



Versionshinweise für Cisco WebEx Meetings Server Version 2.8

Erste Veröffentlichung: 12. April 2017

Letzte Änderung: 15. Juni 2017

Cisco WebEx Meetings Server Software-Dokumentation

Diese Versionshinweise enthalten Informationen zu neuen Funktionen, Anforderungen, Einschränkungen und Vorsichtsmaßnahmen für alle Versionen von Cisco WebEx Meetings Server Version 2.8. Diese Software-Dokumentation wird bei jedem Wartungsupdate aktualisiert, jedoch nicht bei Patches oder Hotfixes. Jedes Wartungsupdate schließt die Funktionen, Anforderungen, Einschränkungen und Fehlerbehebungen vorheriger Versionen ein, falls nicht anders angegeben. Wir empfehlen Ihnen, diese Versionshinweise vor der Bereitstellung von Cisco WebEx Meetings Server durchzusehen, um Informationen zu Problemen, die Ihr System betreffen könnten, zu erhalten.

Die neueste Aktualisierungssoftware für dieses Produkt steht hier zum Download bereit: <http://software.cisco.com/download>.

Wählen Sie **Produkte > Konferenz > Webkonferenz > WebEx Meetings Server > WebEx Meetings Server 2.8**.

Aktualisierungen in der Dokumentation

Datum	Ändern
Montag, 24. April 2017	CSCve05932 wurde zu Behobene Probleme bei Cisco WebEx Meetings Server 2.8, auf Seite 16 hinzugefügt und die Build-Nummer für Version 2.8 auf 2.8.1.17 aktualisiert.
25. Mai 2017	Berichtigt Aufzeichnungen verwalten, auf Seite 4 für CSCve04460. Der Administrator hat eingeschränkten Zugriff auf Aufzeichnungen.

Dokumentation finden

Die Administrationsdokumentation finden Sie unter: <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/tsd-products-support-series-home.html>.

Geben Sie Ihren Nutzern den folgenden URL: <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-user-guide-list.html>.

Neu hinzugekommene und geänderte Funktionen von Cisco WebEx Meetings Server in der Version 2.8

In diesem Abschnitt werden Funktionen beschrieben, die in dieser Version neu hinzugekommen sind oder geändert wurden.

Die ausführliche Liste der Systemanforderungen finden Sie im *Planungsleitfaden und Systemanforderungen für Cisco WebEx Meetings Server in der Version 2.8*. Besuchen Sie http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Alle unterstützten Funktionen von Cisco WebEx Meetings Server (CWMS) Version 2.7 (einschließlich durch Wartungsupdates ergänzte Funktionen) werden in CWMS 2.8 unterstützt. Das Datenblatt für Cisco WebEx Meetings Server liefert einen Überblick über die Funktionen und Vorteile von CWMS. Besuchen Sie http://www.cisco.com/en/US/prod/collateral/ps10352/ps10362/ps12732/data_sheet_c78-717754.html.

Virtuelle Maschinen ersetzen

Mit dieser Funktion können Sie eine virtuelle Maschine ersetzen, ohne das CWMS-System von Grund auf neu erstellen zu müssen. Sie können alle virtuellen Maschinen ersetzen, die Bestandteil eines CWMS-Systems sind, mit Ausnahme des primären Administratorknotens. So können Sie ein System wiederherstellen, wenn einige Knoten repariert werden müssen, aber der primäre Administratorknoten weiterhin funktionstüchtig ist.

Erweiterung des Administrations-Dashboards

Im Dashboard (Administrationsstartseite) werden nun Links zu Informationen über die Rechenzentren angezeigt.

Erweiterung des Anwendungs-Überwachungsprotokolls

Diese Version umfasst die folgenden neuen Konfigurationsoptionen für das Anwendungs-Überwachungsprotokoll: **Meeting-Audit-Protokolle aktivieren** Nach Aktivierung dieser Einstellung schreibt das System weitere Protokolle zu Meetings im Anwendungs-Überwachungsprotokoll.

Diese Einstellung kann von allen Benutzern angezeigt und konfiguriert werden, denen die Prüfer-Rolle zugewiesen ist. Wenn das System keinem Benutzer die Prüfer-Rolle zugewiesen hat, kann diese Einstellung nur von Benutzern mit den folgenden Rollen angezeigt und konfiguriert werden:

- Administrator
- SSO-Administrator
- LDAP-Administrator

Backup Management

Sie können Systemsicherungen anzeigen und eine Sicherung auswählen, um sie für die Notfallwiederherstellung zu prüfen bzw. zu verwenden. Sie haben außerdem die Möglichkeit, ausgewählte Sicherungen zu löschen.

Schaltfläche „Jetzt sichern“

Klicken Sie auf **Jetzt sichern**, um sofort mit der Sicherung Ihres Systems zu beginnen.

- Wird diese Aktion gestartet, kann sie nicht angehalten werden.
- Bis der Backup-Vorgang abgeschlossen ist, dürfen Sie Ihr System nicht herunterfahren, neu starten oder den Wartungsmodus beenden (sofern sich das System im Wartungsmodus befindet).
- Je nach System kann der Backup-Vorgang bis zu einer Stunde in Anspruch nehmen.
- Sie können den Status des Backup-Vorgangs auf der Seite **Backup Management** überwachen.

