Bereitstellen von Remote IP Office SIP-Telefonen mit ASBCE

Version 12.0
Ausgabe 14
April 2024

Hinweis

Es wurden angemessene Anstrengungen unternommen, um sicherzustellen, dass die in diesem Dokument enthaltenen Informationen vollständig und korrekt sind. Avaya 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

„DOKUMENTATION": Dies bezieht sich auf in Form verschiedener Medien veröffentlichte Informationen, die den Benutzern allgemein zugänglich gemacht werden; hierzu können Produktinformationen, Abonnement- oder Dienstleistungsbeschreibungen, Bedienungsanleitungen und Leistungsspezifikationen gehören. Der Begriff „Dokumentation" schließt Marketingmaterialien nicht mit ein. Avaya haftet nur dann für Änderungen, Ergänzungen oder Streichungen der ursprünglich veröffentlichten Fassung dieser Dokumentation, wenn diese Änderungen, Ergänzungen und Streichungen von Avaya selbst oder in ausdrücklichem Auftrag 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 ist nicht verantwortlich für den Inhalt oder die Korrektheit verknüpfter Websites, auf welche auf dieser Website bzw. in dieser/n von Avaya bereitgestellten Dokumentation(en) verwiesen 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 garantiert nicht, dass diese Links jederzeit funktionieren, und hat keinen Einfluss auf die Verfügbarkeit dieser Websites.

Garantie

Avaya gewährt eine eingeschränkte Gewährleistung für Hardware und Software von Avaya. Die Bedingungen der eingeschränkten Gewährleistung können Sie Ihrem mit Avaya geschlossenen Kaufvertrag entnehmen. Darüber hinaus stehen Avaya-Kunden und Dritten die Standard-Gewährleistungsbedingungen 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 „Gewährleistung und Produktlebenszyklus" bzw. auf einer von Avaya bekannt gegebenen Nachfolgeseite zur Verfügung. Beachten Sie hierbei: Bei Erwerb des Produktes/der Produkte von einem Avaya-Channel Partner außerhalb der Vereinigten Staaten und Kanada wird die Gewährleistung von diesem Avaya-Channel Partner und nicht direkt von Avaya erbracht.

„**Gehostete Dienste**": Dies bezeichnet das Abonnement eines von Avayagehosteten Dienstes, das Sie von Avaya oder (ggf.) einem autorisierten Avaya-Channel Partner erworben haben und das in SAS- oder sonstigen Servicebeschreibungen bezüglich des betreffenden gehosteten Dienstes näher beschrieben wird. Wenn Sie ein Abonnement eines gehosteten Dienstes 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 NUR, WENN SIE EIN ABONNEMENT FÜR EINEN VON AVAYA GEHOSTETEN DIENST VON AVAYA ODER EINEM AVAYA-CHANNEL PARTNER (FALLS ZUTREFFEND) ERWERBEN. DIE NUTZUNGSBEDINGUNGEN DER GEHOSTETEN DIENSTE SIND AUF DER AVAYA-WEBSITE HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNTER DEM LINK „Avaya-Nutzungsbedingungen für gehostete Dienste" ODER ETWAIGEN VON AVAYA BEKANNT GEGEBENEN NACHFOLGESEITEN 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 (IM NACHFOLGENDEN ENTWEDER „SIE" ODER DER „ENDNUTZER" BEZEICHNET) DEN NUTZUNGSBEDINGUNGEN ZU. WENN SIE DEN NUTZUNGSBEDINGUNGEN IM NAMEN EINES UNTERNEHMENS ODER EINER ANDEREN RECHTSPERSON 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 AUF DEN GEHOSTETEN DIENST WEDER ZUGREIFEN NOCH IHN NUTZEN UND NIEMANDEN AUTORISIEREN, AUF DEN GEHOSTETEN DIENST ZUZUGREIFEN ODER IHN ZU NUTZEN.

Lizenzen

Die globalen Software-Lizenzbedingungen („Software-Lizenzbedingungen") sind auf der folgenden Website https://www.avaya.com/en/legal-license-terms/ oder auf einer von Avaya benannten Nachfolgeseite verfügbar. Diese Software-Lizenzbedingungen gelten für alle, die Software und/oder Dokumentation installieren, herunterladen und/oder verwenden. Durch Installieren, Herunterladen oder Nutzen der Software, oder Autorisierung anderer dazu, stimmt der Endbenutzer zu, dass die Software-Lizenzbedingungen einen bindenden Vertrag zwischen ihm und Avaya darstellen. Sofern der Endbenutzer die Software-Lizenzbedingungen im Auftrag eines Unternehmens oder einer anderen Rechtsperson akzeptiert, erklärt er, dazu bevollmächtigt zu sein, das Unternehmen oder die Rechtsperson an die Software-Lizenzbedingungen rechtlich zu binden.

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 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, es sei denn mit ausdrücklicher Genehmigung von Avaya. Die unbefugte Vervielfältigung, Übertragung, Verbreitung, Speicherung oder Nutzung ohne ausdrückliche schriftliche Genehmigung von Avaya 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. Sofern nicht anders angegeben, muss jede Instanz eines Produkts separat lizenziert und bestellt werden. 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

Das Folgende gilt nur, wenn der H.264 (AVC)-Codec 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 WURDEN. ES WERDEN KEINE LIZENZEN FÜR ANDERE ZWECKE ERTEILT ODER GEWÄHRT. AUSFÜHRLICHERE INFORMATIONEN ERHALTEN SIE VON MPEG LA, L.L.C. UNTER HTTP://WWW.MPEGLA.COM.

Dienstanbieter

FOLGENDES GILT FÜR CODECS: WENN DER AVAYA CHANNEL PARTNER PRODUKTE HOSTET, DIE DIE CODECS H.264 ODER H.265 VERWENDEN BZW. IN DIE DIESE CODECS EINGEBETTET SIND, AKZEPTIERT UND BESTÄTIGT DER AVAYA CHANNEL PARTNER, DASS ER SELBST FÜR SÄMTLICHE LIZENZ- UND/ODER ANDERE GEBÜHREN IM ZUSAMMENHANG MIT DIESEN CODECS VERANTWORTLICH IST. DER H.264 (AVC)-CODEC 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 WURDEN. ES WERDEN KEINE LIZENZEN FÜR ANDERE ZWECKE ERTEILT ODER GEWÄHRT. 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

Sie nehmen zur Kenntnis und bestätigen, dass Sie für die Einhaltung der geltenden Gesetze und Vorschriften verantwortlich sind, einschließlich, aber nicht beschränkt auf Gesetze und Vorschriften in Bezug auf Anrufaufzeichnung, Datenschutz, geistiges Eigentum, Betriebsgeheimnisse, Betrug und Aufführungsrechte in dem Land oder Gebiet, in dem das Avaya-Produkt verwendet wird.

Gebührenbetrug verhindern

„Gebührenhinterziehung” ist die unberechtigte Nutzung Ihres Telekommunikationssystems durch eine unberechtigte Partei (z. B. Personen, die keine Angestellten, Handlungsbevollmächtigten oder Auftragnehmer sind und die nicht im Auftrag Ihrer Firma arbeiten). 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 vermuten, dass Sie Opfer von Gebührenbetrug geworden sind und technische Unterstützung oder Unterstützung benötigen, wenden Sie sich bitte an Ihren Avaya-Vertriebsmitarbeiter.

Sicherheitsrisiken

Informationen zu den Avaya-Support-Richtlinien zur Sicherheit finden Sie im Bereich „Security Policies and Support“ unter https://support.avaya.com/security.

Verdächtige Sicherheitsschwachstellen bei Avaya-Produkten werden gemäß Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515) gehandhabt.

Marken

Die auf dieser Website, in der Dokumentation, den gehosteten Diensten und in den Produkten von Avaya enthaltenen Marken, Logos und Dienstleistungsmarken („Marken”) sind eingetragene oder nicht eingetragene Marken von Avaya, seinen Partnern, seinen Lizenzgebern, seinen Lieferanten 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. Ohne ausdrückliche schriftliche Genehmigung durch Avaya bzw. des jeweiligen Drittanbieters erteilen die Website, die Dokumentation, die gehosteten Dienste und Produkte weder stillschweigend noch durch Rechtsverwirkung eine Lizenz oder ein sonstiges Recht bezüglich der Marken.

Avaya ist eine eingetragene Marke von Avaya LLC.

Alle Nicht-Avaya-Markennamen sind Eigentum der jeweiligen Inhaber.

Linux® ist eine eingetragene Handelsmarke von Linus Torvalds in den USA und anderen Ländern.

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 kontaktieren

Mitteilungen und Artikel zu Produkten und gehosteten Diensten finden Sie auf der Avaya-Support-Website: https://support.avaya.com. Dort können Sie auch Probleme mit Ihrem Avaya-Produkt oder 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 „Avaya-Support kontaktieren“ aus.

Inhalt

Teil 1: Unterstützung von entfernten SIP-Nebenstellen

Kapitel 1: Unterstützung von Remote-SIP-Nebenstellen auf IP Office

In diesem Abschnitt finden Sie ein Beispiel für die Unterstützung von Remote-SIP-Nebenstellen, die über ein Avaya Session Border Controller (ASBCE) mit einem IP Office verbunden werden. Das ASBCE bietet eine Reihe von Funktionen, die dem Verbindungsprozess zusätzliche Sicherheit bieten.

- Dieses Dokument basiert auf IP Office R11.1.3.1 und ASBCE R10.1.2.
- Für IP Office R11.1.3.1 unterstützt das IP Office IPv6 iOS und Android Avaya Workplace-Client Remote-Nebenstellen mit IPv6. Andernfalls unterstützt IP Office nur IPv4-Remote-Nebenstellen.

Unterstützte SIP-Remote-Nebenstellen

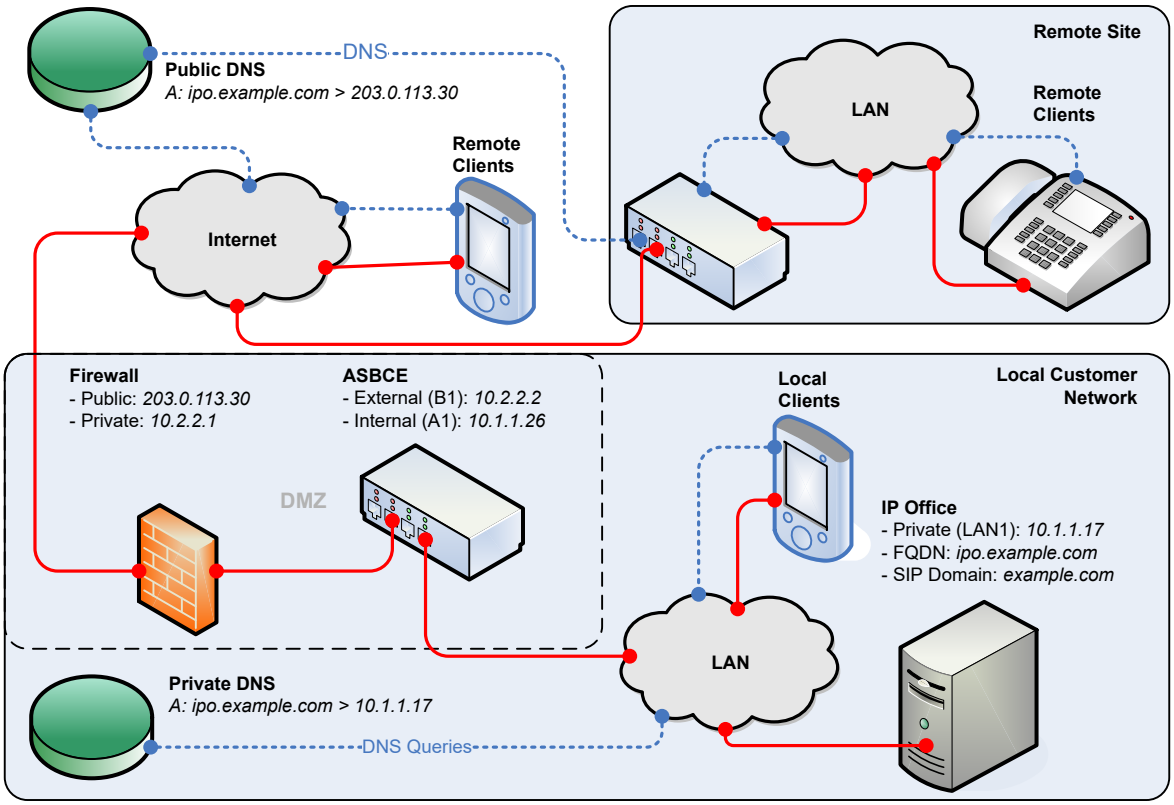
SIP-Schreibtischtelefone	SIP-Softphones
• Telefone der Serie J100 • Telefone der Serie K100 (Avaya Vantage™)	• Avaya Workplace-Client

Verwandte Links

Beispielschema auf Seite 7
Sicherheitsüberlegungen auf Seite 9

Beispielschema

Dieses Schema zeigt das in diesem Dokument verwendete Beispielszenario:



- In diesem Szenario sind die SIP-Nebenstellen Telefone und Avaya Workplace-Client Softphones der Serie J100.
- IP Office ist der SIP-Registrar.
  - In diesem Beispiel wird TLS für die SIP-Verbindungen verwendet. Dazu müssen die IP Office Zertifikate und die Bereitstellung der Zertifikate für das ASBCE berücksichtigt werden.
- Das ASBCE verfügt über öffentliche und private IP-Schnittstellen. Mit diesen fungiert es als Gateway für SIP-Datenverkehr zwischen dem privaten Netzwerk des Kunden und dem öffentlichen Internet.
  - Bei interner Verwendung verbinden sich die SIP-Clients direkt mit dem IP Office.
  - Bei externer Verwendung verbinden sich die SIP-Clients über ASBCE mit dem IP Office.
  - Das ASBCE leitet auch Anfragen nach Dateien weiter, die von den Remote-SIP-Nebenstellen verwendet werden. Zum Beispiel Anforderungen für `.txt`- und `.xml`-Dateien.
- Das Kundennetzwerk umfasst eine Firewall zwischen sich selbst und dem öffentlichen Internet. Avaya empfiehlt dies für eine verbesserte Sicherheit.
  - Die Firewall leitet Datenverkehr von Remote-Nebenstellen an ASBCE weiter.
- Die DNS-Lösung des Kunden stellt Split-DNS bereit. Das heißt:
  - Im privaten Netzwerk des Kunden löst DNS den FQDN des IP Office auf die IP-Adresse des IP Office auf.
  - Im öffentlichen Internet löst DNS den FQDN des IP Office in die öffentliche IP-Adresse der Firewall des Kunden auf.

Verwandte Links

Unterstützung von Remote-SIP-Nebenstellen auf IP Office auf Seite 7

Sicherheitsüberlegungen

Jedes Szenario, in dem Sie IP Office mit dem öffentlichen Internet verbinden, muss die Sicherheit berücksichtigen. IP Office Sicherheitsoptionen und -anforderungen werden im Avaya IP Office™ Platform Sicherheitsrichtlinien Handbuch behandelt.

In diesem Fall macht die Verbindung mit ASBCE eine Reihe zusätzlicher Sicherheitsoptionen verfügbar.

- **Abgleich des User Agents**

  Sie können konfigurieren, welche User-Agent-Zeichenfolgen über ASBCE verbunden werden können. Auf diese Weise können Sie nur Verbindungen von bekannten Anwendungen und Geräten unterstützen. Siehe Konfigurieren eines User-Agent-Profils auf Seite 51.

- **Anwendungsregeln**

  Sie können Anwendungsregeln verwenden, um zu konfigurieren, welchen Medientyp Ihre Verbindungen unterstützen, die maximale Anzahl von Verbindungen und die maximale Anzahl von Verbindungen pro Remote-Nebenstelle. Siehe Erstellen einer Anwendungsregel auf Seite 46.

- **IP/URL-Sperrlisten**

  Sie können diese verwenden, um IP-Adressen oder URLs zu blockieren, bei denen die Benutzername- oder Kennwortregistrierung wiederholt fehlschlägt. Siehe Erstellen einer IP/URI-Blockliste auf Seite 45.

Verwandte Links

Unterstützung von Remote-SIP-Nebenstellen auf IP Office auf Seite 7

Kapitel 2: IP Office Konfiguration für SIP-Remote-Nebenstellen

Dieser Abschnitt enthält eine allgemeine Zusammenfassung der IP Office Konfiguration zur Unterstützung der Remote-SIP-Nebenstellenverbindung über ein ASBCE.

Verwandte Links

IP Office-Konfigurationsprüfliste auf Seite 10
Lizenzen und Abonnements auf Seite 11
IP Office SIP VoIP-Einrichtung auf Seite 11
Festlegen der ASBCE Informationen, die vom IP Office an die Remote-Nebenstellen weitergegeben werden auf Seite 13
Hinzufügen zusätzlicher Einstellungen für Remote-Nebenstellen auf Seite 15
ASBCE zur Whitelist hinzufügen auf Seite 16

IP Office-Konfigurationsprüfliste

#	Aktion	Link/Hinweise	✔
1.	Überprüfen Sie die SIP-VoIP-Einstellungen	Siehe IP Office SIP VoIP-Einrichtung auf Seite 11.	
2.	Einstellung für Remote-Nebenstellen hinzufügen	Siehe Festlegen der ASBCE Informationen, die vom IP Office an die Remote-Nebenstellen weitergegeben werden auf Seite 13.	
3.	Legen Sie die NoUser-Ausgangsnummern fest	Siehe Hinzufügen zusätzlicher Einstellungen für Remote-Nebenstellen auf Seite 15.	
4.	ASBCE der Whitelist hinzufügen	Verhindern, dass IP Office das ASBCE blockiert. Siehe ASBCE zur Whitelist hinzufügen auf Seite 16.	

Verwandte Links

IP Office Konfiguration für SIP-Remote-Nebenstellen auf Seite 10

Lizenzen und Abonnements

Das IP Office benötigt keine zusätzlichen Lizenzen, um den Betrieb mit einem ASBCE zu unterstützen. Die Telefone und Anwendungen, die mit dem IP Office über ASBCE verbunden sind, verwenden dieselben Lizenzen oder Abonnements wie für den lokalen Betrieb.

Verwandte Links

IP Office Konfiguration für SIP-Remote-Nebenstellen auf Seite 10

IP Office SIP VoIP-Einrichtung

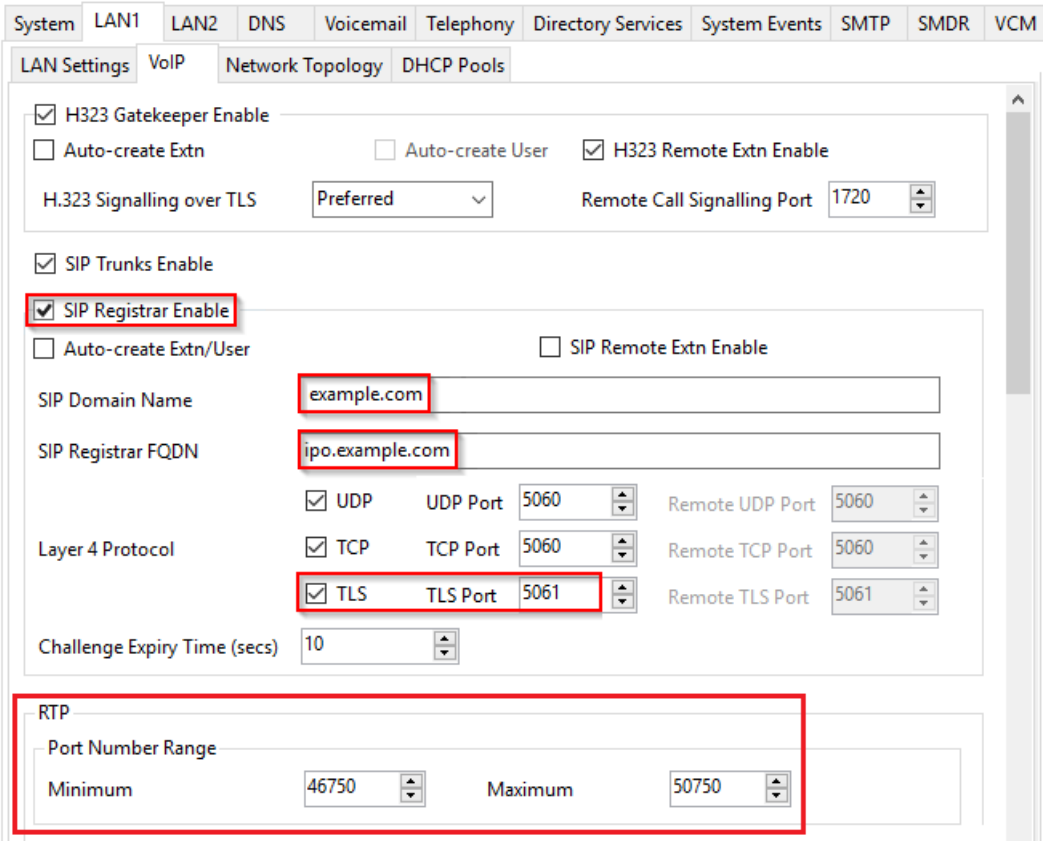
Im folgenden Beispielszenario wird die IP Office Konfiguration zur Unterstützung von SIP-Nebenstellen verwendet. Diese Konfiguration ist für lokale und Remote-SIP-Nebenstellen gleich.

Wichtig:

- Zur Änderung dieser Einstellungen ist ein Neustart von IP Office erforderlich.

Vorgehensweise

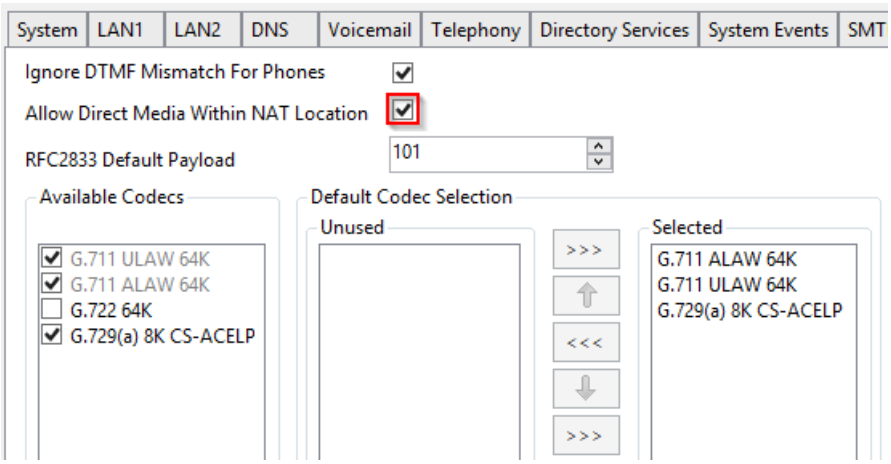
1. Melden Sie sich am IP Office mit IP Office Manager oder IP Office Web Manager an.
2. Wählen Sie **System** oder **Systemeinstellungen** > **System**.
3. Wählen Sie die Registerkarte **LAN1**.



Feld	Beschreibung
SIP-Registrar aktivieren	Ermöglicht die Registrierung von SIP-Nebenstellen beim IP Office.
SIP-Remote-Nst. aktivieren	Deaktivieren. ASBCE verwaltet NAT-Verbindungen von Remote-Nebenstellen.
SIP-Domainname	Legt die Domäne fest, die SIP-Clients für die Registrierung verwenden müssen.
SIP-Registrar FQDN	Legt den vollqualifizierten Domänennamen für das Routing von SIP-Verbindungen an IP Office fest.
Layer-4-Protokoll	Legt die Layer-4-Protokolle und -Ports fest, auf denen das IP Office den SIP-Nebenstellenverkehr abhört.
Portnummerbereich	Legt den Portnummernbereich fest, den das IP Office für RTP- und RTCP-Datenverkehr verwendet.

4. Wählen Sie die untergeordnete Registerkarte **VoIP** aus.

   Aktivieren Sie das Kontrollkästchen **Direktverbindungen mit NAT-Standort zulassen**.



   - Wenn Sie dies aktivieren, können sich Direktverbindungen zwischen Geräten im selben Subnetz befinden, die sich mit NAT mit dem IP Office verbinden. Die Unterstützung über ASBCE erfordert eine zusätzliche Konfiguration, damit sich das ASBCE von den Anrufmedien lösen kann, siehe Aufheben der Verbindung mit Anrufmedien über das ASBCE auf Seite 62.

5. Klicken Sie auf **OK** oder **Update**.
6. Speichern Sie die Einstellungen und starten Sie das IP Office System neu:
   - Wenn Sie IP Office Manager verwenden, speichern Sie die Einstellungen und starten Sie das System neu.
   - Wenn Sie IP Office Web Manager verwenden, klicken Sie auf **In IP Office speichern** und starten Sie das System neu.

Verwandte Links

IP Office Konfiguration für SIP-Remote-Nebenstellen auf Seite 10

Festlegen der ASBCE Informationen, die vom IP Office an die Remote-Nebenstellen weitergegeben werden

Vor der Registrierung beim IP Office fordern Avaya-Nebenstellen die Datei `46xxsettings.txt` an. Diese Datei enthält Einstellungen, die die Nebenstellen verwenden.

Bei Remote-Nebenstellen muss die von IP Office automatisch generierte Datei `46xxsettings.txt` die Adressinformationen enthalten, die die Remote-Nebenstelle zur Verbindung mit ASBCE verwenden kann.

- Nebenstellen fordern die Datei `46xxsettings.txt` an, wenn sie sich zum ersten Mal beim IP Office registrieren.
- Nach Erhalt der Datei `46xxsettings.txt` fordern Nebenstellen die Datei standardmäßig alle 24 Stunden erneut an, um Änderungen anzuwenden.
- Nebenstellen fordern die Datei auch bei jedem Neustart an. Sie können sie entfernt mit SysMonitor oder System Status Application neu starten.

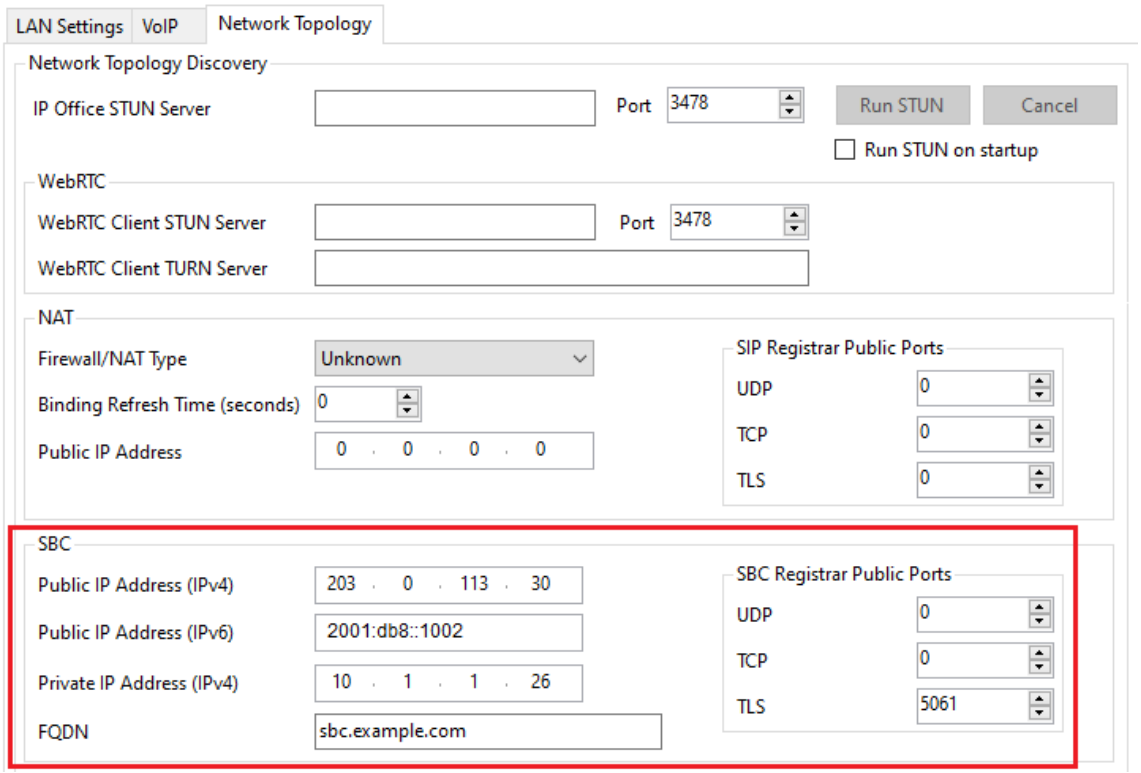
Wichtig:

- Zur Änderung dieser Einstellungen ist ein Neustart von IP Office erforderlich.

Vorgehensweise

1. Melden Sie sich am IP Office mit IP Office Manager oder IP Office Web Manager an.
2. Wählen Sie **System** oder **Systemeinstellungen** > **System**.
3. Wählen Sie das LAN (**LAN1** oder **LAN2**), das mit demselben Netzwerk wie das ASBCE verbunden ist.
4. Wählen Sie **Netzwerktopologie** aus.
   - Wenn Sie IP Office Web Manager verwenden, können Sie diese Einstellungen nur im Offline-Modus ändern. Klicken Sie auf das Symbol und wählen Sie **Offline-Modus** aus.

