UCCX Solution Certificate Management-Leitfaden

Inhalt

Einleitung
Voraussetzungen
Anforderungen
FQDN, DNS und Domänen
Verwendete Komponenten
Hintergrundinformationen
Konfigurieren
Konfigurationsdiagramm
Signierte Zertifikate
Installieren der signierten Tomcat-Anwendungszertifikate
Selbstsignierte Zertifikate
Installation auf Peripherieservern
Eigensignierte Zertifikate generieren
Integration und Client-Konfiguration
UCCX-to-MediaSense
MediaSense-to-Finesse
UCCX-to-SocialMiner
UCCX AppAdmin-Clientzertifikat
UCCX-Plattform-Client-Zertifikat
Client-Zertifikat des Benachrichtigungsdiensts
Finesse Client-Zertifikat
SocialMiner-Clientzertifikat
CUIC-Clientzertifikat
Zugriff auf Drittanbieteranwendungen über Skripts
Überprüfung
Fehlerbehebung
Problem: Ungültige Benutzer-ID/ungültiges Kennwort
Ursachen
Lösung
Problem - CSR-SAN und Zertifikat-SAN stimmen nicht überein
Ursachen
Lösung
Problem - NET::ERR_CERT_COMMON_NAME_INVALID
Ursachen
Lösung
Weitere Informationen
Zertifikatfehler
Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie Cisco Unified Contact Center Express (UCCX) für die Verwendung von selbstsignierten und signierten Zertifikaten konfiguriert wird.

Voraussetzungen

Anforderungen

Bevor Sie mit den in diesem Dokument beschriebenen Konfigurationsschritten fortfahren, stellen Sie sicher, dass Sie auf die Seite Betriebssystem-Administration für folgende Anwendungen zugreifen können:

- UCCX
- SocialMiner
- MediaSense

Ein Administrator sollte außerdem Zugriff auf den Zertifikatsspeicher auf den Client-PCs des Agenten und Supervisors haben.

FQDN, DNS und Domänen

Alle Server in der UCCX-Konfiguration müssen mit DNS-Servern (Domain Name System) und Domänennamen installiert werden. Außerdem müssen Agenten, Supervisoren und Administratoren über den FQDN (Fully Qualified Domain Name) auf die UCCX-Konfigurationsanwendungen zugreifen.

UCCX Version 10.0+ erfordert, dass der Domänenname und die DNS-Server bei der Installation eingetragen werden. Die Zertifikate, die vom UCCX Version 10.0+-Installationsprogramm generiert werden, enthalten den entsprechenden FQDN. Fügen Sie dem UCCX-Cluster die DNS-Server und eine Domäne hinzu, bevor Sie ein Upgrade auf UCCX Version 10.0+ durchführen.

Wenn sich die Domäne ändert oder zum ersten Mal ausgefüllt wird, müssen die Zertifikate neu generiert werden. Nachdem Sie der Serverkonfiguration den Domänennamen hinzugefügt haben, müssen Sie alle Tomcat-Zertifikate neu generieren, bevor Sie sie in den anderen Anwendungen, im Clientbrowser oder bei Generierung der Zertifikatsanforderung (Certificate Signing Request, CSR) für die Signierung installieren.

Verwendete Komponenten

Die in diesem Dokument beschriebenen Informationen basieren auf folgenden Hardware- und Softwarekomponenten:

- UCCX-Webservices
- UCCX-Benachrichtigungsdienst
- UCCX-Plattform - Tomcat
- Cisco Finesse Tomcat
- Cisco Unified Intelligence Center (CUIC) Tomcat
- SocialMiner Tomcat

- MediaSense-Webdienste

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Mit der Einführung von Co-Resident Finesse und CUIC, der Integration von UCCX und SocialMiner für E-Mail und Chat und der Verwendung von MediaSense zum Aufzeichnen, Verstehen und Installieren von Zertifikaten über Finesse ist die Möglichkeit, Zertifikatprobleme zu beheben, von entscheidender Bedeutung geworden.