Blast Dial-Audioankündigungen

Sie können das Beitreten zu einem Blast Dial-Meeting beschleunigen und vereinfachen, indem Sie die die Anforderung überspringen, 1, 2 oder 3 zu drücken. Zudem können Sie konfigurieren, welche Aufforderungen angezeigt werden sollen. Wählen Sie dazu eine der folgenden Optionen aus:

- **Aufforderung „1 drücken“ überspringen**: Der Teilnehmer wird direkt mit dem Meeting verbunden. Die Aufforderung zur Eingabe von 1, 2 oder 3 wird nicht angezeigt. Die PIN-Einstellung bleibt unverändert und die Willkommensansage wird angezeigt.
- **Aufforderung „1 drücken“ mit Willkommensansage überspringen** umgehen: Der Teilnehmer wird direkt mit dem Meeting verbunden. Die Aufforderung zur Eingabe von 1, 2 oder 3 wird nicht angezeigt. Die PIN-Einstellung bleibt unverändert, aber die Willkommensansage wird nicht angezeigt.

Benutzer löschen

Sie können Gastgeber- und Administrator-Kontos löschen. Wenn Sie ein Konto löschen, werden auch die Benutzerdaten sowie die künftigen und wiederkehrenden Meetings, die vom jeweiligen Benutzer abgehalten werden, gelöscht. Vergangene Meetings werden 6 Monate lang gespeichert, da sie für Berichte und zu Zwecken der Rechnungsstellung, Lizenzierung und Überwachung benötigt werden.



Wichtig

Ein gelöschter Benutzer kann nach dem Löschen sechs Monate lang die Adresse nicht verwenden, die mit dem gelöschten Konto verknüpft ist, um Meetings im System beizutreten. Um die Möglichkeit, Meetings als Gastgeber zu leiten, zu deaktivieren, dem Benutzer jedoch weiterhin zu ermöglichen, an Meetings teilzunehmen, legen Sie den Kontostatus des Benutzers auf **INAKTIV** fest.

Ausgewählte Benutzer exportieren

Sie können Benutzer auch anhand von Filtern und einer Suchzeichenfolge suchen. In den Ergebnissen können Sie einen oder mehrere Benutzer auswählen und in eine CSV-Datei (mit durch Kommas getrennten Werten) exportieren. Wenn Sie keine Benutzer auswählen, enthält die exportierte CSV-Datei alle Benutzer, die den ausgewählten Filtern entsprechen.

Unterstützung von Jabber

Diese Version unterstützt erstmalig Cisco Jabber Version 11.8.

Spalte „Zuletzt abgehalten“

Bei Auswahl des Filters **Lizenznehmer mit dauerhaften Lizenzen** oder **Lizenznehmer mit temporären Lizenzen** auf der Registerkarte **Benutzer** ersetzt das System in der Ergebnissen die Spalte **Sitzungstyp** mit der Spalte **Zuletzt abgehalten**. In der Spalte **Zuletzt abgehalten** wird das Datum angezeigt, an dem der entsprechende Benutzer zuletzt ein Meeting abgehalten hat. Wenn das Datum mehr als 6 Monate zurückliegt, wird in der Spalte anstelle des Datums **Über sechs Monate** angezeigt.

Aufzeichnungen verwalten

Sie haben als Administrator zu Zwecken der Dateispeicherverwaltung eingeschränkten Zugriff auf alle Aufzeichnungen im System. Sie können Aufzeichnungen auflisten, suchen und löschen. Prüfer können nur Aufzeichnungen auflisten und suchen.

Meeting-Gastgeber können ihre eigenen Aufzeichnungen löschen. Um Probleme durch eine versehentliche Löschung zu vermeiden, werden gelöschte Aufzeichnungen im System sechs Monate lang gespeichert.

Neue Parameter für die Anpassung von E-Mail-Vorlagen

Diese Version enthält erstmals die Variable „%MeetingNumberNoSpaces%“. Diese Variable stellt die Meeting-Nummer ohne Leerzeichen bereit. Die vorhandene Variable „%MeetingNumber%“ stellt die Meeting-Nummer mit Leerzeichen bereit.

Meeting-Zugriff auf authentifizierte Benutzer beschränken

Meeting-Gastgeber können interne Meetings einrichten, bei denen Teilnehmer sich mittels Single Sign On-Authentifizierung anmelden müssen. Außerdem können Gastgeber interne Meetings einrichten, die nur für eingeladene Benutzer verfügbar sind.

Sie können benutzerdefinierte Tags konfigurieren, um Teilnehmer als interne oder externe Teilnehmer (Gast) zu identifizieren. Diese Tags werden in Berichten zusammen mit den Benutzernamen der Teilnehmer angezeigt.

TLS-Unterstützung

CWMS Version 2.8 unterstützt TLS 1.1 und neuer; TLS 1.0 wird nicht unterstützt, mit einer Ausnahme. Client-Verbindungen zwischen CWMS und SMTP-Servern mit TLS 1.0 werden unterstützt.

CWMS-Version 2.8 unterstützt für sichere Telefonkonferenzen Cisco Unified Communications Server Version 10.5.2 und höher (bis 11.5).

Aktualisierter Browser-Support

Diese Version unterstützt zudem die folgenden Browser-Versionen:

Windows:

- Chrome 57.0.2987
- Edge (auf Windows 10)
- Firefox 52.0.2
- Internet Explorer 11.0.9600

Mac:

- Chrome 57.0
- Firefox 52.0.2
- Safari 10.0.3

Überprüfung der Backup-Daten

Das System überprüft Backups anhand der folgenden Punkte:

- Das Verzeichnis ist vorhanden.
- Die Dateien sind vorhanden.
- Die Prüfsumme ist richtig.
- Der Ordner befindet sich im CWMS-Speicher.

WebEx Meeting Client-Anwendung

Diese Version unterstützt die WebEx Meetings-Anwendung, Version 31.11.6.9 für Windows und Mac.

WebEx-Player für Netzwerkaufzeichnungen

Diese Version unterstützt die folgenden Versionen der Cisco Netzwerkaufzeichnungs-Player:

- **Windows:** 31.11.6.9
- **Mac:** 31.0.0.1100

WebEx-Produktivitätswerkzeuge

Diese Version unterstützt die WebEx Produktivitätswerkzeuge, Version 2.82.7000.1174 für Windows.