5. Geben Sie im Abschnitt **SBC** die folgenden Informationen ein:



Einstellung	Beschreibung
Öffentliche IP-Adresse (IPv4)	Die öffentliche IPv4-Adresse für eingehenden SIP-Client-Datenverkehr in das Kundennetzwerk. • Dies ist die öffentliche IPv4-Adresse des ASBCE oder des internetfähigen Dienstes, wie z. B. der Kunden-Firewall. • Der externe DNS muss den FQDN des IP Office auf diese Adresse auflösen, wenn dies von einer IPv4-Remote-Nebenstelle angefordert wird.
Öffentliche IP-Adresse (IPv6)	Die öffentliche IPv6-Adresse für eingehenden SIP-Client-Datenverkehr in das Kundennetzwerk, wie oben beschrieben. Weitere Informationen finden Sie unter Unterstützung von IPv6-Remote-Nebenstellen auf Seite 73. • Dies ist die öffentliche IPv6-Adresse des ASBCE oder des internetgerichteten Dienstes, wie z. B. der Kunden-Firewall. • Der externe DNS muss den FQDN des IP Office auf diese Adresse auflösen, wenn dies von einer IPv6-Remote-Nebenstelle angefordert wird.
Private IP-Adresse (IPv4)	Die private/interne IPv4-Adresse des ASBCE. • Der interne DNS muss **FQDN** auf diese Adresse auflösen.
FQDN	Der vollqualifizierte Domänenname des ASBCE. Der DNS muss diesen FQDN auf die verwendeten IPv6-Adressen auflösen (IPv4 verwendet den FQDN des IP Office SIP-Registrars).
SIP-Registrar Öffentliche Ports	Die öffentlichen (externen) **TCP**-, **TLS**- und/oder **UDP**-Ports, die externe SIP-Clients verwenden müssen, um eine Verbindung mit dem ASBCE herzustellen.

6. Klicken Sie auf **OK** oder **Update**.

7. Speichern Sie die Einstellungen und starten Sie das IP Office System neu:
   - Wenn Sie IP Office Manager verwenden, speichern Sie die Einstellungen und starten Sie das System neu.
   - Wenn Sie IP Office Web Manager verwenden, klicken Sie auf **In IP Office speichern** und starten Sie das System neu.

Verwandte Links

IP Office Konfiguration für SIP-Remote-Nebenstellen auf Seite 10

Hinzufügen zusätzlicher Einstellungen für Remote-Nebenstellen

Sie können die folgenden **NoUser**-Ausgangsnummern verwenden, um zusätzliche Werte in der automatisch generierten Datei `46xxsettings.txt` festzulegen, die IP Office für Remote-Nebenstellen bereitstellt.

Vorgehensweise

1. Melden Sie sich am IP Office mit IP Office Manager oder IP Office Web Manager an.
2. Klicken Sie auf **Benutzer** oder **Anrufverwaltung** > **Benutzer**.
3. Suchen Sie nach den Einstellungen für den Benutzer namens *NoUser*.
4. Wählen Sie **Ausgangsnummern** aus.
5. Fügen Sie die erforderlichen zusätzlichen *NoUser* Ausgangsnummern hinzu:
   - **SET_STIMULUS_SBC_REG_INTERVAL=**`<seconds>`

     Diese *NoUser* Ausgangsnummer legt das von Telefonen der Serie J100 verwendete Registrierungsintervall fest. Die Standardeinstellung ist 3600 Sekunden (1 Stunde). Wenn Sie Telefone über ASBCE unterstützen, beträgt der empfohlene Wert 180 Sekunden. Der unterstützte Bereich beträgt 180 bis 3600 Sekunden.
   - **PUBLIC_HTTP=**`<file server address>`

     Bei Verwendung der Einstellungen **IP-Adresse des HTTP-Servers** und **HTTP-Umleitung** verwendet IP Office diesen Wert, um die Adresse des öffentlichen Dateiservers festzulegen, die Remote-Nebenstellen mitgeteilt wird.
6. Klicken Sie auf **OK** oder **Update**.
7. Speichern Sie die Einstellungen und starten Sie das IP Office System neu:
   - Wenn Sie IP Office Manager verwenden, speichern Sie die Einstellungen und starten Sie das System neu.
   - Wenn Sie IP Office Web Manager verwenden, klicken Sie auf **In IP Office speichern** und starten Sie das System neu.

Verwandte Links

IP Office Konfiguration für SIP-Remote-Nebenstellen auf Seite 10

ASBCE zur Whitelist hinzufügen

Wenn die Remote-Nebenstelle über ASBCEeine Verbindung mit dem IP Office herstellt, können falsche Registrierungsversuche dazu führen, dass IP Office die ASBCE IP-Adresse blockiert.

Vorgehensweise

1. Melden Sie sich am IP Office mit IP Office Manager oder IP Office Web Manager an.
2. Wählen Sie **System** oder **Systemeinstellungen** > **System**.
3. Wählen Sie **VoIP** > **Zugriffssteuerungslisten** aus.
4. Fügen Sie die interne IP-Adresse des ASBCE zum **IP-Whitelist** hinzu.
5. Klicken Sie auf **OK** oder **Update**.
6. Wenn Sie IP Office Manager verwenden, speichern Sie die Einstellungen im IP Office System.

Verwandte Links

IP Office Konfiguration für SIP-Remote-Nebenstellen auf Seite 10

Kapitel 3: Hinzufügen von IP Office Zertifikaten zum ASBCE

Im Beispielszenario verwendet IP Office sein selbstsigniertes Zertifikat. In diesem Fall benötigt das ASBCE:

- Eine Kopie des IP Office Stammzertifikats. Dies ist die Zertifizierungsstelle (CA).
- Ein Identitätszertifikat für das ASBCE, das von IP Office ausgestellt wurde.
  - **Für IPv4:** Das Zertifikat muss die IP Office FQDN (CN oder SAN)- und IPv4 (SAN)-Adresse enthalten.
  - **Für IPv6:** Zusätzlich zur IP Office FQDN- und IPv4-Adresse muss das ASBCE Identitätszertifikat den ASBCE FQDN und die IPv6-Adresse enthalten.

Verwenden von Zertifikaten von Drittanbietern

Wenn IP Office von einer Drittanbieter-CA ausgestellte Zertifikate verwendet, müssen die für das ASBCE erforderlichen Wurzel- und Identitätszertifikate von dieser CA ausgestellt werden. Die Grundsätze für die im Identitätszertifikat erforderlichen Details bleiben jedoch dieselben, die in diesem Abschnitt der Dokumentation beschrieben sind.

Verwandte Links

ASBCE Zertifikat-Checkliste auf Seite 17
Herunterladen des IP Office-Stammzertifikats auf Seite 18
Hinzufügen des IP Office-Stammzertifikats zum ASBCE auf Seite 19
Erstellen eines ASBCE Identitätszertifikats mithilfe von IP Office Web Manager auf Seite 19
Erstellen eines ASBCE Identitätszertifikats mit Web Control (Plattformansicht) auf Seite 20
Aufteilen des ASBCE Identitätszertifikats auf Seite 21
Hinzufügen des Identitätszertifikats zum ASBCE auf Seite 23

ASBCE Zertifikat-Checkliste

#	Aktion	Link/Hinweise	✔
1.	IP Office Stammzertifikat herunterladen	Siehe Herunterladen des IP Office-Stammzertifikats auf Seite 18.	
2.	Fügen Sie das Stammzertifikat zum ASBCE hinzu.	Siehe Hinzufügen des IP Office-Stammzertifikats zum ASBCE auf Seite 19.	

Die Tabelle wird auf der nächsten Seite fortgesetzt …

#	Aktion	Link/Hinweise	✔
3.	Erstellen Sie ein Identitätszertifikat für das ASBCE	Siehe Erstellen eines ASBCE Identitätszertifikats mithilfe von IP Office Web Manager auf Seite 19.	
4.	Zertifikat aufteilen	Extrahieren Sie separate Zertifikate und private Schlüsseldateien aus dem Identitätszertifikat. Siehe Aufteilen des ASBCE Identitätszertifikats auf Seite 21.	
5.	Fügen Sie die Dateien zum ASBCE hinzu.	Fügen Sie das Identitätszertifikat und die privaten Schlüsseldateien zum ASBCE hinzu. Siehe Hinzufügen des Identitätszertifikats zum ASBCE auf Seite 23.	

Verwandte Links

Hinzufügen von IP Office Zertifikaten zum ASBCE auf Seite 17

Herunterladen des IP Office-Stammzertifikats

Gehen Sie wie folgt vor, um eine Kopie des IP Office Stammzertifikats herunterzuladen.

Vorgehensweise

1. Melden Sie sich mit IP Office Web Manager bei an IP Office.
   - Geben Sie bei einem IP500 V2 die Systemadresse gefolgt von `:8443/WebMgmtEE/WebManagerment.html` ein.
   - Geben Sie bei Linux-basierten Servern die Systemadresse gefolgt von `:7070/WebManagement/WebManagement.html` ein.
2. Wählen Sie **Sicherheit** > **Sicherheitseinstellungen** aus.
3. Wenn sich das IP Office in einem Netzwerk mit mehreren Standorten befindet, klicken Sie auf das ✎ neben dem erforderlichen IP Office.
4. Wählen Sie **Zertifikate** aus.
5. Suchen Sie in **Vertrauenswürdiger Zertifikatspeicher** das Stammzertifikat, das das IP Office System verwendet.
6. Klicken Sie auf das Symbol ⬇ neben dem Zertifikat.
7. Klicken Sie auf **Ja**.
8. Benennen Sie die Datei in `IPO_RootCA.crt` um.

Weitere Schritte

- Gehen Sie auf Hinzufügen des IP Office-Stammzertifikats zum ASBCE auf Seite 19.

Verwandte Links

Hinzufügen von IP Office Zertifikaten zum ASBCE auf Seite 17

Hinzufügen des IP Office-Stammzertifikats zum ASBCE

Gehen Sie wie folgt vor, um die Kopie des IP Office Stammzertifikats in ASBCE hochzuladen.

Voraussetzungen

- Laden Sie das IP Office Stammzertifikat herunter. Siehe Herunterladen des IP Office-Stammzertifikats auf Seite 18.

Vorgehensweise

1. Gehen Sie auf **TLS-Verwaltung** > **Zertifikate**.
2. Klicken Sie auf **Installieren**.
3. Setzen Sie **Typ** auf **CA-Zertifikat**.
4. Geben Sie einen aussagekräftigen Namen für das Zertifikat ein.
5. Aktivieren Sie **Schwaches Zertifikat/schwachen Schlüssel zulassen**.
6. Klicken Sie auf **Datei auswählen** und wählen Sie die Datei `IPO_RootCA.crt` aus.
7. Klicken Sie auf **Hochladen**. Das Menü zeigt eine Warnung an, dass es sich um ein selbstsigniertes Zertifikat handelt.
8. Klicken Sie auf **Fortfahren**. Das Menü zeigt das Zertifikat an.
9. Klicken Sie auf **Installieren**.
10. Klicken Sie auf **Beenden**.

Weitere Schritte

- Verwenden Sie IP Office, um ein Identitätszertifikat für das ASBCE zu erstellen:
  - Informationen zu Abonnementsystemen finden Sie unter Erstellen eines ASBCE Identitätszertifikats mithilfe von IP Office Web Manager auf Seite 19.
  - Weitere Systeme finden Sie unter Erstellen eines ASBCE Identitätszertifikats mit Web Control (Plattformansicht) auf Seite 20.

Verwandte Links

Hinzufügen von IP Office Zertifikaten zum ASBCE auf Seite 17

Erstellen eines ASBCE Identitätszertifikats mithilfe von IP Office Web Manager

Dieser Vorgang generiert ein Identitätszertifikat für das ASBCE mithilfe von IP Office Web Manager.

- Dieser Prozess gilt für IP Office Systeme im Abonnementmodus mit der **automatischen Zertifikatverwaltung**. Weitere Systeme finden Sie unter Erstellen eines ASBCE Identitätszertifikats mit Web Control (Plattformansicht) auf Seite 20.

Vorgehensweise

1. Melden Sie sich mit IP Office Web Manager beim System an.
   - Geben Sie bei einem IP500 V2 die Systemadresse gefolgt von `:8443/WebMgmtEE/WebManagerment.html` ein.
   - Geben Sie bei Linux-basierten Servern die Systemadresse gefolgt von `:7070/WebManagement/WebManagement.html` ein.
2. Wählen Sie **Sicherheit** > **Sicherheitseinstellungen** aus.
3. Wenn sich das IP Office in einem Netzwerk mit mehreren Standorten befindet, klicken Sie auf das neben dem erforderlichen IP Office.
4. Wählen Sie **Zertifikate** aus.
5. Klicken Sie auf **Neu generieren**.
6. Wählen Sie **Zertifikat für einen anderen Computer erstellen** aus.
7. Geben Sie in **Name des Antragstellers** den FQDN des ASBCE ein.
8. Geben Sie in **Alternative Name(n) des Antragstellers** alle zusätzlichen Werte für andere Server und Dienste ein, mit denen sich das ASBCE verbinden muss.
   - **Für IPv4:** Das Zertifikat muss den IP Office FQDN und die IPv4-Adresse enthalten.
   - **Für IPv6:** Zusätzlich zur IP Office FQDN- und IPv4-Adresse muss das ASBCE Identitätszertifikat den ASBCE FQDN und die IPv6-Adresse enthalten.
   - Verwenden Sie kommagetrennte Werte für die erforderlichen Einträge *DNS:<FQDN>* und *IP:<IP address>*.
   - Wenn Sie verschiedene FQDNs für die Avaya one-X® Portal XMPP-Domäne verwenden, geben Sie alle FQDNs als kommagetrennte Liste der DNS-Einträge ein.
9. Klicken Sie auf **OK**. Warten Sie bis zu einer Minute, während IP Office das Zertifikat generiert.
10. Wenn Sie dazu aufgefordert werden, legen Sie ein Verschlüsselungskennwort für das Identitätszertifikat fest und klicken Sie auf **Ja** .
11. Der Browser fordert Sie auf, die Zertifikatdatei herunterzuladen und zu speichern.
12. Benennen Sie die heruntergeladene Datei in `SBCE_ID.p12` um.

Weitere Schritte

- Siehe Aufteilen des ASBCE Identitätszertifikats auf Seite 21.

Verwandte Links

Hinzufügen von IP Office Zertifikaten zum ASBCE auf Seite 17

Erstellen eines ASBCE Identitätszertifikats mit Web Control (Plattformansicht)

Dieser Vorgang generiert ein Identitätszertifikat für ASBCE über die Web Control-Menüs des IP Office Servers.

Vorgehensweise

1. Melden Sie sich bei den IP Office Web Control-Menüs an, indem Sie entweder:
   - Wählen Sie in IP Office Web Manager den primären Server aus. Klicken Sie auf ☰ und wählen Sie **Plattformansicht** aus.
   - Navigieren Sie zu `https://<IP Office IP address>:7071` und melden Sie sich an.
2. Wählen Sie die Registerkarte **Einstellungen** und blättern Sie nach unten zu **Zertifikate**.
3. Wählen Sie **Zertifikat für einen anderen Computer erstellen** aus.
4. Geben Sie folgende Angaben ein:
5. Geben Sie unter **Maschinen-IP** die externe IP-Adresse des ASBCE ein.
6. Geben Sie unter **Kennwort** ein Kennwort ein, um das Zertifikat und den Schlüssel zu verschlüsseln.
7. Geben Sie in **Name des Antragstellers** den FQDN des ASBCE ein.
8. Geben Sie in **Alternative Name(n) des Antragstellers** alle zusätzlichen Werte für andere Server und Dienste ein, mit denen sich das ASBCE verbinden muss.
   - **Für IPv4:** Das Zertifikat muss den IP Office FQDN und die IPv4-Adresse enthalten.
   - **Für IPv6:** Zusätzlich zur IP Office FQDN- und IPv4-Adresse muss das ASBCE Identitätszertifikat den ASBCE FQDN und die IPv6-Adresse enthalten.
   - Verwenden Sie kommagetrennte Werte für die erforderlichen Einträge *DNS:<FQDN>* und *IP:<IP address>*.
   - Wenn Sie verschiedene FQDNs für die Avaya one-X® Portal XMPP-Domäne verwenden, geben Sie alle FQDNs als kommagetrennte Liste der DNS-Einträge ein.
9. Klicken Sie auf **Neu generieren**.
10. Klicken Sie im Popup-Fenster auf den Link und speichern Sie die Datei.
11. Benennen Sie die heruntergeladene Datei in `SBCE_ID.p12` um.

Weitere Schritte

- Siehe Aufteilen des ASBCE Identitätszertifikats auf Seite 21.

Verwandte Links

Hinzufügen von IP Office Zertifikaten zum ASBCE auf Seite 17

Aufteilen des ASBCE Identitätszertifikats

Das von IP Office für das ASBCE erstellte Identitätszertifikat ist eine einzelne Datei. Es enthält sowohl das Zertifikat als auch den privaten Schlüssel. Für die Konfiguration des ASBCE müssen Sie das Identitätszertifikat in separate Zertifikat- und private Schlüsseldateien aufteilen.

Voraussetzungen

- Verwenden Sie IP Office, um ein Identitätszertifikat für das ASBCE zu erstellen:
  - Informationen zu Abonnementsystemen finden Sie unter Erstellen eines ASBCE Identitätszertifikats mithilfe von IP Office Web Manager auf Seite 19.
  - Weitere Systeme finden Sie unter Erstellen eines ASBCE Identitätszertifikats mit Web Control (Plattformansicht) auf Seite 20.

Vorgehensweise

1. Stellen Sie mithilfe von WinSCP über Port 222 und die ipcs-Anmeldung eine Verbindung zur ASBCE Management-IP-Adresse her.
2. Kopieren Sie das für ASBCE (`SBCE_ID.p12`) erstellte IP Office Identitätszertifikat in das Verzeichnis ASBCE **`/home/ipcs`**.
3. Bauen Sie eine Verbindung per SSH mit der ASBCE Verwaltungs-IP mit Port 222 und ipcs-Anmeldung auf.
4. Geben Sie den Befehl **su root** oder **su -root** ein und geben Sie das root-Kennwort von ASBCE ein.
5. Geben Sie die folgenden Befehle ein. Der zu verwendende Befehl hängt davon ab, ob Sie das Zertifikat mit IP Office Web Manager oder den Menüs der Web Control (Plattformansicht) erstellt haben.

   Hinweis:

   - Wenn Sie zur Eingabe eines Kennworts oder einer PEM-Passphrase aufgefordert werden, geben Sie das Kennwort ein, das beim Generieren des Identitätszertifikats für ASBCE angegeben wurde.
   - Wenn das Kennwort Sonderzeichen enthält, müssen Sie diese bei der Eingabe in die Befehlszeile mit dem Präfix `\` versehen. Geben Sie in der Befehlszeile beispielsweise ein `@` im Kennwort als `\@` ein.

   - **IP Office Web Control-Zertifikat:**

     Gehen Sie wie folgt vor, wenn ein Zertifikat über die IP Office Web Control-Menüs generiert wird.

     ```
     openssl pkcs12 -in SBCE_ID.p12 -out SBCE_ID.crt -nokeys -clcerts
     openssl pkcs12 -in SBCE_ID.p12 -out SBCE_ID.key -nocerts
     ```

   - **IP Office Web Manager-Zertifikat:**

     Gehen Sie wie folgt vor, wenn ein Zertifikat mit IP Office Web Manager generiert wird.

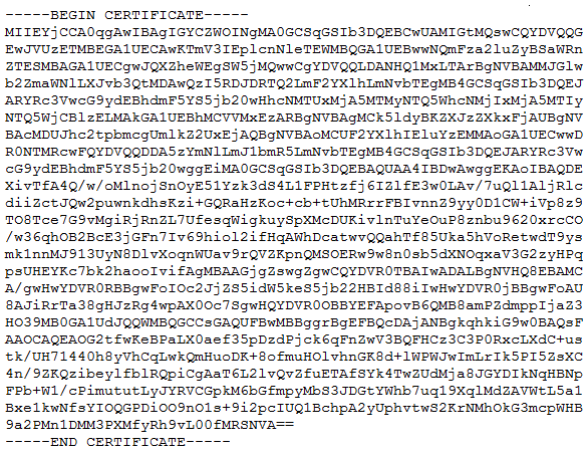
     ```
     openssl enc -base64 -d -in SBCE_ID.p12 -out SBCE_ID_BIN.p12 -A
     openssl pkcs12 -in SBCE_ID_BIN.p12 -out SBCE_ID.crt -nokeys -clcerts
     openssl pkcs12 -in SBCE_ID_BIN.p12 -out SBCE_ID.key -nocerts
     ```

6. Kopieren Sie die neuen Dateien `SBCE_ID.crt` und `SBCE_ID.key` vom ASBCE auf Ihren PC.
7. Die Datei `SBCE_ID.crt` enthält weiterhin das IP Office CA-Stammzertifikat, den privaten Schlüssel und das ASBCE ID-Zertifikat. Um die Datei in ASBCE importieren

zu können, müssen Sie das CA-Zertifikat und den privaten Schlüssel aus der Datei entfernen.

a. Öffnen Sie `SBCE_ID.crt` im WordPad auf Ihrem PC.

b. Löschen Sie alle Zeilen, mit Ausnahme der Zeilen, die sich zwischen den Zeilen **BEGIN-ZERTIFIKAT** und **END-ZERTIFIKAT** befinden. Beispiel:



Weitere Schritte

- Gehen Sie zu Hinzufügen des Identitätszertifikats zum ASBCE auf Seite 23.

Verwandte Links

Hinzufügen von IP Office Zertifikaten zum ASBCE auf Seite 17

Hinzufügen des Identitätszertifikats zum ASBCE

Gehen Sie wie folgt vor, um das Identitätszertifikat zum ASBCE hochzuladen.

Voraussetzungen

- Aufteilen des ASBCE Identitätszertifikats auf Seite 21

Vorgehensweise

1. Gehen Sie auf **TLS-Verwaltung** > **Zertifikate**.
2. Klicken Sie auf **Installieren**.
3. Wählen Sie unter **Typ Zertifikat** aus.
4. Geben Sie einen aussagekräftigen Namen für das Zertifikat ein.
5. Klicken Sie auf **Datei auswählen** und wählen Sie die Datei `SBCE_ID.crt` aus.
6. Wählen Sie **Schlüsseldatei hochladen** aus.
7. Klicken Sie auf **Datei auswählen** und wählen Sie die Datei `SBCE_ID.key` aus.
8. Klicken Sie auf **Hochladen**. Das Menü zeigt das Zertifikat an.
9. Klicken Sie auf **Installieren**.
10. Klicken Sie auf **Beenden**.

11. Greifen Sie mithilfe von SSH über Port 222 und die ipcs-Anmeldung auf die ASBCE Management-IP-Adresse zu.
    a. Geben Sie `su root` oder `su -root` und das ASBCE root-Kennwort ein.
    b. Geben Sie die folgenden Befehle ein und ersetzen Sie `********` durch das bei der Erstellung des Identitätszertifikats festgelegte Kennwort:

```
cd /usr/local/ipcs/cert/key
enc_key SBCE_ID.key ********
```

    - Sie müssen im Kennwort Sonderzeichen mit einem `\` voranstellen. Um beispielsweise ein `@` einzugeben, geben Sie `\@` ein.

Verwandte Links

Hinzufügen von IP Office Zertifikaten zum ASBCE auf Seite 17

Kapitel 4: ASBCE Konfiguration für Remote-SIP-Nebenstellen

In diesem Abschnitt wird die Konfiguration von ASBCE zum Weiterleiten von SIP-Anrufen zwischen den Remote-Nebenstellen und dem IP Office beschrieben.

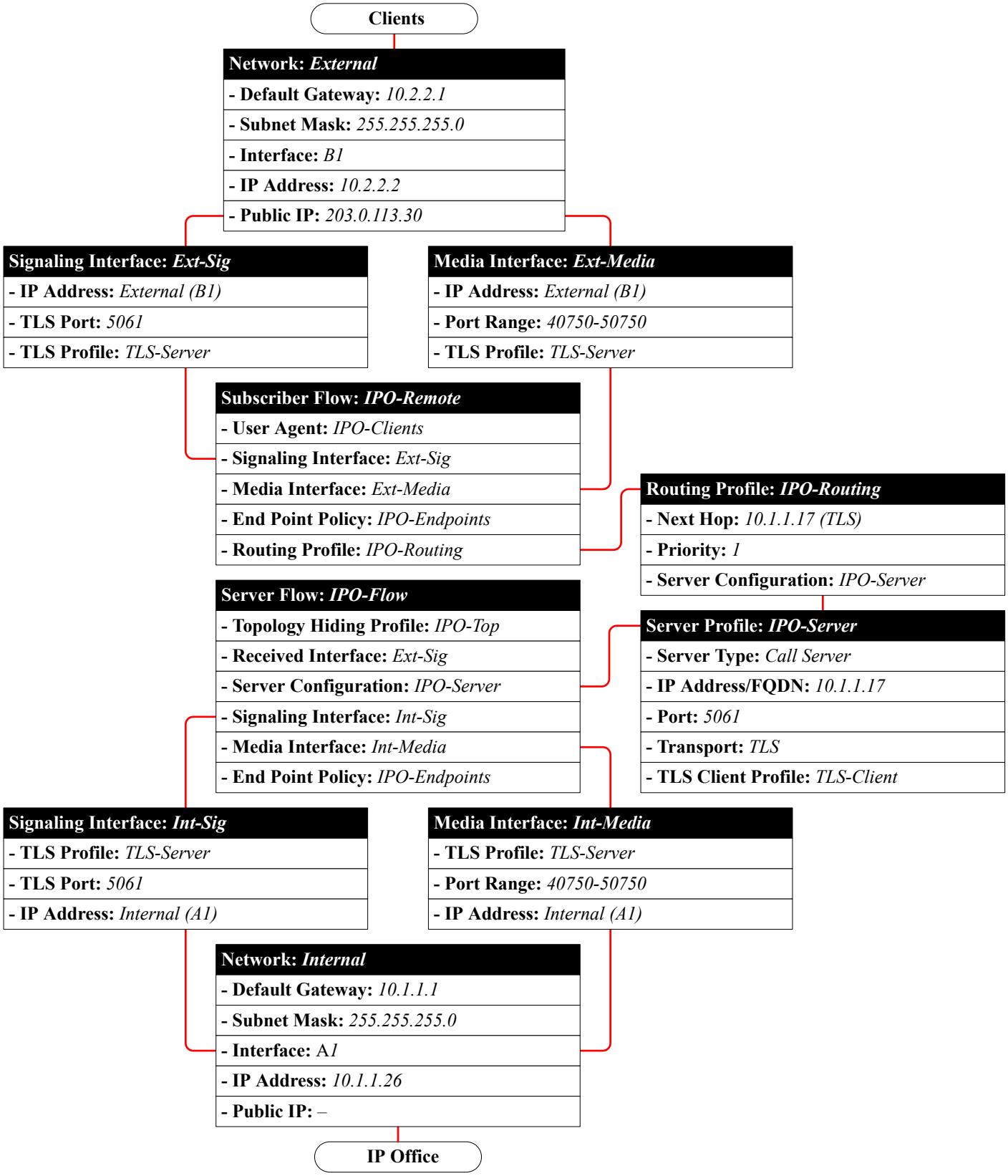
- **IPv6-Support:** Weitere Informationen zur Unterstützung von IPv6-Remote-Nebenstellen finden Sie unter Unterstützung von IPv6-Remote-Nebenstellen auf Seite 73.
  - **Wenn nur IPv6-Remote-Nebenstellen unterstützt werden:** Befolgen Sie den Konfigurationsvorgang in diesem Abschnitt für IPv4, ersetzen Sie jedoch die externen IPv4-Adressen ggf. durch IPv6-Adressen.
  - **Wenn IPv4- und IPv6-Remote-Nebenstellen unterstützt werden:** Sie müssen nach Abschluss der IPv4-Konfiguration zusätzliche Konfigurationsschritte durchführen. Siehe Konfigurationscheckliste für kombinierte IPv4- und IPv6-Remote-Nebenstellen auf Seite 77.

Verwandte Links

Hinzufügen von Reverse Proxys für Dateianforderungen auf Seite 57

ASBCE Zusammenfassung des Anrufverlaufs

Dieses Bild fasst die ASBCE Konfigurationskomponenten zusammen, die für die Verbindung zwischen IPv4-Remote-Nebenstellen und dem IP Office verwendet werden.



Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Klonen vs. Hinzufügen

Wichtig:

Mehrere Prozesse in diesem Dokument weisen Sie an, neue Elemente zu erstellen, indem Sie eine vorhandene Vorlage klonen, anstatt einen neuen Eintrag hinzuzufügen. Das heißt, klicken Sie auf **Klonen** und nicht auf **Hinzufügen**.

