UCCX 11.6 - Kommunikation vor der Veröffentlichung

Inhalt

Einführung

Dieses Dokument beschreibt die UCCX 11.6-Vorabversionskommunikation.

> **Hinweis**: Unified Contact Center Express (UCCX) 11.6 ist eine sehr wichtige Version mit wichtigen Updates für wichtige Funktionen und Wartungs-Updates, die Partnern und Kunden helfen werden. Diese Pre-Release-Mitteilung bietet einen Überblick über kritische Updates und wichtige Informationen, die bei der Planung eines schnellen und reibungslosen Upgrades auf UCCX 11.6 helfen.

Hintergrundinformationen

UCCX 11.6 verfügt über eine Reihe von Funktionen, die darauf abzielen, das Produktfunktionsspektrum und die Produktivität von Agenten, Supervisoren und Administratoren zu verbessern. Die E-Mail- und Chat-Funktionen wurden umfassend aktualisiert, während die Berichterstellung für das Cisco Unified Intelligence Center (CUIC) und Finesse Desktop-Updates die Benutzererfahrung im Contact Center deutlich verbessern. Wichtige Aktualisierungen der Wartungsfreundlichkeit, wie das Context Service Dashboard, wurden ebenfalls hinzugefügt, während das System aktualisiert wurde, um Vorteile wie die kürzere Zeit für Upgrades zu bieten.

Eine Zusammenfassung der neuen Funktionen (eine detaillierte Liste finden Sie in den Versionshinweisen):

Cisco Finesse	UCCX-E-Mail	UCCX-Chat	CUIC und Reporting
• Direktübertragung • Agentenstatus basierend auf Sekundärleitung • Standardmäßige Anzeige von Ursachenkodetiketten • Erweitertes Finesse-Failover • Aktuelle Anrufsverlaufs- und Agentenstatusberichte • Warteschlangenstatistiken für FIPPA • Möglichkeit zum Tätigen von Anrufen aus dem READY-Zustand • Überwachung ausgehender Anrufe auf ACD-Leitung • Verlaufsberichte des Supervisors • Vom System generierte Ursachencodes als Label für Agenten und die Möglichkeit, vom System generierte Ursachencode-Labels zu ändern	• E-Mail CC/BCC/Forward • Antworten und Antworten • E-Mail-Signatur • GMAIL-Unterstützung • Gründe für die Zusammenfassung • Multichannel Agent Summary-Bericht	• Gruppenchat • Gründe für die Zusammenfassung • Chat-Planer muss Öffnungszeiten haben • Typisierungsindikator • Multichannel Agent Summary-Bericht	• Neue Dashboards • Neue Diagramme und Anzeigen von Updates • Berichte mit Gruppenbegründungen für Chat und E-Mail • Multichannel Agent Summary-Bericht

Skriptverbesserungen	Verbesserte Outbound-Kampagnen	SSO	Andere
• Header- und Proxy-	• Möglichkeit zum Speichern der	• Integrierte Windows-Authentifizierung	• ESXi 6.5-Unterstützung

Unterstützung für REST-Anruf • Abrufen des Schritts "Reporting Statistics", damit Agenten auf Basis des Codes für den Grund nicht bereit gezählt werden können • Neuer Schritt zum Erstellen eines JSON-Dokuments • Neuer Schritt für JSON-Dokumentendaten • Als Vorlagen hinzugefügte, auf Kontextdiensten basierende IVR-Skripts • TLS 1.2-Unterstützung	explizit angegebenen Reihenfolge der Felder in der importierten Kontaktliste. • Automatischer Import von Kontaktlisten über SFTP- oder HTTP-Server	• Qualifizierung von 4 neuen IDPs und allgemeiner SAML 2.0-Unterstützung	• TLS-Updates • Verbesserte Upgrade-Zeiten • Unterstützung für HyperFlex

UCCX 11.6-Upgrade vorbereiten

UCCX 11.6 unterstützt direkte Upgrades über folgende Pfade:

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		

Alle technischen Sonderaktionen (ES), die auf den oben genannten Versionen angewendet werden, wirken sich nicht auf den Upgrade-Pfad aus. Das Upgrade kann unabhängig davon, welches ES auf dem System installiert ist, von einer der oben genannten Versionen durchgeführt werden. Wenn nach dem Veröffentlichungsdatum dieses Dokuments eine Softwareversion vorliegt, überprüfen Sie in der UCCX-Software-Kompatibilitätsmatrix, ob ein Upgrade-Pfad verfügbar ist.