Unterstützte Upgrade-Pfade

Diese Version von Cisco WebEx Meetings Server unterstützt jetzt Upgrades von Version 1.x bis 2.8. Folgende Punkte treffen zu:

- Ein Upgrade wird als Ersetzen des Systems definiert, um umfassende Änderungen bereitzustellen, die wir am System vorgenommen haben.

- Ein Update wird als inkrementelle Änderung des Systems definiert. Updates stellen Fehlerbehebungen und kleinere Verbesserungen bereit.
- Bei einem Update werden alle Daten des ursprünglichen Systems beibehalten. Bei einem Upgrade werden mit Ausnahme der Protokolle alle Daten des ursprünglichen Systems beibehalten.
- Wenn Sie ein Upgrade durchführen, können Sie die Hauptversion der Software nicht überspringen, um direkt zum passenden Wartungsupdate zu gelangen.

Beispiel: Um ein Upgrade von Version 1.5 MR5 auf Version 2.8 MR durchzuführen, müssen Sie ein *Upgrade* von Version 1.5 MR5 auf Version 2.8 und anschließend eine *Aktualisierung* auf Version 2.8 MR durchführen.

**Hinweis**

Bei allen Updates kommt es zum Systemausfall. Bei MDC-Systemen können Sie die Aktualisierung für beide Rechenzentren gleichzeitig durchführen.

**Vorsicht**

Klicken Sie für ein Rechenzentrum erst dann **Neustart**, wenn die Aktualisierung des anderen Zentrums abgeschlossen ist und beide die Schaltfläche **Neustart** anzeigen. Wenn Sie von Version 2.5 MR6 oder höher auf 2.8 aktualisieren, kommt es beim Neustart eines Rechenzentrums, bevor die Aktualisierung des anderen Rechenzentrums abgeschlossen ist, zu einem Abbruch der Replikation.

Verwenden Sie die folgende Tabelle, um die Vorgehensweise bei der Aktualisierung auf Cisco WebEx Meetings Server Version 2.8 zu bestimmen.

Installierte Version	Auf Version	Pfad
1.0 bis 1.1	2.8	<ol style="list-style-type: none"> 1 Aktualisierung auf Version 1.5. 2 Aktualisierung auf 1.5MR5 Patch 2 oder höher. 3 Upgrade auf Version 2.8.
1.5 auf 1.5MR4	2.8	<ol style="list-style-type: none"> 1 Aktualisierung auf 1.5MR5 Patch 2 oder höher. 2 Upgrade auf Version 2.8.
1.5 MR5	2.8	<ol style="list-style-type: none"> 1 Aktualisierung auf 1.5MR5 Patch 2 oder höher. 2 Upgrade auf Version 2.8.
1.5 MR5 Patch 2 oder höher	2.8	Upgrade auf Version 2.8.
2.0 auf 2.0MR8	2.8	<ol style="list-style-type: none"> 1 Aktualisierung auf Version 2.0MR9. 2 Aktualisierung auf Version 2.8.

Installierte Version	Auf Version	Pfad
2.0MR9 oder höher	2.8	Aktualisierung auf Version 2.8.
2.5 auf 2.5MR5	2.8	<ol style="list-style-type: none"> 1 Aktualisierung auf Version 2.5MR6. 2 Aktualisierung auf Version 2.8.
2.5MR6	2.8	Aktualisierung auf Version 2.8.
2.6 auf Version 2.6MR2	2.8	<ol style="list-style-type: none"> 1 Aktualisierung auf Version 2.6MR3 2 Aktualisierung auf Version 2.8
2.6MR3 oder höher	2.8	Aktualisierung auf Version 2.8.
2.7 oder alle 2.7MR-Versionen	2.8	Aktualisierung auf Version 2.8.
2.8 oder alle 2.8MR-Versionen	Alle 2.8MR-Versionen	Aktualisierung auf Version 2.8MR.



Wichtig

Sie können während einem Upgrade oder einem Update nicht den Typ der Audioverschlüsselung ändern (Audio Encrypted – AE/Audio Unencrypted – AU). Die einzige Möglichkeit zum Wechsel eines Systems nach Bereitstellung von einer Audioverschlüsselungsart zur anderen ist die Bereitstellung eines neuen Systems.

Weitere Informationen finden Sie in den folgenden Dokumenten:

- *Cisco WebEx Meetings Server-Administrationsleitfaden Version 2.8*: http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html
- *Cisco WebEx Meetings Server-Planungsleitfaden und -Systemvoraussetzungen Version 2.8*: <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html>

Aktualisieren Ihres Hochverfügbarkeitssystems

Bei Systemen, die bereits mit einem bestehenden Hochverfügbarkeitssystem verbunden sind, wird das Hochverfügbarkeitssystem beim Aktualisieren des primären Systems automatisch aktualisiert. Stellen Sie sicher, dass alle virtuellen HA-Maschinen eingeschaltet sind und ausgeführt werden, bevor Sie den Aktualisierungsvorgang starten.

Um ein Hochverfügbarkeitssystem zu Ihrem primären System hinzuzufügen, stellen Sie zunächst das HA-System bereit. Aktualisieren Sie dann das HA-System auf dieselbe Version wie das primäre System. Das HA-System wird am Ende des Aktualisierungsvorgangs neu gestartet. Wir empfehlen, nach dem Neustart 15 Minuten zu warten, bevor Sie das HA-System zum primären System hinzufügen.

