ECDSA-certificaten in een UCCX-oplossing begrijpen

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco Unified Contact Center Express (UCCX) oplossing kunt configureren voor het gebruik van Ellips Digital Curve Digital Signature Algorithm (ECDSA)-certificaten.

Voorwaarden

Vereisten

Zorg er voordat u doorgaat met de configuratiestappen die in dit document zijn beschreven, voor dat u toegang hebt tot de pagina Besturingssysteem (OS) voor deze toepassingen:

- UCCX
- SocialMiner
- Cisco Unified Communications Manager (CUCM)
- UCCX-certificaatconfiguratie voor oplossing - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html

Een beheerder moet ook toegang hebben tot de certificaatwinkel op de agent en de supervisor PC's.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Als onderdeel van de Common Criteria (CC)-certificering heeft Cisco Unified Communications Manager ECDSA-certificaten toegevoegd in versie 11.0. Dit beïnvloedt alle VOS-producten (Voice Operating System) zoals UCCX, SocialMiner, MediaSense, enzovoort uit versie 11.5.

Meer informatie over het **Elliptic Curve Digital Signature Algorithm** kunt u hier vinden: https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767

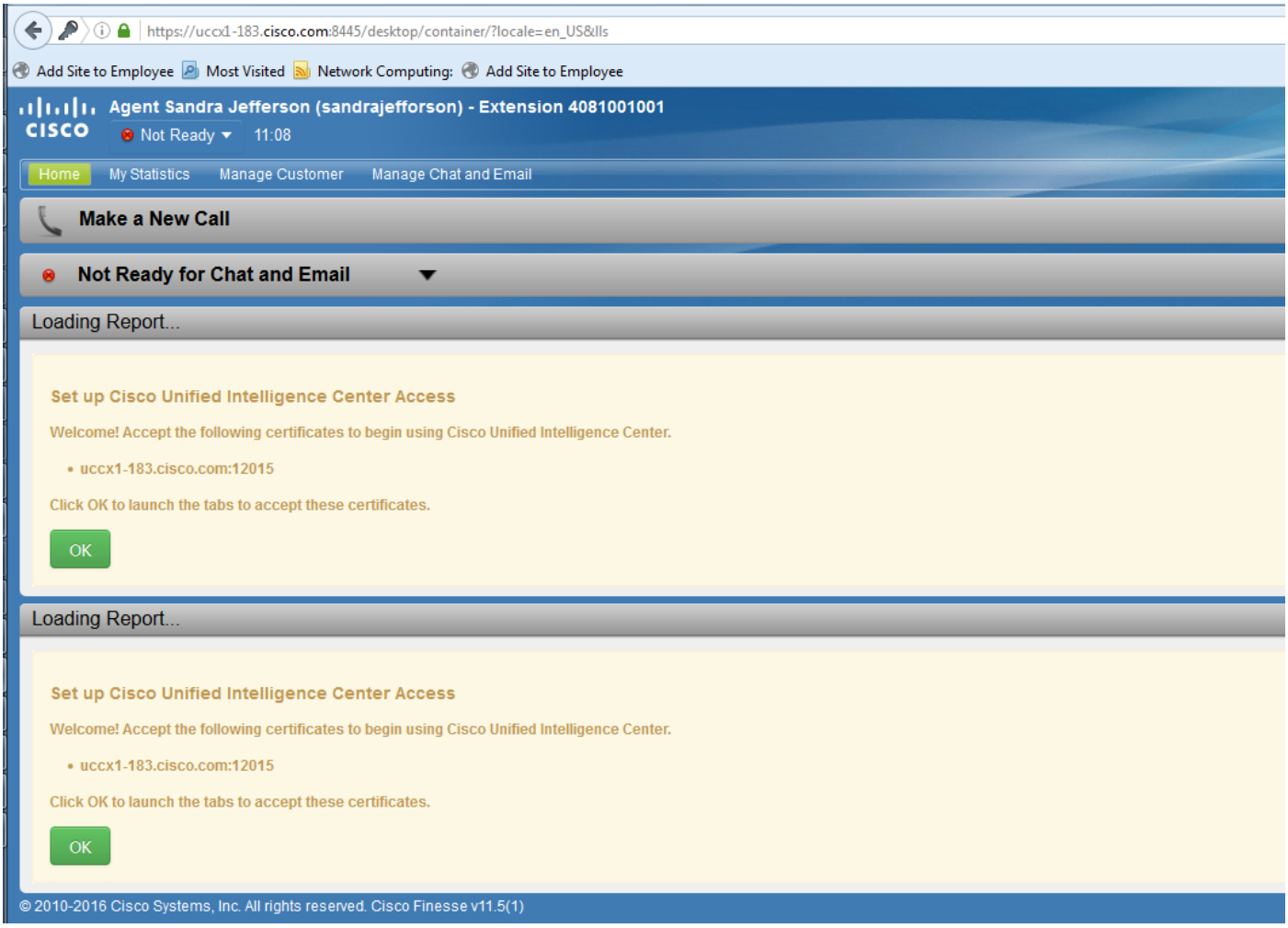
Met betrekking tot de UCCX-oplossing wordt u, wanneer u deze opwaardeert tot 11.5, een aanvullend certificaat aangeboden dat niet eerder aanwezig was. Dit is het Tomcat-ECDSA certificaat.

