Deploying Avaya IP Office™ Platform SSL VPN Services

Issue 7
April 2023

Hinweis

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

Haftungsausschluss für Dokumentation

Der Begriff „Dokumentation" bezieht sich auf in unterschiedlicher Weise veröffentlichte Informationen. Dies kann Produktinformationen, Vorgehensweisen und Leistungsangaben mit einschließen, die im Allgemeinen den Benutzern zur Verfügung gestellt werden. Der Begriff „Dokumentation" schließt Marketingmaterial aus. Avaya haftet nur dann für Änderungen, Ergänzungen oder Streichungen der ursprünglich veröffentlichten Fassung dieser Dokumentation, wenn diese Änderungen, Ergänzungen und Streichungen von Avaya vorgenommen wurden. Der Endnutzer erklärt sich einverstanden, Avaya sowie die Handlungsbevollmächtigten, Angestellten und Beschäftigten von Avaya im Falle von Forderungen, Rechtsstreitigkeiten, Ansprüchen und Urteilen auf der Grundlage von oder in Verbindung mit nachträglichen Änderungen, Ergänzungen oder Streichungen in dieser Dokumentation zu entschädigen und von jeglicher Haftung freizustellen, sofern diese Änderungen, Ergänzungen oder Streichungen vom Endnutzer vorgenommen worden sind.

Haftungsausschluss für Links

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

Der Begriff „**gehostete Dienste**" bezeichnet das Abonnement eines gehosteten Avaya-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 SOFTWARELIZENZBEDINGUNGEN, DIE AUF DER AVAYA-WEBSITE HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNTER DEM LINK „AVAYA-SOFTWARELIZENZBEDINGUNGEN (Avaya-Produkte)" ODER AUF EINER VON AVAYA GEKENNZEICHNETEN NACHFOLGER-WEBSITE VERFÜGBAR SIND, GELTEN FÜR ALLE PERSONEN, DIE AVAYA-SOFTWARE HERUNTERLADEN, NUTZEN UND/ODER INSTALLIEREN, DIE VON AVAYA INC., VON EINER AVAYA-TOCHTERGESELLSCHAFT ODER VON EINEM AVAYA-CHANNELPARTNER (SOFERN ZUTREFFEND) IM RAHMEN EINER GESCHÄFTSVEREINBARUNG MIT AVAYA ODER EINEM AVAYA-CHANNELPARTNER ERWORBEN WURDE. SOFERN AVAYA NICHTS ANDERES SCHRIFTLICH ZUSICHERT, ERTEILT AVAYA DIESE LIZENZ NUR DANN, WENN DIE SOFTWARE ÜBER EINE DER OBEN GENANNTEN OFFIZIELLEN QUELLEN BEZOGEN WORDEN IST; AVAYA BEHÄLT SICH DAS RECHT VOR, GEGEN SIE ODER DRITTE, DIE DIE SOFTWARE OHNE LIZENZ VERWENDEN ODER VERKAUFEN, GERICHTLICHE SCHRITTE EINZULEITEN. MIT DER INSTALLATION, DEM DOWNLOAD ODER DER NUTZUNG DER SOFTWARE BZW. MIT DEM EINVERSTÄNDNIS ZU INSTALLATION, DOWNLOAD ODER NUTZUNG DURCH ANDERE AKZEPTIEREN SIE IN IHREM EIGENEN NAMEN UND IM NAMEN DES UNTERNEHMENS, FÜR DAS SIE DIE SOFTWARE INSTALLIEREN, HERUNTERLADEN ODER NUTZEN (NACHFOLGEND ALS „SIE" BZW. „ENDBENUTZER" BEZEICHNET) DIESE NUTZUNGSBEDINGUNGEN UND GEHEN EINEN RECHTSGÜLTIGEN VERTRAG ZWISCHEN IHNEN UND AVAYA INC. ODER DEM BETREFFENDEN AVAYA-PARTNER EIN („AVAYA").

Avaya gewährt Ihnen eine Lizenz im Rahmen der unten beschriebenen Lizenztypen mit Ausnahme der Heritage Nortel-Software, deren Lizenzrahmen ebenfalls weiter unten beschrieben wird. Wenn die Bestelldokumentation nicht ausdrücklich einen Lizenztyp angibt, ist die anwendbare Lizenz eine designierte Systemlizenz wie unten im Abschnitt „Systembezogene Lizenz (Designated System(s) License (DS)" erläutert. Grundsätzlich wird für jeweils eine (1) Geräteeinheit eine (1) Lizenz vergeben, sofern keine andere Anzahl von Lizenzen oder Geräteeinheiten in der Dokumentation oder anderen Ihnen zur Verfügung stehenden Materialien angegeben ist. „Software" sind Computerprogramme in Objektcode, die von Avaya oder einem Avaya Channel Partner als unabhängiges Produkt oder vorinstalliert auf einem Hardware-Produkt bereitgestellt werden, sowie jegliche Upgrades, Aktualisierungen, Fehlerbehebungen oder geänderte Versionen dieser Programme. Der Begriff „designierter Prozessor" bezeichnet ein einzelnes unabhängiges Computergerät. Der Begriff „Server" bezeichnet einen Satz designierter Prozessoren, der eine Softwareanwendung für mehrere Benutzer (physisch oder virtuell) bereitstellt. Der Begriff „Instanz" bezeichnet eine einzelne Kopie der Software, die zu einem bestimmten Zeitpunkt (i) auf einem physischen Rechner; oder (ii) auf einer bereitgestellten virtuellen Maschine („VM") oder ähnlicher Bereitstellung ausgeführt wird.

Lizenztyp(en)

Systembezogene Lizenz (Designated System(s) License (DS). Ein ENDBENUTZER darf eine Kopie oder Instanz der SOFTWARE nur folgendermaßen installieren und verwenden: 1) auf einer Anzahl designierter Prozessoren bis zu der im Auftrag angegebenen Anzahl von Prozessoren oder 2) bis zu der im Auftrag, in der DOKUMENTATION oder soweit von AVAYA schriftlich autorisierten angegebenen Anzahl von Instanzen der SOFTWARE. AVAYA kann verlangen, dass der oder die designierten Prozessoren durch Angabe ihres Typs, ihrer Seriennummer, ihrer Leistungsmerkmale, ihrer Instanz, ihres Standorts oder sonstiger Merkmale in dem Einzelvertrag identifiziert werden oder von dem Endanwender auf von AVAYA dafür AVAYA speziell eingerichteten elektronischen Wegen mitgeteilt werden.

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

Cluster-Lizenz (Cluster License (CL)). ENDBENUTZER können, wie im Auftrag, in der DOKUMENTATION oder soweit von AVAYA schriftlich autorisiert, jede Kopie oder nur eine Instanz der SOFTWARE bis zur Anzahl der in der Bestellung angegebenen Cluster installieren und verwenden (standardmäßig ein (1) Cluster, wenn keine Angabe erfolgt ist).

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

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

Shrinkwrap Lizenz (Shrinkwrap License – SR). ENDBENUTZER dürfen die SOFTWARE gemäß den Bedingungen der dafür geltenden Lizenzvereinbarung, wie z. B. eine der SOFTWARE beigelegte oder dafür geltende „Shrinkwrap-" oder „Clickthrough-Lizenz" („Shrinkwrap License"), und wie im Auftrag, in der DOKUMENTATION oder soweit von AVAYA schriftlich autorisiert, installieren und nutzen.

Transaktionslizenz (TR). ENDBENUTZER können die SOFTWARE für so viele Transaktionen nutzen, wie sie für eine bestimmte Zeit im Auftrag, in der DOKUMENTATION oder soweit von AVAYA schriftlich autorisiert, festgelegt wurden. Eine „Transaktion" bezeichnet die Einheit, auf der nach Festlegung von AVAYA der Preis der Lizenzvergabe basiert. Diese kann unter anderem nach Nutzung, Zugriff, Interaktion (zwischen Client/Server oder Kunde/Organisation) oder Betrieb der SOFTWARE innerhalb eines bestimmten Zeitraums (z. B. pro Stunde, pro Tag, pro Monat) gemessen werden. Beispiele für Transaktionen sind unter anderem jede abgespielte Begrüßung/Aktivierung für wartende Nachrichten, jede personalisierte Werbung (in jedem Vertriebsweg), jede Rückruffunktion, jeder Live-Agent oder jede Web-Chat-Sitzung, jeder weitergeleitete oder umgeleitete Anruf (in jedem Vertriebsweg). ENDBENUTZER dürfen die Zahl der Transaktionen nicht ohne die vorherige Zustimmung von AVAYA und Zahlung einer Zusatzgebühr überschreiten.

Heritage Nortel-Software

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

Copyright

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

Virtualisierung

Die folgenden Bestimmungen sind anwendbar, wenn das Produkt auf einem virtuellen Computer bereitgestellt wird. Jedes Produkt hat einen eigenen Bestellcode und eigene Lizenztypen. 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

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

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

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

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

Sicherheitsrisiken

Informationen zu den 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 Inc.

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

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

Contents

Kapitel 1: Dokumentänderungen seit der letzten Ausgabe

An diesem Dokument wurden die folgenden Änderungen für IP Office Version 9.1 vorgenommen.

Software Development Kit (SDK)

Um die Partnerkonfiguration von SSL VPN zu erleichtern, wurden zwei SDKs verfügbar gemacht. Diese werden im Abschnitt Konfiguration eines SSL VPN über das SDK auf Seite 54 beschrieben.

AVG-Schnelleinrichtungsassistent

Der AVG-Schnelleinrichtungsassistent wurde aktualisiert. Siehe Anhang A: AVG-Schnelleinrichtungsassistent – Beispiel auf Seite 96.

Kapitel 2: Info zum SSL VPN-Dienst

Die Remote-Zugriffs-Lösung IP Office SSL-VPN ist ein schnelles und einfaches Mittel zur Einrichtung eines sicheren Remote-Zugriffs mit Breitbandgeschwindigkeit. Die Lösung ist darauf ausgelegt, für Avaya und dessen Partner einen zuverlässigen Remote-Zugriff bereitzustellen, durch den die Erbringung von Dienstleistungen optimiert wird und gleichzeitig die Kosten für vor Ort zu erbringende Dienstleistungen gesenkt werden. Mithilfe dieser Lösung können Partnerunternehmen jeder beliebigen Größenordnung eine Infrastruktur aufbauen, die die Verwaltung und Wartung von IP Office-Systemen automatisiert.

Dienstleistungen durch SSL VPN

Der SSL VPN-Dienst ermöglicht ein gesichertes Tunneling zwischen der beim Kunden installierten Avaya IP Office-Hardware und einem Remote-Avaya VPN Gateway (AVG). Dieser sichere Tunnel ermöglicht Supportmitarbeitern, ihren Kunden Fernverwaltungsdienste wie Fehlerverwaltung, Überwachung und Administration anzubieten. Administratoren können dank des Dienstes folgende Aktionen durchführen:

- Weiterleitung von Traffic über den SSL VPN-Dienst mithilfe von Split Tunneling-Routen und statischen Routen
- Remote-Überwachung des IP Office über einen SSL VPN-Dienst, der über System Status Application (SSA) oder SysMonitor mit dem AVG verbunden ist
- Remote-Verwaltung von IP Office-Systemen über Avaya IP Office Manager oder IP Office Manager for Server Edition
- Empfang von SNMP-Traps, Syslog-Einträgen und SMTP-E-Mail-Warnungen vom IP Office über einen SSL VPN-Dienst, der mit einem AVG-Server verbunden ist
- Aktivierung und Deaktivierung des Tunnels über Manager oder IP Office Manager for Server Edition
- Aktivierung und Deaktivierung des Tunnels über Funktionscodes, automatische Weitervermittlung oder satzbasierte Verwaltung
- gleichzeitige Ausführung mehrerer Instanzen des SSL VPN-Dienstes

Verwandte Links

Bereitstellungsoptionen auf Seite 10

Betriebsmodi auf Seite 10

Systemarchitektur auf Seite 13

Systemanforderungen und -beschränkungen auf Seite 16

Entsprechende Dokumentation auf Seite 17

Bereitstellungsoptionen

Remote-Support-Dienste von Avaya

SSL VPN ist ein wesentliches Element der IP Office Support Services (IPOSS), das Avaya in die Lage versetzt, branchenweit unübertroffene technische Fernunterstützung und -fehlerbehebung bereitzustellen. Der Aufbau der SSL VPN-Verbindung mit Avaya wird durch die automatisierte On-Boarding-Funktion deutlich vereinfacht. Der On-Boarding-Vorgang beinhaltet die Extrahierung des Bestands, die Registrierung beim GRT zur Erstellung des installierten Basiseintrags sowie die technische Registrierung für die Remote-Verbindungen mit Avaya.

Detaillierte Informationen zum IPOSS-Wartungsangebot erhalten Sie auf der Seite IP Office Support Services auf dem Vertriebsportal von Avaya.

Remote-Support-Dienste von Avaya-Partnern

Partner können den SSL VPN-Client separat vom IPOSS-Angebot in Kombination mit der AVG-Lösung (Avaya VPN-Gateway) nutzen, um ihre eigene SSL VPN-Infrastruktur zu erstellen. Dieses Dokument stellt Informationen und Verfahrensweisen zur Unterstützung derjenigen Avaya-Partner bereit, die Ihre eigene SSL VPN-Lösung für den Remote-Zugriff als Teil der Wartungsunterstützung für ihre Kunden.

Die vom Partner konfigurierte SSL VPN-Lösung wird auf Standard Edition- und Server Edition IP Office-Systemen unterstützt.

Verwandte Links

Info zum SSL VPN-Dienst auf Seite 9

Betriebsmodi

Betriebsmodi

Der SSL VPN-Dienst wird von IP500v2-Hardware unterstützt. Das Steuermodul IP500 wird nicht unterstützt.

SSL VPN wird von IP Office in den folgenden Modi unterstützt. Der Branch-Modus wird nicht unterstützt.

- IP Office Standard Edition (Betriebsmodi Essential, Advanced und Preferred)
- Server Edition
  - Primäre Server Edition
  - Sekundäre Server Edition
- Erweiterungssystem Server Edition
  - Erweiterungssystem Server Edition (V2), ein IP500v2-Erweiterungssystem
  - Erweiterungssystem Server Edition (L), ein Linux-Erweiterungssystem
- Basic Edition

Hinweis:

Basic Edition wird nur bei Bereitstellungen mit Avaya IP Office Support Services (IPOSS) unterstützt. Basic Edition wird bei Bereitstellungen von SSL VPN für Unterstützungsdienste von Avaya-Partnern unterstützt.

Unterstützte Funktionen

Der verfügbare Funktionsumfang hängt vom verwendeten Betriebsmodus ab. In diesem Abschnitt erhalten Sie einen Überblick über den Funktionsumfang von SSL VPN und die einzelnen Funktionen, die in jedem Modus zur Verfügung stehen.

Unterstützte Funktionen	Betriebsmodus			
	Standard Edition	Server Edition	Erweiterungssystem Server Edition	Basic Edition
Konnektivität				
Ununterbrochene SSL VPN-Verbindung mit einem AVG-Server	✔	✔	✔	✔
Split-Tunneling-Routen	✔	✔	✔	✔
Statische Routen	✔	✔	✔	✔
Gleichzeitige Ausführung mehrerer Instanzen des SSL VPN-Dienstes	✔	✔	✔	✔
Zugriff auf LAN-Geräte (NAPT)	✔	✔	✔	—
Fehlerverwaltung				
Generierung von SNMP-Traps	✔	✔	✔	✔
Generierung von Syslog-Einträgen	✔	✔	✔	—
Generierung von E-Mail-Benachrichtigungen für Alarme	✔	✔	✔	—
Generierung von Probealarmen	✔	✔	✔	✔
Überwachung und Administration				
Remote-Verwaltung über Manager oder IP Office Manager for Server Edition	✔	✔	✔	✔

Table continues…

Unterstützte Funktionen	Betriebsmodus			
	Standard Edition	Server Edition	Erweiterungssystem Server Edition	Basic Edition
Remote-Überwachung über System Status Application	✔	✔	✔	✔
Remote-Überwachung über SysMonitor	✔	✔	✔	✔
Aktivierung und Deaktivierung des SSL VPN-Dienstes über Funktionscodes	✔	✔	✔	—
Aktivierung und Deaktivierung des SSL VPN-Dienstes über satzbasierte Menüs	—	—	—	✔
Aktivierung und Deaktivierung des SSL VPN-Dienstes über Manager oder IP Office Manager for Server Edition	✔	✔	✔	—
Aktivierung und Deaktivierung des SSL VPN-Dienstes über automatische Weitervermittlung	✔	✔	✔	—
Aktivierung und Deaktivierung des SSL VPN-Dienstes über programmierbare Tasten auf Tischtelefonen von Avaya	✔	✔	✔	✔
Remote-Upgrade von IP Office auf neue Versionen	✔	✔	✔	✔

Überwachungs und Administrationstools

Wenn der SSL VPN-Dienst verbunden ist, können Sie das IP Office-System dezentral über den Tunnel verwalten und überwachen.

Mit den folgenden Werkzeugen können Sie das IP-System dezentral verwalten, aktualisieren und konfigurieren:

- IP Office Manager: Eine Administrationsanwendung, mit der Sie die Systemeinstellungen von IP Office Essential Edition-Systemen konfigurieren können.
  - IP Office Manager for Server Edition: Wenn Sie IP Office Manager starten, können Sie über den IP Office Manager for Server Edition-Modus die Konfiguration öffnen. In diesem Modus können Sie Server Edition-Server und -Erweiterungssysteme verwalten.
- IP Office Basic Edition – Web Manager: ein browserbasiertes Werkzeug, mit dem Sie die Systemeinstellungen für IP Office konfigurieren können.

Mit den folgenden Werkzeugen können Sie das IP Office-System dezentral überwachen:

- System Status Application (SSA): System Status Application ist ein Diagnosewerkzeug, mit dem Sie den Status von IP Office-Systemen überwachen können. SSA berichtet historische und Echtzeit-Ereignisse und Status- und Konfigurationsdaten.
- SysMonitor: SysMonitor zeigt Betriebsinformationen über das IP Office-System an. Die Anwendung kann diese Daten erfassen, um Dateien zu Analysezwecken zu protokollieren.

Verwandte Links

Info zum SSL VPN-Dienst auf Seite 9

Systemarchitektur

Der SSL VPN-Dienst ermöglicht ein sicheres Tunneling zwischen der beim Kunden installierten IP Office-Hardware und einem beim Dienstanbieter installierten Avaya VPN Gateway (AVG). Die Informationen in diesem Abschnitt sollen Ihnen ein grundlegendes Verständnis der vom SSL VPN-Dienst verwendeten Netzwerkarchitektur ermöglichen.

Netzwerkkarten

Avaya empfiehlt die Bereitstellung des AVG-Servers in einer zweiarmigen Konfiguration mit zwei Netzwerkkarten (NIC, Network Interface Card). Über die eine Schnittstelle läuft der private Traffic zwischen dem SSL VPN-Dienst und dem geschützten Intranet. Mithilfe dieser Verbindung kann der SSL VPN-Dienst auf interne Ressourcen zugreifen, und Sie können das IP Office-System über eine Management-Station verwalten. Über die zweite Schnittstelle wird der Traffic aus dem und ins Internet abgewickelt.

Verteilung

Am Standort des Dienstanbieters können Sie die Unternehmensverteilung zwischen AVG und dem privaten Netzwerk konfigurieren. Am Standort des Kunden können Sie jedes IP Office-System auf der privaten Seite eines Unternehmensrouters lokalisieren. Am Unternehmensrouter müssen keine Konfigurationsänderungen durchgeführt werden, damit der SSL VPN-Dienst funktioniert.

IP Office leitet Daten mithilfe von Split-Tunneling-Routen oder statischen Routen über den SSL VPN-Dienst an AVG weiter. Zum Senden von Traffic über den SSL VPN-Tunnel müssen Sie eine der folgenden Optionen nutzen:

- dynamische Installation von Split-Tunneling-Routen, bei denen der SSL VPN-Dienst eine Verbindung mit AVG aufbaut, und Löschen dieser Routen nach dem Beenden der Verbindung durch IP Office
- Konfiguration einer statischen Route in IP Office Manager

Split-Tunneling:

Bei der Installation und Konfiguration von AVG können Sie Split-Subnetze oder Host-Adressen für eine Gruppe hinzufügen. Dem IP Office-System werden die Routing-Daten des Tunnels dynamisch mitgeteilt, sobald der SSL VPN-Dienst erfolgreich eine Verbindung mit AVG aufgebaut hat. Die Split-Netzwerk-Routen werden gelöscht, sobald der SSL VPN-Dienst die Verbindung mit AVG beendet.

Informationen über die Konfiguration von Split-Tunneling in AVG über Net Direct finden Sie im Avaya VPN Gateway *Administration Guide* (Administratorhandbuch) (NN46120-105) und dem Avaya VPN Gateway *BBI Application Guide* (BBI-Anwendungsleitfaden) (NN46120-102). Informationen über die Konfiguration von Split-Tunneling über die Befehlszeilenschnittstelle finden Sie unter *CLI Application Guide* (CLI-Anwendungsleitfaden) (NN46120-101).

Statische Routen:

Als Alternative zum Split-Tunneling können Sie direkt im IP Office-System eine statische Route konfigurieren. Bei der Konfiguration einer statischen Route nutzt das System die in Manager konfigurierten IP-Routendaten, um das Ziel für den weitergeleiteten Traffic zu bestimmen. Der SSL VPN-Dienst muss als Ziel festgelegt werden.

Verwenden Sie eine statische Route, wenn:

- Split-Tunneling-Routen in AVG nicht vorgesehen sind und Sie Traffic über den Tunnel senden müssen
- der SSL VPN-Dienst nicht mit AVG verbunden ist und Sie den weiterzuleitenden Traffic über den Tunnel senden wollen, wenn die Verbindung wiederhergestellt ist; in diesem Fall speichert IP Office eine kleine Anzahl an Paketen temporär in einer Warteschlange, die den Verbindungsaufbau anstoßen, sobald der SSL VPN-Dienst betriebsbereit, aber nicht verbunden ist

Es ist möglich, auf dem IP Office-System mehrere statische Routen zu konfigurieren.

Authentifizierung

Jedes IP Office-System kann mehrere SSL VPN-Tunnel unterstützen. Jeder Instanz eines SSL VPN-Dienstes wird eine eindeutige private statische IP-Adresse zugewiesen. Beim Aufbau einer Verbindung mit dem SSL VPN-Dienst authentifiziert AVG das IP Office-System. Bei einer kleinen Anzahl von IP Office-Systemen können Sie die lokale Datenbank des Avaya VPN Gateway (AVG) zur Erstellung der für die Authentifizierung erforderlichen Userdaten verwenden. Bei größeren Bereitstellungen wird die Verwendung eines RADIUS-Servers für die Authentifizierung empfohlen.

