröße 2048 Bit verwenden](#)

[SSLUtil-Tool](#)

[DiagFwCertMgr-Befehl](#)

[Datenschutz-Tool](#)

Einführung

In diesem Dokument werden die neuesten Sicherheitsverbesserungen beschrieben, die mit Unified Contact Center Enterprise (UCCE) 12.5 hinzugefügt wurden.

Voraussetzungen

- UCCE
- Open Secure Sockets Layer (SSL)

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- UCCE 12,5
- SSL öffnen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- UCCE 12,5
- OpenSSL (64 Bit) für Fenster

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

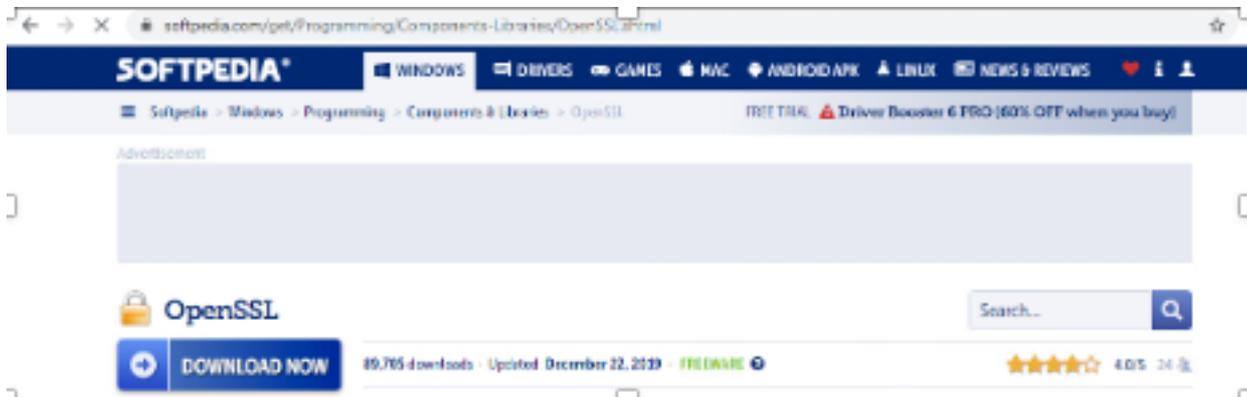
Cisco Security Control Framework (SCF): Das Collaboration Security Control Framework enthält Design- und Implementierungsrichtlinien für den Aufbau einer sicheren und zuverlässigen Collaboration-Infrastruktur. Diese Infrastrukturen sind sowohl für bekannte als auch für neue Angriffsformen ausfallsicher. Referenz [Security Guide for Cisco Unified ICM/Contact Center Enterprise, Version 12.5](#).

Im Rahmen des SCF-Projekts von Cisco wurden zusätzliche Sicherheitsverbesserungen für UCCE 12.5 hinzugefügt. In diesem Dokument werden diese Verbesserungen beschrieben.

