Installieren des IP Office Cloud Operations Manager

Version 11.0
Ausgabe 4
März 2018

Inhalt

Kapitel 1: Installation

Installation

Cloud Operations Manager ist eine Anwendung für die Remote-Unterstützung mehrerer Server Edition- und IP Office Select-Kundennetzwerke.

Cloud Operations Manager erfordert einen separaten CentOS 6.9-Server. Eine Ausführung der Anwendung auf einem bestehenden Server Edition-, IP Office Select- oder IP Office-Anwendungsserver wird nicht unterstützt.

Verwandte Links

[Installationsanforderungen](#) auf Seite 3
[Installieren der Anwendung](#) auf Seite 4
[Upgrade einer vorhandenen Installation](#) auf Seite 5
[Entfernen einer Installation](#) auf Seite 5

Installationsanforderungen

Anforderungen an den Installationsbenutzer

Als Installationsbenutzer benötigen Sie Folgendes:

- Wissen über die Installation und Konfiguration von CentOS 6.9.
- Wissen über die Konfiguration von IP Office, insbesondere die Sicherheitskonfiguration.
- Die Anwendung generiert bei der Installation ein selbstsigniertes Zertifikat. Wenn Sie jedoch Ihr eigenes Zertifikat verwenden, benötigen Sie ein Identitätszertifikat für den Server, das von Ihrer Zertifizierungsstelle ausgestellt wird.

Serveranforderungen

Wichtig:

- Installation und Konfiguration des Betriebssystems werden in dieser Dokumentation nicht behandelt.

- **Betriebssystem:** CentOS 6.9. Das Betriebssystem kann unter https://www.centos.org/download heruntergeladen werden.
  - Die Installation von Cloud Operations Manager wird auf einem bestehenden Server Edition-, IP Office Select- oder IP Office-Anwendungsserver nicht unterstützt.
  - Die Installation wird auf Avaya Operations Support System-Servern unterstützt.
- **Speicher:** 4 GB RAM
- **Speicher:** 100 GB Festplatte

- **Prozessor:** 4-Core-CPU
- **Internetverbindung erforderlich:** Die Installations- und Upgradeprozesse prüfen auf unterschiedliche Komponentenabhängigkeiten und laden diese Abhängigkeiten, wenn sie nicht bereits im Betriebssystem installiert sind, herunter und installieren diese. Daher ist für erfolgreiche Installationen und Upgrades eine Internetverbindung erforderlich.

Anforderungen des Kunden

- Server Edition oder IP Office Select auf IP Office Release 11.0 oder höher.

Verwandte Links

[Installation](#) auf Seite 3

Installieren der Anwendung

Informationen zu diesem Vorgang

Verwenden Sie die folgende Vorgehensweise, um die Cloud Operations Manager-Anwendung und -Datenbank auf dem Server zu installieren.

Voraussetzungen

Wichtig:

Internetverbindung erforderlich: Die Installations- und Upgradeprozesse prüfen auf unterschiedliche Komponentenabhängigkeiten und laden diese Abhängigkeiten, wenn sie nicht bereits im Betriebssystem installiert sind, herunter und installieren diese. Daher ist für erfolgreiche Installationen und Upgrades eine Internetverbindung erforderlich.

Vorgehensweise

1. Laden Sie die aktuelle com-rpms.tar-Datei herunter.
2. Übertragen Sie die com-rpms.tar-Datei in einen persönlichen Ordner auf dem Server.
3. Melden Sie sich am Server als der Root-Benutzer an, und ändern Sie das Verzeichnis in den persönlichen Ordner, der oben verwendet wurde. Beispielsweise `cd /home/Administrator`.
4. Geben Sie den Befehl `tar -xvf com-rpms.tar` ein.
5. Installieren Sie die Software. Welcher Befehl verwendet wird, hängt vom Servertyp ab:
   - **CentOS 6.9 Server:** Geben Sie folgenden Befehl ein:

     `- ./com_rpm.sh standalone com-rpms.zip`
   - **Avaya Operations Support System Server:** Geben Sie den Befehl `./com_rpm.sh install com-rpms.zip` ein

     `- ./com_rpm.sh install com-rpms.zip`
6. Installieren Sie die Software. Welcher Befehl verwendet wird, hängt vom Servertyp ab:
7. Nach der Installation dauert es etwa 30 Sekunden, bis die Anwendung gestartet wird.
8. Melden Sie sich mit dem Administratorbenutzernamen und -kennwort bei der Anwendung an. Die URL lautet https://<server>:7080/com
9. Akzeptieren Sie die Lizenzbedingungen.

10. Ändern Sie das Standardkennwort, wenn Sie dazu aufgefordert werden.
11. Konfigurieren Sie den Server für zusätzliche Benutzer- und Kundenkonten, wie im Handbuch *Verwenden von IP Office Cloud Operations Manager* beschrieben.

Verwandte Links

Installation auf Seite 3

Upgrade einer vorhandenen Installation

Informationen zu diesem Vorgang

Verwenden Sie die folgende Vorgehensweise, um ein Upgrade einer vorhandenen Installation von Cloud Operations Manager durchzuführen.

Voraussetzungen

Warnung:

Beim Upgrade wird die Anwendung neu gestartet. Dadurch werden alle aktuellen Benutzer abgemeldet, und alle derzeit ausgeführten Aktionen werden beendet.

Wichtig:

Internetverbindung erforderlich: Die Installations- und Upgradeprozesse prüfen auf unterschiedliche Komponentenabhängigkeiten und laden diese Abhängigkeiten, wenn sie nicht bereits im Betriebssystem installiert sind, herunter und installieren diese. Daher ist für erfolgreiche Installationen und Upgrades eine Internetverbindung erforderlich.

Vorgehensweise

1. Laden Sie die aktuelle com-rpms.tar-Datei herunter.
2. Übertragen Sie die com-rpms.tar-Datei in einen persönlichen Ordner auf dem Server.
3. Melden Sie sich am Server als der Root-Benutzer an, und ändern Sie das Verzeichnis in den persönlichen Ordner, der oben verwendet wurde. Beispielsweise `cd /home/Administrator`.
4. Geben Sie den Befehl `tar -xvf com-rpms.tar` ein.
5. Geben Sie den Befehl `./com_rpm.sh upgrade com-rpms.zip` ein.

Verwandte Links

Installation auf Seite 3

Entfernen einer Installation

Informationen zu diesem Vorgang

Sie können nur die Anwendung oder die Anwendung und die Datenbankdaten deinstallieren.

Vorgehensweise

1. Melden Sie sich am Server als der Root-Benutzer an, und ändern Sie das Verzeichnis in den persönlichen Ordner, der den für Installation und Upgrades verwendeten `./com-rpm.sh` enthält. Beispielsweise `cd /home/Administrator`.

2. Wenn die vorherigen Installationsdateien gelöscht wurden:
    a. Laden Sie die aktuelle com-rpms.tar-Datei herunter.
    b. Übertragen Sie die com-rpms.tar-Datei in einen persönlichen Ordner auf dem Server.
    c. Melden Sie sich am Server als der Root-Benutzer an, und ändern Sie das Verzeichnis in den persönlichen Ordner, der oben verwendet wurde. Beispielsweise `cd /home/Administrator`.
    d. Geben Sie den Befehl `tar -xvf com-rpms.tar` ein.
3. Wählen Sie den Typ der erforderlichen Deinstallation aus:
    - Wenn Sie nur die Anwendung, aber nicht die Datenbank entfernen möchten: Geben Sie den Befehl `./com_rpm.sh remove` ein
    - Wenn Sie sowohl die Anwendung als auch die Datenbank entfernen möchten: Geben Sie den Befehl `./com_rpms.sh cleanup` ein

Verwandte Links

Installation auf Seite 3

Kapitel 2: IP Office-Konfiguration

IP Office-Konfiguration

In diesem Abschnitt wird die erforderliche Konfiguration für die IP Office-Systeme im Netzwerk eines Kunden beschrieben, die mit Cloud Operations Manager unterstützt werden sollen.

Verwandte Links

Aktivieren von COM-Support auf Seite 7
Ausführlich auf Seite 8

Aktivieren von COM-Support

Informationen zu diesem Vorgang

Um eine Verbindung mit Systemen eines Kunden herzustellen, verwendet Cloud Operations Manager standardmäßig die Einstellungen eines Sicherheitsbenutzers mit dem Namen ***MCMAdmin***, der auf diesen Systemen konfiguriert ist.

Dieser Sicherheitsbenutzer ist standardmäßig deaktiviert, und es wurde kein Kennwort für diesen festgelegt. Der Prozess der Aktivierung des Sicherheitsbenutzers erfordert Administratorzugriff auf das Kundensystem und muss möglicherweise vom ursprünglichen Installationsbenutzer oder Maintainer des Systems durchgeführt werden.

Wenn der Kunde zu einem späteren Zeitpunkt ein weiteres IP Office-System zu seinem Netzwerk hinzufügt, sollten Sie diesen Vorgang wiederholen, damit das neue System Cloud Operations Manager angezeigt wird.

