

UCCX 11.6發佈前通訊

目錄

[簡介](#)

[背景資訊](#)

[為UCCX 11.6升級做準備](#)

[SocialMiner升級和Microsoft Exchange](#)

[適用於UCCX的TLS 1.2支援](#)

[對RTMT和指令碼編輯器的影響](#)

[支援ESXi 6.5](#)

[縮短升級時間](#)

[用於升級和全新安裝的單個ISO](#)

[案頭和瀏覽器更新](#)

[即時報告工具](#)

[瀏覽器的相容模式](#)

[單一登入\(SSO\)](#)

[支援新的身份提供程式](#)

[Finesse容錯移轉增強功能](#)

[重要注意事項](#)

[可維護性增強](#)

[情景服務控制面板和警報](#)

[升級前瞭解](#)

[報告使用者密碼一致性和對LiveData的影響](#)

[報告使用者升級到UCCX 11.6後無法訪問CUIC報告](#)

[電子郵件和Exchange注意事項附件大小限制增加](#)

[計算郵件限制大小](#)

[重要升級注意事項](#)

[獲取文檔並提交服務請求](#)

簡介

本文檔介紹UCCX 11.6預發行版通訊。

附註： Unified Contact Center Express(UCCX)11.6版本是一個非常重要的版本，它包含重要功能更新和可維護性更新，可幫助合作夥伴和客戶。此發佈前溝通概要介紹了關鍵更新和重要資訊，有助於規劃快速平穩地升級到UCCX 11.6。

背景資訊

UCCX 11.6具有許多旨在增強代理、管理人員和管理員的產品功能集和工作效率的功能。電子郵件、聊天功能已進行了重大更新，同時對Cisco Unified Intelligence Center(CUIC)報告和Finesse Desktop更新進行了更新，極大地改善了聯絡中心使用者的體驗。在對系統進行更新時，還新增了重要的可維護性更新（如情景服務控制面板），以提供諸如縮短升級時間之類的好處

新功能的摘要 (有關詳細清單，請參閱發行說明)：

Cisco Finesse

UCCX電子郵件

- 直接轉接
- 基於輔助線路的座席狀態
- 預設顯示原因代碼標籤
- 增強型Finesse故障轉移
- 最近的呼叫歷史記錄和座席狀態報告
- FIPPA的隊列統計資訊
- 能夠從READY狀態發出呼叫
- 能夠監控ACD線路上的出站呼叫
- 管理引擎歷史報表
- 作為座席標籤的系統生成原因代碼以及修改系統生成原因代碼標籤的能力

- 電郵抄送/密件抄送/轉發
- 全部回覆和回覆
- 電子郵件簽名
- GMAIL支援
- 總結原因
- 多通道代理摘要報告

指令碼增強功能

出站活動增強功能

- 進行REST呼叫的報頭和代理支援
- 獲取報告統計資訊步驟，以允許基於未就緒原因代碼對座席計數
- 新建「建立JSON文檔」步驟
- 新建JSON文檔資料步驟
- 作為模板新增的基於上下文服務的IVR指令碼
- TLS 1.2支援

- 能夠儲存匯入的聯絡人清單順序。
- 通過SFTP或HTTP伺服器自單

為UCCX 11.6升級做準備

UCCX 11.6支援從以下路徑直接升級：

10.x	11.0	11.5
10.5(1)SU1	11.0(1)	11.5(1)
10.6(1)	11.0(1)SU1	11.5(1)SU1
10.6(1)SU1		
10.6(1)SU2		

在上述版本上應用的任何工程特別計畫(ES)不會影響升級路徑，可以從上述任何版本執行升級，而不管系統上安裝了哪個ES。如果在本文檔發佈日期之後有軟體版本，請檢視UCCX軟體相容性表以驗證升級路徑的可用性。

SocialMiner升級和Microsoft Exchange

UCCX與SocialMiner互動，以獲得所有電子郵件和聊天功能。應該規劃11.6升級，以確保在同一維護視窗中將UCCX和SocialMiner伺服器都升級到11.6。在UCCX 11.6中，電子郵件和聊天功能經歷了重大更新。使用UCCX 11.6的這些功能 (SocialMiner仍在11.5上)，將會出現意外結果並顯示錯誤/警告。

