Comprendre les améliorations de sécurité UCCE 12.5

Contenu

Introduction

Ce document décrit les dernières améliorations apportées à la sécurité avec Unified Contact Center Enterprise (UCCE) 12.5.

Conditions préalables

- UCCE
- Open Secure Sockets Layer (SSL)

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCCE 12.5
- Ouvrir SSL

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- UCCE 12.5
- OpenSSL (64 bits) pour 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

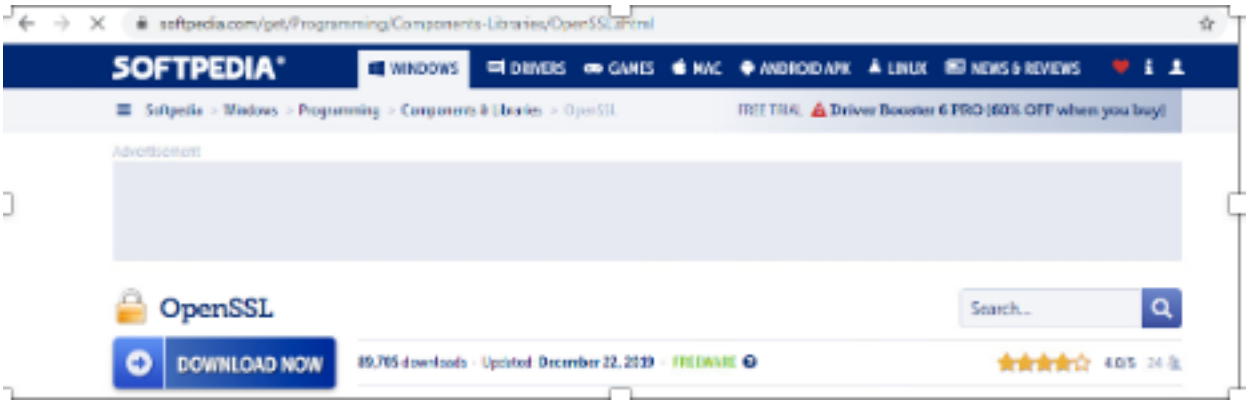
Cisco Security Control Framework (SCF) : Le cadre de contrôle de la sécurité des solutions de collaboration fournit les directives de conception et de mise en oeuvre nécessaires à la création d'une infrastructure de collaboration sécurisée et fiable. Ces infrastructures résistent aux attaques connues et nouvelles. Référence Security Guide for Cisco Unified ICM/Contact Center Enterprise, version 12.5 .

Dans le cadre de l'effort SCF de Cisco, d'autres améliorations de sécurité sont ajoutées pour UCCE 12.5. Ce document présente ces améliorations.

