

UCS Solution-certificaatbeheergids

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[FQDN, DNS en domeinen](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configuratiediagram](#)

[Ondertekende certificaten](#)

[Ondertekende Tomcat-toepassingscertificaten installeren](#)

[Zelfondertekende certificaten](#)

[Installeren op randservers](#)

[Zelfondertekende certificaten regenereren](#)

[Integratie en clientconfiguratie](#)

[UCS-to-MediaSense](#)

[MediaSense-to-Finesse](#)

[UCCX-to-SocialMiner](#)

[UCS AppAdmin-clientcertificaat](#)

[UCS Platform-clientcertificaat](#)

[Clientcertificaat voor kennisgevingservice](#)

[Clientcertificaat voltooien](#)

[SocialMiner-clientcertificaat](#)

[CUIC-clientcertificaat](#)

[Toepassingen van derden die toegankelijk zijn via scripts](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Probleem - Ongeldige gebruikers-id/wachtwoord](#)

[Oorzaken](#)

[Oplossing](#)

[Probleem - MVO-SAN en -certificaat komen niet overeen](#)

[Oorzaken](#)

[Oplossing](#)

[Probleem - NET::ERR_CERT_Common_NAME_INVALIDITY](#)

[Oorzaken](#)

[Oplossing](#)

[Meer informatie](#)

[Certificaatgebreken](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de Cisco Unified Contact Center Express (UCS) kunt configureren voor het gebruik van zelfondertekende en ondertekende certificaten.

Voorwaarden

Vereisten

Zorg ervoor dat u toegang hebt tot de beheerpagina van het besturingssysteem voor deze toepassingen voordat u verder gaat met de configuratiestappen die in dit document worden beschreven:

- UCCX
- SocialMiner
- MediaSense

Een beheerder moet ook toegang hebben tot het certificaatarchief op de client-pc's van de agent en de supervisor.

FQDN, DNS en domeinen

Alle servers in de UCCX-configuratie moeten worden geïnstalleerd met DNS-servers (Domain Name System) en domeinnamen. Het is ook vereist dat agenten, toezichhouders en beheerders toegang hebben tot de UCCX-configuratietoepassingen via de Fully Qualified Domain Name (FQDN).

Voor UCCX, versie 10.0+, moeten de domeinnaam en DNS-servers bij de installatie worden ingevuld. De certificaten die worden gegenereerd door de UCS Versie 10.0+ installateur bevatten de FQDN, al naar gelang van toepassing. Voeg de DNS-servers en een domein toe aan het UCCX-cluster voordat u een upgrade uitvoert naar UCCX versie 10.0+.

Als het domein verandert of voor het eerst wordt ingevuld, moeten de certificaten worden geregenereerd. Nadat u de domeinnaam aan de serverconfiguratie hebt toegevoegd, regeneert u alle Tomcat-certificaten voordat u ze installeert op de andere toepassingen, in de clientbrowsers, of op generatie van de certificaatondertekeningaanvraag (CSR) voor ondertekening.

Gebruikte componenten

De informatie die in dit document wordt beschreven, is gebaseerd op deze hardware- en softwarecomponenten:

- UCX-webservices
- UCS Notification Service
- UCS platform Tomcat
- Cisco Finesse Tomcat
- Tomcat voor Cisco Unified Intelligence Center (CUIC)
- SocialMiner Tomcat
- MediaSense-webservices

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 live is, moet u de potentiële impact van

elke opdracht begrijpen.

Achtergrondinformatie

Met de introductie van co-resident Finesse en CUIC, de integratie tussen UCCX en SocialMiner voor e-mail en chat, en het gebruik van MediaSense om certificaten op te nemen, te begrijpen en te installeren via Finesse, is de mogelijkheid om problemen met certificaten op te lossen nu van cruciaal belang.