Dit is ook vastgelegd in de mededeling vóór de release: https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200651-UCCX-Version-11-5-Prerelease-Field-Commu.html?cachemode=refresh

Agent-ervaring

Na een upgrade naar 11.5 kan de agent worden gevraagd certificaten op het bureaublad te accepteren op basis van de vraag of het certificaat zelf is ondertekend of door de certificeringsinstantie (CA) is ondertekend.

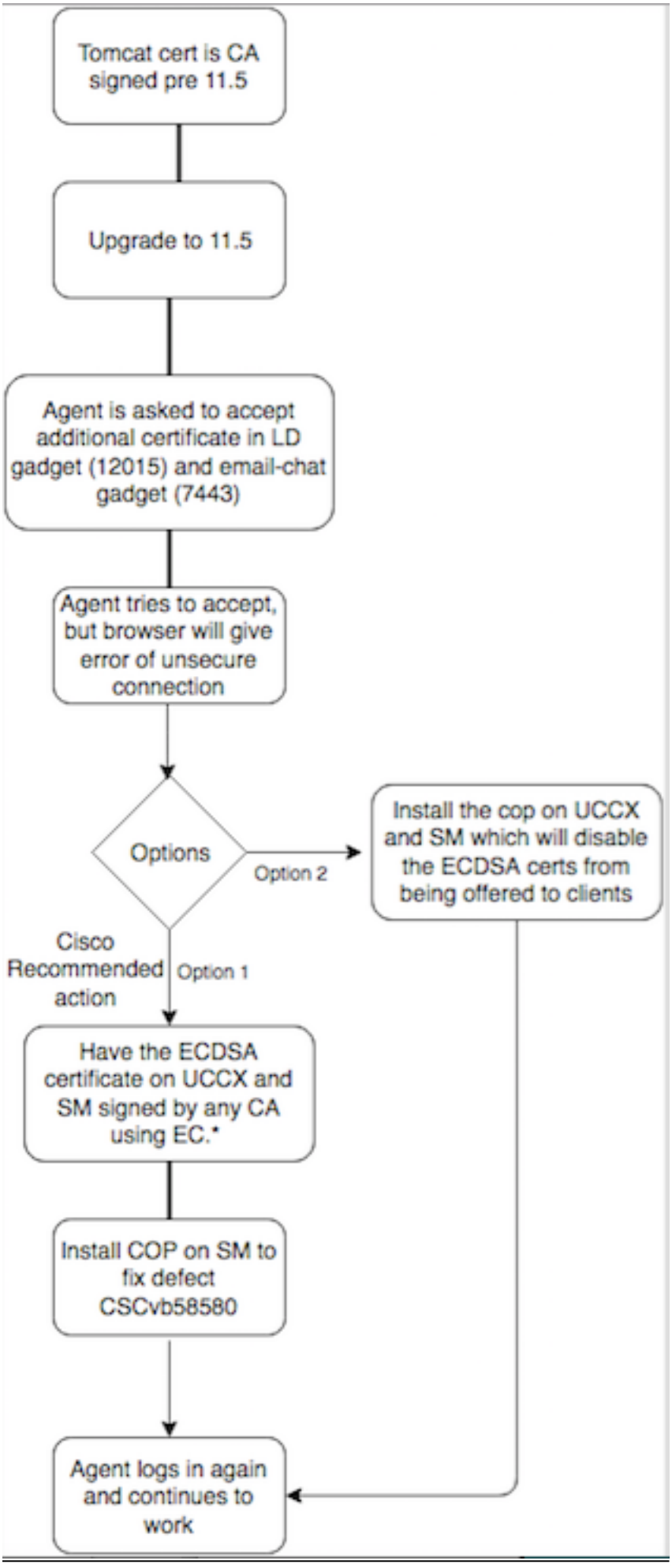
Gebruikerservaring na upgrade naar 11.5



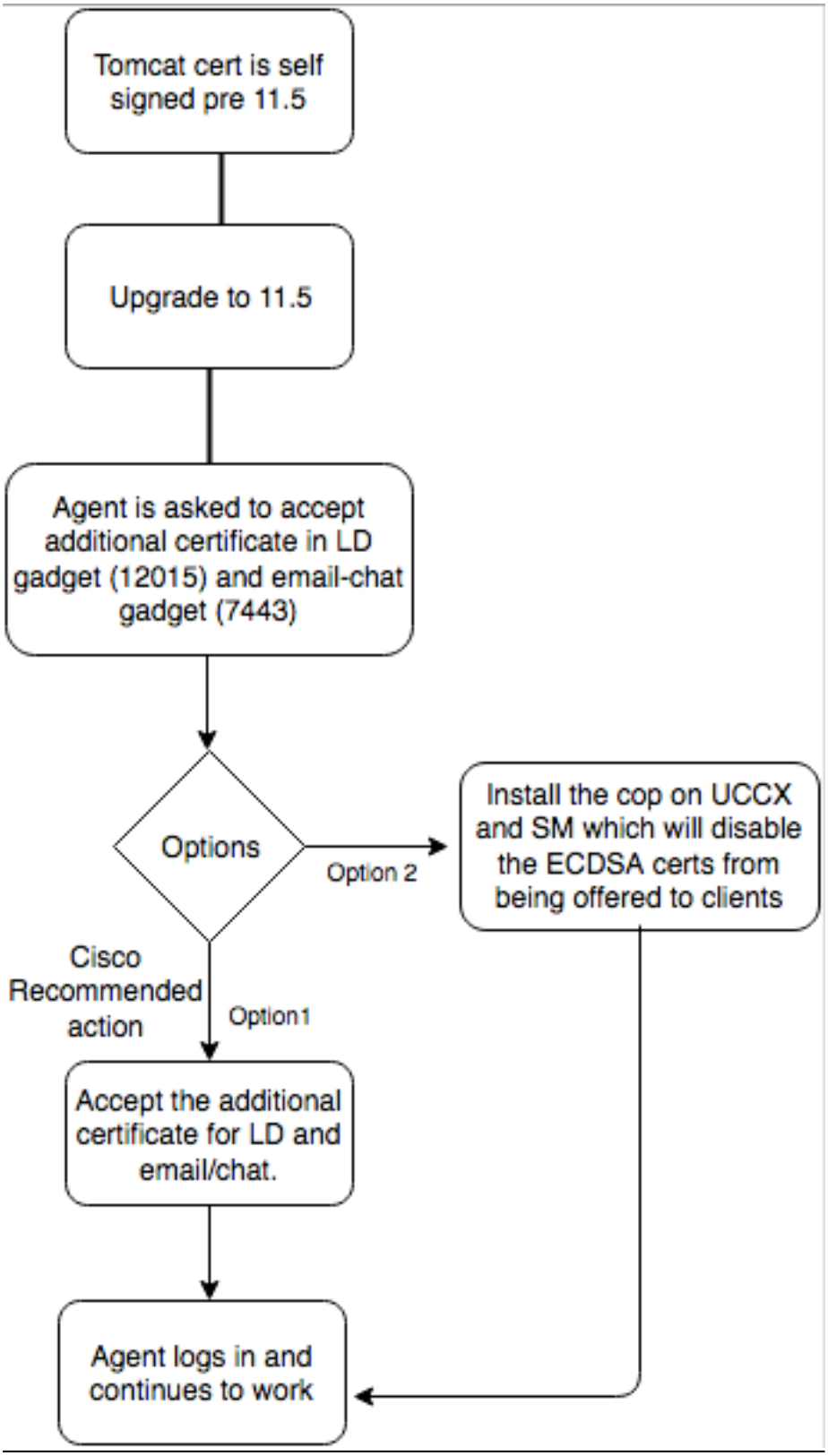
Dit komt doordat het Finesse bureaublad nu een ECDSA-certificaat wordt aangeboden dat niet eerder werd aangeboden.

