

# Compreenda as melhorias de segurança do UCCE 12.5

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Verificação da ISO baixada](#)

[Usar certificados com SHA-256 e tamanho de chave 2048 bits](#)

[Ferramenta SSLUtil](#)

[Comando DiagFwCertMgr](#)

[Ferramenta de proteção de dados](#)

## Introduction

Este documento descreve os aprimoramentos de segurança mais recentes adicionados ao Unified Contact Center Enterprise (UCCE) 12.5.

## Prerequisites

- UCCE
- Open Secure Sockets Layer (SSL)

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCCE 12.5
- SSL aberto

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

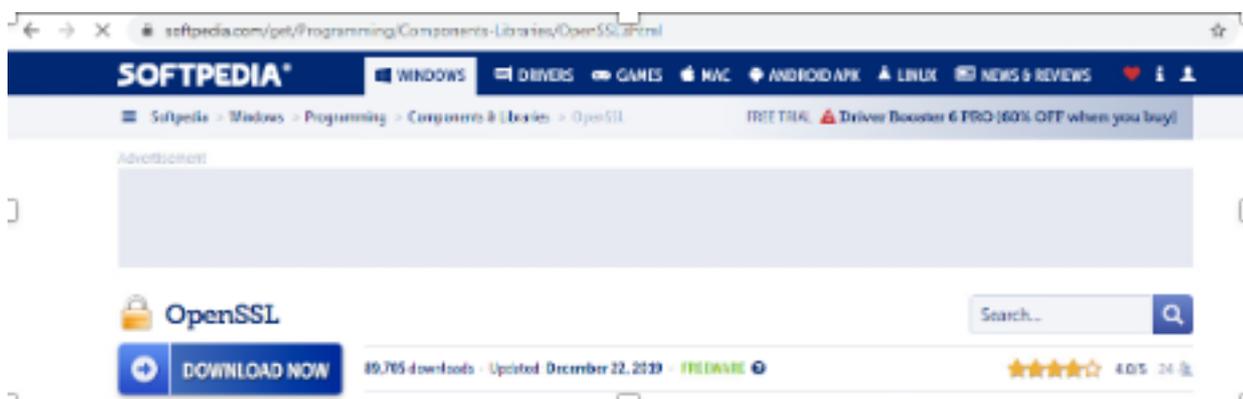
Cisco Security Control Framework (SCF): A estrutura de controle de segurança de colaboração fornece as diretrizes de projeto e implementação para a criação de uma infraestrutura de colaboração segura e confiável. Essas infraestruturas são resilientes a formas conhecidas e novas de ataques. [Guia de Segurança de Referência do Cisco Unified ICM/Contact Center Enterprise, Versão 12.5](#) .

Como parte do esforço de SCF da Cisco, melhorias de segurança adicionais são adicionadas para UCCE 12.5. Este documento descreve esses aprimoramentos.

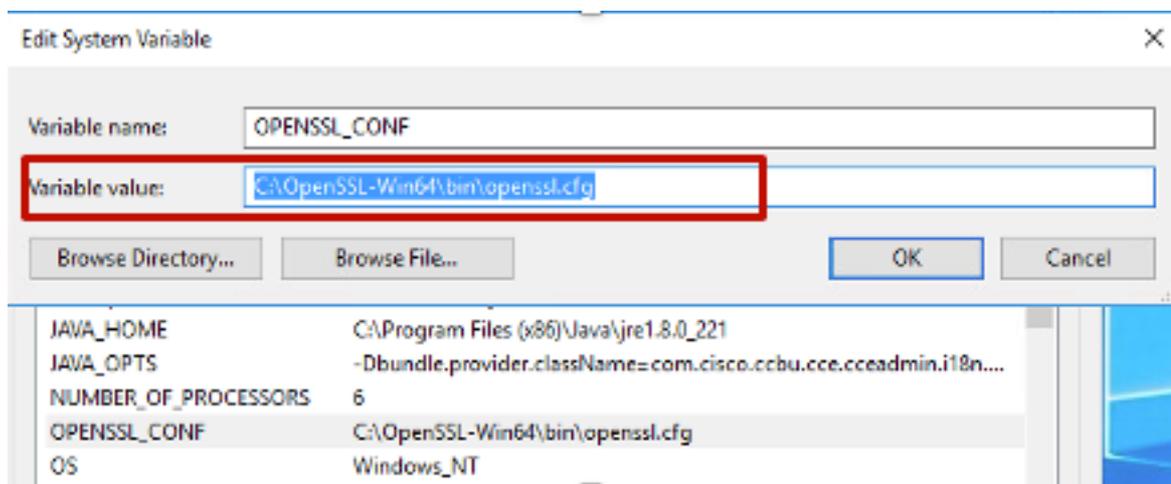
## Verificação da ISO baixada

Para validar o ISO baixado assinado pela Cisco e garantir que ele seja autorizado, as etapas são:

1. Baixe e instale o OpenSSL. Procure por software "openssl softpedia".



2. Confirme o caminho (definido por padrão, mas ainda é bom verificar). No Windows 10, vá para Propriedades do sistema, selecione Variáveis de ambiente.



3. Arquivos necessários para a verificação 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. Execute a ferramenta OpenSSL a partir da linha de comando.

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

5. Executar o comando

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

6. Em caso de falha, a linha de comando mostra um erro como mostrado na imagem

```
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>
```

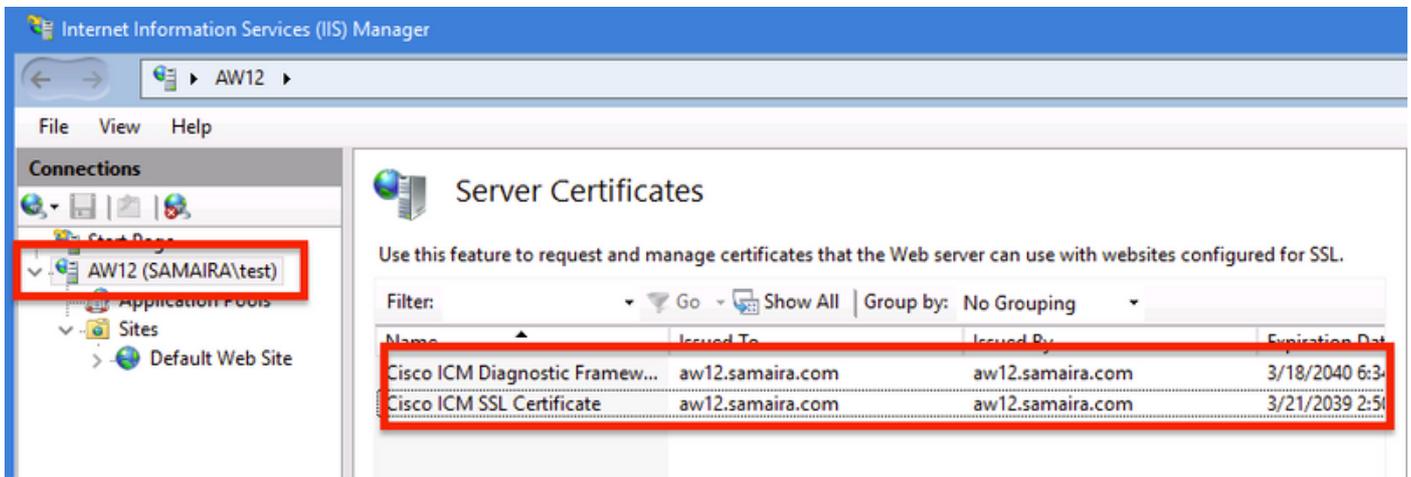
## Usar certificados com SHA-256 e tamanho de chave 2048 bits

Os registros reportam um erro no caso de identificação de certificados não reclamantes (isto é, não atendem ao requisito SHA-256 e/ou keysize 2048 bits).

Há dois certificados importantes do ponto de vista do UCCE:

- certificado de serviço do Cisco ICM Diagnostic Framework
- Certificado SSL do Cisco ICM

Os certificados podem ser revisados na opção Gerenciador dos Serviços de Informações da Internet (IIS) do Windows Server.