Dit document beschrijft het gebruik van zowel zelfondertekende als ondertekende certificaten in de UCCX-configuratieomgeving die het volgende omvat:

- UCS CX-meldingsservices
- UCX-webservices
- UCS X-scripts
- medeingezette Finesse
- Co-ingezette CUIC (gegevens uit het verleden en historische rapportage)
- MediaSense (op Finesse gebaseerde opname en codering)
- SocialMiner (chat)

Certificaten, ondertekend of zelf ondertekend, moeten worden geïnstalleerd op zowel de toepassingen (servers) in de UCCX-configuratie als op de agent en supervisor client-desktops.

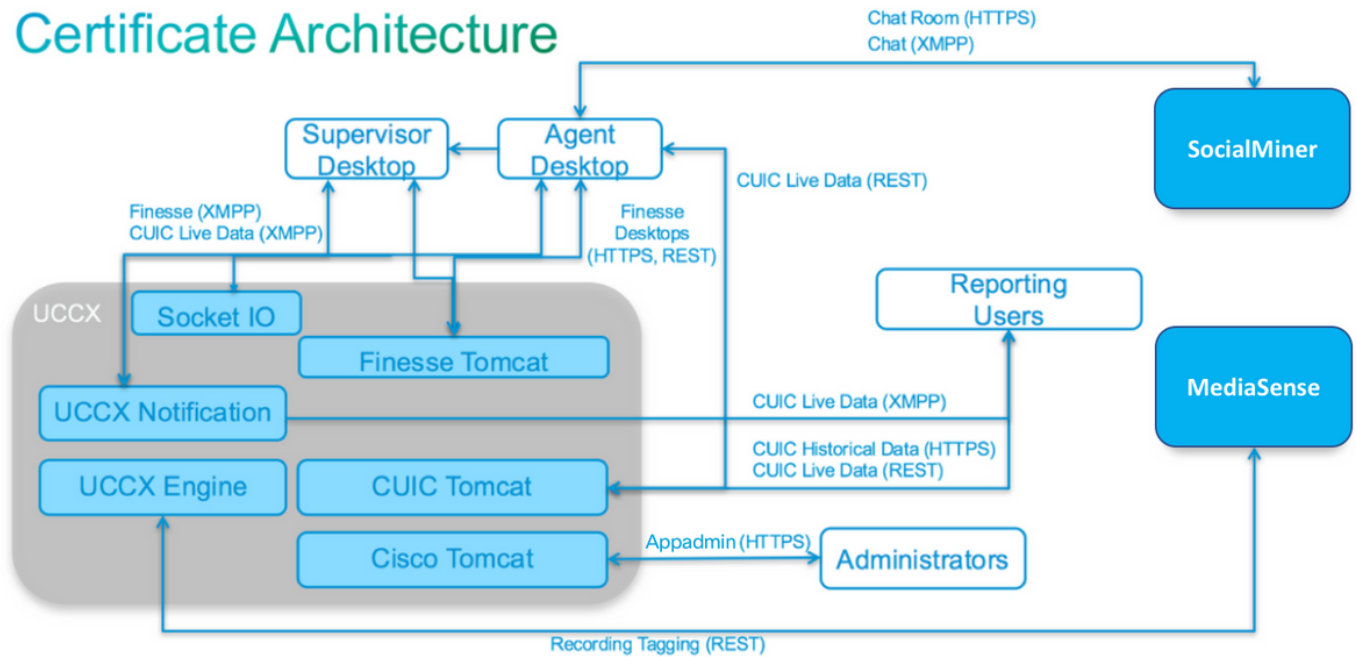
In Unified Communications Operating System (UCOS) 10.5 zijn multiserver-certificaten toegevoegd, zodat één enkele CSR kan worden gegenereerd voor een cluster in plaats van dat voor elk knooppunt in het cluster een afzonderlijk certificaat hoeft te worden ondertekend. Dit type certificaat wordt expliciet niet ondersteund voor UCCX, MediaSense en SocialMiner.

Configureren

In deze sectie wordt beschreven hoe u de UCCX kunt configureren voor het gebruik van zelfondertekende en ondertekende certificaten.

Configuratiediagram

Certificate Architecture



UCCX-oplossingsarchitectuur geldig vanaf UCCX 11.0. HTTPS-communicatiediagram.