<http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html>

Einschränkungen und Vorbehalt

Entfernen eines Internet Reverse Proxys

Als Teil des Deinstallationsvorgangs eines Internet Reverse Proxy (IRP)-Knotens sendet die virtuelle Admin-Maschine eine Deinstallationsnachricht an den IRP-Server. Die Nachricht deinstalliert den IRP-Server und somit alle externen Zugriffsmöglichkeiten auf das System. Diese Nachricht wird als Klartext gesendet und ist nicht authentifiziert. Durchdachte böswillige Codes könnten dieses Verhalten replizieren und zu einer Service-Verweigerung (Denial of Service) führen.

Wir empfehlen, den Zugriff ausschließlich auf Port 64616 auf dem IRP-Knoten und auf die virtuelle Admin-Maschine beschränken.

Produktivitätswerkzeuge

EMC SourceOne

WebEx-Produktivitätswerkzeuge unterstützen nicht EMC SourceOne. Bei Benutzern von EMC SourceOne kann es zu Leistungseinbußen kommen.

Inkompatible Versionen

Jede Version von Cisco WebEx Meetings Server unterstützt eine spezifische Version des Cisco WebEx-Produktivitätswerkzeuge-Clients. Sie können die unterstützte Version der WebEx-Produktivitätswerkzeuge auf der Website von Cisco WebEx Meetings Server durch Anklicken des Downloads-Links herunterladen. Die Verwendung von nicht kompatiblen Versionen dieser beiden Anwendungen kann zu Problemen führen.

Aufzeichnungsbeschränkungen

Die maximale Aufzeichnungsgröße pro Aufzeichnung beträgt 2,2 GB (Systembegrenzung). Bei Multi-Datenzentren müssen Sie darauf achten, dass genügend Speicherplatz für alle Datenzentren vorhanden ist. Die maximale Anzahl von Aufzeichnungen hängt von Ihrer Speicherserverkapazität ab. Anhand der folgenden Formel können Sie die erforderliche Speicherservergröße für einen charakteristischen Fünfjahreszeitraum schätzen:

Geschätzte Meetingstunden, die pro Tag aufgezeichnet werden * 50-100 MB pro Aufzeichnungsstunde * 5 Jahre * 24 Stunden pro Tag * 365 Tage pro Jahr

Es gibt keine Speicherbeschränkungen pro Benutzer. Das System speichert Aufzeichnungen für eine unbegrenzte Zeit, bis Benutzer diese löschen. Um zu vermeiden, dass wichtige Aufzeichnungen versehentlich gelöscht werden, gibt es keine Einstellung zum automatischen Löschen von Aufzeichnungen. Aufzeichnungen, die zur Löschung gekennzeichnet wurden, werden bis zu sechs Monate lang im Speicherserver gespeichert. In dieser Zeit können Benutzer die Aufzeichnungen weiterhin auf anderen Medien archivieren.

Beachten Sie, dass es sich bei der Option **Aufzeichnung** unter **Administrations-Dashboard > Einstellungen > Meetings > Teilnehmerprivilegien** um eine systemweite Einstellung handelt, wenn Sie einen Speicherserver konfigurieren und **Aufzeichnung** aktivieren.

Sitzungstypen

Ein Sitzungstyp ist eine vordefinierte Sammlung von Funktionen und Optionen (ein Profil), die Site-Administratoren für die individuelle Anpassung von und Zuweisung an Benutzer verwenden können. Der Standardsitzungstyp (Meeting) ist der PRO-Sitzungstyp. Da der PRO-Sitzungstyp und die benutzerdefinierten Sitzungstypen zusammenhängen, empfehlen wir Ihnen, den PRO-Sitzungstyp nicht zu ändern. Als Best Practice empfehlen wir, einen benutzerdefinierten Sitzungstyp zu erstellen, der modifiziert werden kann.

Änderungen von SSO und E-Mail-Adresse

Bei dieser Version kann der Identitätsanbieter-Server (IdP, Identity Provider) ein beliebiges eindeutiges und statisches Feld im Active Directory (AD) als NameID für die SSO-Konfiguration verwenden. Wenn Sie die Funktion zur Änderung von E-Mail-Adressen verwenden, ist das Feld „E-Mail AD“ nicht statisch. Ändern Sie die Zuordnung für das Feld „NameID“ auf dem IdP-Server zu einem eindeutigen AD-Feld, das sich vom Feld „E-Mail“ unterscheidet. Wenn Sie die Funktion zur Änderung von E-Mail-Adressen nicht verwenden möchten, muss die Zuordnung für das Feld „NameID“ nicht geändert werden.



Vorsicht

Wenn das Feld „NameID“ zum Feld „E-Mail AD“ zugeordnet wird und Sie die E-Mail-Adressen der Benutzer ändern, erstellt das System für jede geänderte Adresse ein neues Benutzer-Konto.

Outlook wird einmal täglich mit dem Exchange-Server synchronisiert. Wenn Sie die E-Mail-Adresse eines vorhandenen Benutzers auf dem Exchange-Server ändern, wird diese Änderung nicht sofort an Outlook übertragen. Bis zur Synchronisierung erhält das System die alte E-Mail-Adresse des Benutzers und gibt eine Meldung aus, dass der Benutzer nicht gefunden werden kann. Ein stellvertretender (Proxy-)Benutzer kann kein Meeting für den Benutzer ansetzen oder sie als alternativer Gastgeber kennzeichnen, bis die Synchronisierung von Outlook mit dem Exchange-Server erfolgt ist.

Das manuelle Synchronisieren des Systems löst dieses Problem nicht. Bei dieser Einschränkung handelt es sich nicht um ein CWMS-Problem; es ergibt sich aus dem Design von Outlook und Exchange.

Siehe auch [Über die SAML SSO-Konfiguration](#), auf Seite 12

Einschränkung für Windows 10 und Edge-Browser

Der Edge-Browser (für Windows 10) bietet keine Unterstützung für die Wiedergabe von WebEx.-Aufzeichnungen.