建議的升級順序是在同一個維護視窗中升級SocialMiner伺服器和UCCX伺服器。

UCCX 11.6解決方案支援用於UCCX電子郵件功能的Microsoft Exchange Server 2013和2016 — 企業版和標準版。如果使用Microsoft Exchange Server 2013，請確保為Exchange Server 2013安裝累積更新15(KB3197044)，以便Exchange支援TLS 1.2。如果沒有此修補程式，SocialMiner和Microsoft Exchange Server 2013之間的通訊將失敗，電子郵件路由將失敗。如果您已經通過

UCCX安裝了Microsoft Exchange Server 2013 Server安裝程式，請確保在通過UCCX 11.6投入生產之前安裝此修補程式。

Microsoft Exchange Server 2016不需要此功能。

附註： 如果不想對Exchange的連線使用TLS 1.2，可在SocialMiner伺服器上將伺服器TLS的最低版本設定為1.0（請參閱下面TLS一節中的詳細資訊）。如果Exchange和SocialMiner之間存在TLS不匹配，則所有電子郵件源都將失敗。

適用於UCCX的TLS 1.2支援

在UCCX 11.6中，當UCCX充當連線中的客戶端或伺服器時，連線的預設值為TLS 1.2。升級到UCCX 11.6並具有與UCCX互動的第三方應用程式並使用TLS的客戶必須瞭解此更改。

UCCX 11.6還能夠更新客戶端和伺服器連線的最低TLS版本：

- set tls client min-version <1.1或1.0>
- set tls server min-version <1.1或1.0>

範例：set tls server min-version 1.2

如果這是一個高可用性系統，則必須在兩個節點上運行該命令。在運行命令後，必須使用**utils system restart**命令重新啟動系統。

可通過運行以下命令來驗證支援的最低TLS版本：

- show tls client min-version
- show tls server min-version

附註： 如果最低版本設定為1.0，則表示連線將支援1.0、1.1和1.2。

對RTMT和指令碼編輯器的影響

由於安全標準採用TLS 1.2，而且這是標準，因此重新安裝了所有UCCX外掛（如RTMT和指令碼編輯器），以便它們可以繼續使用UCCX 11.6。升級到UCCX後：

1. 下載並在所有以前使用RTMT的電腦上重新安裝RTMT。較舊版本的RTMT無法與UCCX建立連線。
2. 下載並在所有以前使用UCCX指令碼編輯器的電腦上重新安裝UCCX指令碼編輯器。

支援ESXi 6.5

要從UCCX 11.6開始，支援ESXi 6.5。由於VMFS 6的效能問題和VMWare正在進行的調查，只有VMFS 5支援ESXi 6.5。

ESXi 6.5支援	使用ESXi 6.5的VMFS版本	意見
BE6K 是	VMFS 5	對其他應用程式的依賴性阻止使用VMFS 6
非BE6k 是	VMFS 5和VMFS 6	升級ESXi和VMFS可能需要遷移虛擬機器

確保使用為11.6發佈的最新OVA模板。

附註：將來可以為以前的版本更新對VMFS 6的支援。請參閱UCCX虛擬化[Wiki](#)以獲取最新更新。

縮短升級時間

在UCCX 11.6中，已經進行了更新，以減少完成升級操作所需的總時間。作為交換機版本過程的一部分，許多指令碼會按順序運行，以遷移各個應用程式（如Finesse、CUIC和歷史資料）的資料。在UCCX 11.6中，該設計被更新為並行運行指令碼，從而顯著減少了交換機版本所需的時間。

由於客戶資料庫的大小，無法顯示交換機版本的實際時間，但內部測試顯示，交換機版本過程的時間減少了約30%。

用於升級和全新安裝的單個ISO

在UCCX 11.6中，只有1個ISO發佈在Cisco.com上，此ISO可用於升級或全新安裝。ISO遵循UCSInstall_UCCX_11.6.XXXXX-XX.sgn.iso的常規命名約定

此ISO提供兩個引導選項，因此也用作可引導映像。

案頭和瀏覽器更新

即時報告工具

Real Time Reporting Tool不再完全基於瀏覽器，而是使用要求在PC上下載才能訪問的Java Applet。由於大多數瀏覽器都引入了Java安全方面的安全更新，因此有必要將UCCX即時報告(RTR)工具作為在首次安裝時下載的Java Applet來引入。