Zugriff von Dienstagenten

Dienstagenten am Standort des Dienstanbieters können eine Verbindung mit jedem IP Office-System aufbauen, das über eine aktive SSL VPN-Verbindung zu AVG verfügt. Sie können das IP Office-System remote überwachen und verwalten, indem Sie die IP-Adresse des SSL VPN-

Tunnels kontaktieren. Außerdem können sie gleichzeitig auf die IP-Adressen mehrerer SSL VPN-Dienste zugreifen.

AVG sorgt dafür, dass SSL VPN-Tunnel nicht miteinander kommunizieren können. Sie brauchen keine zusätzlichen Einstellungen zu konfigurieren, um sicherzustellen, dass die Tunnel sicher und unabhängig bleiben.

Fehlerverwaltung

Der Fehlerverwaltungsserver ist eine optionale Komponente des SSL VPN-Dienstes. Stellen Sie am Standort des Dienstanbieters einen Fehlerverwaltungsserver bereit, und senden Sie Systemfehler über den SSL VPN-Dienst an diesen Server. Sie können Ereignisfilter festgelegen, die definieren, welche Fehler berichtet werden. So können beispielsweise Filter festgelegt werden, die alle Ereignisse bezüglich des Betriebs des IP Office-Systems berichten; darüber hinaus können spezielle Fehler bezüglich des Betriebs des SSL VPN-Dienstes berichtet werden.

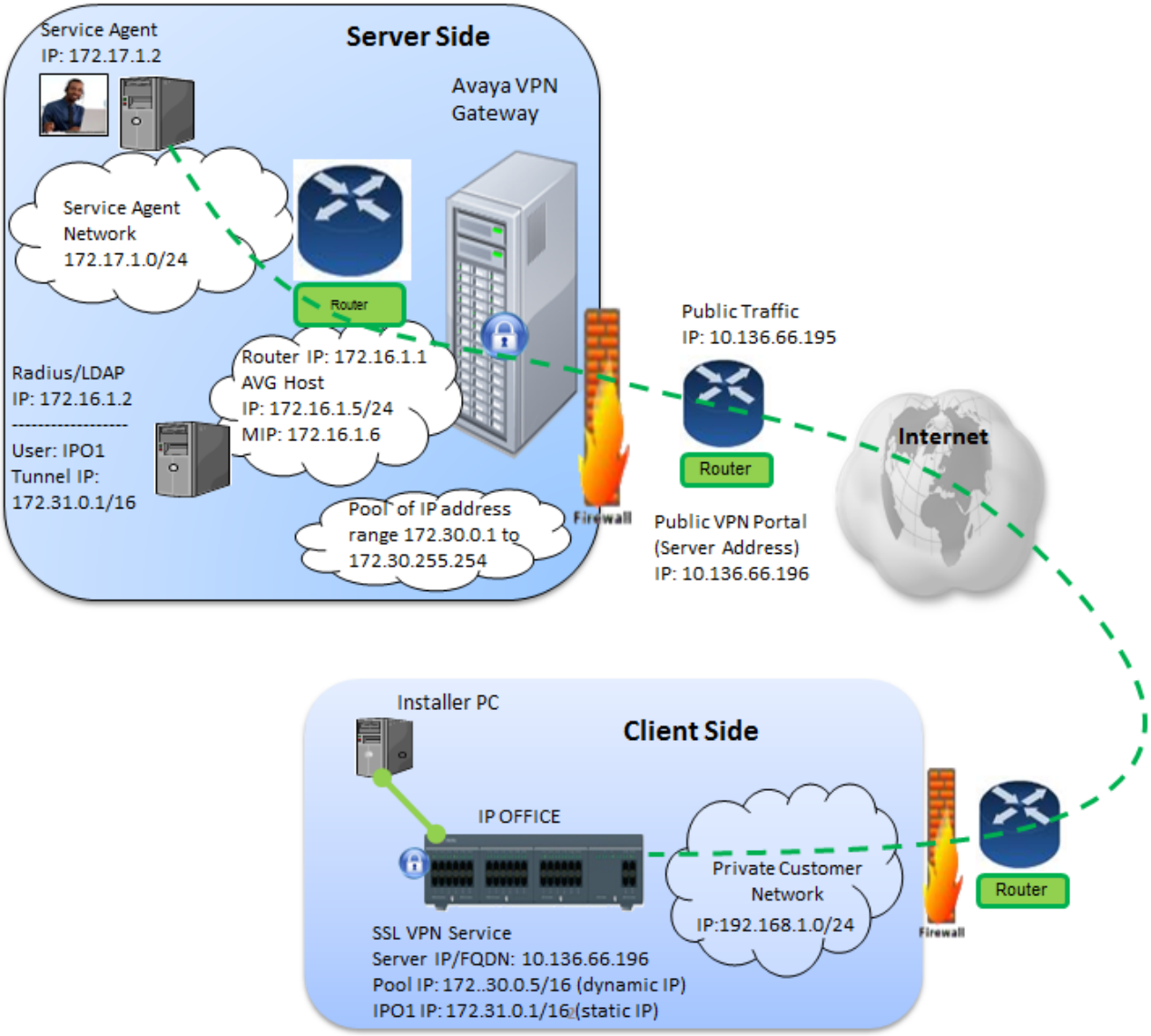
Avaya empfiehlt, den Kontonamen des SSL VPN-Dienstes so festzulegen, dass er dem Namen der SNMP-Agenten-Geräte-ID entspricht. Die SNMP-Agenten-Geräte-ID wird in IP Office Manager im Formular **System** unter **Systemereignisse** > **Konfiguration** konfiguriert.

Firewall-Traversal

Der SSL VPN-Dienst arbeitet transparent innerhalb der Firewall. Wenn Ihr Unternehmensrouter bereits für den HTTP-Traffic konfiguriert wurde, braucht er nicht extra zum Zulassen des SSL VPN-Dienstes konfiguriert werden. Der SSL VPN-Dienst verwendet für seinen TCP-Traffic denselben Zielport.

Architekturbeispiel

Das folgende Diagramm zeigt ein Beispiel für die vom SSL VPN-Dienst verwendete Architektur.



Verwandte Links

[Info zum SSL VPN-Dienst](#) auf Seite 9

Systemanforderungen und -beschränkungen

Anforderungen

Bandbreite:

Achten Sie darauf, dass die Upload-Bandbreite mindestens 90 KBit/s (720 KBit/s) beträgt. Dabei darf die Latenz nicht höher als 150 ms (Round Trip) sein. Durch diese Spezifikation wird

sichergestellt, dass die Avaya Global Services über den SSL VPN-Dienst Remote-Support bieten können.

Authentifizierung:

- Bei einer kleinen Anzahl von IP Office-Systemen können Sie die lokale Datenbank des Avaya VPN Gateway (AVG) zur Erstellung der für die Authentifizierung erforderlichen Userdaten verwenden.
- Große Bereitstellungen erfordern einen RADIUS-Server. Avaya empfiehlt die Nutzung von Avaya Identity Engines Ignition Server als RADIUS-Server.
- Das IP Office-System verwendet digitale Zertifikate, um die Identität von AVG auf Seiten des SSL VPN-Tunnels zu überprüfen. Zertifikate müssen in AVG konfiguriert werden. Außerdem müssen die erforderlichen X.509-Zertifikate im IP Office-Zertifikatspeicher installiert werden.

Lizenzierung:

Für den SSL VPN-Dienst wird kein Lizenzschlüssel benötigt.

Einschränkungen

Small Community Networks:

Wenn IP Office-Systeme in einem Small Community Network (SCN) bereitgestellt werden, kann ein SSL VPN-Dienst zwischen bestimmten Knoten im SCN und in AVG konfiguriert werden. Über die SSL VPN-Verbindung kann remote auf andere Knoten in der SCN-Topologie zugegriffen werden: Der SSL VPN-Dienst kommuniziert nur mit dem IP Office-System, der sein Endpunkt ist. Für jeden Knoten im SCN, auf den remote zugegriffen werden soll, muss ein SSL VPN-Dienst konfiguriert werden.

Zertifikate:

Im Speicher vertrauenswürdiger Zertifikate von IP Office können maximal 25 Zertifikate gespeichert werden.

HTTP-Version:

Wenn Sie einen Browser mit einer neueren HTTP-Version als 1.1 verwenden, können Sie mit SSL VPN NAPT eventuell keine Verbindung zu LAN-Geräten herstellen. Wenn beim Aufbau einer Verbindung zum LAN-Gerät Schwierigkeiten auftreten, sollten Sie Ihre Browsereinstellungen so ändern, dass die HTML-Version 1.1 verwendet wird.

Verwandte Links

Info zum SSL VPN-Dienst auf Seite 9

Entsprechende Dokumentation

Beziehen Sie sich hinsichtlich der Installation, Konfiguration und Verwaltung der SSL VPN-Lösung auf die Dokumentation des Avaya IP Office-Systems, von Avaya VPN Gateway (AVG) und von Avaya Identity Engines Ignition Server. Darüber hinaus finden Sie weitere Informationen zur Unterstützung der Hard- und Software, die Sie in Ihrer Netzwerkinfrastruktur einsetzen, in der Dokumentation anderer Anbieter.

Legen Sie die folgende Avaya Dokumentation bereit, um die SSL VPN-Lösung zu unterstützen.

Avaya VPN Gateway-Dokumentation

- *Avaya VMware Getting Started Guide* (Erste Schritte mit Avaya VMware) - Avaya VPN Gateway (NN46120-302)
- *Avaya VPN Gateway User Guide* (Benutzerhandbuch) (NN46120-104)
- *Avaya VPN Gateway Administration Guide* (Administratorhandbuch) (NN46120-105)
- *Avaya VPN Gateway BBI Application Guide* (BBI-Anwendungsleitfaden) (NN46120-102)
- *Avaya VPN Gateway CLI Application Guide* (CLI-Anwendungsleitfaden) (NN46120-101)

Dokumentation zu Avaya IP Office

- *Avaya IP Office Basic Edition – Web Manager*
- *Avaya IP Office Manager*
- *Verwaltung von Voicemail Pro*
- *Installation von Embedded Voicemail*

Dokumentation zu Avaya Identity Engines Ignition Server

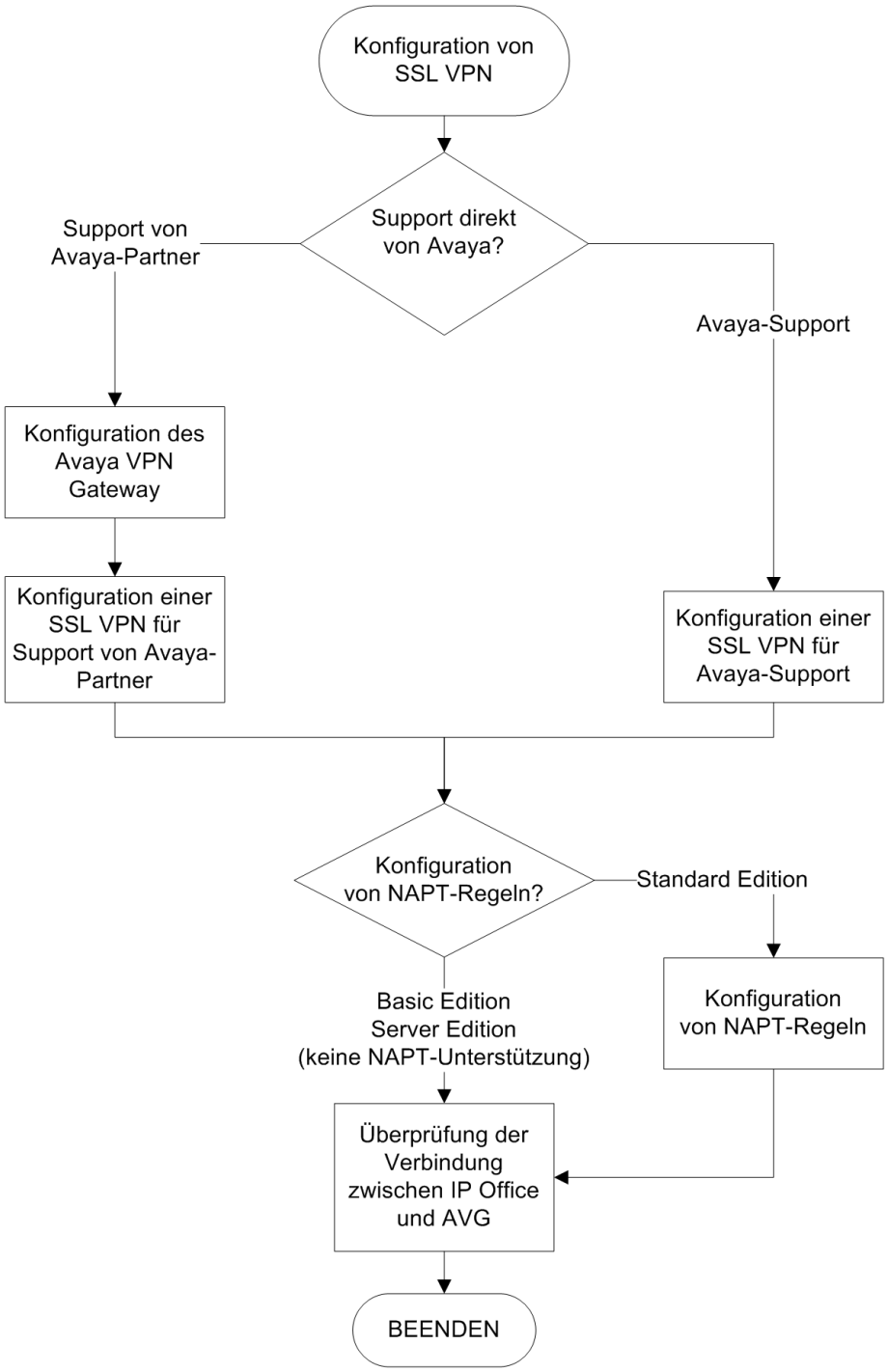
- *Avaya Identity Engines Ignition Server — Configuration Guide* (Avaya Identity Engines Ignition Server — Konfigurationsleitfaden) (NN47280-500)

Verwandte Links

Info zum SSL VPN-Dienst auf Seite 9

Kapitel 3: Workflow für die Konfiguration eines SSL VPN

Hier wird Ihnen der Ablauf der Vorgänge für die Konfiguration eines SSL VPN erklärt.



Navigation

- Konfigurieren des auf Seite 22
- Konfigurieren eines SSL VPN für den Avaya-Support auf Seite 36
- Konfigurieren eines SSL VPN für die Unterstützung durch Avaya-Partner auf Seite 40

- NAPT-Regeln (Network Address & Port Translation, Konvertierung der Netzwerkadressen und Ports) auf Seite 61
- Überprüfen Sie die Verbindung zwischen und auf Seite 64

Kapitel 4: Konfiguration des Avaya VPN Gateway

Zur Bereitstellung von Unterstützung für die SSL VPN-Lösung müssen Avaya-Partner das Avaya VPN Gateway (AVG) konfigurieren.

In diesem Abschnitt finden Sie Informationen über die Aufgaben, die Sie durchführen müssen, wenn Sie AVG installieren und so konfigurieren möchten, dass SSL VPN-Verbindungen mit IP Office-Systemen unterstützt werden.

Bevor das IP Office-System für einen SSL VPN-Dienst konfiguriert werden kann, muss die Infrastruktur konfiguriert werden, mit der der Dienst eine Verbindung aufbaut. In diesem Abschnitt wird die Konfiguration der Zusammenarbeit des AVG mit IP Office-Systemen behandelt. Befolgen Sie die Angaben in der Dokumentations-Suite für AVG und der von anderen Anbietern bereitgestellten Dokumentation, um die Aufgaben durchzuführen, die zur Unterstützung der Hard- und Software in Ihrer Netzwerkinfrastruktur erforderlich sind.

Die Hauptaufgaben für die Bereitstellung des Avaya VPN Gateway werden in diesem Kapitel beschrieben. Hierbei handelt es sich um allgemeine Empfehlungen. Die Einzelheiten der Bereitstellung sind je nach der speziellen Umgebung des Geschäftspartners unterschiedlich.

Verwandte Links

Anfängliche Planung und Einrichtung auf Seite 23
Avaya VPN Gateway-Konfigurationsablauf auf Seite 23
Grundlegende AVG-Konfiguration auf Seite 25
Aktivierung der Remote-Zugriffsdienste auf Seite 26
Aufruf des Net Direct Wizard auf Seite 26
Änderung des Standard-AVG für SSL VPN auf Seite 27
Konfiguration der lokalen Authentifizierung auf Seite 29
Konfiguration der RADIUS-Authentifizierung auf Seite 30
Konfiguration der Attribute auf dem RADIUS-Server auf Seite 32

Anfängliche Planung und Einrichtung

Virtuelle Umgebung

Für den SSL VPN-Client muss das Avaya VPN Gateway (AVG) in einer virtualisierten Umgebung als VPN Gateway-Server installiert sein. Die einzigen unterstützten virtuellen Umgebungen sind ESX- und ESXi-Server. ES gibt drei Modelle des AVG: 3050–VM, 3070–VM und 3090–VM. Die technischen Daten für die einzelnen Modelle finden Sie in der Dokumentation *VMware Getting Started Guide, Avaya VPN Gateway* (Erste Schritte mit Avaya VMware, NN46120-302). Sie können die vollständige AVG-Dokumentation unter http://support.avaya.com herunterladen.

Weitere Informationen zu VMware ESXi-Servern sind unter http://www.vmware.com verfügbar.

Zweiarmige Konfiguration

Installieren Sie das Avaya VPN Gateway (AVG) in einer zweiarmigen Konfiguration. Das bedeutet, dass der AVG-Server mit zwei Netzwerkkarten (NICs) ausgestattet sein muss. Weisen Sie jeder NIC eine statische IP-Adresse zu.

- Eine Schnittstelle bearbeitet den privaten Datenverkehr und wird als Verwaltungsschnittstelle verwendet.
- Die andere Schnittstelle bearbeitet den Internetzugang und das SSL VPN-Tunneling.

AVG-Software

Es gibt zwei Optionen für die Bereitstellung der AVG-Software.

- Bereitstellung virtueller AVG OVF-Geräte
- Autoinstallation von CD-ROM

Informationen zur Installation des AVG finden Sie in der Dokumentation *VMware Getting Started Guide, Avaya VPN Gateway* (Erste Schritte mit Avaya VMware, NN46120-302).

Dienstagenten-PC

Installieren Sie den Dienstagenten-PC (SA-PC) im privaten Netzwerk, und stellen Sie für das Standardgateway die Host-IP-Adresse des Avaya VPN Gateway (AVG) ein.

Auf dem Dienstagenten-PC

- Die IP-Adresse der Verwaltungsschnittstelle (MIP) wird für den Aufruf einer browserbasierten Verwaltungsoberfläche (Management Browser Based Interface, BBI) oder Command Line Interface (CLI) zur Konfiguration und Überwachung des AVG verwendet.
- Die IP-Adresse für das SSL VPN-Tunneling wird zur externen Verwaltung und Überwachung von IP Office-Systemen verwendet.

Verwandte Links

Konfiguration des Avaya VPN Gateway auf Seite 22

Avaya VPN Gateway-Konfigurationsablauf

Hier wird Ihnen der Ablauf der zur Konfiguration des AVG durchzuführenden Vorgänge erklärt.


Konfiguration des Avaya VPN Gateway
AVG-Grundeinstellungen
Aktivieren von Remote Access-Dienst
Ausführen des Net Direct-Assistenten
Abändern der AVG-Standardeinstellungen
Konfiguration von RADIUS-Authentifizierung?
Nein
Ja
Konfiguration von lokaler Authentifizierung
Konfiguration von RADIUS-Authentifizierung
Konfigurationsattribute von RADIUS-Server
Testen von AVG SSL VPN-Bereitstellung
BEENDEN

Navigation

Verwandte Links

Konfiguration des Avaya VPN Gateway auf Seite 22

Grundlegende AVG-Konfiguration

Konfiguration des AVG über den Dienstagenten-PC

Wenn Sie das VPN Gateway zum ersten Mal starten, gelangen Sie ins Menü **Einrichtung**. Dieses Menü enthält den CLI-Befehl **Neu**. Dies ist ein CLI-basierter, intuitiver Assistent für die Erstkonfiguration des AVG, der Standardeinstellungen für die schnelle Einrichtung von SSL-Verbindungen mit IP Office bereitstellt. Er ist nützlich für die Erstkonfiguration und -überprüfung. Dies ist der schnellste Weg für die Erstkonfiguration des AVG. Später kann die browserbasierte Verwaltungsoberfläche (Browser-Based Management Interface, BBI) zum Vornehmen empfohlener Änderungen für die SSL VPN-Verbindungen verwendet werden. Weitere Informationen finden Sie im Benutzerhandbuch *User Guide Avaya VPN Gateway* (NN46120-104).

Nach Verwendung des Befehls „Neu“ zum Aufrufen des Schnelleinrichtungsassistenten sind die folgenden Einstellungen erstellt worden:

- Ein VPN. Das VPN wird normalerweise für den Zugriff auf ein Intranet, Teile eines Intranets oder ein Extranet definiert.
- Ein virtueller SSL-Server der Portal-Kategorie. Diesem wird eine Portal-IP-Adresse zugewiesen, zu der Remote-Benutzer eine Verbindung herstellen sollten, um auf das Portal zuzugreifen. Wenn Sie die VPN-Funktion ohne Application Switch verwenden, wird der Portalserver für den Standalone-Modus eingestellt.
- Es wurde ein Testzertifikat installiert und dem Portalserver zugeordnet.
- Die Authentifizierungsmethode wurde „Local database“ (Lokale Datenbank) eingestellt, und es wurde ein Testbenutzer konfiguriert. Der Testbenutzer gehört zu einer Gruppe namens `trusted`, deren Zugriffsregeln den Zugriff auf alle Netzwerke, Dienste und Pfade erlauben.
- Ein oder mehrere Domainnamen wurden der DNS-Suchliste hinzugefügt, d. h. dass der Remote-Benutzer einen Kurznamen in die diversen Adressfelder des Portals eingeben kann (z. B. „inside“ anstatt „inside.example.com“, falls „example.com“ der Suchliste hinzugefügt wurde).

- Wenn Sie die Umleitung von HTTP zu HTTPS aktiviert haben, wurde ein zusätzlicher HTTP-Server für die Umleitung der in HTTP gestellten Anfragen zu HTTPS erstellt, da der Portalserver eine SSL-Verbindung erfordert.