SocialMiner-Upgrade und Microsoft Exchange

UCCX interagiert mit SocialMiner für alle E-Mail- und Chat-Funktionen. Das 11.6-Upgrade sollte geplant werden, um sicherzustellen, dass sowohl die UCCX- als auch die SocialMiner-Server im gleichen Wartungsfenster auf 11.6 aktualisiert werden. In UCCX 11.6 wurden die E-Mail- und Chat-Funktionen umfangreichen Updates unterzogen. Wenn Sie diese Funktionen von UCCX 11.6 verwenden und SocialMiner noch auf Version 11.5 installiert ist, werden unerwartete Ergebnisse angezeigt, und es werden Fehler/Warnungen angezeigt.

Die empfohlene Reihenfolge für ein Upgrade ist die Aktualisierung des SocialMiner-Servers und der UCCX-Server im gleichen Wartungsfenster.

Die UCCX 11.6-Lösung unterstützt **Microsoft Exchange Server 2013 und 2016 - Enterprise und Standard Edition** für die UCCX E-Mail-Funktionalität. Wenn Sie **Microsoft Exchange Server 2013** verwenden, stellen Sie sicher, dass Sie das kumulierte Update 15 für Exchange Server 2013 (KB3197044) installieren, damit TLS 1.2 von Exchange unterstützt wird. Ohne diesen Patch schlägt die Kommunikation zwischen SocialMiner und **Microsoft Exchange Server 2013** fehl und das E-Mail-Routing schlägt fehl. Wenn Sie bereits über ein UCCX-Server-Setup für **Microsoft Exchange Server 2013** verfügen, stellen Sie sicher, dass Sie diesen Patch installieren, bevor er mit UCCX 11.6 in die Produktionsumgebung integriert wird.

Dies wird für **Microsoft Exchange Server 2016** nicht benötigt.

> **Hinweis**: Wenn Sie TLS 1.2 nicht für Verbindungen zu Exchange verwenden möchten, kann die minimale Server-TLS-Version auf dem SocialMiner-Server auf 1.0 festgelegt werden (siehe Details im TLS-Abschnitt unten). Wenn eine TLS-Diskrepanz zwischen Exchange und SocialMiner besteht, schlagen alle E-Mail-Feeds fehl.

TLS 1.2-Unterstützung für UCCX

In UCCX 11.6 ist der Standardwert TLS 1.2 für Verbindungen, wenn UCCX als Client oder Server in der Verbindung agiert. Kunden, die ein Upgrade auf UCCX 11.6 durchführen und Anwendungen von Drittanbietern verwenden, die mit UCCX interagieren und TLS verwenden, müssen sich dieser Änderung bewusst sein.

UCCX 11.6 bietet außerdem die Möglichkeit, die minimale TLS-Version für Client- und Serververbindungen zu aktualisieren:

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

Beispiel: set tls server min version 1.2

Der Befehl muss auf beiden Knoten ausgeführt werden, wenn es sich um ein Hochverfügbarkeitssystem handelt. Wenn der Befehl ausgeführt wird, muss das System mit dem Befehl **utils system restart** neu gestartet werden.

Die minimale unterstützte TLS-Version kann auch durch Ausführen der folgenden Befehle überprüft werden:

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

> **Hinweis**: Wenn die Mindestversion auf 1.0 festgelegt ist, bedeutet das, dass die Verbindung 1.0, 1.1 und 1.2 unterstützt.

Auswirkungen auf RTMT- und Skripteditor

Aufgrund der Sicherheitsstandards, die TLS 1.2 beinhalten, werden alle UCCX-Plug-Ins wie RTMT und Script Editor neu installiert, sodass sie weiterhin mit UCCX 11.6 verwendet werden können.

