

UCCE 12.5のセキュリティ強化について

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ダウンロードしたISOの確認](#)

[SHA-256およびキーサイズ2048ビットの証明書の使用](#)

[SSLUtilツール](#)

[DiagFwCertMgrコマンド](#)

[データ保護ツール](#)

概要

このドキュメントでは、Unified Contact Center Enterprise(UCCE)12.5で追加された最新のセキュリティ拡張機能について説明します。

前提条件

- UCCE
- SSL (Open Secure Sockets Layer)

要件

次の項目に関する知識があることが推奨されます。

- UCCE 12.5
- オープンSSL

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- UCCE 12.5
- Windows用OpenSSL (64ビット)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

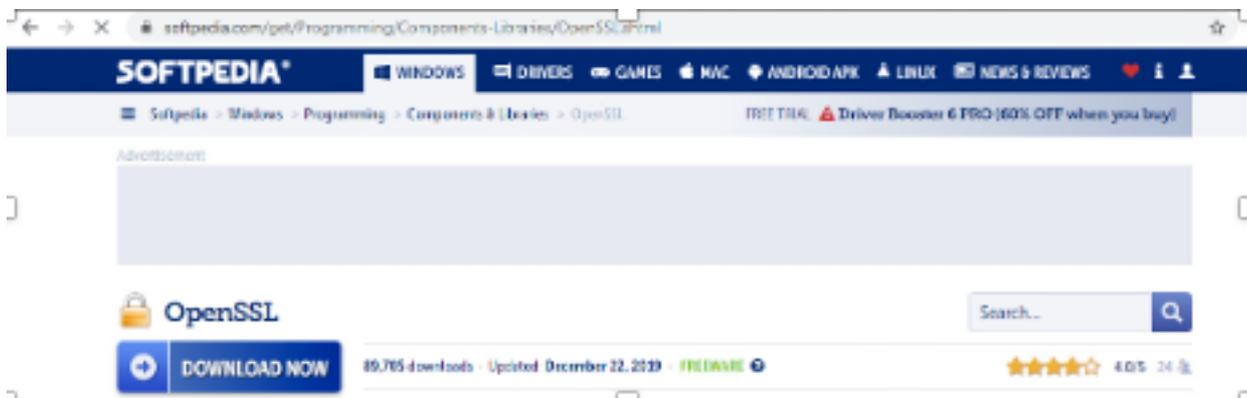
Cisco Security Control Framework(SCF):Collaboration Security Control Frameworkは、セキュアで信頼性の高いコラボレーションインフラストラクチャを構築するための設計および実装ガイドラインを提供します。これらのインフラストラクチャは、既知の攻撃と新しい攻撃の両方に対して復元力があります。Cisco [Unified ICM/Contact Center Enterpriseリリース12.5のセキュリティガイドを参照してください](#)。

シスコのSCFの取り組みの一環として、UCCE 12.5に追加されたセキュリティ強化が加えられました。このドキュメントでは、これらの強化の概要について説明します。

