Compreenda as melhorias de segurança do UCCE 12.5

Contents

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

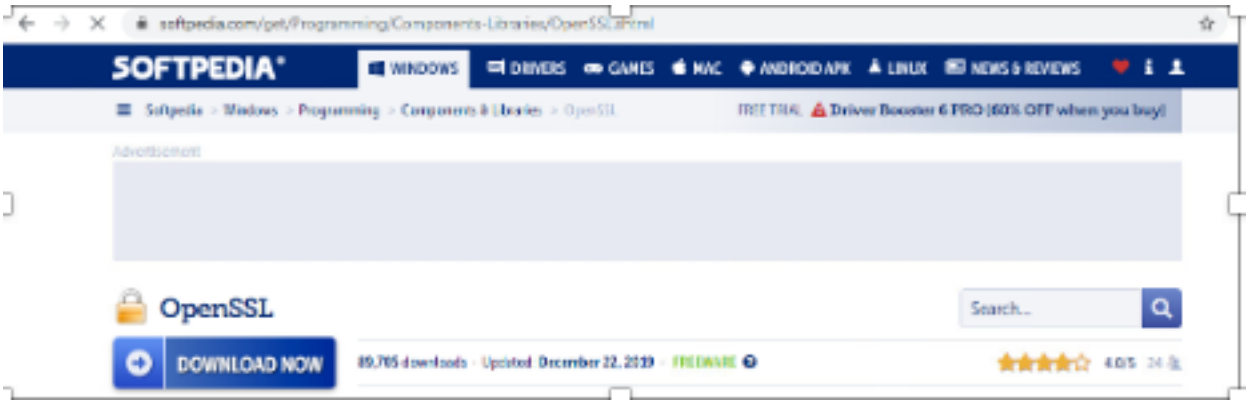
Cisco Security Control Framework (SCF): A estrutura de controle de segurança de colaboração fornece as diretrizes de projeto e implementação para a criação de uma infraestrutura de colaboração segura e confiável. Essas infraestruturas são resilientes a formas conhecidas e novas de ataques. Guia de Segurança 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.