Nach dem Upgrade auf UCCX:

1. Laden Sie RTMT herunter, und installieren Sie es erneut auf allen Computern, auf denen zuvor RTMT installiert war. Ältere Versionen von RTMT können keine Verbindung mit UCCX herstellen.
2. Laden Sie den UCCX-Skripteditor auf allen Computern herunter, auf denen zuvor der UCCX-Skripteditor installiert war, und installieren Sie ihn neu.

Unterstützung für ESXi 6.5

Ab UCCX 11.6 wird ESXi 6.5 unterstützt. Aufgrund von Leistungsproblemen mit VMFS 6 und laufenden Untersuchungen von VMWare wird ESXi 6.5 nur mit VMFS 5 unterstützt.

	ESXi 6.5-Unterstützung	VMFS-Version mit ESXi 6.5	Kommentare
BE6K	Ja	VMFS 5	Die Abhängigkeit von anderen Anwendungen verhinde die Verwendung von VMFS 6
Nicht-BE6k	Ja	VMFS 5 und VMFS 6	Für ein Upgrade von ESXi und VMFS ist möglicherweise eine Migration der VMs erforderlich.

Stellen Sie sicher, dass Sie die neueste OVA-Vorlage verwenden, die für 11.6 veröffentlicht wurde.

> **Hinweis**: Unterstützung für VMFS 6 kann zukünftig für vorherige Versionen aktualisiert werden. Das neueste Update finden Sie im UCCX Virtualization-Wiki.

Schnellere Upgrades

In UCCX 11.6 wurden Updates durchgeführt, um die Gesamtzeit für ein vollständiges Upgrade zu reduzieren. Im Rahmen des Switch-Versions-Prozesses werden mehrere Skripte nacheinander ausgeführt, um Daten für einzelne Anwendungen wie Finesse, CUIC und Verlaufsdaten zu migrieren. In UCCX 11.6 wird das Design aktualisiert, sodass die Skripte parallel ausgeführt werden. Dadurch wird die Zeit für die Switch-Version deutlich reduziert.

Während die tatsächliche Zeit für die Switch-Version aufgrund der Größe der Kundendatenbank nicht angezeigt werden kann, konnten interne Tests eine um 30 % verkürzte Zeitspanne im Switch-Versions-Prozess aufzeigen.

Ein ISO für Upgrades und Neuinstallationen

In UCCX 11.6 wird nur ein ISO veröffentlicht, der auf Cisco.com veröffentlicht wird. Dieser ISO kann entweder für ein Upgrade oder für eine Neuinstallation verwendet werden. Die ISO-Norm entspricht der üblichen Namenskonvention von **UCSInstall_UCCX_11.6.XXXXX-XX.sgn.iso.**

Dieses ISO wird mit beiden Boot-Optionen bereitgestellt und dient somit auch als bootfähiges Image.

Desktop- und Browser-Updates

Realtime Reporting Tool

Das Real Time Reporting Tool ist nicht mehr vollständig browserbasiert, sondern verwendet das Java-Applet, das auf den PC heruntergeladen werden muss, um darauf zugreifen zu können. Da in den meisten Browsern Sicherheitsaktualisierungen für die Java-Sicherheit eingeführt wurden, muss das UCCX Real Time Reporting (RTR)-Tool als Java-Applet eingeführt werden, das während der ersten Installation heruntergeladen wird.

Aktualisiertes Verhalten in 11.6:

1. RTR ist jetzt auch als Plugin heruntergeladen werden, navigieren Sie zu **Extras > Plugins** Seite. Sie ist weiterhin auf der Seite **Tools > RealTime Reporting** vorhanden.
2. Beim erstmaligen Zugriff auf RTR von einem bestimmten PC nach dem Upgrade auf UCCX 11.6 wird ein Java-Applet vom UCCX-Server heruntergeladen. Der Benutzer muss über die Rechte verfügen, den Download zu ermöglichen und das gleiche zu öffnen.