Vorgehensweise

1. Melden Sie sich bei Web Manager auf dem Server Edition/IP Office Select-System an.
2. Klicken Sie auf **Lösung**.
3. Klicken Sie auf die Drop-down-Liste **Aktionen**, und wählen Sie **Cloud Operations Management** aus.
4. Geben Sie das Kennwort ein, das die Systeme in der Kundenlösung für ihre Cloud Operations Manager-Verbindung verwenden sollten, und bestätigen Sie das Kennwort.
5. Klicken Sie auf **Aktivieren und synchronisieren**.
6. Dadurch wird das ***MCMAdmin***-Sicherheitsbenutzerkonto auf dem primären System aktiviert und das Kennwort festgelegt. Die Änderung wird dann mit allen anderen Systemen in der Lösung synchronisiert. Dieser Vorgang kann je nach Anzahl der Systeme in der Lösung mehrere Minuten dauern.

7. Wenn die Meldung angezeigt wird, dass die Synchronisierung erfolgreich war, klicken Sie auf **Abbrechen**.

Verwandte Links

IP Office-Konfiguration auf Seite 7

Ausführlich

In diesem Abschnitt wird vorausgesetzt, dass Sie mit der Sicherheitskonfiguration von IP Office mithilfe von IP Office Manager und IP Office Web Manager vertraut sind. Nehmen Sie keine Änderungen vor, da Sie dadurch die Sicherheit der Kundensysteme gefährden und bestehenden sicheren Zugriff deaktivieren können.

Die IP Office Web Manager-Steuerung stellt eine vereinfachte Methode dar, um auf allen Systemen im Netzwerk eines Kunden Cloud Operations Manager-Unterstützung zu aktivieren. Sie verwendet ein standardmäßiges ***MCMAdmin***-Sicherheitsbenutzerkonto mit einem Kennwort, das angegeben wird, wenn das Verbindungsmenü ausgeführt wird.

In diesem Abschnitt werden die einzelnen Sicherheitsänderungen beschrieben, die auf diesen Systemen vorgenommen werden. Dies kann hilfreich sein, wenn Sie die Sicherheitsverbindung zwischen den Kundensystemen und Cloud Operations Manager ändern möchten. Beispiel:

- Verwenden Sie ein anderes Sicherheits-Dienstbenutzerkonto als ***MCMAdmin***. Das heißt, erstellen Sie einen anderen Dienstbenutzer mit den gleichen Rechten wie der ***MCMAdmin***-Dienstbenutzer.
- Gewähren Sie dem verwendeten Sicherheitskonto zusätzliche Rechte: Erlauben Sie dem gleichen Konto z. B., sich bei IP Office System Status Application anzumelden. Fügen Sie den ***MCMAdmin***-Dienstbenutzer z. B. zur Berechtigungsgruppe ***Geschäftspartner*** hinzu.

Standardsicherheitskonfiguration

- Der Dienstbenutzer ***MCMAdmin*** ist vorhanden, aber das Konto ist standardmäßig deaktiviert.
- Der Dienstbenutzer ist ein Mitglied der ***MCM Admin***-Berechtigungsgruppe.
- Die Berechtigungsgruppe verfügt über die folgenden Sicherheitsrechte:
  - **Sicherheitsverwaltung**: **Eigenes Dienstbenutzerkennwort schreiben**
  - **Webdienste**: **Sichern**, **Upgrade**, **Dienstmonitor lesen**

Verwandte Links

IP Office-Konfiguration auf Seite 7
Hinzufügen eines neuen Dienstbenutzers auf Seite 8
Systemweites Synchronisieren von Sicherheit auf Seite 9

Hinzufügen eines neuen Dienstbenutzers

Informationen zu diesem Vorgang

Die Standardverbindung zwischen Cloud Operations Manager und IP Office verwendet den Benutzernamen und das Kennwort des ***MCMAdmin***-Servers. Sie können einen zusätzlichen Dienstbenutzer hinzufügen und dann den Namen und das Kennwort des Dienstbenutzers in den Cloud Operations Manager-Menüs verwenden, um eine Verbindung zu einem neuen Kunden aufzubauen.

Vorgehensweise

1. Melden Sie sich bei IP Office mithilfe eines Kontos an, das Rechte für die Sicherheitsverwaltung besitzt.
2. Wählen Sie **Security Manager**, und klicken Sie auf **Dienstbenutzer**.
3. Klicken Sie auf **+Dienstbenutzer hinzufügen**.
4. Geben Sie einen Namen ein, und setzen Sie den Kontostatus auf **Aktiviert**.
5. Geben Sie das Kontokennwort ein, und bestätigen Sie es.
6. Wählen Sie im Abschnitt **BERECHTIGUNGSGRUPPEN MCM-Administrator** aus. Sie können auch andere Gruppen auswählen, die auf das gleiche Konto zugreifen können sollen, z. B. "Geschäftspartner" und "Administratorgruppe".
7. Klicken Sie auf **Erstellen**.
8. Synchronisieren Sie die Sicherheitsänderungen mit allen Systemen im Netzwerk. Weitere Informationen hierzu finden Sie unter Systemweites Synchronisieren von Sicherheit auf Seite 9.

Verwandte Links

Ausführlich auf Seite 8

Systemweites Synchronisieren von Sicherheit

Vorgehensweise

1. Melden Sie sich bei IP Office Web Manager mithilfe eines Kontos an, das Rechte für die Sicherheitsverwaltung besitzt.
2. Wählen Sie **Security Manager**, und klicken Sie auf **Dienstbenutzer**.
3. Klicken Sie auf **Serverbenutzer synchronisieren** und **Systemkennwort**.

Verwandte Links

Ausführlich auf Seite 8

Kapitel 3: Anhang

Neustarten der Anwendung

Informationen zu diesem Vorgang

Der Root-Benutzer kann einen Neustart der Anwendung erzwingen.

Vorgehensweise

1. Melden Sie sich am Server als der Root-Benutzer an, und ändern Sie das Verzeichnis in das persönliche Verzeichnis, in dem die für Installationen/Upgrades der Anwendung verwendeten Dateien entpackt wurden.
2. Geben Sie den Befehl `service tomcat-mcm restart` ein.

Neustarten des Datenbankdienstes

Informationen zu diesem Vorgang

Der Root-Benutzer kann einen Neustart des Datenbankdienstes erzwingen.

Vorgehensweise

1. Melden Sie sich am Server als der Root-Benutzer an, und ändern Sie das Verzeichnis in das persönliche Verzeichnis, in dem die für Installationen/Upgrades der Anwendung verwendeten Dateien entpackt wurden.
2. Geben Sie den Befehl `service postgresql-9.6 restart` ein.

Zurücksetzen der Benutzer

Informationen zu diesem Vorgang

Wenn es notwendig sein sollte, kann der Root-Benutzer alle bestehenden Benutzer entfernen und das Standardkennwort des Benutzers **Administrator** wieder reaktivieren.

Warnung:

- Dieser Prozess führt dazu, dass der Cloud Operations Manager-Dienst angehalten und dann neu gestartet wird.
- Bei diesem Prozess werden alle bestehenden Operator- und Administratorbenutzer außer **Administrator** gelöscht.

Vorgehensweise

1. Geben Sie `cd /opt/Avaya/mcm` ein.
2. Geben Sie `./com_password_reset.sh` ein.

Ändern des Datenbankkennworts

Informationen zu diesem Vorgang

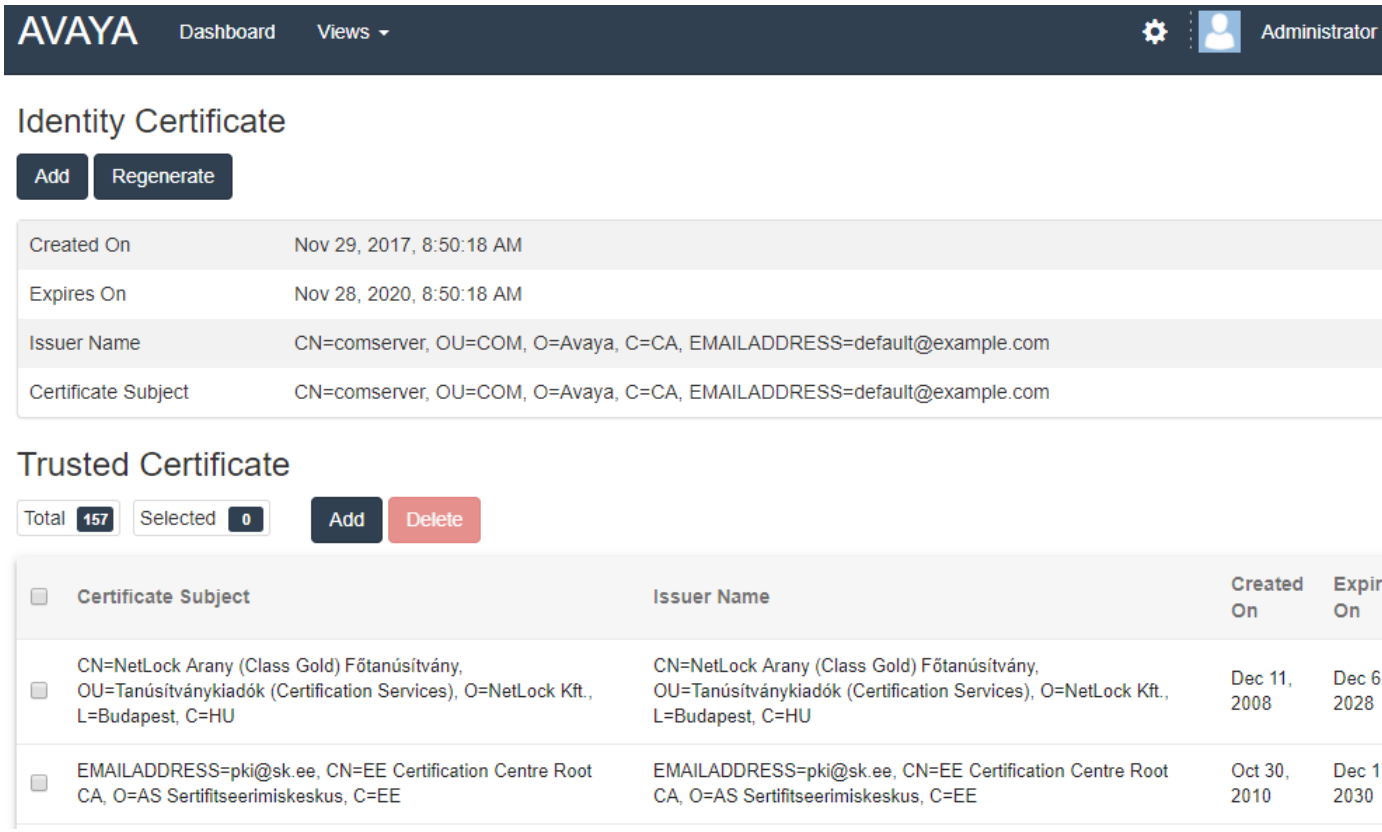
Der Cloud Operations Manager-Server-Maintainer kann das Kennwort der Datenbank ändern, die zum Speichern von Kunden- und Benutzerdaten verwendet wird. Wenn er dies tut, muss das von Cloud Operations Manager verwendete Datenbankkennwort entsprechend geändert werden.

