

Informazioni sui miglioramenti della sicurezza UCCE 12.5

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Verifica dell'ISO scaricato](#)

[Usa certificati con SHA-256 e dimensione chiave 2048 bit](#)

[Strumento SSLUtil](#)

[Comando DiagFwCertMgr](#)

[Strumento di protezione dei dati](#)

Introduzione

In questo documento vengono descritti i più recenti miglioramenti apportati alla sicurezza con Unified Contact Center Enterprise (UCCE) 12.5.

Prerequisiti

- UCCE
- Apri SSL (Secure Sockets Layer)

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- UCCE 12.5
- Apri SSL

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- UCCE 12.5
- OpenSSL (64 bit) per Windows

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

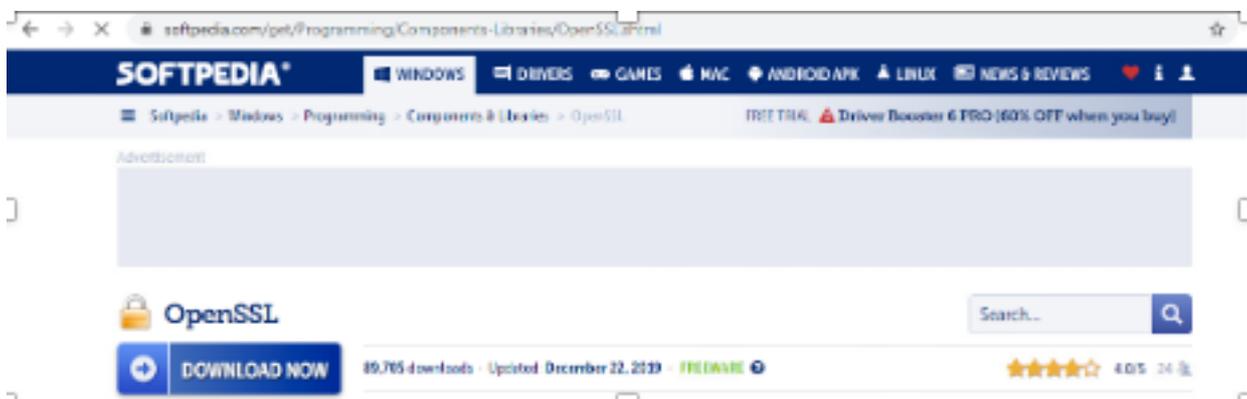
Cisco Security Control Framework (SCF): Collaboration Security Control Framework fornisce le linee guida di progettazione e implementazione per la creazione di infrastrutture di collaborazione sicure e affidabili. Queste infrastrutture sono resistenti sia alle forme di attacco conosciute che a quelle nuove. Guida di riferimento [alla sicurezza per Cisco Unified ICM/Contact Center Enterprise, versione 12.5](#).

Nell'ambito dell'impegno di Cisco per il SCF, sono stati aggiunti ulteriori miglioramenti alla sicurezza per UCCE 12.5. Nel presente documento vengono descritti tali miglioramenti.

