了解UCCE 12.5安全性增强

目录

简介

本文描述关于最新的安全性增强添加与Unified联络中心企业(UCCE) 12.5。

先决条件

- UCCE
- 打开安全套接字协议层(SSL)

要求

Cisco 建议您了解以下主题：

- UCCE 12.5
- 打开SSL

使用的组件

本文档中的信息基于以下软件和硬件版本：

- UCCE 12.5
- Openssl (64位) windows的

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

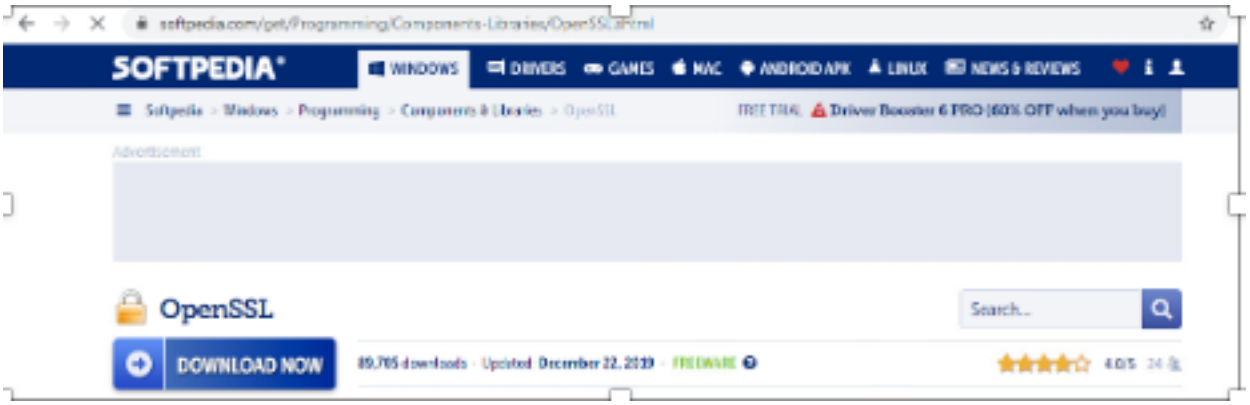
Cisco安全控制框架(SCF) ：协作安全控制框架为构建安全和可靠协作基础设施提供设计和实施指南。这些基础设施是能适应的对攻击著名的和新的表。参考Cisco Unified ICM/Contact中心企业的安全指南，版本12.5。

