UCCE 12.5 보안 개선 사항 이해

목차

소개

이 문서에서는 UCCE(Unified Contact Center Enterprise) 12.5에 추가된 최신 보안 개선 사항에 대해 설명합니다.

사전 요구 사항

- UCCE
- 개방형 SSL(Secure Sockets Layer)

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- UCCE 12.5
- SSL 열기

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- UCCE 12.5
- Windows용 OpenSSL(64비트)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

Cisco SCF(Security Control Framework):Collaboration Security Control Framework는 안전하고 신

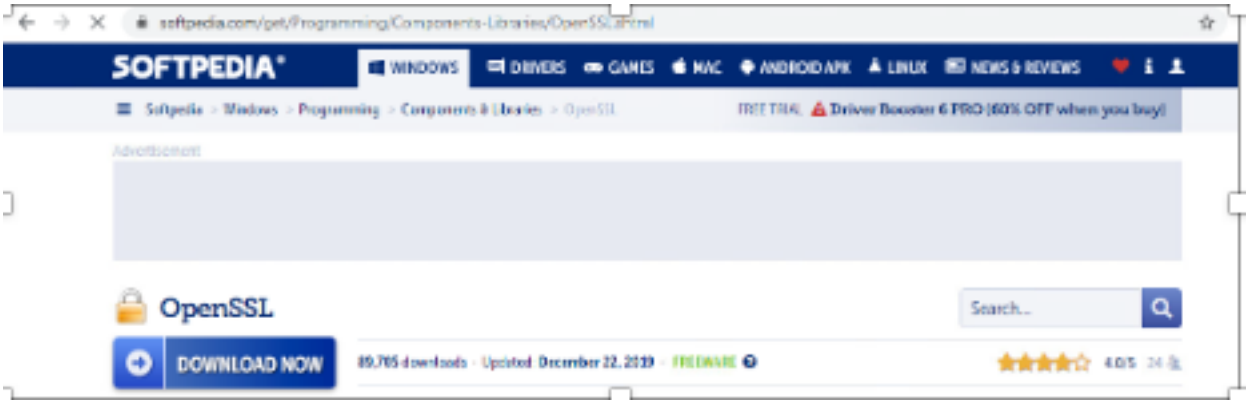
뢰할 수 있는 협업 인프라를 구축하기 위한 설계 및 구현 지침을 제공합니다.이러한 인프라는 잘 알려진 공격과 새로운 형태의 공격에 탄력적입니다.Cisco Unified ICM/Contact Center Enterprise, 릴리스 12.5에 대한 보안 가이드를 참조하십시오.

Cisco의 SCF 노력의 일환으로 UCCE 12.5에 대한 추가적인 보안 개선 사항이 추가되었습니다. 이 문서에서는 이러한 개선 사항을 간략하게 설명합니다.

