Verbeteringen in UCS 12.5 security

Inhoud

Inleiding

Dit document beschrijft de nieuwste beveiligingsverbeteringen die worden toegevoegd aan Unified Contact Center Enterprise (UCCE) 12.5.

Voorwaarden

- UCCES
- Open Secure Socket Layer (SSL)

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- UCS E12.5
- Open SSL

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- UCS E12.5
- OpenSSL (64-bits) voor Windows

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

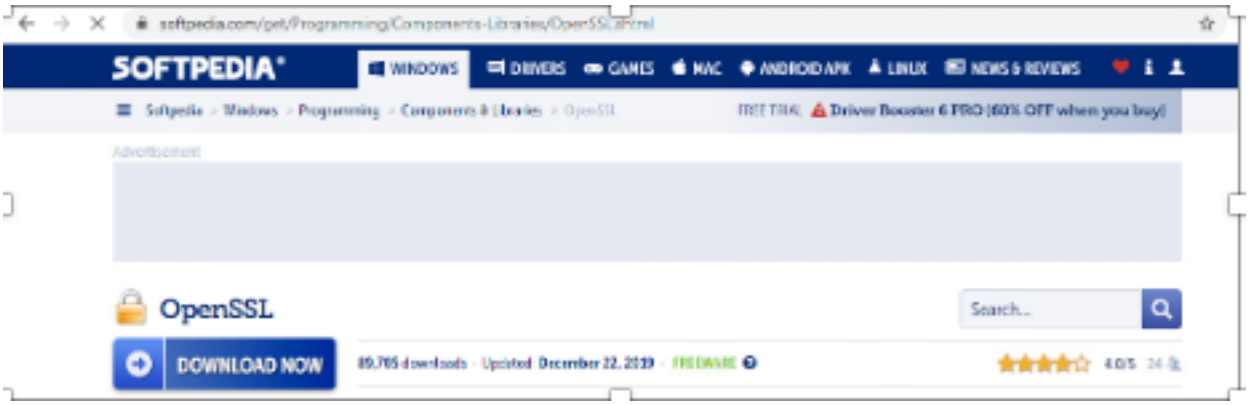
Cisco Security Control Framework (SCF) : Het Collaboration Security Control Framework biedt de ontwerp- en implementatierichtlijnen voor het bouwen van een veilige en betrouwbare samenwerkingsinfrastructuur. Deze infrastructuur is veerkrachtig tegen zowel bekende als nieuwe vormen van aanvallen. Referentiegids voor Cisco Unified ICM/Contact Center Enterprise, release 12.5.

Als deel van Cisco SCF wordt de moeite genomen extra veiligheidsverbeteringen voor UCCE 12.5 toegevoegd. Dit document schetst deze verbeteringen.

