了解UCCE 12.5安全增强功能

目录

简介

本文档介绍Unified Contact Center Enterprise(UCCE)12.5中添加的最新安全增强功能。

先决条件

- UCCE
- 开放安全套接字层(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），用于Windows

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。
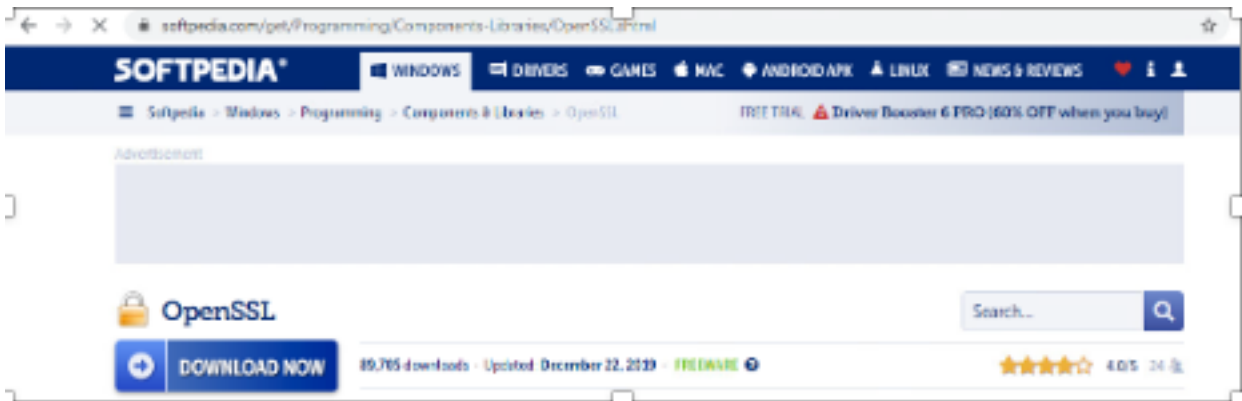
背景信息

思科安全控制框架(SCF):协作安全控制框架为构建安全可靠的协作基础设施提供了设计和实施指南。这些基础设施对已知和新形式的攻击都具有恢复能力。思科[统一ICM/联系中心企业版参考安全指南，版本12.5](#)。
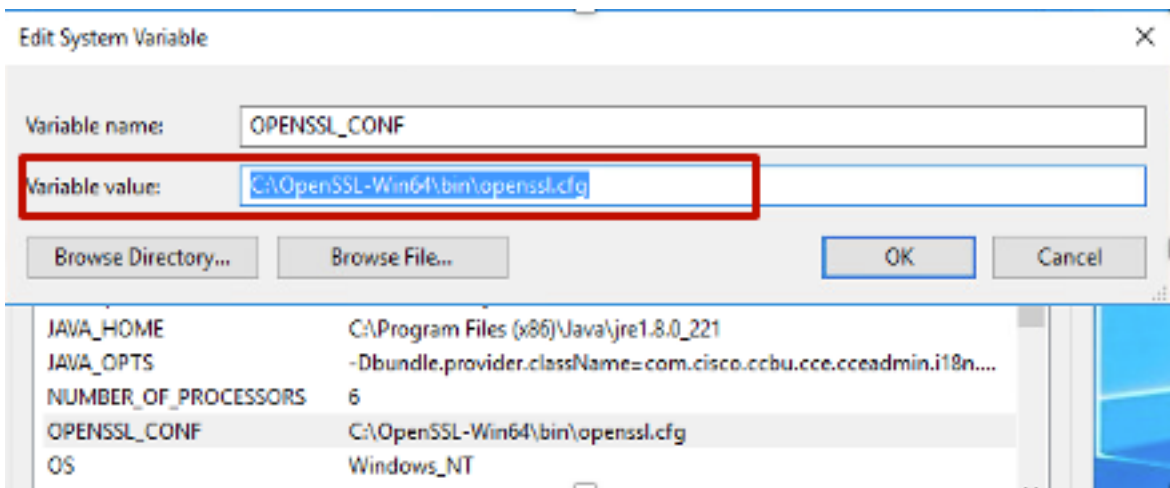
作为思科SCF努力的一部分，UCCE 12.5增加了其他安全增强功能。本文档概述了这些增强功能。