   Hinweis: Dies muss auf jedem PC durchgeführt werden, der nach dem Upgrade auf RTR zugreifen möchte. Nach dem Herunterladen des RTR-Applets kann jeder Benutzer, der Zugriff auf den PC hat, dasselbe öffnen.

Empfohlene Java-Version für die Verwendung von RTR ist **Java 8**. Wenn der Benutzer über Java 7 verfügt, muss der Benutzer TLS 1.2 in der Java-Systemsteuerung aktivieren.

Kompatibilitätsmodus für Browser

Wenn Sie Internet Explorer (IE) verwenden, unterstützt Finesse Desktop den Kompatibilitätsmodus nicht. Wenn der Kompatibilitätsmodus aktiviert ist, werden Änderungen vorgenommen, um einen Agenten zu warnen. Das einzige Szenario, in dem der Kompatibilitätsmodus erforderlich ist, ist der Zugriff auf die alte Benutzeroberfläche für CUIC, der Funktionen wie die Mappe "Sicherheit", "Scheduler" usw. enthält.

Single Sign On (SSO)

UCCX unterstützt jetzt die integrierte Windows-Authentifizierung. Weitere Informationen finden Sie in den UCCX-Versionshinweisen und entsprechenden Dokumenten.

Unterstützung für neue Identitätsanbieter

In UCCX 11.6 werden eine Reihe neuer Identitätsanbieter (IDP) qualifiziert und zur Unterstützung hinzugefügt:

- Microsoft AD FS (Active Directory Federation Services): 2.0, 2.1 und 3.0
- PingFederate: 8,2/2,0
- OpenAM: 10,0,1
- Shibboleth: 3,3/0
- F5:13,0

UCCX 11.6 funktioniert auch mit allen IDPs, die mit SAML v2.0 arbeiten. Solange der IDP den SAML v2.0-Standard bestätigt und in der Lage ist, die UCCX (IdS)-Konfiguration zu übernehmen, kann der IDP auch für UCCX SSO verwendet werden, wenn er nicht Teil der oben genannten

Liste ist.

Failover-Erweiterungen für Finesse

Ab UCCX 11.6 wird das Failover-Verhalten verbessert, um die Mitarbeiterproduktivität während eines Finesse-Failovers sicherzustellen, ohne ein vollständiges System-Failover durchzuführen. Es ist wichtig, das Gleiche zu verstehen, damit die Agenten über Verhaltensänderungen informiert werden.

Übersicht über Verhaltensänderungen.

Szenario	UCCX HA-Verhalten	Finesse Service auf Knoten1	Finesse Service für Knoten 2	Finesse-Clientverh
Ausfall des CCX-Moduls auf Knoten 1	CCX Engine auf Seite B wird Master	Finesse geht aus und kehrt zum IN_SERVICE zurück, sobald es eine Verbindung mit der neuen Master-Engine herstellt.	Finesse geht aus und kehrt zum IN_SERVICE zurück, sobald es eine Verbindung mit der neuen Master-Engine herstellt.	Der Agent erkennt rote Trennleiste un meldet sich automatisch wiede der Finesse-Seite a die zuerst zu IN_SERVICE komm Es kann entweder Knoten1 oder Knot sein.
Ausfall des CCX-Moduls auf Knoten 2	CCX Engine auf Seite A setzt Master fort	Finesse bleibt IN_SERVICE	Finesse geht außer Betrieb und kehrt zum IN_SERVICE zurück, sobald es eine Verbindung zum Master-Modul herstellt.	Agenten, die mit N verbunden sind, werden weiterhin angemeldet. Agenten, die mit N verbunden sind, werden vorübergeh getrennt und erhalt eine Verbindung zu Finesse Service au dem Knoten, der IN_SERVICE ist.
Finesse Service OOS auf Knoten 1	Die Steuerung des Motors ist nicht betroffen.	OUT_OF_SERVICE	Finesse auf Node2 bleibt IN_SERVICE	Alle an Node1 angeschlossenen Agenten werden vorübergehend getrennt und werde auf Node2 mit Fine verbunden. Agenten, die an No angeschlossen sin sind nicht betroffen
Finesse Service OOS auf Knoten 2	Die Steuerung des Motors ist nicht betroffen.	Finesse auf Node1 bleibt IN_SERVICE	OUT_OF_SERVICE	Alle mit Node2 verbundenen Agen werden vorübergeh getrennt und werde auf Node2 mit Fine verbunden. An Node1