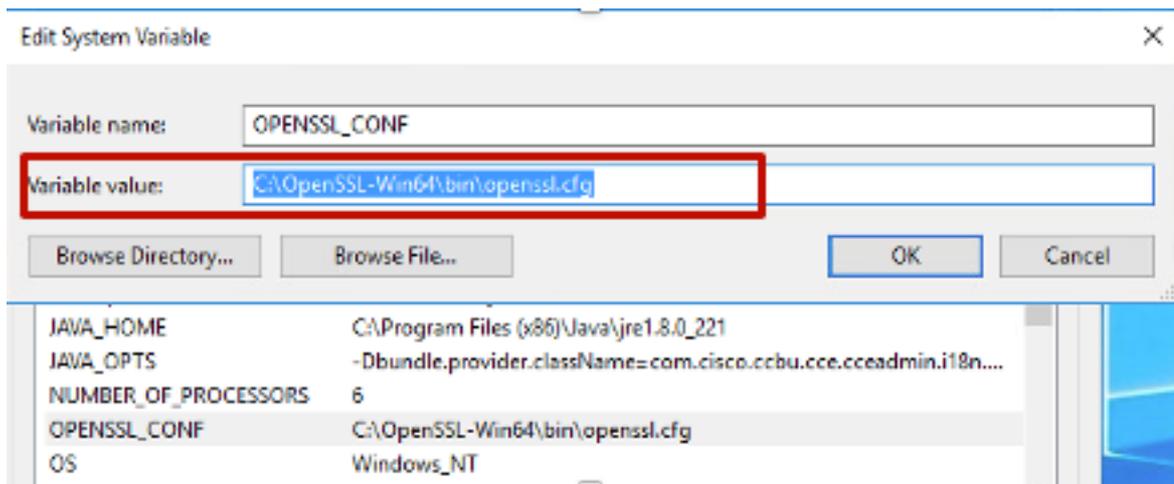
Überprüfung heruntergeladener ISO

Um die heruntergeladene ISO-Zertifizierung, die von Cisco signiert wurde, zu validieren und sicherzustellen, dass sie autorisiert ist, gehen Sie wie folgt vor:

1. Laden Sie OpenSSL herunter, und installieren Sie es. Suchen Sie nach Software "openssl softpedia".



2. Bestätigen Sie den Pfad (dieser ist standardmäßig festgelegt, aber noch gut zu überprüfen). Wählen Sie in Windows 10 unter Systemeigenschaften die Option Umgebungsvariablen aus.



3. Für die ISO-Verifizierung benötigte Dateien

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. Führen Sie das OpenSSL-Tool über die Befehlszeile aus.

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

5. Führen Sie den Befehl aus

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

6. Bei einem Ausfall zeigt die Befehlszeile einen Fehler an, wie im Bild gezeigt.

```
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>
```

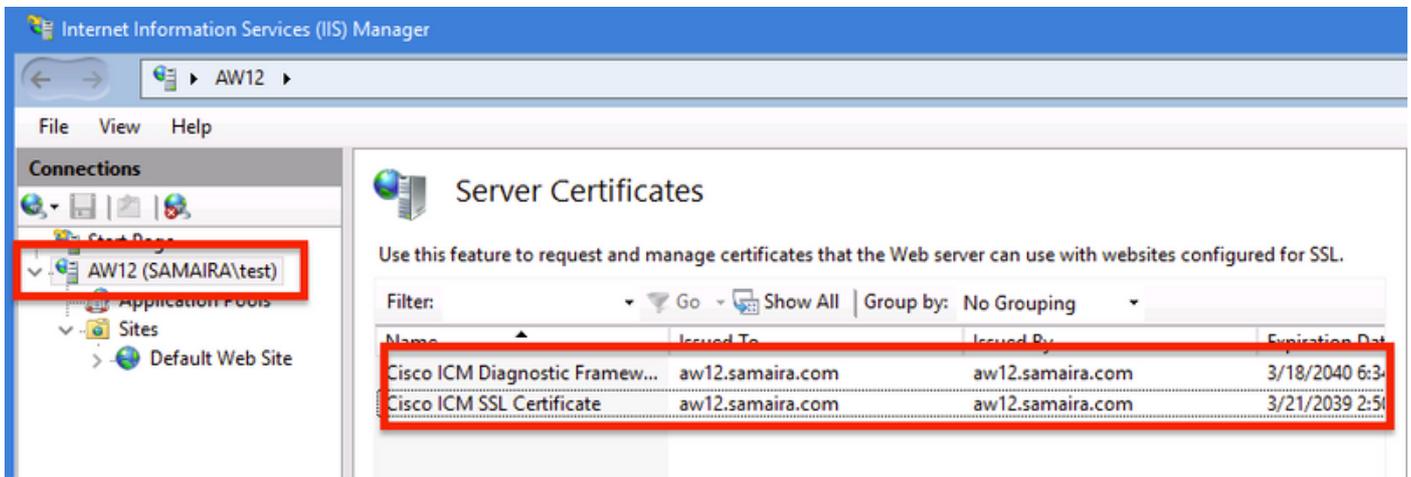
Zertifikate mit SHA-256 und Schlüsselgröße 2048 Bit verwenden

Protokolliert Fehler bei der Identifizierung von nicht beanstandeten Zertifikaten (d. h. wenn die Anforderung SHA-256 und/oder keysize 2048 Bits nicht erfüllt wird).

