Gestisci certificato componenti PCCE per SPOG

Sommario

Introduzione

In questo documento viene descritto come scambiare i certificati SSL autofirmati di Admin Workstation (AW) con Customer Voice Portal (CVP), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (idS) e Virtualized Voice Browser (VB) per Package Contact Center Enterprise (PCCE) Single Pane of Glass (SPOG).

Contributo di Nagarajan Paramasivam e Robert Rogier, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Packaged/Unified Contact Center Enterprise (PCCE/UCCE)
- Piattaforma VOS
- Gestione certificati
- Archivio chiavi dei certificati

Componenti usati

Le informazioni di questo documento si basano sui seguenti componenti:

- Admin Workstation (CEADMIN/SPOG)
- CVP
- Finesse
- CUIC, IDS
- VVB
- Cisco ECE

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

Si consiglia di aver letto e compreso la Guida di amministrazione e configurazione PCCE, in particolare l'appendice di riferimento alla fine che descrive l'impostazione e la configurazione dei certificati. Guida alla configurazione e all'amministrazione di PCCE

Nuova interfaccia utente - SPOG

Packaged CCE 12.0 ha una nuova interfaccia utente conforme ad altre applicazioni per contact center. L'interfaccia utente consente di configurare la soluzione tramite un'unica applicazione. Accedere alla nuova amministrazione di Unified CCE all'indirizzo https://<IP Address>/cceadmin. <Indirizzo IP> è l'indirizzo dell'AW CCE unificato del lato A o B o dell'HDS esterno opzionale.

In questa release, l'interfaccia di amministrazione di Unified CCE consente di configurare quanto segue:

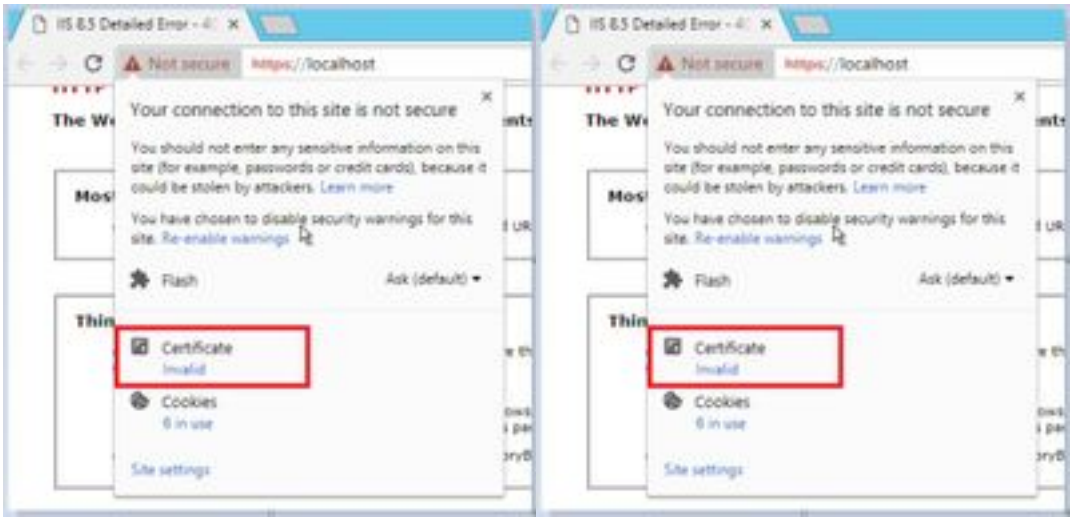
- Campagne
- Cortesia Callback
- Gruppi di server SIP
- Trasferimento file: Il trasferimento di file è possibile solo tramite AW Principal (AW Lato A nell'implementazione di agenti nel 2000 e AW configurato in distribuzioni di agenti 4000 e 12000).
- Modelli di instradamento: Il modello di numero composto in Unified CVP Operations Console è ora denominato modello di routing in Unified CCE Administration.
- Percorsi: In Amministrazione CCE unificata, il codice di routing è ora il prefisso della posizione anziché l'ID del sito.
- Configurazione dispositivo: L'amministrazione CCE unificata consente di configurare i seguenti dispositivi: CVP Server, CVP Reporting Server, VB, Finesse, Identity Service (installazione Single Sign-On).
- Risorse del team: L'amministrazione CCE unificata consente di definire e associare le seguenti risorse per i team di agenti: Variabili Chiamata Layout, Layout Desktop, Rubriche Telefoniche, Flussi Di Lavoro, Motivi (Non Pronto, Disconnetti, Completamento Chiamate).
- E-mail e chat

Prima di gestire il sistema tramite SPOG, è necessario scambiare i certificati SSL tra CVP (Customer Voice Portal), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (idS) e Virtual Voice Browser (VB) e Admin Workstation (AW) per stabilire una comunicazione di trust.

