

Versionshinweise für Cisco Webex Meetings Server Version 4.0

Erste Veröffentlichung: 29 April 2019

Letzte Änderung: 29 April 2019

Software-Dokumentation für Cisco Webex Meetings Server

Diese Software-Dokumentation enthält Informationen zu neuen Funktionen, Anforderungen, Einschränkungen und Probleme für alle Versionen von Cisco Webex Meetings Server 4.0. 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 Software-Dokumentation vor der Bereitstellung von Cisco Webex Meetings Server durchzusehen, um Informationen zu Problemen, die Ihr System betreffen könnten, zu erhalten.

Neue Kunden können Cisco Webex Meetings Server direkt von Cisco Systems, Inc. oder von einem Vertriebsmitarbeiter eines Partners erwerben.

Bestehende Kunden können die OVA-Datei für die Version 4.0 unter Verwendung des Produktaktualisierungstool (PUT) abrufen: <http://upgrad.cloudapps.cisco.com/upgrad/jsp/index.jsp>

Die neuesten Softwareaktualisierungen für dieses Produkt stehen hier zum Download bereit: <http://software.cisco.com/download>.

Produkte **auswählen** > **Konferenzen** > **Webkonferenzen** > **Webex Meetings Server** > **Webex Meetings Server 4.0**.

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>.

Neuheiten bei Cisco Webex Meetings Server Version 4.0

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

Die vollständige Liste der Systemanforderungen finden Sie *im Planungsleitfaden und in den Systemanforderungen für die Cisco Webex Meetings Server Version 4.0*. Besuchen Sie http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

64-Bit-Anwendungsunterstützung für Mac

Apple hat das Ende der Unterstützung für 32-Bit-Anwendungen angekündigt. MacOS High Sierra ist die letzte MacOS-Version für die Unterstützung der 32-Bit-Architektur. Die Webex Meetings-Desktop-Anwendung ist eine 64-Bit-Anwendung.

Avatar-Unterstützung für Mobilgeräte

Mobile Benutzer können Avatare (Bilder) auf die Site hochladen, um sie in der Webex Meetings-Desktop-Anwendung und in ihrer mobilen App zu verwenden.

Bilddateien müssen die folgenden Anforderungen erfüllen:

- Unterstützte Dateiformate: PNG, JPG, JPEG und GIF
Animierte GIF-Dateien werden unterstützt, aber das System wandelt sie in statische Bilder um und verwendet das erste Bild als Avatarbild.
- Minimale Bildabmessungen: 160 x 160 Pixel
- Maximale Bildgröße: 5 MB

Diese Funktion erfordert, dass Sie den Remote-Speicher installiert haben. Das System speichert Avatare auf dem Admin-Server unter `/db/archive/avatars/`.



Hinweis

Bei Systemen mit mehreren Rechenzentren werden die Avatare von einem Rechenzentrum in das andere repliziert.

Browser-Unterstützung

Diese Version unterstützt die folgenden Browser-Versionen:

Windows:

- Google Chrome: 65, 66, 67, 68, 69, 70, 71, 72, 73 und 74
- Microsoft Edge (nur Windows 10): 42.17134.1.0 und 44.17763.1.0
- Microsoft Internet Explorer (IE): 11
- Mozilla Firefox: 59, 60, 61, 62, 63, 64, 65 und 66

Mac:

- Apple Safari: 12.0.1 (14606.2.104.1.1) und 12.1
- Google Chrome: 65, 66, 67, 68, 69, 70, 71, 72, 73 und 74
- Mozilla Firefox: 59, 60, 61, 62, 63, 64, 65 und 66

Cisco Jabber-Unterstützung

Diese Version unterstützt Cisco Jabber Version 12.1.0, 12.1.1, 12.5.0 und 12.6.0.

Anrufer-ID anzeigen

Sie können die Anzeige der Anrufer-ID im Teilnehmerbereich für Einwahlbenutzer aktivieren oder deaktivieren. Um diese Funktion zu aktivieren oder zu deaktivieren, melden Sie sich bei der Webex-Administration an und gehen Sie zu **Einstellungen > Meetings > Meeting-Einstellungen**. Standardmäßig ist diese Funktion deaktiviert.