In diesem Dokument wird die Verwendung von selbstsignierten und signierten Zertifikaten in der UCCX-Konfigurationsumgebung beschrieben. Dabei werden folgende Punkte behandelt:

- UCCX-Benachrichtigungsdienste
- UCCX-Webservices
- UCCX-Skripte
- Co-Resident Finesse
- Co-Resident CUIC (Live-Daten und Verlaufsberichte)
- MediaSense (Aufzeichnung und Tagging auf Finesse-Basis)
- SocialMiner (Chat)

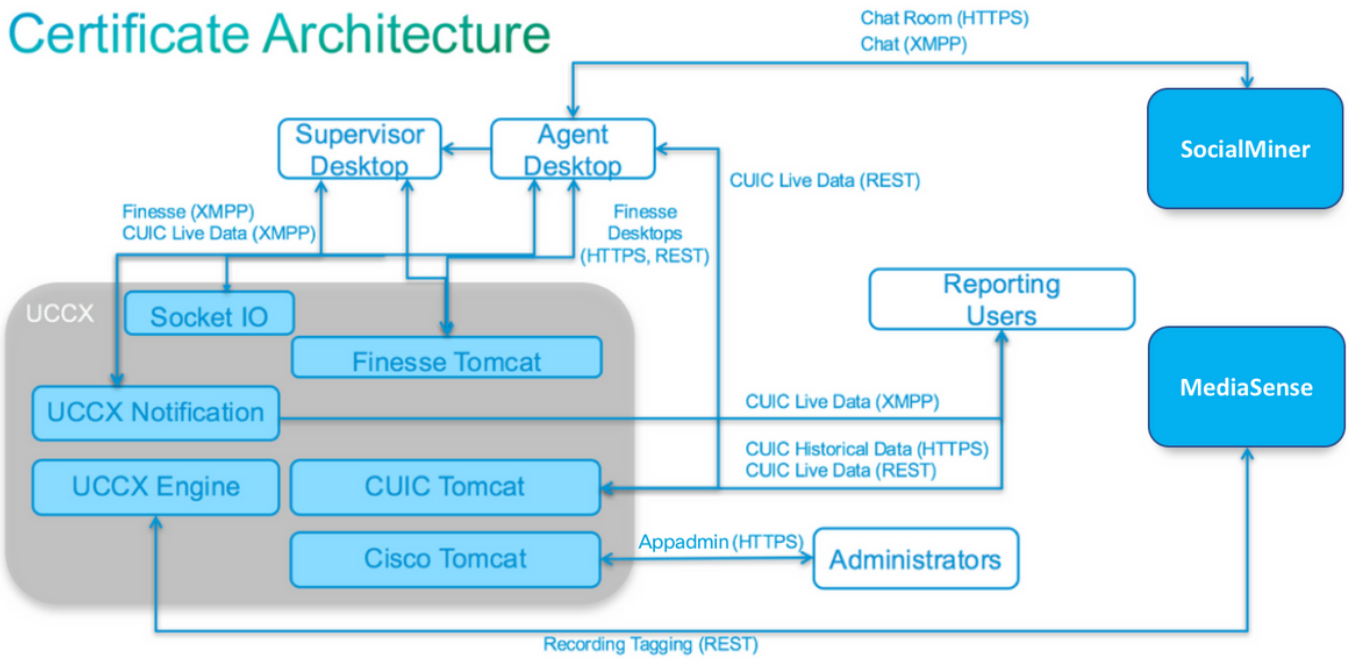
Zertifikate, signiert oder selbstsigniert, müssen sowohl auf den Anwendungen (Servern) in der UCCX-Konfiguration als auch auf den Client-Desktops der Agenten und Supervisoren installiert werden.

In Unified Communications Operating System (UCOS) 10.5 wurden Multi-Server-Zertifikate hinzugefügt, sodass ein einzelner CSR für einen Cluster generiert werden konnte, anstatt ein einzelnes Zertifikat für jeden Knoten im Cluster signieren zu müssen. Dieser Zertifikatstyp wird für UCCX, MediaSense und SocialMiner explizit nicht unterstützt.

Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie das UCCX für die Verwendung von selbstsignierten und signierten Zertifikaten konfigurieren.

Konfigurationsdiagramm



UCCX-Lösungsarchitektur gültig ab UCCX 11.0. HTTPS-Kommunikationsdiagramm.

Signierte Zertifikate

Die empfohlene Methode für das Zertifikatsmanagement für die UCCX-Konfiguration ist die Nutzung signierter Zertifikate. Diese Zertifikate können entweder von einer internen Zertifizierungsstelle (Certificate Authority, CA) oder einer bekannten Zertifizierungsstelle eines Drittanbieters signiert werden.