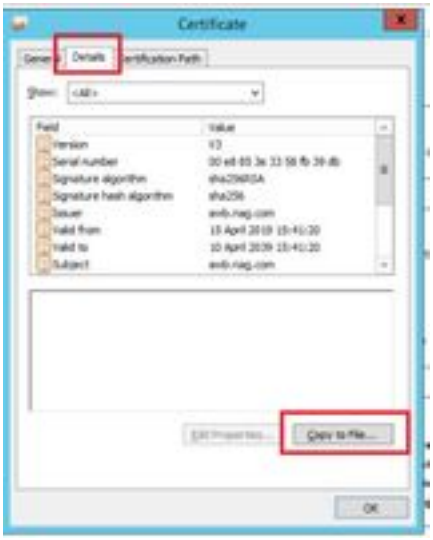
Esportazione certificato SSL

AW (Administration Workstation)

Passaggio 1. Accedere all'URL https://localhost nel server AW e scaricare i certificati SSL del server.



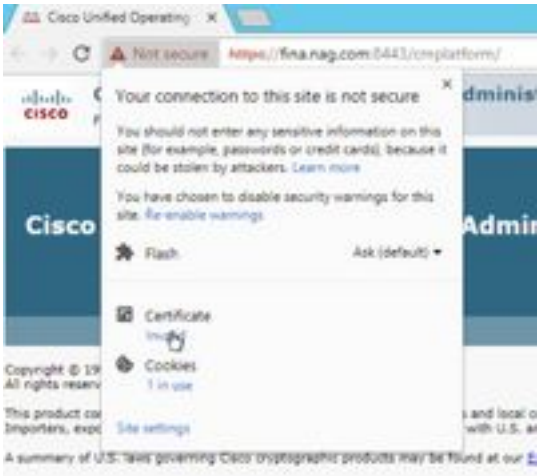
Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.



Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.

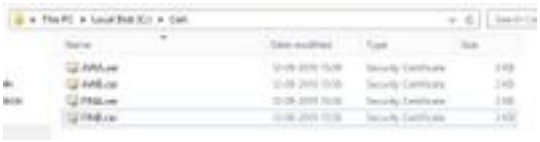
Finesse

Passaggio 1. Accedere alla pagina https://Finesseserver:8443/cmplatform e scaricare il certificato tomcat.



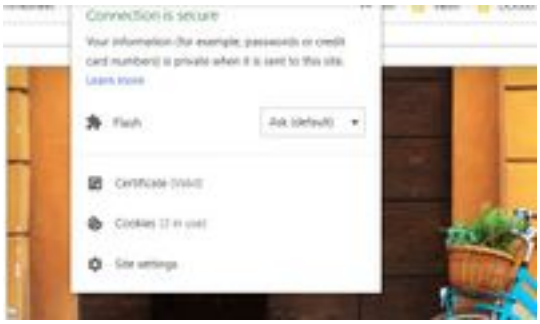
Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.



Cisco ECE

Passaggio 1. Accedere alla pagina https://ECEWebServer e scaricare il certificato SSL del server.



Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

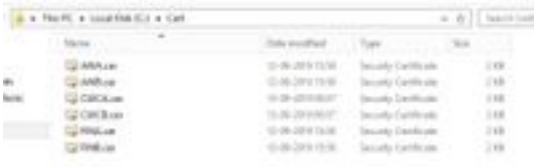
Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.

CUIC

Passaggio 1. Accedere alla pagina https://CUICServer:8443/cmplatform e scaricare il certificato tomcat.

Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.

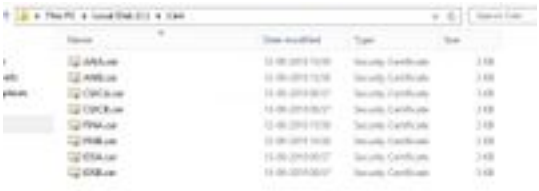


Cisco idS

Passaggio 1. Accedere alla pagina https://IDSServer:8553/idsadmin/ e scaricare il certificato tomcat.

Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.

