Compreenda aprimoramentos de segurança UCCE 12.5

Índice

Introdução

Este original descreve sobre os aprimoramentos de segurança os mais atrasados adicionados com empresa unificada do Contact Center (UCCE) 12.5.

Pré-requisitos

- UCCE
- Abra o secure sockets layer (o SSL)

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCCE 12.5
- Abra o SSL

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- UCCE 12.5
- OpenSSL (64 mordidos) para indicadores

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

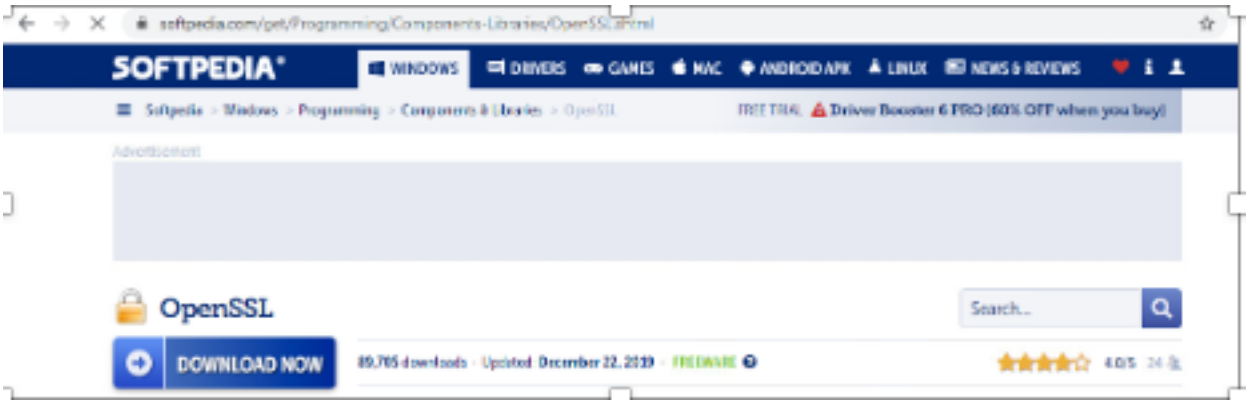
Estrutura de controle do Cisco Security (SCF): A estrutura do controle de segurança da Colaboração fornece o projeto e as diretrizes de implementação construindo infra-estruturas seguras e seguras da Colaboração. Estas infra-estruturas são resilientes aos formulários conhecidos e novos dos ataques. O guia da Segurança da referência para Cisco unificou a empresa do centro ICM/Contact, a liberação 12.5.

Como parte da segurança adicional do esforço SCF de Cisco os realces são adicionados para UCCE 12.5. Este original esboça estes realces.