In gängigen Browsern wie Mozilla Firefox und Internet Explorer werden standardmäßig Root-Zertifikate für bekannte Drittanbieter-CAs installiert. Die Zertifikate für UCCX-Konfigurationsanwendungen, die von diesen CAs signiert werden, sind standardmäßig vertrauenswürdig, da ihre Zertifikatkette in einem Stammzertifikat endet, das bereits im Browser installiert ist.

Das Stammzertifikat einer internen Zertifizierungsstelle kann auch im Clientbrowser über eine Gruppenrichtlinie oder eine andere aktuelle Konfiguration vorinstalliert werden.

Sie können wählen, ob die UCCX-Konfigurationsanwendungszertifikate von einer bekannten Drittanbieter-Zertifizierungsstelle oder von einer internen Zertifizierungsstelle signiert werden sollen. Dies hängt von der Verfügbarkeit und Vorinstallation des Stammzertifikats für die Zertifizierungsstellen im Clientbrowser ab.

Installieren der signierten Tomcat-Anwendungszertifikate

Führen Sie die folgenden Schritte für jeden Knoten der UCCX Publisher- und Subscriber-, SocialMiner-, MediaSense Publisher- und Subscriber-Administrationsanwendungen aus:

1. Navigieren Sie zur Seite **OS Administration (Betriebssystemverwaltung)**, und wählen Sie **Security > Certificate Management (Sicherheit > Zertifikatsverwaltung)**.
2. Klicken Sie auf **CSR erstellen**.
3. Wählen Sie in der Dropdown-Liste **"Zertifikatsliste" aus,** um den Zertifikatsnamen zu übernehmen, und klicken Sie auf **CSR generieren**.

4. Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung,** und wählen Sie **CSR herunterladen aus**.
5. Wählen Sie im Popup-Fenster aus der Dropdown-Liste **Tomcat** aus, und klicken Sie auf **CSR herunterladen**.

Senden Sie den neuen CSR an die Drittanbieter-CA, oder signieren Sie ihn mit einer internen CA, wie zuvor beschrieben. Dieser Prozess muss folgende signierte Zertifikate erstellen:

- Stammzertifikat für die Zertifizierungsstelle
- UCCX Publisher-Anwendungszertifikat
- UCCX Subscriber-Anwendungszertifikat
- SocialMiner-Anwendungszertifikat
- MediaSense Publisher-Anwendungszertifikat
- MediaSense-Teilnehmeranwendungszertifikat

Anmerkung: Lassen Sie das Feld **Distribution** im CSR als FQDN des Servers unverändert.

Anmerkung: Das "Multi-Server (SAN)"-Zertifikat wird für UCCX ab Version 11.6 unterstützt. Das SAN sollte jedoch nur UCCX Node-1 und Node-2 enthalten. Andere Server wie SocialMiner sollten nicht im SAN von UCCX enthalten sein.

Anmerkung: UCCX unterstützt nur Zertifikatschlüssellängen von 1024 und 2048 Bit.

Führen Sie auf jedem Anwendungsserver die folgenden Schritte aus, um das Stammzertifikat und das Anwendungszertifikat auf die Knoten hochzuladen:

Anmerkung: Wenn Sie das Root- und Zwischenzertifikat auf einen Herausgeber (UCCX oder MediaSense) hochladen, sollte es automatisch auf den Abonnenten repliziert werden. Es ist nicht erforderlich, die Stamm- oder Zwischenzertifikate auf die anderen Server ohne Herausgeber in der Konfiguration hochzuladen, wenn alle Anwendungszertifikate über dieselbe Zertifikatskette signiert sind.

1. Navigieren Sie zur Seite **OS Administration (Betriebssystemverwaltung**), und wählen Sie **Security > Certificate Management (Sicherheit > Zertifikatsverwaltung)**.
2. Klicken Sie auf **Zertifikat hochladen**.
3. Laden Sie das Stammzertifikat hoch, und wählen Sie **tomcat-trust** als Zertifikatstyp aus.
4. Klicken Sie auf **Datei hochladen**.
5. Klicken Sie auf **Zertifikat hochladen**.
6. Laden Sie das Anwendungszertifikat hoch, und wählen Sie **Tomcat** als Zertifikatstyp aus.
7. Klicken Sie auf **Datei hochladen**. **Anmerkung:** Wenn eine untergeordnete Zertifizierungsstelle das Zertifikat signiert, laden Sie das Stammzertifikat der untergeordneten Zertifizierungsstelle als *Tomcat-Trust*-Zertifikat anstatt als Stammzertifikat hoch. Wenn ein Zwischenzertifikat ausgestellt wurde, laden Sie dieses Zertifikat zusätzlich zum Anwendungszertifikat in den *tomcat-trust*-Speicher hoch.
8. Starten Sie nach Abschluss des Vorgangs die folgenden Anwendungen neu: Cisco MediaSense Publisher und SubscriberCisco SocialMinerCisco UCCX Publisher und Subscriber