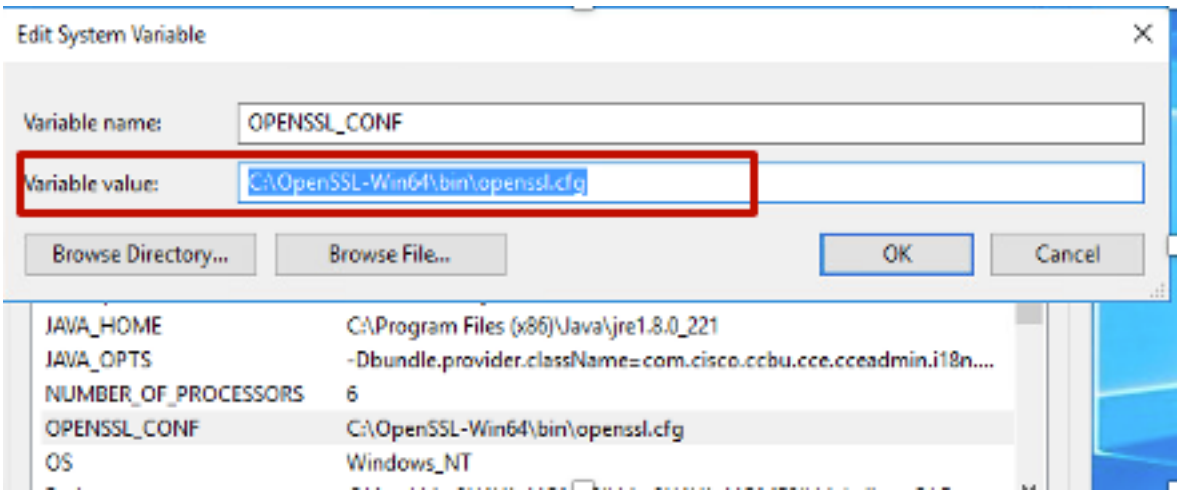
Verificação da ISO baixada

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

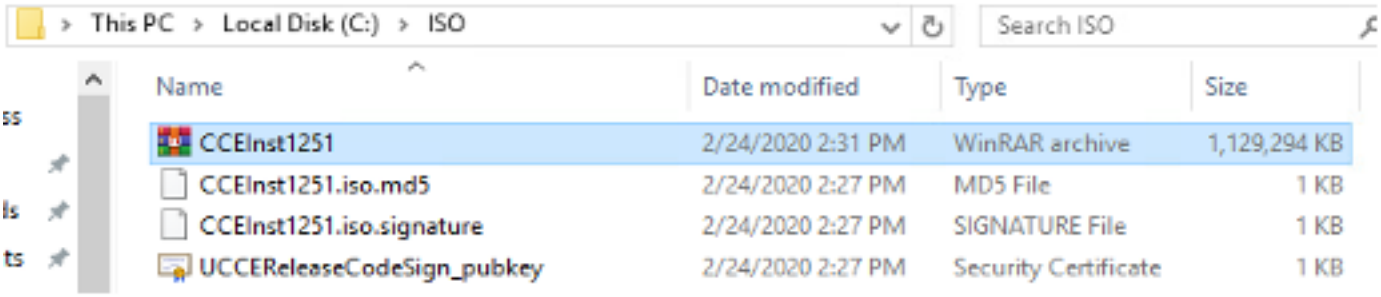
1. Baixe e instale o OpenSSL. Procure por software "openssl softpedia".



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



4. Execute a ferramenta OpenSSL a partir da linha de comando.

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

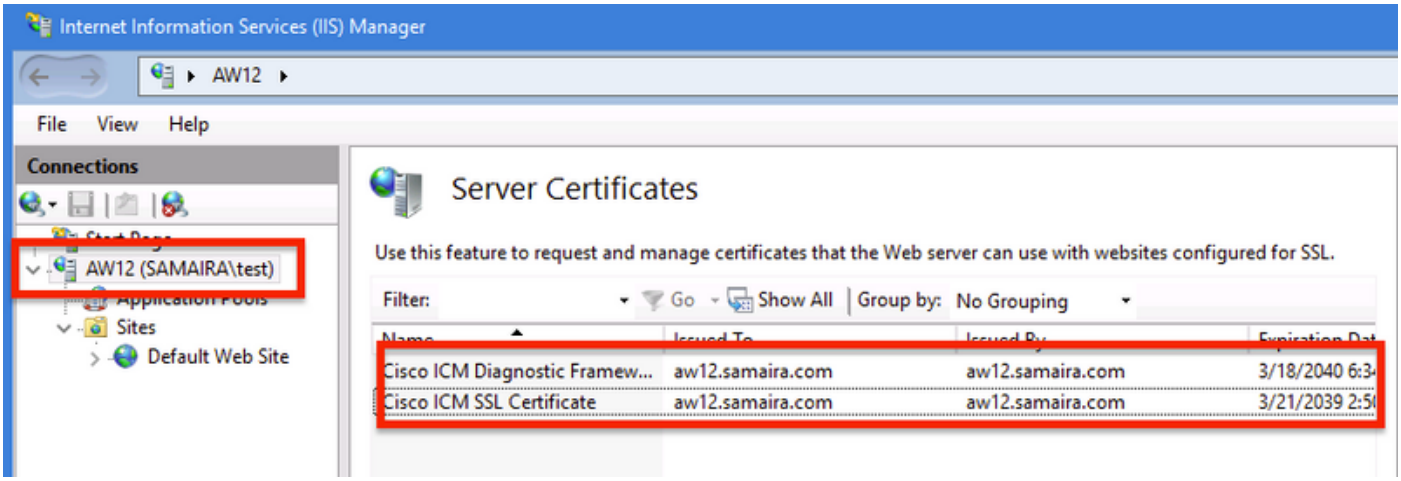
Usar certificados com SHA-256 e tamanho de chave 2048 bits

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.