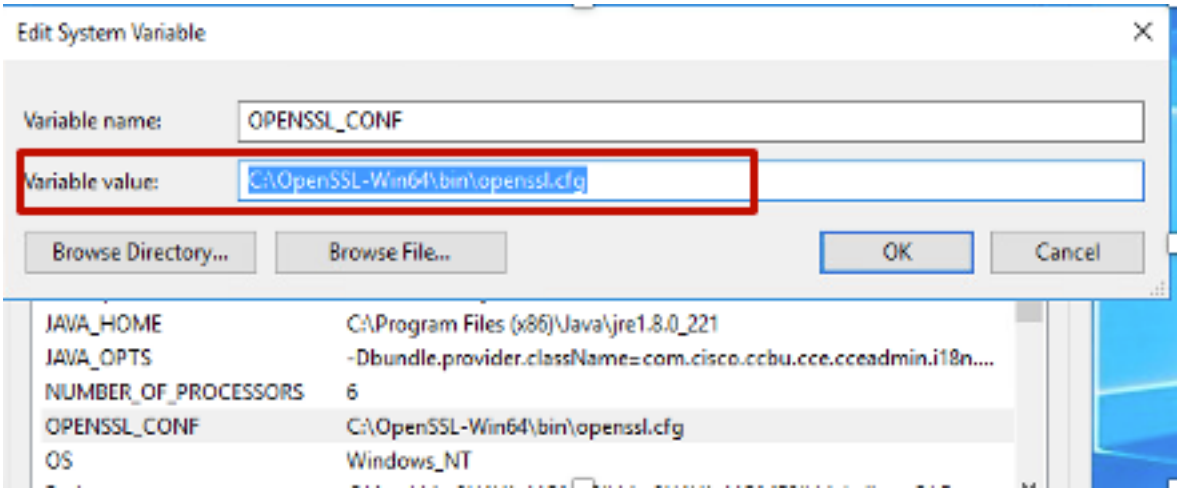
Vérification de l'ISO téléchargée

Afin de valider l'ISO téléchargée signée par Cisco et de s'assurer qu'elle est autorisée, les étapes sont les suivantes :

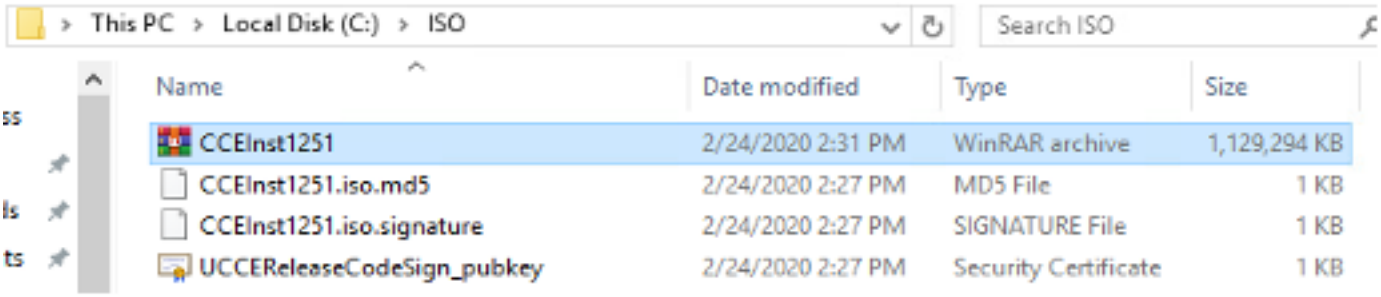
1. Téléchargez et installez OpenSSL. Recherchez le logiciel « openssl softpedia ».



2. Confirmez le chemin d'accès (il est défini par défaut, mais il est toujours correct de le vérifier). Sous Windows 10, accédez à Propriétés système, sélectionnez Variables d'environnement.