Anmerkung: Wenn Sie UCCX, MediaSense und SocialMiner 11.5 oder höher verwenden,

gibt es ein neues Zertifikat namens tomcat-ECDSA. Wenn Sie ein signiertes Tomcat-ECDSA-Zertifikat auf den Server hochladen, laden Sie das Anwendungszertifikat als Tomcat-ECDSA-Zertifikat hoch - nicht als Tomcat-Zertifikat. Weitere Informationen zu ECDSA finden Sie im Abschnitt "Related Information" (Verwandte Informationen) unter dem Link zum Verständnis und zur Konfiguration von ECDSA-Zertifikaten.

Selbstsignierte Zertifikate

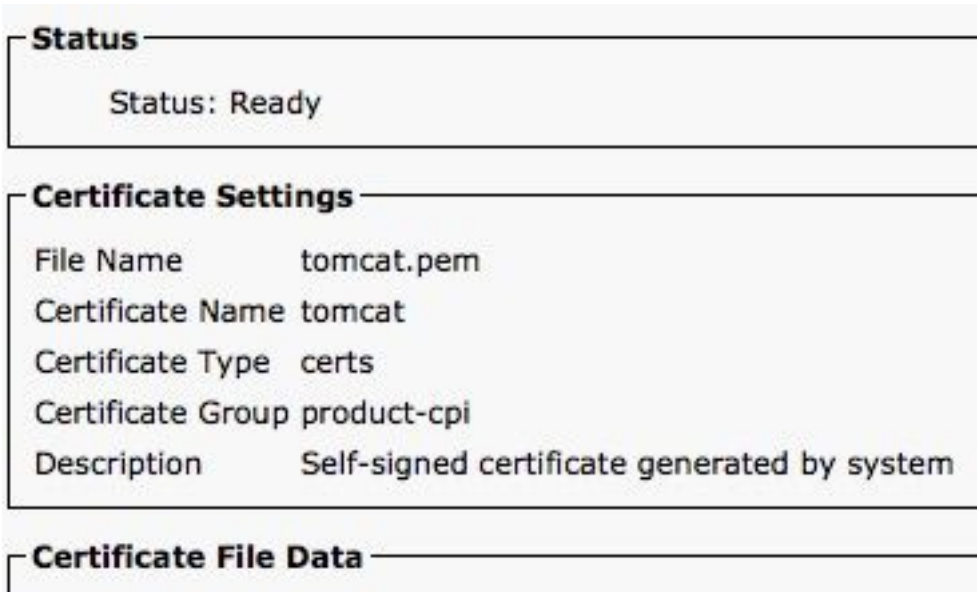
Installation auf Peripherieservern

Alle Zertifikate, die in der UCCX-Konfiguration verwendet werden, sind auf den Konfigurationsanwendungen vorinstalliert und selbstsigniert. Diese selbstsignierten Zertifikate sind nicht implizit vertrauenswürdig, wenn sie einem Clientbrowser oder einer anderen Konfigurationsanwendung vorgelegt werden. Es wird zwar empfohlen, alle Zertifikate in der UCCX-Konfiguration zu signieren, Sie können jedoch die vorinstallierten selbstsignierten Zertifikate verwenden.

Für jede Anwendungsbeziehung müssen Sie das entsprechende Zertifikat herunterladen und in die Anwendung hochladen. Gehen Sie wie folgt vor, um die Zertifikate zu erhalten und hochzuladen:

1. Öffnen Sie die Seite **Betriebssystem-Administration** der Anwendung, und wählen Sie **Sicherheit > Zertifikatsverwaltung aus**.

2. Klicken Sie auf die entsprechende Datei certificate**.pem**, und wählen Sie **Herunterladen**:



3. Um ein Zertifikat in die entsprechende Anwendung hochzuladen, navigieren Sie zur Seite **Betriebssystemverwaltung**, und wählen Sie **Sicherheit > Zertifikatsverwaltung aus**.
4. Klicken Sie auf **Zertifikat hochladen/Zertifikatskette:**

5. Starten Sie nach Abschluss des Vorgangs die folgenden Server neu:

   Cisco MediaSense Publisher und SubscriberCisco SocialMinerCisco UCCX Publisher und Subscriber

Um selbstsignierte Zertifikate auf dem Client-Computer zu installieren, verwenden Sie eine Gruppenrichtlinie oder einen Paketmanager, oder installieren Sie sie einzeln im Browser jedes Agenten-PCs.