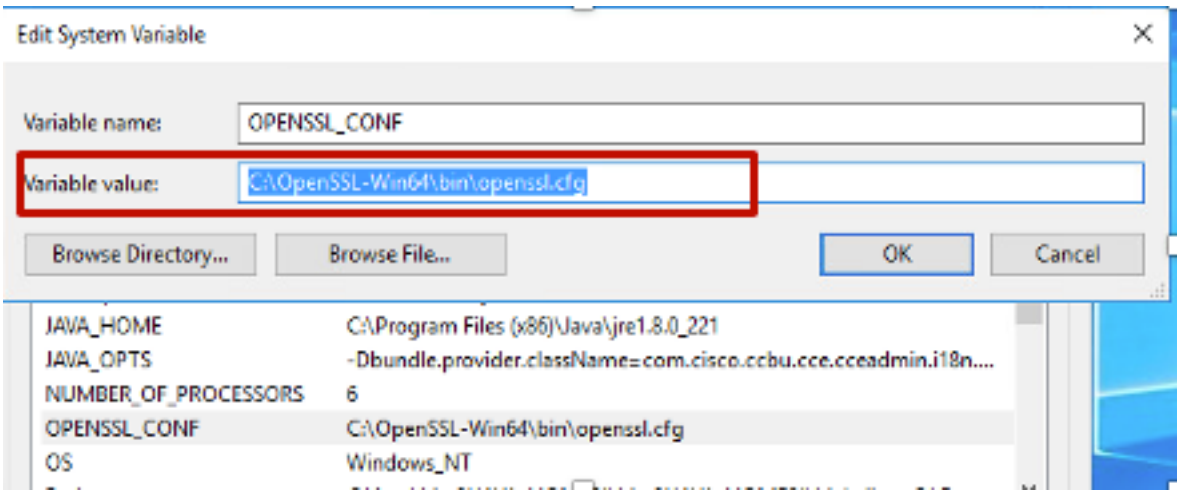
Verificatie van gedownloade ISO

Om de gedownload ISO te valideren die door Cisco is ondertekend en om te waarborgen dat deze is geautoriseerd, worden de volgende stappen gevolgd:

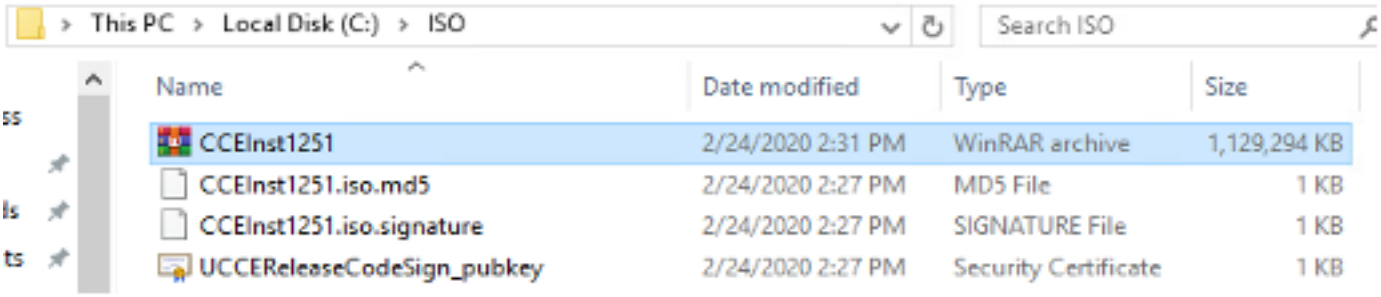
1. Download en Installeer OpenSSL. Zoek naar software "openssl software".



2. Bevestig het pad (dit wordt standaard ingesteld, maar toch goed te controleren). Selecteer in Windows 10 de optie Systeemeigenschappen en selecteer Omgevingsvariabelen.