Ein Ausdruck von Beispiel-Konfigurationseinstellungen aus der Protokolldatei „Schnelleinrichtung“ ist unter Anhang A: AVG Beispielprotokolldatei "Schnelleinrichtung" auf Seite 96 verfügbar.

Verwandte Links

Konfiguration des Avaya VPN Gateway auf Seite 22

Aktivierung der Remote-Zugriffsdienste

Außer der Verwendung der lokalen VM-Konsole zur Konfiguration des VPN muss der Administrator auch das VPN mittels TELNET- oder SSH-Sitzung oder über die BBI verwalten. Damit das VPN-Gateway von außerhalb konfiguriert werden kann, müssen die Remote-Zugriffsdienste aktiviert werden.

Nutzen Sie zum Durchführen des Verfahrens die Befehlszeilen-Oberfläche (Command Line Interface, CLI). Beachten Sie auch die folgenden zugehörigen AVG-Dokumente:

- *Command Reference Avaya VPN Gateway (Befehlsübersicht)*
- *CLI Application Guide Avaya VPN Gateway (CLI-Anwendungsleitfaden)*

Vorgehensweise

1. Melden Sie sich beim AVG an.
2. Geben Sie die folgenden Befehle ein:

```
/cfg/sys/adm/.
        telnet on
        ssh on
/cfg/sys/adm/https/.
        cert 1
        ena true
/cfg/sys/adm/http/.
        ena true
apply
```

Verwandte Links

Konfiguration des Avaya VPN Gateway auf Seite 22

Aufruf des Net Direct Wizard

Mit dem Net Direct Wizard können Sie eine Verknüpfung auf dem Portal erstellen, über die eine vereinfachte Version des Avaya VPN-Clients heruntergeladen und gestartet wird: Der Net Direct-Client. Starten Sie den Net Direct Wizard über die browserbasierte Oberfläche (BBI) von Manager. Siehe *Avaya VPN Gateway BBI Application Guide* (BBI-Anwendungsleitfaden).

Vorgehensweise

1. Melden Sie sich bei der BBI des AVG an.

   Wählen Sie **Wizards** (Assistenten) im linken Navigationsfenster.

2. Klicken Sie auf **Net Direct Wizard**.
3. Wählen Sie auf der Seite **Net Direct settings for the selected VPN** (Net Direct-Einstellungen für das ausgewählte VPN) die Optionsschaltfläche **Enable Net Direct for this VPN** (Net Direct für dieses VPN aktivieren).
4. Auf der Seite **Default IP Pool Settings** (Standardeinstellungen IP-Pool):
   - Wählen Sie unter **Default IPPool** (Standard-IPPool) die Option **Local_pool**.
   - Geben Sie die untere und die obere IP-Adresse für den Poolbereich ein.

Verwandte Links

Konfiguration des Avaya VPN Gateway auf Seite 22

Änderung des Standard-AVG für SSL VPN

Nach Ausführung der Konfigurationsassistenten für Schnelleinstellung und Net Direct muss die Standardkonfiguration geändert werden, um eine SSL VPN-Verbindung mit einem IP Office-System zu unterstützen.

Nutzen Sie zum Durchführen der Aktionen die browserbasierte Oberfläche (Browser-Based Interface, BBI) von AVG. Siehe *Avaya VPN Gateway BBI Application Guide* (BBI-Anwendungsleitfaden).

Dieses Verfahren kommt in Anhang B: Änderung des Standard-AVG für SSL VPN (mit Bildschirmfotos) auf Seite 100 mehrfach vor. Diese Version des Verfahrens beinhaltet Bildschirmfotos der Benutzeroberfläche.

Voraussetzungen

Vergewissern Sie sich, dass das im AVG konfigurierte Standard-Gateway auf ICMP-Anfragen antwortet. Falls das Standard-Gateway nicht auf ICMP-Anfragen reagiert, kann das AVG keine VPN-Dienste bereitstellen.

Vorgehensweise

1. Melden Sie sich als Administrator bei der BBI des AVG an.
2. Wählen Sie im linken Navigationsfenster die Registerkarte **Config** (Konfig.) und dann **VPN Gateway** > **VPN1** > **IP Pool**.
3. Das Standard-VPN aus der grundlegenden AVG-Konfiguration hat eventuell bereits einen lokalen Pool. Falls nicht, müssen Sie dem Standard-VPN einen lokalen Pool hinzufügen. Fügen Sie dem Standard-VPN auf der Seite **Add new IP Address Pool** (Neuen IP-Adressenpool hinzufügen) einen lokalen Pool hinzu.

4. Überprüfen Sie auf der Seite **Modify IP Address Pool** (IP-Adressenpool ändern), ob die Werte in den Feldern **Lower IP** (Untere IP) und **Upper IP** (Obere IP) mit den Werten übereinstimmen, die mit dem Net Direct-Konfigurationsassistenten eingestellt wurden.
5. Wählen Sie auf der Seite **IP Pool** > **Network Attributes Settings** (IP-Pool > Netzwerkattributeinstellungen) die Registerkarte **Network Attributes** (Netzwerkattribute), und geben Sie die Werte für Ihr Netzwerk ein.
6. Stellen Sie auf der Seite **IP Pool** (IP-Pool) den in Schritt 3 erstellten lokalen Pool als **Default IP Pool** (Standard-IP-Pool) ein.
7. Überprüfen Sie auf der Seite**Net Direct Client Access Settings** (Zugangseinstellungen Net Direct Client) die mit dem Net-Direct-Konfigurationsassistenten vorgenommenen Einstellungen.
   - Vergewissern Sie sich, dass **Idle Check** (Inaktivitätsprüfung) auf **off** (aus) gestellt ist.
   - Vergewissern Sie sich, dass das Net Direct-Banner eingestellt ist.
8. Stellen Sie die Portalverbindung für den Aufruf des Net Direct-Clients ein. Wählen Sie auf der Seite **Portal Linkset Configuration** (Konfiguration Portalverbindungen) die Registerkarte **Portal Link** (Portalverbindung). Wählen Sie **Net Direct** im Feld **Verbindungstyp**.
9. Auf der Seite **Networks for Split Tunnels** (Netzwerke für aufgeteilte Tunnel):
   - Stellen Sie **Split Tunnel Mode** (Aufgeteilter Tunnelmodus) auf **Aktiviert.**
   - Stellen Sie die aufgeteilten Tunnelrouten so ein, dass der Dienstagent im privaten Netzwerk erreicht wird.
10. Für VPN1: Rufen Sie die Gruppenseite auf, und wählen Sie **Group1** (Gruppe1). Stellen Sie auf der Seite **Modify a Group** (Gruppe ändern) als IP-Pool den in Schritt 3 erstellten lokalen Pool ein.
11. Rufen Sie die Seite **VPN1** > **Group1** > **Access Lists** (VPN1 > Gruppe1 > Zugriffslisten) auf. Erstellen Sie auf der **Firewall Access List** (Firewall-Zugriffsliste) eine Zugriffsregel, falls eine solche nicht standardmäßig erstellt wurde.
12. Rufen Sie die Seite **VPN1** > **SSL** auf. Stellen Sie auf der Seite **Server Settings** (Servereinstellungen) unter **SSL Settings** (SSL-Einstellungen) für die **Ciphers** (Chiffren) den Wert **AES256-SHA** ein, um eine sichere Verschlüsselung zu erhalten.
13. Rufen Sie die Seite **VPN1** > **Autorisierung** > **Dienste** auf. Entfernen Sie alle in der Standardkonfiguration eingestellten Dienste, da sie von SSL VPN nicht benötigt werden.
14. Rufen Sie die Seite **VPN1** > **Autorisierung** > **Networks (Netzwerke)** auf. Stellen Sie das Autorisierungsnetzwerksubnetz ein, auf das in einer der unter **VPN1** > **Group1** > **Access Lists** (VPN1 > Gruppe1 > Zugriffslisten) eingerichteten Zugriffsregeln verwiesen wird.

    Hinweis:

    Diese Einstellung steuert die wechselseitige Kommunikation über den SSL-VPN-Tunnel. Damit die Kommunikation aktiviert wird, muss eine Liste mit erlaubten

„Intranet“-Netzwerken angegeben werden. Die Inter-VPN-Client-Kommunikation ist standardmäßig gesperrt.

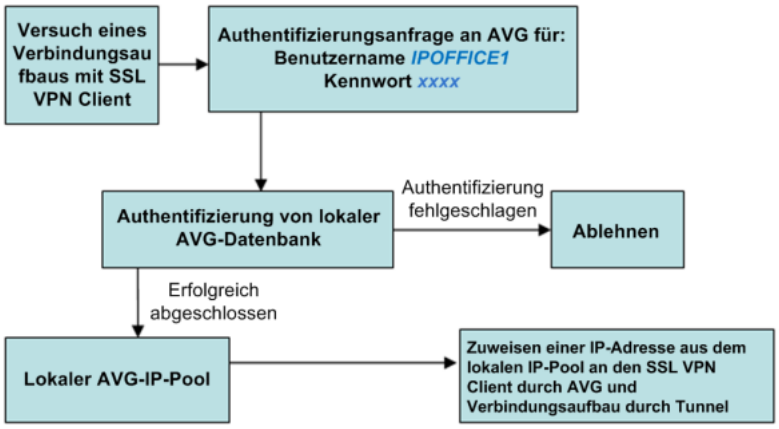
15. Rufen Sie die Seite **VPN1** > **Allgemeine Einstellungen** > **Sitzung** auf. Stellen Sie die **Session Idle Time** (Inaktive Zeit der Sitzung) auf 2 Minuten ein.

Verwandte Links

[Konfiguration des Avaya VPN Gateway](#) auf Seite 22

Konfiguration der lokalen Authentifizierung

Bei einer kleinen Anzahl von IP Office-Systemen können Sie die lokale Datenbank des Avaya VPN Gateway (AVG) zur Erstellung der für die Authentifizierung erforderlichen Userdaten verwenden. Hierdurch lässt sich die Authentifizierung schnell einrichten, wenn keine externen RADIUS-Authentifizierungsserver verfügbar sind. Konfigurieren Sie einen IP-Pool, um IP-Adressen dynamisch an lokale Benutzer zuzuweisen. Die folgende Abbildung zeigt den Authentifizierungsablauf des SSL VPN-Clients und wie die Zuordnung der Adressen aus dem IP-Pool erfolgt.



Dieses Verfahren behandelt die manuellen Schritte für die Konfiguration der lokalen Authentifizierung. Alternativ können Sie die Authentifizierung auch mit dem AVG-Authentifizierungsassistenten konfigurieren.

Vorgehensweise

1. Rufen Sie für **VPN1** die Seite **IP Pool Configuration** (IP-Pool-Konfiguration) auf, und fügen Sie einen lokalen IP-Pool hinzu.
2. Navigieren Sie zu **VPN1** > **IP Pool** > **Add/Modify** (VPN1 > IP-Pool > Hinzufügen/Ändern). Legen Sie den dynamischen Bereich des IP-Pools fest, indem Sie Werte in die Felder **Lower IP** (Untere IP) und **Upper IP** (Obere IP) eingeben.
3. Navigieren Sie zu **VPN1** > **IP Pool** > **Network Attribute** (VPN1 > IP-Pool > Netzwerkattribut). Legen Sie die **Client Netmask** (Netzmaske des Clients) fest.

4. Fügen Sie auf der Seite **Add a Group** (Gruppe hinzufügen) eine neue Gruppe für VPN1 hinzu.
5. Navigieren Sie zu **VPN1** > **<Group_Name>** > **Modify Group** (VPN1 > <Gruppenname> > Gruppe ändern). Weisen Sie der Gruppe auf der Registerkarte **Allgemein** einen lokalen Pool zu, indem Sie sie im Feld **IP Pool** (IP-Pool) auswählen.
6. Geben Sie auf der Registerkarte **Access Lists** (Zugriffslisten) die Zugriffsliste für die lokalen Benutzergruppen an.
7. Weisen Sie auf der Registerkarte **Linksets** (Linksets) die Linksets zu.
8. Bearbeiten Sie die VPN-Authentifizierungseinstellungen. Fügen Sie auf der Seite **Authentication Servers** (Authentifizierungsserver) einen neuen Authentifizierungsserver hinzu.
9. Fügen Sie unter **VPN1** > **<Auth_Server_Name>** > **Add/Modify Users** (VPN1 > <Authentifizierungsservername> > Benutzer hinzufügen/ändern) der Gruppe Benutzer hinzu.
10. Bearbeiten Sie den Authentifizierungsserver, und geben Sie die **Authentication Order** (Authentifizierungsreihenfolge) an.

Verwandte Links

Konfiguration des Avaya VPN Gateway auf Seite 22

Konfiguration der RADIUS-Authentifizierung

Der Hauptvorteil der RADIUS-Authentifizierung besteht darin, dass der SSL VPN-Dienst immer die gleiche Tunnel-IP-Adresse zugewiesen bekommt.

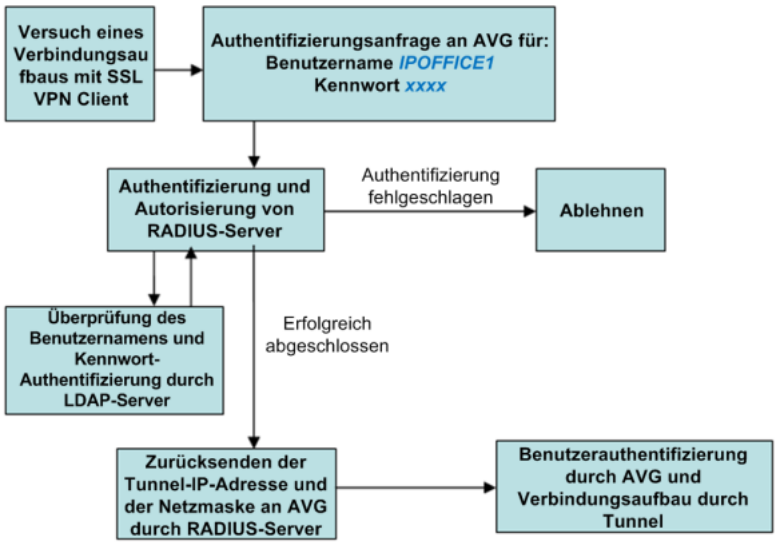
Zur Konfiguration der RADIUS-Authentifizierung müssen Sie einen RADIUS-Server installieren. Avaya empfiehlt die Avaya Identity Engine für einen Radius-Server. Informationen und Software zum Herunterladen finden Sie unter http://support.avaya.com.

RADIUS-Protokollauthentifizierungsinformationen wie Daten von Benutzerkonten und SSL VPN-Tunneldaten wie IP-Adresse und Netzmaske müssen in einer Datenbank gespeichert werden. Es gibt zwei mögliche Optionen:

- Verwenden Sie die lokale Datenbank der Identity Engine zur Speicherung der Benutzerdaten und Bereitstellung von Durchsuchungs-, Authentifizierungs- und Autorisierungsdiensten. Diese Option kann bei einer kleinen Anzahl von Benutzern verwendet werden. Bei der Identity Engine ist die Anzahl der Benutzer stark eingeschränkt. Den exakten Wert finden Sie in der Dokumentation.
- Verwenden Sie einen LDAP-Server für die Speicherung der Anmeldedaten und SSL VPN-Tunneldaten für Durchsuchungs- und Authentifizierungsdienste. Diese Option kann bei Bereitstellungsszenarien mit einer großen Anzahl von Benutzern eingesetzt werden.

Die Dokumentation zum Radius-Server für die Avaya Identity Engine enthält Konfigurationsoptionen für LDAP-Servers verschiedener Hersteller, die bei der Installation hilfreich

sind. Die RADIUS-Authentifizierung mittels LDAP-Server wird in der folgenden Abbildung veranschaulicht. Bitte beachten Sie, dass in dieser RADIUS-Serverkonfiguration bei diesem Verfahren kein LDAP-Server erforderlich ist.



Dieses Verfahren behandelt die manuellen Schritte für die Konfiguration der RADIUS-Authentifizierung. Alternativ können Sie die Authentifizierung auch mit dem AVG-Authentifizierungsassistenten konfigurieren.

Dieses Verfahren kommt in Anhang C: Konfiguration der RADIUS-Authentifizierung (mit Bildschirmfotos) auf Seite 106 mehrfach vor. Diese Version des Verfahrens beinhaltet Bildschirmfotos der Benutzeroberfläche.

Vorgehensweise

1. Melden Sie sich als Administrator bei der BBI des AVG an.
2. Fügen Sie auf der Seite **IP Pool Configuration** (IP-Pool-Konfiguration) einen neuen IP-Adressen-Pool für die RADIUS-Authentifizierung hinzu.
3. Stellen Sie auf der Seite **IP Pool** (IP-Pool) den in Schritt 2 erstellten IP-Adressen-Pool für die RADIUS-Authentifizierung als **Default IP Pool** (Standard-IP-Pool) ein.
4. Ändern Sie das VPN. Füllen Sie auf der Seite **Authentication Servers** > **Add New Authentication Server** (Authentifizierungsserver > Neuen Authentifizierungsserver hinzufügen) die Felder für den RADIUS-Server aus.
5. Konfigurieren Sie die Einstellungen des RADIUS-Authentifizierungsservers. Bitte beachten Sie, dass Hersteller-ID 1872 mit dem Hersteller Alteon verknüpft ist und das AVG bestimmt. Wählen Sie die Registerkarte **Einstellungen**, und füllen Sie die folgenden Felder aus.
   - **Vendor ID (Hersteller-ID): 1872**
   - **Vendor Type (Herstellertyp): 1**
   - **Zeitüberschreitung: 10**

- **Vendor Id for VPN Id (Hersteller-ID für VPN-ID): 1872**
- **Vendor Type for VPN Id (Herstellertyp für VPN-ID): 3**

6. Konfigurieren Sie die RADIUS-Netzwerkattribute. Füllen Sie auf der Registerkarte **Network Attributes** (Netzwerkattribute) die folgenden Felder aus.

Vendor ID Settings (Einstellungen Hersteller-ID)	Vendor Type Settings (Einstellungen Herstellertyp)
Client IP Address (IP-Adresse des Clients): 1872	Client IP Address (IP-Adresse des Clients): 4
Client Netmask (Netzmaske des Clients): 1872	Client Netmask (Netzmaske des Clients): 5
Primary NBNS Server (Primärer NBNS-Server): 1872	Primary NBNS Server (Primärer NBNS-Server): 6
Secondary NBNS Server (Sekundärer NBNS-Server): 1872	Secondary NBNS Server (Sekundärer NBNS-Server): 7
Primary DNS Server (Primärer DNS-Server): 1872	Primary DNS Server (Primärer DNS-Server): 8

7. Konfigurieren Sie die Filterattribute. Füllen Sie auf der Registerkarte „Filter Attributes“ (Filterattribute) die folgenden Felder aus>.
   - **Radius filter attribute (Radius-Filterattribut): Deaktiviert**
   - **Vendor Id for Filter Attribute (Hersteller-ID für Filterattribut): 9**
   - **Vendor Type for Filter Attribute (Herstellertyp für Filterattribut): 1**
8. Geben Sie die Adresse des Radius-Servers an. Wählen Sie die Registerkarte **Server** auf der Seite **RADIUS Servers** (RADIUS-Server).
9. Klicken Sie auf **Hinzufügen**, und geben Sie auf der Seite **Modify RADIUS Server** (RADIUS-Server ändern) die IP-Adresse des RADIUS-Servers und den gemeinsamen geheimen Schlüssel an.
10. Geben Sie auf der Registerkarte **Authentication Order** (Authentifizierungsreihenfolge) die gewünschte Reihenfolge für die Authentifizierungsmethoden an.

Verwandte Links

Konfiguration des Avaya VPN Gateway auf Seite 22

Konfiguration der Attribute auf dem RADIUS-Server

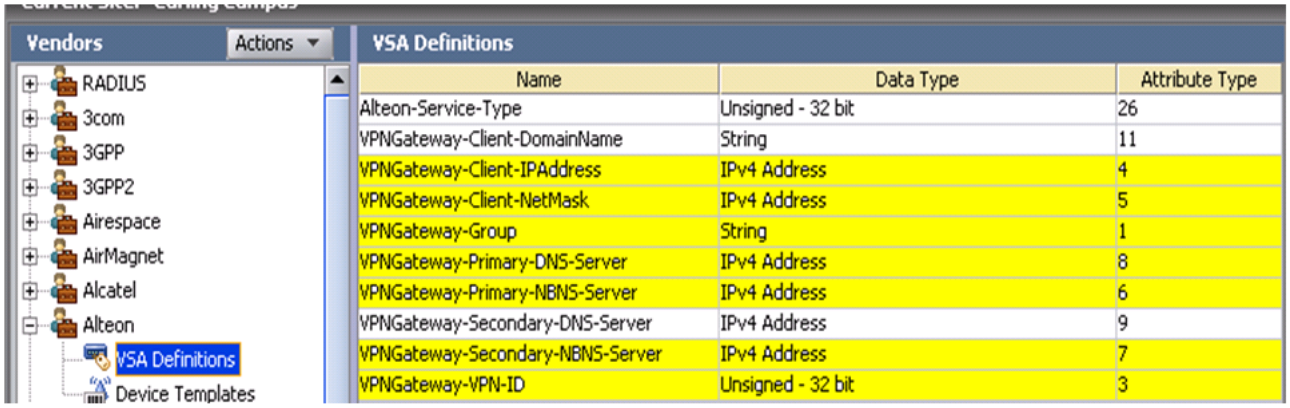
Für den SSL VPN-Dienst wird ein RADIUS-Server benötigt. Avaya empfiehlt die Nutzung von Avaya Identity Engines Ignition Server als RADIUS-Server.

Beim Aufbau einer Verbindung mit dem SSL VPN-Dienst authentifiziert Avaya VPN Gateway (AVG) das IP Office-System, indem die Anwendung eine Anfrage an einen externen RADIUS-Server sendet. In diesem Abschnitt werden die Attribute aufgeführt, die auf dem RADIUS-Server konfiguriert werden müssen.

Zuordnung der Attribute des RADIUS-Servers

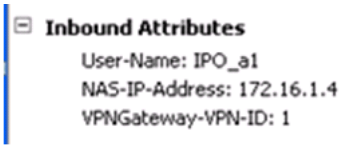
Die herstellerspezifischen Namen für Radius-Attribute sowie die zugehörigen Datentypen und Herstellertypencodes für den Hersteller Alteon (AVG) sind in der folgenden Liste enthalten.

Die folgenden Beispiele wurden mit einem Avaya Identity Engines RADIUS-Server erzielt. Die markierten Attribute wurden bei der Konfiguration des AVG RADIUS-Servers als **Network Attributes** (Netzwerkattribute) und **Einstellungen** konfiguriert.