Installieren Sie für Internet Explorer die selbstsignierten Zertifikate auf der Clientseite im Speicher der **vertrauenswürdigen Stammzertifizierungsstellen**.

Führen Sie für Mozilla Firefox die folgenden Schritte aus:

1. Navigieren Sie zu **Extras > Optionen**.
2. Klicken Sie auf die Registerkarte **Advanced** (Erweitert).
3. Klicken Sie auf **Zertifikate anzeigen**.
4. Navigieren Sie zur Registerkarte **Server**.
5. Klicken Sie auf **Ausnahme hinzufügen**.

Eigensignierte Zertifikate generieren

Falls selbstsignierte Zertifikate ablaufen, müssen sie neu generiert werden, und die Konfigurationsschritte von **Installation auf Peripherieservern** müssen erneut ausgeführt werden.

1. Zugriff auf die Anwendung **Betriebssystem-Administration** und wähle **Sicherheit > Zertifikatsverwaltung**.
2. Klicken Sie auf das entsprechende Zertifikat, und wählen Sie **Regenerieren aus**.
3. Der Server, dessen Zertifikat neu generiert wurde, muss neu gestartet werden.
4. Für jede Anwendungsbeziehung müssen Sie das entsprechende Zertifikat herunterladen und nach den Konfigurationsschritten von **Installation auf Peripherieservern** in die Anwendung hochladen.

Integration und Client-Konfiguration

UCCX-to-MediaSense

Das UCCX nutzt die MediaSense-Webdienste REST Application Programming Interface (API) für zwei Zwecke:

- Abonnement von Benachrichtigungen über neue Aufzeichnungen, die auf dem Cisco Unified Communications Manager (CUCM) aufgerufen werden
- Kennzeichnung von UCCX-Agenten mit Agenten- und CSQ-Informationen (Contact Service Queue)

Das UCCX nutzt die REST-API auf den MediaSense-Administrationsknoten. Es können maximal zwei MediaSense-Cluster verwendet werden. Das UCCX stellt über die REST-API keine Verbindung zu den MediaSense-Erweiterungsknoten her. Beide UCCX-Knoten müssen die

MediaSense REST-API nutzen. Installieren Sie daher die beiden MediaSense Tomcat-Zertifikate auf beiden UCCX-Knoten.

Laden Sie die signierte oder selbstsignierte Zertifikatskette der MediaSense-Server in den UCCX-*Tomcat-Trust*-Schlüsselspeicher hoch.

MediaSense-to-Finesse

MediaSense verwendet die REST-API der Finesse-Webdienste, um Agenten für das Gadget "MediaSense Search and Play" auf Finesse zu authentifizieren.

Der im Finesse XML-Layout für das Such- und Wiedergabe-Gadget konfigurierte MediaSense-Server muss die Finesse REST-API nutzen. Installieren Sie daher die beiden UCCX Tomcat-Zertifikate auf diesem MediaSense-Knoten.

Laden Sie die signierte oder selbstsignierte Zertifikatskette der UCCX-Server in den MediaSense *toCat-Trust*-Schlüsselspeicher hoch.

UCCX-to-SocialMiner

Das UCCX nutzt die REST- und Benachrichtigungs-APIs von SocialMiner, um E-Mail-Kontakte und -Konfigurationen zu verwalten. Beide UCCX-Knoten müssen die REST-API von SocialMiner nutzen und vom Benachrichtigungsdienst von SocialMiner benachrichtigt werden. Installieren Sie daher das SocialMiner Tomcat-Zertifikat auf beiden UCCX-Knoten.

Laden Sie die signierte oder selbstsignierte Zertifikatkette des SocialMiner-Servers in den UCCX-*Tomcat-Trust*-Schlüsselspeicher hoch.

UCCX AppAdmin-Clientzertifikat

Das UCCX AppAdmin-Client-Zertifikat wird für die Administration des UCCX-Systems verwendet. Um das UCCX AppAdmin-Zertifikat für UCCX-Administratoren auf dem Client-PC zu installieren, navigieren Sie für jeden UCCX-Knoten zu **https://<UCCX FQDN>/appadmin/main,** und installieren Sie das Zertifikat über den Browser.