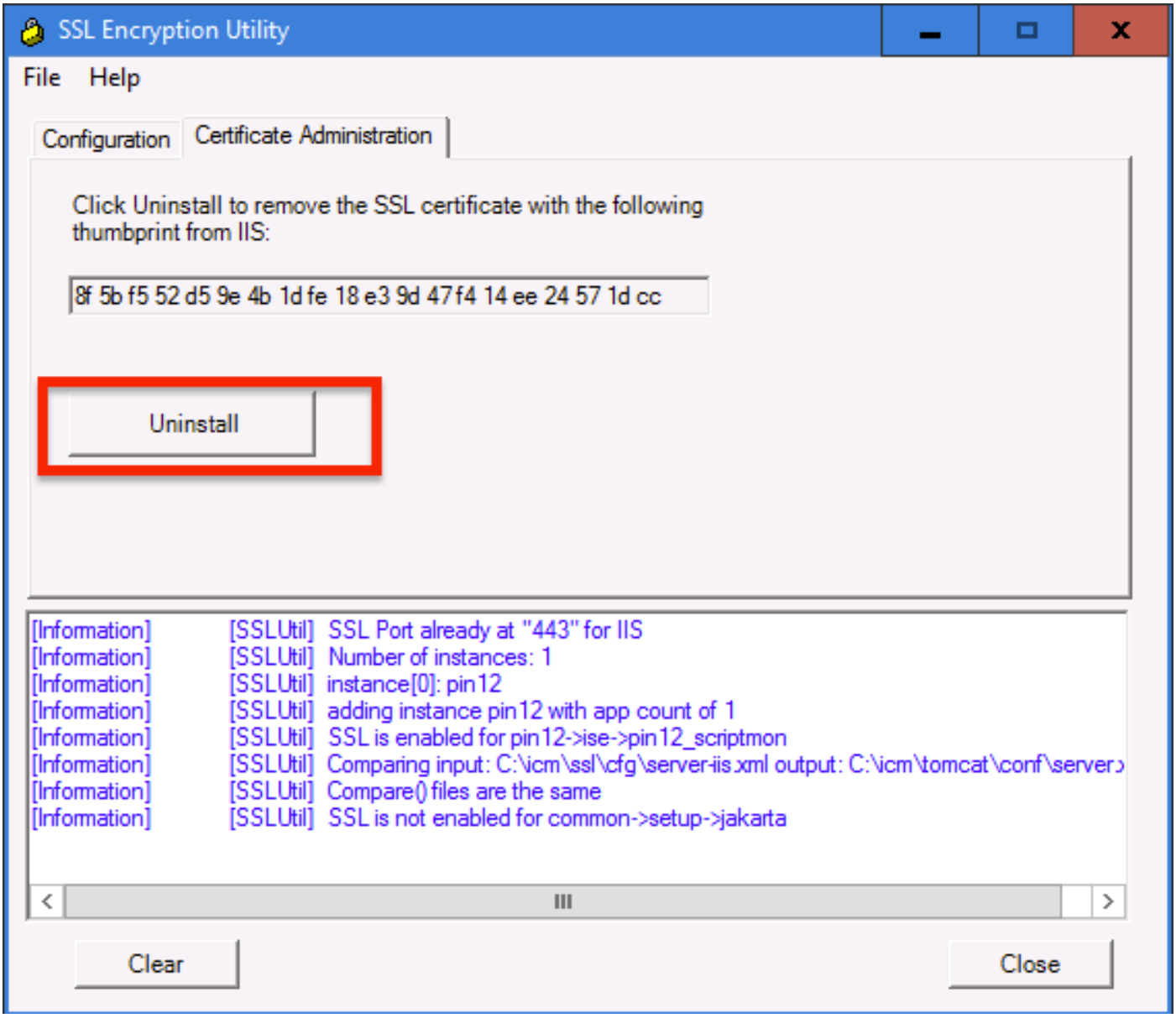
Para certificados autoassinados (para Diagnose Portico ou Configuração da Web) , a linha de erro reportada é:

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

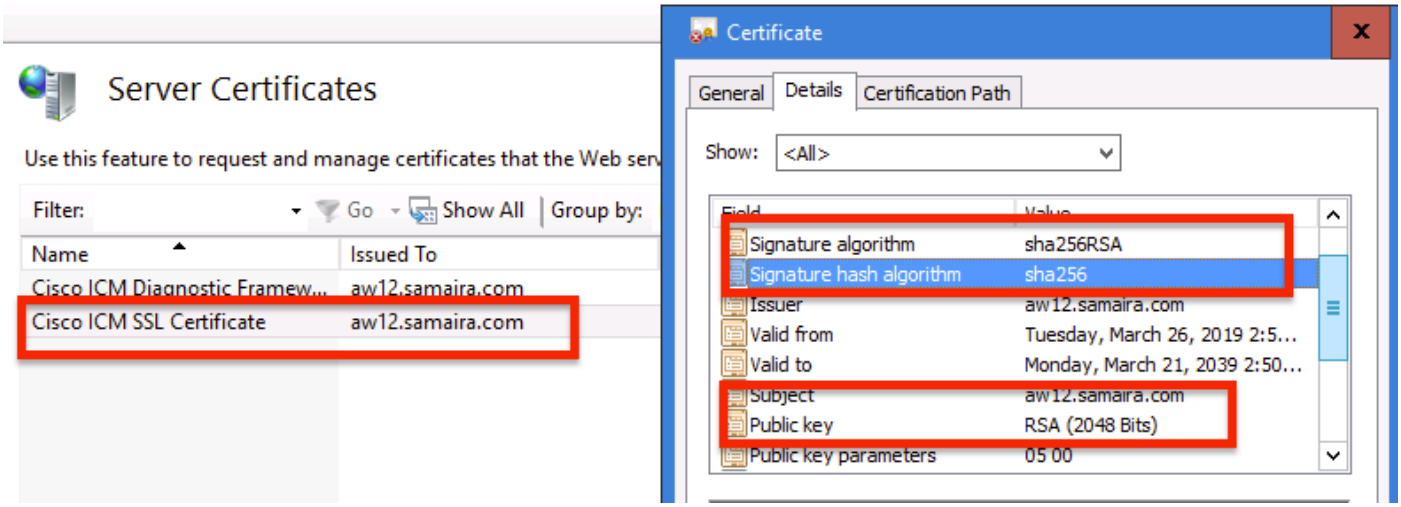
Ferramenta SSLUtil

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

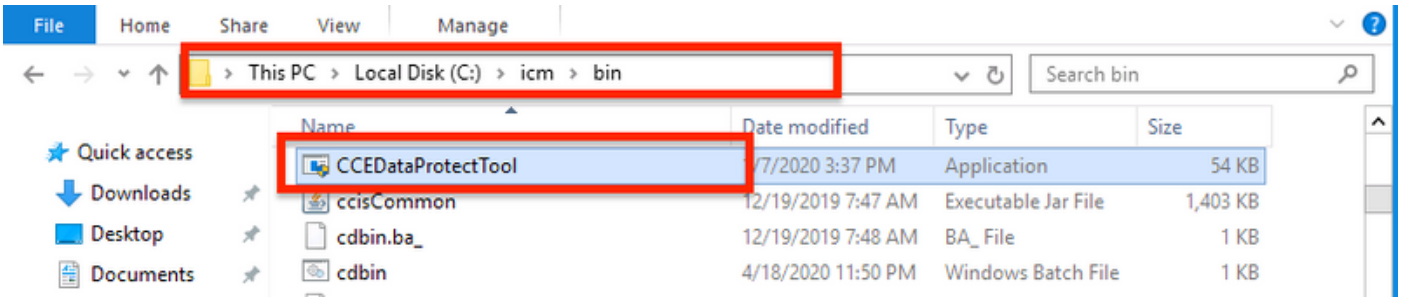
1. CCEDataProtectTool é usado para criptografar e descriptografar informações confidenciais que o registro do Windows armazena nele. Após a atualização para SQL 12.5 , o armazenamento de valores no registro **SQLLogin** precisa ser reconfigurado com CCEDataProtectTool. Somente administrador, usuário 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**.