3. Fichiers nécessaires à la vérification ISO



4. Exécutez l'outil OpenSSL à partir de la ligne de commande.

5. Exécuter la commande

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

6. En cas de défaillance, la ligne de commande affiche l'erreur comme le montre l'image

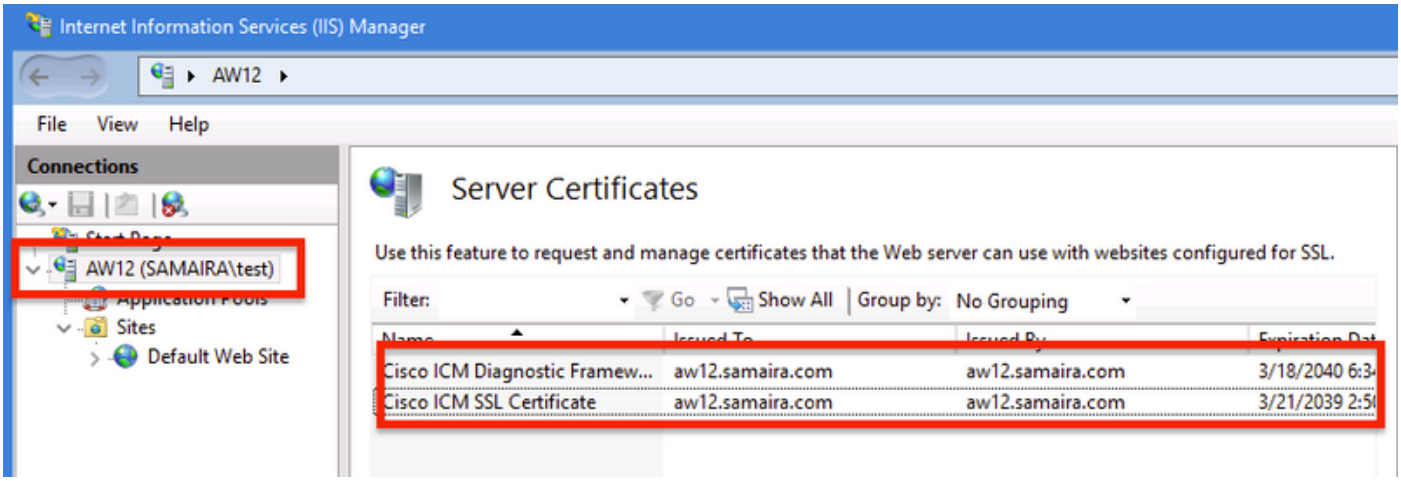
Utiliser des certificats avec SHA-256 et taille de clé 2 048 bits

Les journaux signalent une erreur en cas d'identification de certificats non-plainte (c'est-à-dire non conformes à la spécification SHA-256 et/ou 2 048 bits de taille de clé).

Il existe deux certificats importants du point de vue de l'UCCE :

- Certificat de service Cisco ICM Diagnostic Framework
- Certificat SSL Cisco ICM

Les certificats peuvent être examinés dans l'option Gestionnaire des services Internet (IIS) du serveur Windows.



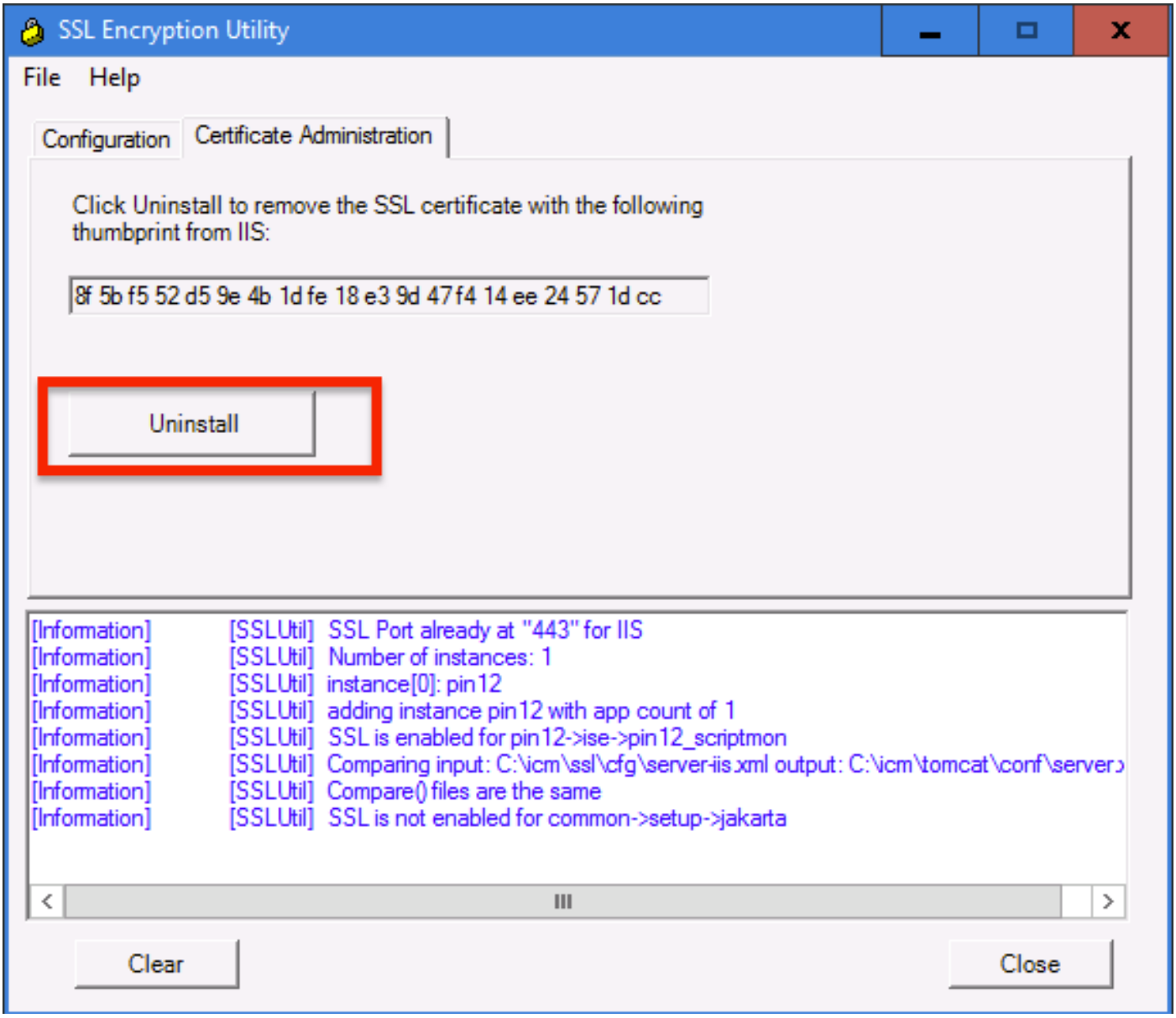
Pour les certificats auto-signés (pour Diagnostiquer Portico ou Configuration Web) , la ligne d'erreur signalée est :