3. Bestanden die nodig zijn voor de ISO-verificatie



4. Start het OpenSSL-gereedschap vanuit de opdrachtregel.

5. Draai de opdracht

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

6. In het geval van een defect toont de opdrachtregel de fout zoals in de afbeelding

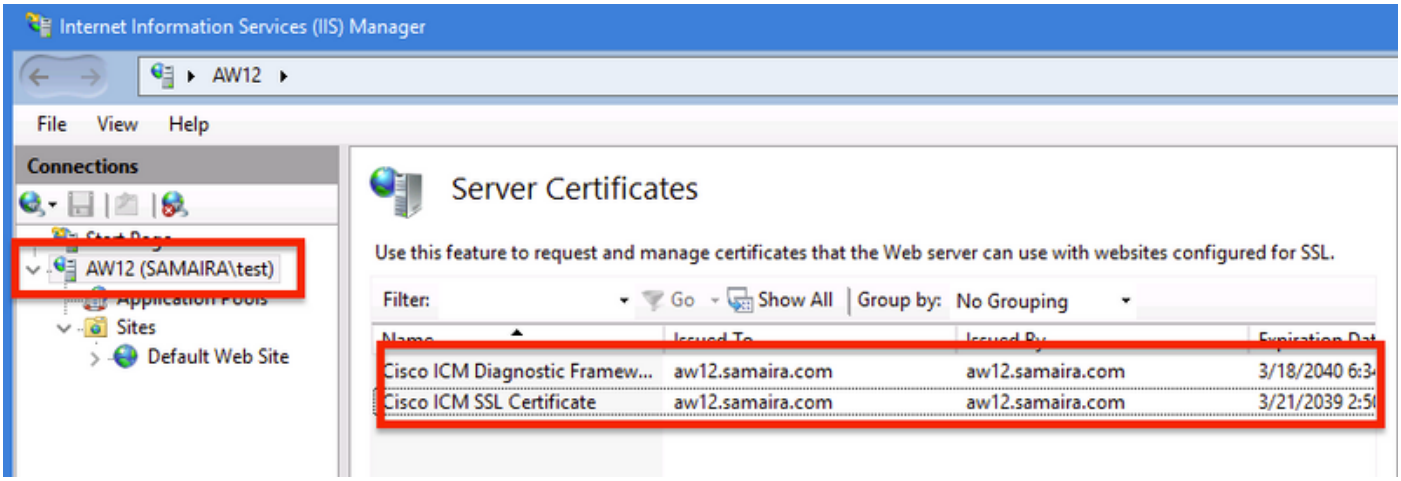
Gebruik certificaten met een SHA-256- en een Key Size-formaat 2048-bits

Logs rapporteert fout bij identificatie van niet-klacht certificaten (d.w.z. niet voldoen aan de SHA-256- en/of de 2048-bits-eis handhaven).

Er zijn twee belangrijke certificaten vanuit het perspectief van UCCE:

- Cisco ICM diagnostisch kaderservicecertificaat
- Cisco ICM SSL-certificaat

De certificaten kunnen worden herzien in de optie Internet Information Services (IS) Manager van Windows server.



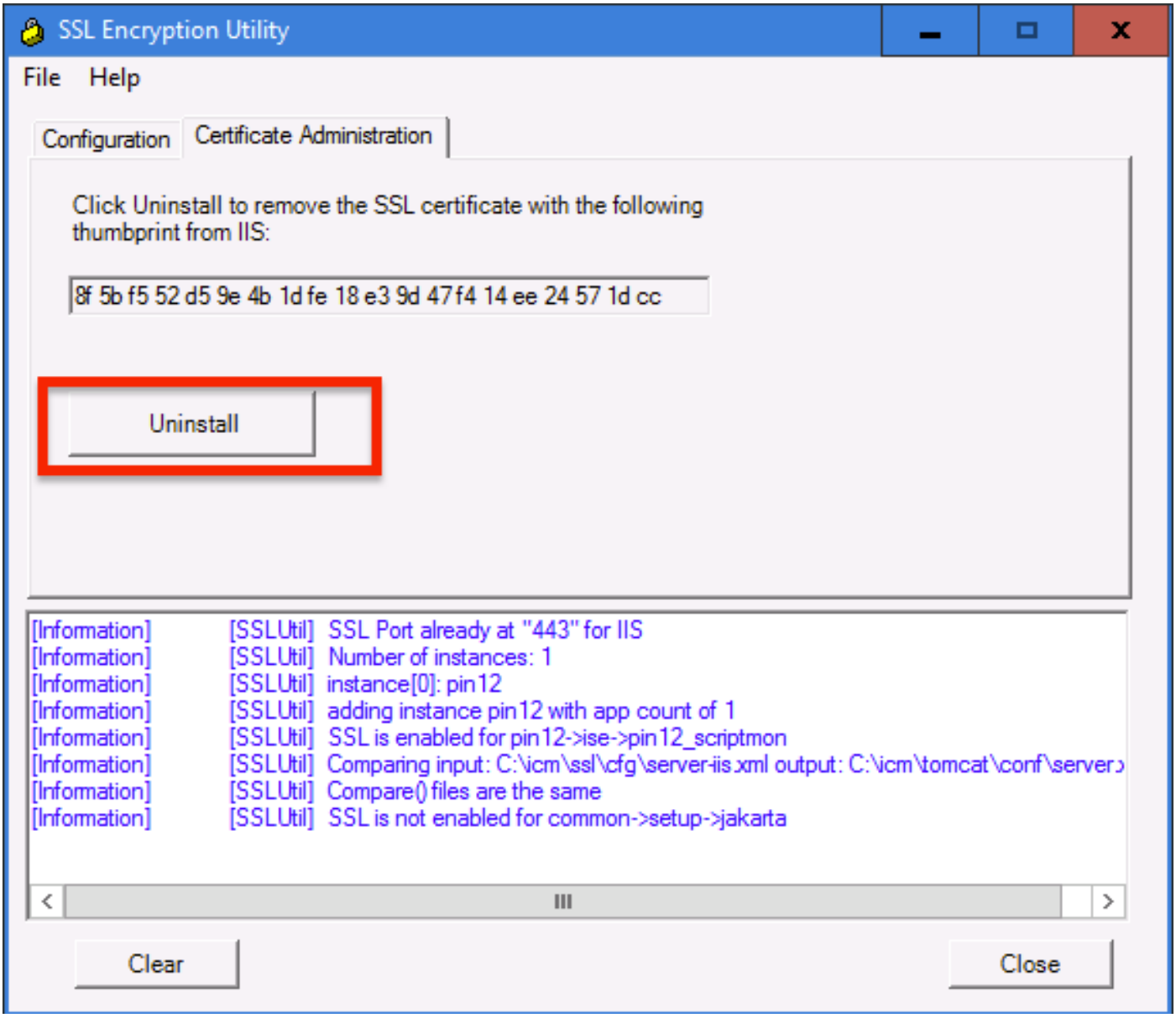
Voor zelfgetekende certificaten (voor Diagnose Portico of Web Setup) is de gerapporteerde foutregel:

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

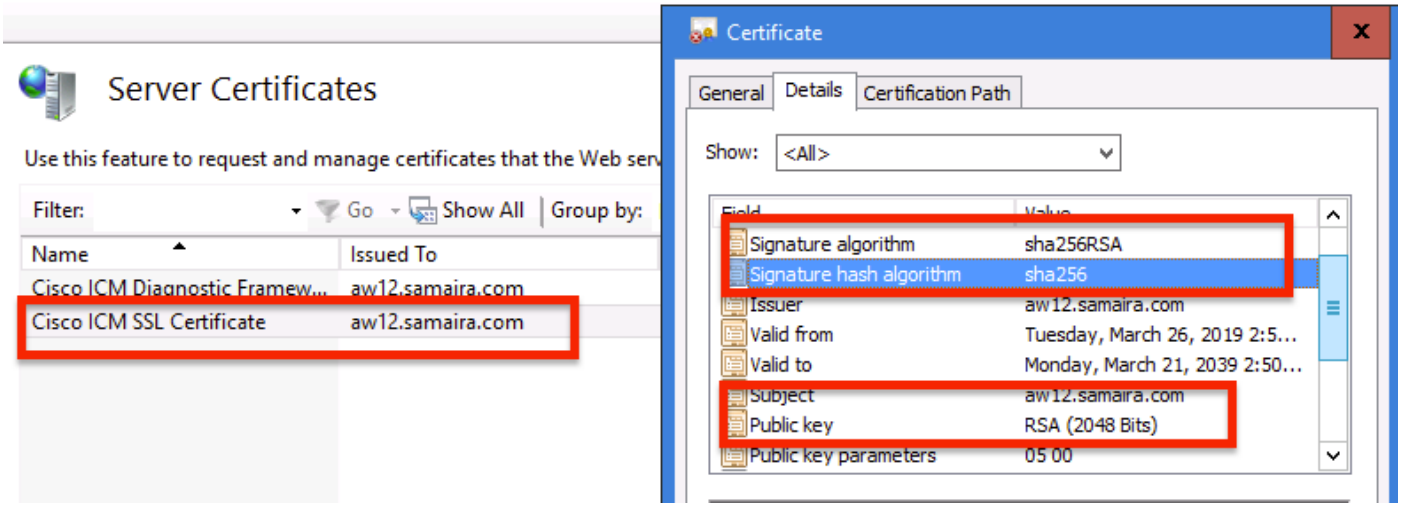
SNELLE FUNCTIE

a. Om zelf-ondertekende certificaten te regenereren (voor WebSetup/CEAdmin pagina) gebruikt u het gereedschap SLB (vanaf locatie C:\icm\bin).