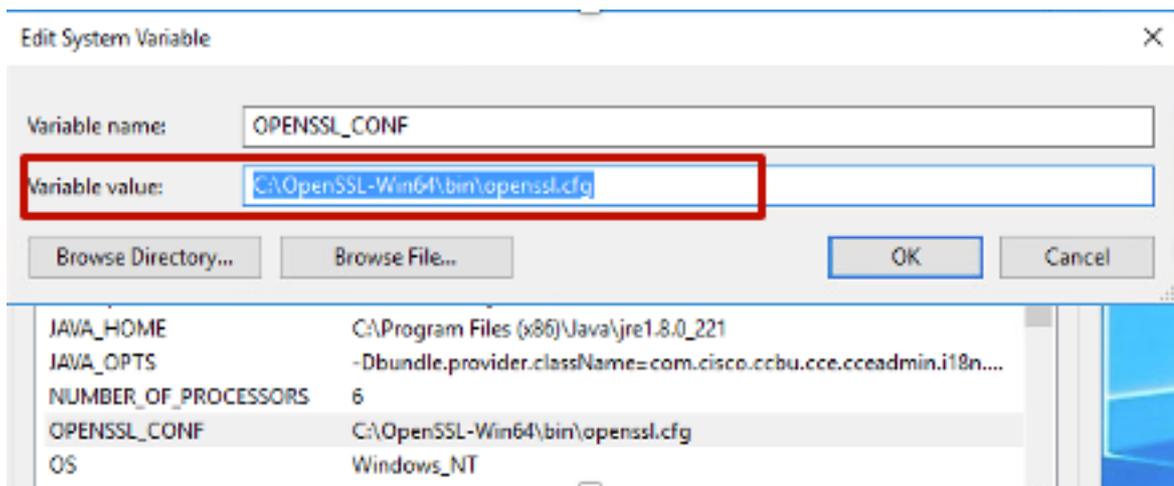
ダウンロードしたISOの確認

シスコによって署名されたダウンロード済みISOを検証し、承認されていることを確認するには、次の手順を実行します。

1. OpenSSLのダウンロードとインストールソフトウェア「openssl softpedia」を検索します。



2.パスを確認します (これはデフォルトで設定されますが、検証には有効です)。Windows 10では、[システムプロパティ]に移動し、[環境変数]を選択します。



3. ISO検証に必要なファイル

Name	Date modified	Type	Size
CCEInst1251	2/24/2020 2:31 PM	WinRAR archive	1,129,294 KB
CCEInst1251.iso.md5	2/24/2020 2:27 PM	MD5 File	1 KB
CCEInst1251.iso.signature	2/24/2020 2:27 PM	SIGNATURE File	1 KB
UCCEReleaseCodeSign_pubkey	2/24/2020 2:27 PM	Security Certificate	1 KB

4. コマンドラインからOpenSSLツールを実行します。

```
C:\OpenSSL-Win64\bin>openssl
OpenSSL>
```

5. 次のコマンドを実行します。

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

6. 障害が発生した場合、コマンドラインにエラーが表示されます (図を参照)

```
OpenSSL> dgst -sha512 -keyform der -verify c:\iso\UCCEReleaseCodeSign_pubkey.der -signature c:\iso\CCEInst1251.iso.signature c:\iso\CCEInst1251.iso
Verification Failure
error in dgst
OpenSSL>
```