Ondertekende certificaten

De aanbevolen methode van certificaatbeheer voor de UCCX-configuratie is om ondertekende certificaten te gebruiken. Deze certificaten kunnen worden ondertekend door een interne certificeringsinstantie (CA) of een bekende derde-certificeringsinstantie.

In grote browsers, zoals Mozilla Firefox en Internet Explorer, worden basiscertificaten voor bekende CA's van derden standaard geïnstalleerd. De certificaten voor UCCX-configuratie-toepassingen die door deze CA's zijn ondertekend, worden standaard vertrouwd, aangezien hun certificaatketen eindigt in een basiscertificaat dat al in de browser is geïnstalleerd.

Het basiscertificaat van een interne CA kan ook vooraf in de clientbrowser worden geïnstalleerd via een groepsbeleid of andere huidige configuratie.

U kunt kiezen of u de UCCX-configuratie-toepassingscertificaten wilt laten ondertekenen door een bekende derde CA of door een interne CA op basis van de beschikbaarheid en voorinstallatie van het basiscertificaat voor de CA's in de clientbrowser.

Ondertekende Tomcat-toepassingscertificaten installeren

Voltooi deze stappen voor elk knooppunt van de UCS Publisher- en Subscriber-, SocialMiner- en MediaSense Publisher- en Subscriber-beheertoepassingen:

1. Navigeer naar de pagina **OS-beheer** en kies **Beveiliging > Certificaatbeheer**.
2. Klik op **Generate CSR**.
3. Kies in de vervolgkeuzelijst **Certificaatlijst** de optie als certificaatnaam en klik op **Generate CSR**.
4. Navigeren naar **Beveiliging > Certificaatbeheer** en kiezen **Download CSR**.
5. Kies in het pop-upvenster de optie **Opslaan** uit de vervolgkeuzelijst en klik op **CSR downloaden**.

Verzend de nieuwe MVO naar de derde CA of onderteken het met een interne CA, zoals eerder beschreven. Dit proces moet de volgende ondertekende certificaten opleveren:

- basiscertificaat voor CA
- UCS Publisher-toepassingscertificaat
- UCS Subscriber-toepassingscertificaat
- SocialMiner-toepassingscertificaat
- MediaSense Publisher-toepassingscertificaat
- MediaSense Subscriber-toepassingscertificaat

Opmerking: Laat het veld **Distribution** in de CSR staan als FQDN van de server.

Opmerking: Het "Multi-server (SAN)"-certificaat wordt vanaf 11.6 release ondersteund voor UCS. Het SAN mag echter alleen UCS Node-1 en Node-2 bevatten. Andere servers, zoals SocialMiner, zouden niet in SAN van UCCX moeten worden omvat.

Opmerking: UCCX ondersteunt alleen certificaathoofd lengten van 1024- en 2048-bits.

Voltooi deze stappen op elke toepassingsserver om het wortelcertificaat en toepassingscertificaat aan de knooppunten te uploaden:

Opmerking: Als u de wortel en de middencertificaten op een uitgever (UCCX of MediaSense) uploadt, zou het automatisch aan de abonnee moeten worden herhaald. Het is niet nodig om de root- of tussenliggende certificaten te uploaden naar de andere, niet-uitgever servers in de configuratie als alle toepassingscertificaten zijn ondertekend via dezelfde certificaatketen.

1. Navigeer naar de pagina **OS-beheer** en kies **Beveiliging > Certificaatbeheer**.
2. Klik op **Uploadcertificaat**.
3. Upload het basiscertificaat en kies **tomcat-trust** als het certificaattype.
4. Klik op **Uploadbestand**.
5. Klik op **Uploadcertificaat**.
6. Upload het aanvraagcertificaat en kies **tomcat** als certificaattype.
7. Klik op **Uploadbestand**. **Opmerking:** Als een ondergeschikte CA het certificaat ondertekent, upload dan het basiscertificaat van de ondergeschikte CA als het *tomcat-trust* certificaat in plaats van het basiscertificaat. Als een tussentijds certificaat wordt afgegeven, uploadt u dit certificaat naar de *tomcat-trust* store naast het aanvraagcertificaat.
8. Start de volgende toepassingen opnieuw op als u deze hebt voltooid: Cisco MediaSense uitgever en abonneeCisco SocialMinerCisco UCS Publisher en Subscriber