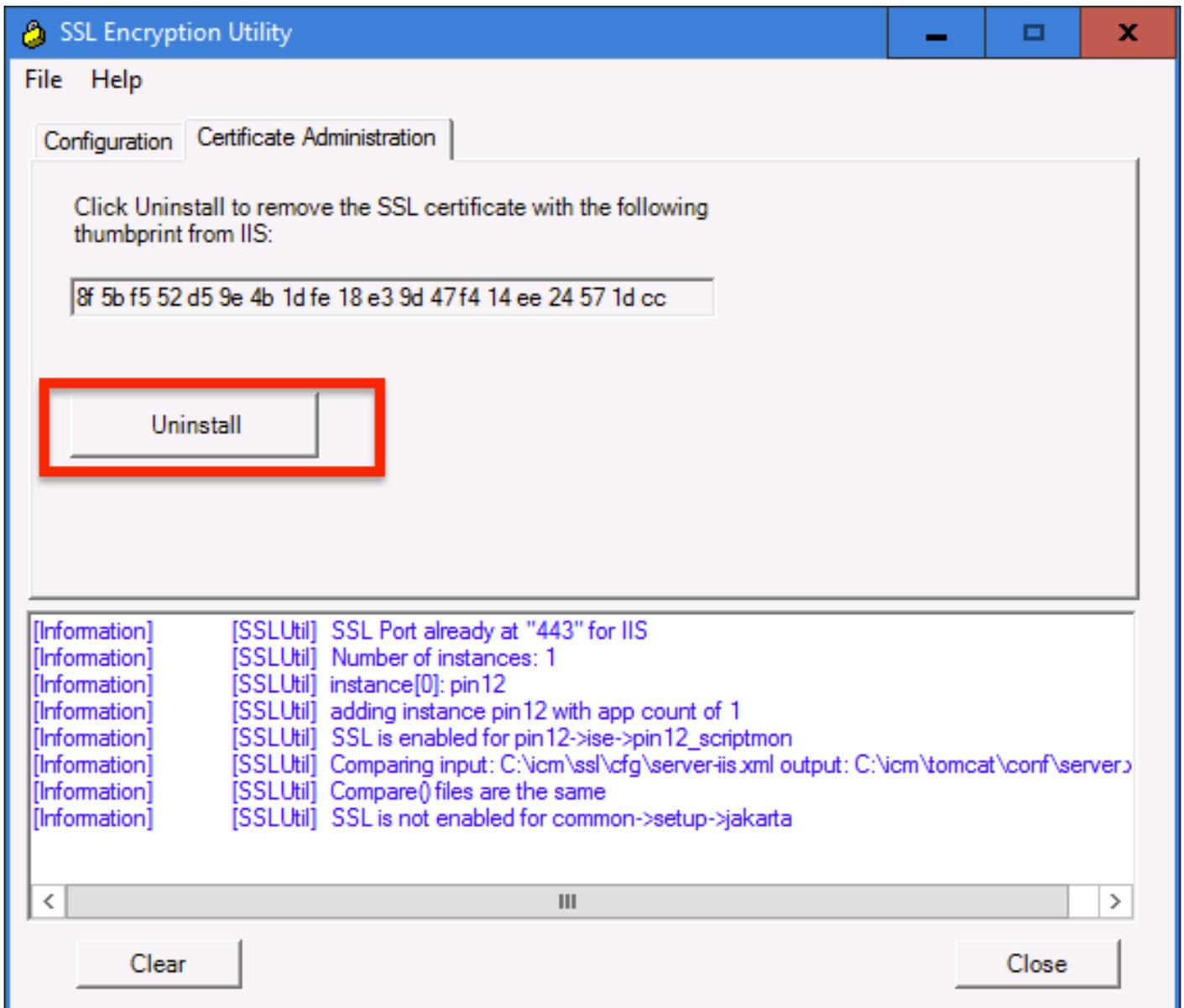
Para certificados autoassinados (para Diagnose Portico ou Configuração da Web) , a linha de erro reportada é:

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

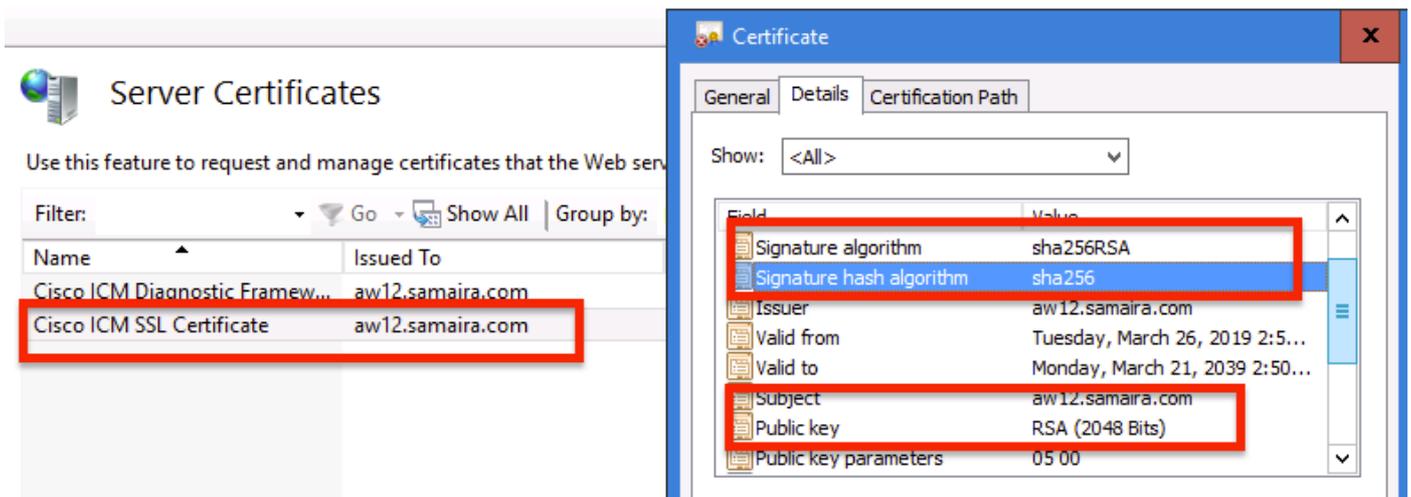
## Ferramenta SSLUtil

a. Para gerar novamente certificados autoassinados (para a página WebSetup/CCEAdmin), use a ferramenta SSLUtil (na localização C:\icm\bin).

b. Selecione Desinstalar para excluir o "Certificado SSL do Cisco ICM" atual.



c. Em seguida, selecione Instalar na ferramenta SSLUtil e, depois que o processo for concluído, observe que o certificado criado agora inclui os bits SHA-256 e keysize '2048'.



## Comando DiagFwCertMgr

Para regenerar um certificado autoassinado para o certificado de serviço do Cisco ICM Diagnostic

Framework, use a linha de comando "DiagFwCertMgr", como mostrado na imagem:

```
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>_
```

## Ferramenta de proteção de dados

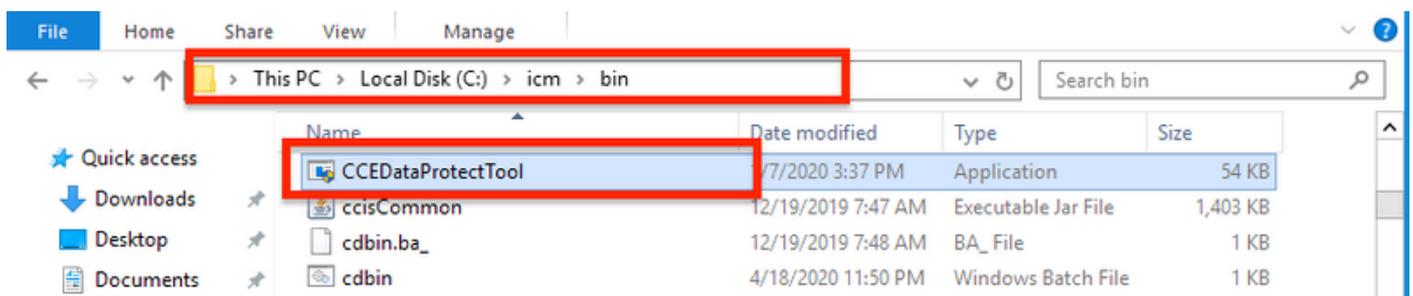
1. CCEDDataProtectTool é usado para criptografar e descriptografar informações confidenciais que o registro do Windows armazena nele. Após a atualização para SQL 12.5 , o armazenamento de valores no registro **SQLLogin** precisa ser reconfigurado com CCEDDataProtectTool. Somente administrador, usuário de domínio com direitos administrativos ou um administrador local pode executar essa ferramenta.

2. Esta ferramenta pode ser usada para visualizar, configurar, editar, remover armazenamento de valores criptografados no registro **SQLLogin**.