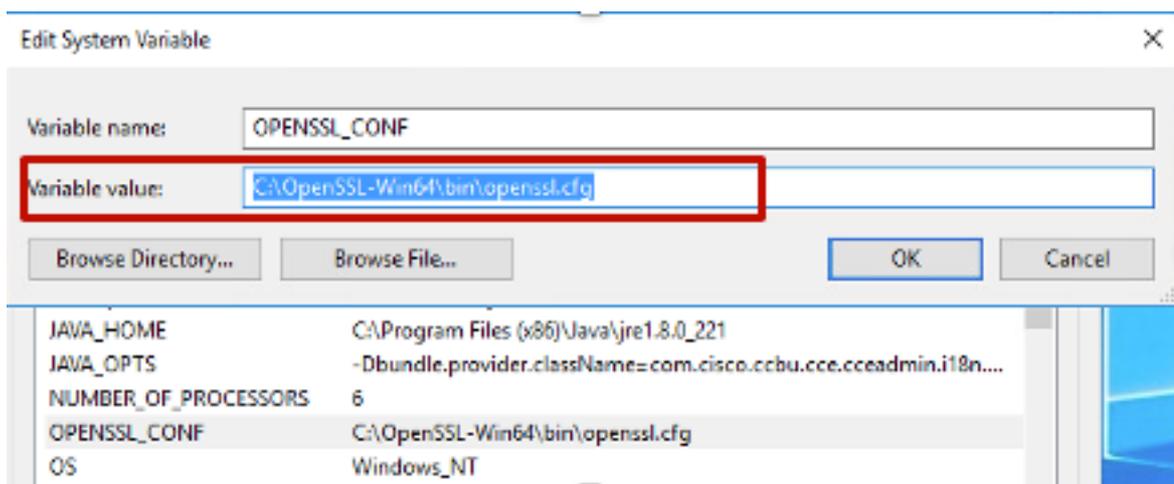
Verifica dell'ISO scaricato

Per convalidare l'ISO scaricato firmato da Cisco e accertarsi che sia autorizzato, i passaggi sono:

1. Scaricare e installare OpenSSL. Cercare software "openssl softpedia".



2. Confermare il percorso (impostazione predefinita, ma comunque valida per la verifica). In Windows 10, andare a Proprietà di sistema, selezionare Variabili di ambiente.



3. File necessari per la verifica ISO

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. Eseguire lo strumento OpenSSL dalla riga di comando.

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

5. Eseguire il comando

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

6. In caso di errore, la riga di comando visualizza l'errore come mostrato nell'immagine

```
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>
```

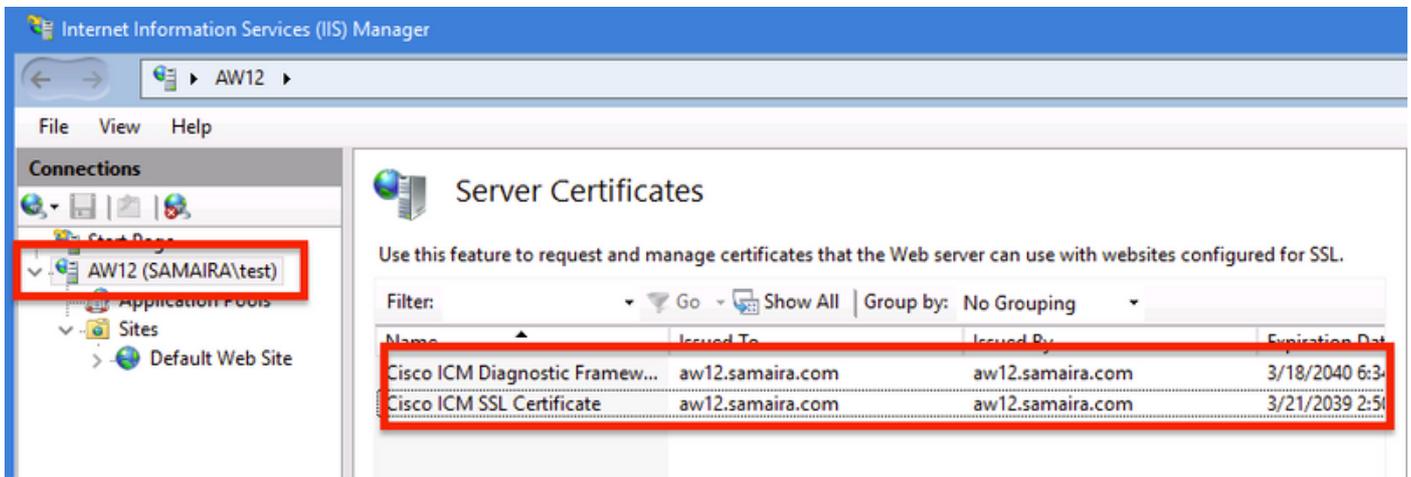
Usa certificati con SHA-256 e dimensione chiave 2048 bit

Registra gli errori di segnalazione in caso di identificazione di certificati non conformi (ovvero non conformi al requisito SHA-256 e/o keysize 2048 bit).