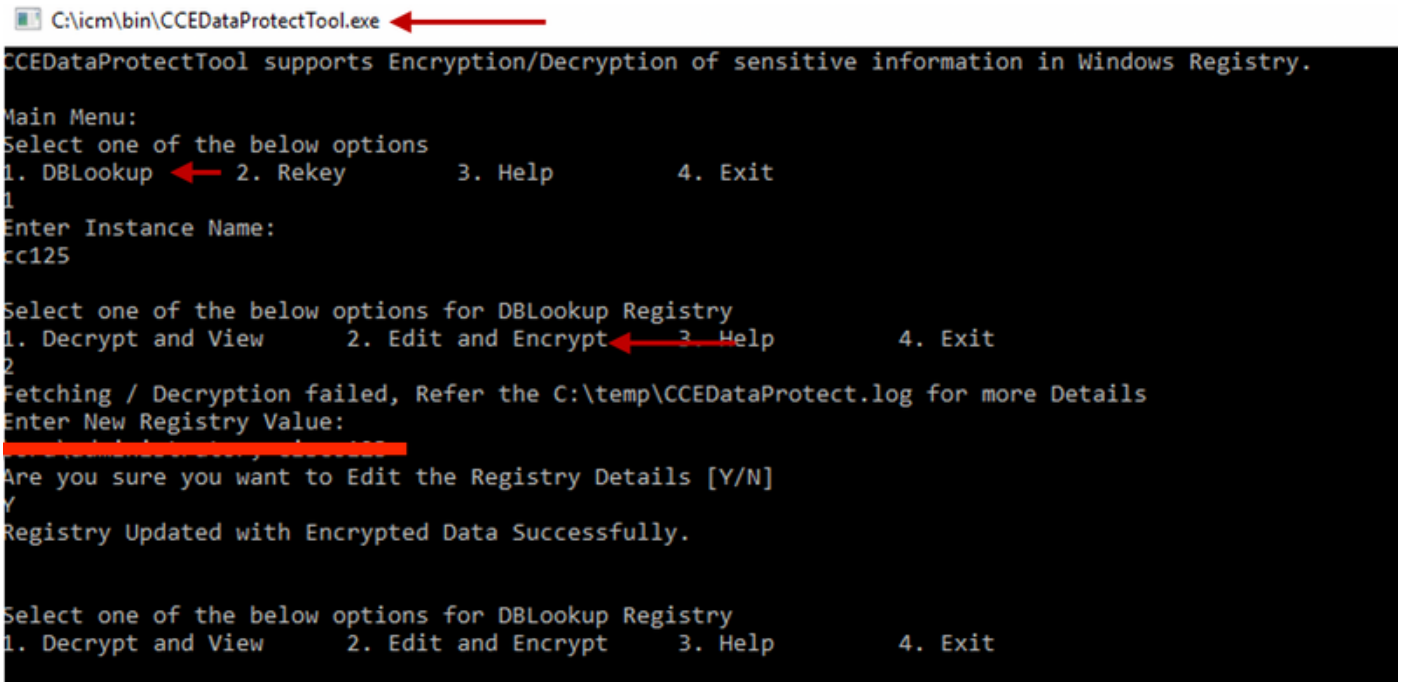
3. A ferramenta está no local;