Virtuelle Desktop-Infrastruktur

Es ist bekannt, dass die folgenden Einschränkungen und Vorbehalte Virtual Desktop Infrastructure (VDI)-Umgebungen beeinträchtigen.

- Citrix XenDesktop und XenApp sind die einzigen Softwareprogramme zur Desktop-Virtualisierung, die für diese Version von Cisco WebEx Meetings Server unterstützt werden.

- Eine architektonische Einschränkung der virtuellen Desktop-Umgebung kann die Videoqualität beeinträchtigen. Die Bildwiederholungsrate ist ggf. gering und führt beim Senden eines Videos zu einem unzureichenden Anwenderergebnis.
- Einige Videodateien können in einer virtuellen Desktop-Umgebung nicht mit anderen geteilt werden.
- Remote Access und Access Anywhere werden in virtuellen Desktopumgebungen nicht unterstützt. Die zugrundeliegende Citrix-Plattform entfernt die Remote Access- und Access Anywhere-Agenten nach dem Neustart des Betriebssystems.

Wichtige Hinweise

CWMS-Lizenzierung

Multi-Datenzentrum-Lizenzen

Die Multi-Datenzentrum (MDC)-Lizenzierung ist erforderlich, um Datenzentren in einem System zusammenzufassen. Für jedes Datenzentrum ist eine MDC-Systemlizenz erforderlich; ein MDC-System benötigt mindestens zwei Lizenzen, jeweils eine pro Datenzentrum. Ein Einzeldatenzentrum (SDC) benötigt keine Systemlizenz. Informationen zu Ihrer Version siehe „Über MDC-Lizenzierung“ im Cisco WebEx Meetings Server-Administrationsleitfaden: <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html>.

Gastgeber-Lizenzen

Die Zählung von Gastgeber (Benutzer)-Lizenzen hat sich mit Version 2.5 wesentlich verändert. Ein Benutzer kann Gastgeber von maximal zwei gleichzeitigen Meetings sein, wofür eine Lizenz verbraucht wird. Zuvor verbrauchte ein Benutzer, der Gastgeber mehrerer Meetings war, mehrere Lizenzen. Zum Ansetzen oder Besuchen eines Meetings ist keine Gastgeber-Lizenz erforderlich. Informationen zu Ihrer Version siehe „Lizenzstatus von Benutzern“ im Cisco WebEx Meetings Server-Administrationsleitfaden: <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html>.

Hypervisor-Unterstützung

Cisco WebEx Meetings Server läuft auf virtuellen VMware-Maschinen.

- Sowohl VMware vSphere als auch VMware vCenter müssen Cisco WebEx Meetings Server bereitstellen. Mithilfe des vSphere-Clients können Sie die OVA-Datei von Cisco WebEx Meetings Server auf einem von vCenter verwalteten ESXi-Host bereitstellen.
- Erwerben Sie VMware vSphere 5.0, 5.0 Update 1, 5.1, 5.5 oder 6.0 für die Verwendung als Hypervisor-Plattform für Cisco WebEx Meetings Server.
 - Erwerben Sie vSphere direkt von Cisco aus der GPL (globale Preisliste). Cisco ist ein autorisierter VMware-Partner und -Verteiler. Dies ist besonders praktisch, wenn Sie gerne alle Produkte „aus einer Hand“ erwerben möchten.
 - Sie können vSphere direkt von VMware über direkt mit VMware abgeschlossene Firmenverträge erwerben.
- Cisco WebEx Meetings Server unterstützt keine anderen Hypervisoren.

- Vollständige Einzelheiten zu den Hypervisor-Anforderungen finden Sie in den *Cisco WebEx Meetings Server-Systemanforderungen* unter http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Unterstützung für 4096-Bit-Zertifikate

Cisco WebEx Meetings Server (CWMS) ist für die Verwendung von 2048-Bit-Zertifikaten für die zugehörigen SSL-Systemzertifikate hartkodiert. Zertifikate können selbstsigniert oder von einer privaten oder öffentlichen Zertifizierungsstelle (CA) signiert sein.

CWMS unterstützt zudem die Verwendung von 4096-Bit-Zertifikaten, wenn diese im folgenden Format importiert werden:

- Zertifikat über sichere Telefonkonferenzen,
- SMTP-Zertifikat,
- SSO-IdP-Zertifikat oder
- Bestandteil eines SSL-Systemzertifikat-Pakets.

Zertifikate, die als Bestandteil eines Systemzertifikat-Pakets importiert werden, müssen von einer privaten oder öffentlichen Zertifizierungsstelle (CA) signiert werden.

Informationen zur Verwendung selbstsignierter Zertifikate

Wir empfehlen Ihnen dringend, anstatt des bereitgestellten selbst signierten Zertifikats ein öffentlich signiertes Zertifikat zu verwenden. Die Browser der Benutzer vertrauen öffentlich signierten Zertifikaten. Dieses Vertrauen ergibt sich automatisch aus der Liste der Root Certificate Authority-Zertifikate auf dem Computer eines jeden Benutzers.

Wenn bei Multi-Datenzentrum-Systemen selbstsignierte Zertifikate verwendet werden, erhält der Benutzer verschiedene Zertifikatswarnungen und muss allen Zertifikaten vertrauen und diese installieren, um das System zu nutzen.