- Sie müssen **Klonen** verwenden, wenn dies in einem Prozess angegeben ist, und das vorhandene Profil klonen, das in den Anweisungen angegeben ist.
- Mit **Hinzufügen** wird ein neuer Eintrag erstellt, der andere Standardeinstellungen als der erwartete Klon hat. Dies führt zu einem fehlerhaften Betrieb.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

ASBCE-Konfigurationsprüfliste

#	Aktion	Link/Hinweise	✔
1.	Firewall-Port-Weiterleitung konfigurieren	Leiten Sie externen Datenverkehr von den Clients an das ASBCE weiter. Siehe Firewall-Konfiguration auf Seite 30.	
2.	Konfigurieren der externen ASBCE Netzwerkschnittstelle	Legen Sie die externen IP-Adressen fest, die vom ASBCE verwendet werden. Siehe Externe ASBCE Schnittstelle konfigurieren auf Seite 31.	
3.	Konfigurieren der internen ASBCE Netzwerkschnittstelle.	Legen Sie die internen IP-Adressen fest, die vom ASBCE verwendet werden. Siehe Interne ASBCE Schnittstelle konfigurieren auf Seite 32.	
4.	TLS-Clientprofil erstellen	Hiermit werden die TLS-Einstellungen festgelegt, die von ASBCE verwendet werden, wenn es eine Verbindung mit dem IP Office herstellt. Siehe Erstellen eines TLS-Clientprofils auf Seite 34.	
5.	TLS-Serverprofil erstellen	Hiermit werden die TLS-Einstellungen festgelegt, die vom ASBCE verwendet werden, wenn Clients und das IP Office eine Verbindung herstellen. Siehe Erstellen eines TLS-Serverprofils auf Seite 35.	
6.	Interne SIP-Medienschnittstelle erstellen	Legen Sie die Ports und Adressen fest, auf denen das ASBCE SIP-Medien vom IP Office abhört. Siehe Erstellen einer internen Signalisierungsschnittstelle auf Seite 39.	

Die Tabelle wird auf der nächsten Seite fortgesetzt …

#	Aktion	Link/Hinweise	✔
7.	Erstellen einer externen SIP-Medienschnittstelle	Legen Sie die Ports und Adressen fest, auf denen das ASBCE auf SIP-Medien für die Remote-Nebenstellen wartet. Siehe Erstellen der externen Signalisierungsschnittstelle auf Seite 40.	
8.	Interne SIP-Signalisierungsschnittstelle erstellen	Legen Sie die Ports und Adressen fest, an denen das ASBCE SIP-Anrufsignale vom IP Office erwartet. Siehe Erstellen einer internen Signalisierungsschnittstelle auf Seite 39.	
9.	Erstellen einer externen SIP-Signalisierungsschnittstelle	Legen Sie die Ports und Adressen fest, an denen das ASBCE SIP-Anrufsignale von den Remote-Nebenstellen erwartet. Siehe Erstellen der externen Signalisierungsschnittstelle auf Seite 40.	
10.	Serverprofil erstellen	Siehe Erstellen eines ASBCE Serverprofils für das IP Office auf Seite 41.	
11.	Serverrouting erstellen	Siehe Erstellen eines Server-Routingprofils auf Seite 43.	
12.	Topologie ausblenden einrichten	Definieren Sie die Konvertierungen von SIP-Header-Informationen, die das ASBCE durchführen muss. Siehe Erstellen einer ASBCE Topologie-Ausblendrichtlinie auf Seite 44.	
13.	Erstellen Sie eine IP/URL-Sperrliste.	Legen Sie die unterstützten Medientypen und die maximale Anzahl von Verbindungen fest. Siehe Erstellen einer IP/URI-Blockliste auf Seite 45.	
14.	Erstellen einer Anwendungsregel.	Legen Sie den Typ und die Anzahl der unterstützten Medienverbindungen fest. Siehe Erstellen einer Anwendungsregel auf Seite 46.	
15.	Erstellen einer Medienregel	Siehe Erstellen einer Medienregel auf Seite 48.	
16.	Erstellen einer Endgerätrichtlinie	Eine Endgerätrichtlinie gruppiert die Anwendungs- und Medienregeln. Siehe Erstellen einer Endgeräterichtliniengruppe auf Seite 50.	
17.	User-Agent-Profil hinzufügen	Definieren Sie die UA-Werte für die Remote-Nebenstellen, bei denen das ASBCE eine Verbindung zulassen soll. Siehe Konfigurieren eines User-Agent-Profils auf Seite 51.	
18.	Erstellen eines Teilnehmer-Flows	Siehe Erstellen des Teilnehmer-Flows auf Seite 52.	
19.	Erstellen eines Server-Flows	Siehe Erstellen eines Server-Flows auf Seite 55.	

Die Tabelle wird auf der nächsten Seite fortgesetzt …

#	Aktion	Link/Hinweise	✔
20.	Reverse Proxy für Avaya Workplace-Client hinzufügen	Anfragen nach Einstellungsdateien von den Clients an IP Office weiterleiten. Siehe Hinzufügen von Reverse Proxys für Dateianforderungen auf Seite 57.	

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Firewall-Konfiguration

Sie müssen die Netzwerkgeräte von Kunden an den Endpunkten deren Netzwerks konfigurieren, um den Verkehr externer Remote-Nebenstellen an ASBCE weiterzuleiten. Der tatsächliche Prozess hängt vom Netzwerk des Kunden und seinen Geräten ab. Im Folgenden finden Sie nur Richtlinien.

Vorgehensweise

1. Aktivieren Sie nur **Layer-3-Nat**.
2. Deaktivieren Sie alle SIP-fähigen Funktionen, beispielsweise ALG.
3. Leiten Sie die folgenden Ports an die IP-Adresse der B1-Schnittstelle des ASBCE weiter.
   - **Für Avaya Workplace-Client und J100 Telefone:**

Transport-/Anwendungsprotokoll		Port	Verwendung
tcp	tls	5061	SIP-TLS-Verbindung zur Registrierung.
	http	80	Allgemeine und sichere Dateianforderungen von Telefonen und Clients, wenn **Bevorzugte Telefonports verwenden** nicht in IP Office aktiviert ist.
	https	443	
	http	8411	Allgemeine und sichere Dateianforderungen von Telefonen und Clients, wenn **Bevorzugte Telefonports verwenden** in IP Office aktiviert ist.
	https	411	
udp	rtp	40750 to 50750	Der Portbereich, der für den Datenverkehr von Anrufmedien (RTP) und Anrufsteuerung (RTCP) verwendet wird.
	rtcp		

Weitere Schritte

- Gehen Sie auf Externe ASBCE Schnittstelle konfigurieren auf Seite 31.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Externe ASBCE Schnittstelle konfigurieren

Fügen Sie Details zum Kundennetzwerk zwischen der Kunden-Firewall und ASBCE hinzu.

- **Duale Unterstützung für IPv4/IPv6:** Zur Unterstützung von IPv4- und IPv6-Remote-Nebenstellen müssen Sie separate Einträge für IPv4 und IPv6 erstellen:
  - Die **IP-Adresse** muss immer die entsprechende *B1* IPv4- oder IPv6-Adresse verwenden.

Wichtig:

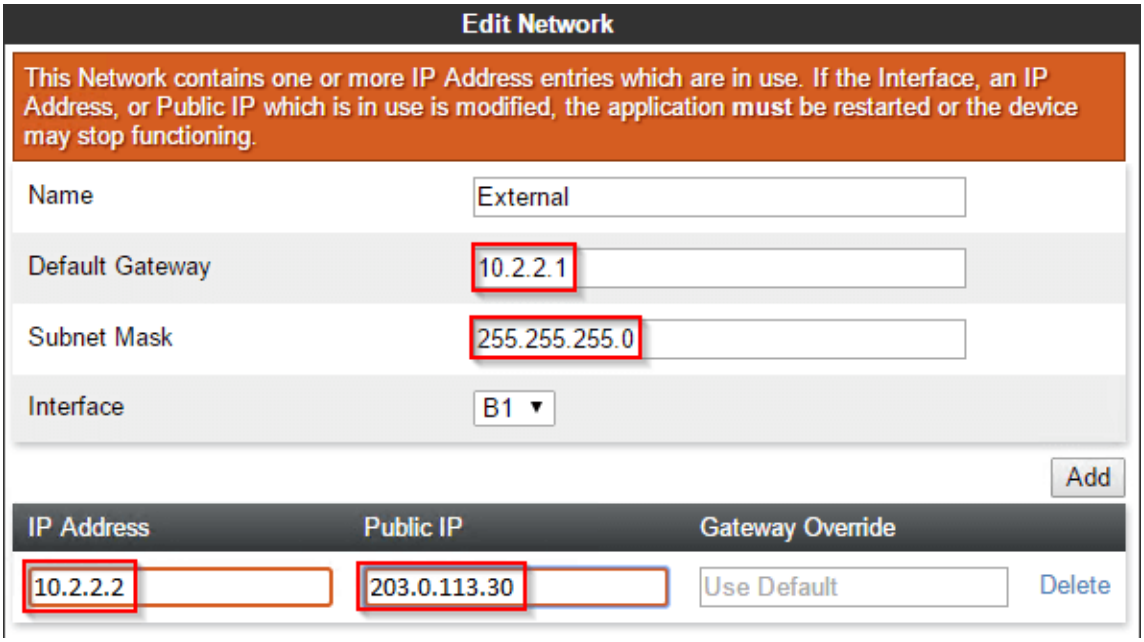
- Für diesen Vorgang müssen Sie ASBCE neu starten. Dadurch werden alle aktuellen Verbindungen über das ASBCE beendet.

Voraussetzungen

- Firewall-Konfiguration auf Seite 30

Vorgehensweise

1. Gehen Sie auf **Gerätespezifische Einstellungen** > **Netzwerk-Management**.
2. Wählen Sie die Registerkarte **Netzwerke** und klicken Sie auf **Hinzufügen**.
3. Geben Sie folgende Angaben ein:



Feld	Beschreibung
Name	Sie verwenden diesen Namen in anderen Menüs, um das Netzwerk auszuwählen.
Standardgateway	Die interne IP-Adresse der Geräte, die den Datenverkehr zwischen dem Kundennetzwerk und dem öffentlichen Internet weiterleiten. Im Beispiel ist dies die interne Adresse der Firewall.
Subnetzmaske	Die IP-Maske für das **Standardgateway** Netzwerk.
Schnittstelle	Wählen Sie die öffentliche Schnittstelle des ASBCE aus.

4. Klicken Sie auf **Hinzufügen** und geben Sie eine IP-Adresse ein, die das ASBCE auf dieser Netzwerkoberfläche verwendet.

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse der ASBCE Schnittstelle ein, die mit der Firewall verbunden ist.
Öffentliche IP-Adresse	Geben Sie die öffentliche IP-Adresse der Firewall ein. Diese muss mit der IP-Adresse übereinstimmen, an die DNS die Remote-Nebenstelle leitet, wenn sie DNS-Suche des vollqualifizierten Domänennamens von IP Office durchführen.

5. Wenn sowohl IPv4- als auch IPv6-Remote-Nebenstellen unterstützt werden, wiederholen Sie den Vorgang, um die IPv6-Einträge zu erstellen.

Weitere Schritte

- Gehen Sie auf Interne ASBCE Schnittstelle konfigurieren auf Seite 32.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Interne ASBCE Schnittstelle konfigurieren

Fügen Sie Details zum Kundennetzwerk zwischen dem ASBCE und dem IP Office hinzu.

- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

Wichtig:

- Für diesen Vorgang müssen Sie ASBCE neu starten. Dadurch werden alle aktuellen Verbindungen über das ASBCE beendet.

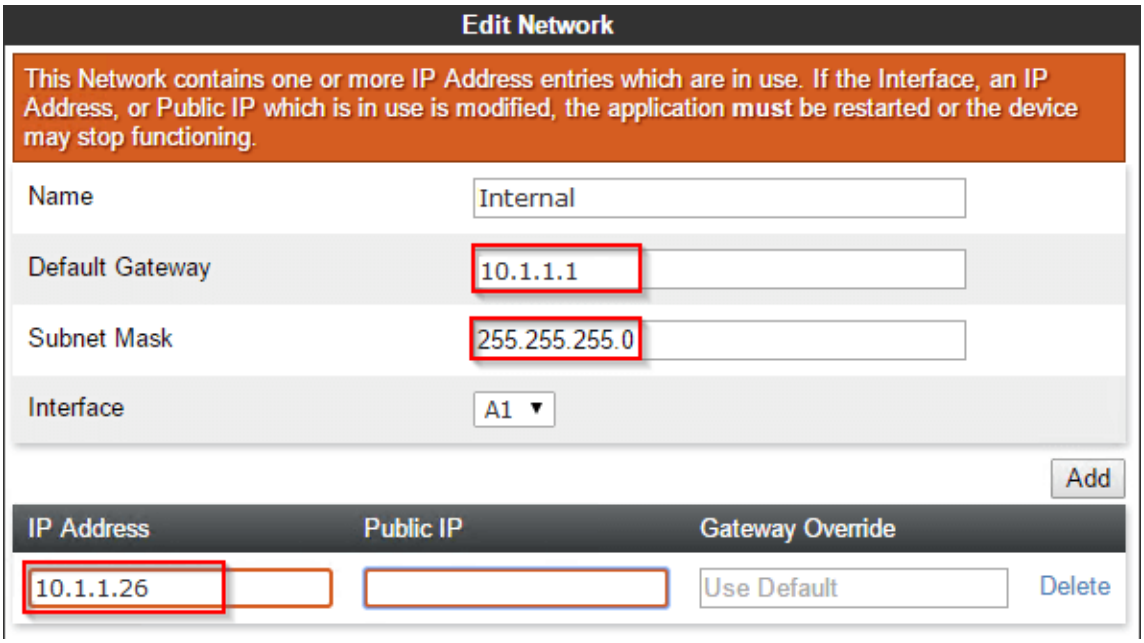
Voraussetzungen

- Externe ASBCE Schnittstelle konfigurieren auf Seite 31

Vorgehensweise

1. Gehen Sie auf **Gerätespezifische Einstellungen** > **Netzwerk-Management**.
2. Wählen Sie die Registerkarte **Netzwerke** und klicken Sie auf **Hinzufügen**.

3. Geben Sie folgende Angaben ein:



Feld	Beschreibung
Name	Sie verwenden diesen Namen in anderen Menüs, um das Netzwerk auszuwählen.
Standardgateway	Die IP-Adresse und das Standard-Gateway für den Datenverkehr innerhalb des Kundennetzwerks.
Subnetzmaske	
Schnittstelle	Wählen Sie die private Schnittstelle des ASBCE aus.

4. Klicken Sie auf **Hinzufügen** und geben Sie eine IP-Adresse ein, die das ASBCE auf dieser Netzwerkoberfläche verwendet.

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse für die ASBCE Schnittstelle ein, die mit dem Kundennetzwerk verbunden ist. Dies ist die IP-Adresse der A1-Schnittstelle.

5. Gehen Sie auf **System Management** und klicken Sie auf **Anwendung neu starten**.

Weitere Schritte

- Gehen Sie auf Erstellen eines TLS-Clientprofils auf Seite 34.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen eines TLS-Clientprofils

Bei TLS-Verbindungen vom ASBCE fungiert es als TLS-Client. Zum Beispiel für Verbindungen zum IP Office und den externen Clients. Das für jede Verbindung verwendete TLS-Clientprofil definiert die verwendeten Zertifikate und andere TLS-Einstellungen.

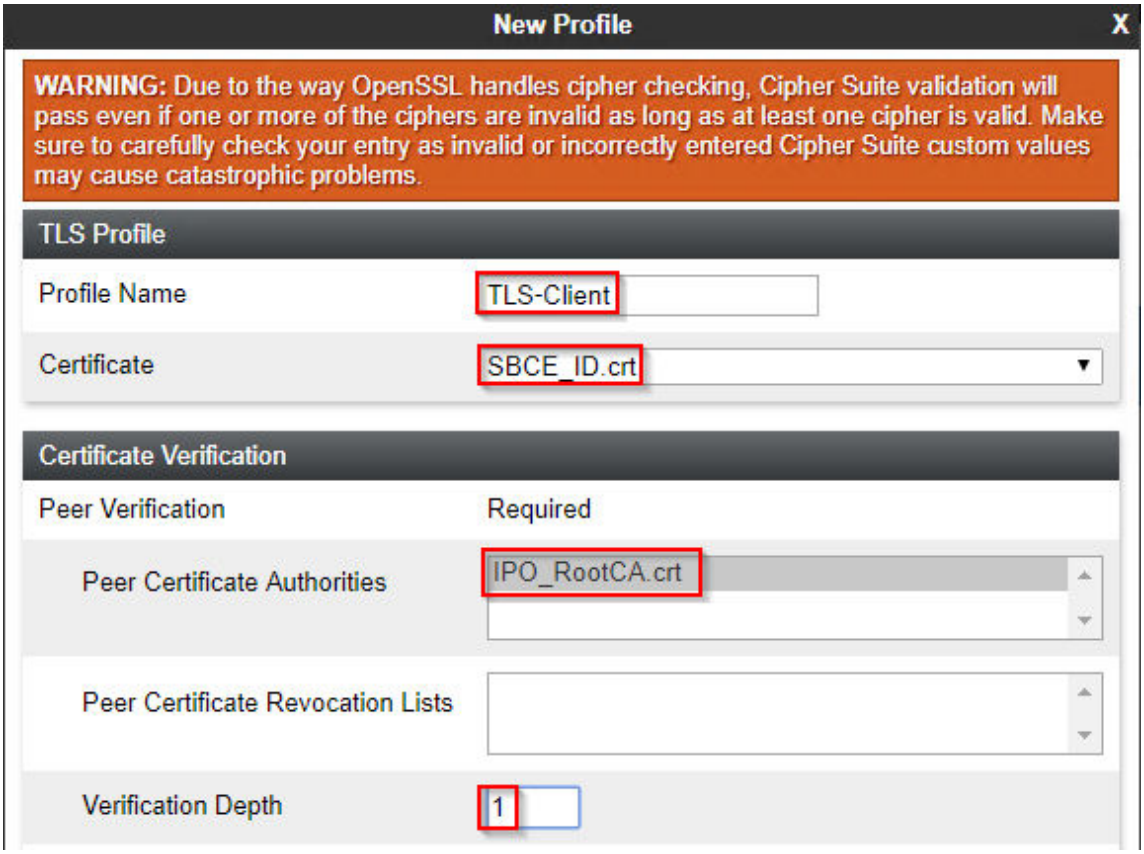
- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

Voraussetzungen

- Interne ASBCE Schnittstelle konfigurieren auf Seite 32.

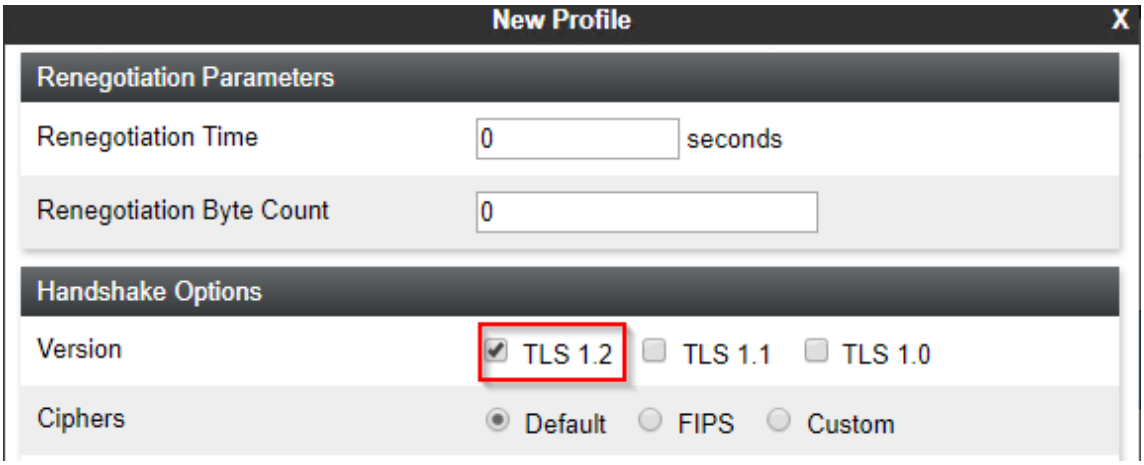
Vorgehensweise

1. Wählen Sie **TLS-Verwaltung** > **Client-Profile** aus.
2. Klicken Sie auf **Hinzufügen**.



3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.
4. Wählen Sie in **Zertifikat** das für das ASBCE erstellte Identitätszertifikat aus.
5. Wählen Sie in **Peer-Zertifikatsaussteller** das Stammzertifikat aus, das zum Erstellen des Identitätszertifikats verwendet wird. Im Beispielszenario ist dies die Datei `IPO_RootCA.crt`, die zum ASBCE hochgeladen wurde.
6. Geben Sie unter **Verifizierungstiefe 1** ein.

7. Klicken Sie auf **Weiter**.



8. Aktivieren Sie **TLS 1.2**.
9. Klicken Sie auf **Beenden**.

Weitere Schritte

- Gehen Sie auf Erstellen eines TLS-Serverprofils auf Seite 35.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen eines TLS-Serverprofils

Bei TLS-Verbindungen mit ASBCE fungiert es als TLS-Server. Zum Beispiel für Verbindungen vom IP Office und von externen Clients. Das für jede Verbindung verwendete TLS-Clientprofil definiert die verwendeten Zertifikate und andere TLS-Einstellungen.

- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

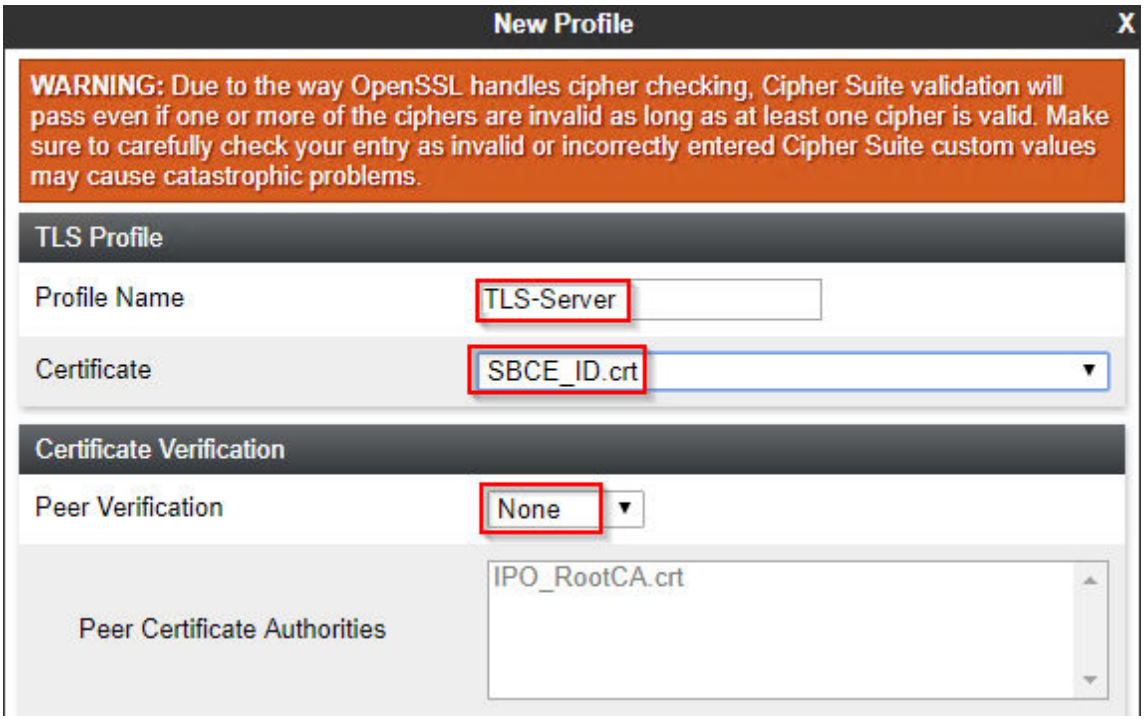
Voraussetzungen

- Erstellen eines TLS-Clientprofils auf Seite 34.

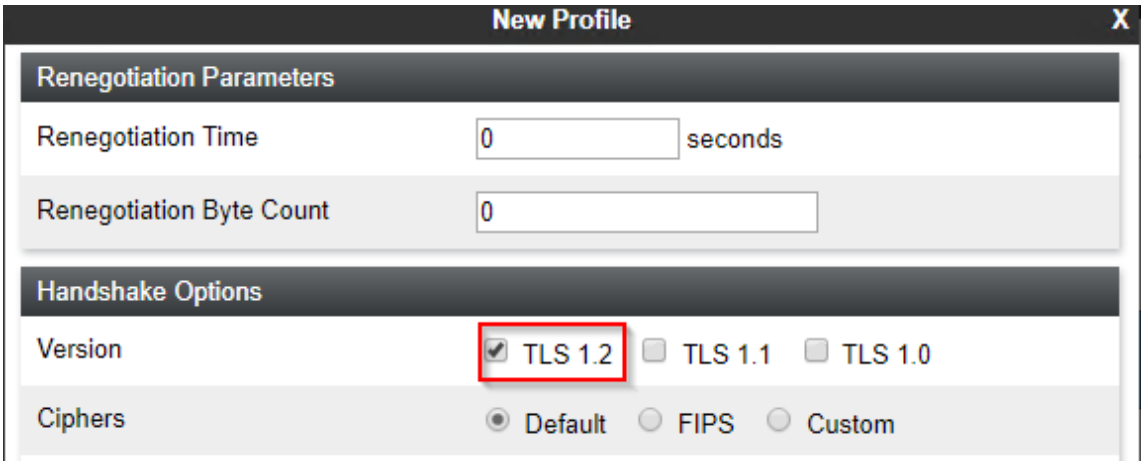
Vorgehensweise

1. Wählen Sie **TLS-Verwaltung** > **Client-Profile** aus.

2. Klicken Sie auf **Hinzufügen**.



3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.
4. Wählen Sie in **Zertifikat** das für das ASBCE erstellte Identitätszertifikat aus.
5. Wählen Sie unter **Peer-Zertifikatsaussteller Keine** aus.
6. Klicken Sie auf **Weiter**.



7. Aktivieren Sie **TLS 1.2**.
8. Klicken Sie auf **Beenden**.

Weitere Schritte

- Gehen Sie auf Erstellen einer internen Medienschnittstelle auf Seite 37.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen einer internen Medienschnittstelle

Sie müssen eine interne Medienschnittstelle erstellen. Das ASBCE nutzt dieses, um SIP-Anrufmedien vom IP Office zu überwachen.

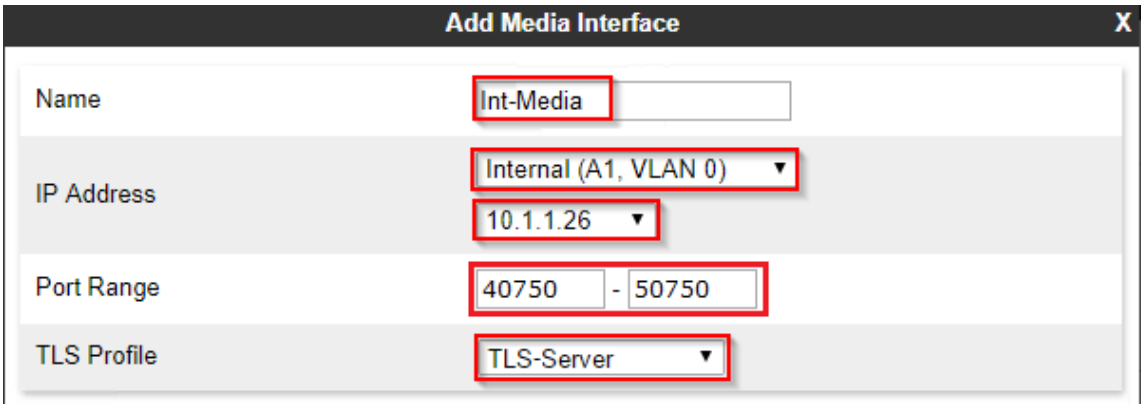
- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

Voraussetzungen

- Erstellen eines TLS-Clientprofils auf Seite 34.

Vorgehensweise

1. Wählen Sie **Gerätespezifische Einstellungen** > **Medien-Schnittstelle** aus.
2. Klicken Sie auf **Hinzufügen**.



3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.
4. Wählen Sie die interne Schnittstelle des ASBCE aus.
5. Wählen Sie für **TLS-Profil** das TLS-Serverprofil aus, das Sie für den Datenverkehr zum ASBCE erstellt haben.
6. Klicken Sie auf **Beenden**.

Weitere Schritte

- Gehen Sie auf Erstellen einer externen Medienschnittstelle auf Seite 38.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen einer externen Medienschnittstelle

Sie müssen eine externe Medienschnittstelle erstellen. Das ASBCE nutzt dieses, um SIP-Anrufmedien von den Remote-Nebenstellen zu überwachen.

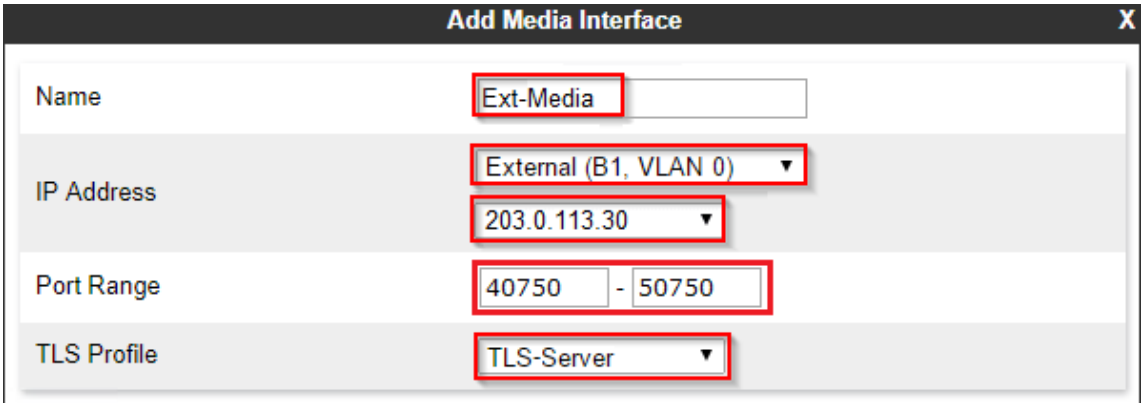
- **Duale Unterstützung für IPv4/IPv6:** Zur Unterstützung von IPv4- und IPv6-Remote-Nebenstellen müssen Sie separate Einträge für IPv4 und IPv6 erstellen:
  - Die **IP-Adresse** muss immer die entsprechende *B1* IPv4- oder IPv6-Adresse verwenden.