Aus UCCE-Perspektive gibt es zwei wichtige Zertifikate:

- Cisco ICM Diagnostic Framework-Servicebescheinigung
- Cisco ICM SSL-Zertifikat

Die Zertifikate können in der IIS-Manager-Option (Internetinformationsdienste) des Windows-Servers überprüft werden.



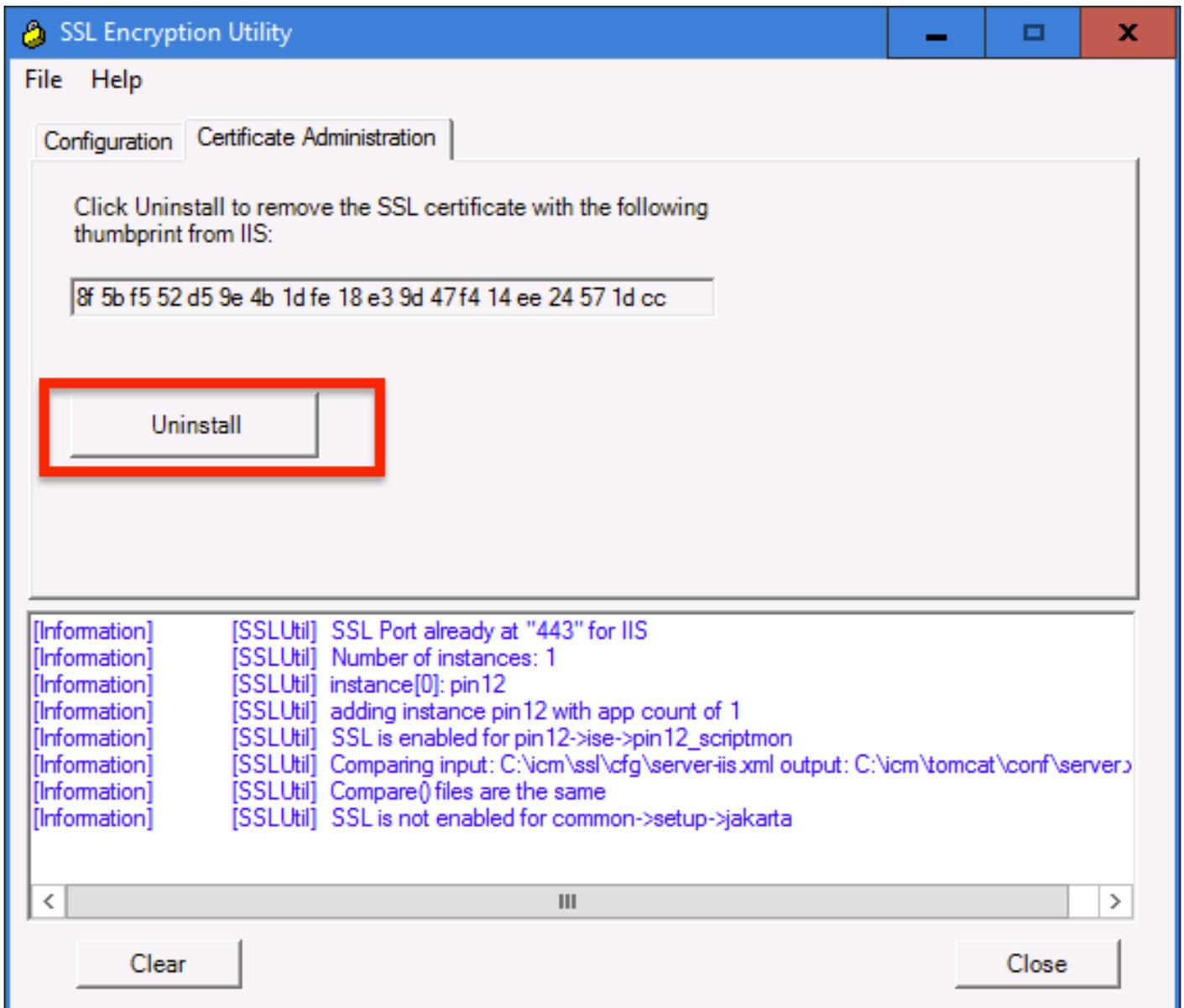
Bei selbstsignierten Zertifikaten (entweder für Diagnose von Portico oder Webeinrichtung) wird folgende Fehlerzeile angezeigt:

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

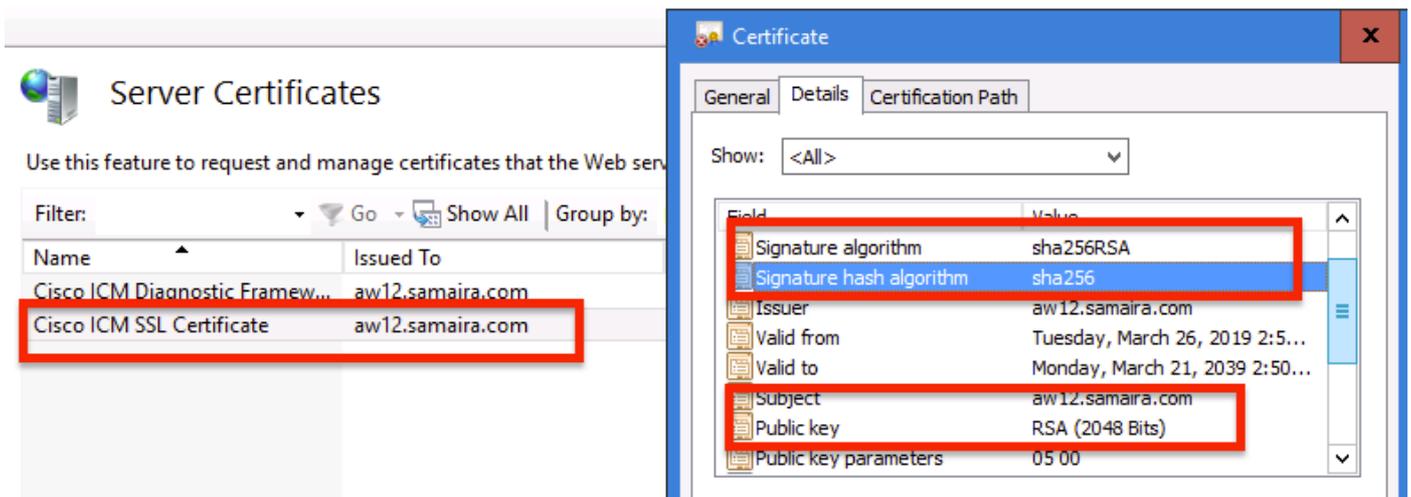
SSLUtil-Tool

a) Um selbstsignierte Zertifikate (für die Webseite WebSetup/CCEAdmin) neu zu generieren, verwenden Sie das SSLUtil-Tool (von C:\icm\bin).

b) Wählen Sie Deinstallieren aus, um das aktuelle "Cisco ICM SSL-Zertifikat" zu löschen.



c) Als Nächstes wählen Sie Installieren in SSLUtil-Tool, und wenn der Prozess beendet ist, beachten Sie, dass das erstellte Zertifikat jetzt SHA-256 enthalten und die Bit '2048' behalten.