作为Cisco的SCF努力附加安全性一部分增强为UCCE 12.5被添加。本文略述这些增强。

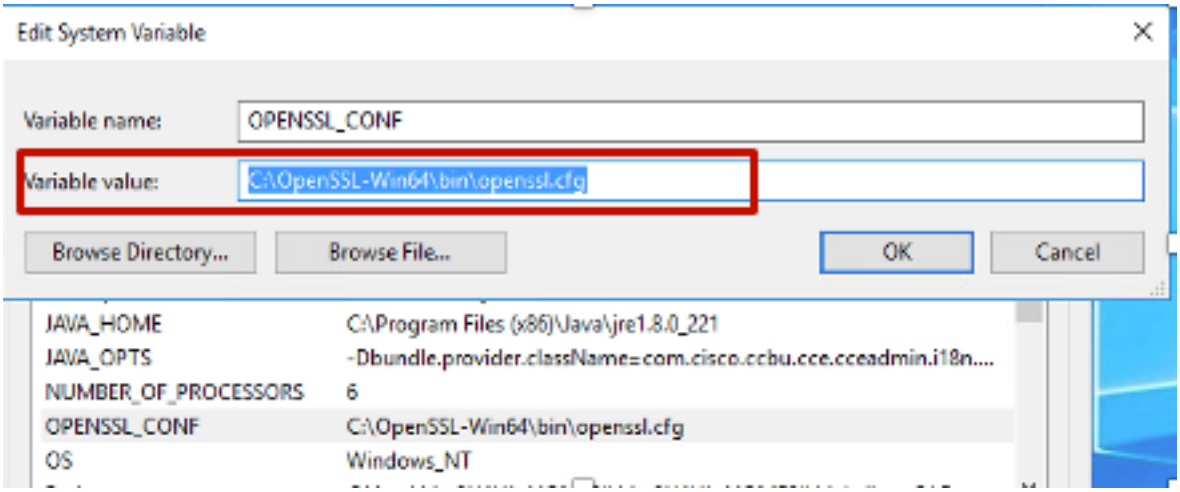
下载的ISO的验证

为了验证Cisco签字的下载的ISO以及保证授权，步骤是：

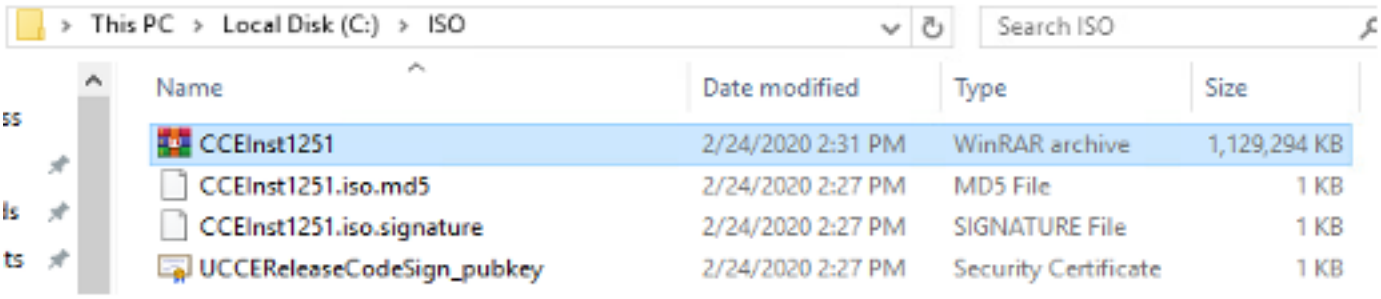
1. 下载并且安装Openssl。搜索软件“openssl softpedia”。



2.确认路径(这默认情况下，但是设置好验证)。在Windows 10，定位的系统Propeties，选择环境变量。



3. 为ISO验证需要的文件



4.从line命令运行Openssl工具。

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

5.运行命令

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

6. 如镜像所显示，在失败情形下， line命令显示错误

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

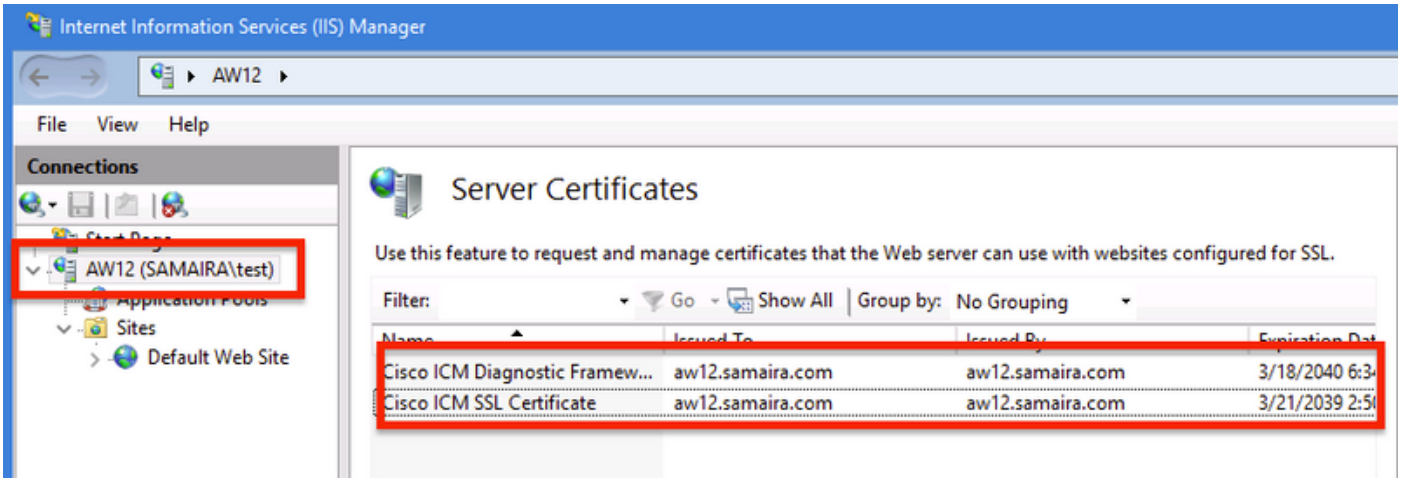
以SHA-256和密钥大小2048位使用证书

日志报告错误在识别非投诉证书情形下(即不满足SHA-256并且/或者keysize 2048个位需求。)