Opmerking: Wanneer u UCCX, MediaSense, en SocialMiner 11.5 en later gebruikt, is er een nieuw certificaat genaamd tomcat-ECDSA. Wanneer u een ondertekend certificaat tomcat-ECDSA aan de server uploadt, upload het toepassingscertificaat als een certificaat van tomcat-ECDSA-niet een certificaat van tomcat. Raadpleeg voor meer informatie over ECDSA de sectie Verwante informatie voor de link om ECDSA-certificaten te begrijpen en te configureren.

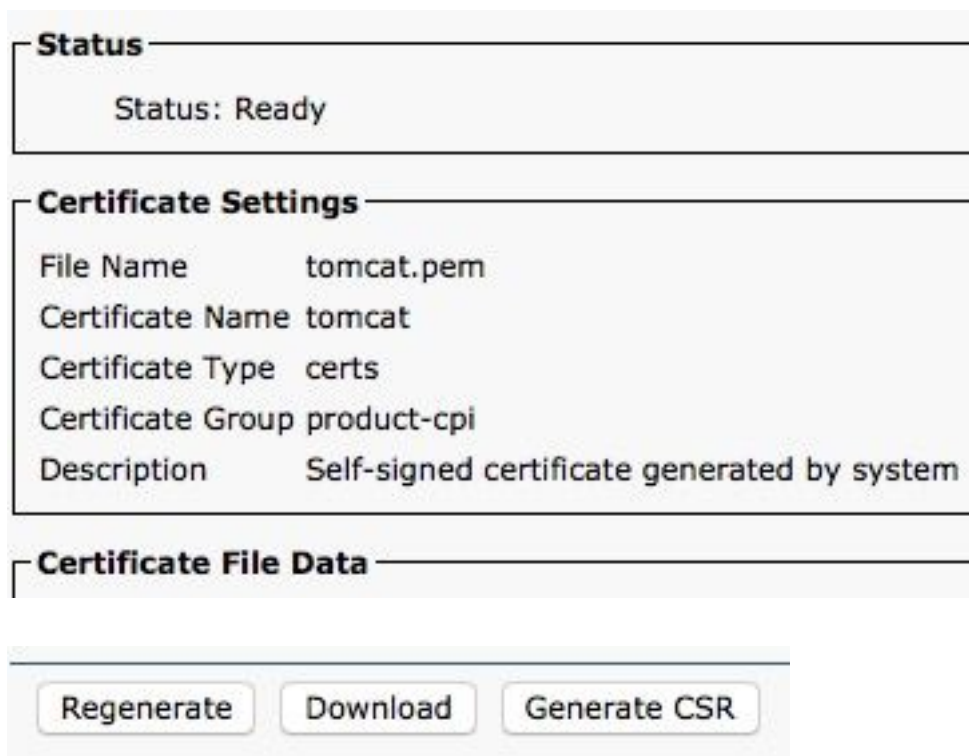
Zelfondertekende certificaten

Installeren op randservers

Alle certificaten die in de UCCX-configuratie worden gebruikt, worden vooraf geïnstalleerd op de configuratietoepassingen en zijn zelf ondertekend. Deze zelf-ondertekende certificaten worden niet impliciet vertrouwd wanneer voorgesteld aan of clientbrowser of een andere configuratietoepassing. Hoewel het is aanbevolen om alle certificaten in de UCCX-configuratie te ondertekenen, kunt u de vooraf geïnstalleerde zelfondertekende certificaten gebruiken.