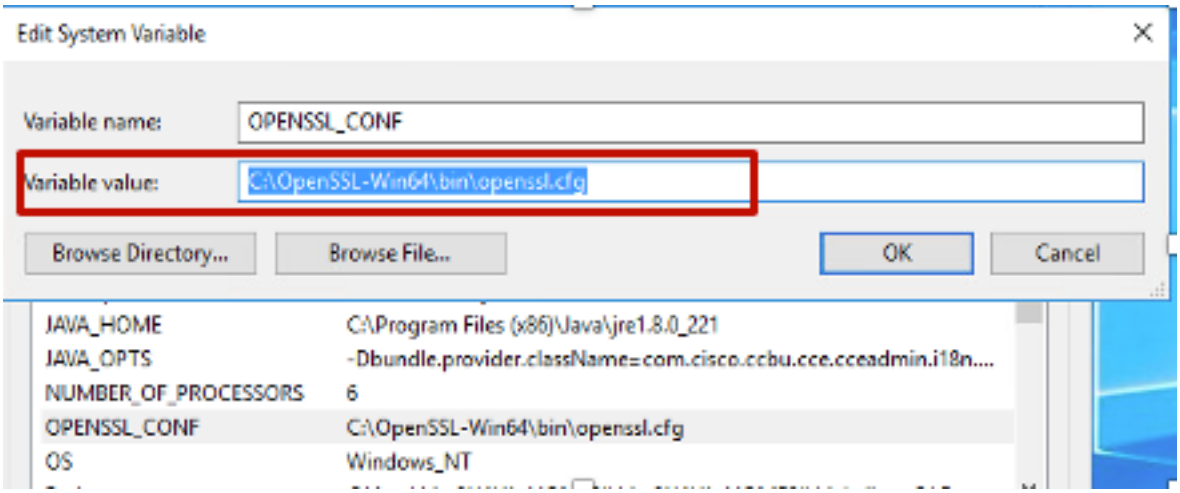
다운로드한 ISO 확인

Cisco에서 서명한 다운로드된 ISO를 검증하고 인증되었는지 확인하려면 다음 단계를 수행하십시오.

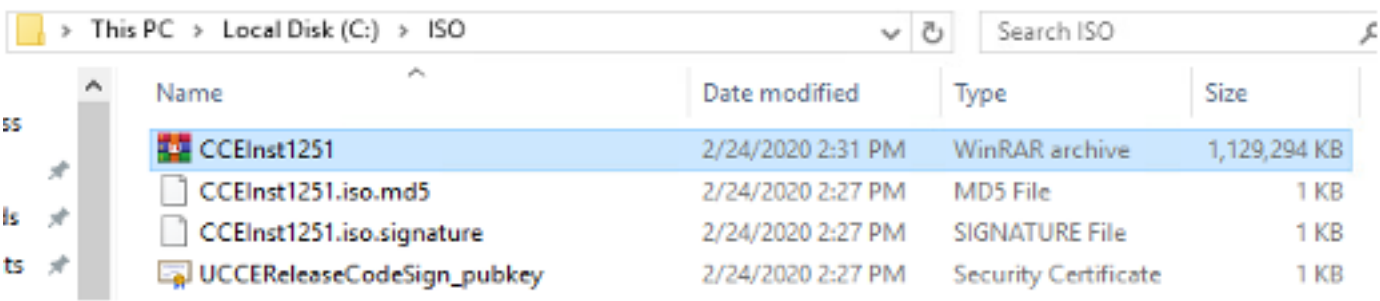
1. OpenSSL을 다운로드하고 설치합니다.소프트웨어 "openssl softpedia"를 검색합니다.



2. 경로를 확인합니다(기본적으로 설정되지만 확인해도 좋습니다). Windows 10에서 시스템 등록 정보로 이동하여 환경 변수를 선택합니다.



3. ISO 확인에 필요한 파일



4. 명령줄에서 OpenSSL 툴을 실행합니다.

5 . 명령 실행

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

6. 오류가 발생할 경우 명령줄에 이미지에 표시된 오류가 표시됩니다.