Wenn die Funktion deaktiviert ist, wird die ID für einen Einwahlbenutzer angezeigt als: Einwahlbenutzer_Nr. Beispiele:

- Einwahlbenutzer_1
- Einwahlbenutzer_2
- Einwahlbenutzer_3

Wenn die Funktion aktiviert ist, wird die ID für einen Einwahlbenutzer angezeigt als: Einwahlbenutzer_Nr. (<caller ID>). Beispiele:

- Einwahlbenutzer_1 (Giacomo Edwards +865516611****)
- Einwahlbenutzer_2 (drahtloser Anrufer +1650400****)
- Einwahlbenutzer_3 (Marc Brown +1917929****)



Hinweis

Aus Datenschutzgründen sind die letzten vier Ziffern durch Sternchen ersetzt. Das Display unterstützt bis zu 63 Zeichen.

Erweiterte Kapazität für Multi-Datenzentren

Cisco Webex Meetings Server unterstützt ein voll funktionsfähiges 4000-Port-System für die folgenden Szenarien:

- Ein Rechenzentrum mit hoher Verfügbarkeit (High Availability – HA) mit VMware V-Center 6.5
- Multi-Datenzentrum (MDC) – Dual Data Center (DDC) mit VMware V-Center 6.5

Sowohl die erweiterte Kapazität als auch die MDC-Funktionen sind für Version 3.0 verfügbar, werden jedoch nicht gemeinsam unterstützt. Diese Version unterstützt zusätzlich zwei großflächige (4000-Port-) Systeme, die zur Erstellung eines MDC zusammengeführt wurden. Wenn Sie bereits über ein großes MDC-System verfügen, können Sie beide Systeme erweitern, um ein besonders großes MDC-System zu erstellen.

Die Funktion für erweiterte Kapazität erfordert für jedes System eine Lizenz. Die Lizenz für erweiterte Kapazität ist nur für große (2000-Port-) Systeme verfügbar.

Mac OS-Unterstützung

Diese Version unterstützt die folgenden macOS-Versionen:

- Sierra 10.12.6
- High Sierra 10.13.6
- Mojave 10.14.1
- Mojave 10.14.2

- Mojave 10.14.3
- Mojave 10.14.4

Moderne Ansicht

Wenn sich Benutzer auf der Webex-Site anmelden, können sie zwischen der klassischen und der modernen Ansicht wählen. In der modernen Ansicht können sie direkt über ein neues Dashboard auf die am häufigsten verwendeten Site-Steuerungen zugreifen. Die Benutzer können problemlos Meetings in persönlichen Räumen starten, an bevorstehenden Meetings teilnehmen und neue Meetings ansetzen.

In der modernen Ansicht ist das Dashboard die Startseite. Die Benutzer können jederzeit zu ihr zurückkehren, indem sie in der linken Navigationsleiste auf klicken. Die moderne Ansicht wird standardmäßig angezeigt, Sie können jedoch die Standardeinstellung für Ihre Webex-Site ändern.

Persönliche Meetingräume

Persönliche Webex-Räume sind virtuelle Konferenzräume, die immer verfügbar sind. Die URL des persönlichen Raums und die Einwahlnummern bleiben unverändert. Benutzer können ihre eigenen Präferenzen für ihre persönlichen Räume festlegen, Instant-Meetings starten und die Links für ein Meeting sofort freigeben.

Smart-Lizenzierung

Bei dieser Version wird die Smart-Software-Lizenzierung eingeführt, die alle Aspekte der Lizenzverwaltung erheblich vereinfacht. Weitere Informationen zu den Vorteilen der Smart-Software-Lizenzierung finden Sie in den folgenden Ressourcen:

HÄUFIG GESTELLTE FRAGEN: <https://www.cisco.com/c/dam/en/us/products/collateral/software/smart-accounts/q-and-a-c67-741561.pdf>

Informationen auf einen Blick: <https://www.cisco.com/c/dam/en/us/products/collateral/ssl-aag.pdf>

„Verwalten von Lizenzen“ im *Administrationsleitfaden für Cisco Webex Meetings Server*:

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

Webex Meetings-Desktop-Anwendung

Die Webex Meetings-Desktop-Anwendung ersetzt die Webex Meeting-Anwendung und die Produktivitätswerkzeuge. Die Webex Meetings-Desktop-Anwendung bietet neue Videofunktionen und Unterstützung für persönliche Meeting-Räume.