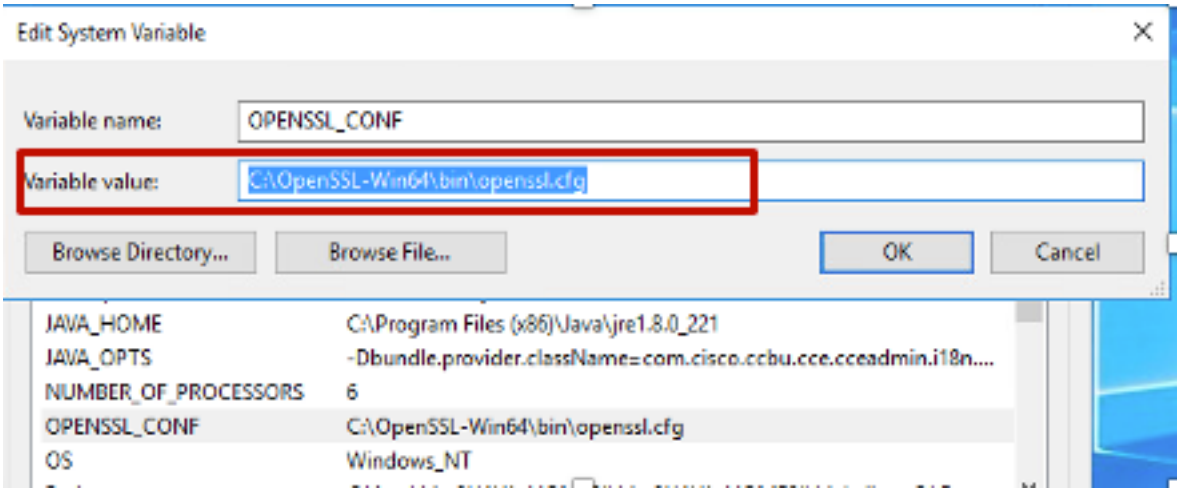
Verificação do ISO transferido

A fim validar o ISO transferido assinado por Cisco assim como assegurar-se de que esteja autorizado, as etapas são:

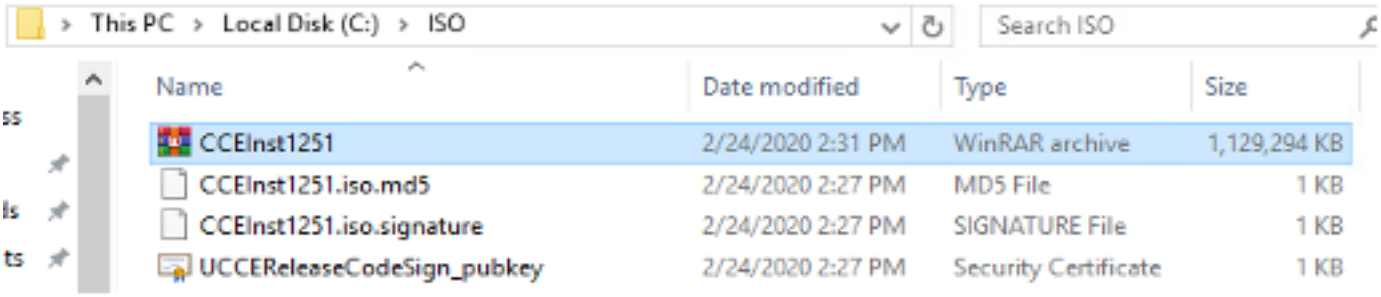
1. Transfira e instale o OpenSSL. Procure pelo software do “softpedia OpenSSL”.



2. Confirme o trajeto (isto é ajustado à revelia, mas ainda bom verificar). Em Windows 10, o sistema empreendedores Propeties, seleciona variáveis de ambiente.



3. Arquivos necessários para a verificação ISO



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

5. Execute o comando

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

6. No caso da falha, a linha de comando mostra o erro segundo as indicações da imagem

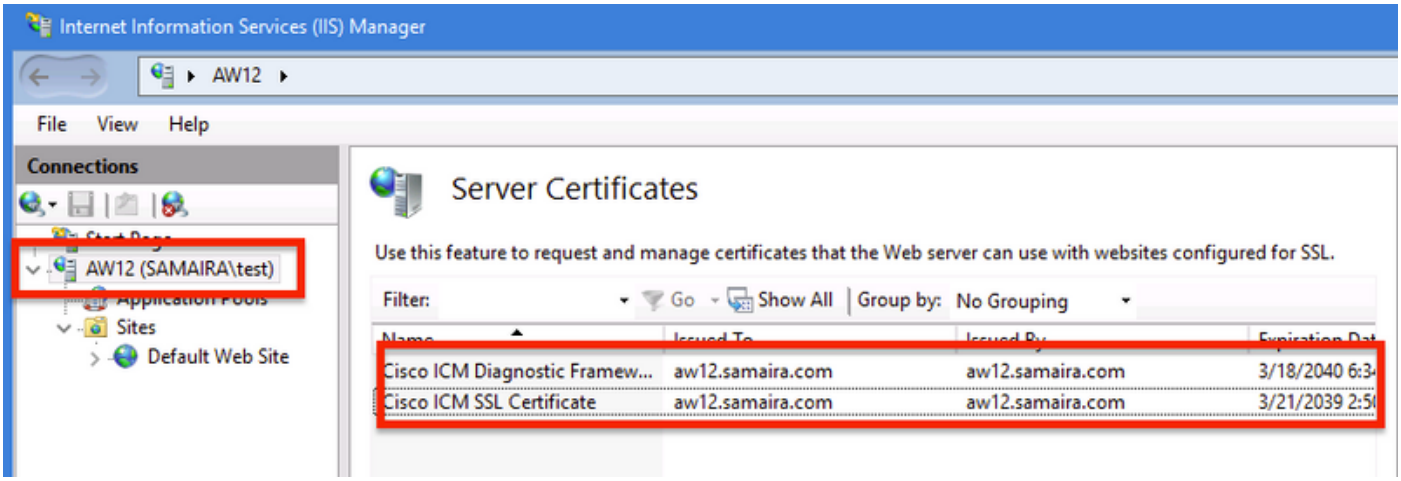
Use Certificados com SHA-256 e bit do tamanho chave 2048