Name	Data Type	Attribute Type
Alteon-Service-Type	Unsigned - 32 bit	26
VPNGateway-Client-DomainName	String	11
VPNGateway-Client-IPAddress	IPv4 Address	4
VPNGateway-Client-NetMask	IPv4 Address	5
VPNGateway-Group	String	1
VPNGateway-Primary-DNS-Server	IPv4 Address	8
VPNGateway-Primary-NBNS-Server	IPv4 Address	6
VPNGateway-Secondary-DNS-Server	IPv4 Address	9
VPNGateway-Secondary-NBNS-Server	IPv4 Address	7
VPNGateway-VPN-ID	Unsigned - 32 bit	3

• Im Folgenden werden die eingehenden Attribute aufgeführt, die während der Authentifizierungsanfrage vom AVG zum Radius-Server kommen.



Die vom AVG gesendeten Radius-Attribute sind:

- o Die NAS-IP-Adresse (allgemeines Radius-Attribut) ist die IP-Adresse des AVG.
- Der Benutzername (allgemeines Radius-Attribut) ist der Name des Benutzerkontos.
- Die VPNGateway-VPN-ID ist ein Alteon-Attribut.

Der IDEngine Radius-Server verfügt über eine standardmäßige interne Attributzuordnung für die am weitesten verbreiteten Radius-Attribute (siehe Tabelle unten). Die markierten Zeilen entsprechen den in der oben angeführten Radius-ANFRAGE enthaltenen Radius-Attributen.

Inbound Attributes

Name	Vendor	Attribute Mapping
Inbound-Digest-Auth-Param	RADIUS	Digest-Auth-Param
Inbound-Digest-Domain	RADIUS	Digest-Domain
Inbound-Digest-Method	RADIUS	Digest-Method
Inbound-Digest-Nonce-Count	RADIUS	Digest-Nonce-Count
Inbound-Digest-Opaque	RADIUS	Digest-Opaque
Inbound-Digest-Qop	RADIUS	Digest-Qop
Inbound-Digest-Realm	RADIUS	Digest-Realm
Inbound-Digest-SIP-AOR	RADIUS	Digest-SIP-AOR
Inbound-Digest-URI	RADIUS	Digest-URI
Inbound-Digest-Username	RADIUS	Digest-Username
Inbound-Framed-Compression	RADIUS	Framed-Compression
Inbound-Framed-Interface-Id	RADIUS	Framed-Interface-Id
Inbound-Framed-IP-Address	RADIUS	Framed-IP-Address
Inbound-Framed-IP-Netmask	RADIUS	Framed-IP-Netmask
Inbound-Framed-MTU	RADIUS	Framed-MTU
Inbound-Framed-Pool	RADIUS	Framed-Pool
Inbound-Framed-Protocol	RADIUS	Framed-Protocol
Inbound-Login-IP-Host	RADIUS	Login-IP-Host
Inbound-NAS-Identifier	RADIUS	NAS-Identifier
Inbound-NAS-IP-Address	RADIUS	NAS-IP-Address
Inbound-NAS-Port	RADIUS	NAS-Port
Inbound-NAS-Port-Id	RADIUS	NAS-Port-Id
Inbound-NAS-Port-Type	RADIUS	NAS-Port-Type
Inbound-Port-Limit	RADIUS	Port-Limit
Inbound-Service-Type	RADIUS	Service-Type
Inbound-Tunnel-Client-Auth-Id	RADIUS	Tunnel-Client-Auth-Id
Inbound-Tunnel-Client-Endpoint	RADIUS	Tunnel-Client-Endpoint
Inbound-Tunnel-Medium-Type	RADIUS	Tunnel-Medium-Type
Inbound-Tunnel-Preference	RADIUS	Tunnel-Preference
Inbound-Tunnel-Private-Group-Id	RADIUS	Tunnel-Private-Group-Id
Inbound-Tunnel-Server-Auth-Id	RADIUS	Tunnel-Server-Auth-Id
Inbound-Tunnel-Server-Endpoint	RADIUS	Tunnel-Server-Endpoint
Inbound-Tunnel-Type	RADIUS	Tunnel-Type
Inbound-User-Name	RADIUS	User-Name

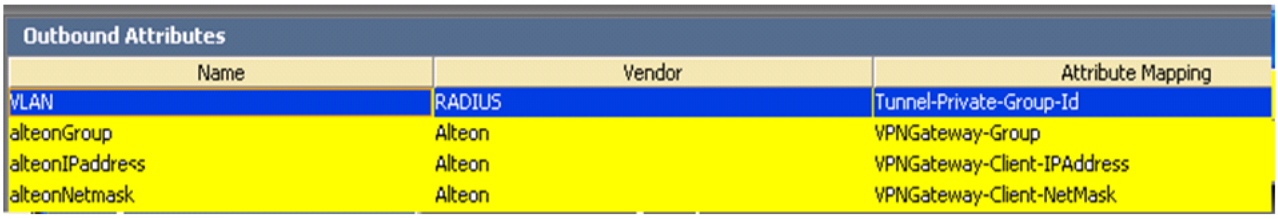
Radius-Server werten die eingehenden Attribute mithilfe von Autorisierungsregeln aus. Die Regel kann ein eingehendes Attribut zur Überprüfung eines Zustands verwenden oder das Attribut in einer Radius-ANTWORT als ausgehenden Wert zurücksenden. Wenn ein vom AVG gesendetes eingehendes Attribut eine Bewertung erfordert, aber nicht zum standardmäßigen Radius-Server-Set gehört, muss es als neues eingehendes Attribut auf dem Radius-Server definiert werden. Beispiele für Authentifizierungsregeln finden Sie unter *Administration der IDEngine*.

• Im Folgenden werden die ausgehenden Attribute aufgeführt, die während der Authentifizierungs-ANTWORT vom Radius-Server zum AVG gesendet werden.

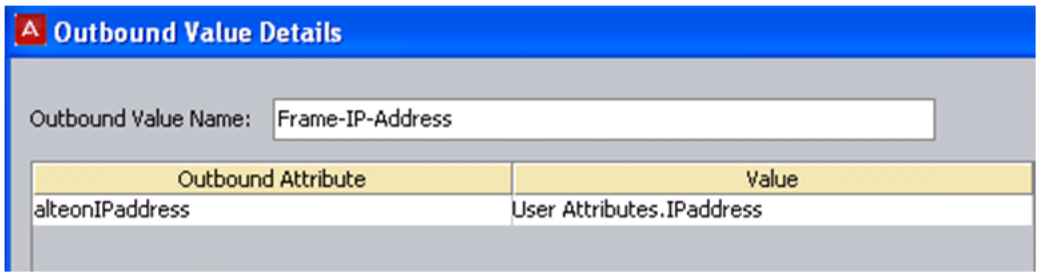
Outbound Attributes

alteonNetmask (VPNGateway-Client-NetMask): 255.255.0.0
alteonGroup (VPNGateway-Group): IPoffice
alteonIPaddress (VPNGateway-Client-IPAddress): 10.1.0.1

Ausgehende Attribute sind die Datenfelder, die der Radius-Server zum Transport der Bereitstellungdaten zum VPN-Gateway verwendet. Die ausgehenden Attribute sind allgemeine oder herstellertypische Radius-Protokollattribute. So wie die eingehenden Attribute müssen auch die ausgehenden Attribute erstellt werden, wenn Sie nicht zum Standardset des Radius-Servers gehören. Im oben angeführten Beispiel müssen die drei ausgehenden Alteon-Attribute (AVG-spezifisch) „alteonGroup“, „alteonIPaddress“ und „alteonNetmask“ auf dem Radius-Server erstellt werden, wie im unten angeführten Beispiel:



Die Werte der ausgehenden Attribute können als statische Werte eingestellt oder Benutzerattributen in der lokalen Datenbank des Radius-Servers oder in einem LDAP-Repository zugeordnet werden. Ein Beispiel für einen Wert eines ausgehenden Attributs, der einem Benutzerattribut in einer Datenbank zugeordnet wird, ist im Folgenden aufgeführt:



Ausgehende Werte sind mit Authentifizierungsregeln verknüpft und werden als Radius-Attribute an das VPN-Gateway gesendet, wenn die Regel ausgewertet wird. Wenn die Auswertung der Regel derart ausfällt, dass die ausgehenden Werte zugelassen werden, so werden diese zur Festlegung der Eigenschaften der Sitzung des Benutzers verwendet. Wenn die Auswertung der Regel derart ausfällt, dass die zurückgesendeten ausgehenden Werte nicht zugelassen werden, so werden diese normalerweise zur Übermittlung von Information über die Ursache der Ablehnung verwendet. Weitere Informationen finden Sie in der Dokumentation zur IDEngine.

Verwandte Links

[Konfiguration des Avaya VPN Gateway](#) auf Seite 22

Kapitel 5: Konfiguration eines SSL VPN für den Avaya-Support

Dieser Abschnitt enthält Informationen über den Konfigurationsvorgang für IP Office, wenn Avaya der Service-Provider ist. Sie können SSL VPN mithilfe des On-Boarding-Vorgangs automatisch konfigurieren.

Sie können mehrere Instanzen des SSL VPN-Dienstes konfigurieren und gleichzeitig ausführen.

Voraussetzungen

Bei der Konfiguration eines SSL VPN-Dienstes kann es sich bei der Adresse des VPN-Gateways um einen FQDN handeln. Sie müssen den DNS-Server konfigurieren, um FQDN-Adressen auflösen zu können. Konfigurieren Sie die DSN-Einstellungen im Formular **System** von IP Office Manager unter **DNS**.

Verwandte Links

[Konfiguration eines SSL VPN mithilfe einer On-Boarding-Datei](#) auf Seite 36
[Verwenden der On-Boarding-Datei zum Bearbeiten eines vorhandenen Dienstes](#) auf Seite 38

Konfiguration eines SSL VPN mithilfe einer On-Boarding-Datei

Die On-Boarding-XML-Datei wird von Avaya zur Verfügung gestellt. Sie enthält die Einstellungen, die zum Aufbau eines gesicherten Tunnels zwischen IP Office und einem AVG-Server benötigt werden. Beim Import der On-Boarding-XML-Datei werden die Einstellungen angewendet, und ein oder mehrere TLS-Zertifikate werden installiert.

Wenn Sie den SSL VPN-Dienst auf einem neuen System konfigurieren, müssen Sie als Erstes eine Bestandsdatei des IP Office-Systems generieren. Wenn Sie Ihr IP Office-System registrieren, wird die generierte Bestandsdatei in das GRT hochgeladen, und die Bestandsdaten werden in die Avaya Customer Support (ACS)-Datenbank geschrieben. Nach der Aktivierung des Remote-Supports können Sie die On-Boarding-XML-Datei von der GRT-Website herunterladen und in Ihr IP Office-System hochladen.

Der On-Boarding-Prozess konfiguriert:

- SSL VPN-Dienstkonfiguration

- Funktionscodes für die Aktivierung und Deaktivierung des SSL VPN-Diensts
- SNMP-Alarm-Traps
- ein oder mehrere TLS-Zertifikate im vertrauenswürdigen IP Office-Zertifikatspeicher

Führen Sie dieses Verfahren mit dem Avaya IP Office Web Manager-Client durch.

⚠ Warnung:

Beim On-Boarding wird automatisch ein SSL VPN-Dienst in der Systemkonfiguration erstellt, und zwar, sobald die On-Boarding-Datei in das System hochgeladen wird. Derartige Dienste dürfen ausschließlich auf Anweisung von Avaya gelöscht oder geändert werden.

Voraussetzungen

Vor dem Beginn müssen Ihnen die Hardware-Codes und die Katalogbeschreibung Ihres IP Office-Systems vorliegen. Beispiel: „IP OFFICE 500 VERSION 2 CONTROL UNIT TAA“ ist ein Hardware-Code und eine Katalogbeschreibung.

Vorgehensweise

1. Wählen Sie **Extras > On-Boarding**.

   Das Dialogfeld „On-Boarding“ wird angezeigt.

2. Wenn der Hardware-Code Ihres IP Office-Systems mit den Buchstaben TAA endet, müssen Sie das Kontrollkästchen neben der Frage **Verwenden Sie TAA-kompatible Hardware?** aktivieren.
3. Klicken Sie auf **Bestandsdatei abrufen**, um einen Bestand Ihres IP Office-Systems zu generieren.
4. Klicken Sie auf **IP Office registrieren**.

   Ein Browser wird geöffnet, und bringt Sie auf die GRT-Website.

5. Melden Sie sich an der Website an, und geben Sie die gewünschten Daten für das IP Office-System ein.
6. Wählen Sie für das IP Office-System die Option **Remote Support** (Remote-Support).
7. Klicken Sie auf **Download** (Herunterladen), und speichern Sie die On-Boarding-Datei.
8. Gehen Sie in das Verzeichnis, in das Sie die On-Boarding-Datei gespeichert haben, und klicken Sie auf **Hochladen**.

   Eine Nachricht bestätigt, dass die On-Boarding-Datei erfolgreich installiert wurde.

Verwandte Links

Konfiguration eines SSL VPN für den Avaya-Support auf Seite 36

Verwenden der On-Boarding-Datei zum Bearbeiten eines vorhandenen Dienstes

Sie können die On-Boarding-Datei verwenden, um den SSL VPN-Dienst zu konfigurieren. Die On-Boarding-Datei enthält die Einstellungen, die für den Aufbau eines gesicherten Tunnels zwischen IP Office und einem AVG-Server erforderlich sind. Nutzen Sie diese Vorgehensweise, wenn Sie den SSL VPN-Dienst bereits in einem IP Office-System konfiguriert haben und die SSL VPN-Konfiguration aktualisieren oder ändern müssen.

Führen Sie die Aktionen über die Avaya IP Office Web Manager-Oberfläche durch.

Voraussetzungen

Vor dem Beginn müssen Ihnen die Hardware-Codes und die Katalogbeschreibung Ihres IP Office-Systems vorliegen. Beispiel: „IP OFFICE 500 VERSION 2 CONTROL UNIT TAA“ ist ein Hardware-Code und eine Katalogbeschreibung.

Vorgehensweise

1. Wählen Sie **Extras > On-Boarding**.

   Das Dialogfeld „On-Boarding“ wird angezeigt.

2. Dieser Schritt ist optional. Gehen Sie wie folgt vor, um einen Bestand Ihres IP Office-Systems zu generieren:

   - Wenn der Hardware-Code Ihres IP Office-Systems mit den Buchstaben TAA endet, müssen Sie das Kontrollkästchen neben der Frage **Verwenden Sie TAA-kompatible Hardware?** aktivieren.
   - Klicken Sie auf **Bestandsdatei abrufen**.

3. Klicken Sie auf **Ändern**.

   Ein Browser wird geöffnet und bringt Sie auf die Avaya Website.

4. Melden Sie sich an der Website an.

   Die Seite „IP Office Remote Connectivity / Password Management“ (Remote-Verbindungen / Passwortverwaltung) wird angezeigt.

5. Klicken Sie auf **Existing IP Office SSL VPN Remote Connectivity** (Bestehende IP Office SSL VPN-Remote-Verbindungen).

6. Wählen Sie **Regenerate on-boarding file (existing properties)** [On-Boarding-Datei neu generieren (bestehende Eigenschaften)].

7. Geben Sie den Namen des SSL VPN-Dienstes und des SSL VPN-Kontos in die entsprechenden Felder ein.

8. Klicken Sie auf **Submit** (Senden).

9. Wählen Sie aus, ob Sie die aktualisierte On-Boarding-Datei per E-Mail erhalten oder herunterladen möchten, und befolgen Sie die Anweisungen auf dem Bildschirm.

10. Sobald Sie die On-Boarding-Datei empfangen oder heruntergeladen haben, speichern Sie sie in Ihrem lokalen System.
11. Wechseln Sie in das Verzeichnis, in das Sie die On-Boarding-Datei gespeichert haben, und klicken Sie in der Web Manager-Oberfläche auf die Option **Hochladen**.

    Eine Nachricht bestätigt, dass die On-Boarding-Datei erfolgreich installiert wurde.

Verwandte Links

Konfiguration eines SSL VPN für den Avaya-Support auf Seite 36

Kapitel 6: Konfiguration eines SSL VPN für die Unterstützung durch Avaya-Partner

Drittanbieter können ihr eigenes Avaya VPN Gateway für die Durchführung von Remote-Kundendienst über die IP Office-SSL-VPN-Technologie nutzen.

Für die Unterstützung von Drittanbietern muss SSL VPN manuell in der Anwendung Manager konfiguriert werden. Sie können ein Standardmodus- oder Server Edition-System konfigurieren. Die manuelle Konfiguration wird im Basic Edition-Modus nicht unterstützt.

Sie können mehrere Instanzen des SSL VPN-Dienstes konfigurieren und gleichzeitig ausführen.

Voraussetzungen

Bei der Konfiguration eines SSL VPN-Dienstes kann es sich bei der Adresse des VPN-Gateways um einen FQDN handeln. Sie müssen den DNS-Server konfigurieren, um FQDN-Adressen auflösen zu können. Konfigurieren Sie die DNS-Einstellungen im Formular **System** von IP Office Manager unter **DNS**.

Konfiguration eines SSL VPN für Unterstützungsvorgänge durch Avaya-Partner

Die folgende Liste zeigt den Ablauf der Vorgänge für die Konfiguration eines SSL VPN für die Unterstützung von Partnern.

- Konfigurieren des SSL-VPN-Dienstes auf Seite 41
- Installation eines Zertifikats auf Seite 43
- Konfigurieren von Funktionscodes auf Seite 44
- Konfigurieren der Alarmbenachrichtigungen auf Seite 48
- Konfiguration statischer Routen auf Seite 52
- Überprüfen der Verbindung mit auf Seite 64
- Versand von Probealarmen auf Seite 66

Verwandte Links

Konfigurieren des SSL VPN-Dienstes auf Seite 41
Installation eines Zertifikats auf Seite 43
Konfiguration der Funktionscodes auf Seite 44
Konfiguration der Alarmbenachrichtigungen auf Seite 48
Konfiguration statischer Routen auf Seite 52

Konfigurieren des SSL VPN-Dienstes

Gehen Sie wie folgt vor, um den SSL VPN-Dienst zu konfigurieren.

Führen Sie diese Aktionen in der Manager-Oberfläche durch. Nutzen Sie zum Konfigurieren eines Server Edition-Systems den IP Office Manager for Server Edition-Modus.

Voraussetzungen

Sie müssen die Werte der folgenden Konfigurationsvariablen kennen.

Tabelle 1: Registerkarte "Dienst"

Variable	Beschreibung
Name des Dienstes	Geben Sie einen Namen für den neuen SSL VPN-Dienst ein.
Kontoname	Geben Sie den Namen des SSL VPN-Dienstkontos ein. Dieser Kontoname wird verwendet, um den SSL VPN-Dienst beim Aufbau einer Verbindung mit AVG zu authentifizieren. **Server Edition-Systeme:** Für die Konfiguration eines Server Edition-Systems empfiehlt Ihnen Avaya, dass Sie denselben Namen für das SSL VPN-Dienstkonto und die SNMP-Agenten-Geräte-ID festlegen. Wenn diese Einstellungen übereinstimmen, kann der technische Support mithilfe dieser Daten die Adresse des SSL VPN-Tunnels identifizieren. Pro System kann nur eine SNMP-Agenten-Geräte-ID konfiguriert werden. Wenn Sie mehrere Instanzen des SSL VPN-Dienstes konfigurieren, können Sie abhängig von Ihrem Bedarf an externem technischen Support einen der SSL VPN-Dienstnamen wählen, um eine Übereinstimmung mit der SNMP-Agenten-Geräte-ID zu erreichen. Sie können sich die Geräte-ID auch ansehen, indem Sie in der Navigationsliste **Netzwerk** wählen und ein Server Edition-System auswählen. Auf dem Bildschirm wird eine Zusammenfassung der Einstellungen des ausgewählten Systems angezeigt.
Kontokennwort	Geben Sie das Kennwort des SSL VPN-Dienstkontos ein.
Kennwort bestätigen	Bestätigen Sie das Kennwort für das SSL VPN-Dienstkonto.
Server-Adresse	Geben Sie die Adresse des VPN-Gateways ein. Bei der Adresse kann es sich um eine FQDN- oder eine IPv4-Adresse handeln.
Servertyp	Wählen Sie AVG aus.
Server-Portnummer	Wählen Sie eine Portnummer aus. Die standardmäßige Portnummer lautet 443.

Tabelle 2: Registerkarte "Sitzung"

Variable	Beschreibung
Bevorzugtes Datenübertragungsprotokoll	Wählen Sie TCP. Hierbei handelt es sich um das Protokoll, das der SSL VPN-Dienst für den Datentransport verwendet. Wenn Sie bei der Konfiguration der Verbindung UDP als Protokoll verwenden, wird in dem Feld UDP angezeigt; der SSL VPN-Dienst verwendet jedoch TCP.
Heartbeat-Intervall	Geben Sie die Länge des Intervalls zwischen Heartbeat-Nachrichten in Sekunden an. Der Standardwert beträgt 30 Sekunden.
Heartbeat-Wiederholungen	Geben Sie die Anzahl unbestätigter Heartbeat-Nachrichten an, die IP Office an AVG sendet, bevor bestimmt wird, dass AVG nicht reagiert. Wenn diese Anzahl aufeinanderfolgender Heartbeart-Nachrichten erreicht ist und AVG sie nicht bestätigt hat, beendet IP Office die Verbindung. Der Standardwert ist 4.
Neuverbindungs-Intervall bei Fehler	Der Zeitraum, der gewartet werden soll, bevor der SSL VPN-Dienst versucht, die Verbindung mit AVG wieder aufzubauen. Der Zeitraum beginnt in dem Moment, in dem der SSL VPN-Tunnel in Betrieb ist und vergebens versucht, eine Verbindung mit AVG aufzubauen oder in dem Moment, in dem die Verbindung mit AVG verloren geht. Der Standardwert beträgt 60 Sekunden.

Vorgehensweise

1. Klicken Sie in der Navigationsliste mit der rechten Maustaste auf **Dienst**.
2. Wählen Sie **NeuSSL VPN-Dienst**.
3. Konfigurieren Sie auf der Registerkarte **Dienst** die in der Tabelle unten aufgeführten Einstellungen.
4. Wählen Sie die Registerkarte **Sitzung**, und konfigurieren Sie die in der Tabelle unten aufgeführten Einstellungen.
5. Wählen Sie die Registerkarte **Ausweichbetrieb**, und wählen Sie eine der folgenden Optionen:
   - zum Aktivieren und Aufbauen einer SSL VPN-Verbindung müssen Sie die Option **Im Ausweichbetrieb** deaktivieren
   - zum Konfigurieren des Dienstes ohne den Aufbau einer SSL VPN-Verbindung müssen Sie die Option **Im Ausweichbetrieb** aktivieren
6. Klicken Sie auf **OK**.
7. Klicken Sie auf das Symbol **Speichern**, um die Konfiguration zu speichern.