Cisco Webex Meetings Server unterstützt die Webex Meetings-Desktop-Anwendungsversion 39.3.0.582 für Windows und Mac.



Achtung

Ansetzen und Bearbeiten von Meetings über Microsoft Outlook für Mac wird nicht unterstützt. Um dieses Problem zu umgehen, können Benutzer Meetings über ihre Webex-Site ansetzen, bearbeiten und starten.

Tabelle 1: Videofunktionen der Webex Meetings Desktop-Anwendung

Funktion	Beschreibung
Video- Miniaturbilder	Videobasierte Teilnehmerliste mit Video- Miniaturbildern.

Funktion	Beschreibung
Video-Selbstansicht in geteilter Vollbildansicht	Sehen Sie Selbstansicht- Videos in der Hauptvideoansicht an, wenn Sie in der Vollbildansicht teilen. Vom Selbstansicht- Videofenster die Sendung von Videos starten oder stoppen.
Hohe Auflösung bis zu 720p	Videos können mit einer hohen Auflösung von bis zu 720p (1280x720) angezeigt werden.
Sperren von Video	Der Moderator kann entscheiden, wessen Video allen Meeting-Teilnehmern angezeigt wird.
HD-Video-decodierte Abladung auf GPU	Unterstützte GPU-Chipsätze können die Host-CPU von dem bei der Decodierung anfallenden Verarbeitungs- aufwand entlasten.
Video-Vollbildansicht	Video- Vollbildansicht mit HD- oder HQ-Videoanzeige (je nach Monitorgröße) und fünf Video- Miniaturbildern.
Erweiterte Video- Vollbildansicht	Erweitern Sie das Video des aktiven Sprechers auf den gesamten Bildschirm, und empfangen Sie gleichzeitig HD-Video.
Kamerawechsel bei laufendem Meeting	Teilnehmer können während eines laufenden Meetings Webcams anschließen und zwischen ihnen wechseln.
Automatische Videoanpassung	Automatische Konfiguration der Videoqualität der Teilnehmer, gemäß der verfügbaren Netzwerk- bandbreite.
Video-Wiedergabe des aktiven Sprechers in geteilter Vollbildansicht	Unverankerte Video-Wiedergabe des aktiven Sprechers, wenn die Vollbildansicht geteilt wird.
Wechsel zum aktiven Sprecher	Automatischer Videowechsel zum am besten hörbaren aktiven Sprecher

Aktualisierungen der Webex Meetings-Desktop-Anwendung können in Form von Patches, Wartungsversionen und Hotfixes bereitgestellt werden.



Achtung

Wenn Ihre Benutzer auch eine Verbindung mit Cloud-basierten Webex-Sites herstellen, können Sie die Webex Meetings-Desktop-Anwendung von diesen Sites aktualisieren. Die aktualisierte Version funktioniert mit Cisco Webex Meetings Server. Die Site, mit der der Benutzer eine Verbindung herstellt, bestimmt den verfügbaren Funktionsumfang.

Webex Netzwerkaufzeichnungs-Player

Diese Version unterstützt die folgenden Versionen des Cisco Netzwerkaufzeichnungs-Players:

- **Windows:** 39.3.0.582
- **Mac:** 39.3.0.582

Unterstützte Upgrade-Pfade

Diese Version von Cisco Webex Meetings Server unterstützt Upgrades von Version 1.5 bis 3.0. 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 3.0 MR durchzuführen, müssen Sie ein *Upgrade* von Version 1.5 MR5 auf Version 3.0 und anschließend eine *Aktualisierung* auf Version 3.0 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 auf **Neu starten**, wenn die Aktualisierung des anderen Zentrums abgeschlossen ist und beide die Schaltfläche **Neu starten** anzeigen.

Verwenden Sie die folgende Tabelle, um Ihren Upgrade-Pfad für Cisco Webex Meetings Server 4.0 zu bestimmen.