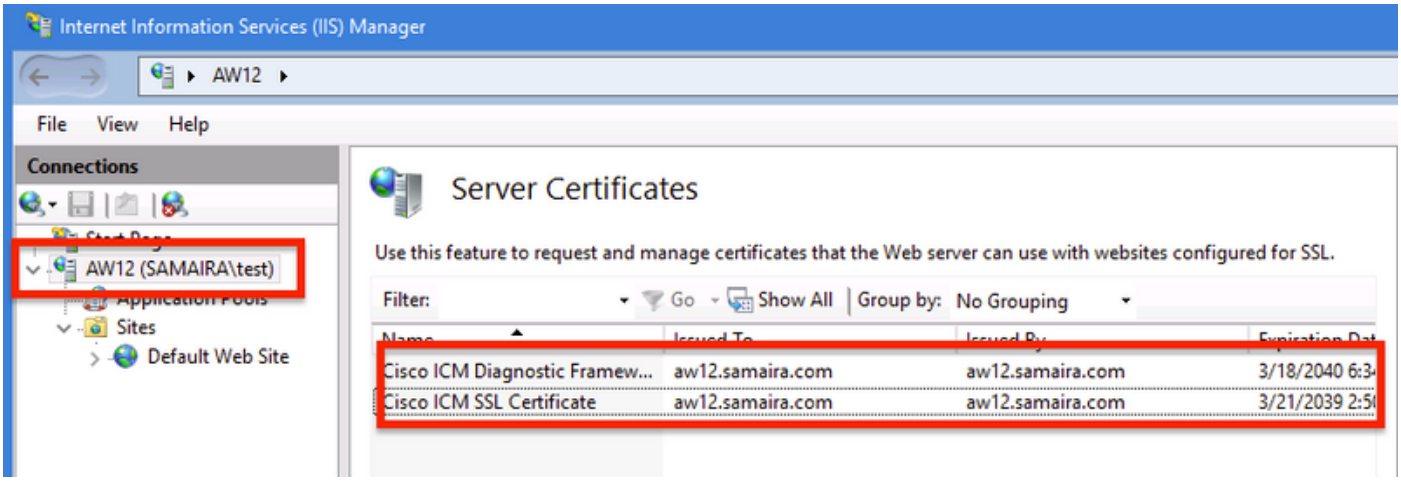
SHA-256 및 키 크기 2048비트의 인증서 사용

비준수 인증서를 식별하는 경우(예: SHA-256 및/또는 키 크기 2048비트 요구 사항을 충족하지 않음) 보고서 오류를 기록합니다.

UCCE의 관점에서는 두 가지 중요한 인증서가 있습니다.

- Cisco ICM 진단 프레임워크 서비스 인증서
- Cisco ICM SSL 인증서

인증서는 Windows 서버의 IIS(인터넷 정보 서비스) 관리자 옵션에서 검토할 수 있습니다.