Vorgehensweise

1. Klicken Sie auf das Symbol ⚙, und wählen Sie **Einstellungen** aus.
2. Verwenden Sie **Datenbankkennwort**, um das Kennwort in das neue Kennwort zu ändern, das vom System-Maintainer bereitgestellt wird.
3. Klicken Sie auf **Speichern**.

Serverzertifikate

Über dieses Menü können Sie Details zum eigenen Identitätszertifikat des Cloud Operations Manager-Dienstes und anderen von diesem Dienst gespeicherten Zertifikaten abrufen.



Identitätszertifikat

Standardmäßig hat der Cloud Operations Manager-Dienst ein eigenes selbstsigniertes Zertifikat, das ab der Installation 3 Jahre gültig ist. Wenn das vorhandene Zertifikat, das vom Server verwendet wird, demnächst abläuft, wird eine 90-Tage-Warnung herausgegeben.

Dieser Abschnitt enthält allgemeine Anweisungen zum Hinzufügen eines Zertifikats zu Ihrem Browser. Normalerweise stellt Ihnen der Systemverwalter eine Kopie des Anwendungszertifikats zur Verfügung, das Sie dann dem Zertifikatspeicher Ihres Browsers hinzufügen können. Bei Bedarf können Sie jedoch über Chrome eine Kopie des Zertifikats herunterladen.

Vertrauenswürdiges Zertifikat

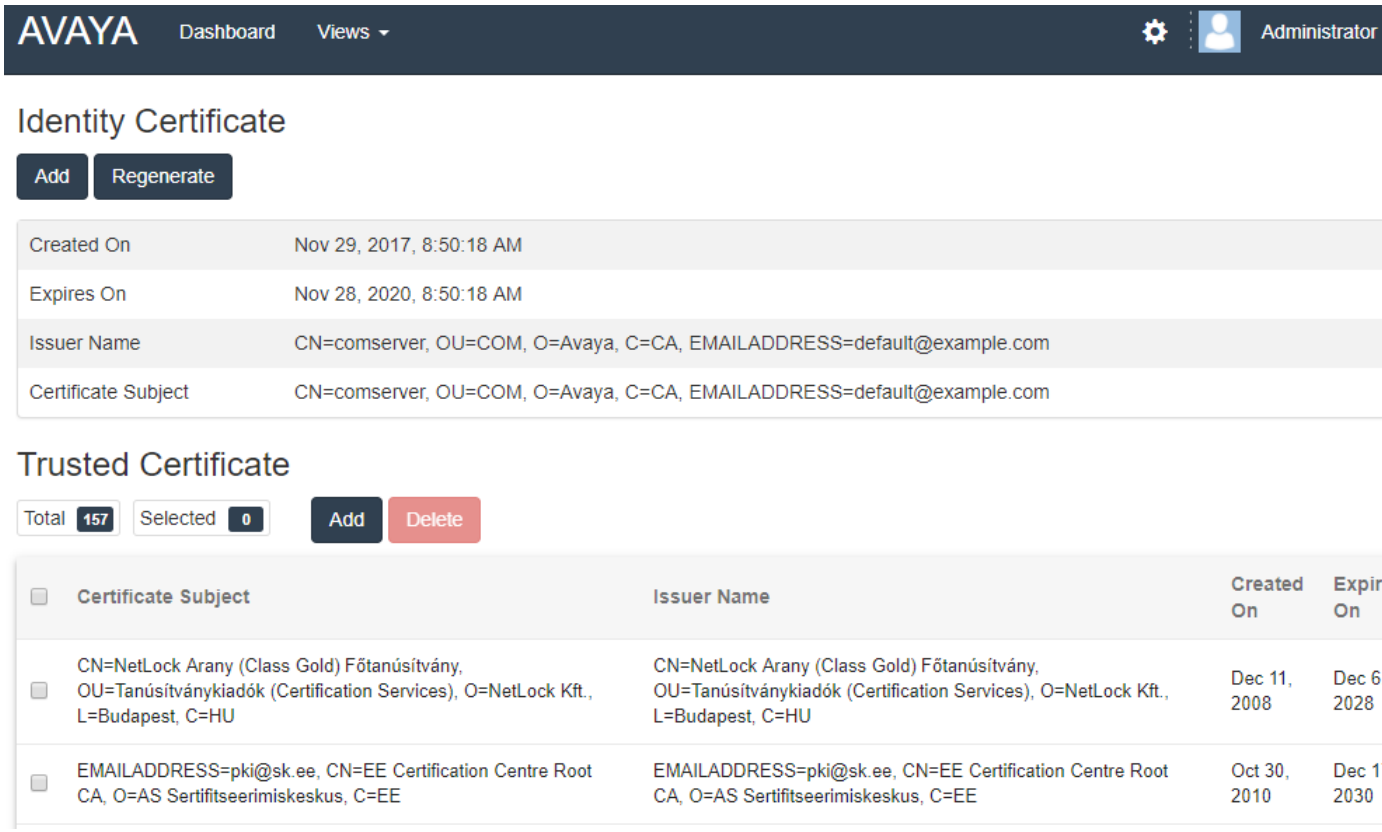
In dieser Tabelle werden alle anderen Zertifikate aufgelistet, die im Cloud Operations Manager-Dienst gespeichert sind. Dabei kann es sich um IP Office-Systemzertifikate und -Zwischenzertifikate handeln.

Verwandte Links

Serverzertifikate auf Seite 12
Serverzertifikate auf Seite 14

Serverzertifikate

Über dieses Menü können Sie Details zum eigenen Identitätszertifikat des Cloud Operations Manager-Dienstes und anderen von diesem Dienst gespeicherten Zertifikaten abrufen.



Identitätszertifikat

Standardmäßig hat der Cloud Operations Manager-Dienst ein eigenes selbstsigniertes Zertifikat, das ab der Installation 3 Jahre gültig ist. Wenn das vorhandene Zertifikat, das vom Server verwendet wird, demnächst abläuft, wird eine 90-Tage-Warnung herausgegeben.

Dieser Abschnitt enthält allgemeine Anweisungen zum Hinzufügen eines Zertifikats zu Ihrem Browser. Normalerweise stellt Ihnen der Systemverwalter eine Kopie des Anwendungszertifikats zur Verfügung, das Sie dann dem Zertifikatspeicher Ihres Browsers hinzufügen können. Bei Bedarf können Sie jedoch über Chrome eine Kopie des Zertifikats herunterladen.

Vertrauenswürdiges Zertifikat

In dieser Tabelle werden alle anderen Zertifikate aufgelistet, die im Cloud Operations Manager-Dienst gespeichert sind. Dabei kann es sich um IP Office-Systemzertifikate und -Zwischenzertifikate handeln.

Verwandte Links

Serverzertifikate auf Seite 11
Erneutes Generieren des Identitätszertifikats auf Seite 13
Hinzufügen eines anderen Identitätszertifikats auf Seite 14

Erneutes Generieren des Identitätszertifikats

Informationen zu diesem Vorgang

Sie können das aktuelle Identitätszertifikat durch ein selbstsigniertes Zertifikat ersetzen, das von der Cloud Operations Manager-Anwendung generiert wurde. Dieses Zertifikat ist für 3 Jahre gültig.

Hinweis:

Um das bestehende Zertifikat zu ersetzen, muss der Cloud Operations Manager-Dienst neu gestartet werden. Näheres dazu erfahren Sie im Handbuch „Installieren von Cloud Operations Manager“.

Vorgehensweise

1. Klicken Sie auf ⚙ und dann auf **Zertifikate**.
2. Klicken Sie auf **Erneut generieren**.
3. Klicken Sie auf **Ja**.

Verwandte Links

Serverzertifikate auf Seite 12

Hinzufügen eines anderen Identitätszertifikats

Informationen zu diesem Vorgang

Sie können das aktuelle Identitätszertifikat ersetzen, das von der Cloud Operations Manager-Anwendung verwendet wird. Das gleiche Zertifikat kann dann für alle Browser und Systeme installiert werden, die Zugriff auf Cloud Operations Manager benötigen.