Installierte Version	Pfad zu Version 4.0
1.5 auf 1.5MR4	<ol style="list-style-type: none"> 1. Aktualisierung auf Version 1.5MR5 2. Aktualisierung auf Version 1.5MR5 Patch 2 oder höher 3. Upgrade auf Version 2.8. 4. Aktualisierung auf Version 2.8MR1 5. Aktualisierung auf Version 2.8MR1 Patch 2 oder höher 6. Upgrade auf Version 4.0
1.5 MR5	<ol style="list-style-type: none"> 1. Aktualisierung auf Version 1.5MR5 Patch 2 oder höher 2. Upgrade auf Version 2.8. 3. Aktualisierung auf Version 2.8MR1 4. Aktualisierung auf Version 2.8MR1 Patch 2 oder höher 5. Upgrade auf Version 4.0

Installierte Version	Pfad zu Version 4.0
Version 1.5 MR5 Patch 2 oder höher	<ol style="list-style-type: none"> 1. Upgrade auf Version 2.8. 2. Aktualisierung auf Version 2.8MR1 3. Aktualisierung auf Version 2.8MR1 Patch 2 oder höher 4. Upgrade auf Version 4.0
2.0 auf 2.0MR8	<ol style="list-style-type: none"> 1. Aktualisierung auf 2.0MR9. 2. Aktualisierung auf Version 2.8. 3. Aktualisierung auf Version 2.8MR1 4. Aktualisierung auf Version 2.8MR1 Patch 2 oder höher 5. Upgrade auf Version 4.0
2.0MR9 oder höher	<ol style="list-style-type: none"> 1. Aktualisierung auf Version 2.8. 2. Aktualisierung auf Version 2.8MR1 3. Aktualisierung auf Version 2.8MR1 Patch 2 oder höher 4. Upgrade auf Version 4.0
2.0 auf 2.0MR8	<ol style="list-style-type: none"> 1. Aktualisierung auf Version 2.0MR9 2. Aktualisierung auf Version 2.8. 3. Aktualisierung auf Version 2.8MR1 4. Aktualisierung auf Version 2.8MR1 Patch 2 oder höher 5. Upgrade auf Version 4.0
Version 2.5MR6 oder höher	<ol style="list-style-type: none"> 1. Aktualisierung auf Version 2.8. 2. Aktualisierung auf Version 2.8MR1 3. Aktualisierung auf Version 2.8MR1 Patch 2 oder höher 4. Upgrade auf Version 4.0
2.6 auf Version 2.6MR2	<ol style="list-style-type: none"> 1. Aktualisierung auf Version 2.6MR3 2. Aktualisierung auf Version 2.8 3. Aktualisierung auf Version 2.8MR1 4. Aktualisierung auf Version 2.8MR1 Patch 2 oder höher 5. Upgrade auf Version 4.0

Installierte Version	Pfad zu Version 4.0
2.6MR3 oder höher	<ol style="list-style-type: none"> 1. Aktualisierung auf Version 2.8 2. Aktualisierung auf Version 2.8MR1 3. Aktualisierung auf Version 2.8MR1 Patch 2 oder höher 4. Upgrade auf Version 4.0
2.7 oder alle 2.7MR-Versionen	<ol style="list-style-type: none"> 1. Aktualisierung auf Version 2.8 2. Aktualisierung auf Version 2.8MR1 3. Aktualisierung auf Version 2.8MR1 Patch 2 oder höher 4. Upgrade auf Version 4.0
2.8	<ol style="list-style-type: none"> 1. Aktualisierung auf Version 2.8MR1 2. Aktualisierung auf Version 2.8MR1 Patch 2 oder höher 3. Upgrade auf Version 4.0
Version 2.8MR1 Patch 2 oder höher	Upgrade auf Version 4.0
Version 3.0 oder alle 3.0MR-Versionen	Aktualisierung auf Version 4.0

**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:

- *Administratorhandbuch für Cisco Webex Meetings Server Version 4.0*: http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html
- *Planungsleitfaden und Systemanforderungen für Cisco Webex Meetings Server 4.0*: <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.

Weitere Informationen finden Sie im *Cisco Webex Meetings Server-Administrationsleitfaden* für Ihre Version:

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

Einschränkungen und Vorbehalte

Nur-Audio-Meetings

Unter den folgenden Umständen kann ein Meeting länger als die maximale Meeting-Dauer von 24 Stunden dauern:

- Alle Teilnehmer eines regulären Webex-Meetings können sich einwählen (nur Audio).
- Kein Teilnehmer startet den Web-Teil des Meetings.

In diesem Fall wird das Meeting fortgesetzt, solange ein Teilnehmer in der Konferenz bleibt. Wenn alle Einwahl-Teilnehmer die Verbindung zur Konferenz trennen, endet das Meeting innerhalb von 24 Stunden nach der Startzeit. Das Meeting endet sofort, wenn das Meeting über die angesetzte Endzeit gelaufen ist.