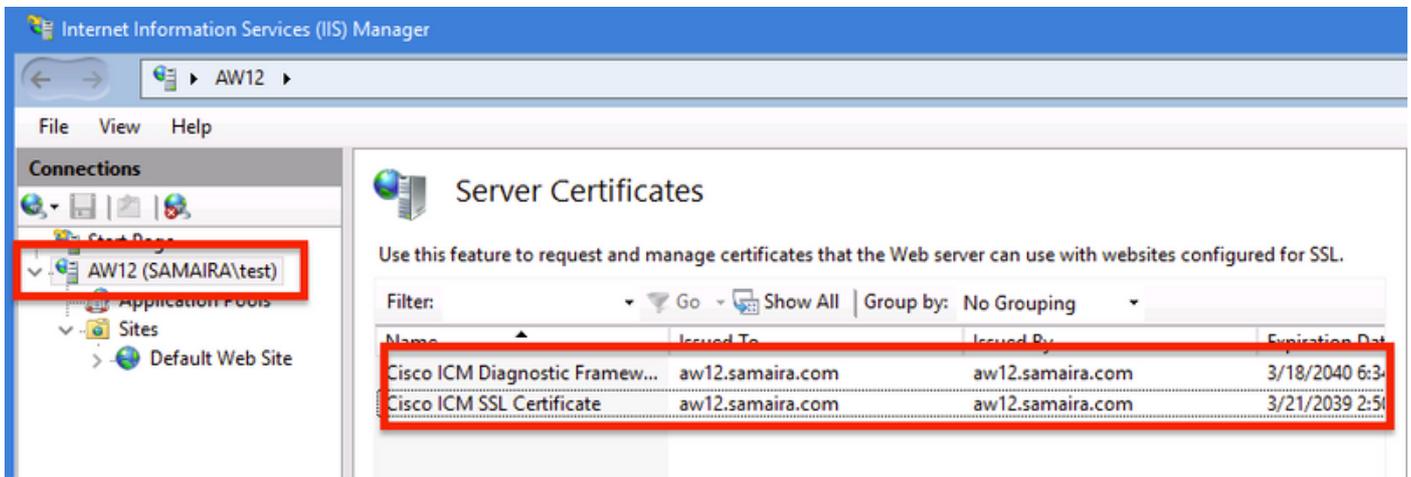
SHA-256およびキーサイズ2048ビットの証明書の使用

ログは、非準拠の証明書を特定した場合にエラーを報告します (SHA-256またはキーサイズ2048ビットの要件を満たしていない場合)。

UCCEの観点からは、次の2つの重要な証明書があります。

- Cisco ICM Diagnostic Frameworkサービス証明書
- Cisco ICM SSL証明書

証明書は、Windowsサーバのインターネットインフォメーションサービス(IIS)マネージャオプションで確認できます。



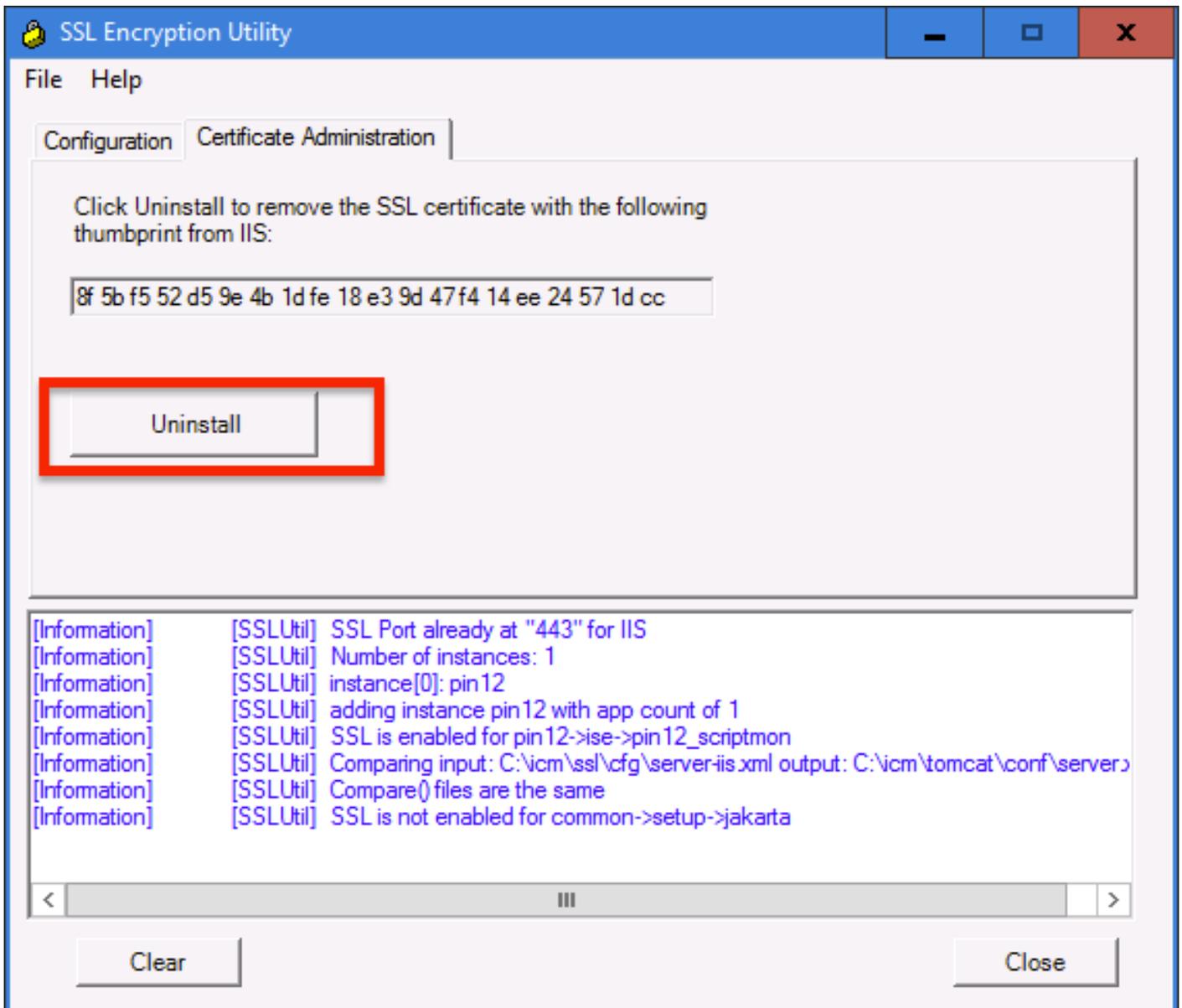
自己署名証明書 (プロファイルの診断またはWebセットアップ用) の場合、次のエラー行が報告されます。