Verwandte Links

Konfiguration eines SSL VPN für die Unterstützung durch Avaya-Partner auf Seite 40

Installation eines Zertifikats

Der SSL VPN-Dienst arbeitet mit digitalen Zertifikaten, um die Identität der Geräte an beiden Enden des SSL VPN-Tunnels zu überprüfen. Diese Vorgehensweise beschreibt, wie man ein Zertifikat im Speicher vertrauenswürdiger IP Office-Zertifikate installiert.

Manager enthält eine Menüoption, mit der Sie die Standardsicherheitseinstellungen in IP Office wiederherstellen können. Wenn Sie die Standardsicherheitseinstellungen wiederherstellen und der SSL-VPN-Dienst sich nicht innerhalb einiger Minuten neu verbindet, müssen Sie das Zertifikat erneut dem Speicher vertrauenswürdiger Zertifikate hinzufügen.

Ähnlich verhält es sich mit der Security Manager-Anwendung, die es Ihnen ermöglicht, das Zertifikat aus dem Speicher vertrauenswürdiger Zertifikate zu löschen. Wenn Sie das Zertifikat mit Security Manager löschen und der SSL VPN-Dienst bereits mit dem AVG verbunden war, trennt der SSL VPN-Dienst die Verbindung, sobald der Tunnel den geheimen Schlüssel beim nächsten Mal neu verhandelt. Diese Neuaushandlung erfolgt standardmäßig alle 8 Stunden und kann je nachdem, welche Einstellungen in AVG festgelegt wurden, auch in einem anderen Intervall erfolgen. Wenn der SSL VPN-Dienst die Verbindung während einer Neuaushandlung beendet, oder wenn Sie den Dienst deaktivieren, bevor die nächste Neuaushandlung erfolgt, können Sie den SSL VPN-Dienst erst wieder aktivieren, nachdem Sie das erforderliche Zertifikat im Speicher vertrauenswürdiger Zertifikate installiert haben.

Voraussetzungen

Sie müssen einen der folgenden Zertifikatstypen installieren:

- das selbstsignierte AVG-Zertifikat des VPN-Portals, mit dem sich der IP Office-SSL-VPN-Dienst verbindet
- Das Zertifikat der CA, die das AVG-Zertifikat signiert hat

Vorgehensweise

1. Wählen Sie **Datei > Erweitert > Sicherheitseinstellungen**.

   Die IP Office-Systeme werden in einem Dialogfeld aufgelistet.

2. Klicken Sie auf das entsprechende Kontrollkästchen, um das IP Office-System auszuwählen, in dem Sie das Zertifikat installieren möchten.

3. Klicken Sie auf **OK**.

   Ein Dialogfeld wird angezeigt.

4. Geben Sie in das Feld **Benutzername für den Dienst** den Namen des IP Office-Administrators ein.

5. Geben Sie in das Feld **Benutzerkennwort für den Dienst** das Kennwort des IP Office-Administrators ein.

6. Klicken Sie auf **OK**.

   Die Anmeldedaten werden akzeptiert.

7. Wählen Sie im Navigationsbereich **Sicherheit > System**, und wählen Sie den Namen der Konfiguration aus.

8. Klicken Sie auf der Registerkarte **Zertifikat** auf die Option **Hinzufügen**.

   Ein Dialogfeld wird angezeigt, das Sie zur Auswahl der Quelle des Zertifikats auffordert.

9. Wählen Sie **Aus Zwischenablage einfügen**, und klicken Sie auf **OK**.

   Ein Dialogfeld wird angezeigt, in das Sie den Text des Zertifikats eingeben können.

10. Kopieren Sie das Zertifikat, und fügen Sie den Text in das offene Fenster ein. Sie müssen auch die Zeilen `-----BEGIN CERTIFICATE-----` und `-----END CERTIFICATE-----` einfügen.

11. Klicken Sie auf **OK**.

    Der Name des Zertifikats wird in der Liste der installierten Zertifikate aufgeführt.

Verwandte Links

Konfiguration eines SSL VPN für die Unterstützung durch Avaya-Partner auf Seite 40

Konfiguration der Funktionscodes

Sie können im IP Office-System Funktionscodes konfigurieren. Diese Funktionscodes lösen eine bestimmte Aktion aus, wenn Sie sie auf einem Tischtelefon wählen, das mit dem IP Office-System verbunden ist. Informationen zur Programmierung von Telefontasten mit Funktionscodes befinden sich in der Dokumentation zu IP Office Manager.

Sie können Funktionscode konfigurieren und verwenden, um den SSL VPN-Dienst zu aktivieren und zu deaktivieren. Wenn Sie die Funktionscodes zum Aktivieren oder Deaktivieren des SSL VPN-Dienstes verwenden, wird der Dienst weiterhin im System bereitgestellt. Die Funktionscodes versetzen den Tunnel in den Status „Betriebsbereit“ oder in einen Ausweichbetriebsstatus.

Im IP Office-System ist eine Reihe von Funktionen vordefiniert, auf die Sie über Funktionscodes zugreifen können. Mithilfe der folgenden vordefinierten Funktionen können Sie Funktionscodes erstellen, mit denen der SSL VPN-Dienst aktiviert oder deaktiviert werden kann:

- Sammelanschluss-Nachtschaltung aus: aktiviert den SSL VPN-Dienst
- Sammelanschluss-Nachtschaltung ein: deaktiviert den SSL VPN-Dienst

Diese Funktionscodes sind intern verfügbar. Sie müssen sie auf einem Telefon wählen, das mit dem IP Office-System verbunden ist. Wenn Sie die Funktionscodes auf einem externen Telefon verwenden möchten, können Sie eine automatische Weitervermittlung konfigurieren. Mithilfe der automatischen Weitervermittlung können Sie sich über eine externe Telefonnummer im IP Office-System einwählen und die Funktionscodes über ein Menüsystem aktivieren.

Verwandte Links

Konfiguration eines SSL VPN für die Unterstützung durch Avaya-Partner auf Seite 40
Konfiguration eines Funktionscodes zur Aktivierung des SSL VPN-Dienstes auf Seite 45
Konfiguration eines Funktionscodes für die Deaktivierung des SSL VPN-Dienstes auf Seite 45
Konfiguration einer automatischen Weitervermittlung auf Seite 46

Konfiguration eines Funktionscodes zur Aktivierung des SSL VPN-Dienstes

Gehen Sie folgendermaßen vor, um einen Funktionscode zu konfigurieren, der den SSL VPN-Dienst aktiviert, wenn er auf einem Tischtelefon gewählt wird, das an das IP Office-System angebunden ist.

Vorgehensweise

1. Wählen Sie in der Navigationsliste **Funktionscode**.

   Die Liste der Standardfunktionscodes wird angezeigt.

2. Klicken Sie mit der rechten Maustaste, und wählen Sie **Neu**.

   Die Registerkarte „Funktionscode“ wird angezeigt.

3. Geben Sie in das Feld **Code *775*x*1** ein. *x* steht hier für eine Instanz des SSL VPN-Dienstes und kann zwischen 1 und 9 liegen. Wenn Sie beispielsweise zwei Instanzen des SSL VPN-Dienstes konfiguriert haben und Funktionscodes für die erste Instanz konfigurieren, müssen Sie ***77511** eingeben.

   Hinweis:

   Sie können dem Funktionscode verschiedene Nummern zuweisen. Für eine einfachere Nutzung empfiehlt Avaya die Verwendung von *775. Dies entspricht *SSL auf einem Tastenfeld.

4. Wählen Sie in der Liste **Funktion** die Option **Sammelanschluss-Nachtschaltung aus**.

5. Geben Sie in das Feld **Telefonnummer** den Namen des SSL VPN-Dienstes in Anführungszeichen an. Beispiel: Wenn der Name des Dienstes Dienst1 ist, geben Sie `„Dienst1“` ein.

   Verwenden Sie den Namen des SSL VPN-Dienstes, den Sie eingegeben haben, als Sie den SSL VPN-Dienst erstellt haben. Informationen zu dieser Einstellung finden Sie unter Konfigurieren des SSL VPN-Dienstes auf Seite 41.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf das Symbol **Speichern**, um die Konfigurationsänderungen zu speichern.

Verwandte Links

Konfiguration der Funktionscodes auf Seite 44

Konfiguration eines Funktionscodes für die Deaktivierung des SSL VPN-Dienstes

Gehen Sie folgendermaßen vor, um einen Funktionscode zu konfigurieren, der den SSL VPN-Dienst deaktiviert, wenn er auf einem Tischtelefon gewählt wird, das an das IP Office-System angebunden ist.

Vorgehensweise

1. Wählen Sie in der Navigationsliste **Funktionscode**.

   Die Liste der Standardfunktionscodes wird angezeigt.

2. Klicken Sie mit der rechten Maustaste, und wählen Sie **Neu**.

   Die Registerkarte „Funktionscode“ wird angezeigt.

3. Geben Sie in das Feld **Code *775*x*0** ein. *x* steht hier für eine Instanz des SSL VPN-Dienstes und kann zwischen 1 und 9 liegen. Wenn Sie beispielsweise zwei Instanzen des SSL VPN-Dienstes konfiguriert haben und Funktionscodes für die erste Instanz konfigurieren, müssen Sie ***77510** eingeben.

   Hinweis:

   Sie können dem Funktionscode verschiedene Nummern zuweisen. Für eine einfachere Nutzung empfiehlt Avaya die Verwendung von *775. Dies entspricht *SSL auf einem Tastenfeld.

4. Wählen Sie in der Liste **Funktion** die Option **Sammelanschluss-Nachtschaltung ein**.

5. Geben Sie in das Feld **Telefonnummer** den Namen des SSL VPN-Dienstes in Anführungszeichen an. Beispiel: Wenn der Name des Dienstes Dienst1 ist, geben Sie „`Dienst1`“ ein.

   Verwenden Sie den Namen des SSL VPN-Dienstes, den Sie eingegeben haben, als Sie den SSL VPN-Dienst erstellt haben. Informationen zu dieser Einstellung finden Sie unter Konfigurieren des SSL VPN-Dienstes auf Seite 41.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf das Symbol **Speichern**, um die Konfigurationsänderungen zu speichern.

Verwandte Links

Konfiguration der Funktionscodes auf Seite 44

Konfiguration einer automatischen Weitervermittlung

Gehen Sie folgendermaßen vor, um eine automatische Weitervermittlung zu konfigurieren. Dank der automatischen Weitervermittlung können Sie über interne und externe Telefonnummern auf das IP Office-System zugreifen und ein Menüsystem verwenden, um den SSL VPN-Dienst zu aktivieren oder zu deaktivieren.

Voraussetzungen

Sie müssen Funktionscodes konfigurieren. Siehe Konfigurieren von Funktionscodes auf Seite 44

Wenn Sie Avaya Voicemail Pro verwenden, muss ein Modul für die unterstützte Vermittlung konfiguriert sein, bevor Sie diese Aktionen durchführen können. Weitere Informationen finden Sie unter *Verwaltung von Voicemail Pro* (15–601063).

Informationen zu diesem Vorgang

Im Rahmen dieser Vorgehensweise erstellen Sie eine automatische Weitervermittlung und ordnen eingehende Anrufe dann dieser automatischen Weitervermittlung zu. In diesem Beispiel wird 0 verwendet, um den SSL VPN-Dienst zu aktivieren, und 1, um ihn zu deaktivieren. Sie können die Funktionen aber jeder beliebigen Taste auf dem Tastenfeld zuweisen.

Vorgehensweise

1. Wählen Sie eine der folgenden Optionen:
   - Wenn Sie Embedded Voicemail verwenden, wählen Sie in der Navigationsliste **Automatische Weitervermittlung**.
   - Wenn Sie Voicemail Pro verwenden, beginnen Sie diese Vorgehensweise mit Schritt 12 auf Seite 47.
2. Klicken Sie mit der rechten Maustaste, und wählen Sie **Neu**.
3. Geben Sie in das Feld **Name** den Namen der automatischen Weitervermittlung ein.
4. Wählen Sie die Registerkarte **Aktionen**.
5. Wählen Sie den Eintrag für den Schlüssel **0**, und klicken Sie auf die Schaltfläche **Bearbeiten**.
6. Wählen Sie in der Liste **Aktionen** eine der folgenden Optionen:
   - Wählen Sie die Vermittlung **Normale Vermittlung**.
   - Wählen Sie **Vermittlung**.
7. Geben Sie in der Liste **Zielrufnummer** den Funktionscode ein, den Sie konfiguriert haben, um den Dienst zu aktivieren, und klicken Sie auf **OK**.
8. Wählen Sie den Eintrag für den Schlüssel **1**, und klicken Sie auf die Schaltfläche **Bearbeiten**.
9. Wählen Sie in der Liste **Aktionen** eine der folgenden Optionen:
   - Wählen Sie die Vermittlung **Normale Vermittlung**.
   - Wählen Sie **Vermittlung**.
10. Geben Sie in der Liste **Zielrufnummer** den Funktionscode ein, den Sie konfiguriert haben, um den Dienst zu deaktivieren, und klicken Sie auf **OK**.
11. Klicken Sie auf das Symbol **Speichern**, um die Konfigurationsänderungen zu speichern.
12. Wählen Sie in der Navigationsliste **Weiterleitung eingehender Anrufe**.
13. Setzen Sie auf der Registerkarte **Standard** das Feld **Trägerpotential** auf **Alle Sprachanrufe**.
14. Wählen Sie in der Liste **Leitungsgruppennummer** die Zeile aus, die Sie zum Aktivieren und Deaktivieren des SSL VPN-Dienstes verwenden möchten.
15. Wählen Sie die Registerkarte **Ziel**.

16. Wählen Sie eine der folgenden Optionen aus:
    - Wenn Sie Embedded Voicemail verwenden, wählen Sie in der Liste **Ziel** die von Ihnen konfigurierte automatische Weitervermittlung aus.
    - Wenn Sie Voicemail Pro verwenden, geben Sie in die Liste Ziel den Wert `VM:<Name>` in die Liste **Ziel** ein. *<Name>* steht für den Namen des Voicemail Pro-Moduls.
17. Klicken Sie auf **OK**.
18. Klicken Sie auf das Symbol **Speichern**, um die Konfigurationsänderungen zu speichern.

Weitere Schritte

Sie können für die automatische Weitervermittlung Eingabeaufforderungen aufzeichnen. Informationen über die Aufzeichnung von Eingabeaufforderungen finden Sie in der Dokumentation Ihres Voicemail-Systems. Wenn Sie Embedded Voicemail verwenden, lesen Sie den *Installation von Embedded Voicemail*. Wenn Sie Voicemail Pro verwenden, lesen Sie *Verwaltung von Voicemail Pro*.

Verwandte Links

Konfiguration der Funktionscodes auf Seite 44

Konfiguration der Alarmbenachrichtigungen

Für den SSL VPN-Dienst kann eine Fehlerverwaltung konfiguriert werden. Beim Konfigurieren der Fehlerverwaltung können Sie Filter festlegen, um die Arten von Ereignissen zu definieren, über die Sie benachrichtigt werden möchten. Sie können beispielsweise Benachrichtigungen über Fehler erhalten, die sich auf den SSL VPN-Dienst beziehen oder die etwas mit dem IP Office-System zu tun haben.

Bei der Konfiguration der Fehlerverwaltung müssen Sie Alarmziele festlegen, an die die Systemfehler berichtet werden. Sie können für die Alarmberichte die folgenden Ziele konfigurieren:

- Ein lokales LAN oder ein Remote-Server für SNMP-Traps
- Ein SMTP-Server in einem lokalen LAN oder ein Remote-SMTP-Server für E-Mail-Benachrichtigungen
- Ein lokales LAN oder ein Remote-Server für Syslog-Einträge

Die konfigurierbaren Alarmziele hängen vom verwendeten Betriebsmodus ab. In der folgenden Tabelle finden Sie die Alarmziele, die in den einzelnen Modi unterstützt werden.

Alarmziel	Betriebsmodus			
	Essential Edition	IP Office Server Edition	Erweiterungssystem Server Edition	Basic Edition
SNMP-Traps				

Table continues…

Alarmziel	Betriebsmodus			
	Essential Edition	IP Office Server Edition	Erweiterungssystem Server Edition	Basic Edition
SNMP in einem lokalen LAN	✔	✔	✔	✔
SNMP über einen SSL VPN-Dienst	✔	✔	✔	✔
E-Mail-Benachrichtigungen				
SMTP-Server in einem lokalen LAN	✔	✔	✔	—
SMTP-Server über einen SSL VPN-Tunnel	✔	✔	✔	—
Syslog-Einträge				
Syslog-Server in einem lokalen LAN	✔	✔	✔	—
Syslog-Server über einen SSL VPN-Tunnel	✔	✔	✔	—

Verwandte Links

Konfiguration eines SSL VPN für die Unterstützung durch Avaya-Partner auf Seite 40
Konfiguration von SNMP-Trap-Zielen auf Seite 49
Konfiguration von E-Mail-Alarmbenachrichtigungen auf Seite 50
Konfiguration von Syslog-Einträgen auf Seite 51

Konfiguration von SNMP-Trap-Zielen

Gehen Sie wie folgt vor, um Systemfehler als SNMP-Traps zu berichten. Sie können Filter festlegen, um die Arten von Ereignissen zu bestimmen, die SNMP-Traps generieren. Sie können beispielsweise SNMP-Traps für SSL VPN-Dienst-bezogene Fehler oder SNMP-Traps für IP Office-System-bezogene Fehler generieren.

Voraussetzungen

Wenn Sie für ein Fehlerereignis eine Ziel-IP-Adresse definieren, verwendet das System eine IP-Routing-Tabelle, um zu ermitteln, welche Schnittstelle beim Senden des Fehlerereignisses verwendet werden sollte. Das Ziel muss eine IPv4-Adresse sein, damit der SNMP-Trap korrekt an den Fehlerverwaltungsserver weitergeleitet werden kann.

Auf dem Zielcomputer, auf dem die SNMP-Traps berichtet werden, muss ein Trap-Listener konfiguriert sein.

Vorgehensweise

1. Klicken Sie in der Navigationsliste auf **System**, und wählen Sie die Registerkarte **Systemereignisse**.

In Manager werden die Registerkarten **Konfiguration** und **Alarme** angezeigt.

2. Wählen Sie auf der Registerkarte **Konfiguration** die Option **SNMP aktiviert**.
3. Geben Sie in das Feld **Community** den Wert `Öffentlich` ein.
4. Klicken Sie auf der Registerkarte **Alarme** auf **Hinzufügen**.
5. Wählen Sie **Trap**, und geben Sie in das Feld **IP-Adresse** eine Zieladresse für den SNMP-Trap ein. .
6. Geben Sie eine Portnummer ein, oder verwenden Sie die Standardportnummer (162).
7. Geben Sie in das Feld **Community** den Wert `Öffentlich` ein.
8. Wählen Sie in der Liste **Ereignisse** den Ereignisfilter aus:
   - Wählen Sie **Dienst**, um SNMP-Traps für Fehler bezüglich des SSL VPN-Dienstes zu generieren.
   - Wählen Sie beliebige Ereignisse bezüglich des Betriebs des IP Office-Systems aus, für das Sie SNMP-Traps generieren möchten. Informationen über diese Optionen finden Sie unter *IP Office Manager*.
9. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.
10. Klicken Sie auf der Registerkarte Alarme auf **OK**.
11. Klicken Sie auf das Symbol **Speichern**, um die Konfigurationsänderungen zu speichern.

Verwandte Links

Konfiguration der Alarmbenachrichtigungen auf Seite 48

Konfiguration von E-Mail-Alarmbenachrichtigungen

Gehen Sie wie folgt vor, um beim Auftreten von Fehlern E-Mail-Benachrichtigungen zu erhalten. Sie können Filter festlegen, um die Arten von Ereignissen zu definieren, über die Sie benachrichtigt werden möchten. Sie können beispielsweise Benachrichtigungen über Fehler erhalten, die sich auf den SSL VPN-Dienst beziehen oder die etwas mit dem IP Office-System zu tun haben.

Voraussetzungen

Auf dem Computer, den Sie für die Fehlerverwaltung verwenden, muss ein SMTP-E-Mail-Server konfiguriert sein. Des Weiteren muss auf dem Computer, auf dem Sie die E-Mail-Benachrichtigungen erhalten möchten, ein E-Mail-Client konfiguriert sein.

Wenn Sie für ein Fehlerereignis eine Ziel-Adresse definieren, nutzt das System eine IP-Routing-Tabelle, um zu ermitteln, welche Schnittstelle beim Senden des Fehlerereignisses verwendet werden sollte. Das Ziel muss eine IPv4-Adresse sein, damit die Benachrichtigung korrekt an den Fehlerverwaltungsserver weitergeleitet werden kann.

Vorgehensweise

1. Klicken Sie in der Navigationsliste auf **System**, und wählen Sie die Registerkarte **Systemereignisse**.

   Manager zeigt die Registerkarten **Konfiguration** und **Alarme** an.

2. Klicken Sie auf der Registerkarte **Alarme** auf **Hinzufügen**.
3. Wählen Sie die Option **E-Mail**, und geben Sie die Adresse, auf der Sie die E-Mail-Benachrichtigungen erhalten möchten, im Feld **E-Mail** ein.
4. Wählen Sie in der Liste **Ereignisse** den Ereignisfilter aus:
   - Wählen Sie **Dienst**, um Benachrichtigungen über Fehler bezüglich des SSL VPN-Dienstes zu erhalten.
   - Wählen Sie alle Ereignisse bezüglich des Betriebs des IP Office-Systems aus, über die Sie Benachrichtigungen erhalten möchten. Informationen über diese Optionen finden Sie unter *IP Office Manager*.
5. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.
6. Klicken Sie auf der Registerkarte Alarme auf **OK**.
7. Wählen Sie die Registerkarte **SMTP**.
8. Geben Sie in das Feld **IP-Adresse** die IP-Adresse des SMTP-Servers ein.
9. Geben Sie in das Feld **Port** die Nummer des SMTP-Servers ein.
10. Geben Sie in das Feld **E-Mail-Adresse des Absenders** die E-Mail-Adresse ein, die das IP Office-System verwenden wird, um E-Mail-Benachrichtigungen zu senden.
11. Wählen Sie **Server erfordert Authentifizierung**.
12. Geben Sie in die Felder **Benutzername** und **Kennwort** die für die Anmeldung am SMTP-Server benötigten Anmeldedaten ein.
13. Klicken Sie auf **OK**.
14. Klicken Sie auf das Symbol **Speichern**, um die Konfigurationsänderungen zu speichern.