Voor elke toepassingsrelatie moet u het juiste certificaat downloaden en uploaden naar de applicatie. Voltooi deze stappen om de certificaten te verkrijgen en te uploaden:

1. Ga naar de pagina **Application OS Administration** en kies **Security > Certificate Management**.
2. Klik op het juiste certificaat **.pem**-bestand en kies **Downloaden**:



The screenshot displays the 'Certificate Management' interface. It is divided into three sections:

- Status:** Shows 'Status: Ready'.
- Certificate Settings:** Lists the following details:
 - File Name: tomcat.pem
 - Certificate Name: tomcat
 - Certificate Type: certs
 - Certificate Group: product-cpi
 - Description: Self-signed certificate generated by system
- Certificate File Data:** This section is currently empty.

At the bottom of the interface, there are three buttons: 'Regenerate', 'Download', and 'Generate CSR'.

3. Om een certificaat op de juiste toepassing te uploaden, navigeer naar de **OS-beheerpagina** en kies **Beveiliging > Certificaatbeheer**.
4. Klik op **Certificaat uploaden / certificaatketen**:



5. Start deze servers na voltooiing opnieuw op:

Cisco MediaSense uitgever en abonnee
Cisco SocialMiner
Cisco UCS Publisher en Subscriber

Om zelf ondertekende certificaten op de clientmachine te installeren, gebruikt u een groepsbeleid of pakketbeheer of installeert u deze afzonderlijk in de browser van elke agent-pc.

Installeer voor Internet Explorer de door de client ondertekende certificaten in het archief van

Trusted Root Certification Authorities.

Voltooi voor Mozilla Firefox de volgende stappen:

1. Ga naar **Gereedschappen > Opties**.
2. Klik op het tabblad **Geavanceerd**.
3. Klik op **Certificaten bekijken**.
4. Navigeer naar het tabblad **Servers**.
5. Klik op **Exceptie toevoegen**.

Zelfondertekende certificaten regenereren

In het geval dat zelfondertekende certificaten verlopen, moeten ze worden geregenereerd en moeten de configuratiestappen van **Installeren op randservers** opnieuw worden uitgevoerd.

1. Toegang tot de toepassing **IOS-beheer** pagina en kies **Beveiliging > Certificaatbeheer**.
2. Klik op het juiste certificaat en kies **Regenerate**.
3. De server waarvan het certificaat is geregenereerd, moet opnieuw worden gestart.
4. Voor elke toepassingsrelatie moet u het juiste certificaat downloaden en het naar de toepassing uploaden volgens de configuratiestappen van **Installeren op randservers**.

Integratie en clientconfiguratie

UCS-to-MediaSense

UCCX gebruikt de MediaSense web services REST Application Programming Interface (API) voor twee doeleinden:

- Om een abonnement te nemen op meldingen van nieuwe opnames die worden aangeroepen op de Cisco Unified Communications Manager (CUCM).
- Zo labelt u opnames van UCCX-agents met informatie over de agent en de Contact Service Queue (CSQ).

UCS gebruikt de REST API op de MediaSense beheerknooppunten. Er zijn maximaal twee in elk MediaSense-cluster. De UCCX maakt geen verbinding via de REST API met MediaSense uitbreidingsknooppunten. Beide UCCX-knooppunten moeten de MediaSense REST API gebruiken, dus installeer de twee MediaSense Tomcat-certificaten op beide UCCX-knooppunten.

Upload de ondertekende of zelf-ondertekende certificaatketen van de MediaSense servers naar de UCCX *tomcat-trust* keystore.

MediaSense-to-Finesse

MediaSense gebruikt de Finesse Web Services REST API om agenten voor de MediaSense Search en Play gadget op Finesse te verifiëren.

De MediaSense-server die op de Finesse XML-lay-out voor de Search and Play-gadget is geconfigureerd, moet de Finesse REST API gebruiken, dus installeer de twee UCCX Tomcat-certificaten op die MediaSense-knooppunt.

Upload de ondertekende of zelf-ondertekende certificaatketen van de UCCX-servers naar de MediaSense *tomcat-trust* keystore.

UCCX-to-SocialMiner

De UCCX gebruikt de SocialMiner REST en Notification API's om e-mailcontacten en configuratie te beheren. Beide UCCX-knooppunten moeten de SocialMiner REST API gebruiken en worden aangemeld door de SocialMiner meldingsdienst, dus installeer het SocialMiner Tomcat-certificaat op beide UCCX-knooppunten.