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

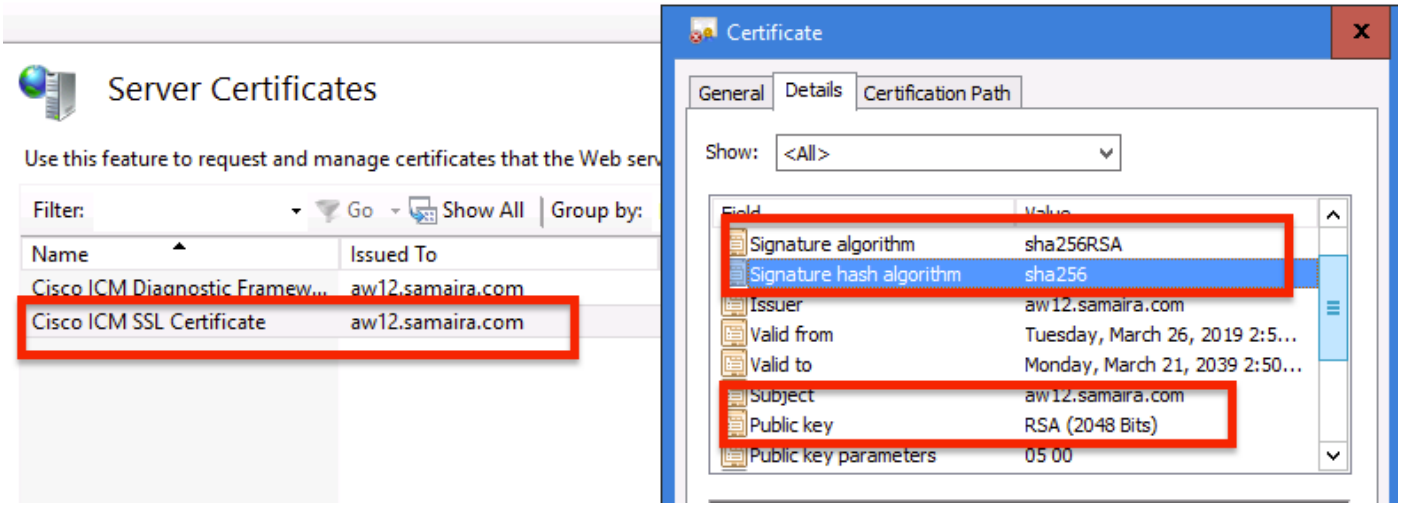
Outil SSLUtil

a. Afin de régénérer les certificats auto-signés (pour la page WebSetup/CCEAdmin), utilisez l'outil SSLUtil (à partir de l'emplacement C:\icm\bin).