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

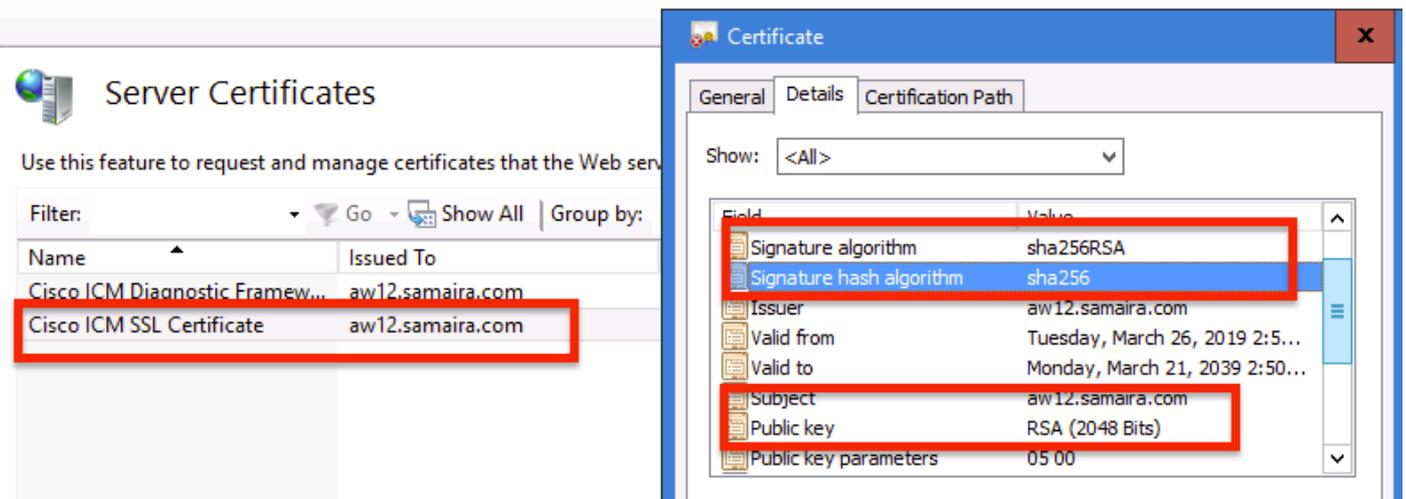
SSLUtilツール

a.自己署名証明書 (WebSetup/CCEAdminページ用) を再生成するには、SSLUtilツール(場所 C:\icm\bin)を使用します。

b.[Uninstall]を選択して、現在の[Cisco ICM SSL Certificate]を削除します。



c.次にInstall in SSLUtilツールを選択し、プロセスが完了したら、作成された証明書にSHA-256ビットとkeysize '2048'ビットが含まれていることを確認します。



DiagFwCertMgrコマンド

Cisco ICM Diagnostic Frameworkサービス証明書の自己署名証明書を再生成するには、次の図に

示すように、コマンドライン「DiagFwCertMgr」を使用します。

```
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

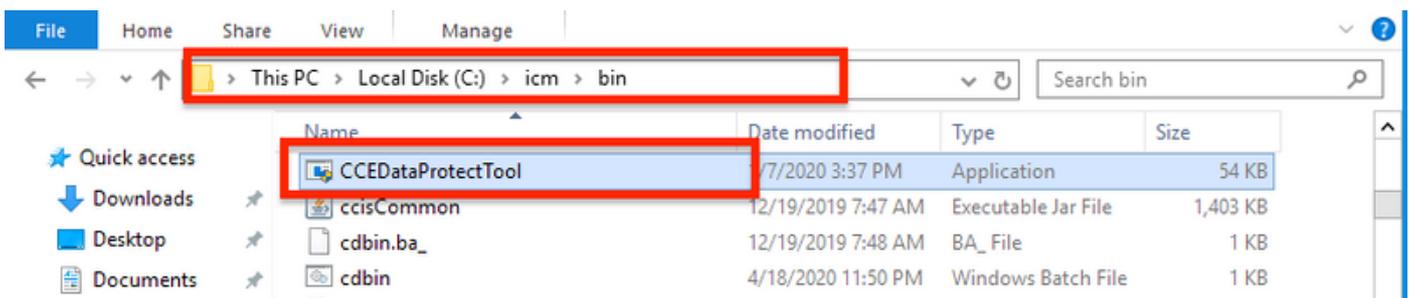
C:\icm\serviceability\diagnostics\bin>_
```

