了解UCCE 12.5安全增强功能

目录

[简介](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)

[背景信息](#)

[已下载ISO的验证](#)

[使用SHA-256和密钥大小为2048位的证书](#)

- [SSLUtil工具](#)
- [DiagFwCertMgr命令](#)

[数据保护工具](#)

简介

本文档介绍随Unified Contact Center Enterprise(UCCE)12.5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
- Windows的OpenSSL（64位）

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):协作安全控制框架提供了用于构建安全可靠的协作基础设施的设计和实施

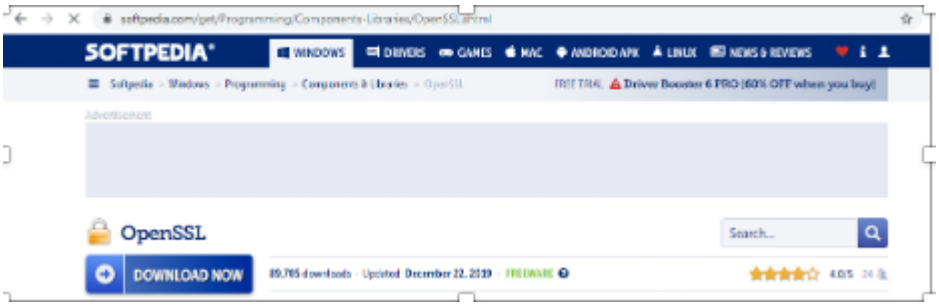
准则。这些基础设施可抵御各种常见攻击和新形式的攻击。Cisco Unified ICM/Contact Center Enterprise参考安全指南，版本12.5。

作为思科SCF工作的一部分，为UCCE 12.5添加了其他安全增强功能。本文档概述这些增强功能。

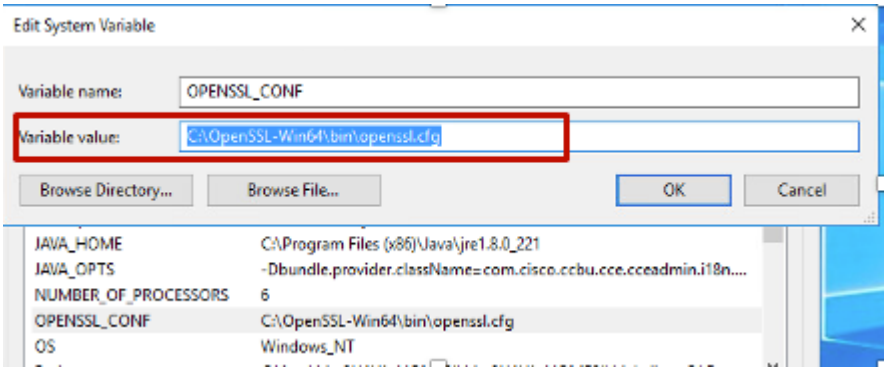
已下载ISO的验证

为了验证由思科签署的已下载ISO并确保其获得授权，步骤如下：

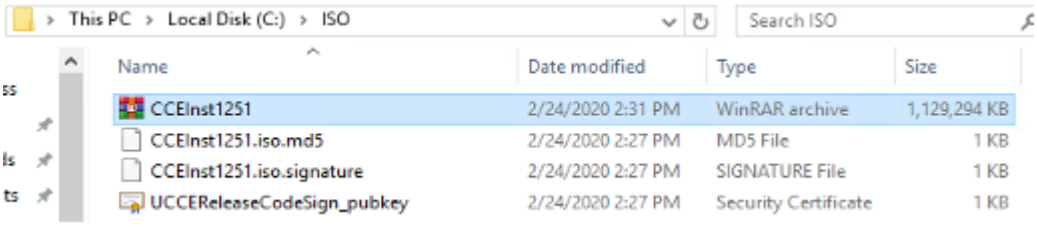
1.下载并安装OpenSSL。搜索软件“openssl softpedia”。



2.确认路径（默认情况下已设置，但仍可以验证）。 在Windows 10中，转至System Properties，选择Environment Variables。



3. ISO验证所需的文件



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，命令行会显示错误，如图所示

```
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>
```