Hinweis

Dieses Szenario gilt nur für reguläre Webex-Meetings, denen nur Einwahl-Teilnehmer beigetreten sind. Dieses Szenario gilt nicht für Meetings mit persönlicher Konferenznummer (PCN) oder für reguläre Webex-Meetings, denen Webteilnehmer beigetreten sind.

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.

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.

Wenn Sie einen Speicherserver konfigurieren und den **Datensatz** unter **Administrations-Dashboard aktivieren**, > **Einstellungen** > **Meetings** > **Teilnehmerprivilegien** ist die Einstellung **Datensatz** eine systemweite Einstellung. Es gibt keine individuellen Meeting-Einstellungen oder -Präferenzen für Aufzeichnungen. Darüber hinaus können Sie die Aufzeichnung nach Sitzungstypen aktivieren oder deaktivieren, die Sie den Benutzern zuweisen.

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“ dem 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.

Wenn Sie vorhaben, die Zuordnung des Feldes „NameID“ von E-Mail auf ein anderes Feld (z. B. EmployeeNumber) zu ändern, müssen sich die Benutzer auf die Änderung vorbereiten. Nachdem Sie die Felder „NameID“ in AD aktualisiert haben, müssen sich die Benutzer bei CWSM anmelden, bevor Sie die E-Mail-Adressen ändern. Wenn sich der Name und die E-Mail-Adresse ändern, stimmt sonst kein Attribut mit dem CWMS-Profil überein. In diesem Szenario verliert das bestehende Profil die Fähigkeit, sich beim System anzumelden, und das System erstellt ein neues Profil.

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.

Durch eine manuelle Synchronisierung der Systeme wird das Problem nicht gelöst. 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 14.

Browser Microsoft Edge

Der Microsoft Edge-Browser unterstützt die Wiedergabe von Webex-Aufzeichnungen nicht.

Unterstützung von vCenter 6.5

Wenn Sie die Datei CWMS OVA auf vCenter 6.5 bereitstellen, gelten die folgenden Einschränkungen:

- Aufgrund von Browser-Einschränkungen und der Größe der Datei CWMS OVA von 16 GB müssen Sie die OVA-Datei unter Verwendung der URL und nicht des lokalen Datei-Uploads bereitstellen.
- Wählen Sie den auf vCenter FLASH basierenden Client aus. Diese Auswahl ist erforderlich, um die vApp-Eigenschaften für die VM-Konfiguration erfolgreich einzugeben: Hostname, Domäne, IP-Adresse, Subnetz und DNS-Konfiguration.

Virtual Desktop-Infrastruktur

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

- Citrix Virtual-Anwendungen und -Desktops 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.

Webex Meetings-Desktop-Anwendung

Die Webex Meetings-Desktop-Anwendung verfügt über die folgenden Einschränkungen. Benutzer können die folgenden Aktionen nicht durchführen:

- Ansetzen eines Jahresmeetings.
- Teilnahme an einem Meeting über eine Video-Adresse.
- Ansetzen von oder Teilnahme an Meetings in einem persönlichen Raum über die Webex Meetings-Desktop-Anwendung.
- Ansetzen von Meetings in einem persönlichen Raum über Microsoft Outlook.
- Verbindung mit und Teilnahme an Meetings über Videogeräte.
- Verbindung mit und Freigabe an Cloud-registrierte Videogeräte.
- Verbindung mit und Freigabe an Share-Geräte.
- Erhalt eines Rückrufs an ein Videogerät während eines Meetings (Mein Videosystem anrufen).
- Start oder Teilnahme an einem Meeting über Microsoft Word, PowerPoint oder Excel.



Achtung

Ansetzen und Bearbeiten von Meetings über Microsoft Outlook für Mac wird nicht unterstützt. Um dieses Problem zu umgehen, können Benutzer Meetings über ihre Webex-Site ansetzen, bearbeiten und starten.

Hinweise zur Aktualisierung

Die Webex Meetings-Desktop-Anwendung ist nicht mit früheren Versionen von Cisco Webex Meetings Server abwärts kompatibel.