3. A ferramenta está no local;

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

4. Navegue até o local e clique duas vezes em CCEDDataProtectTool.exe.

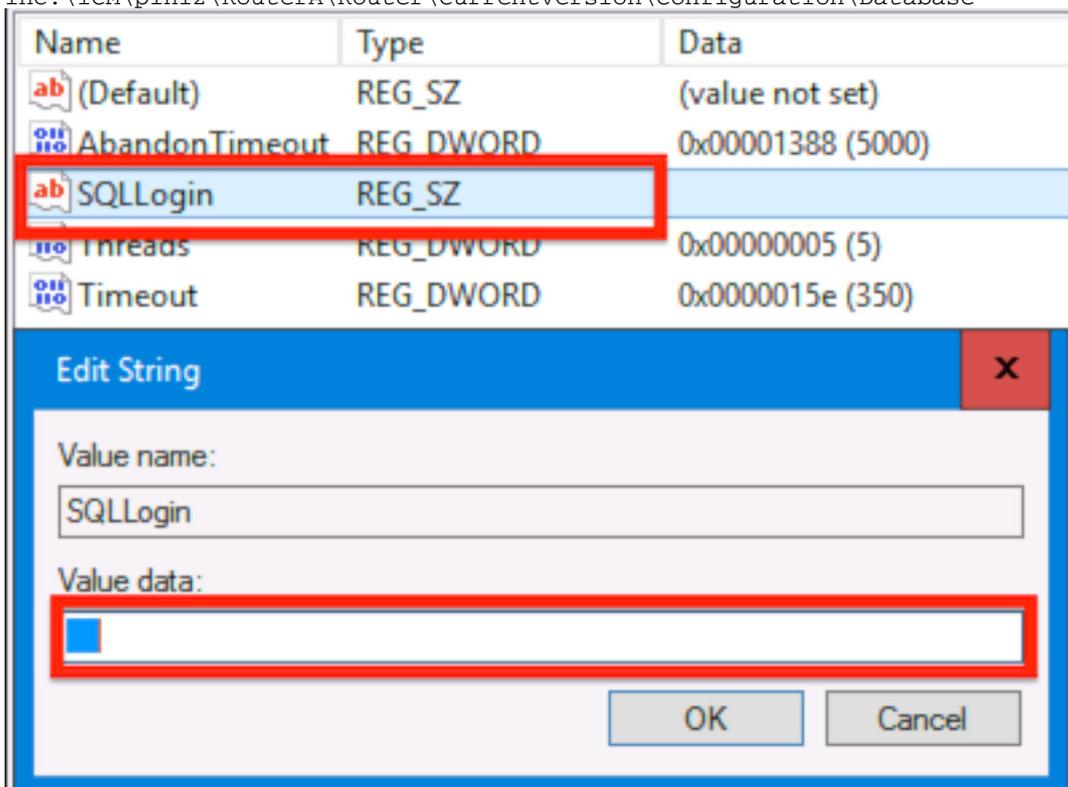


5. Para criptografar , pressione 1 para DBLookup, insira Instance Name (Nome de instância). Em seguida, pressione 2 para selecionar "Edit and Encrypt" (Editar e criptografar)

```
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 até o local do registro e reveja o **SQLLogin** do valor da string parece em branco , como mostrado na imagem :

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



7. Em caso de necessidade de rever o valor encriptado; enquanto linha de comando do CCEDDataProtectTool , selecione pressionar 1 para "Descriptografar e visualizar", como mostrado na imagem;

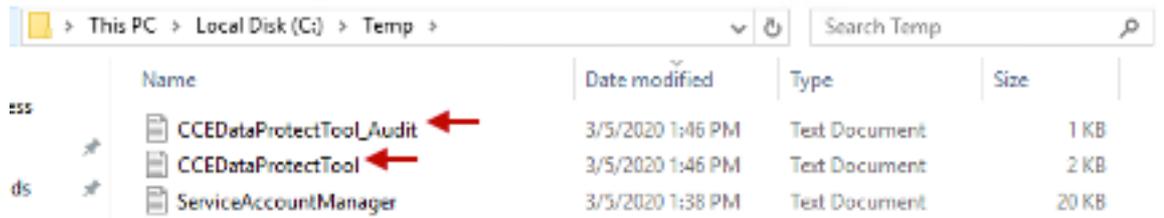
```
Select one of the below options for DBLookup Registry
1. Decrypt and View ← 2. Edit and Encrypt 3. Help 4. Exit
1
```

8. Os registros desta ferramenta podem ser encontrados no local;

```
<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 files 'CCEDDataProtectTool\_Audit' and 'CCEDDataProtectTool'.