Verwandte Links

Konfiguration der Alarmbenachrichtigungen auf Seite 48

Konfiguration von Syslog-Einträgen

Gehen Sie wie folgt vor, um Systemfehler als Syslog-Einträge zu berichten. Sie können Filter festlegen, um die Arten von Ereignissen zu bestimmen, die berichtet werden. Sie können beispielsweise Fehler berichten, die sich auf den SSL VPN-Dienst beziehen oder die sich auf das IP Office-System beziehen.

Voraussetzungen

Auf dem Server, auf dem die Systemfehler berichtet werden sollen, muss ein Syslog-Client konfiguriert sein.

Wenn Sie für ein Fehlerereignis eine Ziel-IP-Adresse definieren, verwendet das System eine IP-Routing-Tabelle, um zu ermitteln, welche Schnittstelle beim Senden des Fehlerereignisses verwendet werden sollte. Das Ziel muss eine IPv4-Adresse sein, damit die Benachrichtigung korrekt an den Fehlerverwaltungsserver weitergeleitet werden kann.

Vorgehensweise

1. Klicken Sie in der Navigationsliste auf **System**, und wählen Sie die Registerkarte **Systemereignisse**.

   In Manager werden die Registerkarten **Konfiguration** und **Alarme** angezeigt.
2. Klicken Sie auf der Registerkarte **Alarme** auf **Hinzufügen**.
3. Wählen Sie die Option **Syslog**, und geben Sie die IP-Adresse des Servers, auf dem der Syslog-Client konfiguriert ist, in das Feld **IP-Adresse** ein.
4. Geben Sie die Portnummer des Servers, auf dem der Syslog-Client konfiguriert ist, in das Feld **Port** ein.
5. Wählen Sie in der Liste **Ereignisse** den Ereignisfilter aus:
   - Wählen Sie **Dienst**, um Fehler bezüglich des SSL VPN-Dienstes zu berichten.
   - Wählen Sie alle Ereignisse bezüglich des Betriebs des IP Office-Systems aus, über die Sie Benachrichtigungen erhalten möchten. Informationen über diese Optionen finden Sie unter *IP Office Manager*.
6. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.
7. Klicken Sie auf der Registerkarte **Alarme** auf **OK**.
8. Klicken Sie auf das Symbol **Speichern**, um die Konfigurationsänderungen zu speichern.

Verwandte Links

Konfiguration der Alarmbenachrichtigungen auf Seite 48

Konfiguration statischer Routen

Wenn Sie Split-Tunneling-Routen in AVG konfigurieren, lernt das IP Office-System die Routing-Informationen für den Tunnel automatisch, wenn der SSL VPN-Dienst eine Verbindung mit AVG aufbaut. Sie können aber auch eine statische Route konfigurieren. In diesem Abschnitt finden Sie Informationen, die Sie dabei unterstützen, zu ermitteln, ob Sie eine statische Route konfigurieren sollten und wenn ja, wie Sie dies tun können.

Bei der Konfiguration einer statischen Route nutzt das System die in Manager konfigurierten IP-Routendaten, um das Ziel für den weitergeleiteten Traffic zu bestimmen. Sie können den SSL VPN-Dienst als Ziel festlegen.

Verwenden Sie eine statische Route, wenn:

- Split-Tunneling-Routen in AVG nicht vorgesehen sind und Sie Traffic über den Tunnel senden müssen
- der SSL VPN-Dienst nicht mit AVG verbunden ist und Sie Traffic in die Warteschlange stellen wollen, der bei der Wiederherstellung der Verbindung weitergeleitet werden soll.

Voraussetzungen

Vor dem Beginn müssen Ihnen folgenden Informationen vorliegen:

- Die Adresse des externen Subnetzes; hierbei handelt es sich um das Subnetz in dem privaten Netzwerk, in dem AVG installiert ist
- Die auf die Subnetz-Adresse angewendete Subnetz-Maske
- Der Name des SSL VPN-Dienstes, den Sie zum Senden von Traffic an dieses externe Subnetz verwenden möchten

Vorgehensweise

1. Wählen Sie in der Navigationsliste **IP-Route**.
2. Klicken Sie mit der rechten Maustaste, und wählen Sie **Neu**.
3. Geben Sie in das Feld **IP-Adresse** die Adresse des externen Subnetzes ein, das sich an dem Ort befindet, an dem AVG installiert ist.
4. Geben Sie in das Feld **Subnetzmaske** die Subnetzmaske ein, die auf das externe Subnetz angewendet werden soll.
5. Achten Sie im Feld **Gateway-IP-Adresse** darauf, dass die Gateway-IP-Adresse 0.0.0.0 lautet.
6. Wählen Sie in der Liste **Ziel** den Namen des SSL VPN-Dienstes aus.

Verwandte Links

Konfiguration eines SSL VPN für die Unterstützung durch Avaya-Partner auf Seite 40

Kapitel 7: Konfiguration eines SSL VPN für Avaya-Partner mit einer SDK

Drittanbieter können ihr eigenes Avaya VPN Gateway für die Durchführung von Remote-Kundendienst über die IP Office-SSL-VPN-Technologie nutzen.

Für die Unterstützung von Drittanbietern kann das SSL VPN mit einem Software Development Kit (SDK) konfiguriert werden. Das SDK ermöglicht den Partnern, ihr eigenes AVG derart einzurichten, dass einige oder alle Aspekte der IP Office-Registrierung und des On-Boarding-Prozesses automatisiert werden. Diese automatisierten Prozesse ersetzen die manuelle Konfiguration.

SDK-Optionen

Es stehen zwei On-Boarding-SDKs zur Verfügung.

- On-Boarding-SDK
- On-Boarding-Express-SDK

On-Boarding-SDK:

Bei jeder neuen Installation von IP Office wird das On-Boarding-SDK auf dem Web-Server des Partners zur Erstellung der On-Boarding-XML-Datei ausgeführt. Diese wird daraufhin über Web Manager auf IP Office hochgeladen. Dieser Vorgang richtet den SSL VPN-Tunnel vom IP Office des Kunden zum AVG des Partners ein.

On-Boarding-Express-SDK:

Das On-Boarding-Express-SDK kann auch ohne eine Internetverbindung ausgeführt werden. Nachdem Sie das SDK ausgeführt haben, wird IP Office automatisch gestartet. Es sammelt alle relevanten Prozessdateien für das On-Boarding und protokolliert diese in einer ZIP-Datei. An dieser Stelle versucht der SSL VPN-Tunnel eine Verbindung mit dem AVG aufzubauen. Dies scheitert jedoch aufgrund eines Authentifizierungsfehlers. Sobald der Partner mithilfe des Inhalts der ZIP-Datei die SSL VPN-Anmeldedaten der entsprechenden Kundenseite erstellt hat, akzeptiert der AVG den Verbindungsaufbau des SSL VPN-Tunnels.

Funktionscodes

IP Office unterstützt mehrere SSL VPN-Dienstinstanzen. Das bedeutet, dass es gleichzeitig zwei aktiv verbundene SSL VPN-Dienste geben kann: einen zum Avaya Support-AVG und einen zum Partnerstandort. Sind zwei SSL VPN-Dienste in IP Office konfiguriert, empfiehlt Avaya die Verwendung der im Folgenden aufgeführten Namens- und Funktionscode-Konventionen für den Avaya Support-SSL-VPN-Dienst und den SSL VPN-Dienst des Partners. Die Konventionen basieren auf:

- Den Ziffern 775 = SSL auf einer Wähltastatur eines Telefons.

- Die vierte Ziffer ist entsprechend der Dienstinstanz entweder 1 oder 2.
- Der Wert der fünften Ziffer ist 1=aktiviert und 0=deaktiviert.

Avaya Support-SSL-VPN-Dienst:

- Dienstname: AVAYA_SUPPORT
- Funktionscode für die Aktivierung des Dienstes AVAYA_SUPPORT: 77511
- Funktionscode für die Deaktivierung des Dienstes AVAYA_SUPPORT: 77510

Partner-SSL-VPN-Dienst:

- Dienstname: BP_SUPPORT
- Funktionscode für die Aktivierung des Dienstes BP_SUPPORT: 77521
- Funktionscode für die Deaktivierung des Dienstes BP_SUPPORT: 77520

Voraussetzungen

- Auf dem PC, auf dem das SDK ausgeführt wird, muss Java Version 1.6 oder höher installiert sein.
- Die IP-Adresse des Tunnels darf nicht zwischen 172.22.0.0 und 172.25.255.255 liegen. Dieser Adressbereich ist für Avaya Support reserviert.

Verwandte Links

Herunterladen der SDK auf Seite 55
Herunterladen der IP Office-Bestandsdatei auf Seite 55
Verwenden des On-Boarding-SDK auf Seite 56
Verwenden des On-Boarding-Express-SDK auf Seite 59

Herunterladen der SDK

Sie können die On-Boarding-SDK und die On-Boarding-Express-SDK von der Avaya DevConnect-Website herunterladen: http://www.devconnectprogram.com/

Verwandte Links

Konfiguration eines SSL VPN für Avaya-Partner mit einer SDK auf Seite 54

Herunterladen der IP Office-Bestandsdatei

Im Folgenden wird beschrieben, wie Sie die IP Office-Bestandsdatei manuell mit Web Manager herunterladen. Die On-Boarding-Express-SDK stellt auch die notwendigen Tools bereit, um den Download automatisch ohne Web Manager auszuführen. Weitere Informationen finden Sie in der Dokumentation zur On-Boarding-Express-SDK.

Vorgehensweise

1. Melden Sie sich bei Web Manager an. Geben Sie in einem Webbrowser die IP-Adresse des IP Office-Systems im folgenden Format ein: `http://<ip_address>/index.html`.

   Die Indexseite des Servers wird geöffnet.
2. Klicken Sie auf **IP Office Web Manager**.
3. Geben Sie auf der Anmeldeseite den Benutzernamen und das Kennwort ein, und klicken Sie auf **Anmelden**.
4. Klicken Sie auf der Lösungsseite auf das Server-Menü rechts des Servers und wählen Sie **On-Boarding**.
5. Klicken Sie auf der On-Boarding-Seite auf **Bestandsdatei abrufen**.

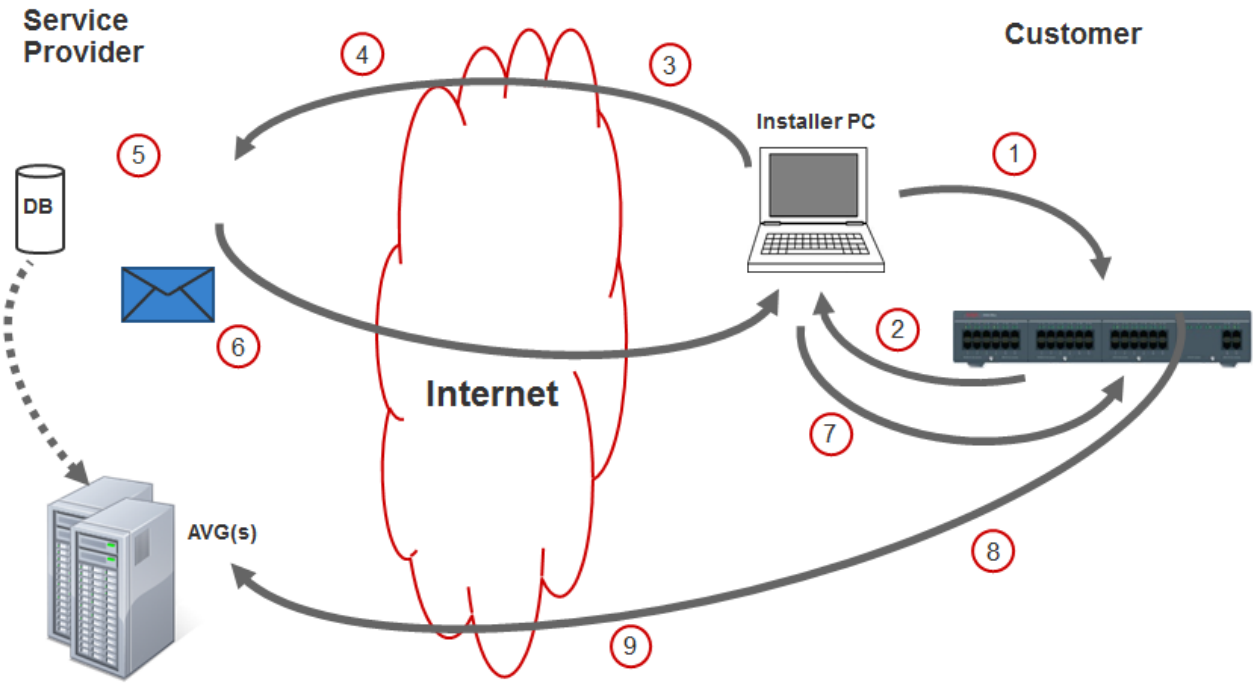
   Die Bestandsdatei wird auf den Installations-PC heruntergeladen.

Verwandte Links

[Konfiguration eines SSL VPN für Avaya-Partner mit einer SDK](#) auf Seite 54

Verwenden des On-Boarding-SDK

Konfigurationsverfahren für SSL-VPN mit dem On-Boarding-SDK



1	Konfigurieren Sie folgende Einstellungen in IP Office: • System-ID • Lizenzen • LAN-Schnittstellen • DNS-Server
2	Laden Sie am Kundenstandort die XML-Bestandsdatei von IP Office auf den Installations-PC herunter.
3	Laden Sie die Bestandsdatei auf die Partnerseite hoch.
4	Speichern Sie die SSL VPN-Anmeldedaten in der Datenbank.
5	Führen Sie das On-Boarding-SDK-Tool aus.
6	Senden Sie die On-Boarding-XML-Datei per E-Mail an den Installations-PC oder laden Sie sie auf diesen hoch.
7	Laden Sie die On-Boarding-XML-Datei auf IP Office hoch.
8	Der SSL VPN-Dienst baut eine Verbindung zum AVG auf.
9	Verifizieren Sie mit SSA die SSL VPN-Verbindung.

Verwandte Links

Konfiguration eines SSL VPN für Avaya-Partner mit einer SDK auf Seite 54
Speichern Sie die Anmeldedaten für SSL VPN in der AVG-Datenbank. auf Seite 57
Ausführen des On-Boarding-SDK auf Seite 57
Hochladen der On-Boarding-Datei und Überprüfen des SSL VPN auf Seite 58

Speichern Sie die Anmeldedaten für SSL VPN in der AVG-Datenbank.

Wenn Sie die lokale AVG-Datenbank nutzen, fügen Sie die Anmeldedaten in der AVG-Konfigurationsschnittstelle zu.

Wenn Sie eine LDAP- oder RADIUS-Datenbank nutzen, verwenden Sie die entsprechenden Schnittstellen, um die Anmeldedaten den Datenbanken hinzuzufügen.

Verwandte Links

Verwenden des On-Boarding-SDK auf Seite 56

Ausführen des On-Boarding-SDK

Es stehen Ihnen zwei Möglichkeiten zur Verfügung, das SDK auszuführen.

- Rufen Sie den Befehlszeilenwrapper für das On-Boarding-DOS-Batchskript mit den entsprechenden Parametern und Eingabe-/Ausgabe-Dateinamen auf.
- Verwenden Sie die veröffentlichten JAVA-APIs.

Weitere Informationen finden Sie im SDK-Entwicklerhandbuch in der SDK-ZIP-Datei.

Das SDK gibt die XML-On-Boarding-Datei aus. Übertragen Sie die Datei auf den Installations-PC am Kundenstandort.

Verwandte Links

Verwenden des On-Boarding-SDK auf Seite 56

Hochladen der On-Boarding-Datei und Überprüfen des SSL VPN

Vorgehensweise

1. Melden Sie sich bei Web Manager an. Geben Sie in einem Webbrowser die IP-Adresse des IP Office-Systems im folgenden Format ein: `http://<ip_address>/index.html`.

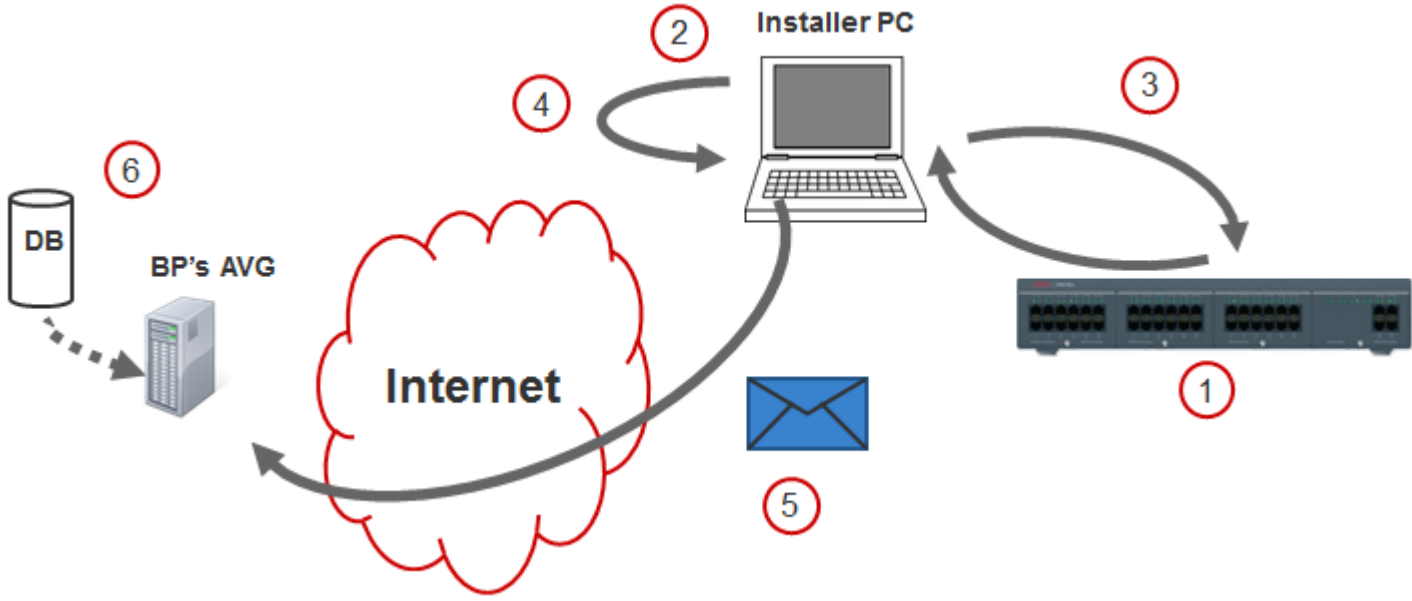
   Die Indexseite des Servers wird geöffnet.
2. Klicken Sie auf **IP Office Web Manager**.
3. Geben Sie auf der Anmeldeseite den Benutzernamen und das Kennwort ein, und klicken Sie auf **Anmelden**.
4. Klicken Sie auf der Lösungsseite auf das Server-Menü rechts des Servers und wählen Sie **On-Boarding**.
5. Klicken Sie auf der On-Boarding-Seite im Bereich Nummer 3 auf **Durchsuchen** und navigieren Sie zum Speicherort der On-Boarding-XML-Datei.
6. Klicken Sie auf **Hochladen**.
7. Überprüfen Sie die SSL-VPN-Verbindung mit der SSA-Anwendung.

Verwandte Links

Verwenden des On-Boarding-SDK auf Seite 56

Verwenden des On-Boarding-Express-SDK

SSL VPN-Konfigurationsverfahren mit dem On-Boarding-Express-SDK



1	Konfigurieren Sie die folgenden IP Office-Einstellungen. • System-ID • Lizenzen • LAN-Schnittstellen • DNS-Server
2	Führen Sie das On-Boarding-Express-SDK aus.
3	Das On-Boarding-Express-SDK tauscht Dateien mit IP Office aus.
4	Das On-Boarding-Express-SDK erstellt eine ZIP-Datei, die alle Dateien für das On-Boarding enthält. Wiederholen Sie die Schritte 1–3 für alle IP Office-Systeme.
5	Übertragen Sie die ZIP-Dateien über eine sichere Verbindung an den Partnerstandort. Nutzen Sie beispielsweise einen Filehosting- oder Cloud-Speicherdienst für die Dateiübertragung.
6	Nutzen Sie alle On-Boarding-Dateien, um einen SSL VPN-Tunnel zu erstellen.

Verwandte Links

Konfiguration eines SSL VPN für Avaya-Partner mit einer SDK auf Seite 54
Ausführen des On-Boarding-Express-SDK auf Seite 60
Verarbeiten der ZIP-Dateien von On-Boarding-Express-SDK auf Seite 60

Ausführen des On-Boarding-Express-SDK

Im Folgenden wird die Standard-Befehlszeilenschnittstelle vorgestellt. Mit der ebenfalls bereitgestellten JAVA API können leicht alternative Benutzerschnittstellen erstellt werden. Die Standardbenutzerschnittstelle sammelt die notwendigen Daten zur Erstellung einer Eigenschaftendatei. Diese wird als Eingabeinformation an die JAVA API weitergeleitet.

Es könnte beispielsweise eine mobile Anwendung erstellt werden, die über ein Formular die notwendigen Daten sammelt. Rufen Sie dann die JAVA API auf. Diese kontaktiert daraufhin IP Office, um die Registrierung abzuschließen und die daraus resultierende ZIP-Datei auszugeben.

Vorgehensweise

1. Bearbeiten Sie die Datei `default_parameters.txt`.
2. Führen Sie die On-Boarding-Express-SDK-Datei `sslvpnOnboardingExpress.bat` mit den entsprechenden Befehlsparametern aus.

   Das On-Boarding-Express-SDK erstellt eine ZIP-Datei mit allen für die Konfiguration des SSL VPN für IP Office notwendigen Dateien. Die ZIP-Datei wird im Ordner `sslvpn_OUTPUT` gespeichert.

Weitere Schritte

Übertragen Sie die ZIP-Dateien über eine sichere Verbindung an den Partnerstandort. Nutzen Sie beispielsweise einen Filehosting- oder Cloud-Speicherdienst für die Dateiübertragung.

Verwandte Links

Verwenden des On-Boarding-Express-SDK auf Seite 59

Verarbeiten der ZIP-Dateien von On-Boarding-Express-SDK

Sobald die von der SDK erstellte ZIP-Datei an den Partnerstandort übermittelt wurde, werden die Anmeldedaten für den SSL VPN-Tunnel der Kundeninstallation in AVG, Radius oder LDAP konfiguriert. Nach Abschluss stellt der SSL VPN-Tunnel eine Verbindung mit AVG her.

Wenn Sie einen gemeinsamen Cloud-Dateispeicherdienst nutzen, kann die Verarbeitung der ZIP-Datei im Partnerstandort innerhalb weniger Sekunden erfolgen. Daraufhin kann das Installationsprogramm direkt nach Ausführung des On-Boarding-Express-Skripts SSA starten, um eine korrekte Verbindung des SSL VPN-Tunnels zu überprüfen.