Werden selbst signierte Zertifikate verwendet, haben manche Benutzer möglicherweise Schwierigkeiten beim Beitreten zu Meetings, da die Browser solchen Zertifikaten standardmäßig nicht vertrauen. In diesem Fall muss der Benutzer eine ausdrückliche Vertrauensstellung herstellen, bevor er einem Meeting auf Ihrer Site beitreten kann. Einige Benutzer wissen möglicherweise nicht, wie mit einem solchen Zertifikat eine Vertrauensstellung hergestellt werden kann. Andere können dies aufgrund der administrativen Einstellungen unter Umständen nicht tun. Verwenden Sie wann immer möglich öffentlich signierte Zertifikate, um das bestmögliche Benutzererlebnis zu gewährleisten.

Das Benutzerhandbuch bietet zu diesem Thema weitere Informationen für Benutzer. Weitere Informationen finden Sie im Abschnitt "Der Meeting-Client lädt nicht" des Kapitels zur "Fehlerbehebung" im *Cisco WebEx Meetings Server-Benutzerhandbuch* unter http://www.cisco.com/en/US/products/ps12732/products_user_guide_list.html.

Unterstützte Verschlüsselung

Cisco WebEx Meetings Server unterstützt folgende Verschlüsselungen:

TLS Version 1.1

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)

TLS Version 1.2

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)

Über die SAML SSO-Konfiguration

Diese Version unterstützt alle eindeutigen Active Directory (AD)-Felder als NameID für die SSO-Konfiguration. Wir empfehlen folgende AD-Attribute als NameID für die SSO-Konfiguration:

- E-Mail
- SAMKontoName
- UserPrincipalName (UPN)
- TelephoneNumber
- EmployeeNumber
- ObjectSid

Erforderliche SAML-Assertion-Attribute

Die folgenden SAML-Assertion-Attribute sind für die Funktion zur automatischen Konto-Erstellung erforderlich:

- Nachname
- Vorname
- E-Mail

**Wichtig**

Das E-Mail-Attribut ist immer erforderlich; auch dann, wenn die Funktion zur automatischen Konto-Erstellung und automatischen Konto-Aktualisierung in der SSO-Konfiguration deaktiviert ist.

Erweitern Ihres Systems

Wenn Sie über Speicherauszüge Ihres vorhandenen Systems (vor der Erweiterung) verfügen, vergewissern Sie sich, dass Ihr erweitertes System bereits betrieben wird, während Sie Ihr vorhandenes System entfernen oder löschen. Dadurch wird das versehentliche Löschen der VMDK-Datei von Festplatte 4, auf welche das erweiterte System u. U. Zugriff hat, verhindert.

Upgrade-Benachrichtigung für die Produktivitätswerkzeuge

Wenn ein zuvor bereitgestelltes Produktivitätswerkzeuge-Paket eine andere Versions- oder Build-Nummer als ein neu eingesetztes Produktivitätswerkzeuge-Paket hat und das Upgrade nicht blockiert wird, werden Sie von Ihrem Produktivitätswerkzeuge-Client mittels eines Upgrade-Warndialogfelds benachrichtigt.

SNMP v2 Community-Namen

Es wird keine voreingestellte SNMP v2 Community-Namenseingabe in Cisco WebEx Meetings Server geben. Der vorhandene voreingestellte Community-Name in Cisco WebEx Meetings Server 1.0, „CWS-Public“, wird nach dem Upgrade entfernt. Es werden lediglich vom Benutzer hinzugefügte SNMP v2 Community-Namen beibehalten.

Bekannte Probleme und Hinweise

Übersetzte Dokumentation

Eine übersetzte Dokumentation für diese Version von Cisco WebEx Meetings Server ist 4 bis 6 Wochen nach Veröffentlichung der englischsprachigen Version verfügbar.

Apple iOS 6.x und SSO

Es besteht ein bekanntes Problem mit Apple iOS 6.x. Single Sign-On (SSO, Einzelanmeldung) funktioniert für interne Benutzer mit iPad/iPhone nicht, die den Safari 6-Webbrowser verwenden. Ein Defekt bei Apple, der in iOS 7 behoben wurde, hat dieses Problem verursacht. Die Fehler-ID für Safari ist 13484525.

Beibehalten des Hostnamens bei Änderung der IP-Adresse Ihrer virtuellen Maschine

Ändern Sie nie die DNS-Einträge für die Hostnamen, die in Ihrer Bereitstellung konfiguriert sind. Sie können den Hostnamen einer virtuellen Maschine ändern, die Teil Ihrer Bereitstellung ist. Die entsprechende IP-Adresse wird automatisch vom DNS abgerufen. Wenn Sie die IP-Adresse einer virtuellen Maschine ändern und den gleichen Hostnamen beibehalten möchten, müssen Sie folgende Schritte durchführen:

- 1 Konfigurieren Sie einen temporären Hostnamen im DNS.
- 2 Ändern Sie den Hostnamen der virtuellen Maschine zum temporären Hostnamen, den Sie konfiguriert haben.
- 3 Verlassen Sie mit dem System den Wartungsmodus, damit der neue Hostname aktiviert wird.
Nach dieser Änderung ist Ihr ursprünglicher Hostname nicht mehr Teil der Bereitstellung.
- 4 Ändern Sie die IP-Adresse des ursprünglichen Hostnamens im DNS in die neue IP-Adresse um.
- 5 Ändern Sie den temporären Hostnamen der virtuellen Maschine zum ursprünglichen Hostnamen.
- 6 Verlassen Sie mit dem System den Wartungsmodus, damit der Hostname aktiviert wird.
Jetzt wird der ursprüngliche Hostname mit Ihrer neuen IP-Adresse konfiguriert.