Voraussetzungen

- Erstellen einer internen Medienschnittstelle auf Seite 37.

Vorgehensweise

1. Gehen Sie auf **Gerätespezifische Einstellungen** > **Medien-Schnittstelle**.
2. Klicken Sie auf **Hinzufügen**.



3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.
4. Wählen Sie die externe Schnittstelle und IP-Adresse des ASBCE aus.
5. Wählen Sie für **TLS-Profil** das TLS-Serverprofil aus, das Sie für den Datenverkehr zum ASBCE erstellt haben.
6. Klicken Sie auf **Beenden**.
7. Wenn sowohl IPv4- als auch IPv6-Remote-Nebenstellen unterstützt werden, wiederholen Sie den Vorgang, um die IPv6-Einträge zu erstellen.

Weitere Schritte

- Gehen Sie auf Erstellen einer internen Signalisierungsschnittstelle auf Seite 39.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen einer internen Signalisierungsschnittstelle

Sie müssen eine interne Signalisierungsschnittstelle erstellen. Das ASBCE nutzt diese, um SIP-Anrufsignalisierung vom IP Office zu überwachen.

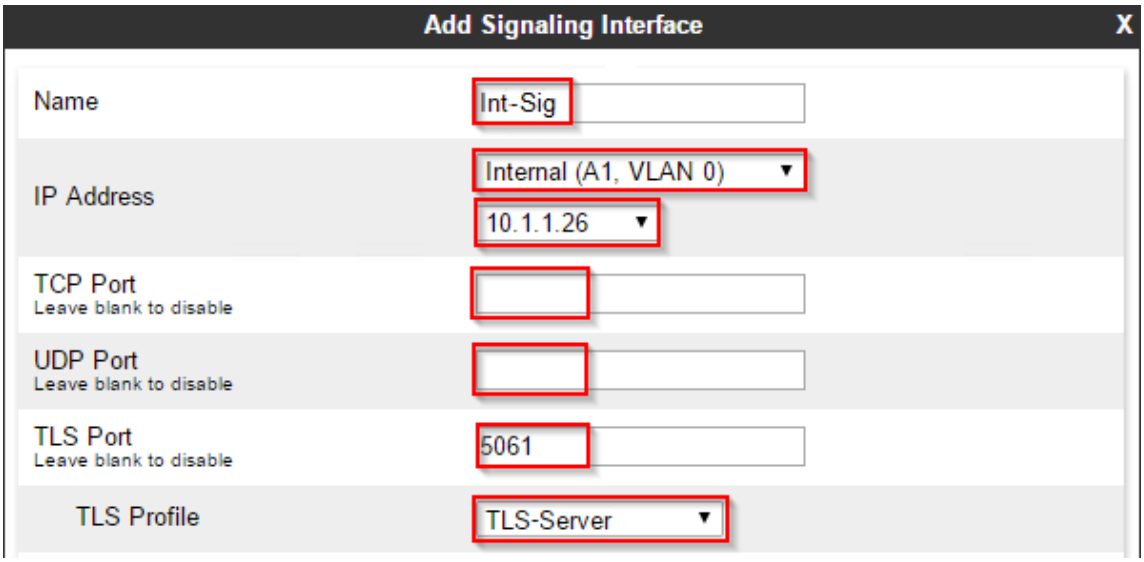
- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

Voraussetzungen

- Erstellen einer externen Medienschnittstelle auf Seite 38.

Vorgehensweise

1. Wählen Sie **Gerätespezifische Einstellungen** > **Signalisierungsschnittstelle** aus.
2. Klicken Sie auf **Hinzufügen**.



3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.
4. Wählen Sie *A1* aus der Dropdown-Liste **IP-Adresse** aus.
5. Lassen Sie das Feld **TCP-Port** leer, um TCP zu deaktivieren.
6. Lassen Sie das Feld **UDP-Port** leer, um UDP zu deaktivieren.
7. Stellen Sie **TLS-Port** so ein, dass es mit dem IP Office TLS-Port übereinstimmt.
8. Wählen Sie für **TLS-Profil** das TLS-Serverprofil aus, das Sie für den Datenverkehr zum ASBCE erstellt haben.
9. Klicken Sie auf **Beenden**.

Weitere Schritte

- Gehen Sie auf Erstellen der externen Signalisierungsschnittstelle auf Seite 40.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen der externen Signalisierungsschnittstelle

Sie müssen eine externe Signalisierungsschnittstelle erstellen. Das ASBCE nutzt dieses, um SIP-Registrierungsnachrichten von den Remote-Nebenstellen zu überwachen.

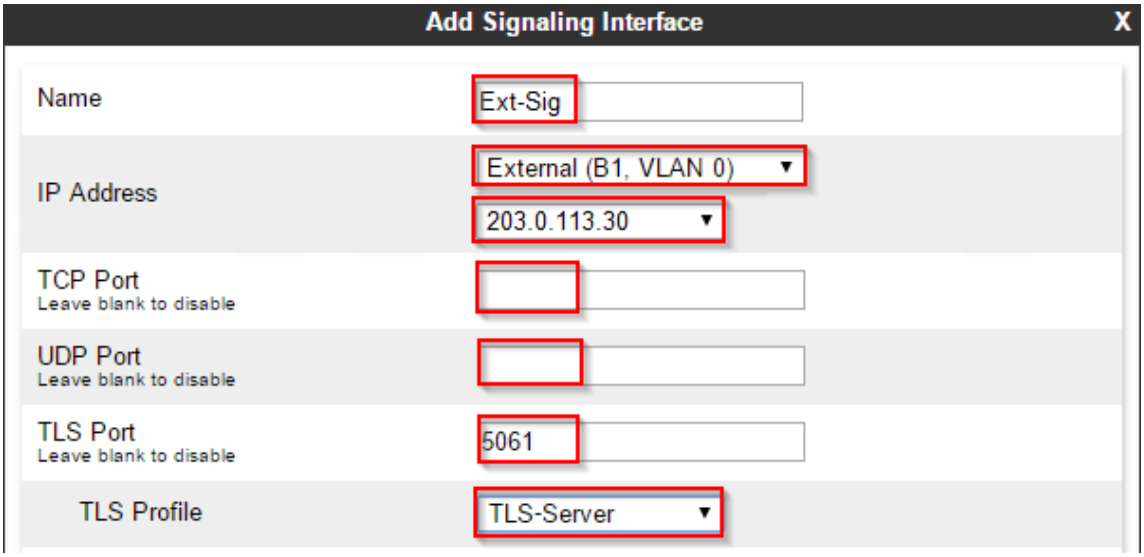
- **Duale Unterstützung für IPv4/IPv6:** Zur Unterstützung von IPv4- und IPv6-Remote-Nebenstellen müssen Sie separate Einträge für IPv4 und IPv6 erstellen:
  - Die **IP-Adresse** muss immer die entsprechende *B1* IPv4- oder IPv6-Adresse verwenden.

Voraussetzungen

- Erstellen einer internen Signalisierungsschnittstelle auf Seite 39.

Vorgehensweise

1. Wählen Sie **Gerätespezifische Einstellungen** > **Signalisierungsschnittstelle** aus.
2. Klicken Sie auf **Hinzufügen**.



3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.
4. Wählen Sie *B1* aus der Dropdown-Liste **IP-Adresse** aus.
5. Lassen Sie das Feld **TCP-Port** leer, um TCP zu deaktivieren.
6. Lassen Sie das Feld **UDP-Port** leer, um UDP zu deaktivieren.
7. Stellen Sie **TLS-Port** so ein, dass es mit dem IP Office TLS-Port übereinstimmt.
8. Wählen Sie für **TLS-Profil** das TLS-Serverprofil aus, das Sie für den Datenverkehr zum ASBCE erstellt haben.
9. Klicken Sie auf **Beenden**.
10. Wenn sowohl IPv4- als auch IPv6-Remote-Nebenstellen unterstützt werden, wiederholen Sie den Vorgang, um die IPv6-Einträge zu erstellen.

Weitere Schritte

- Gehen Sie auf Erstellen eines ASBCE Serverprofils für das IP Office auf Seite 41.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen eines ASBCE Serverprofils für das IP Office

Sie müssen auf dem ASBCE ein Serverprofil erstellen, das der Konfiguration des IP Office entspricht, siehe IP Office SIP VoIP-Einrichtung auf Seite 11.

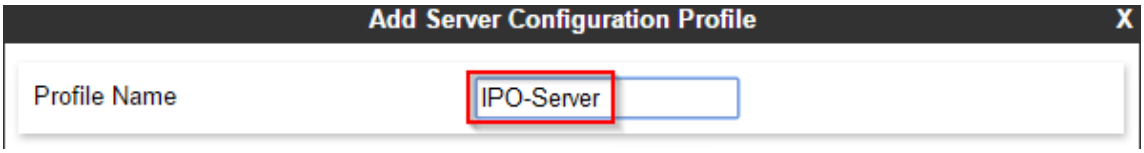
- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

Voraussetzungen

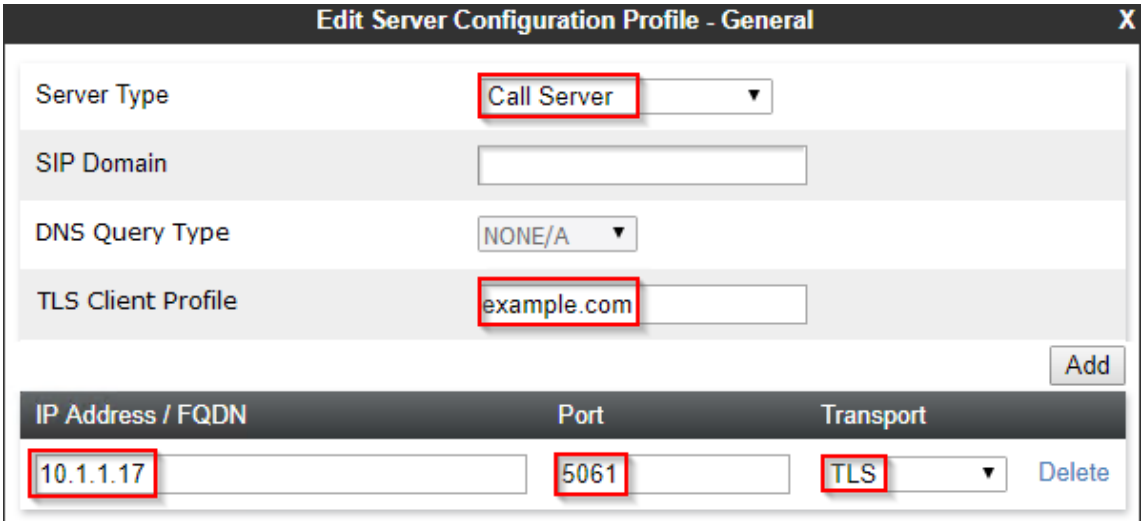
- Erstellen einer internen Signalisierungsschnittstelle auf Seite 39.

Vorgehensweise

1. Wählen Sie **Globale Profile** > **Serverkonfiguration** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.



4. Klicken Sie auf **Weiter**.

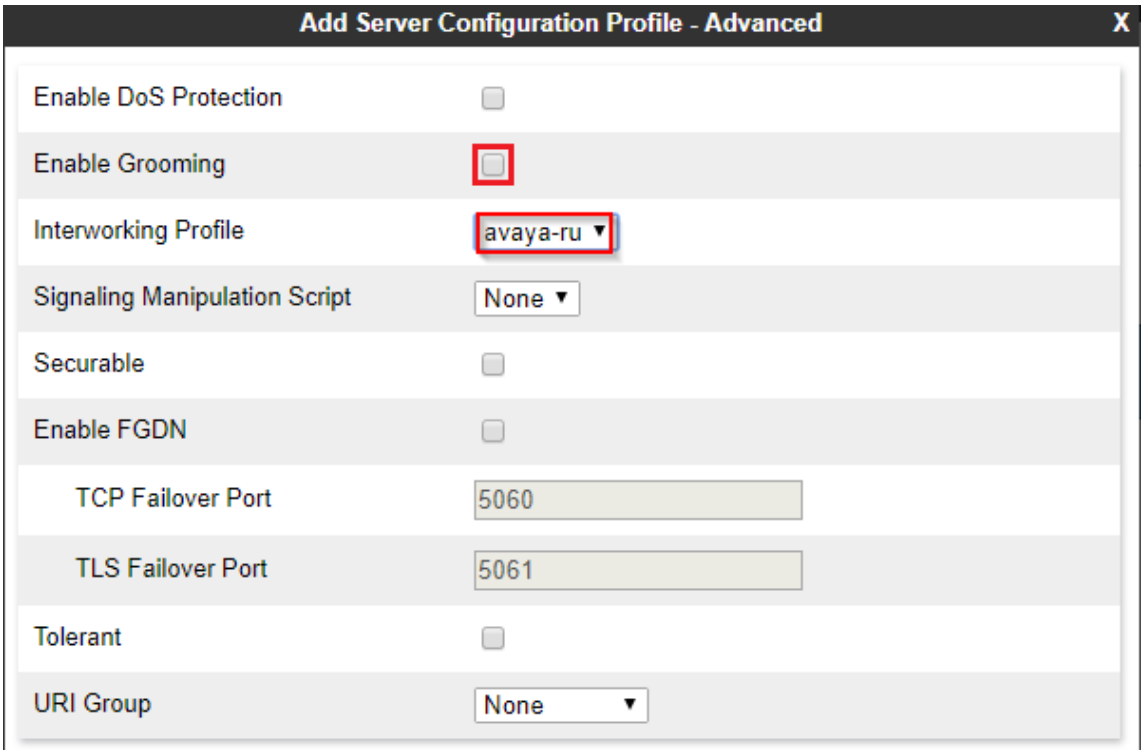


   a. Wählen Sie als **Servertyp** die Option **Anrufserver** aus.
   b. Geben Sie **SIP-Domäne** an, sodass sie mit dem übereinstimmt, was von IP Office für die SIP-Registrierung verwendet wird.
   c. Wählen Sie als **TLS-Client-Profil** das erstellte TLS-Clientprofil aus.

d. Klicken Sie auf **Hinzufügen** und geben Sie die Details für die in der IP Office Konfiguration festgelegten SIP-Verbindungen mit Layer 4-Port ein.
   - Geben Sie als **IP-Adresse/FQDN** die IP-Adresse des IP Office ein.
   - Geben Sie **Port** und **Übertragung** so an, dass sie den IP Office Einstellungen entsprechen.

e. Klicken Sie auf **Weiter**.

5. Klicken Sie auf **Weiter**, um die **Authentifizierungseinstellungen** zu überspringen.
6. Klicken Sie auf **Weiter**, um die **Heartbeat**-Einstellungen zu überspringen.
7. Passen Sie die erweiterten Einstellungen wie folgt an:



a. Deaktivieren Sie das Kontrollkästchen **Grooming aktivieren**.

b. Stellen Sie **Interworking-Profil** auf *avaya-ru* ein.

8. Klicken Sie auf **Beenden**.

Weitere Schritte

- Gehen Sie auf Erstellen eines Server-Routingprofils auf Seite 43.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen eines Server-Routingprofils

Das ASBCE verwendet ein Server-Routingprofil, um den abgeglichenen eingehenden Datenverkehr an den oder die entsprechenden Server weiterzuleiten. In diesem Fall müssen Sie ein Profil erstellen, das den Datenverkehr an IP Office weiterleitet.

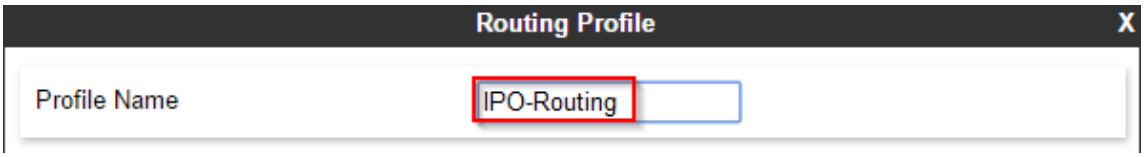
- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

Voraussetzungen

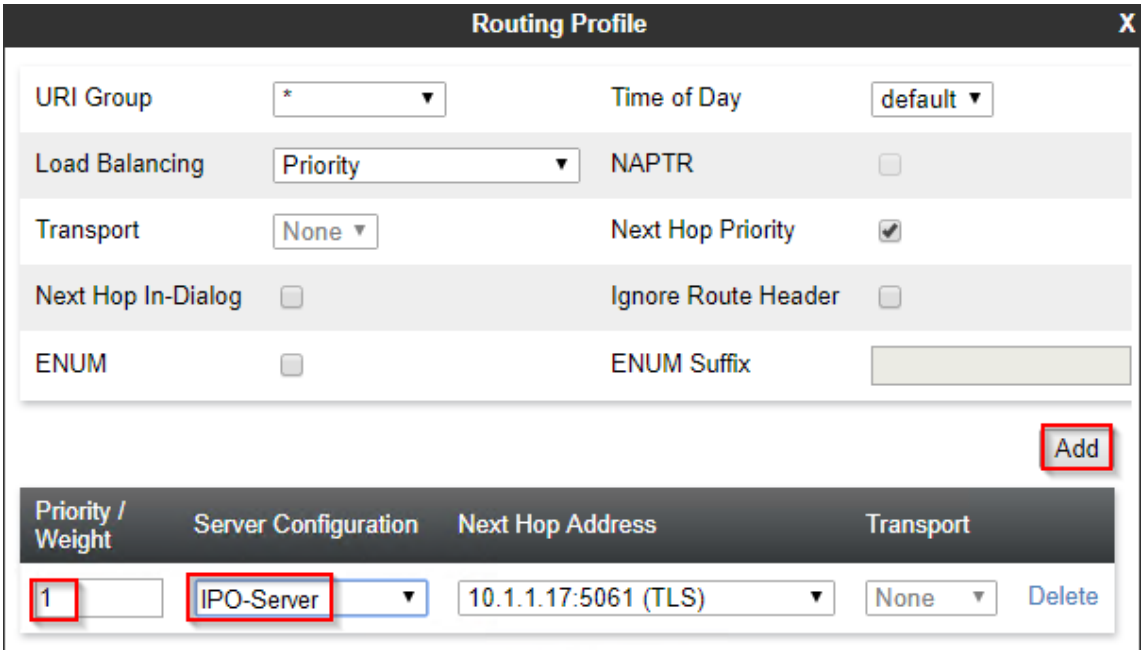
- Erstellen eines ASBCE Serverprofils für das IP Office auf Seite 41.

Vorgehensweise

1. Wählen Sie **Globale Profile** > **Routing** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.



4. Klicken Sie auf **Weiter**.



5. Klicken Sie auf **Hinzufügen**.
6. Setzen Sie **Priorität** auf 1.
7. Stellen Sie **Serverkonfiguration** auf das Serverprofil ein, das für das IP Office erstellt wurde.
8. Wählen Sie in **Adresse des nächsten Sprungs** die IP-Adresse des IP Office aus.

9. Klicken Sie auf **Beenden**.

Weitere Schritte

- Gehen Sie auf Erstellen einer ASBCE Topologie-Ausblendrichtlinie auf Seite 44.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen einer ASBCE Topologie-Ausblendrichtlinie

Das ASBCE kann die Einstellung zum Ausblenden der Topologie verwenden, um Werte in SIP-Nachrichten zu entfernen oder zu ersetzen. Ersetzen Sie beispielsweise eine IP-Adresse in einem SIP-Header durch einen erforderlichen vollqualifizierten Domänennamen.

- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

Voraussetzungen

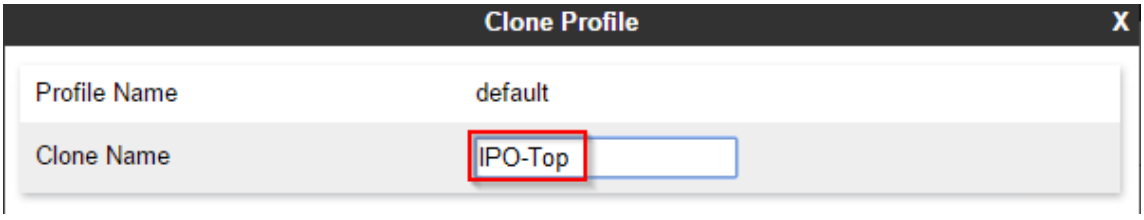
- Erstellen eines Server-Routingprofils auf Seite 43.

Vorgehensweise

1. Wählen Sie **Globale Profile** > **Topologie ausblenden** aus.
2. Wählen Sie das Standardprofil aus und klicken Sie auf **Klonen**.

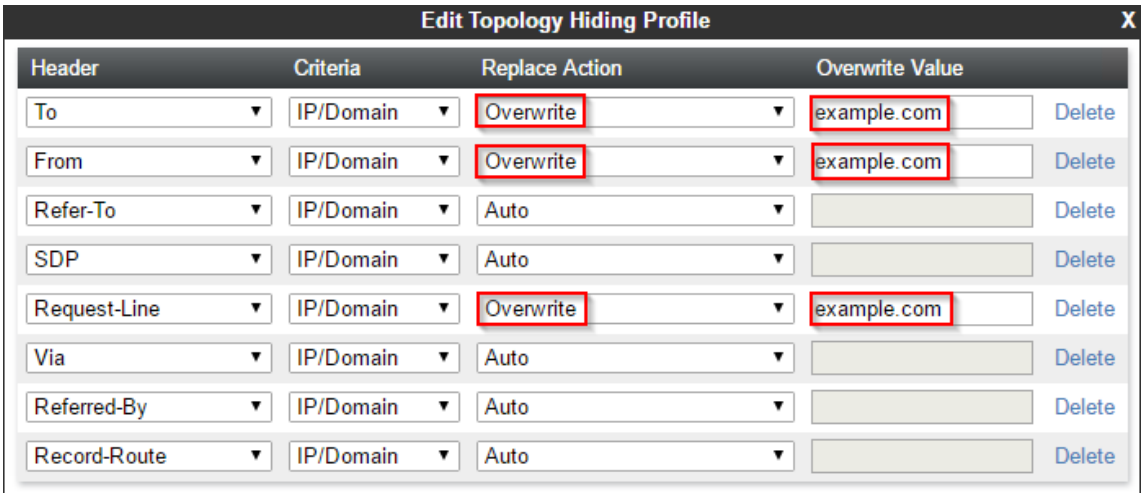
   Wichtig:

   - Sie müssen **Klonen** und das angegebene Profil oder die angegebene Richtlinie verwenden. Mit **Hinzufügen** wird ein neues Profil oder eine neue Richtlinie mit verschiedenen Standardeinstellungen erstellt.
3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.



4. Klicken Sie auf **Beenden**.

5. Wählen Sie das neue Profil aus und klicken Sie auf **Bearbeiten**.



6. Für die Felder **An**, **Von**, **Refer-To**,**SDP** und **Request-Line**:
   a. Setzen Sie **Vorgang „Ersetzen“** auf **Überschreiten**.
   b. Geben Sie die IP OfficeDomäne als **Wert überschreiben** ein.
7. Klicken Sie auf **Beenden**.

Weitere Schritte

- Gehen Sie auf Erstellen einer IP/URI-Blockliste auf Seite 45.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen einer IP/URI-Blockliste

Sie können eine Blockliste verwenden, um die ASBCE Block-IP-Adressen und URIs zu haben, die die Quelle fehlgeschlagener Registrierungsanforderungen sind. Sie können dann die Blockliste zu jedem von Ihnen erstellten Teilnehmer-Flow und Reverse-Proxys hinzufügen.

- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

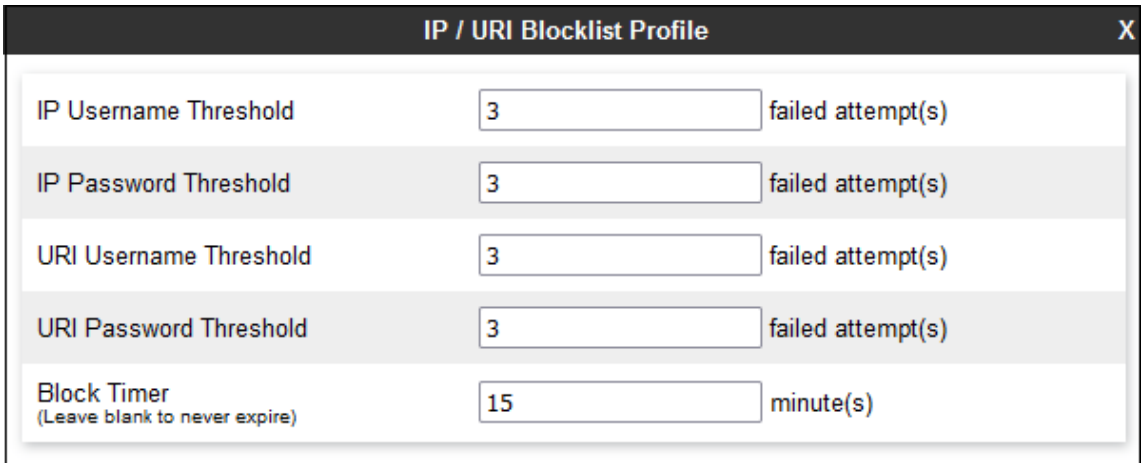
Voraussetzungen

- Erstellen einer ASBCE Topologie-Ausblendrichtlinie auf Seite 44.

Vorgehensweise

1. Wählen Sie **Domänenrichtlinien** > **IP-/URI-Sperrlistenprofil** aus.

2. Klicken Sie auf **Hinzufügen**.



3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.
4. Legen Sie die Anzahl der zulässigen fehlgeschlagenen Namens- und Kennwortversuche fest.
5. Legen Sie fest, wie lange eine IP-Adresse oder ein URI gesperrt wird, nachdem einer der festgelegten Grenzwerte überschritten wurde.
6. Klicken Sie auf **Beenden**.

Weitere Schritte

- Fahren Sie mit Erstellen einer Anwendungsregel auf Seite 46 fort.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen einer Anwendungsregel

Sie können eine Anwendungsregel verwenden, um den Typ der Medienverbindungen einzuschränken, die das ASBCE zulässt. Sie kann auch die maximale Anzahl solcher Verbindungen und die maximale Anzahl von Verbindungen pro Remote-Nebenstelle festlegen.

- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

Voraussetzungen

- Erstellen einer IP/URI-Blockliste auf Seite 45.

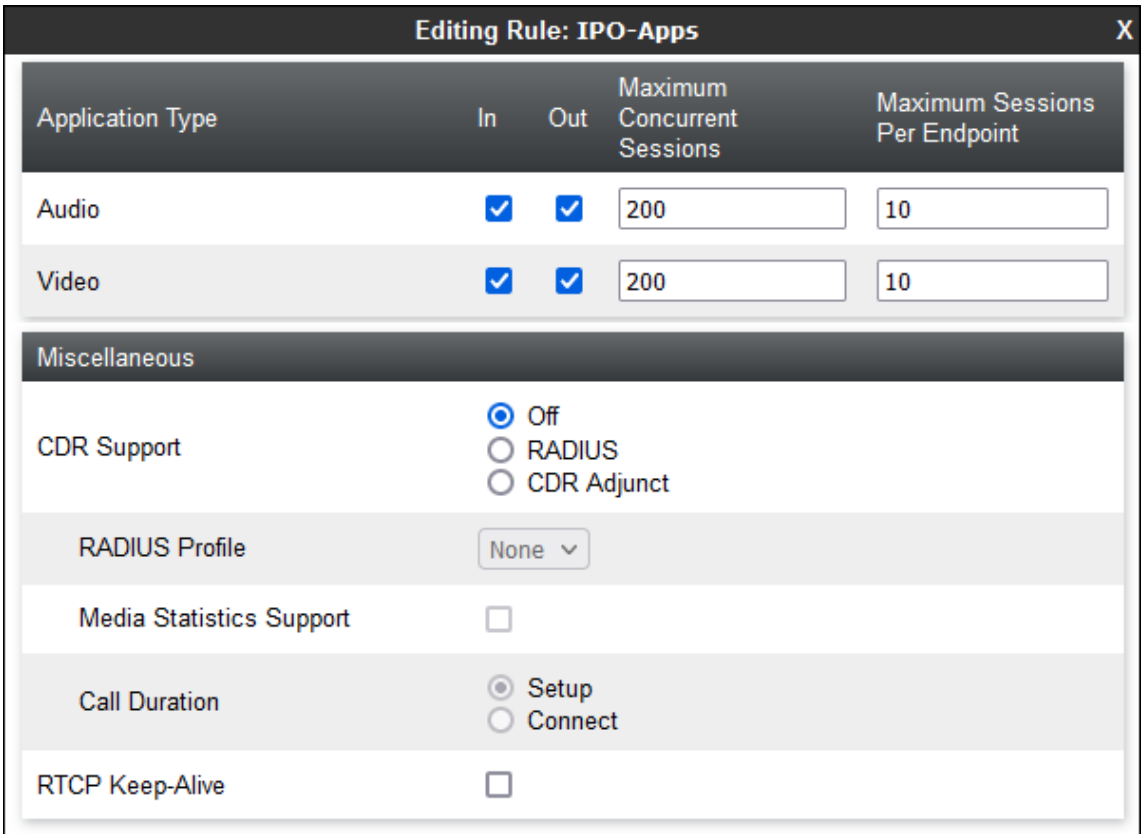
Vorgehensweise

1. Wählen Sie **Domänenrichtlinien** > **Anwendungsregeln** aus.
2. Wählen Sie die *default-low* Richtlinie aus und klicken Sie auf **Klonen**.