Fehler beim CCX-Benachrichtigungsdienst in Knoten 1	Die Steuerung des Motors ist nicht betroffen.	OUT_OF_SERVICE	Finesse auf Node2 wird weiterhin IN_SERVICE sein.	angeschlossene Agenten sind davo nicht betroffen. Alle an Node1 angeschlossenen Agenten werden vorübergehend getrennt und werde auf Node2 mit Fine verbunden.
Fehler beim CCX Notification Service in Knoten 2	Die Steuerung des Motors ist nicht betroffen.	Finesse auf Node1 bleibt IN_SERVICE	OUT_OF_SERVICE	Agenten, die mit N verbunden sind, sir nicht betroffen. Alle mit Node2 verbundenen Agen werden vorübergeh getrennt und werde auf Node2 mit Fine verbunden.
Inselmodus	Beide HA-Knoten werden Master	Finesse auf Node1 ist weiterhin IN_SERVICE und wird mit Engine auf Node1 verbunden.	Finesse geht aus und kehrt zu IN_SERVICE zurück, sobald es mit der Engine auf Node2 verbunden ist, die auch der Master ist.	Agenten, die mit N verbunden sind, sir nicht betroffen. Agenten, die mit N verbunden sind, werden weiterhin angemeldet. Agenten, die mit N verbunden sind, werden vorübergeh getrennt und werde auf dem zweiten Knoten mit dem Finesse Service verbunden.

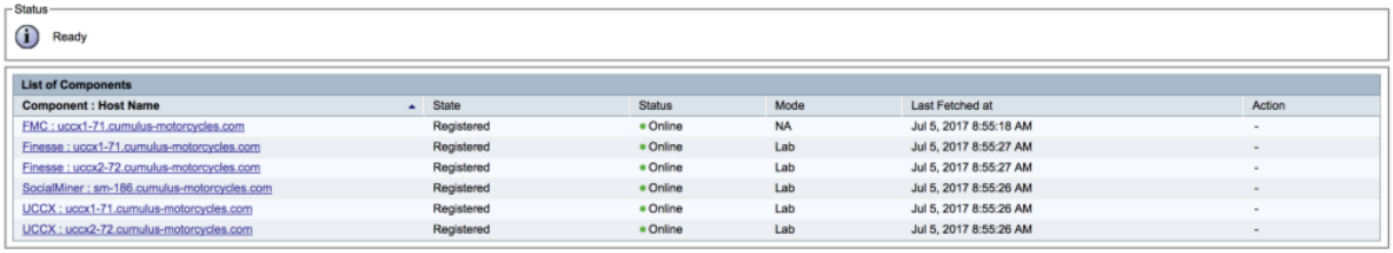
Wichtige Überlegungen

1. UCCX unterstützt kein Load Balancing der Agenten-Anmeldung. Alle Agenten sollten sich nur beim Master Node anmelden. Die Verhaltenserweiterung gilt nur für die Failover-Unterstützung.
2. Es wird nicht unterstützt, beide Knoten gleichzeitig mit demselben Agenten zu verbinden. Dies kann zu Inkonsistenzen in der Mitarbeitererfahrung führen.
3. Falls mehrere Failovers zu Agenten führen, die an beide Knoten angeschlossen sind, sollten alle Agenten frühestens zum Master-Knoten verschoben werden. Dies muss nicht sofort geschehen, aber der Administrator kann dies basierend auf den verfügbaren Wartungsfenstern planen.

Verbesserte Benutzerfreundlichkeit

Context Service Dashboard und Warnungen

In UCCX 11.6 wird ein Dashboard bereitgestellt, um den Status aller Komponenten zu überprüfen, die für den Context Service registriert sind. Auf das Dashboard kann auf der Seite **UCCX Serviceability** zugegriffen werden, wenn Sie zur Seite **Extras > Context Service Status (Status des Kontextdiensts)** navigieren.