Procedure

CA-ondertekende certificaten vóór upgrade


Tomcat cert is CA signed pre 11.5
Upgrade to 11.5
Agent is asked to accept additional certificate in LD gadget (12015) and email-chat gadget (7443)
Agent tries to accept, but browser will give error of unsecure connection
Options
Option 2
Install the cop on UCCX and SM which will disable the ECDSA certs from being offered to clients
Cisco Recommended action
Option 1
Have the ECDSA certificate on UCCX and SM signed by any CA using EC.*
Install COP on SM to fix defect CSCvb58580
Agent logs in again and continues to work

Aanvankelijk ondertekende certificaten



Configureren

De aanbevolen beste praktijk voor dit certificaat

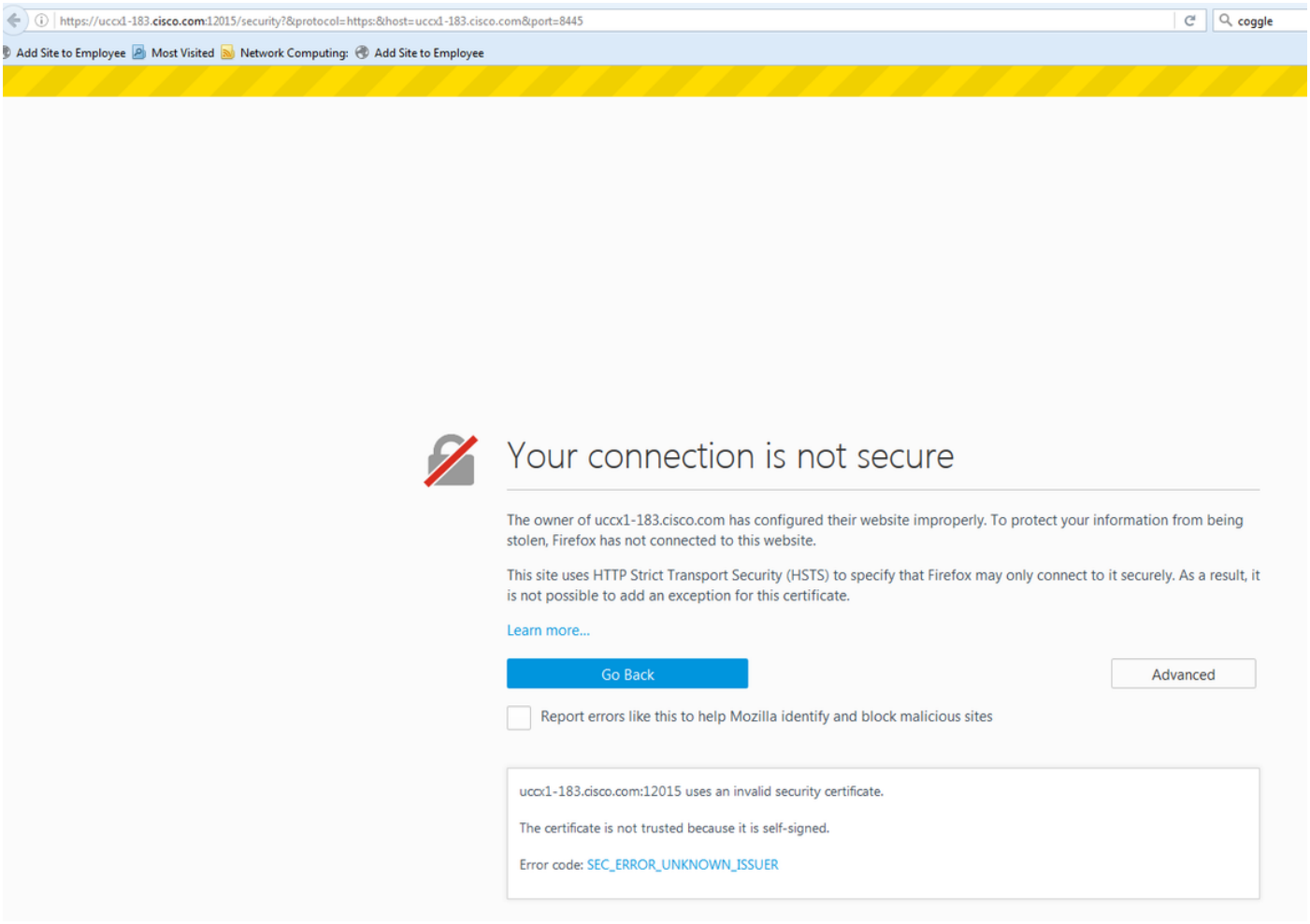
Ondertekende certificaten voor UCCX en SocialMiner

Als u CA-ondertekende certificaten gebruikt, moet dit ECDSA-certificaat worden ondertekend door een certificaatinstantie (CA) en andere certificaten

> Opmerking: Als CA dit ECDSA-certificaat bij RSA tekent, zou dit certificaat niet aan de cliënt worden overgelegd. Voor meer veiligheid zijn de aan de cliënt aangeboden ECDSA-certificaten de aanbevolen beste praktijk.

> **Opmerking**: als het ECDSA-certificaat op SocialMiner is ondertekend door een CA met RSA, veroorzaakt het problemen met e-mail en chatten. Dit is gedocumenteerd in een defect CSCvb58580 en er is een politiebestand beschikbaar. Deze COP garandeert dat ECDSA-certificaten niet aan klanten worden aangeboden. Als u een CA hebt die ECDSA-certificaten met uitsluitend RSA kan ondertekenen, gebruik dit certificaat dan niet.Gebruik de agent zodat het ECDSA-certificaat niet wordt aangeboden en u hebt een RSA-omgeving.

Als u CA-ondertekende certificaten gebruikt en na een upgrade hebt u het ECDSA-certificaat niet ondertekend en geüpload, ervaren agents een bericht om het extra certificaat te aanvaarden. Als ze op **OK** klikken**,** worden ze naar de website verwezen. Dit mislukt echter vanwege de beveiligingsmaatregelen van de kant van de browser, aangezien het ECDSA-certificaat zelf is ondertekend en uw andere webcertificaten door CA zijn ondertekend. Deze mededeling wordt gezien als een veiligheidsrisico.