b. Selecteer Verwijderen om het huidige "Cisco ICM SSL-certificaat" te verwijderen.



c. Selecteer vervolgens Installeer in de bestandsindeling en zodra het proces is voltooid, merk het certificaat dat nu is gemaakt op SHA-256 en controleer de '2048'-bits.



Opdracht DiagFwCertMgr

Om een zelf-ondertekend certificaat voor Cisco ICM diagnostisch Kadercertificaat te regenereren,

gebruikt u de opdrachtregel "**DiagFwCertMgr**", zoals in de afbeelding wordt getoond:

```
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>_
```

Gegevensbeschermingsprogramma

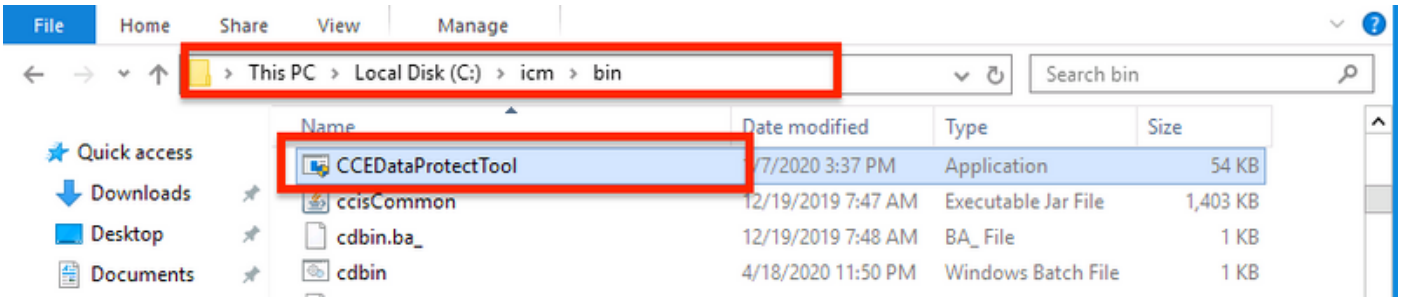
1. CCEDataProtectTool wordt gebruikt om gevoelige informatie te versleutelen en te decrypteren die in het Windows-register opgeslagen wordt. Post upgrade naar SQL 12.5, waardeopslag in de **SQL**-registratie moet opnieuw worden geconfigureerd met CCEDataProtectTool. Alleen een beheerder, een domeingebruiker met administratieve rechten of een lokale beheerder kan dit gereedschap gebruiken.

2. Dit gereedschap kan worden gebruikt om gecodeerde waarde winkel in de Registratie van **het** Sony te bekijken, te configureren,bewerken, **te verwijderen**.

