

TechHinweis zur Handhabung der TLS-Unterstützung mit UCCX

Inhalt

[Einführung](#)

[UCCX fungiert als Server](#)

[UCCX fungiert als Client](#)

[TLS 1.0-Unterstützung wird veraltet](#)

[Nächste Schritte](#)

[TLS-Unterstützungsmatrix](#)

[Aktueller Support](#)

[Nächste Versionen](#)

[SocialMiner- und TLS-Unterstützung](#)

[11,5\(1\)SU1](#)

[11,6](#)

[Häufig gestellte Fragen](#)

[Wie erhalte ich den für die Lösung erforderlichen TLS-Support?](#)

[Wenn Salesforce den Support für TLS 1.0 entfernt und ich eine Version habe, die nur TLS 1.0 für Client-Anfragen unterstützt, schlägt die Anforderung an das Salesforce-System fehl?](#)

[Die Verfügbarkeit von TLS 1.0-Unterstützung stellt ein Sicherheitsrisiko dar. Kann ich TLS 1.0 vollständig aus meiner UCCX-Lösung entfernen?](#)

[Kann jede Verbindung zu/von UCCX auf die oben genannten TLS-Änderungen angewendet werden?](#)

[Anfordern von Dokumentation und Einreichen eines Serviceantrags](#)

Einführung

In diesem Dokument wird beschrieben, wie Cisco Unified Contact Center Express (UCCX) Transport Layer Security (TLS) für verschiedene Integrationstypen mit Anwendungen von Drittanbietern verwendet. Bei diesen Integrationen kann UCCX als Client oder als Server fungieren.

Unterstützt von Abhiram Kramadhati, Cisco Engineering.

UCCX fungiert als Server

Wenn UCCX als Server fungiert und der Remote-Teilnehmer über TLS 1.0, 1.1 oder 1.2 kommuniziert, ist UCCX in der Lage, auf der Grundlage der mit der Unified CCX-Version kompatiblen TLS-Versionen zu kommunizieren:

1. Unified CCX 10.6 - TLS 1.0, 1.1 und 1.2
2. Unified CCX 11.x - TLS 1.0, 1.1 und 1.2

Dies sind Integrationen, bei denen die API-Services des Unified CCX-Systems von einer

Drittanbieteranwendung genutzt werden.

UCCX fungiert als Client

Wenn das UCCX als Client fungiert, wird ein Drittanbieter-Server aufgefordert, einen Service aufzurufen oder Informationen abzurufen. Ein gängiges Beispiel hierfür ist die Integration in ein Salesforce-System für die CRM-Integration. Die Anfragen können von folgenden Quellen stammen:

1. Skript für Unified CCX
2. Finesse-Workflows
3. Finesse-Gadgets

In UCCX-Versionen 10.x, 11.0(1) und 11.5(1) verwendet Unified CCX, wenn diese Anforderung aufgerufen wird, standardmäßig TLS 1.0. Der Drittanbieter-Server sollte in der Lage sein, über TLS 1.0 zu kommunizieren. Andernfalls schlägt die Kommunikation fehl.

TLS 1.0-Unterstützung wird veraltet

Die Unterstützung für TLS 1.0 wird von vielen Anwendungsanbietern veraltet. Die Kommunikation über TLS 1.0 (und sogar die Verfügbarkeit von TLS 1.0) wird von vielen Unternehmen als Schwachstelle angesehen.

Die jüngste Ankündigung hierzu stammt von Salesforce:

<https://help.salesforce.com/articleView?id=000221207&type=1>. Dies ist für UCCX-Kunden relevant, die UCCX in Salesforce integriert haben. Am 17. Februar 2017 hat Salesforce angekündigt, die Unterstützung für TLS 1.0 zu entfernen:

Neue Bereitstellungen: TLS 1.0 ist standardmäßig deaktiviert.

Sandbox-Umgebungen/Entwicklersysteme: TLS 1.0 ist seit dem 25. Juni 2016 um 9:30 Uhr PDT (16:30 UTC) deaktiviert

Produktionssysteme: TLS 1.0 ist seit dem 22. Juli 2017 deaktiviert.

Dies bedeutet, dass UCCX-Lösungen, die Webanfragen an Salesforce-Systeme mit TLS 1.0 aufrufen, diese Daten nicht veröffentlichen können.

Hinweis: Dieselbe Logik gilt für jede solche Integration. Salesforce ist einer dieser Anbieter, der eine entsprechende Ankündigung gemacht hat.

Nächste Schritte

Wenn Integrationen vorhanden sind, die TLS verwenden, stellt die nachfolgende Tabelle die Versionen von Unified CCX dar, die TLS 1.1 und 1.2-Unterstützung für Unified CCX-Integrationen bieten, wenn Unified CCX der Client ist (Salesforce-Integration), sowie die vollständige Entfernung von TLS 1.0 aus Unified CCX.