Dashboard-Problem – Fehler beim Anzeigen bereits begonnener Meetings

In dieser Version von Cisco WebEx Meetings Server kann ein Fehler auftreten, bei dem auf dem Dashboard einige begonnene Meetings nicht angezeigt werden. Dieses Problem tritt unter folgenden Bedingungen auf:

Ein Meeting mit der Einstellung **Teilnehmern erlauben, der Telekonferenz vor dem Gastgeber beizutreten** wurde angesetzt. Ein Teilnehmer tritt dem Meeting per Telefon bei, nutzt aber nicht den Web-Teil. Das Dashboard sollte anzeigen, dass dieses Meeting bereits mit einem Teilnehmer begonnen hat, tut dies aber nicht. Dieses Problem kann dazu führen, dass Benutzer mehrere Meetings ansetzen, was zu Problemen mit der Leistung führen kann.

Audio-Konfiguration

Bitte beachten Sie, dass Sie mit G.711 in Ihren Audio-Konfigurations-Einstellungen eine bessere Sprachqualität erzielen als mit G.729. Beziehen Sie sich für weitere Informationen auf “Über die Konfiguration Ihrer Audio-Einstellungen” des *Cisco WebEx Meetings Server Administration Guide*.

IP Communicator 7.0.x-Endpunkte

IP Communicator 7.0.x-Endpunkte, die an CWMS-Meetings teilnehmen, können in einer Konferenz zu Audioqualitätsproblemen führen (Echo und andere Geräusche), falls eine der folgenden Bedingungen eintritt:

- Der IP Communicator wird nicht stummgeschaltet.
- Ein Teilnehmer, der IP Communicator verwendet, wird zum aktiven Sprecher.

Um dieses Problem zu vermeiden, nehmen Sie Feineinstellungen an der IP-Communicator-Umgebung vor (zum Beispiel Headset, Mikrofon und Lautsprecher), oder verwenden Sie ein anderes traditionelles Telefon.

Mit iOS-Geräten gestartete Meetings

Mit iOS-Geräten gestartete Meetings können nicht aufgezeichnet werden.

Einwahl- und Auswahl-Verbindungen zu einem In Bearbeitung-Meeting

Wenn ein Meeting aufgrund eines Failovers von einem Datenzentrum zu einem anderen wechselt, werden Einwahl- und Auswahl-Verbindungen mit diesem Meeting nicht automatisch neu verbunden. Zur Wiederherstellung der Verbindungen legen die Teilnehmer auf und wählen sich anschließend wieder manuell ein.

Dieses Problem tritt auf, wenn:

- Das installierte System ein großes MDC ist.
- Das Meeting gestartet wird, wenn eines der Datenzentren sich im Wartungsmodus befindet oder abgeschaltet ist.
- Wenn nach Beenden des Wartungsmodus oder Aktivierung des Datenzentrums ein anderes Datenzentrum abgeschaltet oder in den Wartungsmodus versetzt wird.

.mp4-Videodateiformat kann nicht in Windows geteilt werden

Bei Verwendung von QuickTime kann die folgende Meldung erscheinen: "Initialisierung von QuickTime fehlgeschlagen. Fehler Nr. -2093. Stellen Sie sicher, dass QuickTime auf diesem Computer einwandfrei installiert ist."

Diese Fehlermeldung kann anzeigen, dass die Datei QuickTime.qts fehlt, verschoben wurde oder unbrauchbar ist. Die Datei QuickTime.qts befindet sich im Verzeichnis \WINDOWS\SYSTEM. Um dieses Symptom zu beheben, entfernen Sie QuickTime vollständig und installieren Sie es neu.

- 1 Laden Sie die aktuellste Version des QuickTime Player <http://www.apple.com/quicktime/download/> herunter.
- 2 Deinstallieren Sie QuickTime über das Steuerfeld **Programme hinzufügen oder entfernen**. Stellen Sie sicher, dass Sie **Alles deinstallieren** auswählen.
- 3 Löschen Sie den Inhalt des Temp-Ordners, C:\WINDOWS\TEMP (falls vorhanden).
- 4 Installieren Sie QuickTime mithilfe der Version von QuickTime, die Sie heruntergeladen haben.
- 5 Starten Sie Windows neu.

Probleme

Verwenden des Programmfehler-Toolkits

Bekannte Probleme (Programmfehler) werden ihrem Schweregrad entsprechend eingestuft. Diese Software-Dokumentation enthält Beschreibungen zu folgenden Punkten:

- Ungelöste, von Kunden gefundene Programmfehler der Schwere 1–3
- Behobene, von Kunden gefundene Programmfehler der Schwere 1 bis 3
- Behobene, von Cisco gefundene bedeutende Programmfehler

Informationen zu den aufgelisteten Fehlern sowie eine Fehlersuche finden Sie im Cisco Programmfehler-Toolkit.

Bevor Sie beginnen

Um auf das Programmfehler-Toolkit zuzugreifen, benötigen Sie Folgendes:

- Internetverbindung
- Webbrowser
- Cisco.com Nutzerkennung und Kennwort

Schritt 1 Um auf das Programmfehlersuchtool zuzugreifen, gehen Sie zu <https://Tools.Cisco.com/bugsearch/Search>.

Schritt 2 Melden Sie sich mit Ihrer Cisco.com Nutzerkennung und Ihrem Kennwort an.

Schritt 3 Geben Sie die Fehler-ID in das Feld „Suche nach“ ein, und drücken Sie die Eingabetaste.

Tip Sie können auch direkt zu einem bestimmten Fehler wechseln, indem Sie <https://tools.cisco.com/bugsearch/bug/<BUGID>> eingeben, wobei <BUGID> für die ID des Fehlers steht, den Sie suchen (z. B. CSCab12345).

Nächster Schritt

Für weitere Informationen zur Suche nach Programmfehlern, zum Erstellen von gespeicherten Suchanfragen und Erstellen von Programmfehler-Gruppen wählen Sie **Hilfe** auf der **Programmfehler** Seite aus.

Behobene Probleme bei Cisco WebEx Meetings Server Version 2.8

Es gibt keine ungelösten Probleme bei Cisco WebEx Meetings Server Version 2.8 (Build 2.8.1.17).