Upload de ondertekende of zelf-ondertekende certificaatketen van de SocialMiner-server naar de UCCX *tomcat-trust* keystore.

UCS AppAdmin-clientcertificaat

Het UCCX AppAdmin-clientcertificaat wordt gebruikt voor het beheer van het UCCX-systeem. Om het UCCX AppAdmin-certificaat voor UCCX-beheerders te installeren, navigeer op de client-pc naar <https://<UCCX FQDN>/appadmin/main> voor elk van de UCCX-knooppunten en installeer het certificaat via de browser.

UCS Platform-clientcertificaat

De UCCX webservices worden gebruikt voor het leveren van chat contacten aan client browsers. Om het UCCX Platform-certificaat voor UCCX-agents en -supervisors op de client-pc te installeren, navigeer je naar <https://<UCCX FQDN>/appadmin/main> voor elk van de UCCX-knooppunten en installeer je het certificaat via de browser.

Clientcertificaat voor kennisgevingservice

De CCX Notification Service wordt gebruikt door Finesse, UCCX en CUIC om real-time informatie naar de client-desktop te sturen via Extensible Messaging and Presence Protocol (XMPP). Dit wordt gebruikt voor real-time Finesse communicatie en voor CUIC Live Data.

Om het clientcertificaat van de Notification Service op de pc te installeren van de agents en toezichthouders of gebruikers die Live Data gebruiken, navigeer je naar <https://<UCCX FQDN>:7443/> voor elk van de UCCX-knooppunten en installeer je het certificaat via de browser.

Clientcertificaat voltooien

Het Finesse-clientcertificaat wordt door de Finesse-desktops gebruikt om verbinding te maken met het Finesse Tomcat-exemplaar ten behoeve van de REST API-communicatie tussen het bureaublad en de co-resident Finesse-server.

Om het Finesse-certificaat voor agents en supervisors op de client-pc te installeren, navigeer je naar <https://<UCCX FQDN>:8445/> voor elk van de UCCX-knooppunten en installeer je het certificaat via de aanwijzingen van de browser.

Om het Finesse-certificaat voor Finesse-beheerders te installeren, navigeer op de client-pc naar <https://<UCCX FQDN>:845/cfadmin> voor elk van de UCCX-knooppunten en installeer het certificaat via de aanwijzingen in de browser.

SocialMiner-clientcertificaat

Het SocialMiner Tomcat-certificaat moet op de clientmachine worden geïnstalleerd. Zodra een agent een chatverzoek accepteert, wordt de Chat gadget omgeleid naar een URL die de chat room vertegenwoordigt. Deze chatroom wordt gehost door de SocialMiner server en bevat de klant of chat contact.

Om het SocialMiner certificaat in de browser te installeren, op de client-pc, navigeer naar [https://<SocialMiner FQDN>/](https://<SocialMiner FQDN>) en installeer het certificaat via de browser aanwijzingen.

CUIC-clientcertificaat

Het CUIC Tomcat-certificaat moet op de clientmachine worden geïnstalleerd voor agenten, toezichthouders en rapportagegebruikers die de CUIC-webinterface gebruiken voor historische rapporten of Live Data-rapporten, hetzij binnen de CUIC-webpagina of binnen de gadgets in het bureaublad.

Om het CUIC Tomcat-certificaat in de browser te installeren, op de client-pc, navigeer naar <https://<UCCX FQDN>:8444/> en installeer het certificaat via de aanwijzingen van de browser.

CUIC Live Data Certificate (sinds 11.x)

De CUIC gebruikt de Socket IO-service voor de backkend Live-gegevens. Dit certificaat moet op de clientmachine worden geïnstalleerd voor agenten, toezichthouders en rapporterende gebruikers die de CUIC-webinterface voor Live Data gebruiken of die de Live Data gadgets binnen Finesse gebruiken.

Om het Socket IO-certificaat in de browser te installeren, op de client-pc, navigeer naar <https://<UCCX FQDN>:12015/> en installeer het certificaat via de aanwijzingen van de browser.