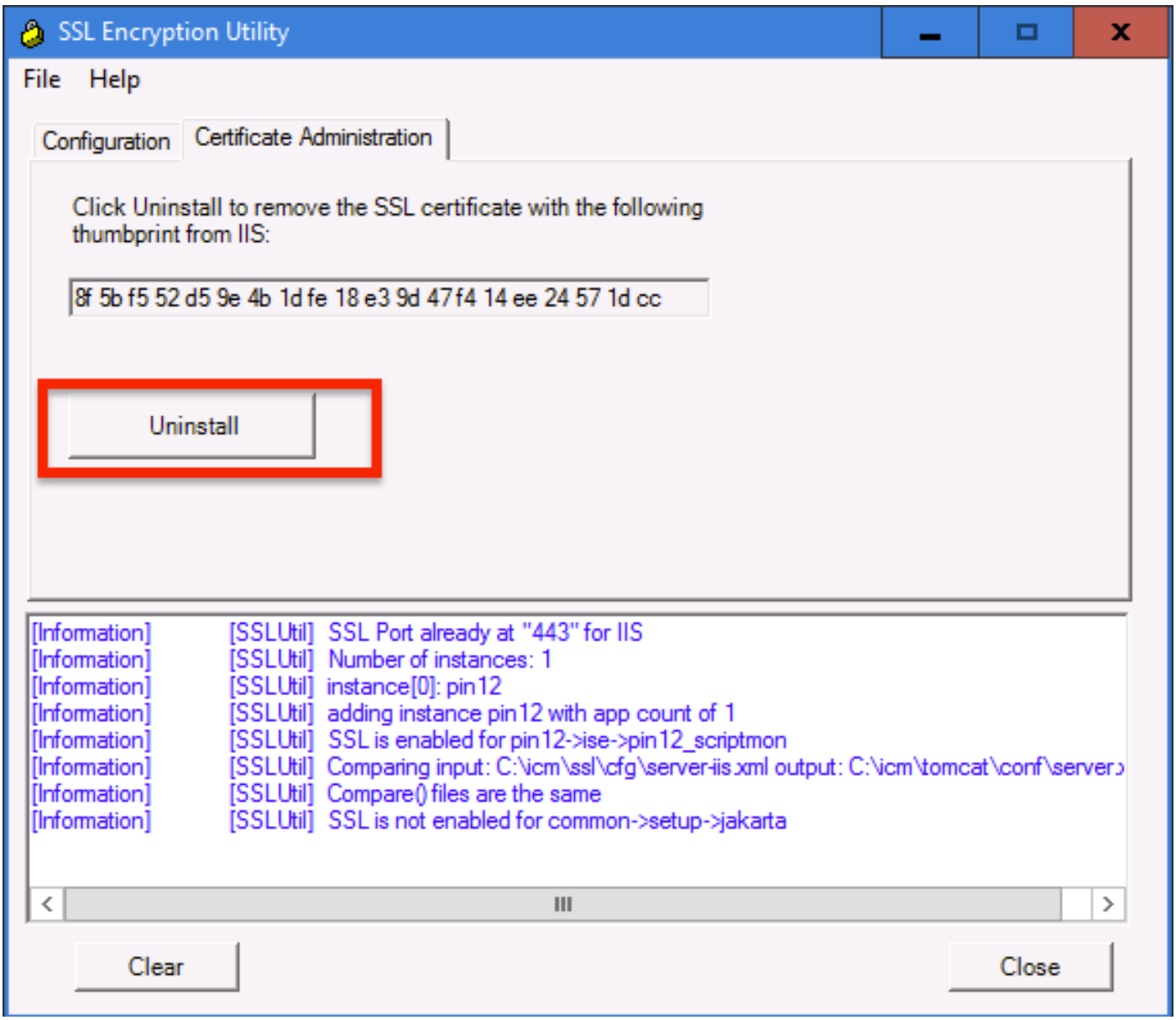
자체 서명 인증서의 경우(Diagnose Portico 또는 Web Setup용), 보고된 오류 라인은 다음과 같습니다.