Wichtig:

- Sie müssen **Klonen** und das angegebene Profil oder die angegebene Richtlinie verwenden. Mit **Hinzufügen** wird ein neues Profil oder eine neue Richtlinie mit verschiedenen Standardeinstellungen erstellt.

3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.
4. Klicken Sie auf **Beenden**.
5. Wählen Sie die neue Richtlinie aus und klicken Sie auf **Bearbeiten**.
6. Wählen Sie aus, ob **Audio** und/oder **Video** zugelassen werden soll.



7. Legen Sie für jeden der oben genannten den Wert **Maximale Anzahl gleichzeitiger Sitzungen** und **Maximale Anzahl Sitzungen pro Endgerät** fest.
8. Klicken Sie auf **Beenden**.

Weitere Schritte

- Fahren Sie mit Erstellen einer Medienregel auf Seite 48 fort.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen einer Medienregel

Sie können eine Medienregel verwenden, um verschiedene Medieneinstellungen zu definieren.

- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

Voraussetzungen

- Erstellen einer Anwendungsregel auf Seite 46.

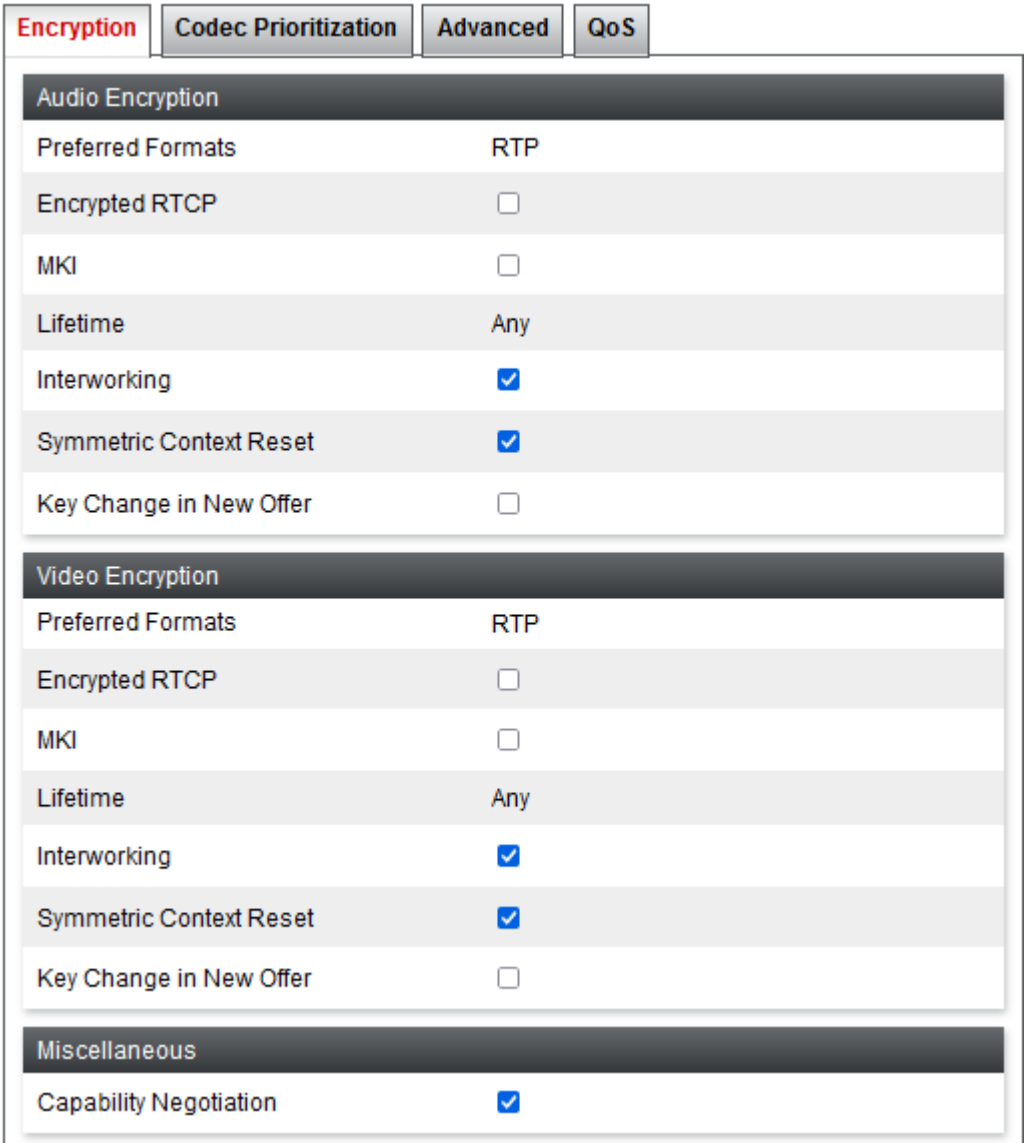
Vorgehensweise

1. Wählen Sie **Domänenrichtlinien** > **Medienregeln** aus.
2. Wählen Sie die *avaya-low-med-enc* Richtlinie aus und klicken Sie auf **Klonen**.

   Wichtig:

   - Sie müssen **Klonen** und das angegebene Profil oder die angegebene Richtlinie verwenden. Mit **Hinzufügen** wird ein neues Profil oder eine neue Richtlinie mit verschiedenen Standardeinstellungen erstellt.
3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.
4. Klicken Sie auf **Beenden**.
5. Wählen Sie die neue Richtlinie aus und klicken Sie auf **Bearbeiten**.

6. Setzen Sie für **Audioverschlüsselung**die **Videoverschlüsselung**-Optionen auf *RTP* und **Bevorzugte Formate**.



   - Wenn Sie SRTP verwenden, legen Sie die Werte **Bevorzugte Formate** und **Verschlüsseltes RTCP** so fest, dass sie mit den **VoIP-Sicherheit**-Einstellungen im IP Office übereinstimmen.
7. Stellen Sie sicher, dass die Einstellung **Erweiterte Einstellungen** > **ANAT aktiviert** nicht ausgewählt ist.
8. Klicken Sie auf **Beenden**.

Weitere Schritte

- Fahren Sie mit Erstellen einer Endgeräterichtliniengruppe auf Seite 50 fort.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen einer Endgeräterichtliniengruppe

Eine Endgeräterichtlinie gruppiert Regeln wie Medien- und Anwendungsregeln. Nach dem Erstellen einer Endpunktrichtlinie können Sie sie mit den von Ihnen erstellten Teilnehmer- und Server-Flows verknüpfen.

- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

Voraussetzungen

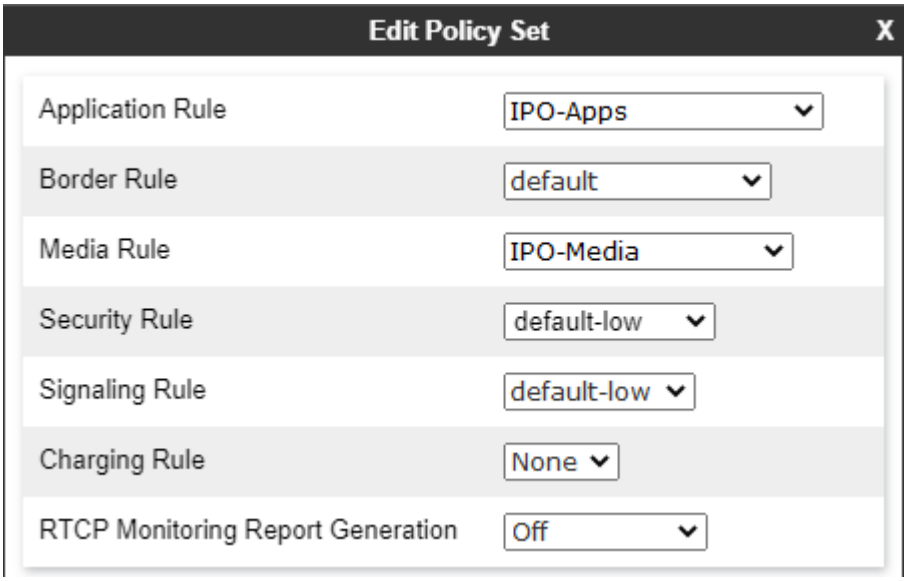
- Erstellen einer Medienregel auf Seite 48.

Vorgehensweise

1. Wählen Sie **Domänenrichtlinien** > **Endpunkt-Richtliniengruppen** aus.
2. Wählen Sie die *default-low* Richtlinie aus und klicken Sie auf **Klonen**.

   Wichtig:

   - Sie müssen **Klonen** und das angegebene Profil oder die angegebene Richtlinie verwenden. Mit **Hinzufügen** wird ein neues Profil oder eine neue Richtlinie mit verschiedenen Standardeinstellungen erstellt.
3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.
4. Klicken Sie auf **Beenden**.
5. Wählen Sie die neue Richtlinie aus und klicken Sie auf **Bearbeiten**.
6. Wählen Sie in **Anwendungsregel** die Anwendungs- und Medienregeln aus, die Sie für die Remote-Nebenstellen erstellt haben.



7. Wählen Sie in **Medienregel** die von Ihnen erstellte Medienregel aus.
8. Klicken Sie auf **Beenden**.

Weitere Schritte

- Fahren Sie mit Konfigurieren eines User-Agent-Profils auf Seite 51 fort.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Konfigurieren eines User-Agent-Profils

Sie können **Benutzer-Agenten** verwenden, um die ASBCE Verbindung auf die Clients und Telefone einzuschränken, die eine übereinstimmende *User Agent* (*UA*) Zeichenfolge senden. Andernfalls kann jedes Telefon oder jeder Client eine Verbindung herstellen.

- **Duale Unterstützung für IPv4/IPv6:** Sie können denselben Eintrag für IPv4- und IPv6-Remote-Nebenstellen verwenden.

Im Folgenden finden Sie Beispiele für *UA*-Zeichenfolgen, die von Avaya-Clients gesendet werden.

Avaya Telefon oder Client	User Agent
Telefone der Serie Avaya 9600	*Avaya one-X Deskphone*
Avaya J159	*Avaya J159 IP Phone 4.0.10.3.2*
Avaya Workplace-Client – Android	*Avaya Communicator Android/3.35.2 (FA-RELEASE80-BUILD.18; Pixel 8 Pro)*
Avaya Workplace-Client – Windows	*Avaya Communicator/3.0 (3.33.0.96.6; Avaya SDK; Microsoft Windows NT 10.0.19045.0)*

- Wie oben dargestellt, kann die *UA*-Zeichenfolge je nach Softwareversion und Plattform variieren.
- Sie können das an ein bestimmtes Telefon oder Softphone gesendete *UA* nach der Registrierung des Telefons oder Clients in SysMonitor anzeigen.

Der UA-Abgleich verwendet einen Regex-Zeichenfolgeabgleich (Regulärer Ausdruck). Im Folgenden finden Sie ein Beispiel für Regex-Zeichenfolgen:

Regulärer Ausdruck	Beschreibung
`Avaya.*`	Entspricht jedem *UA*, der mit *Avaya* beginnt. . entspricht einem beliebigen Zeichen. *.** entspricht einer beliebigen Anzahl von Zeichen.
`Avaya J1.*`	Entspricht der *UA*-Zeichenfolge eines beliebigen Telefons der Serie J100.
`Avaya (J1|Communicator).*`	Entspricht der Zeichenfolge *UA* der Telefone der Serie J100 und Avaya Workplace-Client. Die Klammern *( )* umschließen die möglichen Übereinstimmungen, wobei jede potenzielle Übereinstimmung durch ein |-Zeichen getrennt ist.
`Avaya Communicator\/3\.0 \(3\.33.*`	Entspricht der Zeichenfolge *UA* nur der Windows 3.33-Version von Avaya Workplace-Client. Der Regex-Ausdruck stellt Zeichen ein \ voran, die ansonsten als Regex-Befehle behandelt würden. Zum Beispiel stimmt . mit jedem Zeichen überein, während \. nur mit einem buchstäblichen . Zeichen übereinstimmt.

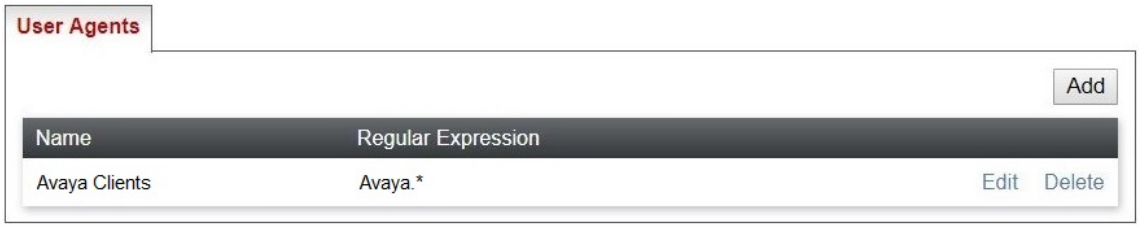
Weitere Informationen zum Erstellen von Regex-Zeichenfolgen finden Sie unter https://learn.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference und https://regex101.com.

Voraussetzungen

- Erstellen einer ASBCE Topologie-Ausblendrichtlinie auf Seite 44.

Vorgehensweise

1. Wählen Sie **System Management** > **Globale Parameter** > **Benutzer-Agenten** aus.
2. Klicken Sie auf **Hinzufügen**.



3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.
4. Geben Sie den regulären Ausdruck für die User-Agent-Zeichenfolge oder -zeichenfolgen ein, die übereinstimmen sollen.
5. Klicken Sie auf **Beenden**.

Weitere Schritte

- Gehen Sie auf Erstellen des Teilnehmer-Flows auf Seite 52.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen des Teilnehmer-Flows

Das ASBCE verwendet einen Teilnehmer-Flow, um eingehende Verbindungen von Remote-Nebenstellen zu bearbeiten.

- **Duale Unterstützung für IPv4/IPv6:** Zur Unterstützung von IPv4- und IPv6-Remote-Nebenstellen müssen Sie separate Einträge für IPv4 und IPv6 erstellen:
  - Die Schnittstellen **Signalisierungsschnittstelle** und **Medien-Schnittstelle** müssen jeweils die entsprechenden externen IPv4- oder IPv6-Schnittstellen verwenden.

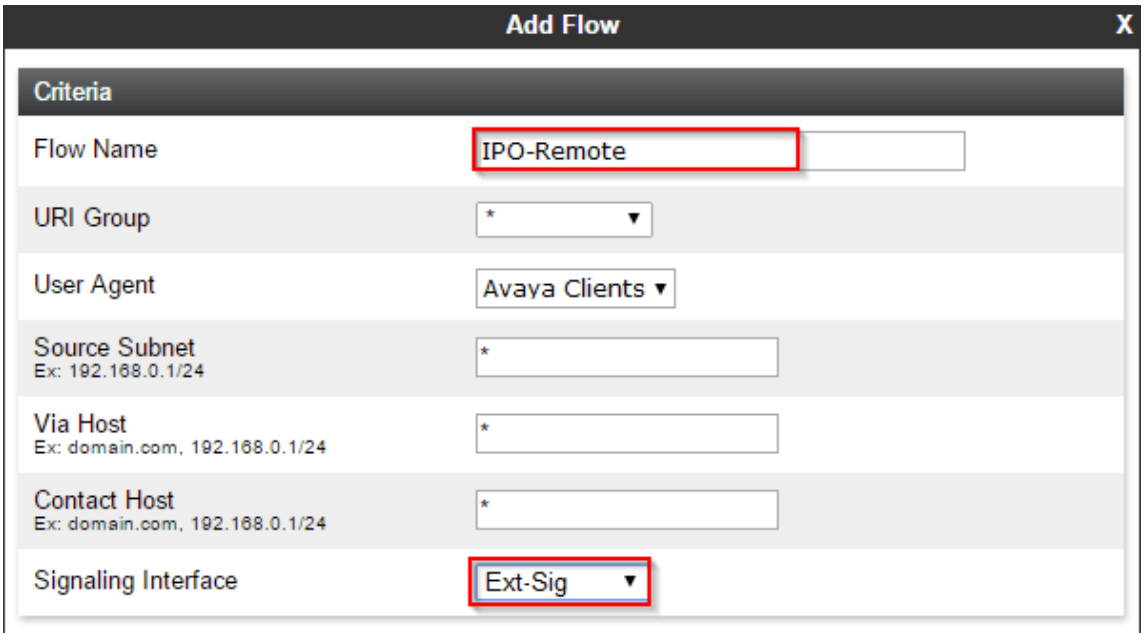
Voraussetzungen

- Konfigurieren eines User-Agent-Profils auf Seite 51.

Vorgehensweise

1. Wählen Sie **Gerätespezifische Einstellungen** > **Endpunkt-Flows** aus.

2. Wählen Sie die Registerkarte **Teilnehmer-Flows** und klicken Sie auf **Hinzufügen**.

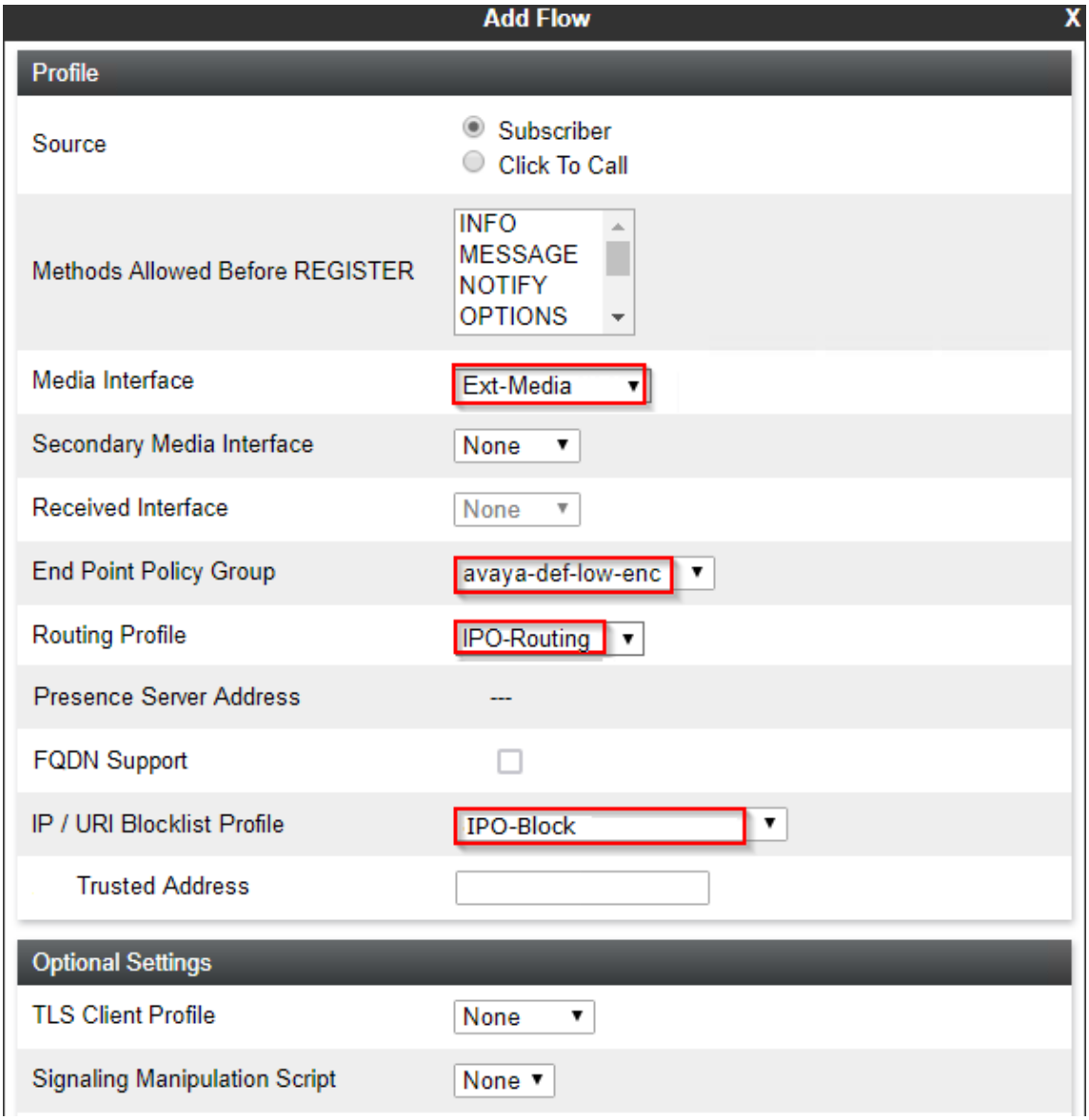


a. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.

b. Wählen Sie bei Bedarf das **Benutzer-Agent** Profil aus, das Sie erstellt haben, um mit der UA der Clients übereinzustimmen, die den Teilnehmer-Flow verwenden dürfen.

c. Wählen Sie die für die Remote-Nebenstellen **Signalisierungsschnittstelle** erstellte externe aus.

3. Klicken Sie auf **Weiter**.



   a. Wählen Sie in **Medien-Schnittstelle** die externe Medienschnittstelle aus, die für die Remote-Nebenstellen erstellt wurde.
   b. Wählen Sie unter **Endpunkt-Richtliniengruppe** *avaya-def-low-enc* aus.
   c. Wählen Sie in **Routing-Profil** das Server-Routingprofil aus, das für das IP Office erstellt wurde.
   d. Wenn Sie ein Blocklistenprofil erstellt haben, wählen Sie es in der **IP-/URI-Sperrlistenprofil** Dropdown-Liste aus.

4. Klicken Sie auf **Beenden**.
5. Wenn sowohl IPv4- als auch IPv6-Remote-Nebenstellen unterstützt werden, wiederholen Sie den Vorgang, um die IPv6-Einträge zu erstellen.

Weitere Schritte

- Gehen Sie auf Erstellen eines Server-Flows auf Seite 55.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Erstellen eines Server-Flows

Das ASBCE verwendet einen Server-Flow, um eingehende Verbindungen vom IP Office Server zu bearbeiten.

- **Duale Unterstützung für IPv4/IPv6:** Zur Unterstützung von IPv4- und IPv6-Remote-Nebenstellen müssen Sie separate Einträge für IPv4 und IPv6 erstellen:
  - Das **Erhaltene Schnittstelle** muss für jeden Server-Flow die entsprechende externe IPv4- oder IPv6-Signalisierungsschnittstelle verwenden.

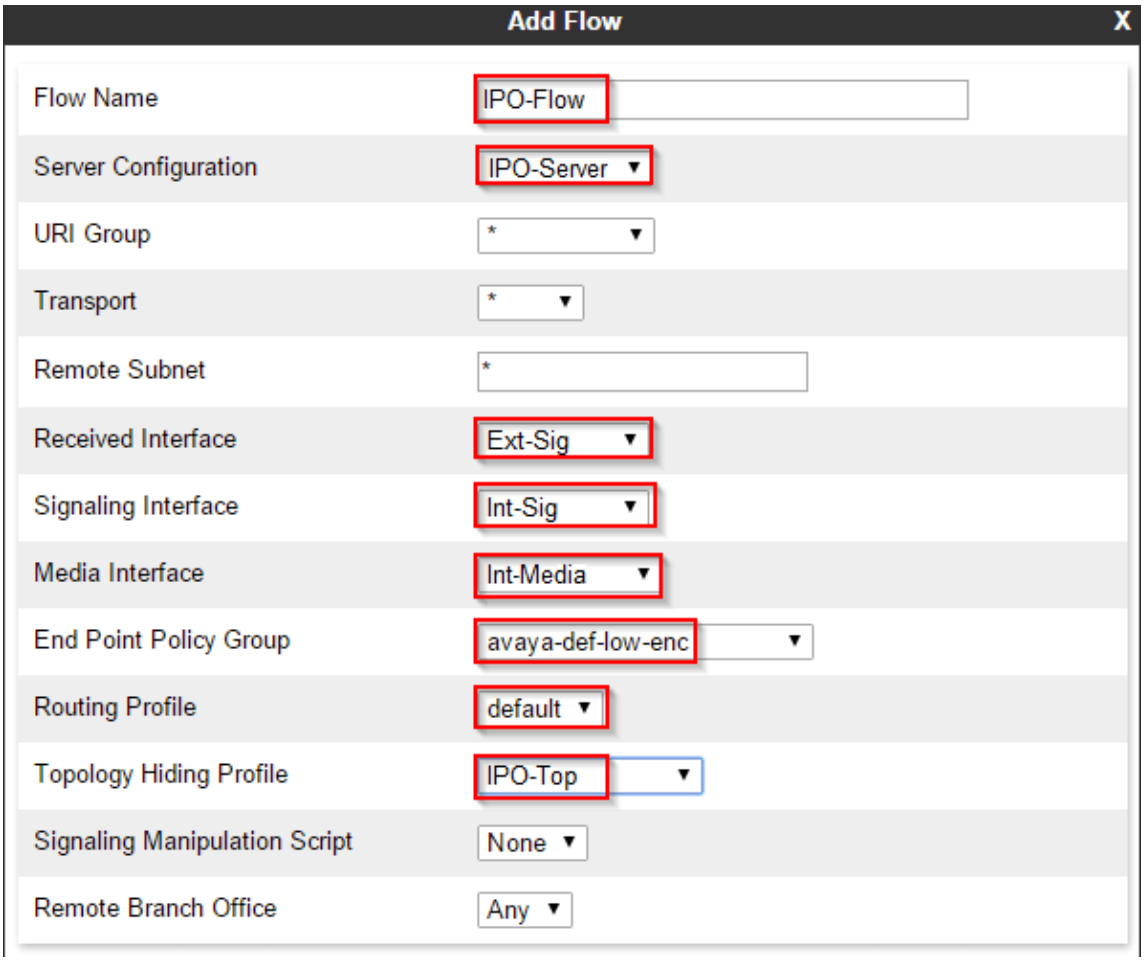
Voraussetzungen

- Erstellen des Teilnehmer-Flows auf Seite 52.

Vorgehensweise

1. Wählen Sie **Gerätespezifische Einstellungen** > **Endpunkt-Flows** aus.

2. Wählen Sie die Registerkarte **Server-Flows** und klicken Sie auf **Hinzufügen**.



   a. Geben Sie in **Flow-Name** einen beschreibenden Namen ein.
   b. Wählen Sie in **Serverkonfiguration** das für den IP Office Server erstellte Serverprofil aus.
   c. Wählen Sie in **Erhaltene Schnittstelle** die externe Signalisierungsschnittstelle aus, die für die Remote-Nebenstellen erstellt wurde.
   d. Wählen Sie in **Signalisierungsschnittstelle** die interne Signalisierungsschnittstelle aus, die für die Remote-Nebenstellen erstellt wurde.
   e. Wählen Sie in **Medien-Schnittstelle** die interne Medienschnittstelle aus, die für die Remote-Nebenstellen erstellt wurde.
   f. Wählen Sie unter **Endpunkt-Richtliniengruppe** *avaya-def-low-enc* aus.
   g. Wählen Sie unter **Routing-Profil** *default* aus.
   h. Wählen Sie in **Profil für ausgeblendete Topologie** das Topologie-Ausblendprofil aus, das für IP Office Remote-Nebenstellen erstellt wurde.
3. Klicken Sie auf **Beenden**.
4. Wenn sowohl IPv4- als auch IPv6-Remote-Nebenstellen unterstützt werden, wiederholen Sie den Vorgang, um die IPv6-Einträge zu erstellen.

Weitere Schritte

- Gehen Sie auf Hinzufügen von Reverse Proxys für Dateianforderungen auf Seite 57.

Verwandte Links

ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25

Hinzufügen von Reverse Proxys für Dateianforderungen

Im Folgenden finden Sie ein Beispiel zum Erstellen von Reverse Proxys für Remote-Nebenstellen. Dadurch können Remote-Nebenstellen Dateien vom IP Office anfordern. Beispiel: Anfordern der Dateien `46xxsettings.txt` und `46xxspecials.txt`.