Toepassingen van derden die toegankelijk zijn via scripts

Als een UCCX-script is ontworpen om toegang te krijgen tot een beveiligde locatie op een server van derden (bijvoorbeeld *Get URL Document* step to an HTTPS URL or a *Make Rest Call* to an HTTPS REST URL), uploadt u de ondertekende of zelf-ondertekende certificaatketen van de dienst van derden naar de UCCX *tomcat-trust* keystore. Om dit certificaat te verkrijgen, raadpleegt u de pagina **Beheer** van UCCX OS en kiest u **Uploadcertificaat**.

De UCCX Engine is geconfigureerd om het platform Tomcat keystore te doorzoeken naar certificaatkettingen van derden wanneer deze certificaten worden aangeboden door applicaties van derden wanneer zij via scriptstappen toegang krijgen tot beveiligde locaties.

De gehele certificaatketen moet worden geüpload naar het platform Tomcat keystore, dat toegankelijk is via de **OS Administration** pagina, omdat de Tomcat keystore standaard geen basiscertificaten bevat.

Nadat u deze acties hebt voltooid, moet u Cisco UCS Engine opnieuw opstarten.

Verifiëren

Om te controleren of alle certificaten correct zijn geïnstalleerd, kunt u de functies testen die in deze sectie worden beschreven. Als er geen certificaatfouten worden weergegeven en alle functies correct functioneren, worden de certificaten correct geïnstalleerd.

- Finesse instellen zodat het automatisch een agent registreert via de workflow. Nadat een oproep door de agent is verwerkt, gebruikt u de MediaSense Search and Play-toepassing om de oproep te vinden. Controleer dat de oproep de agent, een CSQ en teamtags heeft die aan de opnamemetagegevens in MediaSense zijn gekoppeld.
- Configureren van Agent Web Chat via SocialMiner. Neem contact op met de chat via het webformulier. Controleer dat de agent de banner ontvangt om de chat contact te accepteren en ook te verifiëren dat zodra chat contact is geaccepteerd, het chat formulier goed wordt geladen en de agent kan zowel ontvangen als chat berichten verzenden.
- Probeer via Finesse een agent in te loggen. Controleer dat er geen certificaatwaarschuwingen verschijnen en dat de webpagina niet vraagt om de installatie van certificaten in de browser. Controleer of de agent de status correct kan wijzigen en of een nieuwe oproep naar UCCX correct aan de agent wordt gepresenteerd.
- Nadat u de Live Data gadgets in de agent en supervisor Finesse desktop lay-out configureren, logt u in op een agent, een supervisor en een rapportagegebruiker. Controleer dat de Live Data gadgets goed laden, dat de eerste gegevens in het gadget worden ingevuld en dat de gegevens worden ververs wanneer de onderliggende gegevens veranderen.
- Probeer verbinding te maken van een browser met de AppAdmin URL op beide UCCX-knooppunten. Controleer dat er geen certificaatwaarschuwingen verschijnen wanneer deze worden gevraagd op de inlogpagina.

Problemen oplossen

Probleem - Ongeldige gebruikers-id/wachtwoord

UCS FineReader kan niet inloggen met de fout "**Ongeldige gebruikersnaam/wachtwoord**".

Oorzaken

Unified CCX maakt gebruik van de uitzondering "SSLHandshakeException" en slaagt er niet in een verbinding tot stand te brengen met Unified CM.

Oplossing

- Controleer of het Unified CM Tomcat-certificaat niet is verlopen.
- Zorg ervoor dat elk certificaat dat u in Unified CM geüpload heeft een van deze extensies gemarkeerd als kritiek:
 - X509v3 toetsgebruik (OID - 2.5.29.15)
 - X509v3 basisbeperkingen (OID - 2.5.29.19)Als u andere extensies als kritisch markeert, mislukt de communicatie tussen Unified CCX en Unified CM vanwege de mislukking van Unified CM certificaat verificatie.