有两重要证书从UCCE的方面：

- Cisco ICM诊断框架服务证书
- Cisco ICM SSL证书

证书在Windows服务器的互联网信息服务(IIS)管理器选项可以查看。



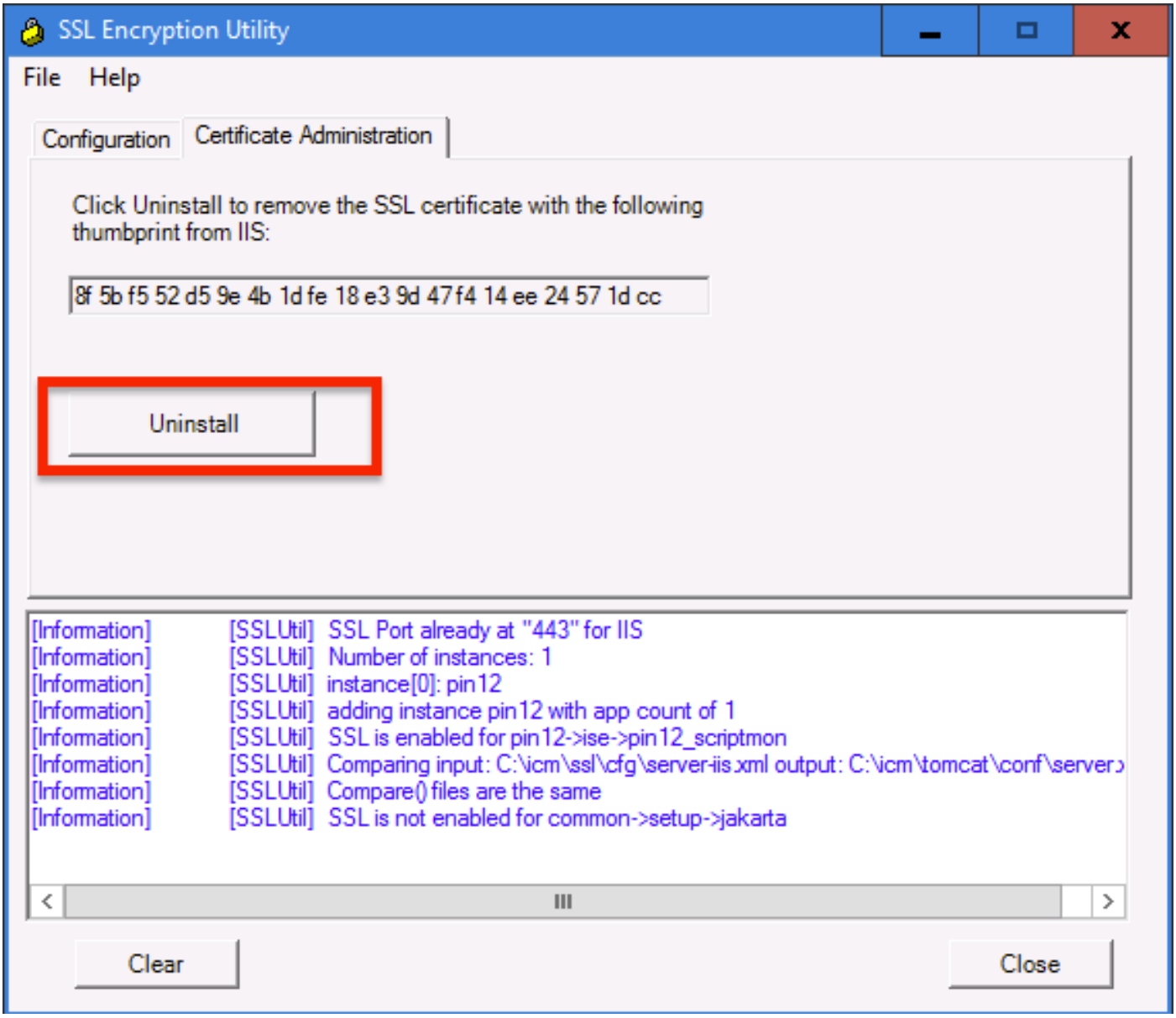
对于自签名证书(设置的Diagnose门廓或Web)，报告的错误线路是：

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

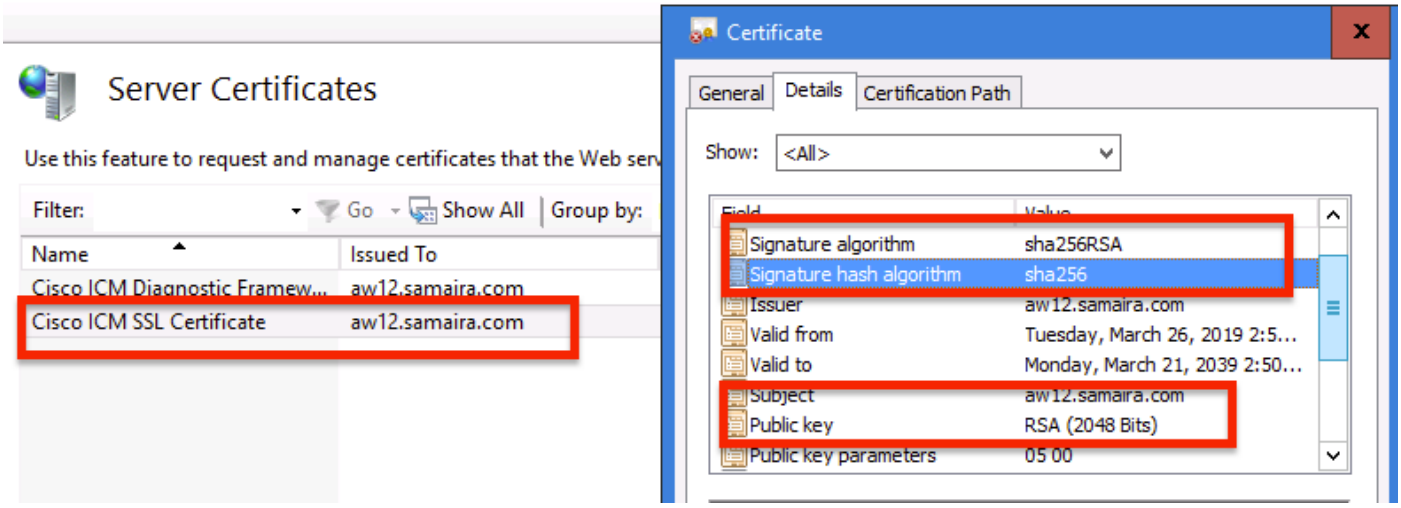
SSLUtil工具

a.为了重新生成自签名证书(WebSetup/CCEAdmin页)使用SSLUtil工具(从位置C:\icm\bin)。

b. 选择卸载删除当前“Cisco ICM SSL证书”。