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

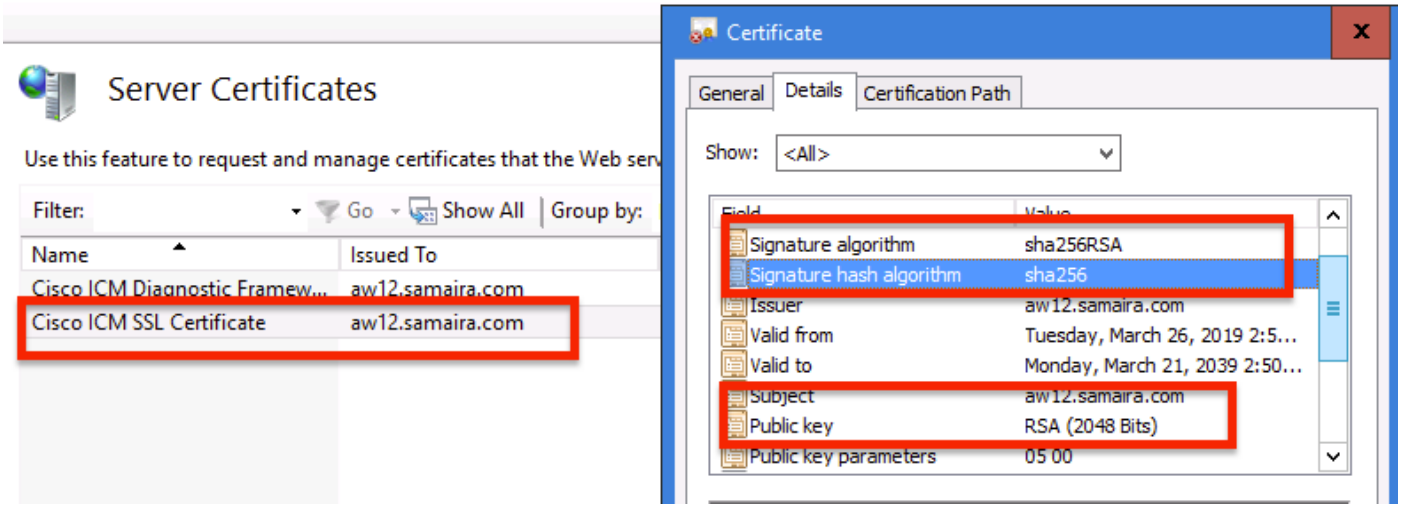
SSLUtil 툴

a.자체 서명 인증서(WebSetup/CCEAdmin 페이지)를 재생성하려면 SSLUtil 툴(C:\icm\bin 위치)을 사용합니다.

b.현재 "Cisco ICM SSL 인증서"를 삭제하려면 제거를 선택합니다.



c. 그런 다음 Install in SSLUtil tool을 선택하고 프로세스가 완료되면 생성된 인증서에 SHA-256 및 키 크기 '2048' 비트가 포함되어 있습니다.



DiagFwCertMgr 명령

Cisco ICM Diagnostic Framework 서비스 인증서에 대해 자체 서명 인증서를 재생성하려면 이미지에 표시된 대로 명령줄 "**DiagFwCertMgr**"을 사용합니다.

```
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>_
```

데이터 보호 툴

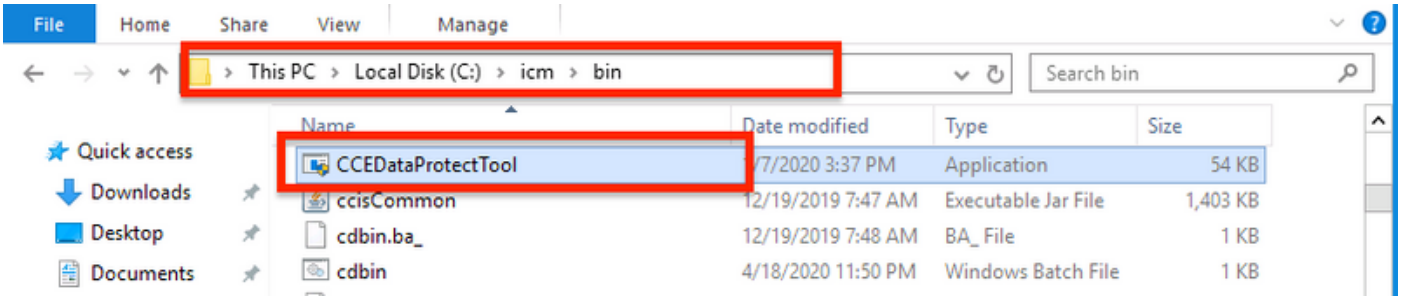
1. CCEDataProtectTool은 Windows 레지스트리가 저장하는 중요한 정보를 암호화하고 해독하는 데 사용됩니다.SQL 12.5로 업그레이드한 후 SQLLogin 레지스트리의 값 저장소를 CCEDataProtectTool로 다시 구성해야 합니다.관리자, 관리자 권한이 있는 도메인 사용자 또는 로컬 관리자만 이 도구를 실행할 수 있습니다.

2. 이 도구를 사용하여 SQLLogin 레지스트리에서 암호화된 값 저장소를 보고, 구성, 편집, 제거할 수 **있습니다**.