Probleem - MVO-SAN en -certificaat komen niet overeen

Het uploaden van een CA ondertekend certificaat toont fout "CSR SAN en Certificate SAN niet overeenkomen".

Oorzaken

CA kan een ander parent-domein toegevoegd hebben in het veld Certificate Subjective Alternative Names (SAN). Standaard beschikt de MVO over deze SAN's:

```
OnderwerpAltName [  
  example.com (NSName)  
  hostname.example.com (NSName)  
]
```

CA's kunnen een certificaat retourneren met een ander SAN dat aan het certificaat is toegevoegd: www.hostname.example.com. Het certificaat heeft in dit geval een extra SAN:

```
OnderwerpAltName [  
  example.com (NSName)  
  hostname.example.com (NSName)  
  
  www.hostname.example.com (NSName)  
]
```

Dit veroorzaakt een SAN-fout.

Oplossing

Voer in de sectie 'Onderwerp Alternatieve naam (SAN's)' van de UCCX-pagina 'Generate Certificate Signing request' (verzoek om certificaat te ondertekenen) de CSR uit met een leeg veld voor het ouderdomein. Op deze manier wordt de CSR niet gegenereerd met een SAN-kenmerk, kan de CA de SAN's formatteren en er zal geen wanverhouding van het SAN-kenmerk optreden wanneer u het certificaat naar UCCX uploadt. Merk op dat het veld Parent Domain standaard is ingesteld voor het domein van de UCCX-server. De waarde moet dus expliciet worden verwijderd terwijl de instellingen voor de CSR zijn geconfigureerd.

Probleem - NET::ERR_CERT_Common_NAME_INVALIDITY

Wanneer u een UCCX-, MediaSense- of SocialMiner-webpagina bezoekt, ontvangt u een foutmelding.

"Uw verbinding is niet privé.

De aanvallers zouden kunnen proberen om uw informatie van <Server_FQDN> (bijvoorbeeld wachtwoorden, berichten, of creditcards) te stelen.
NETTO::ERR_CERT_COMMON_NAME_INVALID

Deze server kon niet bewijzen dat het <Server_FQDN> is; het beveiligingscertificaat is afkomstig van [missing_subjectAltName]. Dit kan veroorzaakt worden door een misconfiguratie of een aanvaller die uw verbinding onderschept."

Oorzaken

Chrome versie 58 heeft een nieuwe beveiligingsfunctie geïntroduceerd waarbij wordt gemeld dat het certificaat van een website niet veilig is als de gemeenschappelijke naam (CN) niet ook als SAN is opgenomen.

Oplossing

- U kunt navigeren naar **Advanced > Ga verder naar <Server FQDN> (onveilig)** om verder te gaan naar de site en de certificaatfout te accepteren.
- U kunt de fout geheel vermijden met CA ondertekende certificaten. Wanneer u een CSR genereert, wordt de FQDN van de server als SAN opgenomen. CA kan de CSR ondertekenen en nadat u het ondertekende certificaat weer naar de server hebt geüpload, krijgt het servercertificaat de FQDN in het SAN-veld, zodat de fout niet wordt weergegeven.

Meer informatie

Zie de sectie "Ondersteuning verwijderen voor commonName matching in certificaten" in [Afschrijvingen en verwijderingen in Chrome 58](#).

Certificaatgebreken

- Cisco bug-id [CSCvb46250](#) - UCS: Tomcat ECDSA certificaat impact op Finesse Live Data
- Cisco bug-id [CSCvb58580](#) - kan niet inloggen op SocialMiner met zowel tomcat als tomcat-ECDSA ondertekend door RSA-certificeringsinstantie
- Cisco bug-id [CSC56174](#) - UCS: Aanmeldingsfout Finesse Agent door SSLHandshakeException
- Cisco bug-id [CSCuv89545](#) - kwetsbaarheid voor Finesse Logjam

Gerelateerde informatie

- [ECDSA-certificaten in een UCS-oplossing begrijpen](#)
- [Ondersteuning van SHA 256 voor UCS](#)
- [Configuratievoorbeeld van UCS-ondertekende en zelfondertekende certificaten](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.