Dal punto di vista dell'UCCE vi sono due importanti certificati:

- Certificato del servizio Cisco ICM Diagnostic Framework
- Certificato SSL ICM Cisco

I certificati possono essere esaminati nell'opzione Gestione Internet Information Services (IIS) di Windows Server.



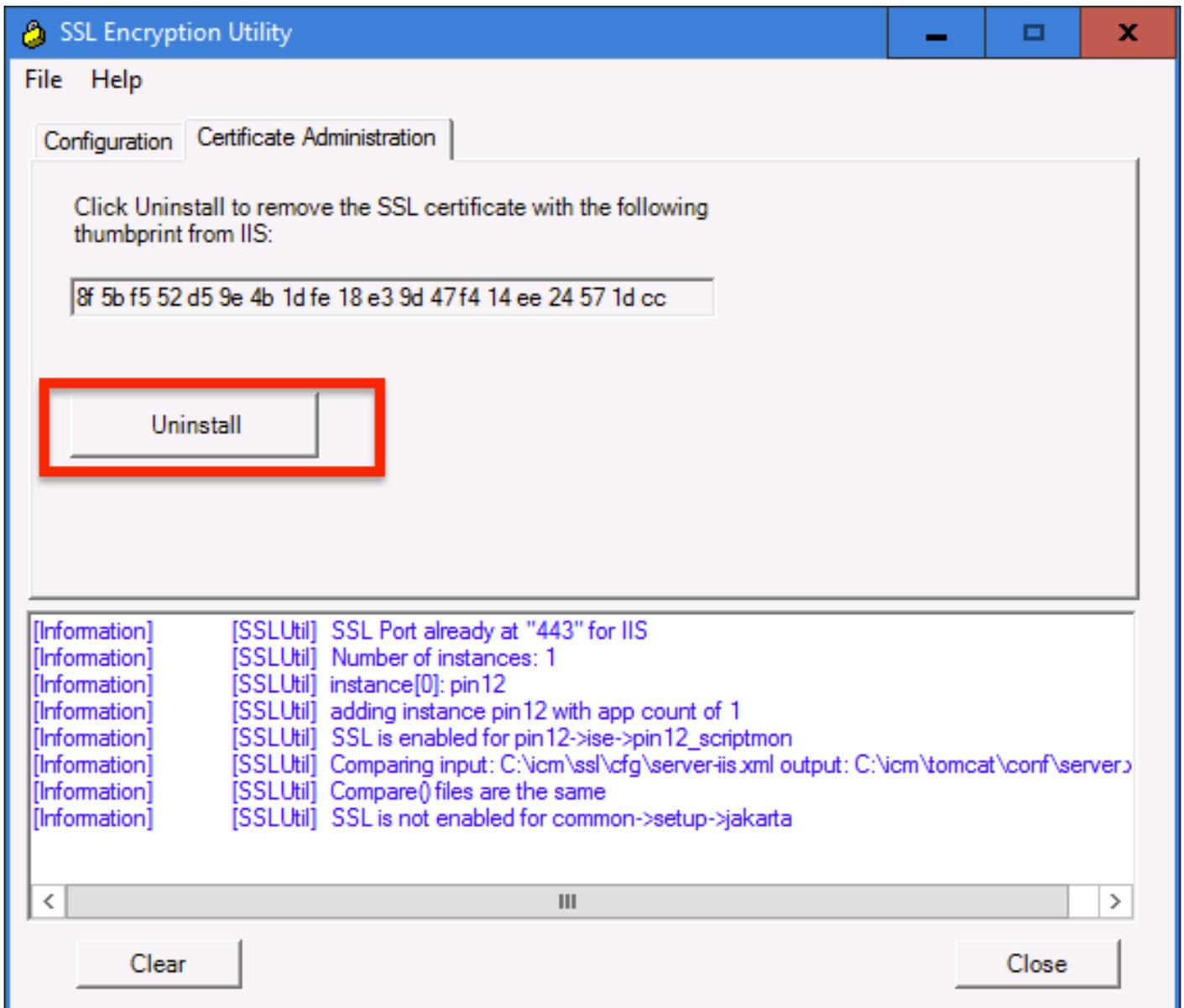
Per i certificati autofirmati (per Diagnose Portico o Web Setup), la riga di errore segnalata è:

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

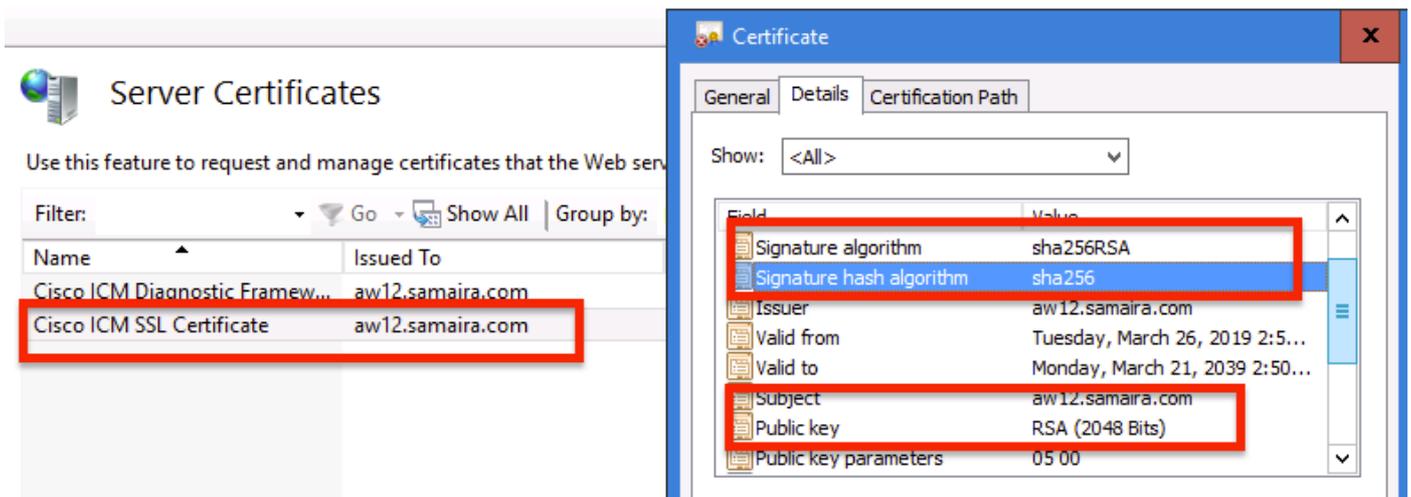
Strumento SSLUtil

r. Per rigenerare i certificati autofirmati (per la pagina WebSetup/CEAdmin), utilizzare lo strumento SSLUtil (dal percorso C:\icm\bin).

b. Selezionare Disinstalla per eliminare il "Certificato SSL ICM Cisco" corrente.



c. Selezionare Install in SSLUtil tool e una volta completato il processo, notare che il certificato creato ora include i bit SHA-256 e keysize '2048'.



Comando DiagFwCertMgr

Per rigenerare un certificato autofirmato per il certificato del servizio Cisco ICM Diagnostic