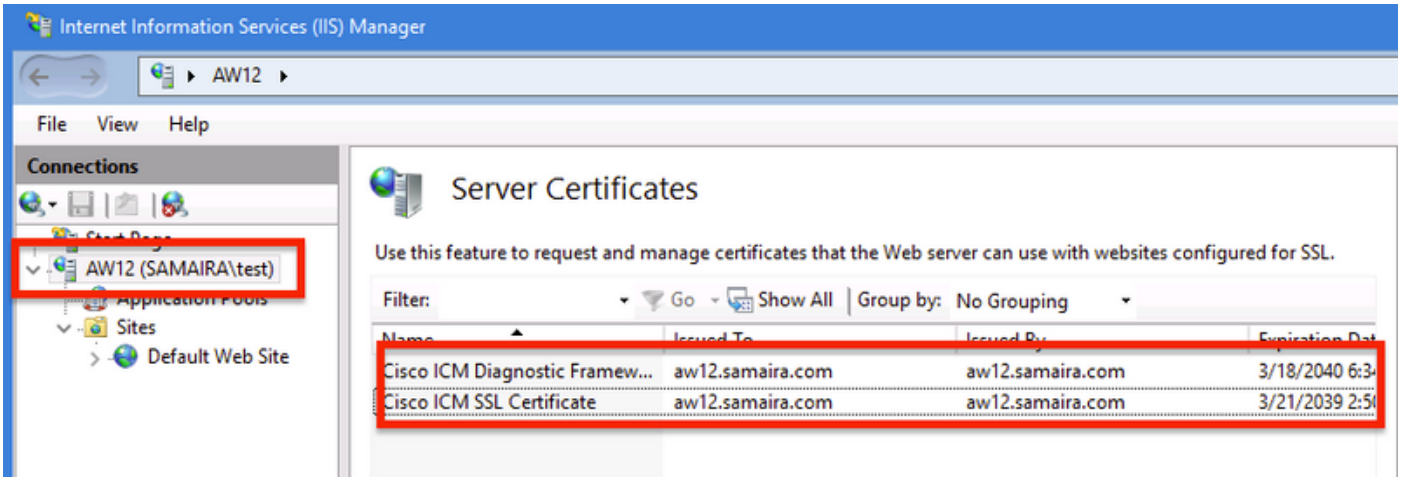
使用SHA-256和密钥大小为2048位的证书

如果发现非投诉证书（即不符合SHA-256和/或keysize 2048位要求），日志会报告错误。

从UCCE的角度来看，有两个重要证书：

- Cisco ICM诊断框架服务证书
- Cisco 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。



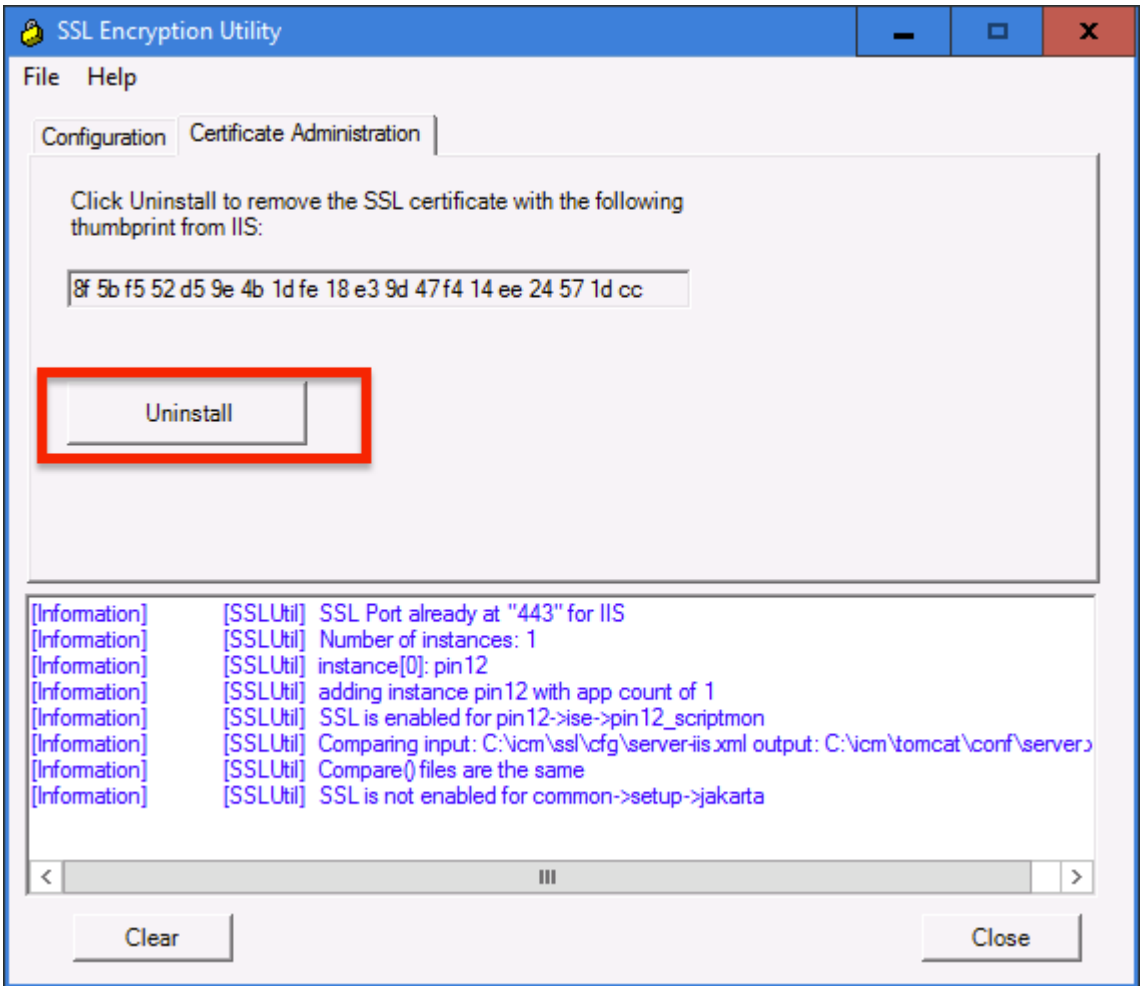
对于自签名证书（用于诊断门户或Web设置），报告的错误行为：

```
Re-generating Cisco ICM SSL Certificate with SHA-256 and key size '2048' and will be binded with port 4
```