Kunden sollten ein Upgrade auf die unten genannten Versionen planen, die die für ihre Umgebung erforderliche TLS-Unterstützung bieten. Für dasselbe Angebot sind keine technischen Sonderaktionen verfügbar.

Aktuelle Kundenversion	Zielversion für TLS 1.1, 1.2 Unterstützung bei UCCX als Client	Zielversion für TLS 1.0-Entfernung aus UCCX
10,0	10,6(1)SU3	11,5(1)SU1
10,5	10,6(1)SU3	11,5(1)SU1
10,6	10,6(1)SU3	11,5(1)SU1
11,0	11,5(1)SU1	11,5(1)SU1
11,5	11,5(1)SU1	11,5(1)SU1

Die ETA für die oben genannten Releases ist noch nicht bestätigt, jedoch noch vor dem Salesforce-Termin. Sie werden auf der Seite zum Herunterladen der Software von cisco.com veröffentlicht.

TLS-Unterstützungsmatrix

Aktueller Support

UCCX-Lösungsversion	TLS-Versionen, wenn UCCX als Server fungiert	TLS-Versionen, bei denen UCCX als fungiert
10,6(1)SU2	1,0, 1,1, 1,2	1,0
11,0(1)	1,0, 1,1, 1,2	1,0
11.0(1)SU1	1,0, 1,1, 1,2	1,0
11,5(1)	1,0, 1,1, 1,2	1,0

Nächste Versionen

UCCX-Lösungsversion	TLS-Versionen, wenn UCCX als Server fungiert	TLS-Versionen, bei denen UCCX als fungiert
10,6(1)SU3	1,0, 1,1, 1,2	1,1, 1,2*
11,5(1)SU1	1,1, 1,2 [#]	1,1, 1,2*
11,6(1)	1,2	1,2

* Standard

[#] siehe Hinweis zu SocialMiner hier

SocialMiner- und TLS-Unterstützung

SocialMiner hat abgesehen von der oben genannten Support-Matrix die folgenden Änderungen:

11,5(1)SU1

11.5(1)SU1 unterstützt weiterhin Exchange 2010. Da Exchange 2010 NUR TLS 1.0 unterstützt, entfernt SocialMiner TLS 1.0 nicht. Um jedoch sicherzustellen, dass die Sicherheit nicht beeinträchtigt wird, unterstützen alle eingehenden Verbindungen TLS 1.0 nicht, und nur die

ausgehende Verbindung verfügt über TLS 1.0, wenn der Drittanbieter-Server nur über TLS 1.0 kommunizieren kann. Andernfalls funktionieren die Verbindungen auf TLS 1.1 und 1.2.

11,6

Bei SocialMiner 11.6 wurde TLS 1.0 entfernt. Wenn der Kunde Exchange 2013 verwendet, verwendet Exchange 2013 standardmäßig TLS 1.0 und alle E-Mail-Kampagnen fehlschlagen, da SocialMiner TLS 1.0 nicht unterstützt. Daher sollte der Kunde TLS 1.1/1.2 auf Exchange 2013 aktivieren, damit er weiterhin mit 11.6 arbeiten kann. Dies ist auch in den Versionshinweisen und der Vorabmitteilung für 11.6 dokumentiert.

Häufig gestellte Fragen

Wie erhalte ich den für die Lösung erforderlichen TLS-Support?

Sie sollten ein Upgrade auf die in der obigen Tabelle aufgeführten Versionen durchführen. Es gibt keine separate Engineering-Sonderaktion oder eine COP-Datei.

Wenn Salesforce den Support für TLS 1.0 entfernt und ich eine Version habe, die nur TLS 1.0 für Client-Anfragen unterstützt, schlägt die Anforderung an das Salesforce-System fehl?

Ja. Tatsächlich funktioniert ein Server, der TLS 1.0 nicht unterstützt, nicht mit UCCX, wenn UCCX nur Anfragen für TLS 1.0 sendet. Dies gilt für die Versionen 10.6(1)SU2, 11.0(1), 11.0(1)SU1 und 11.5(1).

Die Verfügbarkeit von TLS 1.0-Unterstützung stellt ein Sicherheitsrisiko dar. Kann ich TLS 1.0 vollständig aus meiner UCCX-Lösung entfernen?

Ja, bei UCCX 11.5(1)SU1 wird TLS 1.0 für externe HTTPS-Verbindungen vollständig entfernt.

Kann jede Verbindung zu/von UCCX auf die oben genannten TLS-Änderungen angewendet werden?