b. Sélectionnez Désinstaller pour supprimer le certificat SSL Cisco ICM actuel.



c. Ensuite, sélectionnez Installer dans l'outil SSLUtil et une fois le processus terminé, notez que le certificat créé inclut maintenant les bits SHA-256 et de taille de clé '2048'.



Commande DiagFwCertMgr

Afin de régénérer un certificat auto-signé pour le certificat de service Cisco ICM Diagnostic

Framework, utilisez la ligne de commande "**DiagFwCertMgr**« , comme indiqué dans l'image :

```
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>_
```

Outil de protection des données

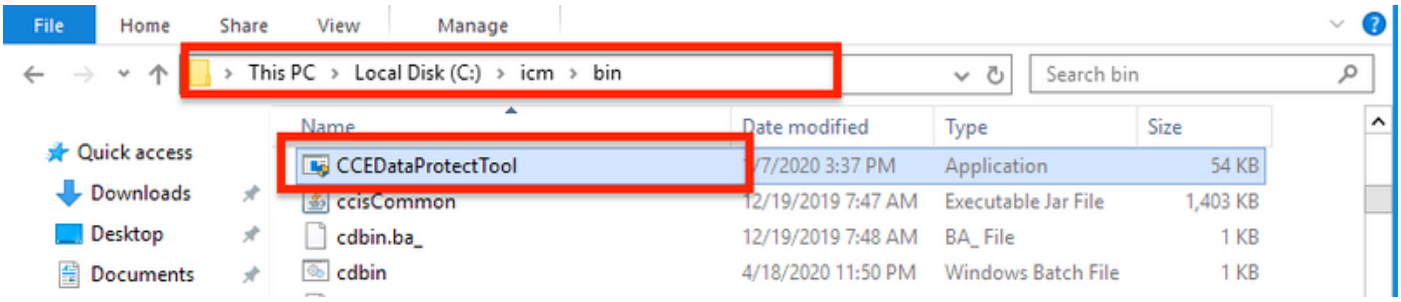
1. CCEDataProtectTool est utilisé pour chiffrer et déchiffrer les informations sensibles que le Registre Windows y stocke. Après la mise à niveau vers SQL 12.5, le magasin de valeurs dans le Registre **SQLLogin** doit être reconfiguré avec CCEDataProtectTool. Seul l'administrateur, l'utilisateur de domaine disposant de droits d'administration ou un administrateur local peut exécuter cet outil.

2. Cet outil peut être utilisé pour afficher, configurer, modifier, supprimer le magasin de valeurs chiffrées dans le Registre **SQLLogin**.