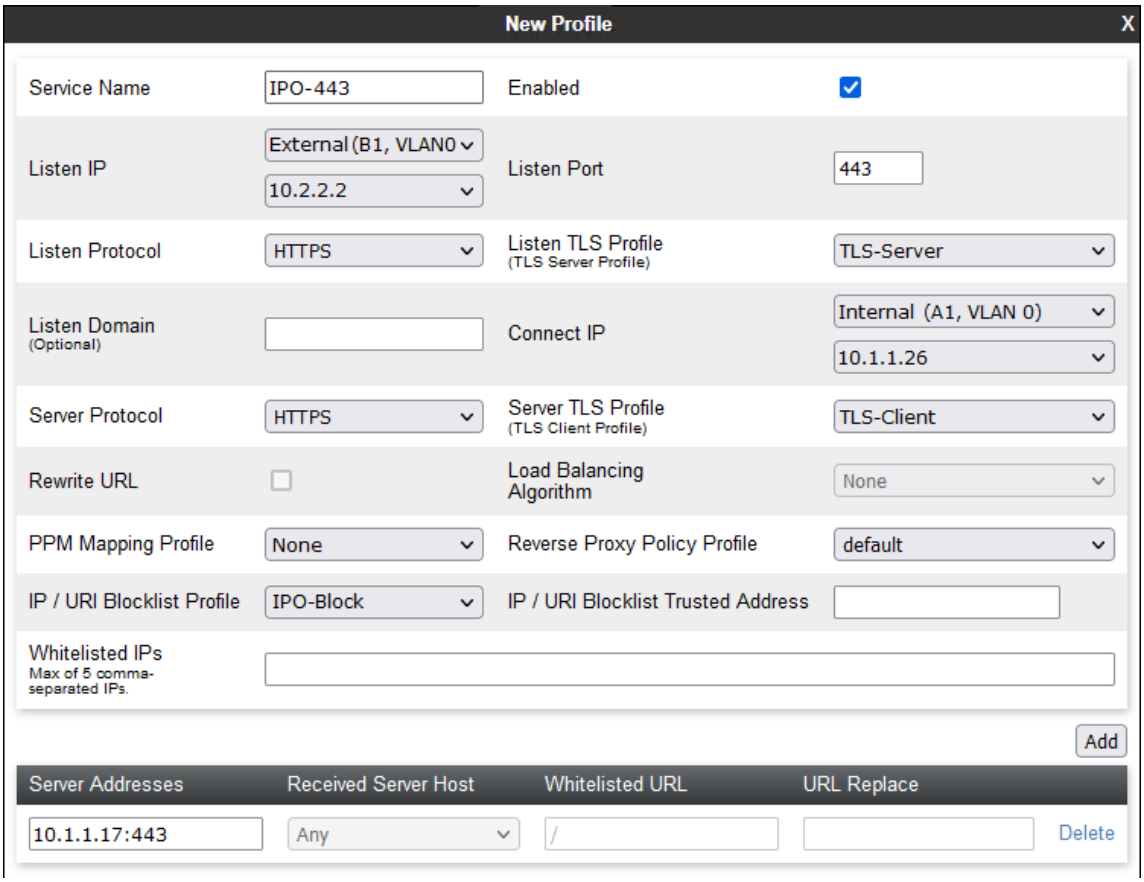
Die erforderlichen Ports und Protokolle hängen von den Anforderungen des Typs der Remote-Nebenstelle ab.

- Standardmäßig verwenden Nebenstellen entweder `http` oder `https`, um bei der ersten Verbindung mit IP Office die Datei `46xxsettings.txt`abzurufen. IP Office verwendet Port `80` bzw. Port `443`.
- Die `46xxsettings.txt` Einstellungen geben an, welche Ports und Protokolle für zukünftige Verbindungen verwendet werden sollen.
- Wenn **System** > **System** > **Bevorzugte Telefonports verwenden** aktiviert ist, weist `46xxsettings.txt` Telefone und Clients an, den Port `8411` für HTTP und den Port `411` für HTTPS-Dateianforderungen zu verwenden, und diese Ports sind auf IP Office aktiviert.
  - Wenn **Bevorzugte Telefonports verwenden** aktiviert ist, ermöglicht das IP Office weiterhin Verbindungen an Port `80` und Port `443`. Das IP Office erfordert dies für die Erstverbindung und für Legacy-Clients.
- **Duale Unterstützung für IPv4/IPv6:** Zur Unterstützung von IPv4- und IPv6-Remote-Nebenstellen müssen Sie separate Einträge für IPv4 und IPv6 erstellen. Jeder Eintrag verwendet die entsprechenden externen IPv4- und IPv6-Schnittstellen.

Vorgehensweise

1. Wählen Sie **Gerätespezifische Einstellungen** > **DMZ-Dienste** > **Relais-Dienste** aus.

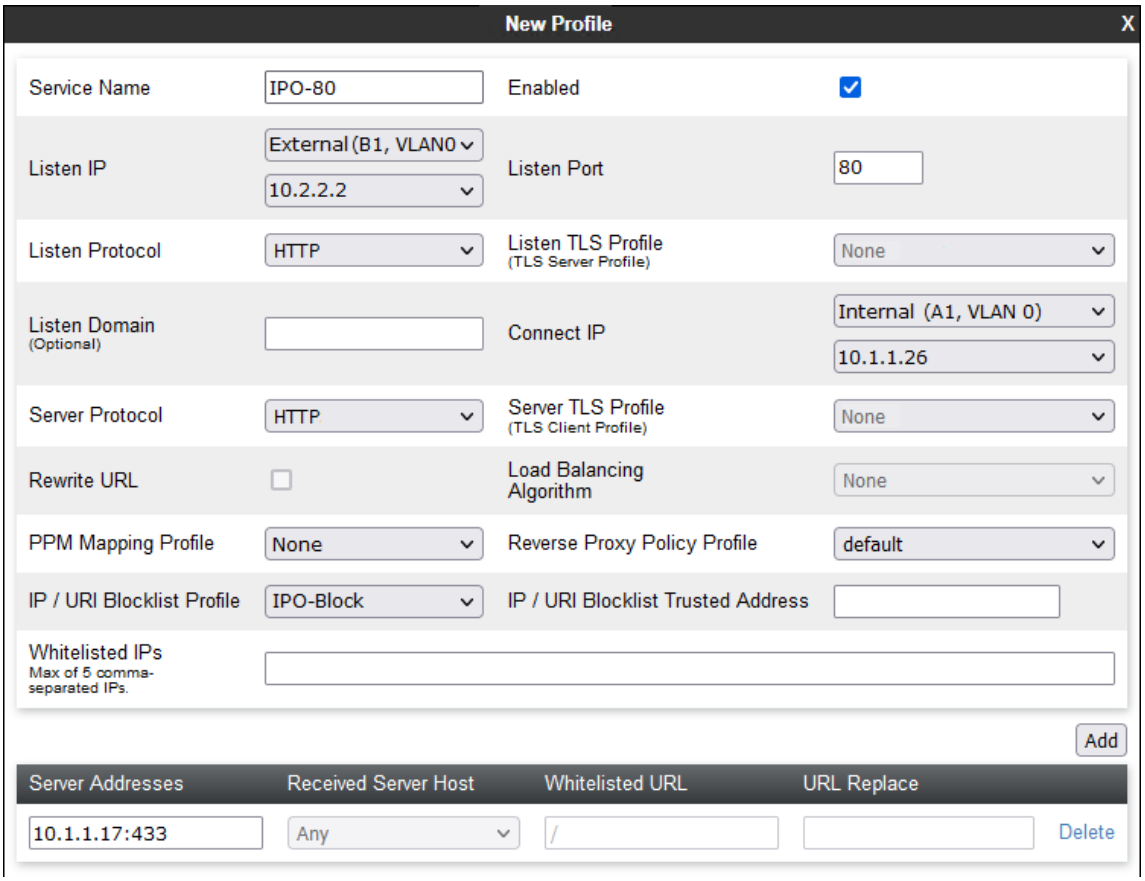
2. Wählen Sie die Registerkarte **Reverse-Proxy** und klicken Sie auf **Hinzufügen**.



   a. Geben Sie unter **Dienst-Name** einen aussagekräftigen Namen für den Reverse Proxy ein.
   b. Wählen Sie in **Listening-IP** die externe *B1* Schnittstelle und die IP-Adresse aus.
   c. Setzen Sie **Listening-Port** auf `443`.
   d. Setzen Sie **Listening-Protokoll** auf **HTTPS**.
   e. Wählen Sie in **Listening-TLS-Profil** das TLS-Serverprofil aus.
   f. Wählen Sie in **Verbindungs-IP** die interne *A1* Schnittstelle und IP-Adresse aus.
   g. Wählen Sie unter **Server-Protokoll HTTPS** aus.
   h. Wählen Sie in **Server-TLS-Profil** das TLS-Clientprofil aus.
   i. Wenn Sie eine Blockliste erstellt haben, wählen Sie sie über das **IP-/URI-Sperrlistenprofil** Dropdown-Menü aus.
   j. Klicken Sie auf **Hinzufügen**:
   k. Geben Sie unter **Server-Adresse** die IP Office IP-Adresse gefolgt von `:443` ein.

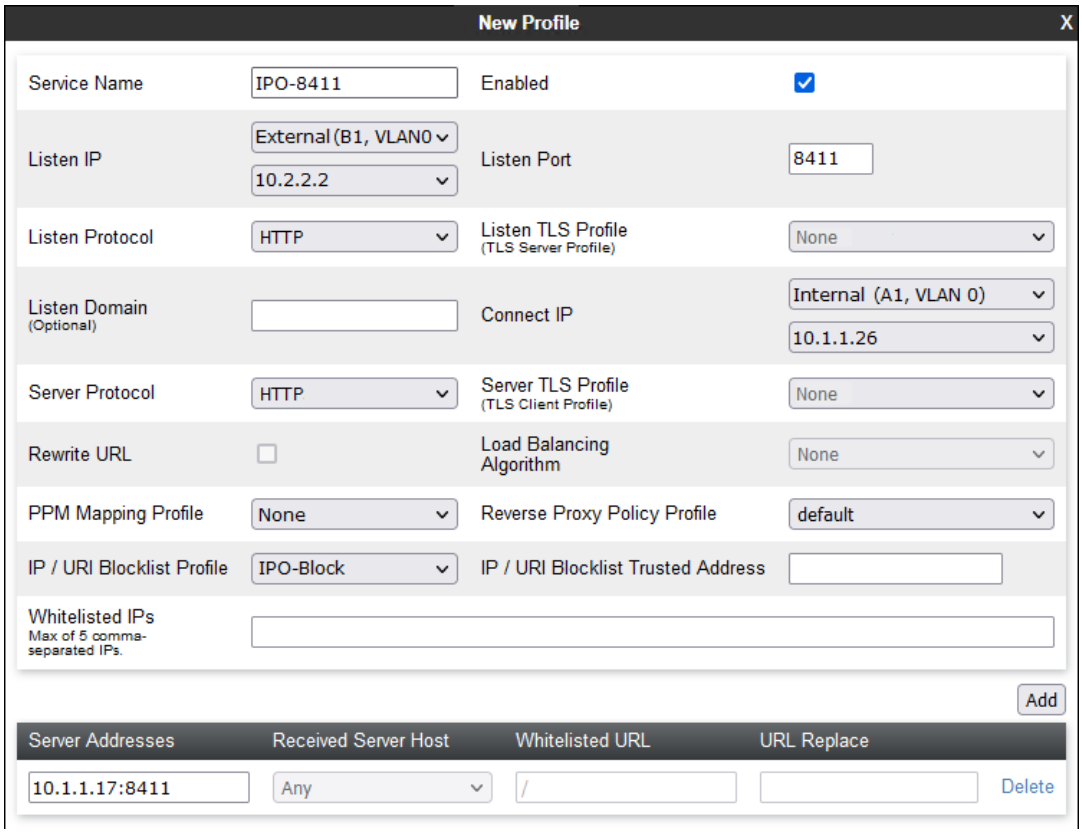
3. Klicken Sie auf **Beenden**.

4. Wiederholen Sie das Verfahren, um einen Proxy für HTTP-Dateianforderungen an Port `80` hinzuzufügen. Dieser Proxy verwendet keine TLS-Profile.

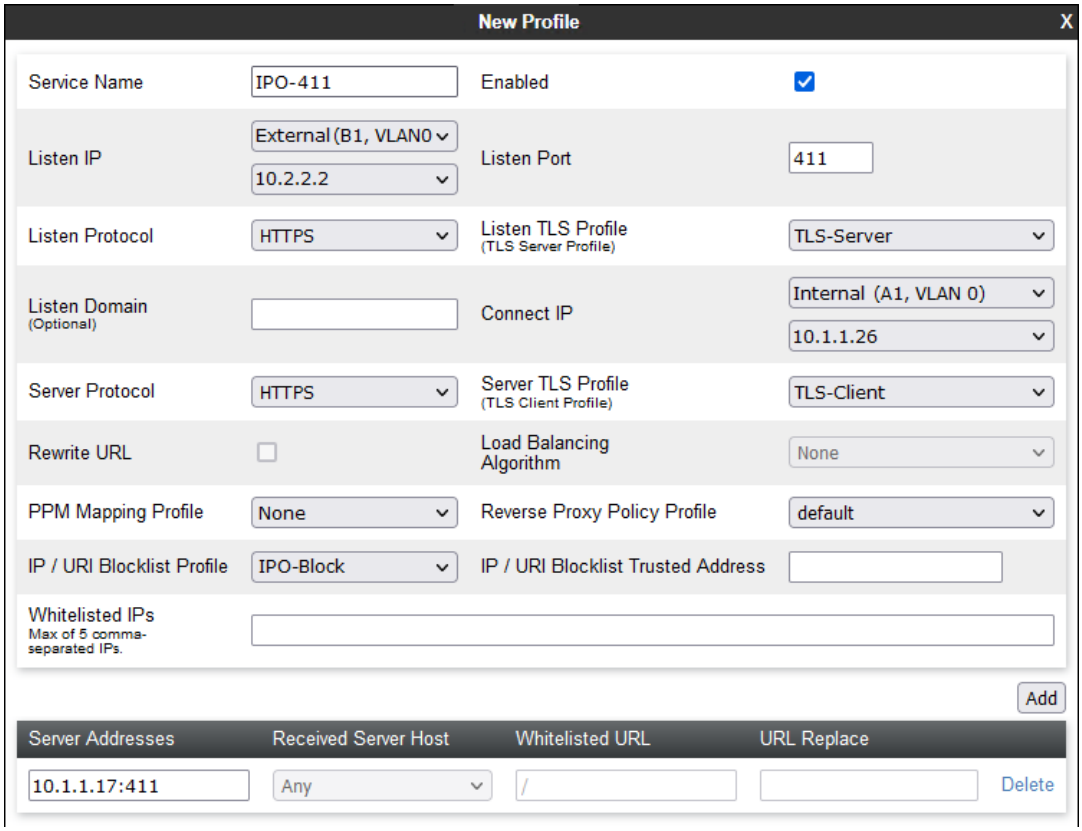


5. Klicken Sie auf **Beenden**.

6. Wenn auf dem IP Office **Bevorzugte Telefonports verwenden** aktiviert ist:
   a. Fügen Sie einen Reverse Proxy für HTTP am Port `8411` hinzu.



b. Fügen Sie einen Reverse Proxy für HTTPS am Port `411` hinzu.



7. Wenn sowohl IPv4- als auch IPv6-Remote-Nebenstellen unterstützt werden, wiederholen Sie den Vorgang, um die IPv6-Einträge zu erstellen.

Verwandte Links

[ASBCE Konfiguration für Remote-SIP-Nebenstellen](#) auf Seite 25

Kapitel 5: Aufheben der Verbindung mit Anrufmedien über das ASBCE

Das ASBCE bleibt normalerweise Teil aller von ihm weitergeleiteten Anrufe. Alle Anrufmedien und Anrufsignale bleiben mit dem ASBCE verankert und erfordern daher Bandbreite und Verarbeitung vom ASBCE.

In Szenarien, in denen die beteiligten Netzwerke direktes Routing zwischen allen Anrufenden unterstützen, können Sie die Verbindung der Anrufmedien über das ASBCE aufheben. Durch das Aufheben der Verbindung werden die Bandbreite und die Ressourcen reduziert, die vom ASBCE benötigt werden. Das ASBCE bearbeitet weiterhin die Anrufsignalisierung.

- Bei Remote-Nebenstellen im selben Remote-Subnetz ermöglicht ASBCE das Aufheben der Verbindung zwischen den Remote-Nebenstellen im Subnetz Direktverbindungen.
- Möglicherweise können Sie das Aufheben der Verbindung auch in anderen Szenarien verwenden. Zum Beispiel zwischen Remote-Nebenstellen in zwei separaten Subnetzen. Weitere Informationen finden Sie unter https://documentation.avaya.com/bundle/GUID-416B16B1-7DB4-4C01-A966-3E62EFEA4D43/page/Media_Unanchoring_scenarios.html.

Beim Aufheben der Verbindung werden die folgenden zusätzlichen ASBCE Konfigurationselemente verwendet:

- **Sitzungsverlauf**

  Ein Sitzungsverlauf definiert ein Paar Netzwerkadressbereiche und welche Sitzungsrichtlinie ASBCE für den Datenverkehr zwischen diesen Netzwerken anwenden soll. Bei Direktverbindungen an einem Remote-Standort wird der Adressbereich des Standorts für beide Netzwerke im Sitzungsverlauf festgelegt.

- **Sitzungsrichtlinie**

  Eine Sitzungsrichtlinie legt fest, wie das ASBCE Anrufmedien behandeln soll. Sie können dieselbe Sitzungsrichtlinie für mehrere Sitzungsverläufe verwenden.

Verwandte Links

Erstellen einer Sitzungsrichtlinie für einen Remote-Standort auf Seite 62
Erstellen eines Sitzungsverlaufs für den Remote-Standort auf Seite 64

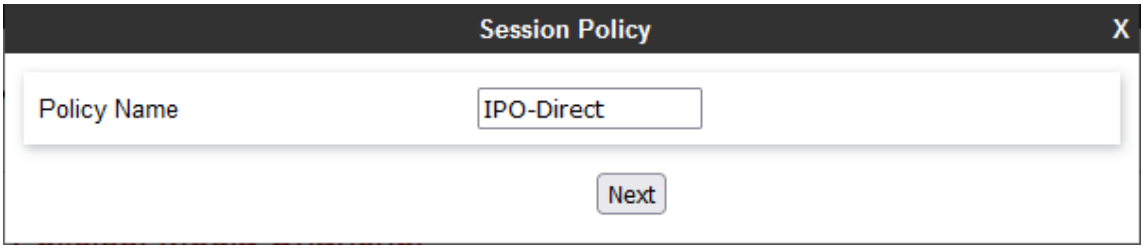
Erstellen einer Sitzungsrichtlinie für einen Remote-Standort

Eine Sitzungsrichtlinie legt fest, wie ASBCE den Datenverkehr zwischen Standorten behandeln soll, der mit jedem Sitzungsverlauf übereinstimmt, der die Richtlinie verwendet. Sie können

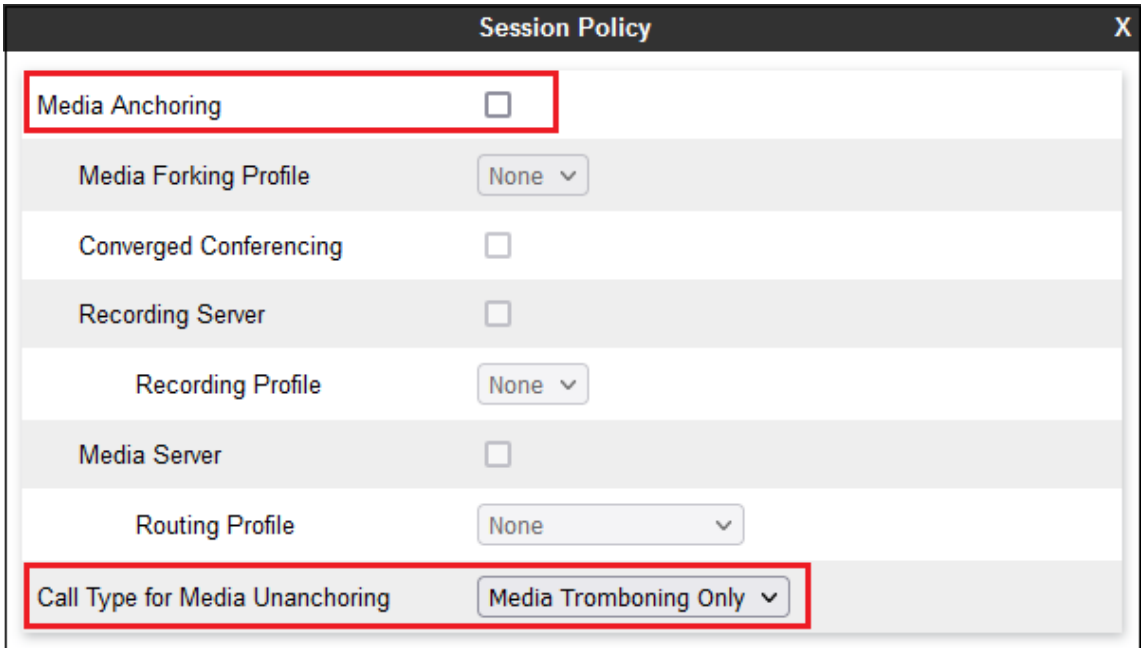
dieselbe Richtlinie für mehrere Sitzungsverläufe verwenden. Das heißt, für mehrere Remote-Standorte.

Vorgehensweise

1. Wählen Sie **Domänenrichtlinien** > **Sitzungsrichtlinien** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.



4. Klicken Sie auf **Weiter**.



5. Deaktivieren Sie **Media Anchoring**.
6. Setzen Sie **Anruftyp für Media-Unanchoring** auf **Nur Media-Tromboning**.
7. Klicken Sie auf **Beenden**.

Weitere Schritte

- Gehen Sie auf Erstellen eines Sitzungsverlaufs für den Remote-Standort auf Seite 64.

Verwandte Links

Aufheben der Verbindung mit Anrufmedien über das ASBCE auf Seite 62

Erstellen eines Sitzungsverlaufs für den Remote-Standort

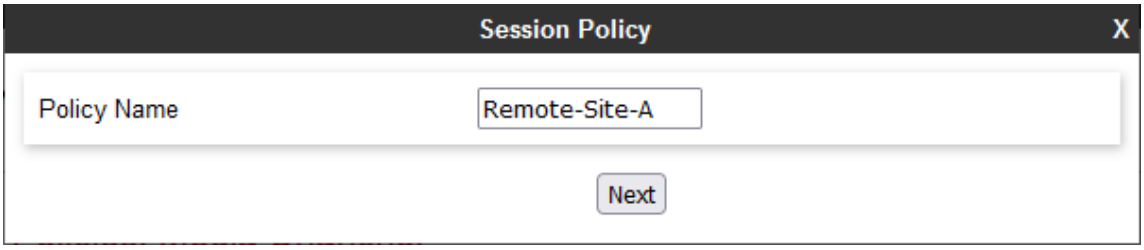
Ein Sitzungsverlauf definiert Adressbereiche, zwischen denen das ASBCE eine Sitzungsrichtlinie anwenden soll. Bei einem Remote-Subnetz sind die Adressbereiche auf beiden Seiten gleich.

Voraussetzungen

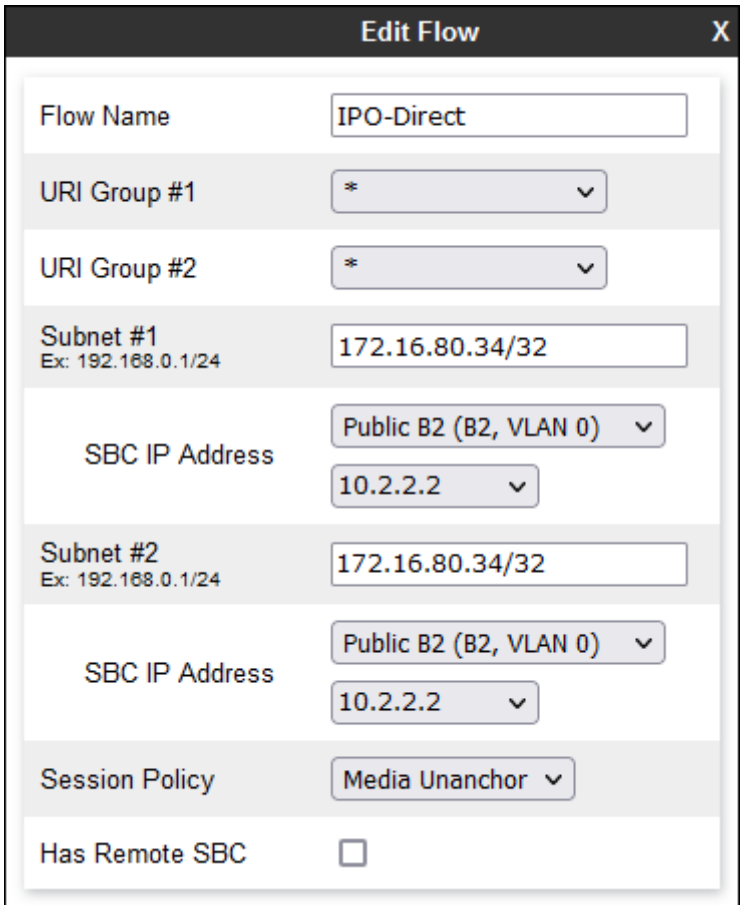
- Erstellen einer Sitzungsrichtlinie für einen Remote-Standort auf Seite 62.

Vorgehensweise

1. Wählen Sie **Netzwerk und Flows** > **Sitzungsverläufe** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie bitte einen Namen ein. Sie können diese Option dann verwenden, um die Richtlinie in anderen Menüs auszuwählen.



4. Klicken Sie auf **Weiter**.



5. Legen Sie für **Subnetz#1** den IP-Adressbereich fest, der von Remote-Nebenstellen am Remote-Standort verwendet wird. Stellen Sie **SBC-IP-Adresse** auf die externe Schnittstelle des ASBCE ein.
6. Legen Sie die gleichen Werte für **Subnetz#2** fest.
7. Wählen Sie für **Sitzungsrichtlinie** die von Ihnen erstellte Sitzungsrichtlinie aus.
8. Klicken Sie auf **Beenden**.

Verwandte Links

Aufheben der Verbindung mit Anrufmedien über das ASBCE auf Seite 62

Kapitel 6: Unterstützung von Avaya Workplace-Client als Remote-Nebenstelle

Dieser Abschnitt enthält Hinweise zum Betrieb von Avaya Workplace-Client, wenn es als Remote-SIP-Nebenstelle für IP Office verwendet wird.

Verwandte Links

[Avaya Workplace-Client SIP-Registrierung](#) auf Seite 66
[Überprüfen der Remote-Einstellungen](#) auf Seite 67

Avaya Workplace-Client SIP-Registrierung

1. Benutzer können ihre Avaya Workplace-Client beim Start mit den folgenden Methoden registrieren:

   - **Direkte Registrierung:**

     Der Benutzer gibt die IP Office Adresse im Format `https://<IPOffice_FQDN>/46xxsettings.txt` ein, wenn `://<IPOffice_FQDN>/` der FQDN des auf dem IP Office konfigurierten SIP-Registrars ist.

     - Bei Remote-Nebenstellen löst öffentliches DNS den FQDN auf die öffentliche IP-Adresse der Netzwerk-Firewall des Kunden auf.
     - Für IPv6 muss der Benutzer `https://<SBC_FQDN>/46xxsettings.txt` verwenden, wobei <SBC_FQDN> der FQDN des ASBCE ist.

   - **E-Mail-basierte Adressregistrierung:**

     Der Benutzer gibt seine E-Mail-Adresse ein. Der Client kontaktiert Avaya Spaces, wobei das für die E-Mail-Domäne des Kunden konfigurierte Profil die FQDN-Adresse des IP Office Systems bereitstellt.

     - Dieses Registrierungsverfahren wird für IPV6-Remote-Nebenstellen nicht unterstützt.

   - **SSO-Anmeldung**

     Bei dieser Anmeldemethode wurden dieselben Avaya Spaces Profilinformationen wie bei der E-Mail-basierten Registrierung oben verwendet.

     - Dieses Registrierungsverfahren wird für IPV6-Remote-Nebenstellen nicht unterstützt.

2. Nach Erhalt der Datei `46xxsettings.txt` von IP Office sendet Avaya Workplace-Client eine DNS-Anfrage nach der IP-Adresse des FQDN, der ihm in der **SIP_CONTROLLER_LIST** in der Datei `46xxsettings.txt` zugewiesen wurde.
   - Bei Remote-Nebenstellen werden die in der automatisch generierten Datei `46xxsettings.txt` verwendeten Werte in den **System** > **LAN1** > **Netzwerktopologie** > **SBC**-Einstellungen in der IP Office Konfiguration festgelegt.
3. Der Client versucht dann, sich mit der vom DNS-Server zurückgegebenen IP-Adresse als SIP-Nebenstelle zu registrieren. Bei einer Remote-Nebenstelle ist dies die öffentliche IP-Adresse des Kunden für seine Netzwerk-Firewall oder ASBCE.

Verwandte Links

Unterstützung von Avaya Workplace-Client als Remote-Nebenstelle auf Seite 66

Überprüfen der Remote-Einstellungen

Mit einem Remote-PC können Sie die Einstellungen für Remote-Nebenstellen anzeigen und überprüfen.