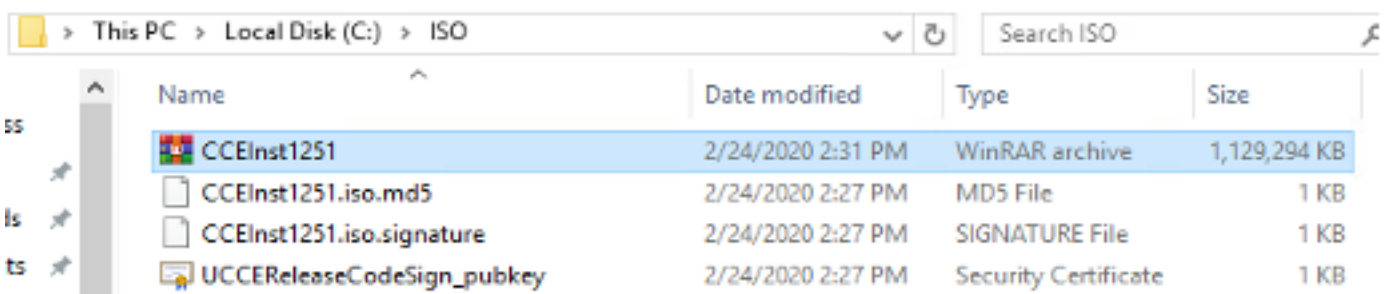# 已下载ISO的验证

为了验证思科签署的下载ISO并确保其已获得授权，步骤如下：

1.下载并安装OpenSSL。搜索软件"openssl softpedia"。

2.确认路径（默认情况下已设置，但仍可以验证）。 在Windows 10中，转到系统属性，选择环境变量。

3. ISO验证所需文件

4.从命令行运行OpenSSL工具。

5. 运行命令

```
dgst -sha512 -keyform der -verify <public Key.der> -signature <ISO image.iso.signature> <ISO Image>
```
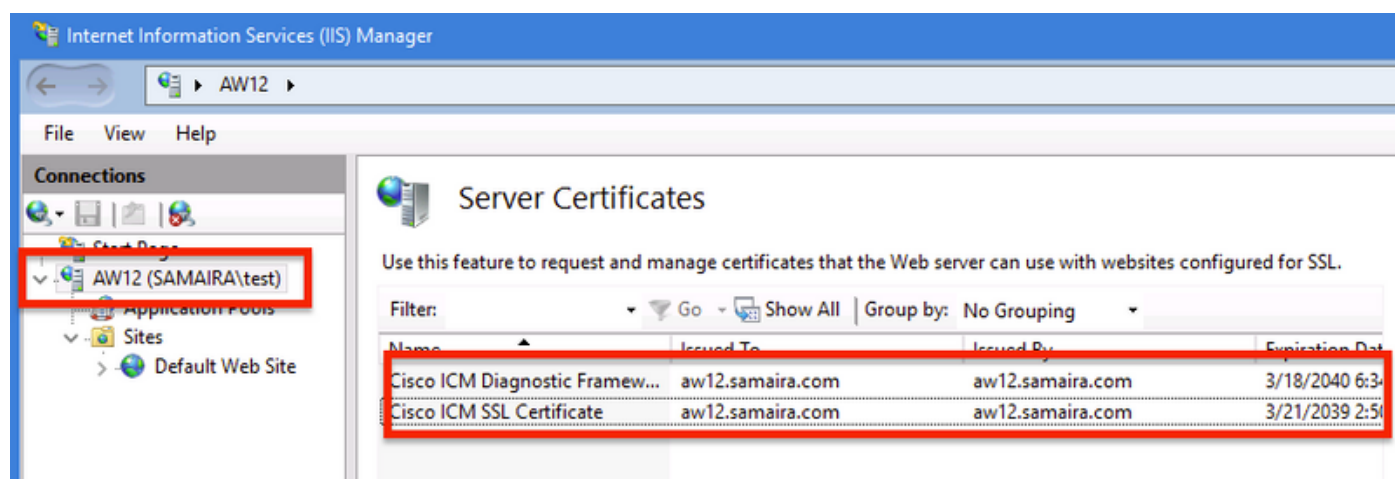
6.如果发生故障，命令行显示错误，如图所示