11.6中更新的行為：

1. RTR現在還可以作為外掛下載，請導航到**工具>外掛**頁。它繼續存在於**Tools > RealTime Reporting**頁中。
2. 從給定的PC升級到UCCX 11.6後首次訪問RTR時，會從UCCX伺服器下載一個Java小程式。使用者必須有許可權允許下載並開啟該下載。

附註：升級後，需要在每台要訪問RTR的PC上完成此操作。下載RTR小程式後，任何有權訪問PC的使用者都可以開啟該小程式。

建議使用RTR的Java版本是**Java 8**。如果使用者具有Java 7，則使用者必須在Java控制面板中啟用TLS 1.2。

瀏覽器的相容模式

如果您使用的是Internet Explorer(IE),Finesse案頭不支援相容模式。如果已啟用相容模式，則進行更改以向代理顯示警告。唯一需要相容性模式的場景是訪問包含安全抽屜、計畫程式等功能的CUIC的舊UI。

單一登入(SSO)

UCCX現在支援整合的Windows身份驗證。有關詳細資訊，請參閱UCCX發行說明和相關文檔。

支援新的身份提供程式

在UCCX 11.6中，許多新的身份提供方(IDP)已獲得資格並新增以提供支援：

- Microsoft AD FS (Active Directory聯合身份驗證服務) : 2.0、2.1和3.0
- PingFederate:8.2.2.0
- OpenAM:10.0.1
- 希博萊斯 : 3.3.0
- F5:13.0

UCCX 11.6還可以與任何使用SAML v2.0的IDP配合使用。只要IDP確認符合SAML v2.0標準並能滿足UCCX(IdS)配置，即使該IDP不屬於上述清單的一部分，也可以用於UCCX SSO。

Finesse容錯移轉增強功能

從UCCX 11.6開始，故障切換行為得到了增強，以確保在Finesse故障切換期間代理的生產效率，而無需執行完整的系統故障切換。因此，要使座席能夠瞭解行為的變化，瞭解這一點非常重要。

行為變化概述。

案例	UCCX高可用性行為	Node1上的Finesse
Node1上的CCX引擎故障	SideB上的CCX引擎成為主引擎	Finesse停止服務，連線到新的主引擎後立即
Node2上的CCX引擎故障	A端的CCX引擎繼續主處理	Finesse仍為IN_SERVICE
Node1上的Finesse服務OOS	引擎主運行不受影響	OUT_OF_SERVICE
Node2上的Finesse服務OOS	引擎主運行不受影響	Node1上的Finesse將繼續為IN_SERVICE
Node1上的CCX通知服務失敗	引擎主運行不受影響	OUT_OF_SERVICE
節點2上的CCX通知服務失敗	引擎主運行不受影響	Node1上的Finesse繼續為IN_SERVICE
島模式	兩個HA節點均成為主節點	Node1上的Finesse繼續為IN_SERVICE，並

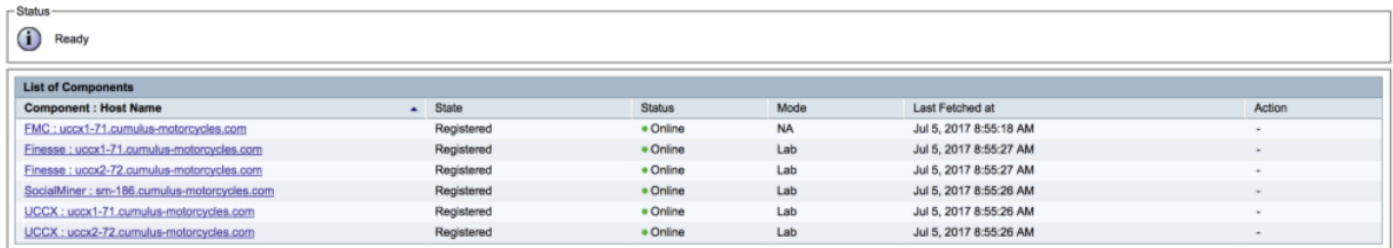
重要注意事項

1. UCCX不支援代理登入的負載均衡。所有代理只應登入到主節點。行為的增強功能僅適用於故障切換支援。
2. 不支援同時對兩個節點進行相同的代理登入。這可能導致座席體驗不一致。
3. 如果發生多個故障轉移，導致代理同時連線到兩個節點，則所有代理應儘早移動到主節點。它不需要立即執行，但管理員可以根據可用的維護視窗對此進行計畫。