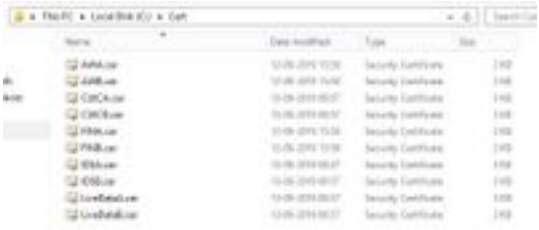


LiveData

Passaggio 1. Accedere alla pagina https://LiveDataServer:8444/cuic/gadget/LiveData/ e scaricare il certificato tomcat.

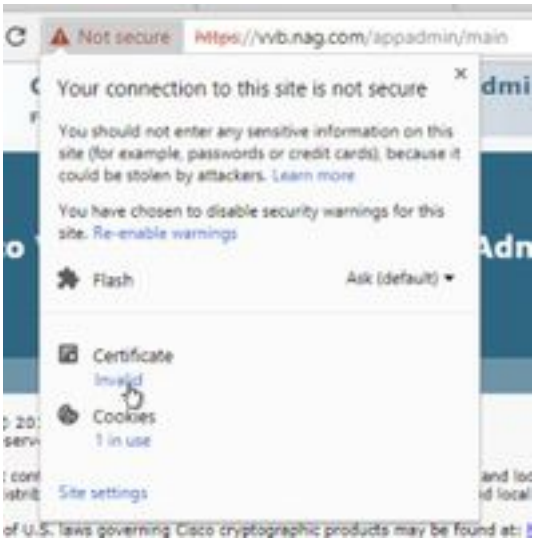
Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.



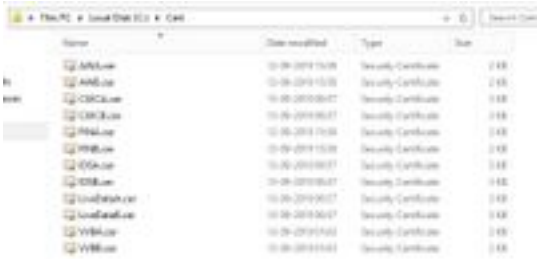
VVB

Passaggio 1. Accedere alla pagina https://VVBServer/appadmin/main e scaricare il certificato tomcat.



Passaggio 2. Nella finestra del certificato, passare alla scheda Dettagli e fare clic sul pulsante Copia nel file.

Passaggio 3. Selezionare X.509 (CER) con codifica Base 64 e memorizzare il certificato nell'archivio locale.



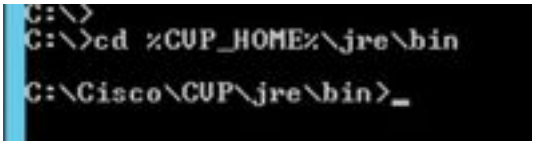
Importazione certificato SSL in keystore

CVP Call Server e server di report

Passaggio 1. Accedere al server CVP e copiare i certificati AW CCE Admin nella cartella **C:\cisco\cvp\conf\security**.

Passaggio 2. Passare alla pagina **%CVP_HOME%\conf** e aprire security.properties per copiare la password del keystore.

Passaggio 3. Aprire il prompt dei comandi come amministratore ed eseguire il comando **cd %CVP_HOME%\jre\bin**.



Passaggio 4. Utilizzare questo comando per importare i certificati AW nel server CVP.

keytool -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias awa.nag.com -file C:\Cisco\CVP\conf\security\AWA.cer

Passaggio 5. Quando viene richiesta la password, incollare la password copiata dal file security.properties.

Passaggio 6. Digitare **sì** per considerare attendibile il certificato e assicurarsi di ottenere il risultato **Certificato aggiunto al keystore.**

Passaggio 7. Viene visualizzato un messaggio di avvertenza insieme all'importazione completata. Ciò è dovuto al formato proprietario Keystore, è possibile ignorarlo.

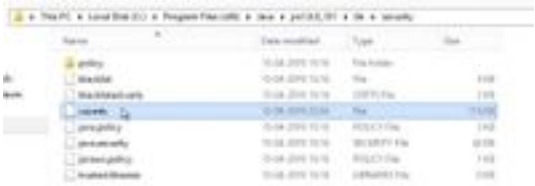
Avviso:

Il keystore JCEKS utilizza un formato proprietario. È consigliabile eseguire la migrazione a PKCS12, un formato standard del settore che utilizza "keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore -deststoretype pkcs12".

Admin Workstation

Passaggio 1. Accedere al server AW e aprire il prompt dei comandi come amministratore.

Passaggio 2. Passare a C:\Program Files(x86)\Java\jre1.8.0_181\lib\security e verificare che il file cacerts esista.