Vorgehensweise

1. Verwenden Sie **nslookup**, um zu überprüfen, ob DNS den FQDN für IP Office auf die richtigen IP-Adressen auflöst.

```
C:\ nslookup ipo.example.com
Server:  Unknown
Address: 203.0.113.30
```

2. Fordern Sie mit einem Browser die Datei `46xxsettings.txt` vom IP Office an. Geben Sie beispielsweise `ipo.example.com/46xxsettings.txt` ein.
3. Überprüfen Sie den angezeigten Portbereich. Avaya Workplace-Client kann RTP/RTCP-Ports im Bereich `40750 to 50750` verwenden.

```
# SIPXAUTOGENERATEDSETTINGS
IF $SIG_IN_USE SEQ H323 GOTO 96X1AUTOGENERATEDSETTINGS
SET RTP_PORT_LOW 40750
SET RTP_PORT_RANGE 10002
SET TLSSRVRID 1
```

4. Andere Einstellungen zeigen die Werte an, die von Avaya Workplace-Client für die Verbindung mit IP Office-Diensten verwendet werden:

```
# K1EXAUTOGENERATEDSETTINGS
SET ENABLE_AVAYA_CLOUD_ACCOUNTS 1
SET SIP_CONTROLLER_LIST ipo.example.com:5061;transport=tls
SET CONFERENCE_FACTORY_URI "ConfServer@ipo.example.com"
SET PSTN_VM_NUM "VM.user@ipo.example.com"
SET SETTINGS_FILE URL "https://ipo.example.com:411/46xxsettings.txt"
SET FQDN IP MAP "ipo.example.com=10.1.1.17"
```

5. Überprüfen Sie bei Kontakten und Anwesenheitsdiensten, ob die Werte `IPO_PRESENCE_ENABLED` und `IPO_CONTACTS_ENABLED` auf `1` eingestellt sind.

```
# SETTINGSK1EX
SET SSOENABLED 0
SET EWSSSO 0
SET SIPREGPROXYPOLICY "alternate"
SET IPO_PRESENCE_ENABLED 1
SET IPO_CONTACTS_ENABLED 1
SET DND_SAC_LINK 1
SET POUND_KEY_AS_CALL_TRIGGER 0
```

Verwandte Links

Unterstützung von Avaya Workplace-Client als Remote-Nebenstelle auf Seite 66

Kapitel 7: Überprüfen des Status der Remote-Nebenstelle im ASBCE

Das ASBCE bietet eine Reihe von Menüs, die den Status der Verbindungen anzeigen und versuchen, Verbindungen zu erstellen.

Verwandte Links

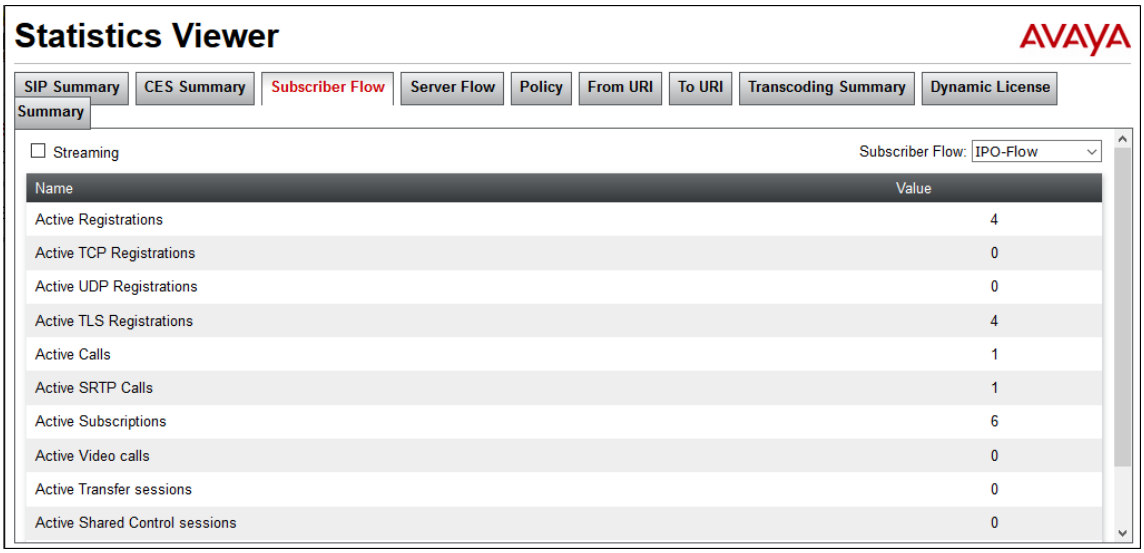
[Anzeigen von ASBCE SIP-Statistiken](#) auf Seite 69
[Anzeigen von ASBCE Benutzerstatistiken](#) auf Seite 70
[Anzeigen von ASBCE Vorfällen](#) auf Seite 70

Anzeigen von ASBCE SIP-Statistiken

Das **Statistikanzeige** kann Details zur Anzahl der Remote-Nebenstellenverbindungen und -anrufe anzeigen.

Vorgehensweise

1. Wählen Sie **Status** > **SIP-Statistik**
2. Wählen Sie **Teilnehmer-Flow** und dann in der Dropdown-Liste den Flow aus, der für Remote-Nebenstellen erstellt wurde.
3. Der Viewer zeigt Details wie die Anzahl der Registrierungen, die Anzahl der Anrufe usw. an.



Verwandte Links

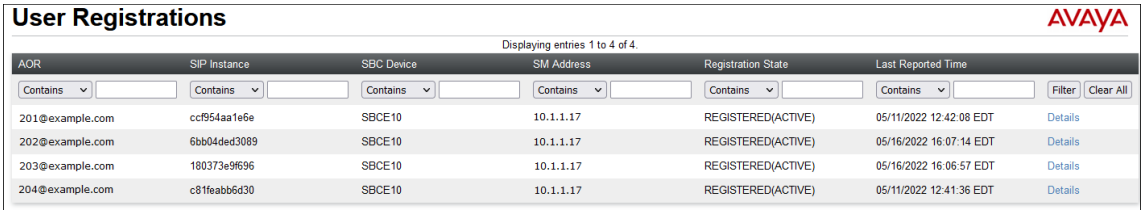
Überprüfen des Status der Remote-Nebenstelle im ASBCE auf Seite 69

Anzeigen von ASBCE Benutzerstatistiken

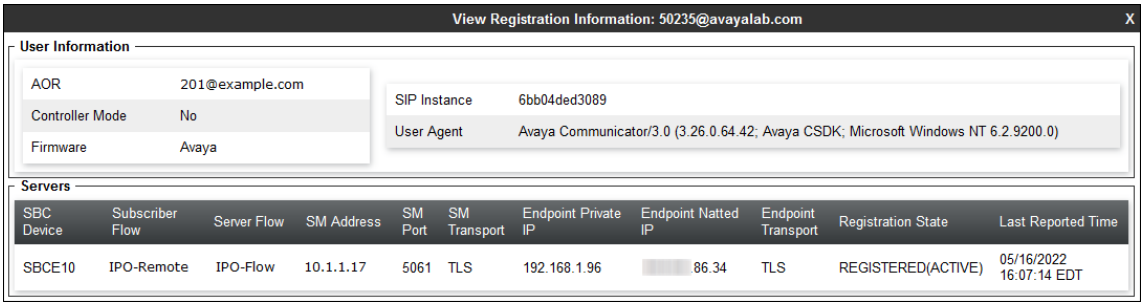
Das **Statistikanzeige** kann Details zu einzelnen Remote-Nebenstellen anzeigen.

Vorgehensweise

1. Wählen Sie **Status** > **Benutzerregistrierung**
2. Der Viewer zeigt Details zu SIP-Clients an, die über das ASBCE registriert sind.



3. Um zusätzliche Informationen für einen bestimmten Benutzer anzuzeigen, klicken Sie auf **Details**.



Verwandte Links

Überprüfen des Status der Remote-Nebenstelle im ASBCE auf Seite 69

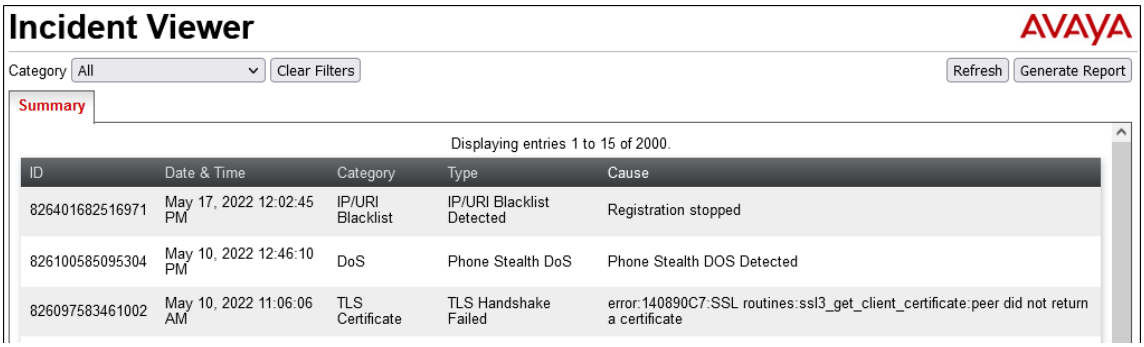
Anzeigen von ASBCE Vorfällen

Das ASBCE kann Details zu Problemen wie Zertifikatfehler und Registrierungsprobleme anzeigen. Wenn bei Remote-Nebenstellen Probleme bei der Verbindung mit IP Office auftreten, kann dies den Grund anzeigen, wenn das Problem in auf dem ASBCE auftritt.

Vorgehensweise

1. Wählen Sie **Ereignisse** aus.

2. Die Ansicht zeigt Details zu Vorfällen an.



Verwandte Links

Überprüfen des Status der Remote-Nebenstelle im ASBCE auf Seite 69

Teil 2: Unterstützung von IPv6

Kapitel 8: Unterstützung von IPv6-Remote-Nebenstellen

Für IP Office R11.1.3.1 und höher unterstützt das IP Office Avaya Workplace-Client Remote-Nebenstellen auf iOS und Android mit IPv6.

Verwandte Links

IPv6-Unterstützung für Remote-Nebenstellen auf Seite 73
Schema der IPv6-Remote-Nebenstelle auf Seite 74
Einschränkungen von IPv6-Remote-Nebenstellen auf Seite 74
DNS-Konfiguration für die Unterstützung von IPv6-Remote-Nebenstellen auf Seite 75
Zertifikatkonfiguration für IPv6-Remote-Nebenstellenunterstützung auf Seite 75
Avaya Spaces Konfiguration für IPv6-Remote-Nebenstellenunterstützung auf Seite 76
Konfigurationscheckliste für IPv6-Remote-Nebenstellen auf Seite 76
Konfigurationscheckliste für kombinierte IPv4- und IPv6-Remote-Nebenstellen auf Seite 77

IPv6-Unterstützung für Remote-Nebenstellen

Für IP Office R11.1.3.1 und höher kann Remote Mobile Avaya Workplace-Client IPv6 verwenden.

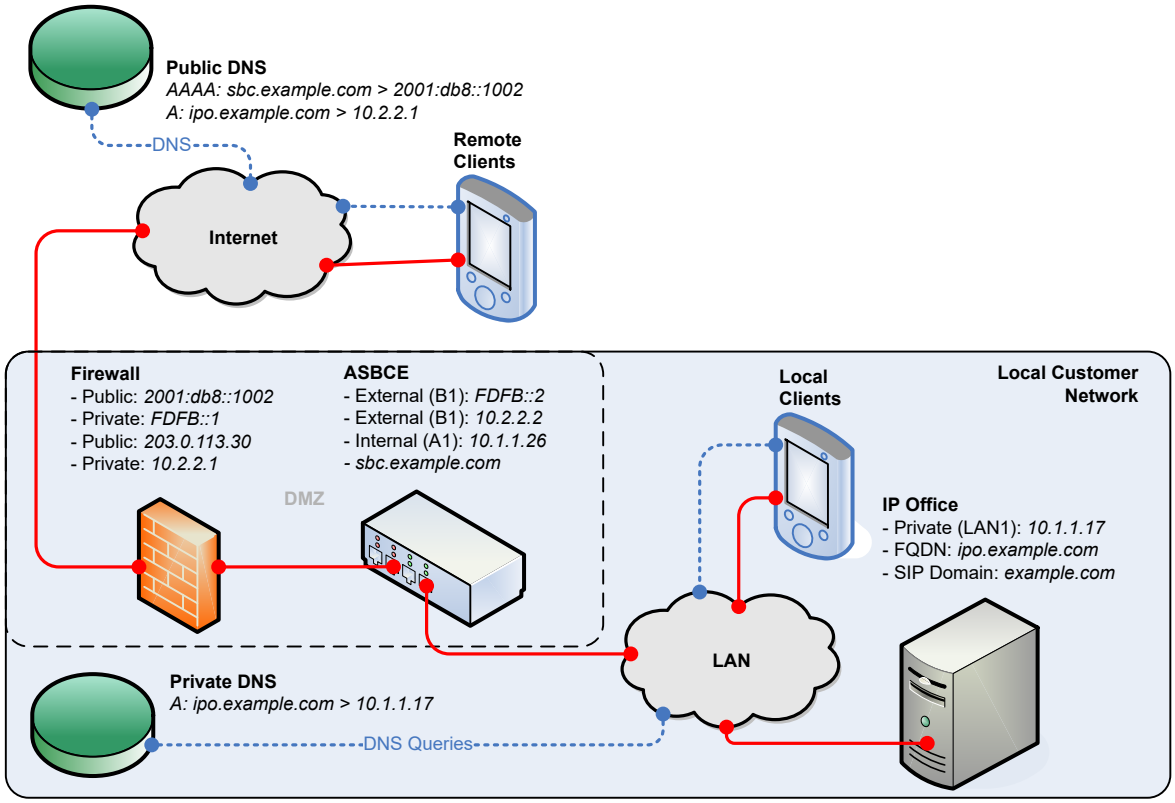
- Sie können IP Office so konfigurieren, dass der entfernte mobile Avaya Workplace-Client den FQDN des ASBCE mit der automatisch generierten Datei `46xxsettings.txt` erhält.
- Für die Verbindung muss ein ASBCE R10.1.2 in einer Dual-Stack-Installation installiert sein. Das ASBCE führt das Routing zwischen den IPv6-Clients und dem IPv4 IP Office durch.
- Avaya Workplace-Client:
  - iOS: Avaya Workplace-Client R3.35 und höher.
  - Android: Avaya Workplace-Client R3.35.1 und höher.
  - iPad- und Vantage-Geräte sind nicht in der IPv6-Unterstützung enthalten.
- SIP-Telefone und -Clients im privaten Netzwerk des Kunden verwenden weiterhin IPv4, um eine direkte Verbindung mit IP Office herzustellen.
- Wenn das Netzwerk, mit dem Avaya Workplace-Client verbunden ist, IPv4 und IPv6 unterstützt, verwendet Avaya Workplace-Client standardmäßig IPv4.

Verwandte Links

Unterstützung von IPv6-Remote-Nebenstellen auf Seite 73

Schema der IPv6-Remote-Nebenstelle

Das folgende Schema ist ein Beispiel für die Unterstützung von IPv6-Remote-Nebenstellen.



- Das IP Office stellt den Remote-Nebenstellen den FQDN von ASBCE zur Verfügung.
- Das öffentliche DNS löst den FQDN von ASBCE auf die öffentliche IPv6-Adresse der Kunden-Firewall auf.
- Die Firewall leitet die von den Remote-Nebenstellen verwendeten Ports an die externe Schnittstelle des ASBCE weiter.
- Der Dual-Stack ASBCE verarbeitet das Routing zwischen IPv6- und IPv4-Adressen.
- Bei internen Nebenstellen löst das private DNS den FQDN IP Office auf die IPv4-Adresse des IP Office Systems auf.

Verwandte Links

Unterstützung von IPv6-Remote-Nebenstellen auf Seite 73

Einschränkungen von IPv6-Remote-Nebenstellen

- Während Firmware für den Betrieb des Telefons IPv6 der Serie J100 vorhanden ist, müssen sie IPv4 für die Remote-Nebenstellenverbindung mit IP Officeverwenden.
- Avaya Spaces unterstützt IPv6 nicht. Daher unterstützt Avaya Workplace-Client mit IPv6 keine von Avaya Spaces bereitgestellten Funktionen. Beispiel:
  - Keine Client-Registrierung mit E-Mail- oder SSO-Anmeldung.

    - Keine Sofortnachrichten, wenn IP Office als Messaging-Server Avaya Spaces konfiguriert ist.
- Wenn das Netzwerk, mit dem Avaya Workplace-Client verbunden ist, IPv4 und IPv6 unterstützt, verwendet Avaya Workplace-Client standardmäßig IPv4.

Verwandte Links

Unterstützung von IPv6-Remote-Nebenstellen auf Seite 73

DNS-Konfiguration für die Unterstützung von IPv6-Remote-Nebenstellen

Um IPv6 zu unterstützen, muss das DNS den FQDN des ASBCE zusätzlich zum FQDN des IP Office auflösen:

- Das öffentliche DNS für den FQDN des IP Office muss immer noch in eine IPv4-Adresse aufgelöst werden.
- Das öffentliche DNS muss den FQDN des ASBCE auch auf eine IPv6-Adresse auflösen. Dazu muss der Kunde `AAAA` Records zu seinem öffentlichen DNS-Dienst hinzufügen.
- Lokale Nebenstellen stellen weiterhin eine direkte Verbindung mit IP Office über IPv4-Adressen her. Dies wird durch das private DNS des Kunden behoben.

Verwandte Links

Unterstützung von IPv6-Remote-Nebenstellen auf Seite 73

Zertifikatkonfiguration für IPv6-Remote-Nebenstellenunterstützung

Wenn IPv6-Remote-Nebenstellen unterstützt werden, muss zusätzlich zum IP Office FQDN und zur IPv4-Adresse das ASBCE Identitätszertifikat den FQDN und die IPv6-Adresse des ASBCE enthalten.

- Der FQDN von ASBCE kann als Teil des allgemeinen Zertifikatnamens (CN) oder des alternativen Betreffnamens (SAN) hinzugefügt werden.
- Die IPv6-Adresse muss zum SAN hinzugefügt werden.

Verwandte Links

Unterstützung von IPv6-Remote-Nebenstellen auf Seite 73

Avaya Spaces Konfiguration für IPv6-Remote-Nebenstellenunterstützung

Avaya Spaces unterstützt IPv6 nicht. Daher unterstützt Avaya Workplace-Client mit IPv6 keine von Avaya Spaces bereitgestellten Funktionen. Beispiel:

- Keine Client-Registrierung mit E-Mail- oder SSO-Anmeldung.
- Keine Sofortnachrichten, wenn IP Office als Messaging-Server Avaya Spaces konfiguriert ist.

Leere Anmeldeseite

Wenn Sie die SSO-Unterstützung nicht deaktivieren, sehen Benutzer des IPv6-Clients bei der Anmeldung eine leere Seite. Um sich anzumelden, müssen sie die leere Seite schließen und sich dann direkt mit der Adresse der Datei `46xxsettings.txt` von IP Office anmelden.

- Wenn Sie möchten, dass IPv4-Clientbenutzer weiterhin SSO verwenden können, müssen Sie die Benutzer der IPv6-Remote-Nebenstelle anweisen, die leere Seite zu schließen und sich mit der Adresse der Datei `46xxsettings.txt` von IP Office anzumelden.
- Andernfalls müssen Sie eine Datei `46xxspecials.txt` mit der Einstellung `SET SIPSSO 0` in IP Office hinzufügen, damit keine leere Seite angezeigt wird, wenn der Benutzer Avaya Workplace-Client startet. Beachten Sie, dass dies alle Benutzer von Avaya Workplace-Client betrifft.

```
...
SETTINGSEQNX
SET SIPSSO 0
GOTO GENERALSPECIALS
```

Verwandte Links

Unterstützung von IPv6-Remote-Nebenstellen auf Seite 73

Konfigurationscheckliste für IPv6-Remote-Nebenstellen

Wenn Sie nur Remote-Nebenstellen von IPv6 unterstützen, befolgen Sie denselben Konfigurationsprozess wie für IPv4, ersetzen Sie jedoch die externen IPv4-Adressen ggf. durch IPv6-Adressen. Siehe ASBCE Konfiguration für Remote-SIP-Nebenstellen auf Seite 25.

#	Aktion	Link/Hinweise	✔
1.	Öffentliche DNS-Unterstützung für IPv6 konfigurieren	DNS muss den FQDN des ASBCE auf die IPv6-Adresse auflösen, um den Datenverkehr zum ASBCE zu ermöglichen. Siehe DNS-Konfiguration für die Unterstützung von IPv6-Remote-Nebenstellen auf Seite 75.	
2.	Fügen Sie den FQDN und die IPv6-Adresse des ASBCE in das ASBCE Identitätszertifikat ein.	Siehe Zertifikatkonfiguration für IPv6-Remote-Nebenstellenunterstützung auf Seite 75.	

Die Tabelle wird auf der nächsten Seite fortgesetzt …

#	Aktion	Link/Hinweise	✔
3.	Deaktivieren Sie den Avaya Spaces Support.	Siehe Avaya Spaces Konfiguration für IPv6-Remote-Nebenstellenunterstützung auf Seite 76.	
4.	Festlegen der öffentlichen IPv6-Adresse in IP Office	Sie müssen den Remote-Nebenstellen die IPv6-Adresse geben, die für die SIP-Registrierung und Anrufe verwendet werden soll. Siehe Festlegen der ASBCE Informationen, die vom IP Office an die Remote-Nebenstellen weitergegeben werden auf Seite 13.	
5.	ASBCE Anrufverlauf konfigurieren	Befolgen Sie den gleichen ASBCE Konfigurationsprozess wie für IPv4, verwenden Sie jedoch ggf. IPv6-Adressen. Siehe ASBCE-Konfigurationsprüfliste auf Seite 28.	

Verwandte Links

Unterstützung von IPv6-Remote-Nebenstellen auf Seite 73

Konfigurationscheckliste für kombinierte IPv4- und IPv6-Remote-Nebenstellen

Diese Checkliste setzt voraus, dass Sie die ASBCE Konfiguration zur Unterstützung von IPv4-Remote-Nebenstellen abgeschlossen haben. Siehe ASBCE-Konfigurationsprüfliste auf Seite 28. Die Hinweise zeigen an, wo für ASBCE die Unterstützung von IPv4- und IPv6-Remote-Nebenstellen eine zusätzliche Konfiguration erforderlich ist.

#	Aktion	Link/Hinweise	✔
1.	Öffentliche DNS-Unterstützung für IPv6 konfigurieren	DNS muss den FQDN des ASBCE auf die IPv6-Adresse auflösen, um den Datenverkehr zum ASBCE zu ermöglichen. Siehe DNS-Konfiguration für die Unterstützung von IPv6-Remote-Nebenstellen auf Seite 75.	
2.	Fügen Sie den FQDN und die IPv6-Adresse des ASBCE in das ASBCE Identitätszertifikat ein.	Die ASBCE Identität muss den FQDN und die IPv4-Adresse des IP Office sowie den FQDN und die IPv6-Adresse des ASBCE enthalten. Siehe Avaya Spaces Konfiguration für IPv6-Remote-Nebenstellenunterstützung auf Seite 76.	
3.	Deaktivieren Sie den Avaya Spaces Support.	Avaya Spaces wird mit IPv6 nicht unterstützt. Siehe Avaya Spaces Konfiguration für IPv6-Remote-Nebenstellenunterstützung auf Seite 76.	

Die Tabelle wird auf der nächsten Seite fortgesetzt …

#	Aktion	Link/Hinweise	✔
4.	Festlegen der öffentlichen IPv6-Adresse in IP Office	Sie müssen den Remote-Nebenstellen die IPv6-Adresse geben, die für die SIP-Registrierung und Anrufe verwendet werden soll. Siehe Festlegen der ASBCE Informationen, die vom IP Office an die Remote-Nebenstellen weitergegeben werden auf Seite 13.	
5.	Firewall-Port-Weiterleitung konfigurieren	Fügen Sie einen neuen Eintrag hinzu, z. B. den IPv4-Eintrag, aber verwenden Sie ggf. die IPv6-Adressen. Siehe Firewall-Konfiguration auf Seite 30.	
6.	Konfigurieren der externen ASBCE Netzwerkschnittstelle	Fügen Sie einen neuen Eintrag für die externe Schnittstelle hinzu, aber verwenden Sie die IPv6-Adressen. Siehe Externe ASBCE Schnittstelle konfigurieren auf Seite 31.	
7.	Konfigurieren der internen ASBCE Netzwerkschnittstelle	Verwenden Sie den vorhandenen IPv4-Eintrag. Siehe Interne ASBCE Schnittstelle konfigurieren auf Seite 32.	
8.	TLS-Clientprofil erstellen	Verwenden Sie den vorhandenen IPv4-Eintrag. Siehe Erstellen eines TLS-Clientprofils auf Seite 34.	
9.	TLS-Serverprofil erstellen	Verwenden Sie den vorhandenen IPv4-Eintrag. Siehe Erstellen eines TLS-Serverprofils auf Seite 35.	
10.	Interne SIP-Medienschnittstelle erstellen	Verwenden Sie den vorhandenen IPv4-Eintrag. Siehe Erstellen einer internen Medienschnittstelle auf Seite 37.	
11.	Erstellen einer externen SIP-Medienschnittstelle	Fügen Sie einen neuen Eintrag hinzu, z. B. den IPv4-Eintrag, aber verwenden Sie ggf. die IPv6-Adressen. Siehe Erstellen einer externen Medienschnittstelle auf Seite 38.	
12.	Interne SIP-Anrufsignalisierungsschnittstelle erstellen	Verwenden Sie den vorhandenen IPv4-Eintrag. Siehe Erstellen einer internen Signalisierungsschnittstelle auf Seite 39.	
13.	Erstellen einer externen SIP-Anrufsignalisierungsschnittstelle	Fügen Sie einen neuen Eintrag hinzu, z. B. den IPv4-Eintrag, aber verwenden Sie ggf. die IPv6-Adressen. Siehe Erstellen der externen Signalisierungsschnittstelle auf Seite 40.	
14.	Serverprofil erstellen	Verwenden Sie den vorhandenen IPv4-Eintrag. Siehe Erstellen eines ASBCE Serverprofils für das IP Office auf Seite 41.	

Die Tabelle wird auf der nächsten Seite fortgesetzt …

#	Aktion	Link/Hinweise	✔
15.	Serverrouting erstellen	Verwenden Sie den vorhandenen IPv4-Eintrag. Siehe Erstellen eines Server-Routingprofils auf Seite 43.	
16.	Topologie ausblenden einrichten	Verwenden Sie den vorhandenen IPv4-Eintrag. Siehe Erstellen einer ASBCE Topologie-Ausblendrichtlinie auf Seite 44.	
17.	Erstellen Sie eine IP/URL-Sperrliste.	Verwenden Sie den vorhandenen IPv4-Eintrag. Siehe Erstellen einer IP/URI-Blockliste auf Seite 45.	
18.	Erstellen einer Anwendungsregel.	Verwenden Sie den vorhandenen IPv4-Eintrag. Siehe Erstellen einer Anwendungsregel auf Seite 46.	
19.	Erstellen einer Medienregel	Verwenden Sie den vorhandenen IPv4-Eintrag. • Stellen Sie sicher, dass **Erweiterte Einstellungen** > **ANAT aktiviert** nicht ausgewählt ist. Siehe Erstellen einer Medienregel auf Seite 48.	
20.	Erstellen einer Endgerätrichtlinie	Verwenden Sie den vorhandenen IPv4-Eintrag. Siehe Erstellen einer Endgeräterichtliniengruppe auf Seite 50.	
21.	User-Agent-Profil hinzufügen	Verwenden Sie den vorhandenen IPv4-Eintrag. Siehe Konfigurieren eines User-Agent-Profils auf Seite 51.	
22.	Erstellen eines Teilnehmer-Flows	Fügen Sie einen neuen Eintrag hinzu, z. B. den IPv4-Eintrag: • Legen Sie die Medien- und Signalisierungsschnittstellen für die Verwendung der externen IPv6-Schnittstellen fest. Siehe Erstellen des Teilnehmer-Flows auf Seite 52.	
23.	Erstellen eines Server-Flows	Fügen Sie einen neuen Eintrag hinzu, z. B. den IPv4-Eintrag: • Legen Sie die externe IPv6-Signalisierungsschnittstelle als **Erhaltene Schnittstelle** fest. Siehe Erstellen eines Server-Flows auf Seite 55.	
24.	Reverse Proxy für Avaya Workplace-Client hinzufügen	Fügen Sie neue Proxys über die externe B1-Schnittstelle hinzu, die für IPv6-Adressen konfiguriert ist. Siehe Hinzufügen von Reverse Proxys für Dateianforderungen auf Seite 57.	

Verwandte Links

Unterstützung von IPv6-Remote-Nebenstellen auf Seite 73

Teil 3: Ausfallsicherheit

Kapitel 9: ASBCE und IP Office-Ausfallsicherheit

IP Office unterstützt eine Reihe von Ausfallsicherheitsoptionen, einschließlich Ausfallsicherheit für SIP-Telefone und SIP-Softphone-Anwendungen. Weitere Informationen können Sie dem IP Office Überblick über Ausfallsicherheit-Handbuch entnehmen.