Verwandte Links

Verwenden des On-Boarding-Express-SDK auf Seite 59

Kapitel 8: NAPT-Regeln (Network Address & Port Translation, Konvertierung der Netzwerkadressen und Ports)

Verwenden Sie einen SSL VPN-Dienst und NAPT-Regeln zum Aufbau von Remote-Kommunikationssitzungen mit LAN-Geräten wie z. B. einem IP Office UCM-Modul. Um ein LAN-Gerät mit dem privaten IP Office-Netzwerk zu verbinden, startet der Support-Anbieter an seinem Standort eine Kommunikationsanwendung und gibt die folgenden Konfigurationsparameter für die Sitzung an:

- Die IP-Adresse eines SSL VPN-Tunnels
- Die Nummer des externen Ports für das LAN-Gerät

IP Office verwendet die NAPT-Regeln zur Zuordnung der IP-Adresse des Tunnels und der Nummer des externen Ports zur richtigen IP-Adresse und Portnummer im privaten Netzwerk.

Verwandte Links

Konfiguration der NAPT-Regeln auf Seite 61
Löschen von NAPT-Regeln auf Seite 62

Konfiguration der NAPT-Regeln

Führen Sie diese Aktionen auf der Oberfläche von Manager durch. Sie können bis zu 64 Regeln konfigurieren.

Bei der Konfiguration einer NAPT-Regel müssen Sie einen Anwendungstyp auswählen. Die folgenden Anwendungsoptionen sind verfügbar:

- Benutzerdefiniert
- VMPro
- one-X Portal
- SSH
- TELNET

- RDP (Remote Desktop Protocol)
- Web Control

Sie können die Einstellung **Benutzerdefiniert** für die Konfiguration einer NAPT-Regel für einen neuen Anwendungstyp verwenden. Sie können die Einstellung **Benutzerdefiniert** auch mit einer geänderten **External Port Number** (Nummer des externen Ports) verwenden, um zwei gleichzeitige Kommunikationssitzungen zu öffnen, wobei die gleiche Anwendung zum Aufbau der Verbindung mit dem gleichen LAN-Gerät verwendet wird. Um beispielsweise zwei gleichzeitige SSH-Sitzungen mit der gleichen IP-Adresse als Ziel zu aktivieren, müssen die beiden NAPT-Regeln in etwa folgendermaßen aussehen.

Anwendung	Protokoll	Nummer des externen Ports	Interne IP-Adresse	Nummer des internen Ports
SSH	TCP	22	192.168.0.40,1	22
Benutzerdefiniert	TCP	221	192.168.0.40,1	22

Vorgehensweise

1. Wählen Sie in der Navigationsliste **Dienst**.
2. Wählen Sie in der Liste **Dienst** den SSL VPN-Dienst aus, für den Sie die NAPT-Regeln konfigurieren möchten.
3. Wählen Sie im Detailfenster für den Dienst die Registerkarte **NAPT**.
4. Rufen Sie unter **Anwendung** die Dropdown-Liste auf, und wählen Sie einen Anwendungstyp.

   Die Felder **Protokoll** und **Portnummer** werden automatisch mit den Standardwerten befüllt.
5. (Optional) Wenn Sie eine **Benutzerdefinierte** Anwendung konfigurieren möchten, müssen Sie den Eintrag im Feld **External Port Number** (Nummer des externen Ports) ändern.
6. Wiederholen Sie die Schritte 4 und 5, um weitere Regeln hinzuzufügen.

Verwandte Links

NAPT-Regeln (Network Address & Port Translation, Konvertierung der Netzwerkadressen und Ports) auf Seite 61

Löschen von NAPT-Regeln

Vorgehensweise

Zum Löschen einer NAPT-Regel verwenden Sie die leere Spalte auf der linken Seite der Tabelle. Klicken Sie mit der rechten Maustaste in die leere Zelle neben der Regel, die Sie löschen wollen, und wählen Sie das Löschen-Symbol.

Verwandte Links

NAPT-Regeln (Network Address & Port Translation, Konvertierung der Netzwerkadressen und Ports) auf Seite 61

Kapitel 9: Überprüfen Sie die Verbindung zwischen IP Office und AVG.

Wenden Sie die Vorgehensweise in diesem Kapitel an, um die Verbindung zwischen dem IP Office-System und AVG zu testen.

Verwandte Links

Überprüfung der Verbindung mit SysMonitor auf Seite 64
Überprüfung der Bereitstellung von AVG SSL VPN mittels System Status Application auf Seite 65
Überprüfung der Verbindung über die BBI des AVG auf Seite 65
Versand von Probealarmen auf Seite 66

Überprüfung der Verbindung mit SysMonitor

Mit der System Status Application (SSA) können Sie Betriebsbereitschaft des SSL VPN-Tunnels überprüfen. Starten Sie die SSA, und überprüfen Sie, ob die Konfigurationseinstellungen für den Tunnel aufgeführt werden.

Sie können auch folgendermaßen vorgehen, um mithilfe von SysMonitor die SSL VPN-Verbindung zwischen dem IP Office-System und dem AVG zu überprüfen.

Vorgehensweise

1. Wählen Sie **Start > Programme > IP Office > Monitor**.

   SysMonitor baut eine Verbindung mit dem IP Office-Server auf und zeigt ein Systemprotokoll an.

2. Wählen Sie **Filters > Trace** (Filter > Protokoll), und klicken Sie auf die Registerkarte **VPN**.
3. Stellen Sie im Bereich „SSL VPN“ sicher, dass **Session** (Sitzung) und **Session State** (Sitzungsstatus) aktiviert sind. Klicken Sie auf **OK**.

   Das SysMonitor-Protokoll führt die Aktivität des SSL VPN-Dienstes unter dem Namen auf, den Sie für den Dienst konfiguriert haben.

4. Suchen Sie den Namen des Dienstes, und überprüfen Sie die folgenden Daten:

Session state change (Änderung des Sitzungsstatus)	Bei Aktivierung des SSL VPN-Dienstes durchläuft der Sitzungsstatus die folgenden Stufen: • Auflösung des Domänennamens • Start der Sitzung • Verbindung der IP-Adresse von IP Office mit der IP-Adresse des VPN-Gateways Wenn IP Office den Domänennamen nicht auflösen kann, wird die folgende Fehlermeldung angezeigt: „DNS failed to resolve host name <x.x.x> and reached MAX retries. Restart session.“ (DNS konnte den Hostnamen <x.x.x> nicht auflösen und hat MAX-Wiederholungen erreicht. Starten Sie die Sitzung neu.)

Verwandte Links

Überprüfen Sie die Verbindung zwischen IP Office und AVG. auf Seite 64

Überprüfung der Bereitstellung von AVG SSL VPN mittels System Status Application

Führen Sie die folgenden Schritte aus, um die Bereitstellung von AVG SSL zu überprüfen.

1. Starten Sie die IP Office System Status Application (SSA), und überprüfen Sie, ob der SSL VPN-Tunnel **Betriebsbereit** ist und die **IP-Adresse des Tunnels** angezeigt wird.
2. Pingen Sie IP Office von außerhalb an. Rufen Sie auf dem Computer des Service Agents ein Befehlsfenster auf, und führen Sie unter Verwendung der IP-Adresse des Tunnels einen Ping-Befehl aus. Der Ping sollte erfolgreich sein.

Verwandte Links

Überprüfen Sie die Verbindung zwischen IP Office und AVG. auf Seite 64

Überprüfung der Verbindung über die BBI des AVG

Vorgehensweise

1. Melden Sie sich bei der BBI des AVG an.
2. Erweitern Sie **Überwachen** im linken Navigationsfenster.
3. Wählen Sie unter **Überwachen** die Option **Benutzer**.

4. In der Spalte **Source IP** (Quell-IP) wird Folgendes angezeigt:
   - Die IP-Adresse von IP Office
   - Die IP-Adresse des SSL VPN-Tunnels, die dem lokalen Benutzer zugeordnet ist.

Verwandte Links

Überprüfen Sie die Verbindung zwischen IP Office und AVG. auf Seite 64

Versand von Probealarmen

Gehen Sie folgendermaßen vor, um über System Status Application (SSA) einen Probealarm zu senden. Nutzen Sie den Probealarm, um ein Fehlerereignis zu generieren.

Voraussetzungen

Es muss ein Alarmziel definiert sein. Wenn Sie für das Fehlerereignis eine Ziel-IP-Adresse definieren, verwendet das System eine IP-Routing-Tabelle, um zu ermitteln, welche Schnittstelle beim Senden des Fehlerereignisses verwendet werden sollte.

Vorgehensweise

1. Nutzen Sie eine der folgenden Methoden, um SSA zu starten:
   - Starten Sie SSA über die IP Office-Admin-DVD.
   - Wählen Sie **Start > Programs > IP Office > System Status**.
   - Wählen Sie in Manager oder IP Office Manager for Server Edition die Option **Datei > Erweitert > System Status**.
2. Wählen Sie aus der Navigationsliste **Alarme > Dienst**.
3. Klicken Sie auf die Schaltfläche **Alarm testen**.

   In der Tabelle werden die Ergebnisse des Tests angezeigt:

Wert	Beschreibung
Letztes Datum des Fehlers	Datum und Uhrzeit des Alarms.
Zeitpunkte	Die Anzahl der Vorkommnisse des Alarms, seit die Steuereinheit das letzte Mal neu gestartet oder der Alarm zurückgesetzt wurde.
Fehlerbeschreibung	Bei Probealarmen wird die folgende Nachricht angezeigt: „Vom Operator ausgelöster Probealarm.“

   Wenn Sie ein Alarmziel für einen SNMP-Trap definiert haben, generiert der Probealarm die folgenden Daten:

```
Enterprise: ipoGenTraps
Bindings (8)
Binding #1: ipoGTEventStdSeverity.0 *** (int32) major(4)
Binding #2: ipoGTEventDateTime.0 *** (octets)
Binding #3: ipoGTEventDevID.0 *** (octets)
```

```
Binding #4: sysDescr.0 *** (octets)
Binding #5: ipoGTEventReason.0 *** (int32) testAlarm(39)
Binding #6: ipoGTEventData.0 *** (octets)
Binding #7: ipoGTEventAlarmDescription.0 *** (octets) Operator initiated test
alarm - do not process
Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) (zero-length)
```

Verwandte Links

Überprüfen Sie die Verbindung zwischen IP Office und AVG. auf Seite 64

Kapitel 10: Überwachen und Verwalten des IP Office-Systems

Wenn der SSL VPN-Dienst verbunden ist, können Sie das IP Office-System remote über den Tunnel überwachen. Zusätzlich können Sie das IP Office-System remote verwalten und aktualisieren. Dank des SSL VPN-Services können Sie Thick-Anwendungen und webbasierte Anwendungen so nutzen, als ob sie direkt über eine lokale LAN-Schnittstelle angebunden wären. In diesem Abschnitt erhalten Sie Informationen über die unterstützten Anwendungen und ihre Nutzung.

Überwachungswerkzeuge

Mit den folgenden Werkzeugen können Sie das IP Office-System dezentral überwachen:

- System Status Application (SSA): System Status Application ist ein Diagnosewerkzeug, mit dem Sie den Status von IP Office-Systemen überwachen können. SSA berichtet historische und Echtzeit-Ereignisse und Status- und Konfigurationsdaten.
- SysMonitor: SysMonitor zeigt Betriebsinformationen über das IP Office-System an. Die Anwendung kann diese Daten erfassen, um Dateien zu Analysezwecken zu protokollieren.

Verwaltungswerkzeuge

Mit den folgenden Werkzeugen können Sie das IP Office-System remote verwalten, aktualisieren und konfigurieren:

- IP Office Manager: Eine Administrationsanwendung, mit der Sie die Systemeinstellungen von IP Office Essential Edition-Systemen konfigurieren können.
  - IP Office Manager for Server Edition: Wenn Sie IP Office Manager starten, können Sie über den IP Office Manager for Server Edition-Modus die Konfiguration öffnen. In diesem Modus können Sie Server Edition-Server und -Erweiterungssysteme verwalten.
- IP Office Basic Edition – Web Manager: ein browserbasiertes Werkzeug, mit dem Sie die Systemeinstellungen für IP Office konfigurieren können.

Fehlerberichterstattung

Mit dem SSL VPN-Dienst können Sie Systemfehler an einen Remote-Fehlerverwaltungsserver am Standort des Dienstanbieters senden, auf dem AVG installiert ist. Sie können Filter einrichten, um zu definieren, welche Fehler berichtet werden und die Ziele konfigurieren, an die die Fehler gesendet werden.

Informationen zur Fehlerberichterstattung finden Sie unter Konfigurieren der Alarmbenachrichtigungen auf Seite 48

Betriebsmodi

Welche Werkzeuge Sie zum Überwachen und Verwalten des IP Office-Systems verwenden können, hängt vom verwendeten Betriebsmodus ab. In der folgenden Tabelle finden Sie die Werkzeuge, die in den einzelnen Modi unterstützt werden.

Werkzeuge	Betriebsmodus			
	Essential Edition	IP Office Server Edition	Erweiterungssystem Server Edition	Basic Edition
SSA	✔	✔	✔	✔
SysMonitor	✔	✔	✔	✔
Manager(Vereinfacht)	—	—	—	✔
Manager (Standard) und IP Office Manager for Server Edition	✔	✔	✔	—
Web Manager	—	—	—	✔
Fehlerberichterstattung	✔	✔	✔	✔

Verwandte Links

Remote-Überwachung von IP Office mit SSA auf Seite 69
Remote-Überwachung von IP Office mit SysMonitor auf Seite 70
Remote-Überwachung von LAN-Geräten mit dem SSL VPN-Tunnel auf Seite 71
Remote-Konfiguration von IP Office mit Web Manager auf Seite 72
Remote-Konfiguration von IP Office über Manager auf Seite 72
Remote-Konfiguration von Server Edition-Systemen mit IP Office Manager for Server Edition auf Seite 73
Remote-Konfiguration von Server Edition-Systemen mit Web Control auf Seite 75

Remote-Überwachung von IP Office mit SSA

Nutzen Sie diese Vorgehensweise, um über den SSL VPN-Tunnel eine Verbindung zwischen System Status Application (SSA) und IP Office aufzubauen.

Voraussetzungen

Der SSL VPN-Tunnel muss betriebsbereit sein, und Sie müssen über die folgenden Informationen verfügen:

- die IP-Adresse des SSL VPN-Tunnels
- den Benutzernamen des IP Office-Administratorkontos
- das Kennwort des IP Office-Administratorkontos

Vorgehensweise

1. Nutzen Sie eine der folgenden Methoden, um SSA zu starten:
   - Starten Sie SSA über die IP Office-Admin-DVD.
   - Wählen Sie **Start > Programs > IP Office > System Status**.
   - Wählen Sie in Manager oder IP Office Manager for Server Edition die Option **Datei > Erweitert > System Status**.
2. Geben Sie in das Feld **IP-Adresse der Steuereinheit** die IP-Adresse des SSL VPN-Tunnels ein.
3. Geben Sie in das Feld **Benutzername** den Benutzernamen des IP Office-Administratorkontos ein.
4. Geben Sie in das Feld **Kennwort** das Kennwort für das IP Office-Administratorkonto ein.
5. Klicken Sie auf **Anmelden**.

Verwandte Links

Überwachen und Verwalten des IP Office-Systems auf Seite 68

Remote-Überwachung von IP Office mit SysMonitor

Nutzen Sie diese Vorgehensweise, um über den SSL VPN-Tunnel eine Verbindung zwischen SysMonitor und IP Office aufzubauen.

Voraussetzungen

Der SSL VPN-Tunnel muss betriebsbereit sein, und Sie müssen über die folgenden Informationen verfügen:

- die IP-Adresse des SSL VPN-Tunnels
- das Kennwort des IP Office-Administratorkontos

Vorgehensweise

1. Wählen Sie **Start > Programme > IP Office > Monitor**.
2. Klicken Sie auf das Symbol **Select Unit** (Einheit auswählen).

   Ein Dialogfeld wird angezeigt.

3. Geben Sie in das Feld **IP-Adresse der Steuereinheit** die IP-Adresse des SSL VPN-Tunnels ein.
4. Geben Sie in das Feld **Password** (Kennwort) das Kennwort des IP Office-Administratorkontos ein.
5. Klicken Sie auf die Schaltfläche „Durchsuchen“ neben dem Feld **Trace Log Settings Filename** (Dateiname der Trace-Protokoll-Einstellungen). Wechseln Sie in das Verzeichnis, in dem Sie das Trace-Protokoll speichern möchten, und klicken Sie auf **Open** (Öffnen).
6. Klicken Sie auf **OK**.

Verwandte Links

Überwachen und Verwalten des IP Office-Systems auf Seite 68

Remote-Überwachung von LAN-Geräten mit dem SSL VPN-Tunnel

Gehen Sie folgendermaßen vor, um mithilfe der NAPT (Network Address & Port Translation) eine Verbindung mit einem LAN-Gerät im IP Office-Netzwerk über den SSL VPN-Tunnel herzustellen. Sie können die Verbindung mit einem LAN-Gerät mithilfe einer Kommunikationsanwendung herstellen, in der eine entsprechende NAPT-Regel konfiguriert ist. Informationen zum Konfigurieren von NAPT-Regeln finden Sie unter NAPT-Regeln (Network Address & Port Translation, Konvertierung der Netzwerkadressen und Ports) auf Seite 61.

Voraussetzungen

Der SSL VPN-Tunnel muss betriebsbereit sein, und Sie müssen über die folgenden Informationen verfügen:

- Die IP-Adresse des SSL VPN-Tunnels
- Die in der NAPT-Regel für das zu verbindende LAN-Gerät konfigurierte Nummer des externen Ports

Vorgehensweise

1. Rufen Sie die Kommunikationsanwendung auf, die Sie für den Aufbau der Verbindung mit einem LAN-Gerät über den SSL VPN-Tunnel verwenden.
2. Richten Sie unter Verwendung der IP-Adresse des SSL VPN-Tunnels und der Nummer des externen Ports des LAN-Geräts eine Kommunikationssitzung ein.

Verwandte Links

Überwachen und Verwalten des IP Office-Systems auf Seite 68

Remote-Konfiguration von IP Office mit Web Manager

Nutzen Sie diese Vorgehensweise, um über den SSL VPN-Tunnel eine Verbindung zwischen Web Manager und IP Office aufzubauen.

Informationen über die Nutzung von Web Manager zum Konfigurieren des IP Office-Systems finden Sie unter *Avaya IP Office Basic Edition – Web Manager.*

Voraussetzungen

Der SSL VPN-Tunnel muss betriebsbereit sein, und Sie müssen über die folgenden Informationen verfügen:

- die IP-Adresse des SSL VPN-Tunnels
- den Kontonamen des IP Office-Administratorkontos
- das Kennwort des IP Office-Administratorkontos

Vorgehensweise

1. Geben Sie die IP-Adresse für Web Management im folgenden Format in einen Browser ein: `https://10.0.0.1:8443/webmanagement/WebManagement.html`. Hierbei steht *10.0.0.1* für die IP-Adresse des SSL VPN-Tunnels.

   Sollte der Browser eine Sicherheitswarnung ausgeben, befolgen Sie die angezeigten Menüeinstellungen, um mit dem Verbindungsaufbau fortzufahren.
2. Wenn das Anmeldemenü angezeigt wird, geben Sie den Benutzernamen und das Kennwort des Systemadministrators ein.
3. Klicken Sie auf **Anmelden**.

   Die Startseite der webbasierten Systemverwaltung wird angezeigt.

Verwandte Links

Überwachen und Verwalten des IP Office-Systems auf Seite 68

Remote-Konfiguration von IP Office über Manager

Sie können Manager nutzen, um das IP Office-System remote über den SSL VPN-Tunnel zu verwalten. Wenn Sie Manager über den SSL VPN-Tunnel verwenden, wird die automatische Erkennung von IP Office-Systemen nicht unterstützt. Sie müssen die IP-Adresse des Systems konfigurieren, mit dem Sie eine Verbindung aufbauen wollen. Nutzen Sie diese Vorgehensweise, um über den SSL VPN-Tunnel eine Verbindung zwischen Manager und IP Office aufzubauen.

Informationen über die Konfiguration von Manager und seine Nutzung zur Verwaltung eines IP Office-Systems finden Sie unter *Avaya IP Office Manager*.

Voraussetzungen

Der SSL VPN-Tunnel muss betriebsbereit sein, und Sie müssen über die folgenden Informationen verfügen:

- die IP-Adresse des SSL VPN-Tunnels
- den Kontonamen des IP Office-Administratorkontos
- das Kennwort des IP Office-Administratorkontos

Vorgehensweise

1. Wählen Sie **Start > Programs > IP Office > Manager**.
2. Klicken Sie auf das Symbol **Konfiguration vom IP Office öffnen**.

   Das Dialogfeld „IP Office auswählen“ wird angezeigt.
3. Geben Sie die IP-Adresse des SSL VPN-Tunnels in das Feld **Geräte-/Broadcast-Adresse** ein, und klicken Sie auf **Aktualisieren**.
4. Wählen Sie das IP Office-System aus, das Sie konfigurieren möchten, und klicken Sie auf **OK**.

   Das Dialogfeld „Benutzeranmeldung für Konfigurationsdienst“ wird angezeigt.
5. Geben Sie den Benutzernamen des IP Office-Administratorkontos in das Feld **Benutzername für den Dienst** ein, und geben Sie das Kennwort für das IP Office-Administratorkonto in das Feld **Benutzerkennwort für den Dienst** ein. Klicken Sie auf **OK**.

Verwandte Links

Überwachen und Verwalten des IP Office-Systems auf Seite 68

Remote-Konfiguration von Server Edition-Systemen mit IP Office Manager for Server Edition

Sie können mit IP Office Manager for Server Edition die folgenden Systeme remote über den SSL VPN-Tunnel verwalten:

- Primäre Server Edition
- Sekundäre Server Edition
- Erweiterungssystem Server Edition

Voraussetzungen

Der SSL VPN-Tunnel muss betriebsbereit sein, und Sie müssen über die folgenden Informationen verfügen:

- die IP-Adresse des SSL VPN-Tunnels
- den Kontonamen des IP Office Manager for Server Edition-Administratorkontos

- das Kennwort des IP Office Manager for Server Edition-Administratorkontos

Informationen zu diesem Vorgang

Für die Remote-Konfiguration von Server Edition-Systemen muss ein SSL VPN-Dienst zwischen AVG und Primäre Server Edition konfiguriert sein. Dann können Konfigurationsänderungen auf die Server Edition-Systeme angewendet werden, die an den primären Server angebunden sind. Sie müssen zunächst einen SSL VPN-Dienst zwischen jedem Server Edition-System und AVG konfigurieren.