Os logs relatam o erro no caso de identificar Certificados da NON-queixa (isto é não encontrando o SHA-256 e/ou keysize uma exigência de 2048 bit.)

Há dois Certificados importantes da perspectiva de UCCE:

- Certificado diagnóstico do serviço da estrutura de Cisco ICM
- Certificado de Cisco ICM SSL

Os Certificados podem ser revistos na opção do gerente do Internet Information Services (IIS) do server dos indicadores.



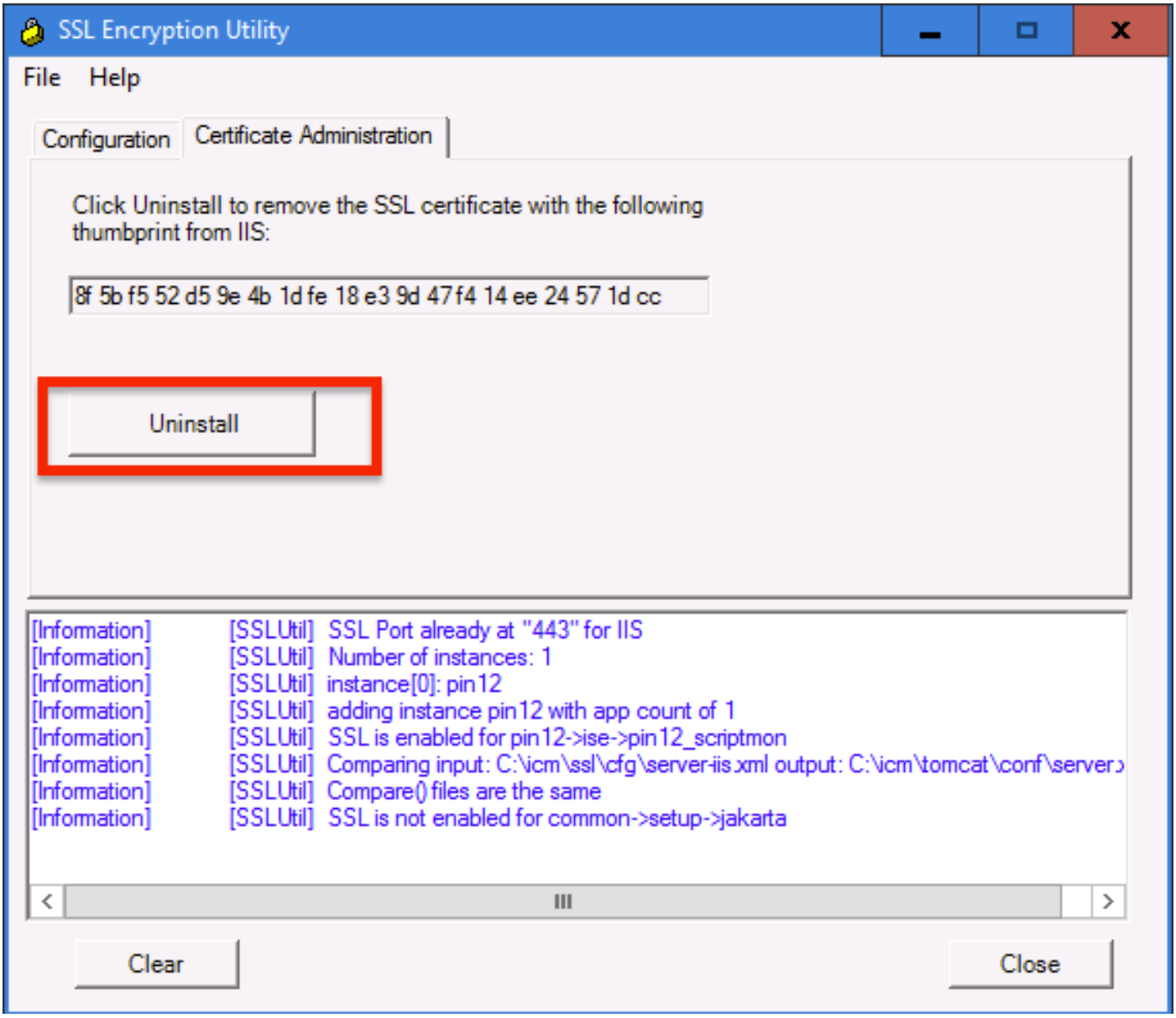
Para certificados auto-assinados (para o pórtico ou a Web Diagnose Setup), a linha do erro relatada é:

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

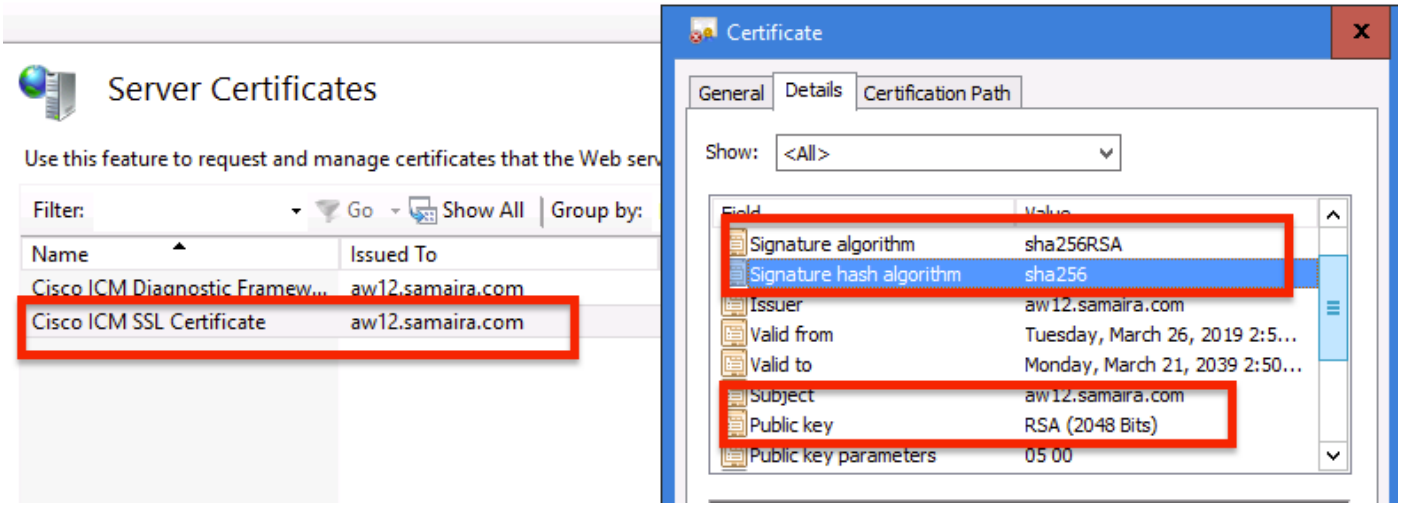
Ferramenta de SSLUtil

a. A fim regenerar a ferramenta de SSLUtil do uso dos certificados auto-assinados (para a página WebSetup/CCEAdmin) (do lugar C:\icm\bin).