UCCX-Plattform-Client-Zertifikat

Die UCCX-Webdienste werden für die Übermittlung von Chat-Kontakten an Client-Browser verwendet. Um das UCCX-Plattformzertifikat für UCCX-Agenten und -Supervisoren auf dem Client-PC zu installieren, navigieren Sie zu **https://<UCCX FQDN>/appadmin/main** für jeden UCCX-Knoten, und installieren Sie das Zertifikat über den Browser.

Client-Zertifikat des Benachrichtigungsdiensts

Der CCX Notification Service wird von Finesse, UCCX und CUIC verwendet, um Echtzeitinformationen über Extensible Messaging and Presence Protocol (XMPP) an den Client-Desktop zu senden. Diese Funktion wird für die Finesse-Echtzeitkommunikation sowie für CUIC Live Data verwendet.

Um das Notification Service-Client-Zertifikat auf dem PC der Agenten und Supervisoren oder

Reporting-Benutzer zu installieren, die Live Data verwenden, navigieren Sie für jeden UCCX-Knoten zu **https://<UCCX FQDN>:7443/,** und installieren Sie das Zertifikat über den Browser.

Finesse Client-Zertifikat

Das Finesse Client-Zertifikat wird von den Finesse-Desktops verwendet, um eine Verbindung zur Finesse Tomcat-Instanz für die REST-API-Kommunikation zwischen dem Desktop und dem mitresidierenden Finesse-Server herzustellen.

Um das Finesse-Zertifikat für Agenten und Supervisoren auf dem Client-PC zu installieren, navigieren Sie für jeden UCCX-Knoten zu **https://<UCCX FQDN>:8445/**, und installieren Sie das Zertifikat über die Browser-Eingabeaufforderungen.

Um das Finesse-Zertifikat für Finesse-Administratoren auf dem Client-PC zu installieren, navigieren Sie für jeden UCCX-Knoten zu **https://<UCCX FQDN>:8445/cfadmin,** und installieren Sie das Zertifikat über die Browser-Eingabeaufforderungen.

SocialMiner-Clientzertifikat

Das SocialMiner Tomcat-Zertifikat muss auf dem Client-Computer installiert sein. Sobald ein Mitarbeiter eine Chat-Anfrage annimmt, wird das Chat-Gadget an eine URL umgeleitet, die den Chat-Raum darstellt. Dieser Chat-Raum wird vom SocialMiner-Server gehostet und enthält den Kunden- oder Chat-Kontakt.

Um das SocialMiner-Zertifikat im Browser zu installieren, navigieren Sie auf dem Client-PC zu **https://<SocialMiner FQDN>/** und installieren Sie das Zertifikat über die Browser-Eingabeaufforderungen.

CUIC-Clientzertifikat

Das CUIC Tomcat-Zertifikat sollte auf dem Client-Computer für Agenten, Supervisoren und Benutzer installiert werden, die die CUIC-Webschnittstelle für Verlaufsberichte oder Live Data-Berichte verwenden. Dies gilt entweder für die CUIC-Webseite oder für die Desktop-Gadgets.

Um das CUIC Tomcat-Zertifikat im Browser auf dem Client-PC zu installieren, navigieren Sie zu **https://<UCCX FQDN>:8444/**, und installieren Sie das Zertifikat über die Browser-Eingabeaufforderungen.

CUIC Live Data-Zertifikat (seit 11.x)

Der CUIC verwendet den Socket-E/A-Dienst für die Live-Backend-Daten. Dieses Zertifikat sollte auf dem Client-Computer für Agenten, Supervisoren und Reporting-Benutzer installiert werden, die die CUIC-Webschnittstelle für Live-Daten verwenden oder die Live-Daten-Gadgets in Finesse verwenden.

Um das Socket IO-Zertifikat im Browser zu installieren, navigieren Sie auf dem Client-PC zu **https://<UCCX FQDN>:12015/**, und installieren Sie das Zertifikat über die Browser-Eingabeaufforderungen.