c. 其次请选择在SSLUtil工具的安装和，一旦进程完成，注意当前创建的证书包括SHA-256和keysize '2048'位。



DiagFwCertMgr命令

如镜像所显示，为了重新生成Cisco ICM诊断框架服务证书的一自签名证书，请使用line命令

“DiagFwCertMgr”， ：

```
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>_
```

数据保护工具

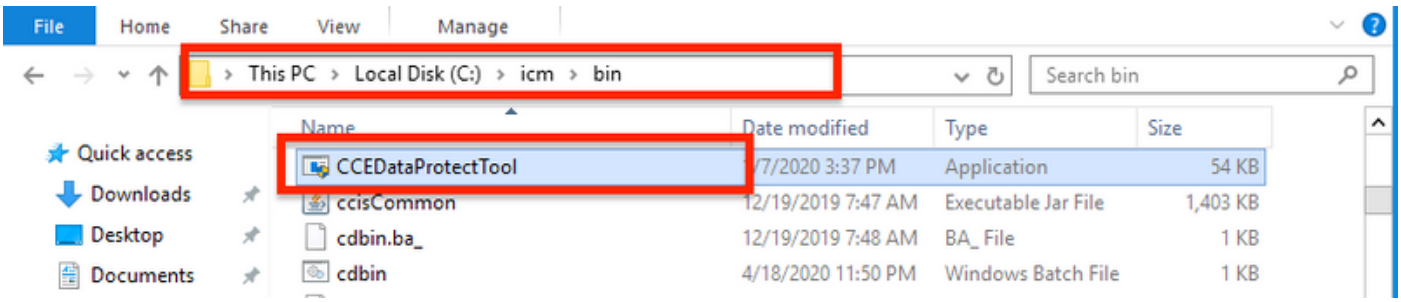
1. CCEDataProtectTool用于加密和解密Windows注册表在它存储的敏感信息。张贴升级对SQL 12.5， **SQLLogin**注册需要的值存储重新配置CCEDataProtectTool。只有管理员、域用户有administrattive权利的或者本地管理员能运行此工具。