DiagFwCertMgr-Befehl

Um ein selbstsigniertes Zertifikat für das Cisco ICM Diagnostic Framework-Dienstzertifikat neu zu

erstellen, verwenden Sie die Befehlszeile "DiagFwCertMgr", wie in der Abbildung gezeigt:

```
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

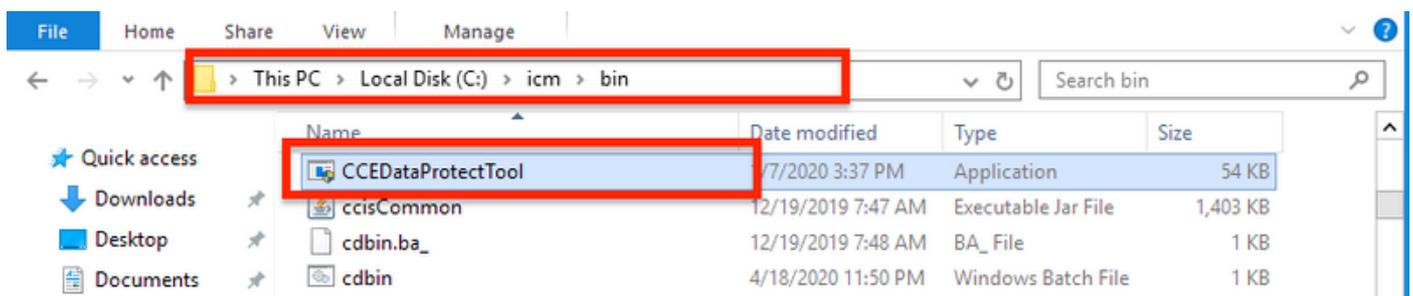
C:\icm\serviceability\diagnostics\bin>
```

Datenschutz-Tool

1. CCEDDataProtectTool wird zum Verschlüsseln und Entschlüsseln vertraulicher Informationen verwendet, die in der Windows-Registrierung gespeichert werden. Nach dem Upgrade auf SQL 12.5 muss der Wertspeicher in der **SQLLogin**-Registrierung mit CCEDDataProtectTool neu konfiguriert werden. Dieses Programm kann nur von einem Administrator, Domänenbenutzer mit Administratorrechten oder einem lokalen Administrator ausgeführt werden.
2. Dieses Tool kann zum Anzeigen, Konfigurieren, Bearbeiten, Entfernen des verschlüsselten Wertspeichers in der **SQLLogin**-Registrierung verwendet werden.
3. Das Tool ist am richtigen Ort.

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

4. Navigieren Sie zum Speicherort, und doppelklicken Sie auf CCEDDataProtectTool.exe.



5. Zum Verschlüsseln drücken Sie 1 für DBLookup, und geben Sie Instanzname ein. Drücken Sie anschließend 2, um "Bearbeiten und Verschlüsseln" auszuwählen.

```
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. Navigieren Sie zum Registrierungsart, und überprüfen Sie den String-Wert **SQLLogin**, wie im Bild gezeigt:

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 [X]

Value name:

Value data:

7. Falls der verschlüsselte Wert überprüft werden muss; Wählen Sie in der Befehlszeile von CCEDDataProtectTool die Option 1 für "Entschlüsseln und Anzeigen" aus, wie im Bild gezeigt.

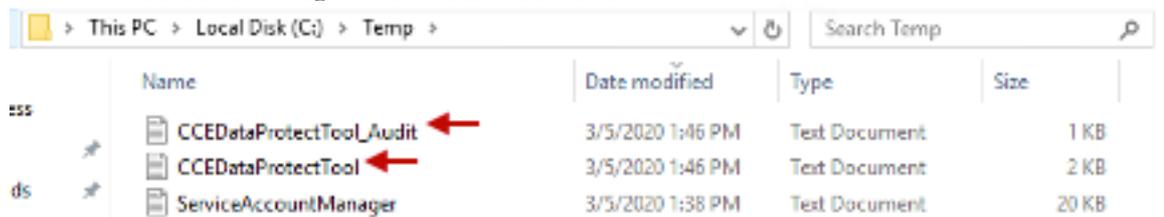
```
Select one of the below options for DBLookup Registry
1. Decrypt and View ← 2. Edit and Encrypt 3. Help 4. Exit
1
████████████████████████████████████████████████████████████████████████████████
```

8. Alle Protokolle für dieses Tool finden Sie am Speicherort.

<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.