Zugriff auf Drittanbieteranwendungen über Skripts

Wenn ein UCCX-Skript für den Zugriff auf einen sicheren Speicherort auf einem Drittanbieterserver konzipiert ist (z. B. "*URL-Dokument abrufen"* zu einer HTTPS-URL oder "*Make Rest Call"* zu einer HTTPS-REST-URL), laden Sie die signierte oder selbstsignierte Zertifikatkette des Drittanbieterdiensts in den UCCX-Schlüsselspeicher *für* die *Vertrauensstellung hoch.* Um dieses Zertifikat zu erhalten, rufen Sie die Seite UCCX **OS Administration (UCCX-BS-Administration**) auf, und wählen Sie **Upload Certificate (Zertifikat hochladen)**.

Die UCCX-Engine ist so konfiguriert, dass die Plattform Tomcat Keystore nach Zertifikatsketten von Drittanbietern durchsucht wird, wenn diese Zertifikate von Drittanbieteranwendungen bereitgestellt werden, wenn diese über Skriptschritte auf sichere Standorte zugreifen.

Die gesamte Zertifikatskette muss in den Tomcat-Schlüsselspeicher der Plattform hochgeladen werden, auf den über die Seite **OS Administration** zugegriffen werden kann, da der Tomcat-Schlüsselspeicher standardmäßig keine Stammzertifikate enthält.

Starten Sie nach Abschluss dieser Aktionen die Cisco UCCX Engine neu.

Überprüfung

Um sicherzustellen, dass alle Zertifikate korrekt installiert sind, können Sie die in diesem Abschnitt beschriebenen Funktionen testen. Wenn keine Zertifikatfehler auftreten und alle Funktionen ordnungsgemäß funktionieren, werden die Zertifikate richtig installiert.

- Konfigurieren Sie Finesse so, dass ein Agent automatisch über den Workflow aufgezeichnet wird. Nachdem ein Anruf vom Agenten bearbeitet wurde, suchen Sie ihn mit der Anwendung MediaSense Search and Play. Stellen Sie sicher, dass der Anruf mit den Aufzeichnungs-Metadaten in MediaSense einen Agenten, eine CSQ und Team-Tags verbunden hat.
- Konfigurieren von Agent Web Chat über SocialMiner Senden Sie einen Chat-Kontakt über das Webformular. Vergewissern Sie sich, dass der Mitarbeiter das Banner zur Annahme des Chat-Kontakts erhält, und dass das Chat-Formular ordnungsgemäß geladen wird, sodass der Mitarbeiter Chat-Nachrichten empfangen und senden kann.
- Versuchen Sie, einen Agenten über Finesse anzumelden. Stellen Sie sicher, dass keine Zertifikatwarnungen angezeigt werden und dass die Webseite nicht zur Installation von Zertifikaten im Browser auffordert. Vergewissern Sie sich, dass der Agent den Status ordnungsgemäß ändern kann, und dass dem Agenten ein neuer Anruf bei UCCX korrekt angezeigt wird.
- Melden Sie sich nach der Konfiguration der Live-Daten-Gadgets im Finesse-Desktop-Layout des Agenten und Supervisors bei einem Agenten, einem Supervisor und einem Benutzer an, der Berichte erstellt. Stellen Sie sicher, dass die Live-Daten-Gadgets ordnungsgemäß geladen werden, dass die ursprünglichen Daten in das Gadget eingefügt werden und dass die Daten aktualisiert werden, wenn sich die zugrunde liegenden Daten ändern.
- Versuchen Sie, eine Verbindung von einem Browser zur AppAdmin-URL auf beiden UCCX-Knoten herzustellen. Vergewissern Sie sich, dass keine Zertifikatwarnungen angezeigt werden, wenn Sie auf der Anmeldeseite dazu aufgefordert werden.

Fehlerbehebung

Problem: Ungültige Benutzer-ID/ungültiges Kennwort

UCCX Finesse Agents können sich nicht mit der Fehlermeldung **"Ungültige Benutzer-ID/Kennwort"** anmelden.

Ursachen

Unified CCX löst eine Ausnahme "SSLHandshakeException" aus und kann keine Verbindung mit Unified CM herstellen.

Lösung

- Vergewissern Sie sich, dass das Unified CM Tomcat-Zertifikat nicht abgelaufen ist.
- Stellen Sie sicher, dass für jedes in Unified CM hochgeladene Zertifikat eine der folgenden Erweiterungen als kritisch markiert ist:
  X509v3-Schlüsselverwendung (OID - 2.5.29.15)
  X509v3 Basic Constraints (OID - 2.5.29.19)
  Wenn Sie andere Erweiterungen als kritisch markieren, schlägt die Kommunikation zwischen Unified CCX und Unified CM aufgrund des Fehlers der Unified CM-Zertifikatverifizierung fehl.