Diese Aktualisierungen gelten nur für HTTPS-Verbindungen. JDBC-Verbindungen können weiterhin auf TLS 1.0 betrieben werden.

Anfordern von Dokumentation und Einreichen eines Serviceantrags

Informationen zum Erhalten von Dokumentation, zum Verwenden des Cisco Bug Search Tool (BST), zum Einsenden einer Serviceanfrage und zum Sammeln zusätzlicher Informationen finden Sie unter What's New in Cisco Product Documentation (Neuerungen in der Cisco

Produktdokumentation) unter:

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Abonnieren Sie What's New in Cisco Product Documentation (Neuigkeiten in der Cisco Produktdokumentation), die alle neuen und überarbeiteten technischen Dokumentationen von Cisco als RSS-Feed auflistet und Inhalte direkt über eine Reader-Anwendung an Ihren Desktop übermittelt. Die RSS Feeds sind ein kostenloser Service.

DIE SPEZIFIKATIONEN UND INFORMATIONEN ZU DEN PRODUKTEN IN DIESEM HANDBUCH KÖNNEN OHNE VORHERIGE ANKÜNDIGUNG GEÄNDERT WERDEN. ALLE AUSSAGEN, INFORMATIONEN UND EMPFEHLUNGEN IN DIESEM HANDBUCH SIND GENAU ANGESEHEN, WERDEN JEDOCH OHNE JEDLICHE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GARANTIE VORGELEGT. DIE BENUTZER MÜSSEN DIE VOLLSTÄNDIGE VERANTWORTUNG FÜR DIE ANWENDUNG ALLER PRODUKTE ÜBERNEHMEN.

DIE SOFTWARELIZENZ UND DIE EINGESCHRÄNKTE GARANTIE FÜR DAS BEGLEITENDE PRODUKT SIND IM LIEFERUMFANG DES PRODUKTS ENTHALTENEN INFORMATIONSPAKET AUFGEFÜHRT UND HIERIN DURCH DIESE BEZUGNAHME ENTHALTEN. WENN SIE DIE SOFTWARELIZENZ ODER DIE EINGESCHRÄNKTE GARANTIE NICHT FINDEN KÖNNEN, WENDEN SIE SICH AN IHREN CISCO VERTRETER, UM EINE KOPIE ZU ERHALTEN.

Die Implementierung der TCP-Header-Komprimierung bei Cisco ist eine Anpassung eines Programms, das von der University of California, Berkeley (UCB) als Teil der Public Domain-Version von UCB des UNIX-Betriebssystems entwickelt wurde. Alle Rechte vorbehalten. Copyright © 1981, Verwaltungsrat der University of California.

UNGEACHTET JEDLICHER ANDERER HIERIN ENTHALTENEN GEWÄHRLEISTUNG WERDEN ALLE DOKUMENTDATEIEN UND SOFTWARE DIESER LIEFERANTEN "WIE BESEHEN" MIT ALLEN FEHLERN BEREITGESTELLT. CISCO UND DIE OBEN GENANNTEN LIEFERANTEN SCHLIESSEN ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN AUS, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT, DER HANDELSÜBLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG ODER AUFGRUND VON HANDEL TICE.

CISCO ODER SEINE ZULIEFERER SIND IN KEINEM FALL FÜR INDIREKTE, SONDERSCHÄDEN, FOLGESCHÄDEN ODER ZUFÄLLIGE SCHÄDEN HAFTBAR, EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, VERLUSTEN ODER SCHÄDEN AN DATEN, DIE AUS DER VERWENDUNG ODER UNMÖGLICHKEIT ZUR NUTZUNG DIESES HANDBUCHS VON CISCO ODER CISCO ODER SER DIE HÖHER WURDEN ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN BERATT.

IP-Adressen und Telefonnummern, die in diesem Dokument verwendet werden, sind nicht als tatsächliche Adressen und Telefonnummern vorgesehen. Beispiele, Befehlsausgabe, Netzwerktopologiediagramme und andere im Dokument enthaltene Abbildungen dienen lediglich der Veranschaulichung. Die Verwendung tatsächlicher IP-Adressen oder Telefonnummern in diesem Zusammenhang ist unabsichtlich und zufällig.

Alle gedruckten Kopien und Duplikate gelten als nicht kontrollierte Kopien, und die Online-Originalversion sollte für die neueste Version verwendet werden.

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und

Faxnummern finden Sie auf der Cisco Website unter www.cisco.com/go/offices.

Cisco und das Cisco Logo sind Marken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den USA und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter www.cisco.com/go/trademarks. Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs "Partner" impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1110 R)

©2016 Cisco Systems, Inc. Alle Rechte vorbehalten.