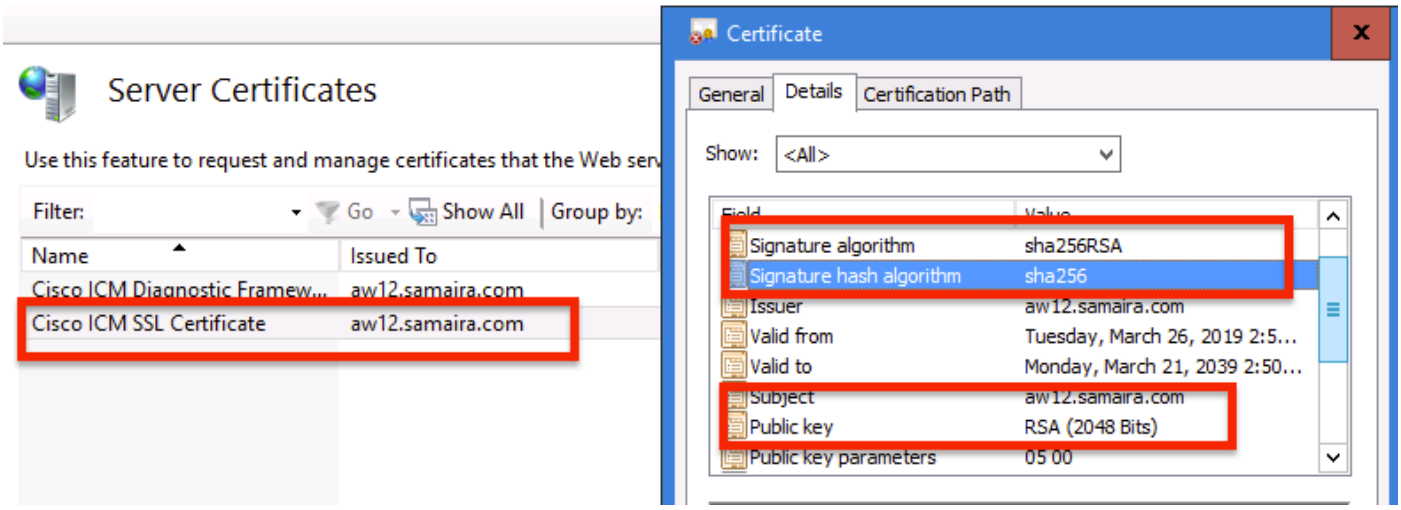
SSLUtil工具

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 Certificate”。



c.然后选择Install in SSLUtil tool（安装在SSLUtil工具中），在过程完成之后，请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