Status

Ready

List of Components

Component : Host Name	State	Status	Mode	Last Fetched at	Action
FMC : 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	-

Die folgenden Status müssen interpretiert werden:

Registriert	Verbindungsstatus	Status angezeigt
JA	200	· ONLINE
JA	NICHT-200	· ONLINE
JA	K/A	· OFFLINE
Nein	200	· OFFLINE
Nein	NICHT-200	· OFFLINE
K/A	K/A	· GESPERRT
K/A	K/A	· UNBEKANNT*

* Wenn das CS Dashboard den Status aufgrund von Fehlern oder Zeitüberschreitungen nicht abrufen kann.

Diese Informationen können auch in einem JSON/Textformat exportiert werden.

Zusätzlich zum Dashboard wird eine RTMT-Warnung hinzugefügt:
ContextServiceStepsExecutionProblem

Dies wird ausgelöst, wenn:

1. Schritte des Context Service im Skript-Timeout aufgrund von Verbindungsproblemen mit der Context Service-Cloud.
2. Die Schritte des Kontextservices schlagen aufgrund eines Fehlers in der Context Service-Cloud fehl.

Wissen vor dem Upgrade

Reporting User Password Consistency und Impact auf LiveData

Ab UCCX 11.6 verwenden LiveData- und Verlaufsberichte zum Einrichten der Datenquelle das Reporting User-Kennwort. Wenn die Kennwörter nicht zwischen den Knoten übereinstimmen, wirkt sich dies auf die Berichterstellung aus.

Stellen Sie vor dem Upgrade sicher, dass das Kennwort für beide Knoten konsistent ist. Sie können Folgendes überprüfen:

1. Navigieren Sie zu **Extras > Passwortverwaltung**.
2. Klicken Sie auf **Konsistenz überprüfen**.

3. Wenn keine Fehler auftreten, sind Sie gut. Wenn Konsistenzfehler auftreten (insbesondere beim Berichtsbenutzer), aktualisieren Sie das Kennwort auf beiden Knoten.

Berichtspflichtige Benutzer können nach dem Upgrade auf UCCX 11.6 nicht auf CUIC-Berichte zugreifen

Das Cisco Unified Intelligent Center (CUIC) ermöglicht den Zugriff auf Berichte anhand der Berechtigungen, die dem Benutzer für den Zugriff zugewiesen wurden. Je nach Berechtigungsstufe erhält der Benutzer Zugriff auf die Agentenberichte, die Supervisor-Berichte oder den vollständigen Bericht, der dem Berichtadministrator festgelegt wurde.

Diese Berechtigungen werden von Unified Contact Center Express (UCCX) synchronisiert, basierend auf der Rolle, die dem Benutzer auf dem UCCX zugewiesen wurde. Der Benutzer kann durch Ausführen des Befehls **utils cuic user make-admin CCX\<Benutzername> eigens zum CUIC-Administrator ernannt werden.**

Während des Upgrade-Vorgangs werden die Berechtigungen zwischen UCCX und den CUIC-Anwendungen neu synchronisiert und somit die dem Benutzer erteilten erweiterten CUIC-Administratorrechte überschrieben. Der Benutzer sieht daher nur die Berichte, die seine ursprüngliche Rolle zulässt.

So gewähren Sie Zugriff auf die Berichte, die der Benutzer vor dem Upgrade hatte:

1. Führen Sie **utils cuic user make-admin CCX\<username>** auf beiden UCCX-Knoten aus.

2. Starten Sie den CUIC Reporting Service auf beiden UCCX-Knoten neu.

Erhöhter Größengrenzwert für E-Mails und Exchange-Überlegungen

In UCCX 11.6 werden die Beschränkungen für die Größe von Anhängen wie folgt aktualisiert:

- Max. Anzahl von Anhängen durch einen Agenten: 10
- Max. Anzahl von Anhängen durch einen Agenten: 20 MB
- Max. Größe einer einzelnen Anlage durch einen Agenten: 10 MB