2. 此工具可以用于查看，配置，编辑，删除**SQLLogin**注册的加密的值存储。

3. 工具在位置被找到;

```
<Install Directory>:\icm\bin\CCEDataProtectTool.exe
```

4. 导航对位置和双击CCEDataProtectTool.exe。

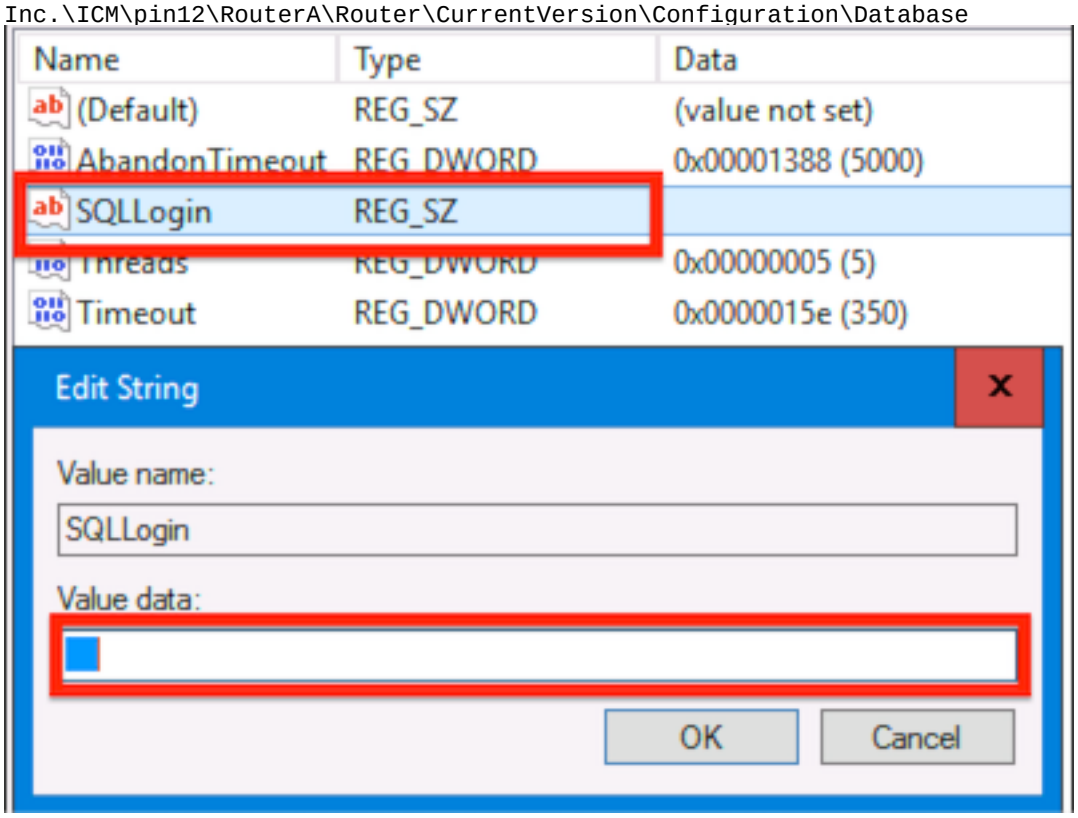


5. 为了加密，请按1 DBLookup的，回车实例名字。其次，请按2选择"Edit and Encrypt"

```
C:\icm\bin\CCEDataProtectTool.exe
CCEDataProtectTool 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\CCEDataProtect.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.如镜像所显示，导航对注册位置和复核字符串值SQLLogin查找空白， ：

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



7.假如需要查看加密的值;当CCEDataProtectTool line命令，精选按1 “解密和视图的”时，如镜像所显示，;

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

8. 此工具的所有日志可以在位置找到;

```
<Install Directory>:\temp

Audit logs filename : CCEDataProtectTool_Audit
CCEDataProtectTool logs : CCEDataProtectTool
```