可維護性增強

情景服務控制面板和警報

在UCCX 11.6中，提供了一個控制面板來驗證註冊到Context Service的所有元件的狀態。您可以導航到工具>上下文服務狀態頁，在UCCX可維護性頁面上訪問該控制面板。



The screenshot shows a 'Status' window with a 'Ready' indicator. Below it is a 'List of Components' table with the following data:

Component : Host Name	State	Status	Mode	Last Fetched at	Action
FMG : uccx1-71.cumulus-motorcycles.com	Registered	Online	NA	Jul 5, 2017 8:55:18 AM	-
Finesse : uccx1-71.cumulus-motorcycles.com	Registered	Online	Lab	Jul 5, 2017 8:55:27 AM	-
Finesse : uccx2-72.cumulus-motorcycles.com	Registered	Online	Lab	Jul 5, 2017 8:55:27 AM	-
SocialMiner : sm-186.cumulus-motorcycles.com	Registered	Online	Lab	Jul 5, 2017 8:55:26 AM	-
UCCX : uccx1-71.cumulus-motorcycles.com	Registered	Online	Lab	Jul 5, 2017 8:55:26 AM	-
UCCX : uccx2-72.cumulus-motorcycles.com	Registered	Online	Lab	Jul 5, 2017 8:55:26 AM	-

以下是幾個要解釋的狀態：

已註冊 連線狀態 顯示狀態

是 200 ·**在線**
是 非200 ·**在線**
是 不適用 ·**脫機**
否 200 ·**脫機**
否 非200 ·**脫機**
不適用 不適用 ·**已停止**
不適用 不適用 ·**未知***

*當CS控制面板由於錯誤或超時而無法檢索狀態時。

此資訊也可以以JSON/文本格式匯出。

除了控制面板之外，還新增了RTMT警報：**ContextServiceStepsExecutionIssue**

在以下情況下觸發：

1. 由於上下文服務雲的連線問題，上下文服務指令碼中的步驟超時。
2. 由於上下文服務雲中出現錯誤，上下文服務步驟失敗。

升級前瞭解

報告使用者密碼一致性和對LiveData的影響

從UCCX 11.6開始，LiveData和「歷史報表」都使用報告使用者密碼設定資料來源。如果節點之間的密碼不匹配，則報告會受到影響。

升級之前，請確保兩個節點之間的密碼一致。您可以透過以下步驟進行驗證：

1. 導覽至Tools > Password Management。
2. 按一下Check Consistency。
3. 如果沒有錯誤，您就沒問題。如果一致性不匹配（尤其是與報告使用者不匹配），請更新兩個節點上的密碼。

報告使用者升級到UCCX 11.6後無法訪問CUIC報告

Cisco Unified Intelligent Center(CUIC)允許根據分配給訪問使用者的許可權訪問報告。根據許可權級別，使用者可訪問座席報告、主管報告或報告管理員的完整報告集。

根據在UCCX上分配給使用者的角色，從Unified Contact Center Express(UCCX)同步這些許可權。可以通過運行命令`utils cuic user make-admin CCX\`

在升級過程中，UCCX和CUIC應用程式之間的許可權會重新同步，因此授予使用者的提升的CUIC管理員許可權會被覆蓋。因此，使用者只能看到其原始角色所允許的報告。

要提供對使用者升級前所擁有的報告的訪問許可權，請執行以下操作：

1. 在兩台UCCX節點上運行`utils cuic user make-admin CCX\。`
2. 在兩個UCCX節點上重新啟動CUIC報告服務。

電子郵件和Exchange注意事項附件大小限制增加

在UCCX 11.6中，附件大小限制更新為：

- 座席的最大附件數：10
- 座席連線的最大總大小：20MB
- 座席單個連線的最大大小：10MB

雖然UCCX解決方案允許增加附件大小，但是會在Exchange（郵件伺服器）上更新郵件大小限制，以便不會阻止附件。可以根據企業範圍的IT策略應用此限制。如果Exchange伺服器阻止該消息，代理將看到以下錯誤：「無法回覆客戶的電子郵件。按一下傳送以重試或請求。如果問題仍然存在，請與系統管理員聯絡。」