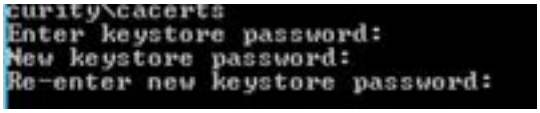
Passaggio 3. Digitare il comando **cd %JAVA_HOME%** e immettere il comando.

Passaggio 4. Utilizzare questo comando per importare i certificati Finesse nel server AW.

keytool -import -file C:\Users\Administrator.NAG\Downloads\Cert\FINA.cer -alias fina.nag.com-keystore .\lib\security\cacerts

Passaggio 5. La prima volta che si utilizza questo strumento chiave, **modificare** la password per modificare la password di un archivio certificati.

Passaggio 6. Immettere una nuova password per il keystore e immetterla nuovamente per confermare la password.



Passaggio 7. Digitare **yes** per considerare attendibile il certificato e assicurarsi di ottenere il risultato **Certificato aggiunto al keystore.**

Nota: Ripetere i passi da 1 a 7 con tutti gli altri nodi Finesse e con tutti i nodi CUIC

Passaggio 8. Se la password del keystore è stata immessa in modo errato o ha eseguito i passaggi senza essere reimpostata, si prevede che venga generata questa eccezione.

Considerare attendibile il certificato? [no]: sì

Il certificato è stato aggiunto al keystore

errore keytool: java.io.FileNotFoundException: .\lib\security\cacerts (impossibile trovare il percorso specificato)

Immettere la password del keystore:
errore keytool: java.io.IOException Il keystore è stato alterato o la password non è corretta

Passaggio 9. Per modificare la password del keystore, utilizzare questo comando e riavviare la procedura dal passaggio 4 con la nuova password.

keytool -storepasswd -keystore .\lib\security\cacerts

Passaggio 10. Dopo l'importazione, utilizzare questo comando per visualizzare il certificato dal keystore.

keytool -list -keystore .\lib\security\cacerts -alias fina.nag.com

keytool -list -keystore .\lib\security\cacerts -alias cuic.nag.com

Finesse, CUIC, Cisco idS e VB

Passaggio 1. Accedere alla pagina di amministrazione del sistema operativo del server Finesse e caricare i certificati SSL AW nel trust Tomcat.

Passaggio 2. Passare a **Amministrazione sistema operativo > Protezione > Gestione certificati.**

Passaggio 3. Fare clic su Carica certificato\Catena certificati e selezionare l'opzione Tomcat-trust dall'elenco a discesa.

Passaggio 4. Esplorare l'archivio certificati nell'archivio locale e fare clic su Pulsante Carica.

Passaggio 5. Ripetere i passaggi per caricare tutti i certificati del server AW nel cluster Finesse.

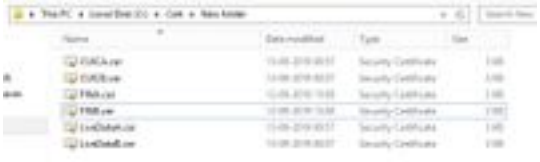
Nota: Non è necessario caricare il certificato tomcat-trust nel nodo secondario, poiché viene replicato automaticamente.

Passaggio 6. Riavviare il servizio Tomcat per rendere effettive le modifiche apportate al certificato.

Passaggio 7. In CUIC, IDS e VVB, seguire i passaggi da 2 a 4 e caricare il certificato AW.

Scambio di certificati tra Finesse e CUIC/LiveData

Passaggio 1. Conservare i certificati Finesse, CUIC e LiveData in una cartella separata.



Passaggio 2. Accedere alla pagina Amministrazione del sistema operativo Finesse, CUIC e LiveData.

Passaggio 3. Passare a **Amministrazione sistema operativo > Protezione > Gestione certificati.**

Passaggio 4. Fare clic su Carica certificato\Catena certificati e selezionare l'opzione Tomcat-trust dall'elenco a discesa.

Passaggio 5. Esplorare l'archivio certificati nell'archivio locale e selezionare Certificato server come di seguito, quindi fare clic su Pulsante Carica.

In Finesse server - CUIC e LiveData come attendibilità Tomcat

In CUIC Server - Finesse e LiveData come trust tomcat

In LiveData Server - CUIC e Finesse come trust Tomcat

> **Nota:** Non è necessario caricare il certificato tomcat-trust nel nodo secondario, poiché viene replicato automaticamente.

Passaggio 6. Riavviare il servizio Tomcat su ogni nodo per rendere effettive le modifiche al certificato.