Voltooi deze stappen op elk knooppunt van UCCX Publisher en Subscriber en SocialMiner, na een upgrade naar UCCX en SocialMiner op versie 11.5:

1. Navigeer naar de pagina **OS-beheer** en kies **Beveiliging > certificaatbeheer**.

2. Klik op **Generate CSR**.

3. Selecteer in de vervolgkeuzelijst **certificaatlijst de optie ECDSA** als de certificaatnaam en klik op **Generate CSR**.

4. Navigeer in **Security > certificaatbeheer** en kies **CSR** downloaden.

5. Kies in het pop-upvenster de optie **ECDSA** in de vervolgkeuzelijst en klik op **CSR downloaden**.

Stuur de nieuwe CSR naar de derde CA of teken het met een interne CA die EG-certificaten tekent. Dit zou deze ondertekende certificaten opleveren:

- Root Certificate voor de CA (Als u dezelfde CA gebruikt voor Application Certificaten en EC-certificaten, kunt u deze stap overslaan)
- ECDSA-ondertekend certificaat voor UCCX uitgever
- UCCX Subscriber ECDSA-ondertekend certificaat
- Certificaat voor lagere ECDSA-tekens

Opmerking: Als u de root- en tussentijdse certificaten op een uitgever (UCCX) uploadt, wordt deze automatisch naar de abonnee gerepliceerd. Het is niet nodig om de wortel- of tussencertificaten op de andere, niet-uitgeverij servers in de configuratie te uploaden als alle toepassingscertificaten worden ondertekend via dezelfde certificatenketen. U kunt ook dit uploaden van basiscertificaat overslaan als dezelfde CA het EC-certificaat heeft getekend en u dit al hebt gedaan toen u de UCCX-toepassingscertificaten hebt ingesteld.

Voltooi deze stappen op elke toepassingsserver om het basiscertificaat en het EG-certificaat te uploaden naar de knooppunten:

1. Navigeer naar de pagina **OS-beheer** en kies **Beveiliging > certificaatbeheer**.

2. Klik op **Uploadcertificaat**.

3. Upload het basiscertificaat en kies **om te vertrouwen** als het certificaattype.

4. Klik op **Upload File**.

5. Klik op **Uploadcertificaat**.

6. Upload het toepassingscertificaat en kies **om ECDSA** als het certificaattype te kiezen.

7. Klik op **Upload File**.

Opmerking: Als een ondergeschikte CA het certificaat tekent, uploadt u het basiscertificaat van de ondergeschikte CA als het certificaat *om te vertrouwen* in plaats van het basiscertificaat. Als een tussentijds certificaat wordt afgegeven, kunt u dit certificaat naast het aanvraagcertificaat uploaden naar de *tomcat-trust* winkel. Ook kunt u dit uploaden van het basiscertificaat overslaan als dezelfde CA het EC-certificaat heeft getekend en u hebt dit al gedaan toen u UCCX-toepassingscertificaten hebt ingesteld.

8. Start deze toepassingen na voltooiing:

    Cisco SocialMinerCisco UCCX uitgever en abonnement

Zelfondertekende certificaten voor UCCX en SocialMiner

Als UCCX of SocialMiner zelfondertekende certificaten gebruiken, moeten de agenten worden geadviseerd de certificaatwaarschuwing te aanvaarden die zij in het Gadget chat-e-mail en de Gadgets voor Live Data worden aangeboden.

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

Installeer voor Internet Explorer de zelf-getekende certificaten aan de kant van de client in de winkel **Trusted Root-certificeringsinstanties**.

Voltooi de volgende stappen voor Mozilla Firefox:

1. Blader naar **Gereedschappen > Opties**.

2. Klik op het tabblad **Geavanceerd**.

3. Klik op **Certificaten bekijken**.

4. Navigeer naar het tabblad **servers**.

5. Klik op **Uitzondering toevoegen**.

1. Opmerking: U kunt ook de security uitzondering toevoegen om het certificaat te installeren, dat gelijkwaardig is aan het bovenstaande proces. Dit is een eenmalige configuratie op de klant.