Problem - CSR-SAN und Zertifikat-SAN stimmen nicht überein

Beim Hochladen eines CA-signierten Zertifikats wird der Fehler "CSR SAN and Certificate SAN does not match" angezeigt.

Ursachen

Die Zertifizierungsstelle hat möglicherweise eine weitere übergeordnete Domäne in das Feld Subjekt Alternative Namen (SAN) des Zertifikats eingefügt. Standardmäßig verfügt der CSR über folgende SANs:

```
SubjectAltName [
  example.com (dNSName)
  hostname.example.com (dNSName)
]
```

Die CAs können ein Zertifikat zurückgeben, dem ein anderes SAN hinzugefügt wurde: www.hostname.example.com Das Zertifikat enthält in diesem Fall ein zusätzliches SAN:

```
SubjectAltName [
  example.com (dNSName)
  hostname.example.com (dNSName)

  www.hostname.example.com (dNSName)
]
```

Dies verursacht den SAN-Diskrepanzfehler.

Lösung

Generieren Sie im Abschnitt "Subject Alternate Name (SANs)" der UCCX-Seite "Generate

Certificate Signing Request" den CSR mit einem leeren Feld für die übergeordnete Domäne. Auf diese Weise wird der CSR nicht mit einem SAN-Attribut generiert, die CA kann die SANs formatieren, und es besteht keine Abweichung zwischen den SAN-Attributen, wenn Sie das Zertifikat auf UCCX hochladen. Beachten Sie, dass das Feld Parent Domain (Übergeordnete Domäne) standardmäßig die Domäne des UCCX-Servers enthält. Der Wert muss daher explizit entfernt werden, während die Einstellungen für den CSR konfiguriert werden.

Problem - NET::ERR_CERT_COMMON_NAME_INVALID

Wenn Sie auf eine UCCX-, MediaSense- oder SocialMiner-Webseite zugreifen, wird eine Fehlermeldung angezeigt.

"Ihre Verbindung ist nicht privat.

Angreifer versuchen möglicherweise, Ihre Daten von <Server_FQDN> zu stehlen (z. B. Kennwörter, Nachrichten oder Kreditkarten). NETZ::ERR_CERT_COMMON_NAME_INVALID

Dieser Server konnte nicht nachweisen, dass er <Server_FQDN> ist. sein Sicherheitszertifikat stammt von [missing_subjectAltName]. Dies kann durch eine falsche Konfiguration oder durch einen Angreifer verursacht werden, der Ihre Verbindung abfängt."

Ursachen

Chrome Version 58 führte eine neue Sicherheitsfunktion ein, bei der es berichtet, dass das Zertifikat einer Website nicht sicher ist, wenn sein gemeinsamer Name (CN) nicht auch als SAN enthalten ist.

Lösung

- Sie können zu **Erweitert > Weiter zu <Server_FQDN> (unsicher)** navigieren, um mit dem Standort fortzufahren und den Zertifikatfehler zu akzeptieren.
- Sie können den Fehler mit CA-signierten Zertifikaten ganz vermeiden. Wenn Sie einen CSR generieren, wird der FQDN des Servers als SAN eingeschlossen. Die Zertifizierungsstelle kann den CSR signieren. Nachdem Sie das signierte Zertifikat auf den Server hochgeladen haben, enthält das Zertifikat des Servers den FQDN im SAN-Feld, sodass der Fehler nicht angezeigt wird.

Weitere Informationen

Siehe den Abschnitt "Entfernen Unterstützung für commonName Matching in Zertifikaten" in Deprecations and Removals in Chrome 58.

Zertifikatfehler

- Cisco Bug-ID CSCvb46250 - UCCX: Tomcat ECDSA-Zertifikat Auswirkung auf Finesse Live Data
- Cisco Bug-ID CSCvb58580 - Anmeldung bei SocialMiner mit Tomcat und Tomcat-ECDSA von RSA CA nicht möglich

- Cisco Bug-ID CSCvd56174 - UCCX: Fehler bei der Anmeldung beim Finesse-Agent aufgrund einer SSLHandshakeException
- Cisco Bug-ID CSCuv89545 - Finesse Logjam-Schwachstelle

Zugehörige Informationen

- ECDSA-Zertifikate in einer UCCX-Lösung verstehen
- SHA 256-Unterstützung für UCCX
- Konfigurationsbeispiel für signierte und selbstsignierte UCCX-Zertifikate
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.