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

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

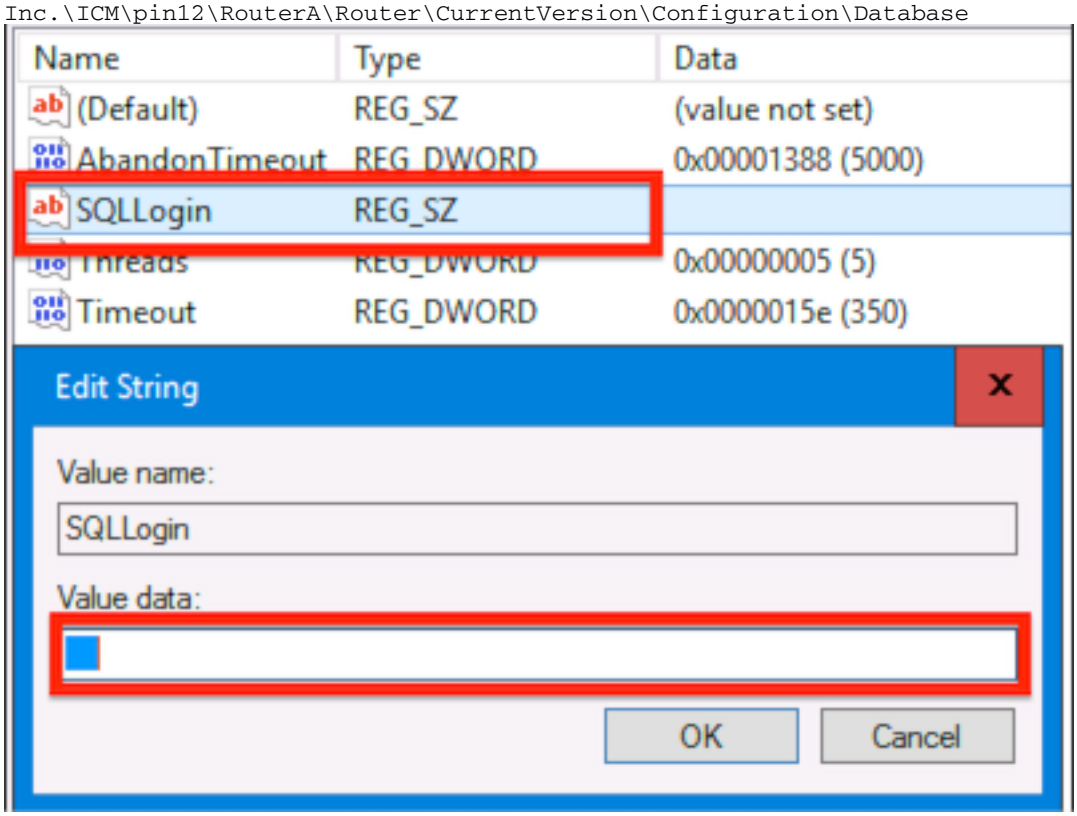


5. Para criptografar , pressione 1 para DBLookup, insira Instance Name (Nome de instância). Em seguida, pressione 2 para selecionar "Edit and Encrypt" (Editar e criptografar)

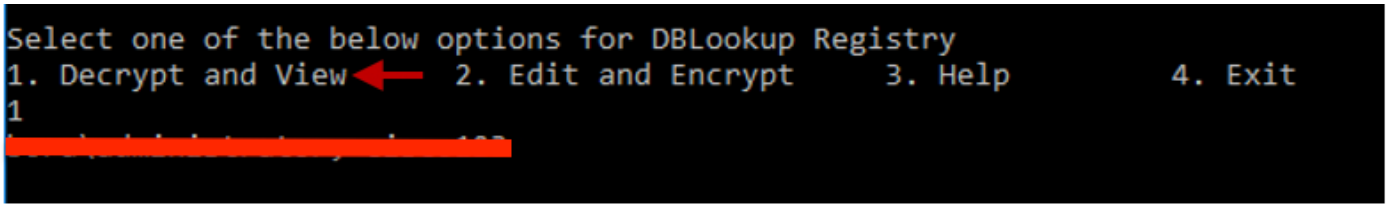


6. Navegue até o local do registro e reveja o **SQLLogin do** valor da string parece em branco , como mostrado na imagem :

```
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 CCEDataProtectTool , selecione pressionar 1 para "Descriptografar e visualizar", como mostrado na imagem;



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

```
<Install Directory>:\temp

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