Während die UCCX-Lösung die Erhöhung der Dateigröße für Anhänge zulässt, wird das **Größenlimit für Nachrichten** auf der Exchange (Mail-Server) aktualisiert, sodass die Anhänge nicht blockiert werden. Diese Obergrenze kann auf Grundlage einer unternehmensweiten IT-Richtlinie angewendet werden. Wenn der Exchange-Server die Nachricht blockiert, sieht der Agent den Fehler: "Die E-Mail des Kunden konnte nicht beantwortet werden. Klicken Sie auf Senden, um es erneut zu versuchen oder anzufordern. Wenn das Problem weiterhin besteht, wenden Sie sich an Ihren Systemadministrator."

Berechnen der Nachrichtenbegrenzungsgröße

Nachrichtengröße = Größe der E-Mail enthält Anhänge + Base64-Codierung

Base64-Codierung = ~33 % der Nachrichtengröße

Empfohlene Formel: **Nachrichtengröße = 1,5*Größe der E-Mail enthält Anhänge**

Beispiel: Wenn die Nachrichtengröße 9 MB beträgt (einschließlich Anlagen), sollte die Nachrichtengröße als Grenzwert (9*1,5) = 14 MB festgelegt werden.

Da UCCX 11.6 eine Dateigröße von bis zu 20 MB zulässt, muss die Nachrichtengröße auf **1,5*20 MB=30 MB** begrenzt werden, wenn Sie diese erhöhte Obergrenze für die UCCX-Lösung nutzen müssen.

Der Grenzwert kann auf dem Exchange-Server festgelegt werden, indem der Befehl ausgeführt wird:

Set-TransportConfig - ExternalDsnMaxMessageAttachSize 30 MB - InternalDsnMaxMessageAttachSize 30 MB - MaxReceiveGröße 30 MB - MaxSendSize 30 MB

Wichtige Upgrade-Überlegungen

- Löschen Sie nach dem Upgrade den Cache aller Agentencomputer. Andernfalls können Probleme im Zusammenhang mit Statusänderungen und Echtzeitdaten auf dem Desktop festgestellt werden.
- Das benutzerdefinierte Layout von Finesse Desktop wird nicht automatisch migriert. Stellen Sie sicher, dass Sie dies berücksichtigen und das Layout nach dem Upgrade korrekt konfiguriert haben.
- Aktualisieren Sie die VM-Einstellungen, um sie der neuesten OVA-Vorlage für UCCX 11.6 zuzuordnen. Wenn Sie eine Neuinstallation durchführen, verwenden Sie die OVA-Vorlage.
- Wenn Sie das Upgrade während der Produktionszeiten durchführen, führen Sie das Upgrade auf dem Nicht-Master-Knoten durch, um mögliche Unterbrechungen zu vermeiden.
- In UCCX 1.6 kann die Plattform Tomcat während des Upgrades neu gestartet werden. Dies hat keine Auswirkungen auf die Benutzer, kann jedoch eine RTMT-Warnung generieren. Dies kann ignoriert werden.
- Installieren Sie nach dem Upgrade alle Instanzen von RTMT und Script Editor neu.
- Stellen Sie sicher, dass das Plug-in nach dem Upgrade bei allen Supervisoren und Administratoren, die das Real Time Reporting Tool verwenden, installiert ist.
- Wenn Sie über TLS-Integrationen verfügen, überprüfen Sie den TLS-Support, und stellen Sie sicher, dass die richtigen Versionen installiert sind.
- Überprüfen Sie die Browseranforderungen, und nehmen Sie ggf. Änderungen vor.
- Machen Sie sich mit den neuen Finesse Failover-Erweiterungen vertraut, und besprechen Sie mit den Agenten dieses aktualisierte Verhalten.

Dokumentation abrufen und Serviceanfrage einreichen

Weitere Informationen zum Erhalt von Dokumentation finden Sie im Cisco Bug Search Tool (BST), beim Einreichen einer Serviceanfrage und beim Sammeln weiterer Informationen unter What's New in Cisco Product Documentation (Neuigkeiten 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 JEGLICHE 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 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 JEGLICHER 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 HANDBUFS 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.