Ungelöste Probleme bei Cisco WebEx Meetings Server Version 2.8

Es gibt keine ungelösten Probleme bei Cisco WebEx Meetings Server Version 2.8 (Build 2.8.1.17).

Behobene Probleme bei Cisco WebEx Meetings Server 2.8

In der folgenden Tabelle werden die Probleme aufgeführt, die in Cisco WebEx Meetings Server 2.7MR2 vorlagen und in dieser Version behoben wurden.

Tabelle 1: Behobene Probleme bei Cisco WebEx Meetings Server 2.8 (Build 2.8.1.17)

Bezeichnung	Schweregrad	Beschreibung
CSCvd28091	1	jdk/jre-Software muss zur Behebung verschiedener Sicherheitsschwachstellen aktualisiert werden
CSCvc84858	2	Audioprobleme, die durch das Fehlen adäquater Sicherheitsrichtlinien in SELinux verursacht werden
CSCvd03369	2	Meeting kann aufgrund einer Datenbankausnahme nicht beendet werden

Bezeichnung	Schweregrad	Beschreibung
CSCvd47160	2	Beitritt zu Meeting über Firefox 52.0 (32-Bit) ist nicht möglich
CSCve05932	2	Meeting kann nicht gestartet werden, wenn die Option „Verschlüsselung vertraulicher Informationen“ aktiviert ist
CSCvb67814	3	Neuer Stellvertreter kann einzelne Instanzen des wiederkehrenden Meetings eines früheren Stellvertreters nicht bearbeiten
CSCvb75607	3	Sicherheitskonfiguration für Benutzersitzung wirkt sich nicht auf Endbenutzerseite aus
CSCvb78854	3	Beitritt zum Audio-Teil mit veralteter Meeting-Nummer führt zu einer ungültigen Meeting-Nummer
CSCvb79074	3	Browser friert ein, wenn viele (mehr als 35 alternative Gastgeber) zum wiederkehrenden Meeting hinzugefügt werden
CSCvb96230	3	Delegierung für PCN-Meeting wird nicht gemäß der Dokumentation/Konstruktion ausgeführt
CSCvc01124	3	Aktualisierung von 2.6 auf 2.7 aufgrund von rsa-cryptoj-6.1.3.2-13.x86_64 RPM fehlgeschlagen
CSCvc03322	3	Im benutzerdefinierten Teilnehmerbericht wird angezeigt, dass sich Benutzer mit der ersten Zugangsnummer einwählen, was falsch ist
CSCvc03356	3	Berichtsspeicher für Speicher- und Portprüfungen ist nicht über IRP erreichbar
CSCvc14829	3	Beitritt zu Meetings über Edge-Browser mit einem temporären Client schlägt aufgrund eines langen Dateinamens für den temporären Client fehl
CSCvc31861	3	Nach Installation des Meeting-Clients über MSI werden nach dem ersten Start weiterhin neue Dateien erstellt
CSCvc31886	3	Übereinstimmungsfehler bei Datenbank von 2.6 auf 2.7, weil bei Verwendung der Funktion für den Sitzungstyp die Konfiguration unverändert bleibt
CSCvc44204	3	db_set_cron_timing.sh führt zu langsamem Neustart
CSCvc46118	3	Option „Jeder darf im Meeting präsentieren“ funktioniert nach Aktivierung nicht ordnungsgemäß
CSCvc46151	3	Dashboard-Aktualisierungen werden unterbrochen; offenbar bestehen Lücken zwischen den Zeiträumen, wenn keine Aktualisierungen stattfinden
CSCvc47765	3	Erhöhung des HSTS-Timers für max. Alter
CSCvc78296	3	CWMS PT-Meeting wird in Outlook in der Add-In-Liste verlangsamt bzw. in verminderter Leistung angezeigt

Bezeichnung	Schweregrad	Beschreibung
CSCvc94595	3	Beurteilung von Orion für OpenSSL Januar 2017
CSCvc96137	3	In Outlook werden Meetings, die ein CWMS-Meeting und eine hohe Anzahl von Teilnehmern enthalten, verlangsamt geöffnet
CSCvc96249	3	IE 11 auf Windows 10 kann Aufzeichnungen nicht ordnungsgemäß streamen
CSCvc97876	3	CWMS sollte nach einem Wechsel des Speicherservers neu starten, wenn es aus dem Wartungsmodus geschaltet wird
CSCvc98147	3	CWMS-Aktualisierung schlägt fehl, wenn SELinux deaktiviert ist
CSCvd20436	3	Datenbankfehler: Bitte stellen Sie den virtuellen Computer erneut bereit
CSCvd20975	3	Beitritt zu WebEx Meeting als Gast über Edge-Browser und temporärem Meeting-Client nicht möglich
CSCvd41260	3	Vorheriger alternativer Gastgeber, der über die Webseite mithilfe der Option „Nur speichern“ vom Meeting entfernt wurde, empfängt weiterhin Erinnerungen

Weiterführende Informationen und Serviceanfragen

Näheres zum Einreichen einer Serviceanfrage und weiterführende Informationen erhalten Sie unter <http://www.cisco.com/c/en/us/support/index.html>.

Sie können außerdem Cisco Security RSS-Feeds abonnieren und Benachrichtigungen erhalten, wenn neue Informationen verfügbar sind. Inhalts-Feeds sind sowohl für Version 1.0 als auch 2.0 des RSS-Formats verfügbar. Besuchen Sie <http://tools.cisco.com/security/center/rss.x?i=44>.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT 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. All rights reserved. Copyright © 1981, Regents of the University of California.

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.

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: <http://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)

© 2017 Cisco Systems, Inc. All rights reserved.