3. L'outil se trouve à l'emplacement ;

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

4. Accédez à l'emplacement et double-cliquez sur CCEDataProtectTool.exe.

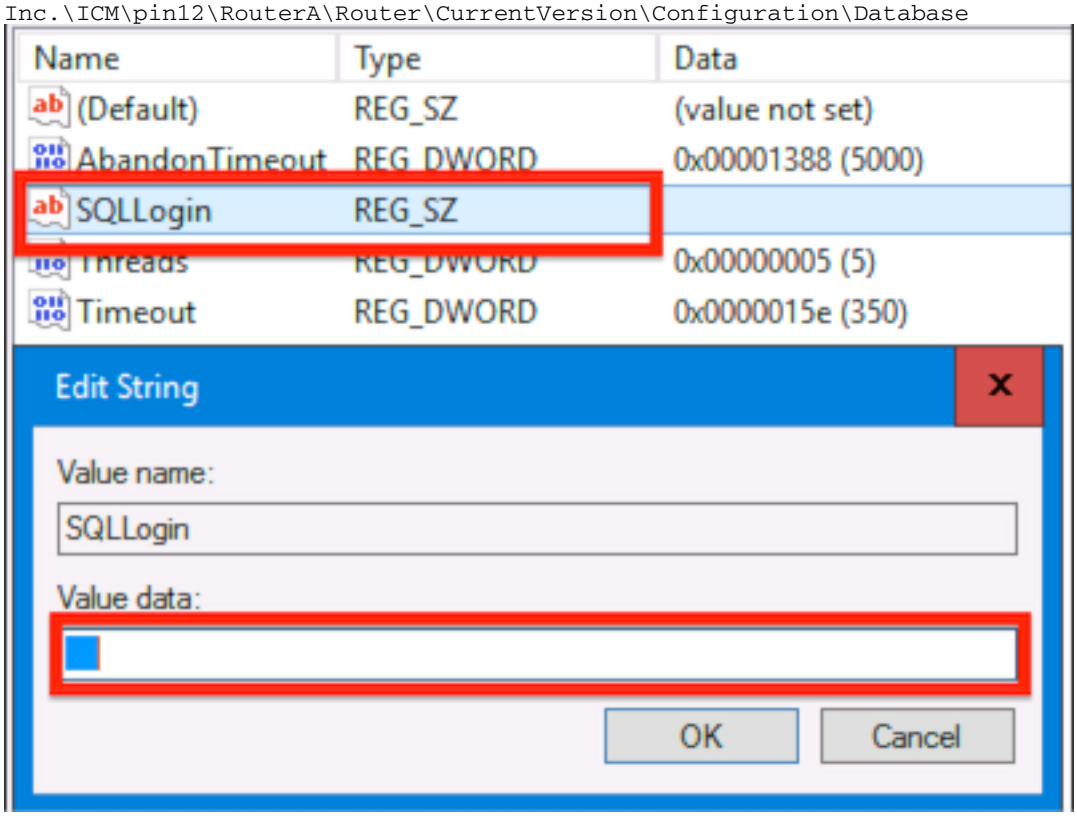


5. Afin de chiffrer , appuyez sur 1 pour DBLookup, saisissez Nom de l'instance. Ensuite, appuyez sur 2 pour sélectionner « Modifier et chiffrer »

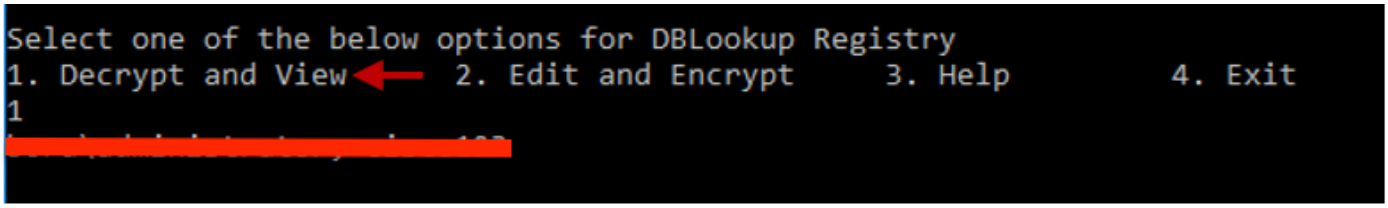
```
C:\icm\bin\CCEDataProtectTool.exe
CCEDataProtectTool supports Encryption/Decryption of sensitive information in Windows Registry.

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. Accédez à l'emplacement du Registre et consultez la valeur de chaîne **SQLLogin** vide, comme illustré dans l'image :

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



7. En cas de besoin de revoir la valeur chiffrée ; tandis que la ligne de commande de CCEDataProtectTool, sélectionnez 1 pour « Décrypter et afficher », comme indiqué dans l'image ;



8. Tous les journaux de cet outil se trouvent à l'emplacement ;

```
<Install Directory>:\temp

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