b. Seleto desinstale para suprimir de “do certificado atual Cisco ICM SSL”.



c. Em seguida seleto instale na ferramenta de SSLUtil e uma vez que o processo termina, observe o certificado criado agora para incluir o SHA-256 e keysize bit '2048'.



Comando de DiagFwCertMgr

A fim regenerar um certificado auto-assinado para o certificado diagnóstico do serviço da

estrutura de Cisco ICM, use a linha de comando “**DiagFwCertMgr**”, segundo as indicações da 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 da proteção de dados

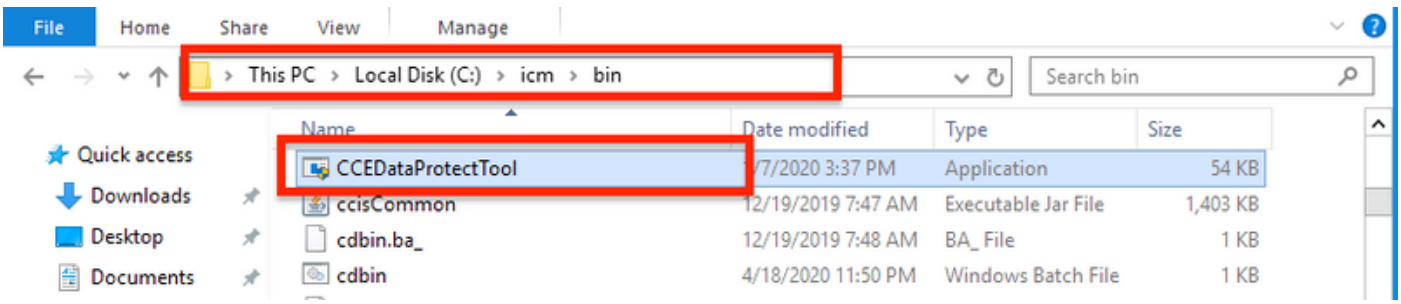
1. CCEDataProtectTool é usado para cifrar e decifrar a informação sensível que o registro de Windows armazena nele. Afixe a elevação a SQL 12.5, loja do valor na necessidade do registro de **SQLLogin** de ser reconfigurado com CCEDataProtectTool. Somente o administrador, o usuário de domínio com direitos administrattive, ou um administrador local podem executar esta ferramenta.

2. Esta ferramenta pode ser usada para ver, configura, edita, remove a loja do valor cifrado no registro de **SQLLogin**.