計算郵件限制大小

郵件大小=包含附件的郵件大小+ Base64編碼

Base64編碼=消息大小的~33%

建議的公式是郵件大小= 1.5*郵件大小包括附件

範例：如果郵件大小為9MB（包括附件），則郵件大小應設定為 $(9*1.5)= 14\text{MB}$ 。

既然UCCX 11.6允許最大為20MB的附件大小，那麼如果您必須在UCCX解決方案端利用此增加的限制，則需將郵件大小限制設為 $1.5*20\text{MB}=30\text{MB}$ 。

可以通過運行以下命令在Exchange伺服器上設定限制：

```
Set-TransportConfig -ExternalDsnMaxMessageAttachSize 30 MB -  
InternalDsnMaxMessageAttachSize 30MB -MaxReceiveSize 30MB -MaxSendSize 30MB
```

重要升級注意事項

- 升級後清除所有代理電腦的快取。如果沒有，則可以看到與案頭上的狀態變化和即時資料相關的問題。

- Finesse案頭自定義佈局不會自動遷移。確保將此因素考慮在內，並在升級後正確配置佈局。
- 更新VM設定以與UCCX 11.6的最新OVA模板匹配。如果要執行全新安裝，請使用OVA模板。
- 如果在生產時間內執行升級，請在非主節點上執行升級，以避免任何潛在的中斷。
- 在UCCX 11.6中，Platform Tomcat可以在升級過程中重新啟動。這對使用者沒有影響，但可能生成RTMT警報。這一點可以忽略。
- 升級後，重新安裝RTMT和指令碼編輯器的所有例項。
- 確保使用Real Time Reporting Tool的所有主管和管理員在升級後都安裝了外掛。
- 如果您有任何TLS整合，請檢視TLS支援並驗證您是否使用正確的版本進行設定。
- 檢視瀏覽器要求，並根據需要進行更改。
- 熟悉新的Finesse故障轉移增強功能，並與代理商討論此更新行為。

獲取文檔並提交服務請求

有關如何取得檔案、使用Cisco Bug Search Tool(BST)、提交服務請求和收集其他資訊的資訊，請參閱思科產品檔案的新增內容，網址為

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

訂閱思科產品文檔的新增功能，該文檔將所有新的和修訂的思科技術文檔列為RSS源，並使用閱讀器應用程式將內容直接傳送到您的案頭。RSS訂閱源是一項免費服務。

本手冊中產品的規格和資訊如有更改，恕不另行通知。本手冊中的所有陳述、資訊和建議都被認為是準確的，但是不提供任何形式的擔保，無論是明示的還是暗示的。使用者必須對應用任何產品承擔全部責任。

隨附產品的軟體許可證和有限保修在隨產品一起提供的資訊包中規定，並在此納入此參考。如果您無法找到軟體許可證或有限保修，請聯絡您的思科代表獲取副本。

TCP報頭壓縮的Cisco實現是對加州大學伯克利分校(UCB)開發的一個程式的調整，該程式是UCB公共域版UNIX作業系統的一部分。版權所有。版權所有© 1981, Regents of the University of California。

無論此處提供任何其他擔保，這些供應商的所有文檔檔案和軟體均按「原樣」提供，且存在所有錯誤。思科和上述供應商不承擔任何明示或暗示的擔保，包括但不限於適銷性、特定用途的適用性和非侵權性擔保，或因交易、使用或商業慣例過程中產生的擔保。

在任何情況下，思科或其供應商對於任何間接、特殊、後果或附帶損害，包括（但不限於）因使用或無法使用本手冊而導致利潤損失或資料損失或損壞，即使已通知思科或其供應商可能遭受此類損害。

本文檔中使用的任何Internet協定(IP)地址和電話號碼都不是實際地址和電話號碼。本文檔中包含的任何示例、命令顯示輸出、網路拓撲圖和其他圖僅作說明之用。在說明性內容中使用實際IP地址或

電話號碼是無意的，而且純屬巧合。

所有列印副本和重複軟副本被視為非受控副本，應參考原始聯機版本以獲得最新版本。

思科在全球擁有200多個辦事處。思科網站www.cisco.com/go/offices上列出了地址、電話號碼和傳真號碼。

思科和思科標誌是思科及/或其位於美國和其他國家/地區的附屬機構的商標或註冊商標。要檢視思科商標清單，請訪問此URL:www.cisco.com/go/trademarks。文中所提及之第三方商標均屬於其各自所有者的財產。使用「合作夥伴」一詞並不表示思科與其他任何公司之間存在合作夥伴關係。
(1110R)

©2016 Cisco Systems , Inc.保留所有權利。