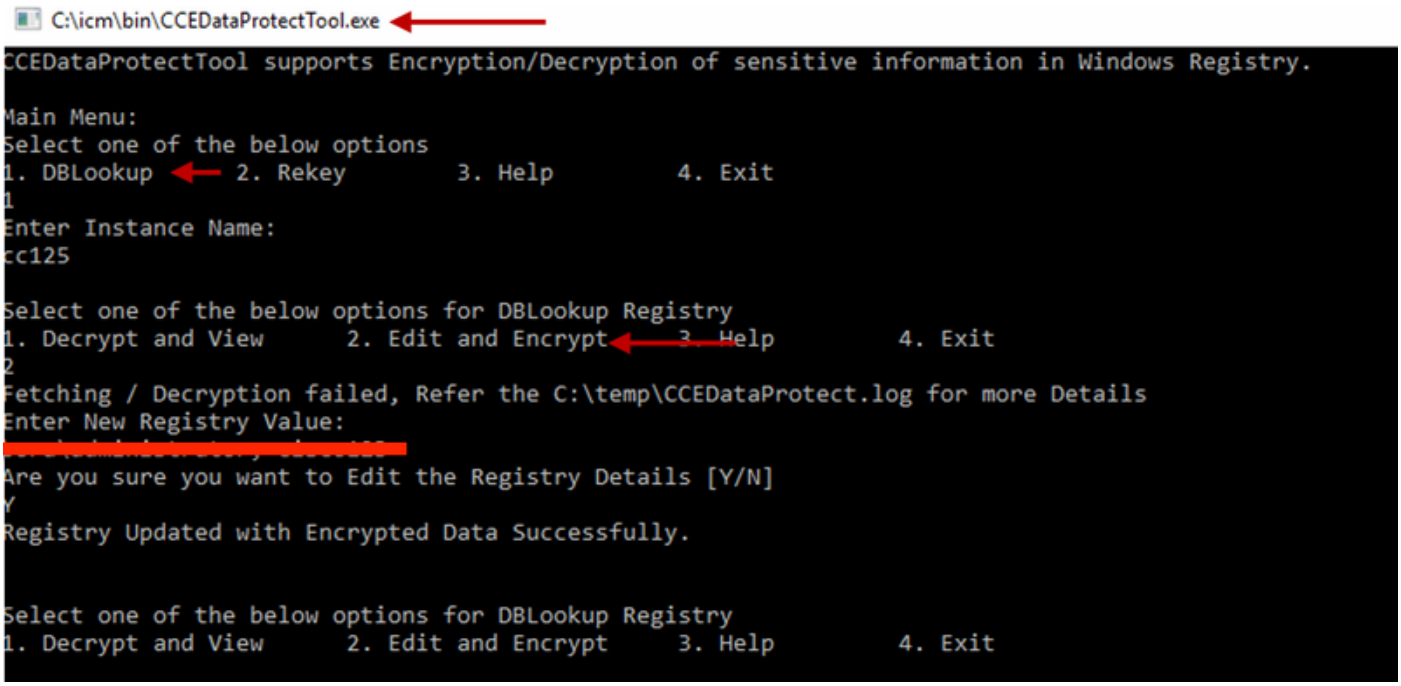
3. 도기가 위치에 있을 것

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

4. 위치로 이동하고 CCEDataProtectTool.exe를 두 번 클릭합니다.