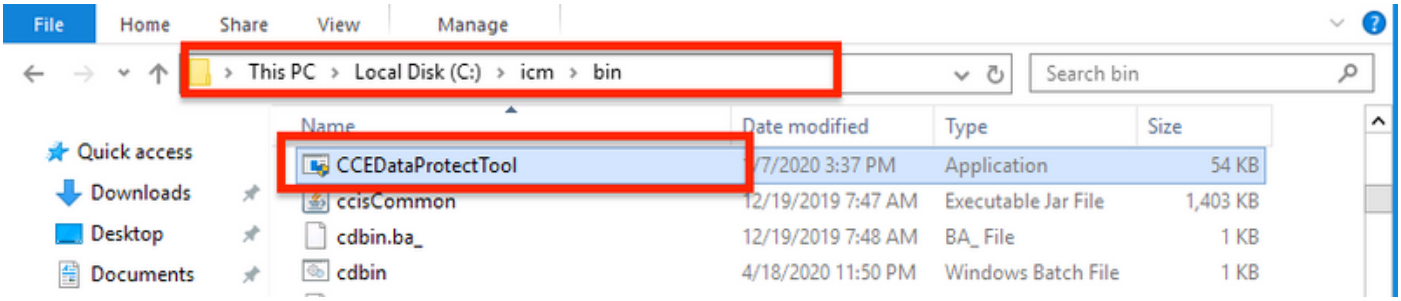
1.CCEDataProtectTool用于加密和解密Windows注册表存储在其中的敏感信息。升级到SQL 12.5后，需要使用CCEDataProtectTool重新配置SQLogin注册表中的值存储。只有管理员、具有管理权限的域用户或本地管理员可以运行此工具。