Nachdem Sie Ihr System auf CWMS 4.0 aktualisiert haben, können Sie wählen, ob Sie die Anwendung an die Endbenutzer weitergeben möchten oder ob diese sie selbst herunterladen dürfen.

Wenn Sie die Webex Meetings-Desktop-Anwendung an Benutzer weitergeben, müssen diese sich mit ihren vorhandenen Anmeldeinformationen bei der Anwendung anmelden. Dies gilt auch dann, wenn sie zuvor die Optionen „Anmeldeinformationen speichern“ und „Automatisch anmelden“ für Webex-Produktivitätswerkzeuge ausgewählt haben.

Wenn Sie Benutzern das Herunterladen und Installieren der Anwendung erlauben, müssen Benutzer von Microsoft Windows zuerst die Webex-Produktivitätswerkzeuge deinstallieren.

Wenn diese Option zulässig ist, haben einige Benutzer die Wahlmöglichkeit, die Webex-Produktivitätswerkzeuge weiterhin zu verwenden. Diese Benutzer sind nicht in der Lage, Instant-Meetings durch Klicken auf die Schaltfläche **Meeting starten** zu starten. Ein Hotfix ist verfügbar, um dieses Problem zu beheben.

Wichtige Hinweise

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 5.5, 6.0 oder 6.5 zur 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.
- Weitere Informationen zu den Hypervisor-Anforderungen finden Sie im *Planungsleitfaden und in den Systemanforderungen für Cisco Webex Meetings Server* unter http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

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 „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)

TLS-Unterstützung

Diese Version unterstützt TLS 1.1 und höher; TLS 1.0 wird nicht unterstützt, mit einer Ausnahme. Client-Verbindungen von Cisco Webex Meetings Server (CWMS) zu einem SMTP-Server mit TLS 1.0 werden unterstützt.

Diese Version unterstützt Cisco Unified Call Manager (CUCM) 8.6 oder 9.0 ohne TLS/SRTP sowie CUCM 9.1, 10.0, 10.5, 11.0 (1a), 11.5 (1) SU1, 11.5 (1) SU3 und 12.0 für sichere Telekonferenzen.

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:

- Lastname
- Firstname
- 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 sich VMware-Schnappschüsse in Ihrem vorhandenen System (vor der Erweiterung) befinden, entfernen Sie diese, bevor Sie mit der Erweiterung beginnen.

Für die Systemerweiterung ist die Festplatte des virtuellen Computers (VMDK) vom ursprünglichen System zum Zielsystem (erweitert) erforderlich. Wenn Sie Schnappschüsse auf dem ursprünglichen System belassen und dem Zielsystem zuordnen, wird das Zielsystem aufgrund von Inkonsistenzen der Schnappschüsse nicht eingeschaltet.

SNMP v2 Community-Namen

Es gibt keine voreingestellte Namenseingabe für die SNMP v2 Community in Cisco Webex Meetings Server. 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.

Übersetzte Dokumentation

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

Bekannte Probleme und Hinweise

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.

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“ im *Cisco Webex Meetings Server-Administrationsleitfaden*.

.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 Players <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.

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.

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.
- nach Beenden des Wartungsmodus oder Aktivierung des Datenzentrums ein anderes Datenzentrum abgeschaltet oder in den Wartungsmodus versetzt wird.

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.

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.

Aktualisierung von 3.0 Patch 1 schlägt fehl.

Die Aktualisierung von Version 3.0 Patch 1 (3.0.1.33) schlägt fehl, da in der Datei cwms.pub fehlerhafte Daten vorhanden sind. Umgehen Sie das Problem vor der Aktualisierung von 3.0 Patch 1 folgendermaßen:

1. Wechseln Sie zu <https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvj70890>.
2. Laden Sie die angehängte Datei herunter: `fix_update.zip` und kopieren Sie sie in das Verzeichnis `/archive` auf der primären Admin-VM.
3. Verwenden Sie SSH, um sich mit der primären Admin-VM zu verbinden, und navigieren Sie zum Verzeichnis `/archive`.
4. Entpacken Sie die Datei: `fix_update.zip`.

5. Machen Sie die entpackte Datei ausführbar: **chmod +x fix_update**.
6. Führen Sie die ausführbare Datei aus: **./fix_update**.
7. Nachdem die Erfolgsmeldung angezeigt wurde, fahren Sie mit der Aktualisierung fort.

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.