Framework, utilizzare la riga di comando "**DiagFwCertMgr**", come mostrato nell'immagine:

```
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

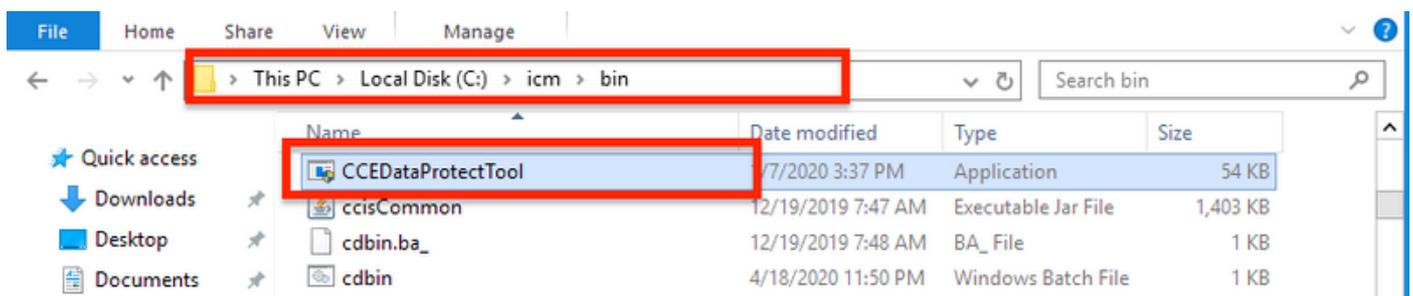
C:\icm\serviceability\diagnostics\bin>_
```

Strumento di protezione dei dati

1. CCEDDataProtectTool viene utilizzato per crittografare e decrittografare le informazioni riservate memorizzate nel Registro di sistema di Windows. Dopo l'aggiornamento a SQL 12.5, è necessario riconfigurare l'archivio valori nel Registro di sistema **SQLLogin** con CCEDDataProtectTool. Questo strumento può essere eseguito solo da un amministratore, da un utente di dominio con diritti amministrativi o da un amministratore locale.
2. Questo strumento può essere utilizzato per visualizzare, configurare, modificare, rimuovere l'archivio valori crittografato nel Registro di sistema **SQLLogin**.
3. L'utensile si trova nella posizione;

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

4. Passare alla posizione e fare doppio clic su CCEDDataProtectTool.exe.



5. Per crittografare , premere 1 per DBLookup, immettere il nome dell'istanza. Quindi, premere 2 per selezionare "Edit and Encrypt" (Modifica e crittografia)

```
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. Passare alla posizione del Registro di sistema e rivedere Valore stringa **SQLLogin** sembra vuoto, come mostrato nell'immagine:

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

Value name:
SQLLogin

Value data:
[Redacted]

OK Cancel

7. In caso sia necessario rivedere il valore cifrato; nella riga di comando di CCEDDataProtectTool, selezionare premere 1 per "Decrypt and View", come mostrato nell'immagine;

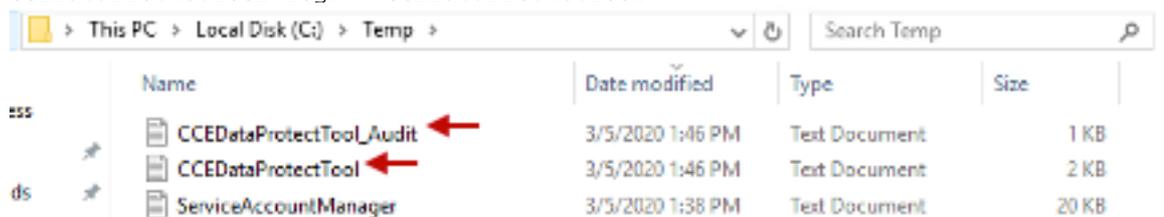
```
Select one of the below options for DBLookup Registry
1. Decrypt and View ← 2. Edit and Encrypt 3. Help 4. Exit
1
████████████████████████████████████████████████████████████████████████████████
```

8. Tutti i registri relativi a questo strumento sono disponibili nel percorso;

<Install Directory>:\temp

Audit logs filename : CCEDDataProtectTool_Audit

CCEDDataProtectTool logs : CCEDDataProtectTool



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 table of files:

	Name	Date modified	Type	Size
sss	CCEDDataProtectTool_Audit ←	3/5/2020 1:46 PM	Text Document	1 KB
	CCEDDataProtectTool ←	3/5/2020 1:46 PM	Text Document	2 KB
ds	ServiceAccountManager	3/5/2020 1:38 PM	Text Document	20 KB