Hinweis:

Um das bestehende Zertifikat zu ersetzen, muss der Cloud Operations Manager-Dienst neu gestartet werden. Näheres dazu erfahren Sie im Handbuch „Installieren von Cloud Operations Manager“.

Vorgehensweise

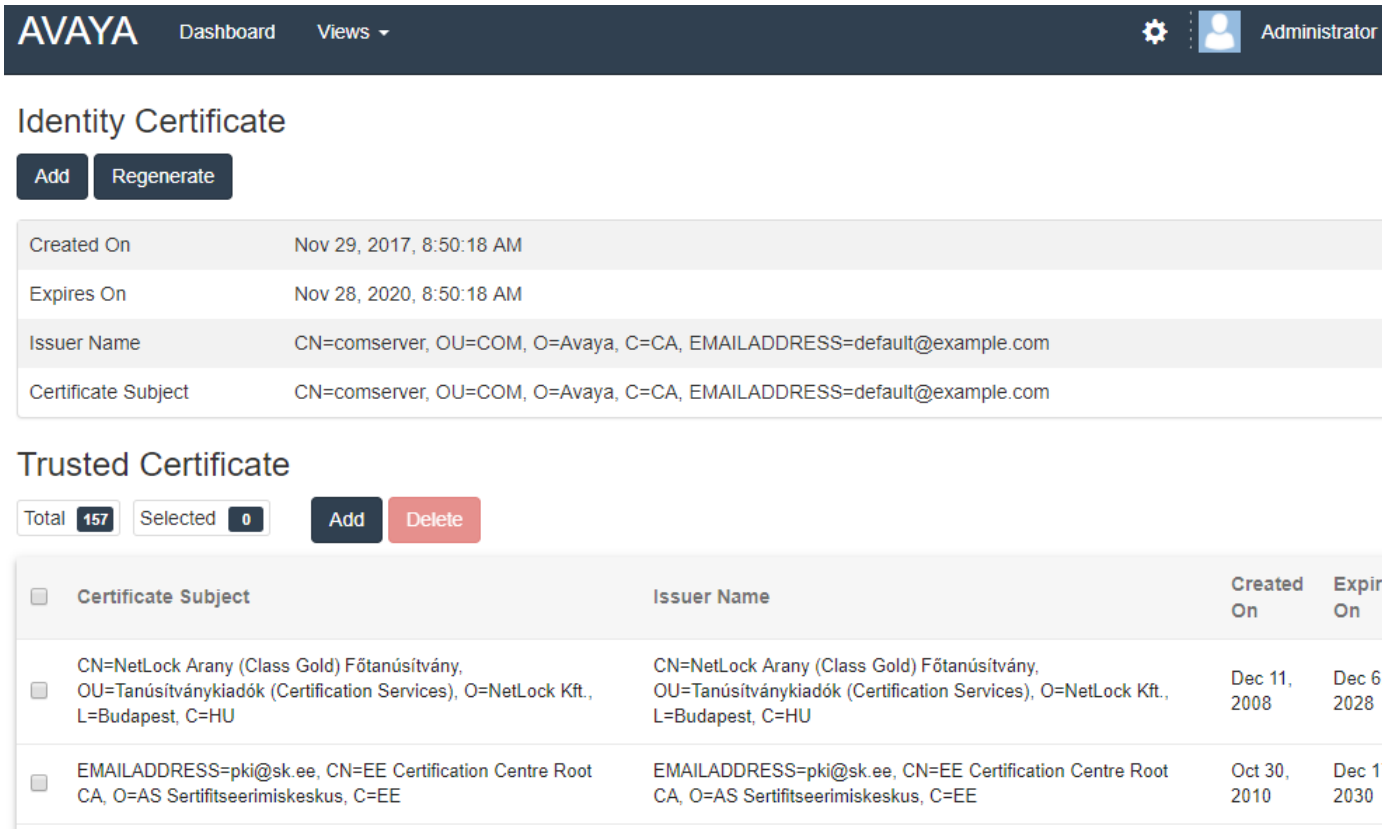
1. Klicken Sie auf ⚙ und dann auf **Zertifikate**.
2. Klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Datei auswählen** und wählen Sie die neue Zertifikatdatei aus.
4. Geben Sie im Feld **Zertifikatkennwort** das Kennwort für die Zertifikatdatei ein.
5. Klicken Sie auf **Senden**.

Verwandte Links

Serverzertifikate auf Seite 12

Serverzertifikate

Über dieses Menü können Sie Details zum eigenen Identitätszertifikat des Cloud Operations Manager-Dienstes und anderen von diesem Dienst gespeicherten Zertifikaten abrufen.



Identitätszertifikat

Standardmäßig hat der Cloud Operations Manager-Dienst ein eigenes selbstsigniertes Zertifikat, das ab der Installation 3 Jahre gültig ist. Wenn das vorhandene Zertifikat, das vom Server verwendet wird, demnächst abläuft, wird eine 90-Tage-Warnung herausgegeben.

Dieser Abschnitt enthält allgemeine Anweisungen zum Hinzufügen eines Zertifikats zu Ihrem Browser. Normalerweise stellt Ihnen der Systemverwalter eine Kopie des Anwendungszertifikats zur Verfügung, das Sie dann dem Zertifikatspeicher Ihres Browsers hinzufügen können. Bei Bedarf können Sie jedoch über Chrome eine Kopie des Zertifikats herunterladen.

Vertrauenswürdiges Zertifikat

In dieser Tabelle werden alle anderen Zertifikate aufgelistet, die im Cloud Operations Manager-Dienst gespeichert sind. Dabei kann es sich um IP Office-Systemzertifikate und -Zwischenzertifikate handeln.

Verwandte Links

Serverzertifikate auf Seite 11
Herunterladen des Serverzertifikats auf Seite 16
Hinzufügen eines Zertifikats zu Chrome auf Seite 16
Hinzufügen eines Zertifikats zu Explorer auf Seite 17
Hinzufügen eines Zertifikats zu Windows auf Seite 17
Hinzufügen eines Zertifikats zu Firefox auf Seite 18

Herunterladen des Serverzertifikats

Informationen zu diesem Vorgang

Normalerweise stellt Ihnen der Systemverwalter eine Kopie des Anwendungszertifikats zur Verfügung, das Sie dann dem Zertifikatspeicher Ihres Browsers hinzufügen können. Bei Bedarf können Sie jedoch über Chrome eine Kopie des Zertifikats herunterladen.

Vorgehensweise

1. Melden Sie sich bei Cloud Operations Manager an.
2. Drücken Sie `Strg+Feststelltaste+I`.
3. Wählen Sie im Bereich rechts die Option **Sicherheit**. Falls nötig, klicken Sie auf das Symbol **>>**, um **Sicherheit** auszuwählen.
4. Klicken Sie auf **Zertifikat anzeigen**. Das Zertifikat wird angezeigt.
5. Klicken Sie auf **Details**.
6. Wählen Sie **In Datei kopieren**.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie **DER-codiert-binär X.509 (.CER)** und klicken Sie auf **Weiter**.
9. Geben Sie den Speicherpfad und den Dateinamen ein. Dazu können Sie die Schaltfläche **Durchsuchen** verwenden.
10. Klicken Sie auf **Weiter**.
11. Klicken Sie auf **Fertig stellen** und dann auf **OK**.

Verwandte Links

Serverzertifikate auf Seite 14

Hinzufügen eines Zertifikats zu Chrome

Informationen zu diesem Vorgang

Gehen Sie folgendermaßen vor, um Ihrem Browser das Cloud Operations Manager-Zertifikat hinzuzufügen.

Auf Windows-PCs nutzen Explorer, Edge und Chrome alle denselben Zertifikatspeicher.

Vorgehensweise

1. Klicken Sie auf das Symbol und wählen Sie **Einstellungen**.
2. Klicken Sie auf **Erweitert**. Klicken Sie auf **HTTP/SSL-Zertifikate und -Einstellungen verwalten**.
3. Klicken Sie auf **Importieren**.
4. Klicken Sie auf **Weiter** und **Durchsuchen**, um zum Speicherort der heruntergeladenen Datei zu navigieren. Wählen Sie sie aus und klicken Sie auf **Öffnen**.
5. Klicken Sie auf **Weiter**. Klicken Sie auf **Alle Zertifikate in folgendem Speicher speichern**.
   - Wenn Sie das vom Server selbst generierte Zertifikat verwenden, wählen Sie **Vertrauenswürdige Stammzertifizierungsstellen**.

- Wenn Sie ein Zertifikat von einer anderen Quelle verwenden, wählen Sie **Zwischenzertifizierungsstellen**.

6. Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.
7. Klicken Sie auf **OK** und dann auf **Schließen**.

Verwandte Links

Serverzertifikate auf Seite 14

Hinzufügen eines Zertifikats zu Explorer

Informationen zu diesem Vorgang

Gehen Sie folgendermaßen vor, um Ihrem Browser das Cloud Operations Manager-Zertifikat hinzuzufügen.

Auf Windows-PCs nutzen Explorer, Edge und Chrome alle denselben Zertifikatspeicher.