Vorbereitungen

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

- Internetverbindung
- Webbrowser
- Cisco.com Nutzerkennung und Kennwort

Prozedur

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**.

Tipp Sie können auch direkt zu einem bestimmten Programmfehler wechseln, indem Sie <https://tools.cisco.com/bugsearch/bug/<BUGID>> eingeben, wobei <BUGID> für die ID des von Ihnen gesuchten Programmfehlers steht (z. B. CSCab12345).

Nächste Maßnahme

Weitere Informationen zur Suche nach Programmfehlern, zum Erstellen von gespeicherten Suchanfragen und Erstellen von Programmfehler-Gruppen finden Sie unter **Hilfe** auf der Seite **Programmfehler-Toolkit**.

Behobene Probleme bei Cisco Webex Meetings Server 4.0

Die folgende Tabelle enthält Probleme (Bugs), die in dieser Version behoben wurden.

Tabelle 2: Behobene Probleme bei Cisco Webex Meetings Server 4.0 (Build 4.0.1.19)

Einschränkungs-ID	Schweregrad	Überschrift
CSCvp08700	3	Win: Alter PT kann Meetings, die von der neuen Webex-Anwendung angesetzt wurden, nicht aktualisieren/löschen.
CSCvm99626	4	Zwischenzertifikat verloren nach Aktualisierung auf 2.8 MR2 oder 3.0 MR2

Ungelöste Probleme bei Cisco Webex Meetings Server 4.0

Die folgende Tabelle enthält Probleme (Bugs), die in dieser Version noch nicht gelöst wurden.

Tabelle 3: Ungelöste Probleme bei Cisco Webex Meetings Server 4.0 (Build 4.0.1.19)

Einschränkungs-ID	Schweregrad	Überschrift
CSCvp34644	2	T39-Meeting-Absturz bei der Freigabe
CSCvp30778	3	Desktop-App konnte das Webex-Meeting nicht ohne Fehlermeldung starten
CSCvo98359	3	Alter PT: Starten des Instant-Meetings über den alten PT ist bei der Anmeldung bei der 4.0-Site fehlgeschlagen.
CSCvp32096	3	Teilnehmer kann die E-Mail „Aufzeichnung bereit“ nicht empfangen

Behobene Probleme bei Cisco Webex Meetings Server 4.0

In der folgenden Tabelle werden die in einer früheren Version ungelösten Probleme (Bugs) aufgeführt und für diese Version geschlossen.

Tabelle 4: Behobene Probleme bei Cisco Webex Meetings Server 4.0 (Build 4.0.1.19)

Einschränkungs-ID	Schweregrad	Überschrift
CSCvj02258	3	Automatisches Upgrade auf 3.0 über das System mit HA schlägt fehl
CSCvn47005	3	Die Wochenende-Tage im Kalender sind falsch
CSCvn67024	3	Anmeldung bei PT nicht möglich, wenn CUCM Publisher ausgefallen ist und die Verzeichnisintegration zu CUCM Sub wechselt
CSCvp16492	3	Wenn ein Anruf vom SRTP-Endpunkt an den RTP-Endpunkt übergeben wird, ist kein Audio vorhanden.
CSCvo56983	3	Benutzer werden nicht im Suchfeld von der Admin-Seite oder vom Feld "Teilnehmer" aus der Web-Meeting-Einrichtung aufgefüllt.
CSCvp03915	3	Das SNMP-USM-Benutzerpasswort darf kein „\$“-Zeichen enthalten.
CSCvn77979	4	Die Option „Alle Benutzer zwingen, das Passwort alle XX Tag(e) zu ändern“ betrifft auch LDAP-Benutzer.
CSCvo51406	4	Call-Me-Nummern werden nicht im Edge-Browser angezeigt.

Einschränkungs-ID	Schweregrad	Überschrift
CSCvo12211	4	Die Anzahl der Teilnehmer im Meeting-Suchergebnis zeigt nicht die genauen Werte an.

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>.