使用带SHA-256和密钥大小2048位的证书

在识别非投诉证书（即不满足SHA-256和/或密钥大小2048位要求）时记录报告错误。

从UCCE的角度来看，有两个重要证书：

- 思科ICM诊断框架服务证书
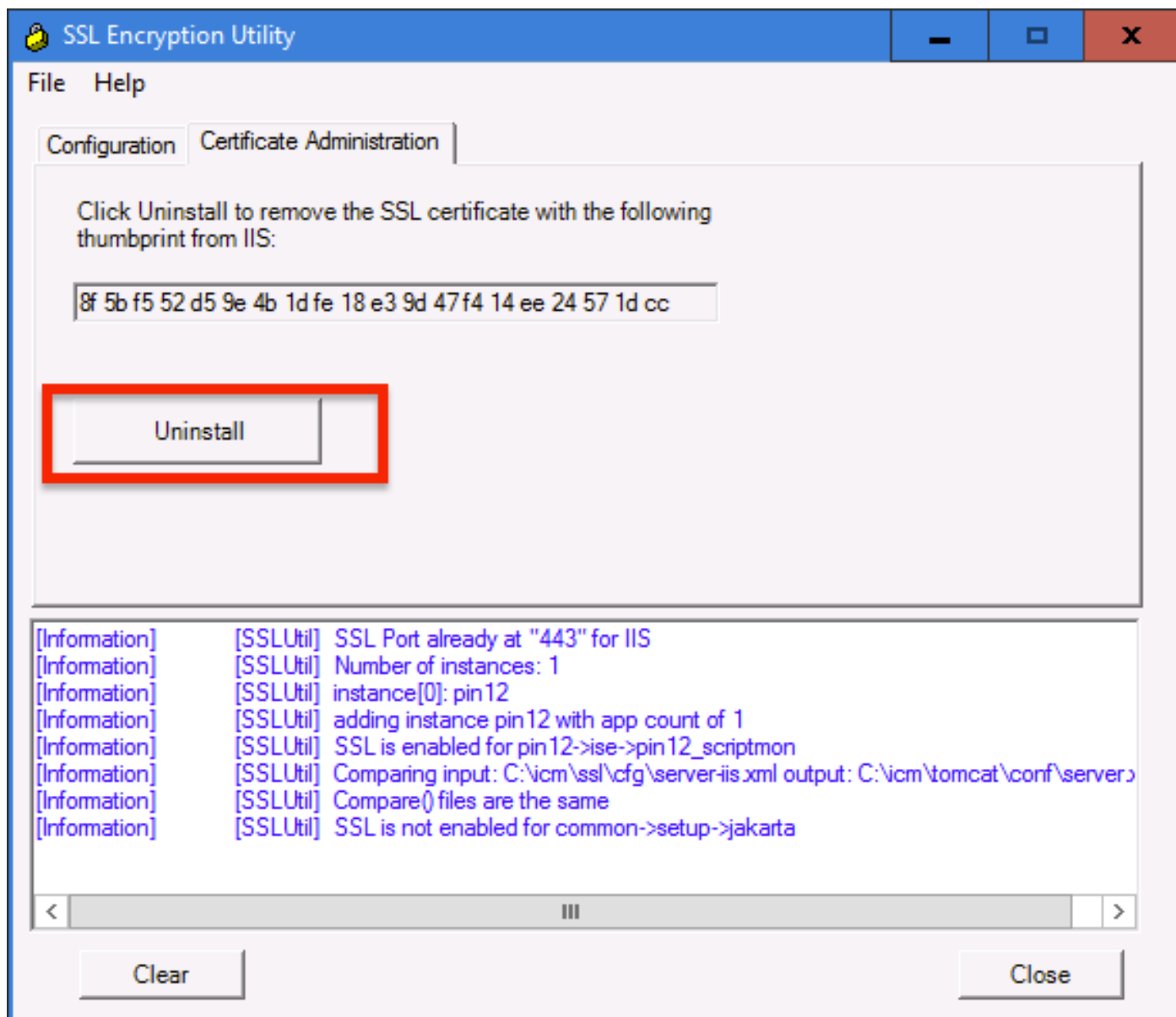- 思科ICM SSL证书

可以在Windows服务器的Internet信息服务(IIS)管理器选项中查看证书。

对于自签名证书（用于诊断门户或Web设置），报告的错误行为：

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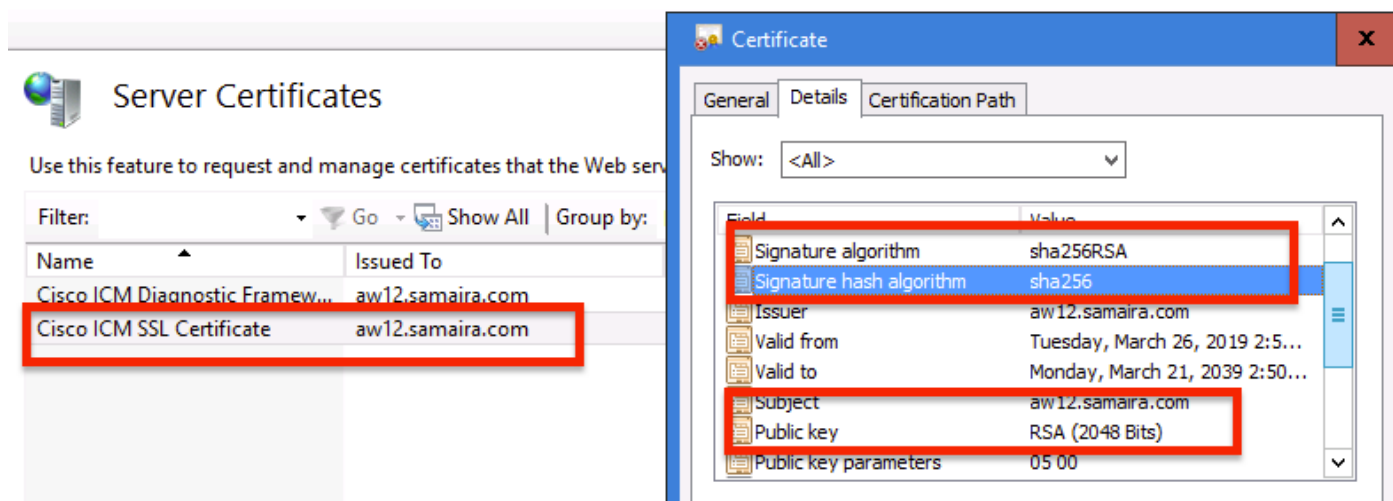
SSLUtil工具

