TechNote on Handling TLS Support with UCCX

Contents

Introduction

This document describes how Cisco Unified Contact Center Express (UCCX) uses Transport Layer Security (TLS) for different types of integration with the third party applications. These integrations can be where the UCCX functions as a client or where the UCCX functions as a server.

Contributed by Abhiram Kramadhati, Cisco Engineering.

UCCX Functions as a Server

When UCCX functions as a server, and the remote party communicates using TLS 1.0, 1.1 or 1.2, UCCX is capable of the communication based on the TLS versions compatible with the Unified CCX version:

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

These are integrations where the API services of the Unified CCX system is utilized by a third party application.

UCCX Functions as a Client

When the UCCX functions as a client, it requests a third party server to invoke a service or obtains information. A common example, in this case, is integration to a Salesforce system for CRM integration. The requests can be either from:

1. Unified CCX Script
2. Finesse Workflows
3. Finesse Gadgets

In UCCX versions 10.x, 11.0(1) and 11.5(1), when Unified CCX invokes this request it uses TLS 1.0 by default.The third party server should be able to communicate using TLS 1.0 or else the communication will fail.

TLS 1.0 Support is being Deprecated

The support for TLS 1.0 is deprecated by many application providers.The communication on TLS 1.0 (and even the availability of TLS 1.0) is considered as a vulnerability by many organizations.

The most recent announcement in this regard has been from Salesforce: https://help.salesforce.com/articleView?id=000221207&type=1. This is relevant to UCCX customers who have UCCX integrated with Salesforce. As on 17th February 2017, Salesforce has announced that they will be removing support for TLS 1.0:

New deployments: TLS 1.0 disabled by default

Sandbox environments/developer systems: TLS 1.0 disabled post June 25, 2016, at 9:30 AM PDT (16:30 UTC)

Production systems: TLS 1.0 disabled post July 22, 2017

This means that UCCX solutions that invoke web requests to Salesforce systems using TLS 1.0, fails to post these dates.

> **Note**: The same logic applies to any such integration. Salesforce is one such vendor who has made an announcement in this regard.

Next Steps

If there exist integrations that use TLS, the below table represents the versions of Unified CCX that provide TLS 1.1 and 1.2 support for Unified CCX integrations when Unified CCX is the client (Salesforce integration) and also the removal of TLS 1.0 from the Unified CCX completely.

Customers should plan to upgrade to the versions mentioned below that provide the TLS support that is necessary for their environment. There are no Engineering Specials available for the same.

Current customer release	Target release for TLS 1.1, 1.2 support when UCCX is client	Target release for TLS 1.0 rem from 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

The ETA for the above releases are not yet confirmed but it is before the Salesforce deadline. They are published on the cisco.com Software Download page.

TLS Support Matrix

Current Support

UCCX Solution version	TLS versions when UCCX functioning as server	TLS versions when UCCX functioni client
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

Upcoming Releases

UCCX Solution version	TLS versions when UCCX functioning as server	TLS versions when UCCX functioni client
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

***** default

see note about SocialMiner here

SocialMiner and TLS support

SocialMiner has these changes apart from the above-mentioned support matrix:

11.5(1)SU1

11.5(1)SU1 still supports Exchange 2010. Since Exchange 2010 supports ONLY TLS 1.0, SocialMiner will not remove TLS 1.0. However, to ensure that the security is not compromised all incoming connections will not support TLS 1.0 and only the outgoing connection will have TLS 1.0, if the 3rd party server can communicate on TLS 1.0 only. Otherwise, connections will work on TLS 1.1 and 1.2

11.6

SocialMiner 11.6 has TLS 1.0 removed. If the customer uses Exchange 2013, by default Exchange 2013 uses TLS 1.0 and all email campaigns fail since SocialMiner does not support

TLS 1.0. Hence, the customer should enable TLS 1.1/1,2 on Exchange 2013 so that it can continue to work with 11.6. This is documened in the release notes and the pre-release communication for 11.6 as well.

FAQ

How to get the TLS support needed for the solution?

You should upgrade to the versions as listed in the table above. There are not any separate Engineering Special or a cop file.

If Salesforce removes TLS 1.0 support and I am on a version that supports only TLS 1.0 for client requests, does request to Salesforce system fail?

Yes. In fact, any server that does not support TLS 1.0 will not work with UCCX if UCCX is sending requests on TLS 1.0 only and this is true for versions 10.6(1)SU2, 11.0(1), 11.0(1)SU1, 11.5(1).

TLS 1.0 support being available is a security risk. Can I remove TLS 1.0 completely from my UCCX solution?

Yes, UCCX 11.5(1)SU1 onwards has TLS 1.0 removed completely for external HTTPS connections.

Does every connection to/from UCCX be applicable to the above mentioned TLS changes?

These updates are for HTTPS connections only. JDBC connections can still operate on TLS 1.0.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)