Vaak gestelde vragen (FAQ)

We hebben een door de CA ondertekend certificaat en willen het ECDSA-certificaat gebruiken dat door een EG-CA moet worden ondertekend. Terwijl we wachten tot het door CA ondertekende certificaat beschikbaar is, moeten we Live Data omhoog hebben. Wat kan ik doen?

We willen dit aanvullende certificaat niet tekenen of we willen dat de agents dit aanvullende certificaat aanvaarden. Wat kan ik doen?

Hoewel de aanbeveling is om ECDSA-certificaten aan de browsers te laten voorleggen, is er een optie om deze uit te schakelen. U kunt een politiebestand op UCCX en SocialMiner installeren dat garandeert dat alleen de RSA-certificaten aan de klant worden aangeboden. Het ECDSA-certificaat blijft in de hoofdwinkel, maar wordt niet aan de klanten aangeboden.

Als ik deze agent gebruik om ECDSA-certificaten uit te schakelen die aan de klanten worden aangeboden, kan ik het dan weer toestaan?

Ja, er is een terugdraaiende agent. Als dit certificaat is toegepast, kunt u het laten ondertekenen en uploaden naar de server(s).

Zouden alle certificaten aan ECDSA worden afgegeven?

Momenteel niet, maar verdere veiligheidsupdates op het VOS-platform in de toekomst.

Wanneer installeert u de UCCX COP?

- Wanneer u zelfondertekende certificaten gebruikt en geen extra certificaten wilt accepteren
- Wanneer u geen extra certificaat kunt verkrijgen dat door CA is ondertekend

Wanneer installeert u de SM COP?

- Wanneer u zelfondertekende certificaten gebruikt en geen extra certificaten wilt accepteren
- Wanneer u geen extra certificaat kunt verkrijgen dat door CA is ondertekend
- Wanneer u een CA hebt die ECDSA certificaten met slechts RSA kan ondertekenen

Wat zijn de certificaten die standaard door verschillende webserverinstanties worden aangeboden?

certificaatcombinatie/webserver	Standaard Agent-ervaring na upgrade naar 11.5 (zonder agent)	UCCX Tomcat	UCCX OpenFire (Cisco Unified CCX-melding)	UCCX SocketIO	Socia Tom
Zelfgetekende Tomcat-ECDSA	Middelen zouden worden gevraagd certificaten in Live Data gadget en chat e-mail gadget te aanvaarden	zelfgetekend	zelfgetekend	zelfgetekend	zelfge
RSA, ondertekend Tomcat, RSA, ondertekend Tomcat-ECDSA	Agent kan Finesse en Live Data gebruiken, maar e-mailchat wordt niet geladen en de website SocialMiner laadt niet.*	RSA	RSA	RSA	RSA
RSA heeft Tomcat ondertekend, EG CA ondertekend, Tomcat-ECDSA	Middelen kunnen Finesse gebruiken met zowel Live Data als chat-e-mail*	RSA	RSA	ECDSA	RSA
RSA, ondertekend Tomcat, zelf	De	RSA	RSA	Zelfgetekend (agents	RSA

ondertekend Tomcat-ECDSA	medewerkers zouden worden gevraagd om extra certificaten in het gadget Live Data en e-mailchat te accepteren. Accepteer het certificaat van Live Data gadget niet, accepteer het certificaat van e-mailchat gadget.*	kunnen niet accepteren vanwege browser opgelegde veiligheidsmaatregel. Raadpleeg de screenshot hierboven. U moet het door een EG CA ondertekende certificaat verkrijgen of de agent op UCCX installeren om de aan de klanten aangeboden ECDSA-certificaten uit te schakelen.)

Gerelateerde informatie

- UCCX ECDSA COP - https://software.cisco.com/download/release.html?mdfid=286309734&softwareid=280840578&release=11.5(1)&flowid=80822
- SocialMiner ECDSA COP - https://software.cisco.com/download/release.html?mdfid=283613136&flowid=73189&release=11.5(1)&softwareid=283812550&sortparam=
- UCCX-certificaatinformatie - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html