Vorgehensweise

1. Klicken Sie auf **Extras** und wählen Sie **Internetoptionen**.
2. Wählen Sie die Registerkarte **Inhalte** und klicken Sie auf **Zertifikate**.
3. Klicken Sie auf **Importieren**.
4. Klicken Sie auf **Weiter** und **Durchsuchen**, um zum Speicherort der heruntergeladenen Datei zu navigieren. Wählen Sie sie aus und klicken Sie auf **Öffnen**.
5. Klicken Sie auf **Weiter**. Klicken Sie auf **Alle Zertifikate in folgendem Speicher speichern**.
   - Wenn Sie das vom Server selbst generierte Zertifikat verwenden, wählen Sie **Vertrauenswürdige Stammzertifizierungsstellen**.
   - Wenn Sie ein Zertifikat von einer anderen Quelle verwenden, wählen Sie **Zwischenzertifizierungsstellen**.
6. Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.
7. Klicken Sie auf **OK** und dann auf **Schließen**.
8. Klicken Sie auf **OK**.

Verwandte Links

Serverzertifikate auf Seite 14

Hinzufügen eines Zertifikats zu Windows

Informationen zu diesem Vorgang

Auf Windows-PCs nutzen Explorer, Edge und Chrome alle denselben Zertifikatspeicher.

Vorgehensweise

1. Doppelklicken Sie auf die Zertifikatdatei.
2. Klicken Sie auf der Registerkarte **Allgemein** auf **Zertifikat installieren**.
3. Wählen Sie **Aktueller Benutzer** und klicken Sie auf **Weiter**.

4. Wählen Sie **Alle Zertifikate in folgendem Speicher speichern**.
   - Wenn Sie das vom Server selbst generierte Zertifikat verwenden, wählen Sie **Vertrauenswürdige Stammzertifizierungsstellen**.
   - Wenn Sie ein Zertifikat von einer anderen Quelle verwenden, wählen Sie **Zwischenzertifizierungsstellen**.
5. Klicken Sie auf **Weiter**. Es wird eine Zusammenfassung der ausgewählten Optionen angezeigt.
6. Klicken Sie auf **Fertig stellen**.

Verwandte Links

Serverzertifikate auf Seite 14

Hinzufügen eines Zertifikats zu Firefox

Informationen zu diesem Vorgang

Gehen Sie folgendermaßen vor, um Ihrem Browser das Cloud Operations Manager-Zertifikat hinzuzufügen.

Vorgehensweise

1. Klicken Sie auf das Symbol und wählen Sie **Optionen**. Alternativ klicken Sie auf das Symbol **Einstellungen**, sofern es auf der Startseite des Browsers angezeigt wird.
2. Klicken Sie auf **Erweitert** und wählen Sie dann **Zertifikate**.
3. Klicken Sie auf **Zertifikate anzeigen**.
4. Klicken Sie auf „Zertifizierungsstellen“.
5. Klicken Sie auf **Importieren**. Navigieren Sie zum Speicherort der vom Server heruntergeladenen CRT- oder PEM-Datei. Wählen Sie die Datei aus und klicken Sie auf **Öffnen**.
6. Aktivieren Sie alle Kontrollkästchen, um dem Zertifikat zu vertrauen.
7. Klicken Sie doppelt auf **OK**.

Verwandte Links

Serverzertifikate auf Seite 14

Debugdateien

Die Anwendung kann Details der Vorgänge in Protokolldateien aufzeichnen. Diese Dateien können hilfreich sein, um Probleme zu diagnostizieren, wenn so scheint, als ob die Anwendung nicht ordnungsgemäß ausgeführt wird.

Die Cloud Operations Manager-Debugdateien werden unter `/opt/Avaya/mcm/apache-tomcat/logs` gespeichert.

Verwandte Links

Ändern des Protokolliergrads der Anwendung auf Seite 19

Herunterladen der Protokolldateien auf Seite 19

Ändern des Protokolliergrads der Anwendung

Informationen zu diesem Vorgang

Die Anwendung kann Details der Vorgänge in Protokolldateien aufzeichnen. Standardmäßig werden Protokolldateien für Vorgänge der letzten 5 Tage oder weniger gespeichert. Diese Dateien können hilfreich sein, um Probleme zu diagnostizieren, wenn es so scheint, als ob die Anwendung nicht ordnungsgemäß ausgeführt wird. Sie können von Avaya angefordert werden (siehe Herunterladen der Protokolldateien auf Seite 19).

Sie können den Protokolliergrad der Informationen anpassen. Da die Protokollierung vieler Informationen die Systemleistung beeinträchtigen kann, sollten nur diejenigen Informationen protokolliert werden, die zur Behebung eines Problems erforderlich sind.

Vorgehensweise

1. Klicken Sie auf das Symbol ⚙, und wählen Sie **Einstellungen** aus.
2. Legen Sie die **Protokollebene** auf die erforderliche Ebene fest. Folgende Optionen stehen zur Verfügung:
   - **FEHLER**: nur Fehlerberichte in die Anwendungsprotokolle einschließen.
   - **INFO**: allgemeine Informationen und Fehlerberichte in die Anwendungsprotokolle einschließen.
   - **DEBUG**: umfassende Anwendungsinformationen und Fehlerberichte in die Anwendungsprotokolle einschließen.
3. Klicken Sie auf **Speichern**.

Verwandte Links

Debugdateien auf Seite 18

Herunterladen der Protokolldateien

Informationen zu diesem Vorgang

Sie können die Protokolldateien herunterladen, die Cloud Operations Manager für die durchgeführten Vorgänge aufgezeichnet hat. Die Anwendung speichert Protokolldateien für die Aktivitäten der letzten 5 Tage.

Beachten Sie, dass die Ebene der Aktivitäten, die in die Protokolldateien aufgenommen werden, angepasst werden kann. Weitere Informationen hierzu finden Sie unter Ändern des Protokolliergrads der Anwendung auf Seite 19.

Vorgehensweise

1. Klicken Sie auf das Symbol ⚙, und wählen Sie **Einstellungen** aus.
2. Klicken Sie auf **Protokolle herunterladen**.
3. Die Protokolle werden als eine ZIP-Datei heruntergeladen. Die genaue Download-Methode und der Speicherort hängen vom verwendeten Browser ab.

Verwandte Links

Debugdateien auf Seite 18

Sichern und Wiederherstellen

Die Cloud Operations Manager-Schnittstelle unterstützt eine Sicherungs- und Wiederherstellungsoption, die von Administratoren verwendet werden kann. Eine Sicherung schließt die Benutzer, die Kunden, die Anwendungseinstellungen und das Serverzertifikat ein.

Die Daten werden in einer ZIP-Datei unter `/opt/Avaya/mcm/backup` gesichert. Der Name der Sicherungsdatei enthält Datum und Uhrzeit, z. B. `backup-20170714-125620.zip`

Derzeit wird nur eine einzelne Sicherungsdatei unterstützt.

Verwandte Links

Sichern der Anwendungseinstellungen auf Seite 20
Wiederherstellen der Anwendungseinstellungen auf Seite 20

Sichern der Anwendungseinstellungen

Vorgehensweise

1. Klicken Sie auf **Verwalten** und dann auf **Sichern und Wiederherstellen**.
2. Klicken Sie auf **Sichern**.
3. Wenn Sie gefragt werden, ob der Vorgang fortgesetzt werden soll, klicken Sie auf **Ja**.
4. Die aktualisierte Sicherung wird jetzt aufgelistet.

Verwandte Links

Sichern und Wiederherstellen auf Seite 20

Wiederherstellen der Anwendungseinstellungen

Vorgehensweise

1. Klicken Sie auf **Verwalten** und dann auf **Sichern und Wiederherstellen**.
2. Klicken Sie auf **Wiederherstellen**.
3. Wenn Sie gefragt werden, ob der Vorgang fortgesetzt werden soll, klicken Sie auf **Ja**.
4. Sie müssen sich erneut anmelden, um den Vorgang fortzusetzen.

Verwandte Links

Sichern und Wiederherstellen auf Seite 20

Ändern des Anwendungsports

Informationen zu diesem Vorgang

Für den Browserport, der für den Zugriff auf Cloud Operations Manager verwendet wird, kann bei Bedarf die für HTTPS-Zugriff verwendete Standardeinstellung 7080 geändert werden.

- Sie müssen sicherstellen, dass der ausgewählte Port nicht bereits von einem anderen Dienst verwendet wird, der auf dem PC ausgeführt wird.

Vorgehensweise

1. Suchen Sie die Datei `/opt/Avaya/mcm/generation.properties`.
2. Bearbeiten Sie die Datei mithilfe von **vi** oder **ed**, indem Sie den Wert **PORT_SECURE** in den erforderlichen Port ändern. Dies ist der Port, der für HTTPS-Zugriff verwendet wird. Standardmäßig lautet er ***7080***.

   Die Option **PORT_PLAIN** kann verwendet werden, um den für HTTP-Zugriff verwendeten Port zu ändern. Zugriffe unter dieser Adresse werden automatisch zum obigen sicheren HTTPS-Port umgeleitet.
3. Generieren Sie die Servereinstellungsdatei, die von der Anwendung verwendet wird, mithilfe des Befehls `/opt/Avaya/mcm/gen_server_xml.sh` neu.
4. Starten Sie die Anwendung mithilfe des Befehls `service tomcat-mcm restart` neu.