Dieser Abschnitt dieses Dokuments gibt einen Überblick über die zusätzliche Konfiguration, die erforderlich ist, um einer vorhandenen Konfiguration Unterstützung für Ausfallsicherheit hinzuzufügen. Die wichtigsten zusätzlichen Schritte sind:

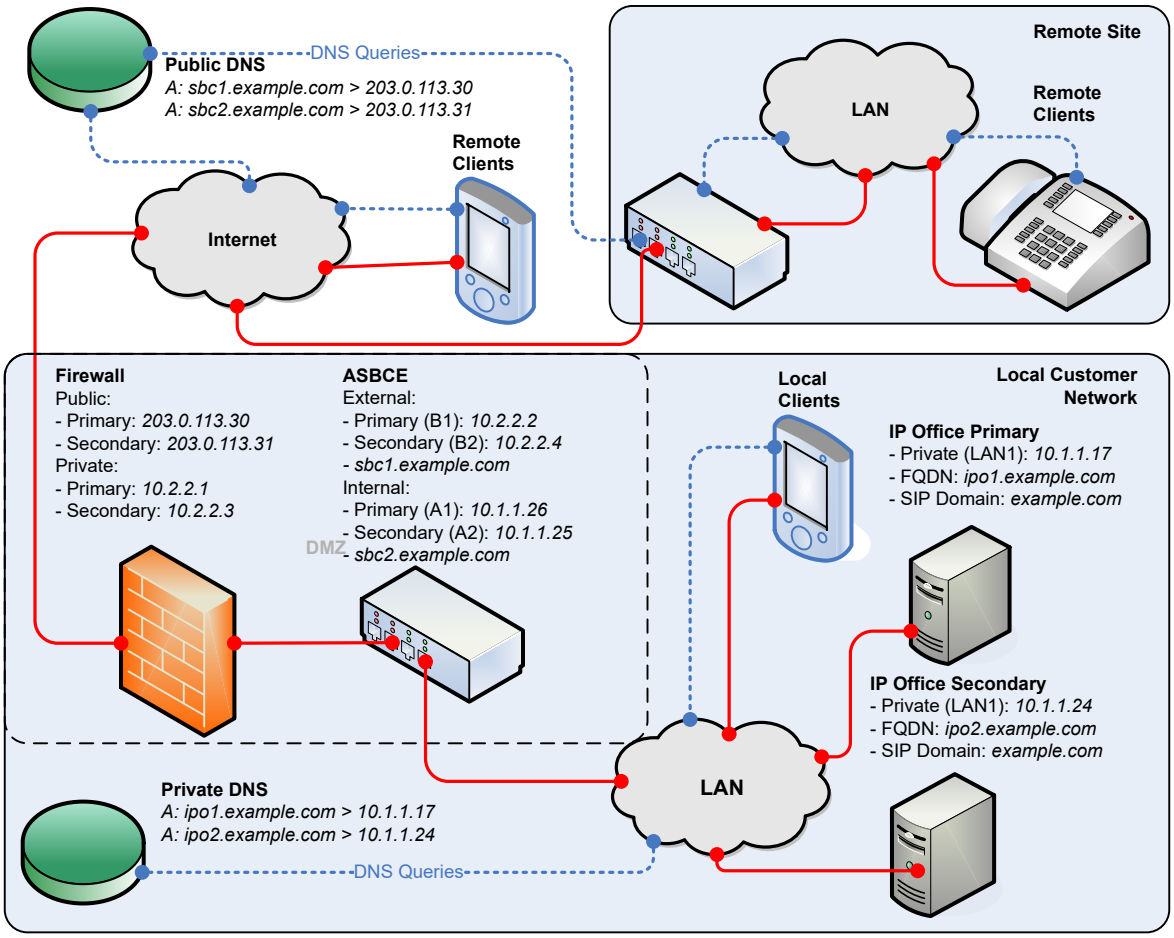
- IP Office kann die IP-Adresse der Remote-Nebenstelle nicht verwenden, um einem Standort in der IP Office Konfiguration zu entsprechen. Um daher Standorteinstellungen in der Ausfallsicherheit zu verwenden, müssen Sie den Standort in der Nebenstellenkonfiguration konfigurieren.

Verwandte Links

Beispiel für ein Ausfallsicherheitsschema auf Seite 81
Erstellen eines Identitätszertifikats für das sekundäre IP Office auf Seite 82
Installieren des sekundären IP Office Identitätszertifikats auf Seite 83
Konfigurieren von IP Office für Ausfallsicherheit von Remote-Nebenstellen auf Seite 84
Konfigurieren des Avaya one-X Portal auf Seite 84
Konfigurieren von ASBCE für Ausfallsicherheit auf Seite 85
DNS für Ausfallsicherheit konfigurieren auf Seite 85

Beispiel für ein Ausfallsicherheitsschema

Im Folgenden finden Sie ein Beispielschema für eine ausfallsichere Konfiguration.



Für eine ausfallsichere Unterstützung von Remote-Nebenstellen verwendet ASBCE zwei Sets öffentlicher/privater IP-Adressen:

- Das ASBCE leitet ein Set an den primären IP Office Server und das andere Set an den sekundären IP Office Server weiter.
- Diese Logik ist unabhängig von der ASBCE Installation gleich: Simplex, HA, zwei separate ASBCE Server oder Dual-Stack.

Verwandte Links

ASBCE und IP Office-Ausfallsicherheit auf Seite 81

Erstellen eines Identitätszertifikats für das sekundäre IP Office

Das sekundäre IP Office erfordert ein Identitätszertifikat, das vom primären IP Office ausgestellt wurde.

Vorgehensweise

1. Melden Sie sich bei den IP Office Web Control-Menüs an, indem Sie entweder:
   - Wählen Sie in IP Office Web Manager den primären Server aus. Klicken Sie auf ☰ und wählen Sie **Plattformansicht** aus.
   - Navigieren Sie zu `https://<IP Office IP address>:7071` und melden Sie sich an.
2. Gehen Sie zur Registerkarte **Einstellungen** und scrollen Sie nach unten zu **Zertifikate**.
3. Geben Sie folgende Angaben ein:

Wert	Beschreibung
Maschinen-IP	Geben Sie die IP-Adresse des sekundären Servers ein.
Kennwort	Geben Sie ein Kennwort ein, um das Zertifikat und den Schlüssel zu verschlüsseln.
Name des Antragstellers	Geben Sie den FQDN des sekundären IP Office ein.
Alternative Name(n) des Antragsteller	Listen Sie den FQDN des sekundären IP Office, die sekundäre XMPP-Domäne, die SIP-Domäne und die internen und externen IP-Adressen des sekundären IP Office auf.

4. Klicken Sie auf **Neu generieren** und **Anwenden**.
5. Klicken Sie im Popup-Fenster auf den Link, um das Zertifikat herunterzuladen.
6. Klicken Sie auf **OK**.
7. Benennen Sie die heruntergeladene Datei in `IPOSEC_ID.p12` um.

Weitere Schritte

- Installieren des sekundären IP Office Identitätszertifikats auf Seite 83.

Verwandte Links

ASBCE und IP Office-Ausfallsicherheit auf Seite 81

Installieren des sekundären IP Office Identitätszertifikats

Sie müssen das für das sekundäre IP Office erstellte Identitätszertifikat hinzufügen.

Voraussetzungen

- Erstellen eines Identitätszertifikats für das sekundäre IP Office auf Seite 82.

Vorgehensweise

1. Melden Sie sich mit IP Office Web Manager beim System an.
   - Geben Sie bei einem IP500 V2 die Systemadresse gefolgt von `:8443/WebMgmtEE/WebManagerment.html` ein.
   - Geben Sie bei Linux-basierten Servern die Systemadresse gefolgt von `:7070/WebManagement/WebManagement.html` ein.

2. Gehen Sie auf **Sicherheitsmanager** > **Zertifikate**.
3. Klicken Sie auf das Symbol neben dem sekundären Server.
4. Klicken Sie auf **Festlegen**.
5. Navigieren Sie zur Identitätszertifikatsdatei und wählen Sie sie aus.
6. Geben Sie das Kennwort ein.
7. Klicken Sie auf **Hochladen**.

Verwandte Links

ASBCE und IP Office-Ausfallsicherheit auf Seite 81

Konfigurieren von IP Office für Ausfallsicherheit von Remote-Nebenstellen

Zusätzlich zur Standardkonfiguration für Ausfallsicherheit (siehe IP Office Überblick über Ausfallsicherheit) müssen Sie das sekundäre IP Office wie folgt konfigurieren:

- Stellen Sie die SIP-Registrareinstellungen mit Ausnahme von **SIP-Registrar FQDN** auf die gleichen Einstellungen wie auf dem primären IP Office Server ein. Dazu gehört auch die Übereinstimmung mit **SIP-Domainname**. Siehe IP Office SIP VoIP-Einrichtung auf Seite 11.
- Stellen Sie den **SIP-Registrar FQDN** so ein, dass er mit dem in DNS konfigurierten FQDN übereinstimmt, um SIP-Datenverkehr an den sekundären IP Office Server weiterzuleiten.
- Legen Sie die **SBC** Einstellungen fest, die die Remote-Nebenstellen verwenden müssen, um eine Verbindung mit dem ASBCE herzustellen, das konfiguriert ist, um SIP-Anrufe an das sekundäre ASBCE weiterzuleiten. Siehe Festlegen der ASBCE Informationen, die vom IP Office an die Remote-Nebenstellen weitergegeben werden auf Seite 13.

Verwandte Links

ASBCE und IP Office-Ausfallsicherheit auf Seite 81

Konfigurieren des Avaya one-X Portal

Sie müssen den Avaya one-X Portal Dienst mit dem Domänennamen des sekundären IP Office konfigurieren.

Vorgehensweise

1. Melden Sie sich bei den Avaya one-X Portal Administratormenüs an, entweder:
   - Wählen Sie in IP Office Manager **Anwendungen** > **one-X Portal** > aus.
   - Navigieren Sie zu `https://<portal IP address>:9443/onexportal-admin.html` und melden Sie sich als Administrator an.

2. Wählen Sie **Konfiguration** > **Host-Domänenname**aus.
    a. Setzen Sie den **Domänennamen des sekundären Hosts** auf den FQDN des sekundären Avaya one-X Portal.
    b. Klicken Sie auf **Speichern**.
3. Klicken Sie auf das Symbol oben in den Menüs, um den Avaya one-X Portal neu zu starten.

Verwandte Links

ASBCE und IP Office-Ausfallsicherheit auf Seite 81

Konfigurieren von ASBCE für Ausfallsicherheit

Die ASBCE Konfigurationsschritte entsprechen denen für die Einrichtung eines einzelnen Servers. Es ist erforderlich, zusätzliche Einträge zu erstellen, jedoch die öffentlichen und privaten IP-Adressen des sekundären IP Office Servers zu verwenden.

Verwandte Links

ASBCE und IP Office-Ausfallsicherheit auf Seite 81

DNS für Ausfallsicherheit konfigurieren

Die DNS-Serverkonfiguration entspricht der für einen einzelnen IP Office Server. DNS erfordert zusätzliche Records für den FQDN des sekundären IP Office und des ASBCE-Servers.

Verwandte Links

ASBCE und IP Office-Ausfallsicherheit auf Seite 81

Kapitel 10: Überprüfen der Ausfallsicherheitskonfiguration

Sie können die folgenden Methoden verwenden, um die Ausfallsicherheitsinformationen zu überprüfen, die IP Office den Remote-Nebenstellen bereitstellt.

Verwandte Links

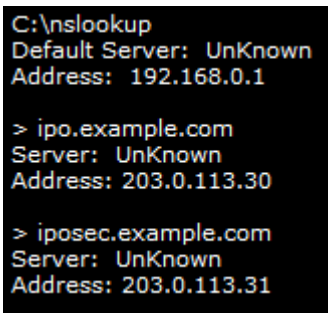
[Überprüfen des Ausfallsicherheits-DNS-Routings](#) auf Seite 86
[Anzeigen der ASBCE Ablaufverfolgung](#) auf Seite 87
[Überprüfen der Avaya one-X Portal Antworten](#) auf Seite 88

Überprüfen des Ausfallsicherheits-DNS-Routings

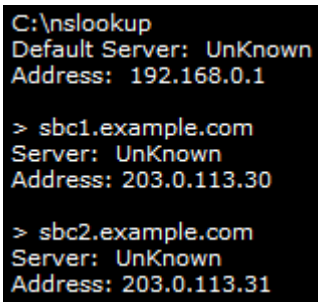
Mit einem Remote-PC können Sie überprüfen, ob DNS Anfragen korrekt aufgelöst werden.

Vorgehensweise

1. Verwenden Sie den Befehl `nslookup`, um zu überprüfen, ob DNS die FQDNs des primären IP Office und sekundären IP Office zu den richtigen IP-Adressen auflöst. Beispiel:



2. Verwenden Sie den Befehl `nslookup`, um zu überprüfen, ob DNS die FQDNs des primären und sekundären ASBCE auflöst.



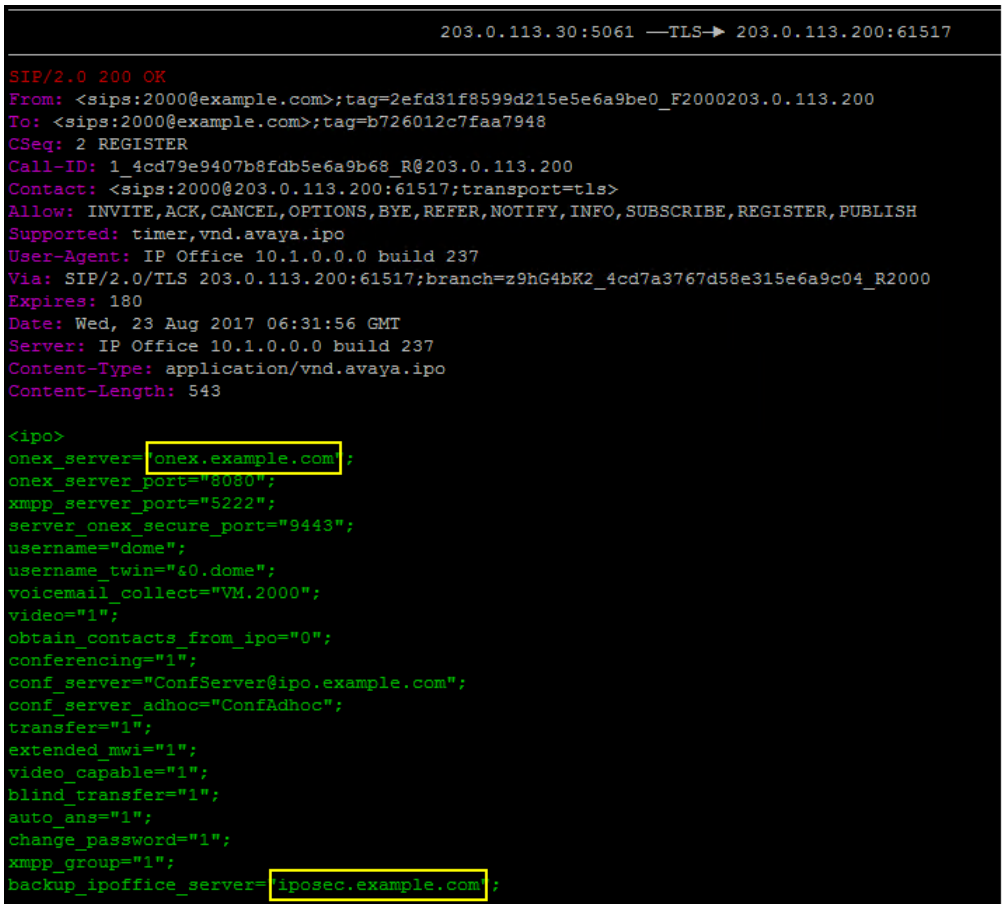
Verwandte Links

[Überprüfen der Ausfallsicherheitskonfiguration](#) auf Seite 86

Anzeigen der ASBCE Ablaufverfolgung

Im Folgenden finden Sie ein Beispiel für eine TraceSBC-Sitzung für die Registrierung eines Clients. Sie zeigt die an den Client gesendete SIP *200 OK* Antwort an.

Die Antwort enthält eine Reihe von Konfigurationseinstellungen. Bei Remote-Nebenstellen enthält die Antwort den SBC FQDN, den Sie auf dem sekundären IP Office konfiguriert haben.



- **Während des normalen Betriebs:**

  Die *200 OK* Antwort zeigt die Werte *onex_server* und *backup_ipoffice_server* an, die mit dem primären bzw. sekundären Server festgelegt wurden.

- **Während der Ausfallsicherheit:**

  Der Wert *onex_server* enthält den FQDN des sekundären Portals und *backup_ipoffice_server* ist *0.0.0.0*.

Verwandte Links

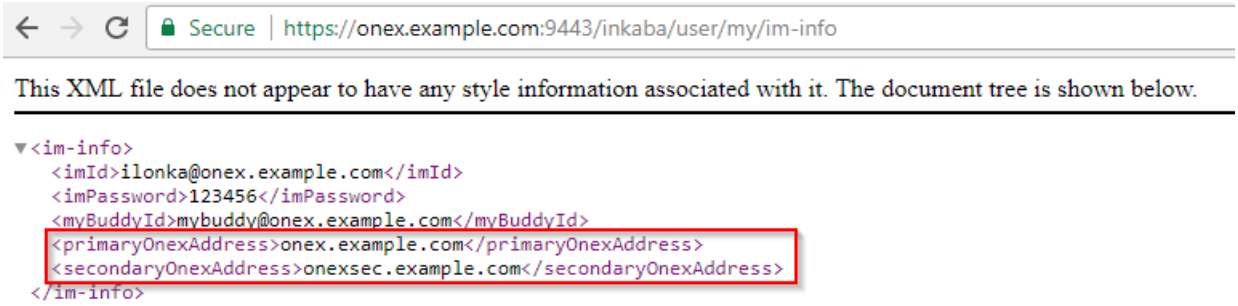
[Überprüfen der Ausfallsicherheitskonfiguration](#) auf Seite 86

Überprüfen der Avaya one-X Portal Antworten

Wenn ein Client XMPP-Informationen vom primären Avaya one-X Portal Dienst anfordert, enthält die Antwort die primären und sekundären XMPP-Serveradressen.

Vorgehensweise

1. Geben Sie während des normalen Betriebs mithilfe eines Browsers `https://<FQDN>:9443/inkaba/user/my/im-info` ein, wobei *<FQDN>* der FQDN des primären Avaya one-X Portal Dienstes ist.



2. Überprüfen Sie, ob die Antwort die FQDNs des primären und sekundären Avaya one-X Portal Dienstes enthält.

   a.

   b. Die Antwort sollte den FQDN des primären IP Office Servers enthalten.

3. Geben Sie in einem Browser `https://<FQDN>:9443/inkaba/user/my/sip-info` ein, wobei *<FQDN>* der FQDN des primären Avaya one-X Portal Dienstes ist.

4. Wenn Sie die Schritte während der Ausfallsicherheit wiederholen, verwenden Sie den FQDN des sekundären Avaya one-X Portal Servers.

   - Die `im-info` Informationen sind identisch.
   - Die `sip-info` Informationen zeigen den FQDN des sekundären IP Office Servers an.

Verwandte Links

Überprüfen der Ausfallsicherheitskonfiguration auf Seite 86

Teil 4: Weitere Informationen

Kapitel 11: Zusätzliche Hilfe und Dokumentation

Auf den folgenden Seiten finden Sie Quellen für zusätzliche Hilfe.

Verwandte Links

Zusätzliche Handbücher und Benutzerhandbücher auf Seite 91
Hilfe erhalten auf Seite 91
Avaya-Geschäftspartner suchen auf Seite 92
Zusätzliche IP Office-Ressourcen auf Seite 92
Schulung auf Seite 93

Zusätzliche Handbücher und Benutzerhandbücher

Die Website Avaya Dokumentationscenter enthält Benutzerhandbücher und Handbücher für Avaya-Produkte, einschließlich IP Office.

- Eine Liste der aktuellen IP Office-Handbücher und -Benutzerhandbücher finden Sie im Dokument Avaya IP Office™ Platform – Handbücher und Benutzerhandbücher.
- Die Websites Avaya IP Office Knowledgebase und Avaya Support bieten auch Zugriff auf die technischen Handbücher und Benutzerhandbücher für IP Office.
  - Beachten Sie, dass diese Websites Benutzer nach Möglichkeit an die Version des Dokuments umleiten, das von Avaya Dokumentationscenter gehostet wird.

Weitere Dokumenttypen und Ressourcen finden Sie auf den verschiedenen Avaya-Websites (siehe Zusätzliche IP Office-Ressourcen auf Seite 92).

Verwandte Links

Zusätzliche Hilfe und Dokumentation auf Seite 91

Hilfe erhalten

Avaya verkauft IP Office über akkreditierte Geschäftspartner. Diese Geschäftspartner bieten direkten Support für ihre Kunden und können Probleme ggf. an Avaya eskalieren.

Wenn Ihr IP Office-System derzeit keinen Avaya-Geschäftspartner hat, der Support und Wartung-bereitstellt, können Sie das Avaya Partner Locator-Tool verwenden, um einen Geschäftspartner zu finden. Siehe Avaya-Geschäftspartner suchen auf Seite 92.

Verwandte Links

Zusätzliche Hilfe und Dokumentation auf Seite 91

Avaya-Geschäftspartner suchen

Wenn Ihr IP Office-System derzeit keinen Avaya-Geschäftspartner hat, der Support und Wartung-bereitstellt, können Sie das Avaya Partner Locator-Tool verwenden, um einen Geschäftspartner zu finden.

Vorgehensweise

1. Gehen Sie über einen Browser zu Avaya-Website unter https://www.avaya.com.
2. Wählen Sie **Partner** und dann **Partner suchen**.
3. Geben Sie Ihre Standortinformationen ein.
4. Wählen Sie für IP Office-Geschäftspartnern mithilfe des **Filters** die Option **Kleines/ Mittelständisches Unternehmen** aus.

Verwandte Links

Zusätzliche Hilfe und Dokumentation auf Seite 91

Zusätzliche IP Office-Ressourcen

Zusätzlich zur Dokumentationswebsite (siehe Zusätzliche Handbücher und Benutzerhandbücher auf Seite 91) gibt es eine Reihe von Websites, die Informationen über Avaya-Produkte und -Dienste bereitstellen, einschließlich IP Office.

- Avaya-Website (https://www.avaya.com)

  Dies ist die offizielle Avaya-Website. Die Startseite bietet außerdem Zugriff auf individuelle Avaya-Webseiten für unterschiedliche Regionen und Länder.

- **Avaya Vertriebs- und Partnerportal** *(*https://sales.avaya.com*)*

  Dies ist die offizielle Webseite für alle Avaya-Geschäftspartner. Die Seite erfordert die Registrierung mit einem Nutzernamen und Passwort. Nach dem Zugriff können Sie das Portal so anpassen, dass die Produkte und Informationstypen angezeigt werden, die Sie anzeigen möchten.

- **Avaya IP Office Knowledgebase** *(*https://ipofficekb.avaya.com*)*

  Diese Website bietet Zugriff auf eine regelmäßig aktualisierte Online-Version der IP Office-Benutzerhandbücher und des technischen Handbuchs.

- **Avaya Support** *(*https://support.avaya.com*)*

  Diese Website bietet Zugriff auf Avaya-Produktsoftware, -Dokumentation und andere Dienste für Avaya-Produktinstallateure und -Wartungspersonal.

  - **AvayaSupport-Foren** *(*https://support.avaya.com/forums/index.php*)*

    Diese Website bietet Foren zur Besprechung von produktbezogenen Problemen.

- **Internationale Avaya-Benutzergruppe** *(*https://www.iuag.org*)*

  Dies ist die Organisation für Avaya-Kunden. Sie bietet Diskussionsgruppen und -foren.

- **Avaya DevConnect** *(*https://www.devconnectprogram.com/*)*

  Diese Website enthält Details zu APIs und SDKs für Avaya-Produkte, einschließlich IP Office. Die Website bietet auch Anwendungshinweise für Produkte von Drittanbietern (also nicht von Avaya), die mit IP Office unter Verwendung dieser APIs und SDKs interagieren.

- **Avaya Learning** *(*https://www.avaya-learning.com/*)*

  Diese Website bietet Zugriff auf Schulungskurse und Akkreditierungsprogramme für Avaya-Produkte.

Verwandte Links

Zusätzliche Hilfe und Dokumentation auf Seite 91

Schulung

Avaya-Schulungen und -Anmeldeinformationen sollen sicherstellen, dass unsere Geschäftspartner die nötigen Kenntnisse und Fähigkeiten besitzen, um die Lösungen von Avaya erfolgreich zu verkaufen, zu implementieren, Support zu bieten und kontinuierlich die Erwartungen der Kunden zu übertreffen. Die folgenden Berechtigungen sind verfügbar:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Karten mit Anmeldeinformationen sind auf der Avaya Learning-Website verfügbar.

Verwandte Links

Zusätzliche Hilfe und Dokumentation auf Seite 91

Kapitel 12: Glossar

Im Folgenden finden Sie Definitionen für Begriffe, die in diesem Dokument verwendet werden.

Verwandte Links

A-Record auf Seite 94
AAAA Record auf Seite 94
ASBCE auf Seite 95
DNS auf Seite 95
Domänenname auf Seite 95
FQDN auf Seite 95
Verwaltungs-IP auf Seite 96
SBC auf Seite 96
DNS aufteilen auf Seite 96
SRV-Record auf Seite 96
XMPP auf Seite 97

A-Record

„Address Record”. Ein grundlegender DNS-Record, der einen Domänennamen oder FQDN einer IPv4-Adresse zuordnet. Für IPv6-Adressen verwendet DNS `AAAA`-Records.

Verwandte Links

Glossar auf Seite 94

AAAA Record

Auch als „quad-A Record” bezeichnet. DNS-Dienste verwenden `AAAA` Records, um einen Domänennamen oder FQDN einer IPv6-Adresse zuzuordnen. Dies sind die `A` Records, die für IPv4-Adressen verwendet werden.

Verwandte Links

Glossar auf Seite 94

ASBCE

„Avaya Session Border Controller for Enterprise”. Die Avaya Plattform zur Bereitstellung von SBC-Diensten für ein Kundennetzwerk.

Verwandte Links

Glossar auf Seite 94

DNS

„Domänennamenanbieter”. Ein Server oder Dienst, der IP-Adressinformationen als Reaktion auf eine Domänennamen- oder FQDN-Abfrage bereitstellt. Wenn eine Anwendung beispielsweise versucht, eine Verbindung mit `www.example.com` herzustellen, kontaktiert sie zuerst den DNS-Server in ihrem Netzwerk. Der DNS-Server löst die Textadresse `www.example.com` auf die erforderliche numerische IP-Adresse auf. Bei diesem Vorgang überprüft der DNS-Server die DNS-Records, die er besitzt, und ggf. die von anderen DNS-Servern im Netzwerk oder Internet.

Verwandte Links

Glossar auf Seite 94

Domänenname

Die Textadresse, die zur Identifizierung eines Netzwerks von Geräten verwendet wird. Ein DNS-Server übersetzt den Domänennamen und die vollqualifizierten Domänennamen in einzelne IP-Adressen.

Verwandte Links

Glossar auf Seite 94

FQDN

„Vollständig qualifizierter Domänenname”. Die Volltextadresse, die einem bestimmten Server, Dienst oder Client innerhalb einer Domäne zugewiesen ist.

Verwandte Links

Glossar auf Seite 94

Verwaltungs-IP

Die IP-Adresse, die für den Administratorzugriff auf den ASBCE Server verwendet wird. Dies ist eine andere Adresse als die, die für die vom ASBCE bereitgestellten internen und externen Netzwerkverkehrsschnittstellen verwendet wird.

Verwandte Links

Glossar auf Seite 94

SBC

„Session Border Controller”. Ein SBC ist ein Gerät, das die SIP-Anrufsignalisierung und SIP-Medien zwischen zwei Netzwerken steuert.

Verwandte Links

Glossar auf Seite 94

DNS aufteilen

Die Verwendung von FQDNs und DNS-Servern zur Weiterleitung von Datenverkehr innerhalb und zwischen Netzwerken vereinfacht die Netzwerkwartung. Es können jedoch Probleme auftreten, wenn Sie FQDN-Routing für internen und externen Netzwerkverkehr verwenden. Dies kann dazu führen, dass das Netzwerk internen Datenverkehr an interne Dienste extern weiterleitet. Dadurch werden interne Dienste und Adressen sichtbar, die verborgen bleiben müssen.

Split DNS verwendet einen öffentlichen DNS-Dienst für den externen Datenverkehr zum Kundennetzwerk und einen privaten DNS-Dienst für den internen Datenverkehr innerhalb des Kundennetzwerks.

Kunden können Split-DNS über einen einzigen DNS-Server an den Endpunkten des Kundennetzwerks oder über separate öffentliche und private DNS-Server konfigurieren.

Verwandte Links

Glossar auf Seite 94

SRV-Record

„Service Record”. Bei Domänen, die mehrere Dienste unterstützen, z. B. `www.example.com` oder `sip.example.com`, reichen DNS-`A`Records möglicherweise nicht aus, um das erforderliche Routing durchzuführen. DNS `SRV`-Records bieten Zuordnungen für bestimmte Dienste, die innerhalb einer Domäne ausgeführt werden.

Verwandte Links

Glossar auf Seite 94

XMPP

„Extensible Messaging and Presence Protocol”. XMPP ist ein offenes Standardprotokoll, mit dem Geräte Instant Message-, Anwesenheits- und Kontaktinformationen austauschen können.

Verwandte Links

Glossar auf Seite 94

Index

O

P

Q

R

S

T

U

V

W

Z