3. A ferramenta é encontrada no lugar;

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

4. Navegue ao lugar e fazer duplo clique CCEDataProtectTool.exe.

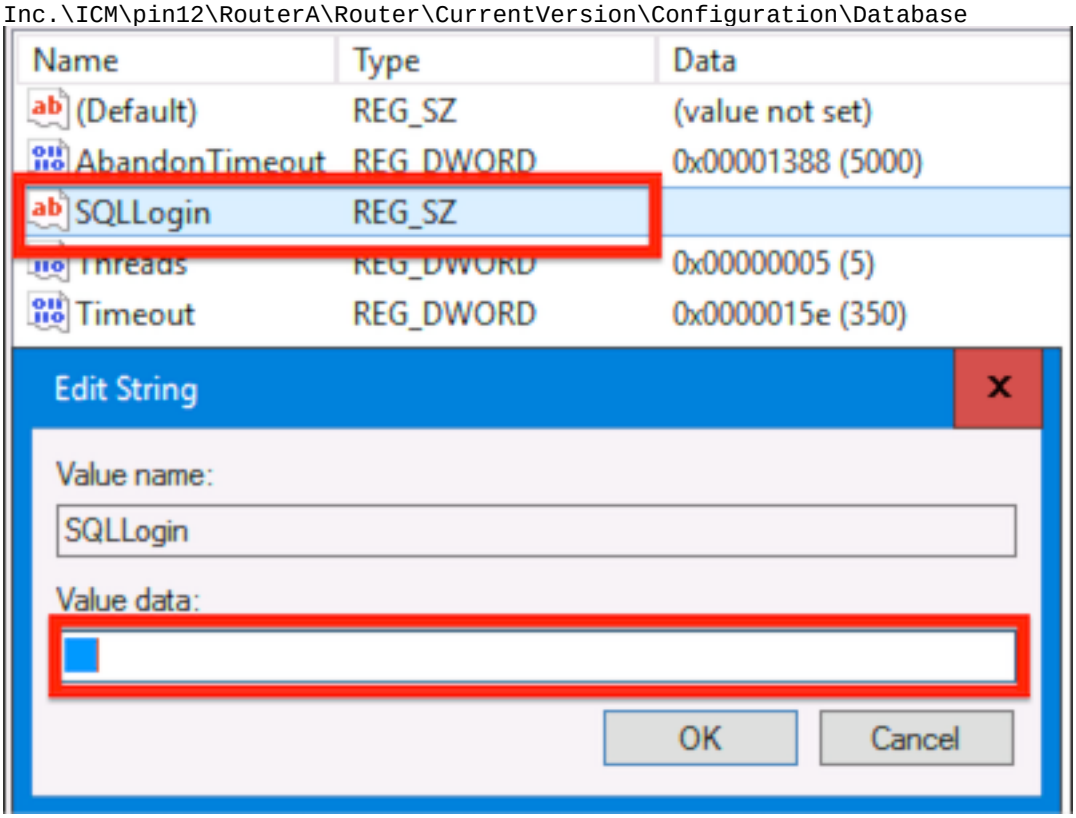


5. A fim cifrar, pressione 1 para DBLookup, dão entrada com o nome de instância. Em seguida, pressione 2 para selecionar “editam e cifram”

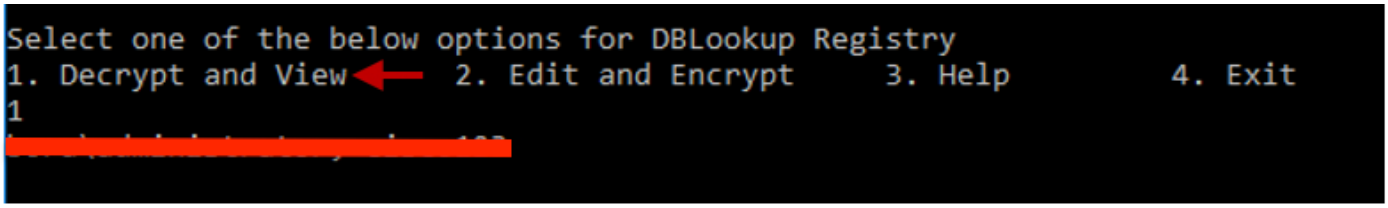
```
C:\icm\bin\CCEDataProtectTool.exe
CCEDataProtectTool supports Encryption/Decryption of sensitive information in Windows Registry.

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. Navegue ao lugar do registro e à placa dos olhares de **SQLLogin do** valor de série da revisão, segundo as indicações da imagem:

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



7. Em caso de necessidade para rever o valor cifrado; quando linha de comando de CCEDataProtectTool, imprensa seleta 1 para o “Decrypt e a vista”, segundo as indicações da imagem;



8. Todos os logs para esta ferramenta podem ser encontrados no lugar;

```
<Install Directory>:\temp

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