Befehlszusammenfassung

Aktion	Befehl
Erweitern der TAR-Datei	`tar -xvf com-rpms.tar`
Installieren auf einem OSS-Server	`./com_rpm.sh install com-rpms.zip`
Installieren auf einem eigenständigen Server	`./com_rpm.sh standalone com-rpms.zip`
Entfernen der Anwendung	`./com_rpm.sh remove`
Upgrade	`./com_rpm.sh upgrade com-rpms.zip`
Entfernen der Anwendung und Datenbank	`./com_rpms.sh cleanup`
Neustarten des Anwendungsdienstes	`service tomcat-mcm restart`
Neustarten des Datenbankdienstes	`service postgresql-9.6 restart`
Zurücksetzen des Administratorkennworts	`cd /opt/Avaya/mcm` `./com_password_reset.sh`

Gültige

Hinweis

Es wurden angemessene Anstrengungen unternommen, um sicherzustellen, dass die in diesem Dokument enthaltenen Informationen vollständig und korrekt sind. Avaya Inc. übernimmt jedoch keine Haftung für eventuelle Fehler. Avaya behält sich das Recht vor, die in diesem Dokument enthaltenen Informationen ohne entsprechende Mitteilung an eine Person oder Organisation zu ändern und zu korrigieren.

Haftungsausschluss für Dokumentation

(ii) Der Begriff „Dokumentation" bezeichnet veröffentlichte Informationen in unterschiedlichen Medien; hierzu können Produktinformationen, Bedienungsanleitungen und Leistungsspezifikationen gehören, die Endbenutzern von Produkten allgemein verfügbar sind. Der Begriff „Dokumentation" schließt Marketingmaterial aus. Avaya haftet nur dann für Änderungen, Ergänzungen oder Streichungen der ursprünglich veröffentlichten Fassung dieser Dokumentation, wenn diese Änderungen, Ergänzungen und Streichungen von Avaya vorgenommen wurden. Der Endnutzer erklärt sich einverstanden, Avaya sowie die Handlungsbevollmächtigten, Angestellten und Beschäftigten von Avaya im Falle von Forderungen, Rechtsstreitigkeiten, Ansprüchen und Urteilen auf der Grundlage von oder in Verbindung mit nachträglichen Änderungen, Ergänzungen oder Streichungen in dieser Dokumentation zu entschädigen und von jeglicher Haftung freizustellen, sofern diese Änderungen, Ergänzungen oder Streichungen vom Endnutzer vorgenommen worden sind.

Haftungsausschluss für Links

Avaya haftet nicht für die Inhalte und die Zuverlässigkeit der Websites ab, auf die auf dieser Website oder in der von Avaya bereitgestellten Dokumentation verwiesen (verlinkt) wird. Avaya haftet nicht für die Verlässlichkeit von auf diesen Websites enthaltenen Informationen, Aussagen oder Inhalten und unterstützt nicht notwendigerweise die Produkte, Dienstleistungen oder Informationen, die auf diesen beschrieben oder angeboten werden. Avaya kann nicht garantieren, dass diese Links jederzeit funktionieren, und hat keinen Einfluss auf die Verfügbarkeit dieser Websites.

Gewährleistung

Avaya gewährt eine eingeschränkte Gewährleistung für Hardware und Software von Avaya. Die Bedingungen der eingeschränkten Gewährleistung können Sie Ihrem Kaufvertrag entnehmen. Darüber hinaus stehen die Standardgewährleistungsbedingungen von Avaya sowie Informationen über den Support für dieses Produkt während der Gewährleistungszeit auf der Avaya-Support-Website https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 unter dem Link „Warranty & Product Lifecycle" bzw. einer von Avaya bekannt gegebenen Nachfolgeseite allen Avaya-Kunden und Dritten zur Verfügung. Beachten Sie hierbei: Wenn die Produkte von einem Avaya-Channel Partner außerhalb der Vereinigten Staaten und Kanada erworben werden, wird die Gewährleistung von diesem Channel Partner und nicht direkt von Avaya erbracht.

Der Begriff „gehostete Dienste" bezeichnet das Abonnement eines gehosteten Diensts, das Sie von Avaya oder (falls zutreffend) einem autorisierten Avaya-Channel Partner erworben haben

und das in SAS- oder sonstigen Servicebeschreibungen bezüglich des betreffenden gehosteten Diensts näher beschrieben wird. Wenn Sie ein Abonnement eines gehosteten Diensts erwerben, ist die oben genannte eingeschränkte Gewährleistung gegebenenfalls nicht gültig, Sie haben jedoch möglicherweise Anspruch auf Support-Leistungen in Verbindung mit dem gehosteten Dienst. Dies ist in den Dokumenten der Servicebeschreibung für den betreffenden gehosteten Dienst näher beschrieben. Setzen Sie sich mit Avaya oder (ggf.) mit dem Avaya-Channel Partner in Verbindung, wenn Sie weitere Informationen hierzu wünschen.

Gehosteter Dienst

FOLGENDE BESTIMMUNGEN GELTEN, WENN SIE EIN ABONNEMENT FÜR EINEN GEHOSTETEN DIENST VON AVAYA ODER EINEM AVAYA-VERTRIEBSPARTNER (FALLS ZUTREFFEND) ERWERBEN. DIE NUTZUNGSBEDINGUNGEN DER GEHOSTETEN DIENSTE SIND AUF DER AVAYA-WEBSEITE HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNTER DEM LINK „Avaya Nutzungsbedingungen für gehostete Dienste” ODER ETWAIGEN VON AVAYA BEKANNTGEGEBENEN NACHFOLGER-WEBSITES ABRUFBAR UND GELTEN FÜR ALLE PERSONEN, DIE DEN GEHOSTETEN DIENST AUFRUFEN ODER NUTZEN. INDEM SIE DEN GEHOSTETEN DIENST AUFRUFEN ODER NUTZEN ODER ANDERE DAZU AUTORISIEREN, STIMMEN SIE IN IHREM NAMEN UND IM AUFTRAG IHRER ORGANISATION (NACHFOLGEND „SIE” ODER DER „ENDBENUTZER”) DEN NUTZUNGSBEDINGUNGEN ZU. WENN SIE DEN NUTZUNGSBEDINGUNGEN IM NAMEN EINES UNTERNEHMENS ODER EINER ANDEREN JURISTISCHEN PERSON ZUSTIMMEN, GARANTIEREN SIE, DASS SIE AUTORISIERT SIND, DIESE ENTITÄT AN DIE VORLIEGENDEN NUTZUNGSBEDINGUNGEN ZU BINDEN. WENN SIE DAZU NICHT BEFUGT SIND ODER SIE DIESEN NUTZUNGSBESTIMMUNGEN NICHT ZUSTIMMEN MÖCHTEN, DÜRFEN SIE NICHT AUF DEN GEHOSTETEN DIENST ZUGREIFEN ODER DIESEN NUTZEN UND NIEMANDEN AUTORISIEREN, AUF DEN GEHOSTETEN DIENST ZUZUGREIFEN ODER IHN ZU NUTZEN.

Lizenzen

DIE LIZENZBESTIMMUNGEN FÜR DIE SOFTWARE, DIE AUF DER AVAYA-WEBSITE UNTER HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNTER DEM LINK „AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” BZW. EINER VON AVAYA BEKANNT GEGEBENEN NACHFOLGESEITE AUFGEFÜHRT SIND, GELTEN FÜR ALLE PERSONEN, DIE SOFTWARE VON AVAYA HERUNTERLADEN, NUTZEN BZW. INSTALLIEREN, WELCHE IM RAHMEN EINES KAUFVERTRAGS MIT AVAYA BZW. EINEM AUTORISIERTEN AVAYA-CHANNEL PARTNER VON AVAYA INC., EINEM VERBUNDENEN UNTERNEHMEN VON AVAYA BZW. EINEM AUTORISIERTEN AVAYA-CHANNEL PARTNER BEZOGEN WURDE. SOFERN NICHT ANDERWEITIG VON AVAYA SCHRIFTLICH BESTÄTIGT, VERLÄNGERT AVAYA DIESE LIZENZ NICHT, WENN DIE SOFTWARE NICHT ÜBER EINE DER OBEN GENANNTEN OFFIZIELLEN QUELLEN BEZOGEN WURDE. AVAYA BEHÄLT SICH DAS RECHT VOR, GEGEN SIE ODER DRITTE, WELCHE DIE SOFTWARE OHNE LIZENZ VERWENDEN ODER VERKAUFEN, GERICHTLICHE SCHRITTE EINZULEITEN. MIT DER INSTALLATION, DEM DOWNLOAD ODER DER NUTZUNG DER SOFTWARE BZW. MIT DEM EINVERSTÄNDNIS ZUR INSTALLATION, DEM DOWNLOAD ODER DER NUTZUNG DURCH ANDERE AKZEPTIEREN SIE IN IHREM EIGENEN NAMEN UND IM NAMEN DES UNTERNEHMENS, FÜR DAS SIE DIE SOFTWARE INSTALLIEREN, HERUNTERLADEN ODER NUTZEN (NACHFOLGEND ALS „SIE” UND „ENDBENUTZER” BEZEICHNET), DIESE NUTZUNGSBEDINGUNGEN UND GEHEN EINEN RECHTSGÜLTIGEN VERTRAG MIT AVAYA INC. ODER DEM BETREFFENDEN AVAYA-PARTNER EIN („AVAYA”).