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。

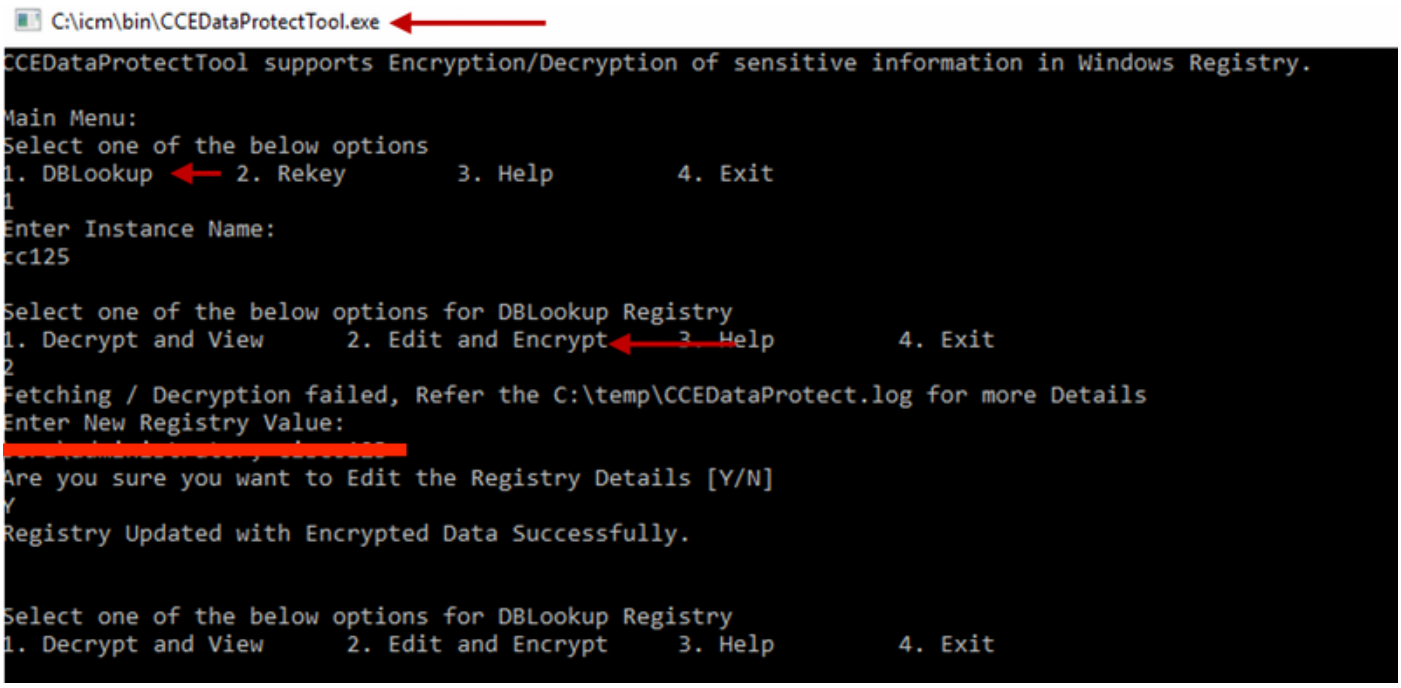
3.在位置找到工具；

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

4.导航到位置并双击CCEDataProtectTool.exe。

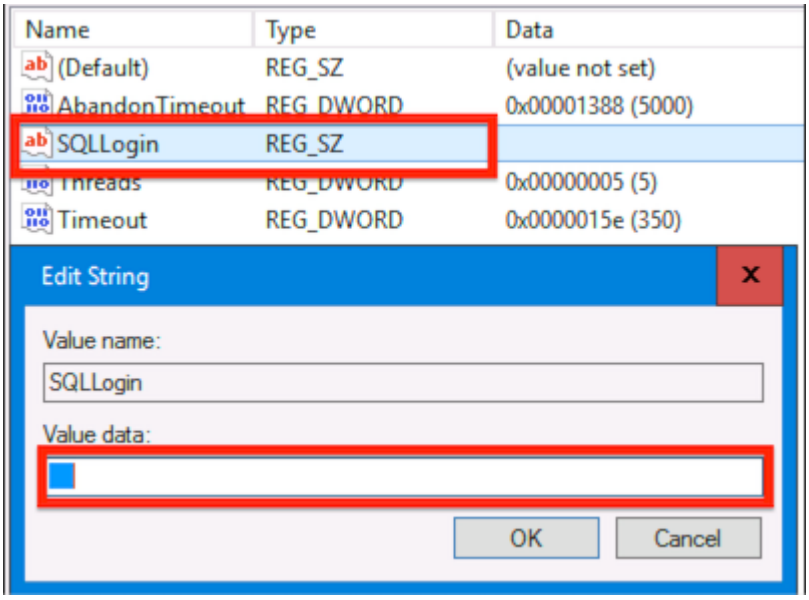


5.要加密，请按1对DBLookup，请输入实例名称。下一步，按2选择“编辑并加密”

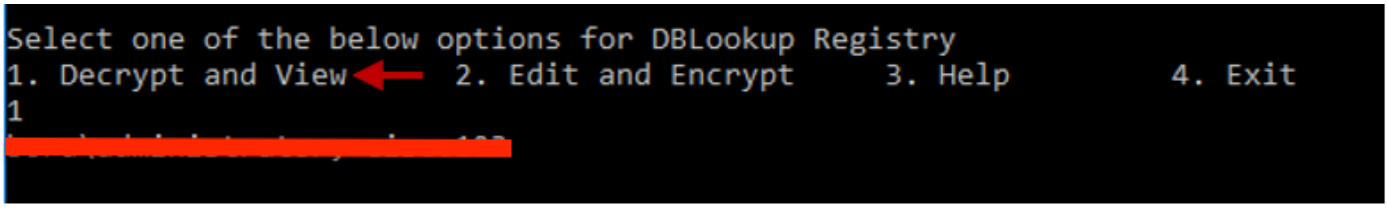


6.导航到注册表位置并查看字符串值SQLLogin看起来为空，如图所示：

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



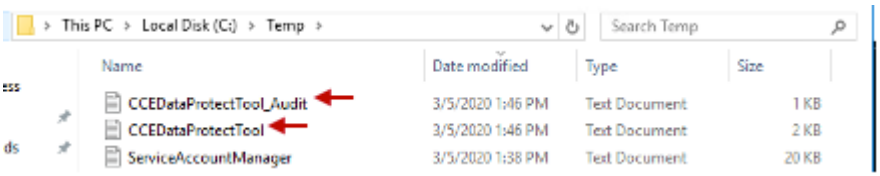
7.需要审核加密值的情况；在CCEDataProtectTool的命令行中，选择“Decrypt and View”按1，如图所示；



8.此工具的任何日志都可在位置中找到;

```
<Install Directory>:\temp

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



关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。