3. Gereedschap wordt op de plaats gevonden;

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

4. Navigeer naar locatie en dubbelklik op CCEDataProtectTool.exe.

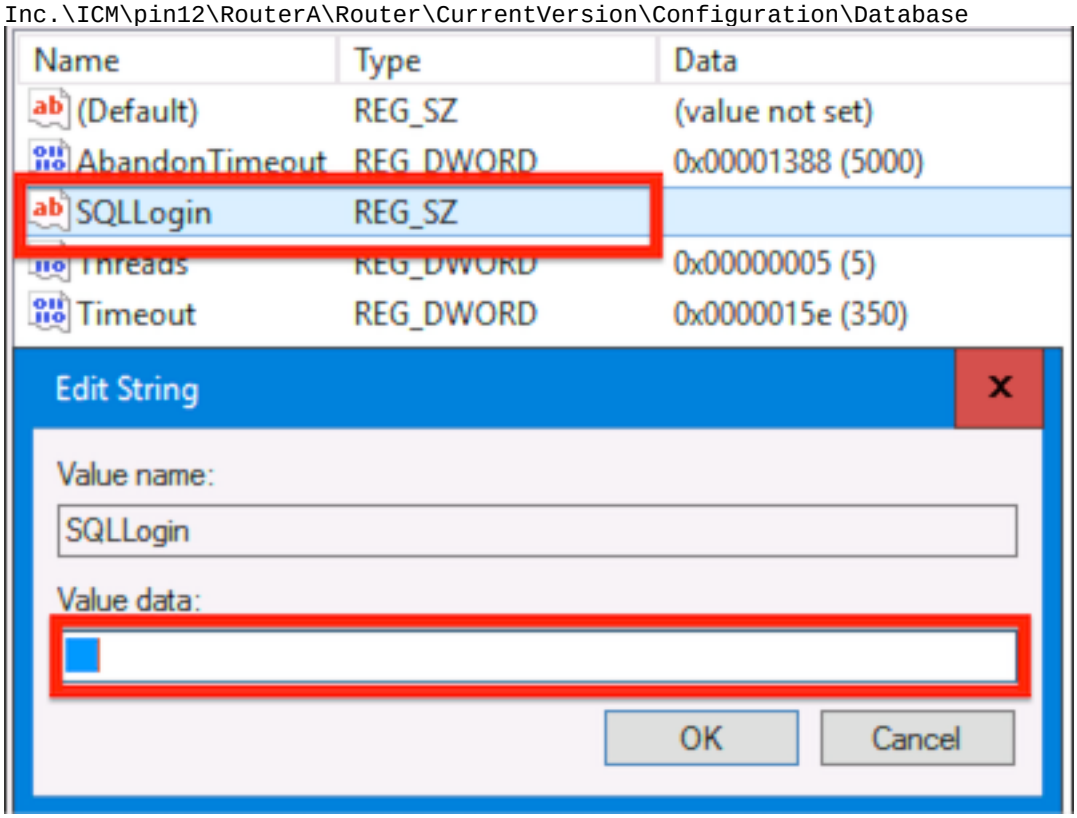


5. Voer de naam van de instantie in om te versleutelen, op 1 voor DBLookup te drukken. Druk vervolgens op 2 om "Bewerken en versleutelen" te selecteren

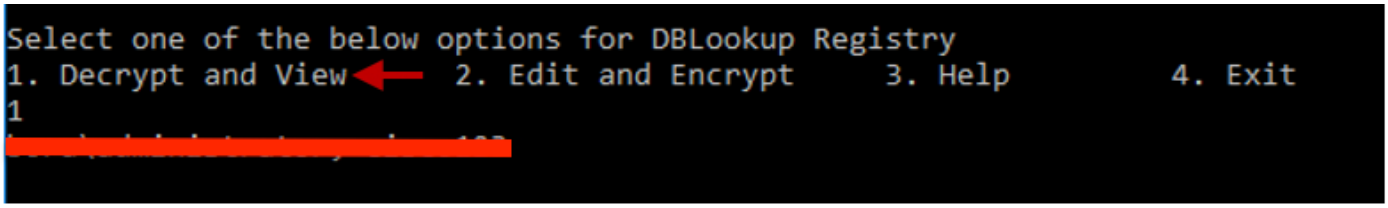
```
C:\icm\bin\CCEDataProtectTool.exe
CCEDataProtectTool supports Encryption/Decryption of sensitive information in Windows Registry.

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. Navigeer naar registratielocatie en revisie string string string string kant-out blanco, zoals getoond in de afbeelding:

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



7. Indien de gecodeerde waarde moet worden herzien; terwijl opdrachtregel van CCEDataProtectTool is ingesteld, selecteert u 1 voor "Decrypt and View", zoals in de afbeelding wordt getoond;



8. Alle logbestanden voor dit gereedschap zijn te vinden op de locatie;

```
<Install Directory>:\temp

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