Avaya gewährt Ihnen eine Lizenz im Rahmen der unten beschriebenen Lizenztypen mit Ausnahme der Heritage Nortel-Software, deren Lizenzrahmen ebenfalls weiter unten beschrieben wird. Ist in der Auftragsdokumentation kein eindeutiger Lizenztyp angegeben, handelt es sich bei der gültigen Lizenz um eine entsprechend vorgesehene Systemlizenz, wie im Abschnitt zur vorgesehenen Systemlizenz beschrieben. Grundsätzlich wird für jeweils eine (1)

Geräteeinheit eine (1) Lizenz vergeben, sofern keine andere Anzahl von Lizenzen oder Geräteeinheiten in der Dokumentation oder anderen Ihnen zur Verfügung stehenden Materialien angegeben ist. „„Software“" sind Computerprogramme in Objektcode, die von Avaya oder einem Avaya Channel Partner als unabhängiges Produkt oder vorinstalliert auf einem Hardware-Produkt bereitgestellt werden, sowie jegliche Upgrades, Aktualisierungen, Fehlerbehebungen oder geänderte Versionen dieser Programme. Der Begriff „designierter Prozessor ”bezeichnet ein einzelnes unabhängiges Computergerät. Der Begriff „Server” bezeichnet eine Gruppe von designierten Prozessoren, die eine Softwareanwendung für mehrere Benutzer bereitstellt (virtuell oder physisch). Der Begriff „Instanz” bezeichnet eine einzelne Kopie der Software, die zu einem bestimmten Zeitpunkt (i) auf einem physischen Rechner oder (ii) auf einer bereitgestellten virtuellen Maschine („VM”) oder ähnlicher Bereitstellung ausgeführt wird.

Lizenztyp(en)

Systembezogene Lizenz (Designated System(s) License (DS). Ein Endbenutzer darf eine Kopie oder Instanz der Software nur folgendermaßen installieren und verwenden: 1) auf einer Anzahl vorgesehener Prozessoren bis zu der im Auftrag angegebenen Anzahl von Prozessoren oder 2) bis zu der im Auftrag, in der Dokumentation oder soweit von Avaya schriftlich autorisierten angegebenen Anzahl von Instanzen der Software. Avaya ist berechtigt zu verlangen, dass der oder die betreffenden Rechner durch Angabe ihres Typs, ihrer Seriennummer, ihrer Leistungsmerkmale, ihrer Instanz, ihres Standorts oder sonstiger Merkmale in dem Einzelvertrag identifiziert werden oder Avaya von dem Endanwender zu diesem Zweck auf elektronischem Wege mitgeteilt werden.

Mehrplatzlizenz (Concurrent User License (CU). Der Endanwender ist berechtigt, die Software auf mehrere bezeichnete Rechner oder auf einem oder mehreren Servern zu installieren, wobei jedoch gewährleistet sein muss, dass auf die Software jeweils nur von der lizenzierten Anzahl Arbeitsplätze oder Einheiten (Unit) aus gleichzeitig zugegriffen werden kann. Eine „Einheit” in diesem Sinne ist eine Funktionseinheit, die nach Festlegung von Avaya als Grundlage für die Berechnung der Lizenzgebühr dient und bei der es sich unter anderem um einen Agenten, Port oder Nutzer, ein E-Mail-Konto oder Voicemailkonto einer natürlichen Person oder einer Unternehmenseinheit (z. B. Webmaster oder Help-Desk) oder um einen Verzeichniseintrag in der Verwaltungsdatenbank, die von dem Produkt genutzt wird, um einem Nutzer den Zugriff auf die Software zu ermöglichen, handeln kann. Einheiten können mit einem bestimmten angegebenen Server oder einer Instanz der Software verknüpft sein.

Cluster-Lizenz (CL). Ein Endbenutzer darf eine Kopie oder Instanz der Software nur auf der Anzahl von Clustern installieren oder verwenden, die auf dem Auftrag angegeben ist, dabei gilt ein Standard von einem (1) Cluster, falls nichts angegeben ist. „Ein Cluster” bezeichnet eine Gruppe von Servern und andere Ressourcen, die als einzelnes System agieren.

Enterprise-Lizenz (EN). Ein Endbenutzer darf eine Kopie oder Instanz der Software nur für die unternehmensweite Nutzung einer unbegrenzten Anzahl von Instanzen der Software installieren und verwenden, die im Auftrag angegeben ist oder soweit von Avaya schriftlich autorisiert.

Nutzer-Namenslizenz (Named User License (NU). Der Endbenutzer darf (i) die einzelnen Exemplare bzw. Instanzen der Software für jeden autorisierten, namentlich benannten Nutzer (nachstehend definiert) auf einem bestimmten Rechner oder Server installieren und nutzen, oder (ii) die einzelnen Exemplare bzw. Instanzen der Software auf einem Server installieren und nutzen, zu dem nur namentlich benannte Nutzer Zugriff haben. Ein „namentlich benannter Nutzer” bezeichnet einen Benutzer oder ein Gerät, der bzw. das von Avaya eine ausdrückliche Genehmigung zum Zugriff auf die Software und deren Nutzung erhalten hat. Nach alleinigem Ermessen von Avaya kann ein „registrierter Benutzer” ohne Einschränkung namentlich, in seiner Unternehmensfunktion (z. B. Webmaster oder Helpdesk), durch ein E-Mail-Konto oder ein Voicemailkonto im Namen einer Person oder einer Unternehmensfunktion oder als Verzeichniseintrag in einer vom Produkt verwendeten Verwaltungsdatenbank, die einem einzelnen Benutzer den Zugriff auf die Software gestattet, registriert sein.

Shrinkwrap Lizenz (Shrinkwrap License - SR). Der Endanwender ist berechtigt, Software nach Maßgabe der Bestimmungen der „Shrinkwrap” oder „Clickthrough” Lizenzen, die der Software beiliegen oder auf diese anwendbar sind, zu installieren und zu nutzen („Shrinkwrap-Lizenz”).

Heritage Nortel-Software

„Heritage Nortel-Software” bezeichnet die Software, die im Dezember 2009 von Avaya als Teil des Erwerbs von Nortel Enterprise Solutions Business übernommen wurde. Die Heritage Nortel-Software ist als Software in der Heritage Nortel-Produktliste auf https://support.avaya.com/LicenseInfo unter folgendem Link (bzw. einer von Avaya bekannt gegebenen Nachfolgeseite) zu finden: „Heritage Nortel Products”. Für die Heritage Nortel-Software gewährt Avaya dem Kunden hierunter eine Heritage Nortel-Softwarelizenz. Diese gilt jedoch lediglich im Umfang der autorisierten Aktivierungs- oder Verwendungsebene, zu den in der Dokumentation angegebenen Zwecken und eingebettet in, zur Ausführung auf oder zur Kommunikation mit Avaya-Geräten. Gebühren für Heritage Nortel-Software können auf dem Umfang der autorisierten Aktivierung oder Verwendung gemäß einer Bestellung oder Rechnung basieren.

Copyright

Das Material dieser Website, die Dokumentation, Software, der gehostete Dienst oder die Hardware, die von Avaya bereitgestellt werden, dürfen nur für die anderweitig ausdrücklich festgelegten Verwendungszwecke verwendet werden. Sämtliche der von Avaya bereitgestellten Inhalte dieser Website, die Dokumentation, der gehostete Dienst und die Produkte, einschließlich Auswahl, Layout und Design der Inhalte, sind Eigentum von Avaya oder den Lizenzgebern des Unternehmens und sind durch Urheberrechte und andere Gesetze zum Schutz geistigen Eigentums, einschließlich des Sui-Generis-Rechts zum Schutz von Datenbanken, geschützt. Es ist Ihnen nicht gestattet, den Inhalt, darunter Code und Software, zur Gänze oder teilweise zu ändern, zu kopieren, zu vervielfältigen, neu zu veröffentlichen, hochzuladen, im Internet zu veröffentlichen, zu übertragen oder zu vertreiben. Die unbefugte, ohne ausdrückliche und schriftliche Genehmigung von Avaya erfolgende Vervielfältigung, Übertragung, Verbreitung, Speicherung und/oder Nutzung kann unter dem geltenden Recht straf- oder zivilrechtlich verfolgt werden.

Virtualisierung

Die folgenden Bestimmungen sind anwendbar, wenn das Produkt auf einem virtuellen Computer bereitgestellt wird. Jedes Produkt hat einen eigenen Bestellcode und eigene Lizenztypen. Beachten Sie, dass jede Instanz eines Produkts separat lizenziert und bestellt werden muss, sofern nicht etwas anderes angegeben wird. Wenn der Endanwender-Kunde oder Avaya-Channel Partner zwei Instanzen von Produkten desselben Typs installieren möchte, dann müssen von diesem Typ zwei Produkte bestellt werden.

Komponenten von Drittanbietern

„Komponenten von Drittanbietern” sind bestimmte im Produkt enthaltene Softwareprogramme oder Teile davon oder gehostete Dienste, die Software (einschließlich Open Source-Software) enthalten können, die auf der Grundlage von Vereinbarungen mit Drittanbietern vertrieben werden („Drittanbieterkomponenten”), die möglicherweise die Rechte für bestimmte Teile des Produkts erweitern oder einschränken („Drittanbieterbestimmungen”). Informationen zum Vertrieb des Betriebssystem-Quellcodes von Linux (bei Produkten mit Linux-Quellcode) sowie zur Bestimmung der Urheberrechtsinhaber der Drittanbieterkomponenten und der geltenden Drittanbieterbestimmungen finden Sie bei den Produkten, in der Dokumentation oder auf der Website von Avaya unter https://support.avaya.com/Copyright (oder etwaigen von Avaya bekanntgegeben Nachfolger-Websites). Die Open-Source-Software-Lizenzbedingungen, die als Bestimmungen von Drittanbietern stammen, entsprechen den Lizenzrechten, die in den Lizenzbedingungen erteilt werden, und enthalten möglicherweise weitere rechtliche Vorteile für Sie, wie die Veränderung und Verbreitung der Open-Source-Software. Die Bestimmungen von Drittanbietern haben Vorrang gegenüber diesen Software-Lizenzbedingungen, jedoch nur in

Bezug auf jeweilige Drittkomponenten und nur solange die Software-Lizenzbedingungen für Sie größere Einschränkungen bedeuten als die jeweiligen Bestimmungen von Drittanbietern.