a.要重新生成自签名证书（对于WebSetup/CCEAdmin页面），请使用SSLUtil工具(从位置 C:\icm\bin)。

b.选择Uninstall以删除当前的"Cisco ICM SSL证书"。

c.接下来选择在SSLUtil工具中安装，并在流程完成后，注意现在创建的证书包括SHA-256和密钥大小"2048"位。

DiagFwCertMgr命令

要为Cisco ICM诊断框架服务证书重新生成自签名证书，请使用命令行"**DiagFwCertMgr**"，如图所示：

```
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>_
```
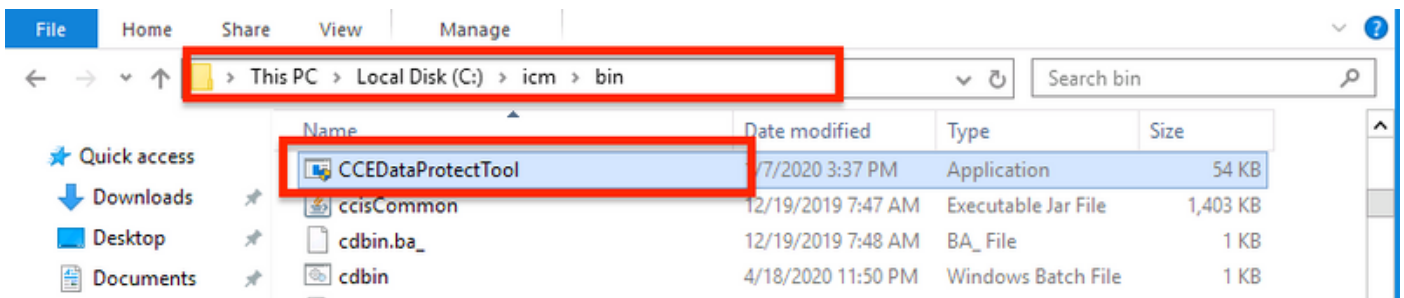
数据保护工具

1. **CCEDataProtectTool**用于加密和解密Windows注册表中存储的敏感信息。升级到SQL 12.5后，需要使用CCEDataProtectTool重新配置**SQLLogin注**册表中的值存储。只有管理员、具有管理员权限的域用户或本地管理员才能运行此工具。

2.**此**工具可用于查看、配置、编辑、删除SQLogin注册表中的加密**值存**储区。

3.**在**位置找到工具；

```
<Install Directory>:\icm\bin\CCEDataProtectTool.exe
```
4.**导航**到位置，然后双击CCEDataProtectTool.exe。

5.**要**加密，请按1进行DBLookup，请输入实例名称。然后，按2选择"编辑并加密"

```
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:

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
```
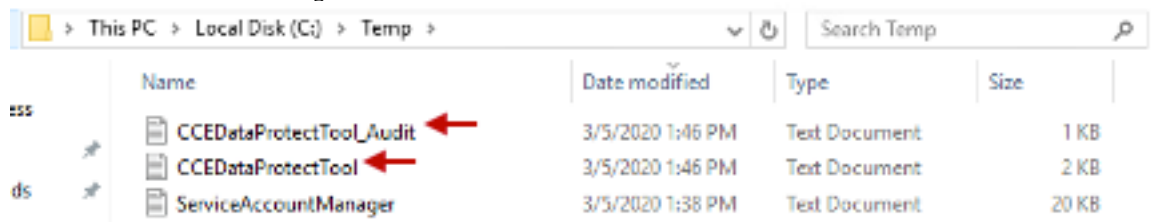
6.导航到注册表位置并查看字符串值SQLLogin看起来为空，如图所示：

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

7.需要复核加密值的；当CCEDataProtectTool的命令行（如图所示）中，为"解密并查看"选择按1;

8.此工具的任何日志都可在位置找到;

```
<Install Directory>:\temp
```

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