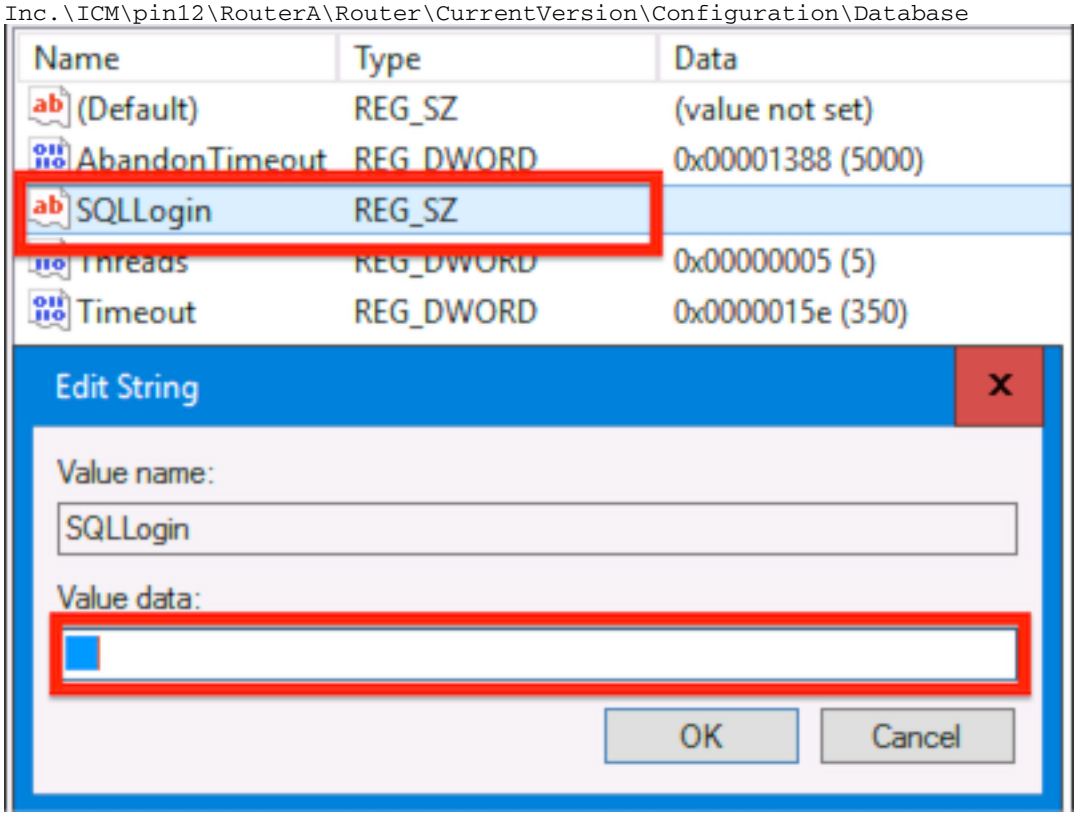


5. 암호화하려면 DBLookup에 대해 1을 누르고 인스턴스 이름을 입력합니다.다음으로, 2를 눌러 "Edit and Encrypt(편집 및 암호화)"를 선택합니다.

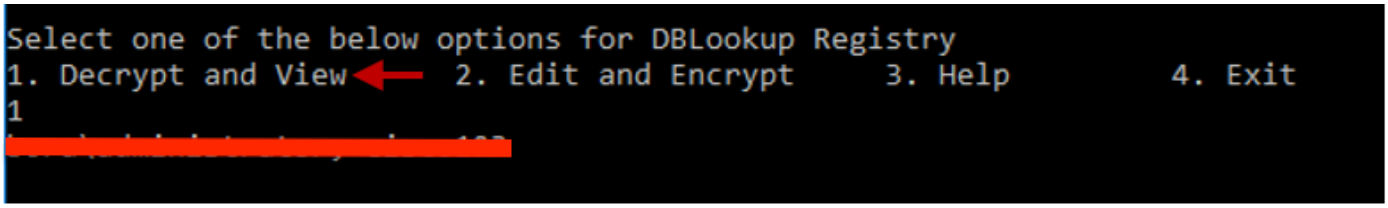


6. 레지스트리 위치로 이동하고 이미지에 표시된 것처럼 문자열 값 **SQLLogin**이 비어 있는 것을 검토합니다.

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



7. 암호화된 가치에 대한 검토가 필요한 경우CCEDataProtectTool의 명령행에서 이미지에 표시된 대로 "Decrypt and View(암호 해독 및 보기)"에 대해 1을 선택합니다.



8. 이 공구에 관한 로그를 위치에 찾을 수 있을 **것**

```
<Install Directory>:\temp

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