Die folgenden Bestimmungen sind anwendbar, wenn der Codec H.264 (AVC) mit dem Produkt vertrieben wird. DIESES PRODUKT WIRD IM RAHMEN DER AVC-PATENT-PORTFOLIO-LIZENZ FÜR DEN PRIVATEN ODER ANDERWEITIG UNENTGELTLICHEN GEBRAUCH DURCH ENDKUNDEN LIZENZIERT. DIE LIZENZ GEWÄHRT (i) DIE CODIERUNG VON VIDEODATEN GEMÄSS DEM AVC-STANDARD („AVC-VIDEO”) UND/ODER (ii) DIE DECODIERUNG VON AVC-VIDEODATEN, DIE VON EINEM KUNDEN ZU PRIVATEN ZWECKEN CODIERT ODER VON EINEM VIDEO-ANBIETER MIT GÜLTIGER LIZENZ FÜR DIE BEREITSTELLUNG VON AVC-VIDEO BEZOGEN WURDE. FÜR ANDERE ZWECKE WIRD WEDER EXPLIZIT NOCH IMPLIZIT EINE LIZENZ GEWÄHRT. AUSFÜHRLICHE INFORMATIONEN ERHALTEN SIE VON MPEG LA, L.L.C. UNTER HTTP://WWW.MPEGLA.COM.

Dienstanbieter

DIE FOLGENDEN BESTIMMUNGEN SIND ANWENDBAR, WENN PRODUKTE ODER SERVICES VON AVAYA VON EINEM CHANNEL PARTNER GEHOSTET WERDEN. DAS PRODUKT ODER DER GEHOSTETE SERVICE VERWENDEN MÖGLICHERWEISE KOMPONENTEN VON DRITTANBIETERN, FÜR DIE BESTIMMUNGEN VON DRITTANBIETERN GELTEN UND DIE ERFORDERN, DASS EIN DIENSTANBIETER UNMITTELBAR VON DEM DRITTANBIETER EIGENSTÄNDIG LIZENZIERT SEIN MUSS. WENN EIN AVAYA-CHANNEL PARTNER PRODUKTE VON AVAYA HOSTET, MUSS DIES SCHRIFTLICH VON AVAYA AUTORISIERT WORDEN SEIN, UND WENN DIESE GEHOSTETEN PRODUKTE BESTIMMTE SOFTWARE VON DRITTANBIETERN VERWENDEN ODER BEINHALTEN, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF MICROSOFT-SOFTWARE ODER CODECS, IST DER AVAYA-CHANNEL PARTNER VERPFLICHTET, AUF KOSTEN DES AVAYA-CHANNEL PARTNERS DIREKT VOM JEWEILIGEN DRITTANBIETER EIGENSTÄNDIG DIE ENTSPRECHENDEN LIZENZVEREINBARUNGEN ZU BESCHAFFEN.

IN BEZUG AUF CODECS GILT FOLGENDES: WENN DER AVAYA-CHANNEL PARTNER PRODUKTE HOSTET, DIE DEN CODEC G.729, H.264 ODER H.265 VERWENDEN ODER BEINHALTEN, BESTÄTIGT DER AVAYA-CHANNEL PARTNER UND ERKENNT AN, DASS DER AVAYA-CHANNEL PARTNER FÜR SÄMTLICHE ZUGEHÖRIGEN GEBÜHREN UND/ODER LIZENZGEBÜHREN AUFZUKOMMEN HAT. DER CODEC G.729 WIRD VON SIPRO LAB TELECOM INC. LIZENZIERT; SIEHE WWW.SIPRO.COM/CONTACT.HTML. DER CODEC H.264 (AVC) WIRD IM RAHMEN DER AVC-PATENT-PORTFOLIO-LIZENZ FÜR DEN PRIVATEN ODER ANDERWEITIG UNENTGELTLICHEN GEBRAUCH DURCH ENDKUNDEN LIZENZIERT. DIE LIZENZ GEWÄHRT (I) DIE CODIERUNG VON VIDEODATEN GEMÄSS DEM AVC-STANDARD („AVC-VIDEO”) UND/ODER (II) DIE DECODIERUNG VON AVC-VIDEODATEN, DIE VON EINEM KUNDEN ZU PRIVATEN ZWECKEN CODIERT ODER VON EINEM VIDEO-ANBIETER MIT GÜLTIGER LIZENZ FÜR DIE BEREITSTELLUNG VON AVC-VIDEO BEZOGEN WURDE. ES WIRD KEINE LIZENZ GEWÄHRT ODER FÜR ANDERE ZWECKE IMPLIZIERT. WEITERE INFORMATIONEN ZU DEN CODECS H.264 (AVC) UND H. 265 (HEVC) ERHALTEN SIE VON MPEG LA, L.L.C. UNTER HTTP://WWW.MPEGLA.COM.

Einhaltung der Gesetze

Der Kunde bestätigt und erkennt an, dass er verpflichtet ist, alle geltenden Gesetze und Vorschriften, einschließlich der Gesetze und Vorschriften in Bezug auf das Aufzeichnen von Anrufen, Datenschutz, geistiges Eigentum, Geschäftsgeheimnisse, Betrug und Musikaufführungsrechte, in dem Land oder Gebiet einzuhalten, in dem das Avaya-Produkt verwendet wird.

Gebührenbetrug verhindern

„Gebührenbetrug“ ist die unbefugte Nutzung Ihres Telekommunikationssystems durch eine dazu nicht berechtigte Person (z. B. jemand, der kein Mitarbeiter, Vertreter, Auftragnehmer Ihres

Unternehmens oder anderweitig im Auftrag Ihres Unternehmens tätig ist). Sie sollten sich darüber im Klaren sein, dass Gebührenbetrug in Verbindung mit Ihrem System möglich ist und gegebenenfalls zu erheblichen zusätzlichen Gebühren für Ihre Telekommunikationsdienste führen kann.

Avaya-Hilfe bei Gebührenbetrug

Wenn Sie den Verdacht haben, dass Sie Opfer von Gebührenbetrug sind und technische Unterstützung benötigen, rufen Sie die Hotline für Gebührenbetrug des Technical Service Center an: +1-800-643-2353 (USA und Kanada). Weitere Support-Telefonnummern finden Sie auf der Avaya-Support-Website unter https://support.avaya.com bzw. auf einer von Avaya bekannt gegebenen Nachfolgeseite.

Sicherheitsrisiken

Informationen zu den Sicherheits-Supportrichtlinien von Avaya finden Sie unter https://support.avaya.com/security im Abschnitt „Security Policies and Support“.

Mutmaßliche Sicherheitsrisiken in Bezug auf Avaya-Produkte werden nach dem Supportverfahren für die Avaya-Produktsicherheit gehandhabt (https://support.avaya.com/css/P8/documents/100161515).

Herunterladen der Dokumentation

Die aktuellsten Versionen der Dokumentation finden Sie auf der Avaya-Support-Website unter https://support.avaya.com bzw. auf einer von Avaya bekannt gegebenen Nachfolgeseite.

Avaya-Support

Mitteilungen zu Produkten und gehosteten Diensten sowie Artikel finden Sie auf der Support-Website von Avaya: https://support.avaya.com. Dort können Sie auch Probleme mit Ihrem Avaya-Produkt oder Ihrem gehosteten Dienst melden. Eine Liste mit Support-Telefonnummern und Kontaktadressen finden Sie auf der Support-Website von Avaya unter https://support.avaya.com (bzw. auf einer von Avaya bekannt gegebenen Nachfolgeseite). Scrollen Sie ans Ende der Seite, und wählen Sie „Contact Avaya Support“ aus.

Marken

Die auf dieser Website, in der/den Dokumentation(en), den gehosteten Diensten und im/in den Produkt(en) von Avaya enthaltenen Marken, Logos und Dienstleistungsmarken („Marken”) sind eingetragene oder nicht eingetragene Marken von Avaya, seinen Partnern oder anderen Drittparteien. Die Nutzung dieser Marken ist nur nach vorheriger schriftlicher Genehmigung von Avaya oder der betreffenden Drittpartei, die Eigentümer der Marke ist, gestattet. Der Inhalt dieser Website, der Dokumentation(en), den gehosteten Diensten und des/der Produkt(e) darf keinesfalls dahingehend ausgelegt werden, dass stillschweigend, durch Verwirkung oder auf andere Weise eine Lizenz oder ein Recht an den Marken ohne die ausdrückliche und schriftliche Genehmigung von Avaya oder der betreffenden Drittpartei gewährt wird.

Avaya ist eine eingetragene Marke von Avaya Inc.

Alle Nicht-Avaya-Markennamen sind Eigentum der jeweiligen Inhaber. Linux® ist eine eingetragene Handelsmarke von Linus Torvalds in den USA und anderen Ländern.

Index

T

U

W

Z