DIE SPEZIFIKATIONEN UND INFORMATIONEN ZU DEN PRODUKTEN IN DIESEM HANDBUCH KÖNNEN OHNE VORHERIGE ANKÜNDIGUNG GEÄNDERT WERDEN. ALLE ANWEISUNGEN, INFORMATIONEN UND EMPFEHLUNGEN IN DIESEM HANDBUCH WERDEN ALS RICHTIG ANGENOMMEN, WERDEN JEDOCH OHNE JEDLICHE WIE AUCH IMMER GEARTETE, AUSDRÜCKLICHE ODER STILLSCHWEIGENDE, GARANTIE ABGEGEBEN. DIE BENUTZER TRAGEN DIE VOLLSTÄNDIGE VERANTWORTUNG FÜR IHRE ANWENDUNG VON PRODUKTEN.

DIE SOFTWARELIZENZ UND EINGESCHRÄNKTE GARANTIE FÜR DAS BEGLEITENDE PRODUKT WERDEN IM INFORMATIONSPAKET, DAS IM LIEFERUMFANG DIESES PRODUKTS ENTHALTEN IST, DARGELEGT UND GELTEN HIERMIT ALS BESTANDTEIL DIESER VEREINBARUNG. WENN SIE DIE SOFTWARELIZENZ ODER BESCHRÄNKTE GARANTIE NICHT FINDEN KÖNNEN, WENDEN SIE SICH AN EINEN VERTRETER VON CISCO, UM EINE KOPIE ZU ERHALTEN.

Die Cisco Implementierung der TCP-Headerkomprimierung ist eine Adaption eines Programms, das an der University of California, Berkeley (UCB), als Teil der Public-Domain-Version der UCB für das UNIX-Betriebssystem entwickelt wurde. Alle Rechte vorbehalten. Copyright © 1981 Verwaltungsrat der University of California.

UNGEACHTET JEDLICHER ANDERER HIERIN ENTHALTENEN GARANTIEBESTIMMUNG WERDEN ALLE DOKUMENTDATEIEN UND DIE SOFTWARE DIESER LIEFERANTEN, „WIE BESEHEN“ UND OHNE GARANTIE AUF FEHLERFREIHEIT ZUR VERFÜGUNG GESTELLT. CISCO UND ALLE ZUVOR GENANNTE LIEFERANTEN ÜBERNEHMEN KEINERLEI, AUSDRÜCKLICHE ODER STILLSCHWEIGENDE, GARANTIEN, EINSCHLIEBLICH UND OHNE EINSCHRÄNKUNG, DIEJENIGEN DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG ODER DIEJENIGEN, DIE AUS DEM VERLAUF DES HANDELNS, DER VERWENDUNG ODER DES HANDELSBRAUCHS ENTSTEHEN.

IN KEINEM FALL SIND CISCO ODER SEINE LIEFERANTEN HAFTBAR FÜR INDIREKTE, SPEZIELLE SCHÄDEN, FOLGESCHÄDEN ODER NEBENSCHÄDEN JEDLICHER ART, EINSCHLIEBLICH UND OHNE EINSCHRÄNKUNG, SCHÄDEN AUS ENTGANGENEM GEWINN ODER DATENVERLUST AUFGRUND DER VERWENDUNG ODER NICHT UNFÄHIGKEIT DER VERWENDUNG DIESES HANDBUCHS. DIES GILT AUCH FÜR DEN FALL, DASS CISCO ODER SEINE LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN AUFMERKSAM GEMACHT WURDEN.

Sämtliche in diesem Dokument verwendeten IP-Adressen und Telefonnummern sind als Beispiele zu verstehen und beziehen sich nicht auf tatsächlich existierende Adressen und Telefonnummern. Die in diesem Dokument enthaltenen Beispiele, Befehlsanzeigeausgaben, Netzwerktopologie-Diagramme und anderen Abbildungen dienen lediglich zur Veranschaulichung. Die Verwendung tatsächlicher IP-Adressen oder Telefonnummern in diesem Zusammenhang ist zufällig und nicht beabsichtigt.

Für gedruckte und kopierte digitale Versionen dieses Dokuments besteht keine Gewährleistung. Die aktuelle Online-Version enthält die neueste Version.

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen und Telefonnummern 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 Vereinigten Staaten und anderen Ländern. Eine Liste der Marken von Cisco finden Sie auf folgender Website: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Die genannten Handelsmarken von Drittanbietern sind Eigentum der jeweiligen Inhaber. Die Verwendung des Worts "Partner" deutet keine Handelsbeziehung zwischen Cisco und anderen Unternehmen an. (1721R)

© 2019 Cisco Systems, Inc. Alle Rechte vorbehalten.