データ保護ツール

1. CEDataProtectToolは、Windowsレジストリが格納する機密情報を暗号化および復号化するために使用されます。SQL 12.5へのアップグレード後、SQLLoginレジストリの値ストアをCEDataProtectToolで再構成する必要があります。このツールを実行できるのは、管理者権限を持つ管理者、ドメインユーザー、またはローカル管理者のみです。
- 2.このツールは、SQLLoginレジストリの暗号化された値ストアの表示、構成、編集、削除に使用できます。
- 3.ツールは場所にあります。

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

4.場所に移動し、[CEDataProtectTool.exe]をダブルクリックします。



5.暗号化するには、[DBLookup]に1を押し、[Instance Name]を入力します。次に、2を押しして[Edit and Encrypt]を選択します

```
C:\icm\bin\CCEDDataProtectTool.exe
CCEDDataProtectTool 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\CCEDDataProtect.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.レジストリの場所へ移動し、「文字列値SQLLoginが空のように表示されます（図を参照）。

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

Name	Type	Data
(Default)	REG_SZ	(value not set)
AbandonTimeout	REG_DWORD	0x00001388 (5000)
SQLLogin	REG_SZ	
Threads	REG_DWORD	0x00000005 (5)
Timeout	REG_DWORD	0x0000015e (350)

Edit String dialog box showing Value name: SQLLogin and Value data: [Redacted].

(7)暗号化値の確認が必要な場合図に示すように、CCEDDataProtectToolのコマンドラインで、[Decrypt and View]に1を選択します。

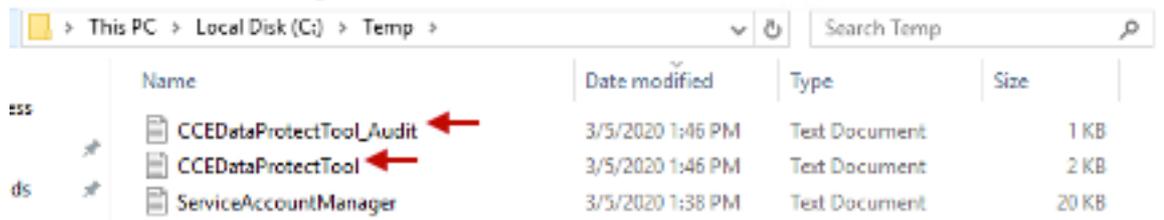
```
Select one of the below options for DBLookup Registry
1. Decrypt and View ← 2. Edit and Encrypt          3. Help          4. Exit
1
```

8.このツールのログは、場所にあります。

<Install Directory>:\temp

Audit logs filename : CCEDataProtectTool_Audit

CCEDataProtectTool logs : CCEDataProtectTool



The screenshot shows a Windows File Explorer window with the address bar set to 'This PC > Local Disk (C:) > Temp >'. The search bar contains 'Search Temp'. The main area displays a list of files with columns for Name, Date modified, Type, and Size. Two files, 'CCEDataProtectTool_Audit' and 'CCEDataProtectTool', are highlighted with red arrows. The file 'ServiceAccountManager' is also visible in the list.

	Name	Date modified	Type	Size
ESS	CCEDataProtectTool_Audit	3/5/2020 1:46 PM	Text Document	1 KB
ds	CCEDataProtectTool	3/5/2020 1:46 PM	Text Document	2 KB
	ServiceAccountManager	3/5/2020 1:38 PM	Text Document	20 KB