Nutzen Sie diese Vorgehensweise, um über den SSL VPN-Tunnel eine Verbindung zwischen IP Office Manager for Server Edition und Primäre Server Edition aufzubauen.

Informationen über die Nutzung von IP Office Manager for Server Edition finden Sie unter *Avaya IP Office Manager*.

Vorgehensweise

1. Wählen Sie **Start > Programs > IP Office > Manager**.
2. Wählen Sie **Datei > Voreinstellungen**.
3. Wählen Sie **Fernzugriff für Multi-Site verwenden**, und klicken Sie auf **OK**.
4. Klicken Sie auf das Symbol **Konfiguration vom IP Office öffnen**.

   Das Dialogfeld „IP Office auswählen“ wird angezeigt.
5. Geben Sie die IP-Adresse des SSL VPN-Tunnels in das Feld **Geräte-/Broadcast-Adresse** ein, und klicken Sie auf **Aktualisieren**.
6. Wählen Sie das Server Edition-System aus, das Sie konfigurieren möchten.

   Wenn Sie das Server Edition-System auswählen, wird die Option zum Öffnen mit Server Edition angezeigt und standardmäßig aktiviert.
7. Wenn eine Verbindung mit Primäre Server Edition besteht und Sie Konfigurationsänderungen an Server Edition-Systemen durchführen möchten, die damit verbunden sind, wählen Sie **Fernzugriff verwenden**. Wenn eine direkte Verbindung mit dem Server Edition-System besteht, brauchen Sie diese Option nicht auszuwählen.
8. Klicken Sie auf **OK**.

   Das Dialogfeld „Benutzeranmeldung für Konfigurationsdienst“ wird angezeigt.
9. Geben Sie den Benutzernamen des IP Office Manager for Server Edition-Administratorkontos in das Feld **Benutzername für den Dienst** ein, und geben Sie das Kennwort für das IP Office Manager for Server Edition-Administratorkonto in das Feld **Benutzerkennwort für den Dienst** ein. Klicken Sie auf **OK**.
10. Wählen Sie in der Navigationsliste **Netzwerk**.

    Das Bild „Zusammenfassung“ wird angezeigt. In der Tabelle unten im Bild werden alle Server Edition-Systeme aufgeführt.
11. Wählen Sie das Server Edition-System aus, das Sie konfigurieren möchten.

    Das Bild „Zusammenfassung“ enthält die Konfigurationsdaten des ausgewählten Systems.

Verwandte Links

Überwachen und Verwalten des IP Office-Systems auf Seite 68

Remote-Konfiguration von Server Edition-Systemen mit Web Control

Sie können die Web Control-Oberfläche nutzen, um IP Office Manager for Server Edition zu starten und Server Edition-Systeme remote über den SSL VPN-Tunnel zu verwalten.

Sie können mit IP Office Manager for Server Edition die folgenden Systeme remote über den SSL VPN-Tunnel verwalten:

- Primäre Server Edition
- Sekundäre Server Edition
- Erweiterungssystem Server Edition

Voraussetzungen

Der SSL VPN-Tunnel muss betriebsbereit sein, und Sie müssen über die folgenden Informationen verfügen:

- die IP-Adresse des SSL VPN-Tunnels
- den Kontonamen des Web Control-Administratorkontos
- das Kennwort des Web Control-Administratorkontos

Informationen zu diesem Vorgang

Für die Remote-Konfiguration von Server Edition-Systemen muss ein SSL VPN-Dienst zwischen AVG und Primäre Server Edition konfiguriert sein. Dann können Konfigurationsänderungen auf die Server Edition-Systeme angewendet werden, die an den primären Server angebunden sind. Sie müssen zunächst einen SSL VPN-Dienst zwischen jedem Server Edition-System und AVG konfigurieren.

Nutzen Sie diese Vorgehensweise, um IP Office Manager for Server Edition über die Web Control-Oberfläche zu starten und um über den SSL VPN-Tunnel eine Verbindung mit Primäre Server Edition aufzubauen.

Informationen über die Nutzung von IP Office Manager for Server Edition finden Sie unter *Avaya IP Office Manager*.

Vorgehensweise

1. Öffnen Sie einen Browser, und geben Sie `https://<IP-Adresse>:7070` ein. Bei *<IP-Adresse>* handelt es sich hier um die Adresse des SSL VPN-Tunnels, der für Primäre Server Edition konfiguriert ist.
2. Geben Sie die Administrator-Anmeldedaten in die Felder **Anmeldung** und **Kennwort** ein, und klicken Sie auf **Anmelden**.

Der Homescreen wird angezeigt und führt alle Server Edition-Server und Erweiterungssysteme auf.

3. Klicken Sie auf **Verwalten**.

   IP Office Manager for Server Edition wird geöffnet und zeigt das Bild „Zusammenfassung“ an.

4. Wählen Sie **Datei > Schließen**, um die Konfiguration zu schließen.
5. Wählen Sie **Datei > Voreinstellungen**.
6. Wählen Sie **Fernzugriff für Multi-Site verwenden**, und klicken Sie auf **OK**.
7. Klicken Sie auf das Symbol **Konfiguration vom IP Office öffnen**.

   Das Dialogfeld „IP Office auswählen“ wird angezeigt.

8. Geben Sie die IP-Adresse des SSL VPN-Tunnels in das Feld **Geräte-/Broadcast-Adresse** ein, und klicken Sie auf **Aktualisieren**.
9. Wählen Sie den Server Edition-Server.

   Wenn Sie das Server Edition-System auswählen, wird die Option zum Öffnen mit Server Edition angezeigt und standardmäßig aktiviert.

10. Wählen Sie **Fernzugriff verwenden**, und klicken Sie auf **OK**.

    Das Dialogfeld „Benutzeranmeldung für Konfigurationsdienst“ wird angezeigt.

11. Geben Sie den Benutzernamen des IP Office Manager for Server Edition-Administratorkontos in das Feld **Benutzername für den Dienst** ein, und geben Sie das Kennwort für das IP Office Manager for Server Edition-Administratorkonto in das Feld **Benutzerkennwort für den Dienst** ein. Klicken Sie auf **OK**.

    IP Office Manager for Server Edition wird geöffnet und zeigt das Bild „Zusammenfassung“ an.

12. Wählen Sie in der Tabelle unten im Bild Primäre Server Edition aus.
13. Klicken Sie in der Liste **Öffnen . . .** rechts im Bild auf **Konfiguration**.

    Ein Navigationsbaum wird für das System angezeigt.

14. Sobald Sie das ausgewählte System konfiguriert haben und Ihre Änderungen gespeichert haben, wählen Sie in der Navigationsliste **Netzwerk**, um zum Bild **Zusammenfassung** zurückzukehren.
15. Um andere Server Edition-Systeme zu konfigurieren, die an den Primäre Server Edition-Server angebunden sind, wählen Sie das System in der Tabelle unten im Bild „Zusammenfassung“ aus.

    Das Bild „Zusammenfassung“ enthält die Konfigurationsdaten des ausgewählten Systems.

Verwandte Links

Überwachen und Verwalten des IP Office-Systems auf Seite 68

Kapitel 10: Remote-Upgrade von IP Office

Sie können den SSL VPN-Tunnel verwenden, um ein Upgrade des IP Office-Systems am Standort des Dienstanbieters durchzuführen. Diese Funktion steht nur zur Verfügung, wenn Sie ein Upgrade von einem System der Version 8.1 auf eine höhere Software-Version durchführen.

Wenn Sie Manager über den SSL VPN-Tunnel verwenden, wird die automatische Erkennung von IP Office-Systemen nicht unterstützt.

Führen Sie diese Vorgehensweise am Standort des Dienstanbieters durch, und nutzen Sie dabei die Manager-Oberfläche auf dem Server des Dienstanbieters. Nutzen Sie zum Konfigurieren eines Server Edition-Systems den IP Office Manager for Server Edition-Modus.

Voraussetzungen

Am Standort des Dienstanbieters muss mithilfe der IP Office-Admin-DVD die neue Software auf dem Dienstagenten-PC installiert werden.

Der SSL VPN-Tunnel muss betriebsbereit sein, und Sie müssen über die folgenden Informationen verfügen:

- die IP-Adresse des SSL VPN-Tunnels

Vorgehensweise

1. Wählen Sie **Datei > Voreinstellungen > Erkennung**.
2. Geben Sie in das Feld **IP-Suchkriterien** die IP-Adresse des SSL VPN-Tunnels ein, und klicken Sie auf **OK**.
3. Wählen Sie **Datei > Erweitert > Upgrade**.

   Der Upgrade-Assistent wird angezeigt.

   Hinweis:

   Wenn ein Dialogfeld angezeigt wird und Sie zum Öffnen einer Konfigurationsdatei auffordert, klicken Sie auf „Abbrechen“, und fahren Sie mit diesem Schritt fort. Vor dem Durchführen eines Upgrades brauchen Sie keine Konfigurationsdatei zu öffnen.
4. Geben Sie in das Feld **Geräte-/Broadcast-Adresse** die IP-Adresse des SSL VPN-Tunnels ein, und klicken Sie auf **Aktualisieren**.

   Geben Sie keine Broadcast-Adresse ein. Broadcast-Adressen werden im Rahmen von Remote-Upgrades über eine SSL VPN-Verbindung nicht unterstützt.
5. Klicken Sie auf das entsprechende Kontrollkästchen, um das System auszuwählen, für das Sie ein Upgrade durchführen möchten, und klicken Sie auf **Upgrade**.

Nach dem Abschluss des Upgrades wird IP Office neu gestartet, und die Verbindung mit dem SSL VPN-Dienst wird automatisch wiederhergestellt.

Kapitel 11: Überwachen des SSL VPN-Dienstes

Zusätzlich zum IP Office-System können Sie auch den SSL VPN-Tunnel überwachen. Dieser Abschnitt bietet Informationen über die Überwachungswerkzeuge, die für den SSL VPN-Dienst zur Verfügung stehen, und ihre Nutzung.

Sie können die folgenden Werkzeuge verwenden, um den SSL VPN-Dienst zu überwachen:

- System Status Application (SSA): System Status Application ist ein Diagnosewerkzeug, mit dem Sie den Status des SSL VPN-Tunnels überwachen können. SSA berichtet historische und Echtzeit-Ereignisse.
- SysMonitor: SysMonitor zeigt Betriebsdaten des SSL VPN-Tunnels an. Die Anwendung kann diese Daten erfassen, um Dateien zu Analysezwecken zu protokollieren. Sammeln Sie mit diesem Werkzeug nur dann Informationen, wenn Sie von Mitarbeitern des technischen Supports dazu aufgefordert werden.
- Fehlerberichterstattung: Der SSL VPN-Dienst generiert für seine eigenen Komponenten Fehler, wenn ein Problem auftritt. Es ist möglich, Ereignisfilter einzurichten, um beim Auftreten dieser Fehler eine Benachrichtigung zu erhalten und das Ziel zu konfigurieren, an das Benachrichtigungen gesendet werden. Informationen zum Einrichten von Ereignisfiltern und Konfigurieren von Alarmzielen finden Sie in Konfiguration der Alarmbenachrichtigungen auf Seite 48.

Verwandte Links

Anzeigen des Tunnel-Status auf Seite 79
Überwachen von Alarmen mit SSA auf Seite 83
Beheben von Problemen mit dem SSL VPN-Dienst auf Seite 84

Anzeigen des Tunnel-Status

Gehen Sie wie folgt vor, um den Status des SSL VPN-Tunnels über System Status Application (SSA) anzuzeigen.

Vorgehensweise

1. Nutzen Sie eine der folgenden Methoden, um SSA zu starten:
   - Starten Sie SSA über die IP Office-Admin-DVD.

- Wählen Sie **Start > Programs > IP Office > System Status**.
- Wählen Sie in Manager die Option **Datei > Erweitert > System Status**.

2. Wählen Sie in der Navigationsliste **IP-Netzanbindung > SSL VPN**.

   In einer Zusammenfassungstabelle werden Informationen über jeden konfigurierten SSL VPN-Dienst konfiguriert.

3. Um detaillierte Informationen über einen bestimmten SSL VPN-Dienst zu erhalten, markieren Sie den SSL VPN-Dienst, und klicken Sie auf **Auswählen**.

   In einer detaillierten Tabelle werden die Statusinformationen des ausgewählten SSL VPN-Dienstes angezeigt.

Verwandte Links

Überwachen des SSL VPN-Dienstes auf Seite 79
Tunnel-Status-Feldbeschreibungen: Zusammenfassungstabelle auf Seite 80
Tunnel-Status-Feldbeschreibungen: Detailtabelle auf Seite 81

Tunnel-Status-Feldbeschreibungen: Zusammenfassungstabelle

System Status Application (SSA) zeigt die folgenden Zusammenfassungsinformationen für den SSL VPN-Dienst an:

Wert	Beschreibung
Name	Der Name des SSL VPN-Dienstes, der in IP Office konfiguriert ist.
Status des Dienstes	Gibt an, ob SSL VPN betriebsbereit oder im Ausweichbetrieb ist.
Zeit der letzten Verbindung	Der Zeitstempel der letzten erfolgreichen Verbindung.
Zeit der letzten Verbindungstrennung	Der Zeitstempel der letzten Verbindungsunterbrechung.
IP-Adresse des Tunnels	Die IP-Adresse des SSL VPN-Tunnels.
Insgesamt verpasste Heartbeats	Die zusammengefasste Anzahl der verpassten Heartbeat-Signale. Der Zähler wird auf 0 zurückgesetzt, wenn IP Office neu gestartet wird oder wenn die Bereitstellung von SSL VPN-Dienst in Manager aufgehoben wird.
Insgesamt verpasste Keepalives	Für UDP-Verbindungen werden Keepalives genutzt. UDP wird vom SSL VPN-Dienst nicht unterstützt. Der Wert ist 0.
Lokaler TCP-Endpunkt	Die TCP IP-Adresse und Portnummer von IP Office.
Entfernter TCP-Endpunkt	Dies ist die öffentliche Adresse und Portnummer von AVG. Die VIP von AVG.

Table continues…

Wert	Beschreibung
Lokaler UDP-Endpunkt	UDP wird vom SSL VPN-Dienst nicht unterstützt. Der Wert ist 0.
Entfernter UDP-Endpunkt	UDP wird vom SSL VPN-Dienst nicht unterstützt. Der Wert ist 0.

Verwandte Links

Anzeigen des Tunnel-Status auf Seite 79

Tunnel-Status-Feldbeschreibungen: Detailtabelle

System Status Application (SSA) zeigt die folgenden Details für den SSL VPN-Dienst an:

Wert	Beschreibung
Name des Dienstes	Der Name des in IP Office konfigurierten Dienstes.
Status des Dienstes	Gibt an, ob SSL VPN betriebsbereit oder im Ausweichbetrieb ist.
Kontoname	Der Kontoname des SSL VPN-Dienstes. Dieser Kontoname wird verwendet, um den SSL VPN-Dienst beim Aufbau einer Verbindung mit AVG zu authentifizieren.
Server-Adresse	Die Adresse des VPN-Gateway-Servers am Standort des Dienstanbieters. Bei der angezeigten Adresse kann es sich um eine IPv4-Adresse oder eine FQDN-Adresse handeln.
Servertyp	Der SSL VPN-Dienst wird vom Avaya VPN-Gateway unterstützt. Der Servertyp lautet AVG.
Protokoll	Der SSL VPN-Dienst nutzt für den Datentransport das Protokoll TCP. Wenn Sie bei der Konfiguration der Verbindung UDP als Protokoll verwenden, wird in dem Feld UDP angezeigt; der SSL VPN-Dienst verwendet jedoch TCP.
Zeitpunkt der letzten Verbindung	Der Zeitstempel der letzten erfolgreichen Verbindung.
Zeitpunkt der letzten Verbindungstrennung	Der Zeitstempel der letzten Verbindungsunterbrechung.
IP-Adresse des Tunnels	Die IP-Adresse des SSL VPN-Tunnels.
Subnetzmaske des Tunnels	Die Subnetzmaske des SSL VPN-Tunnels.
Gateway-Adresse des Tunnels	Die standardmäßige Gateway-IP-Adresse von IP Office.
Domäne des Tunnels	Die Adresse der Domäne des Tunnels.
Lokale TCP IP-Adresse	Die TCP IP-Adresse von IP Office.

Table continues…

Wert	Beschreibung
Lokaler TCP-Port	Der TCP-Port von IP Office. Die Port-Nummer ist dynamisch.
Entfernte TCP IP-Adresse	Die TCP IP-Adresse des AVG-Servers.
Entfernter TCP-Port	Der TCP-Port des AVG-Servers. Die standardmäßige Portnummer lautet 443.
Lokale UDP IP-Adresse	UDP wird vom SSL VPN-Dienst nicht unterstützt. Der Wert ist 0.
Lokaler UDP-Port	UDP wird vom SSL VPN-Dienst nicht unterstützt. Der Wert ist 0.
Entfernte UDP IP-Adresse	UDP wird vom SSL VPN-Dienst nicht unterstützt. Der Wert ist 0.
Entfernter UDP-Port	UDP wird vom SSL VPN-Dienst nicht unterstützt. Der Wert ist 0.
Primäre DNS-Adresse	Die Adresse des primären DNS-Servers, der in AVG konfiguriert ist. Die Adresse wird aus informativen Gründen bereitgestellt und wird nicht von IP Office verwendet.
Sekundäre DNS-Adresse	Die Adresse des sekundären DNS-Servers, der in AVG konfiguriert ist. Die Adresse wird aus informativen Gründen bereitgestellt und wird nicht von IP Office verwendet.
Primäre WINS-Adresse	Der primäre WINS, der in AVG konfiguriert ist. Die Adresse wird aus informativen Gründen bereitgestellt und wird nicht von IP Office verwendet.
Sekundäre WINS-Adresse	Der sekundäre WINS, der in AVG konfiguriert ist. Die Adresse wird aus informativen Gründen bereitgestellt und wird nicht von IP Office verwendet.
Insgesamt verpasste Heartbeats	Die zusammengefasste Anzahl der verpassten Heartbeat-Signale. Der Zähler wird auf 0 zurückgesetzt, wenn IP Office neu gestartet wird oder wenn die Bereitstellung von SSL VPN-Dienst in Manager aufgehoben wird.
Insgesamt verpasste Keepalives	Für UDP-Verbindungen werden Keepalives genutzt. UDP wird vom SSL VPN-Dienst nicht unterstützt. Der Wert ist 0.

Verwandte Links

[Anzeigen des Tunnel-Status](#) auf Seite 79

Überwachen von Alarmen mit SSA

Nutzen Sie diese Vorgehensweise, um sich die Systemfehler bezüglich des SSL VPN-Dienstes anzusehen, die in System Status Application (SSA) berichtet wurden.

Vorgehensweise

1. Nutzen Sie eine der folgenden Methoden, um SSA zu starten:
   - Starten Sie SSA über die IP Office-Admin-DVD.
   - Wählen Sie **Start > Programs > IP Office > System Status**.
   - Wählen Sie in Manager die Option **Datei > Erweitert > System Status**.
2. Wählen Sie aus der Navigationsliste **Alarme > Dienst**.

   Eine Tabelle mit den Systemfehlern wird angezeigt. Systemfehler bezüglich des SSL VPN-Dienstes werden anhand des Dienstnamens identifiziert.

Verwandte Links

Überwachen des SSL VPN-Dienstes auf Seite 79
Beschreibungen des SSA-Alarms auf Seite 83

Beschreibungen des SSA-Alarms

Die folgenden Systemfehler beziehen sich auf den SSL VPN-Dienst und werden in System Status Application (SSA) berichtet.

Name	Beschreibung
Letztes Datum des Fehlers	Datum und Uhrzeit des Alarms.
Zeitpunkte	Die Anzahl der Vorkommnisse des Alarms, seit die Steuereinheit das letzte Mal neu gestartet oder der Alarm zurückgesetzt wurde.

Table continues…

Name	Beschreibung
Fehlerbeschreibung	Die Alarme bezüglich des SSL VPN-Dienstes zeigen die folgenden Fehlermeldungen gefolgt vom Namen des SSL VPN-Dienstes an: • SSL VPN außer Betrieb aufgrund geplanter Wartungsarbeiten • SSL VPN außer Betrieb aufgrund eines nicht erreichbaren Servers oder Netzwerkfehlers • SSL VPN außer Betrieb aufgrund eines Fehlers bei der Aushandlung der TLS-Sitzung • SSL VPN außer Betrieb aufgrund eines Fehlers bei der Neuaushandlung des TLS-Sitzungsschlüssels • SSL VPN außer Betrieb aufgrund fehlender Ressourcen des IP Office • SSL VPN außer Betrieb aufgrund eines internen Fehlers in IP Office • SSL VPN außer Betrieb aufgrund zu vieler verpasster Heartbeat-Nachrichten • SSL VPN außer Betrieb aufgrund fehlgeschlagener Auflösung des FQDN des Servers • SSL VPN außer Betrieb aufgrund einer doppelten IP-Adresse, die an einer anderen Schnittstelle von IP Office erkannt wurde • SSL VPN außer Betrieb aufgrund fehlgeschlagener Authentifizierung • SSL VPN außer Betrieb aufgrund eines SOCKS-Protokollfehlers • SSL VPN außer Betrieb aufgrund eines vom Server gemeldeten Fehlers

Verwandte Links

Überwachen von Alarmen mit SSA auf Seite 83

Beheben von Problemen mit dem SSL VPN-Dienst

Sie können die von SysMonitor erfassten Informationen nutzen, um Verbindungsfehler zu beheben. SysMonitor erfasst Informationen, die beim Beheben von Problemen helfen können, wenn der SSL VPN-Dienst keine Verbindung mit AVG aufbauen kann und System Status

Application (SSA) nicht ausreichend Informationen bereitstellen kann, um die Hauptursache dafür zu identifizieren.

Nutzen Sie diese Vorgehensweise nur dann zum Sammeln von Informationen, wenn Sie von Mitarbeitern des technischen Supports dazu aufgefordert werden.

Vorgehensweise

1. Wählen Sie **Start > Programme > IP Office > Monitor**.

   SysMonitor baut eine Verbindung mit dem IP Office-Server auf und zeigt ein Systemprotokoll an.

2. Wählen Sie **Filters > Trace** (Filter > Protokoll), und klicken Sie auf die Registerkarte **VPN**.
3. Wählen Sie im Bereich „SSL VPN“ die vom technischen Support angegebenen Filter aus.
4. Klicken Sie auf **OK**.

   Das SysMonitor-Protokoll führt die Aktivität des SSL VPN-Dienstes unter dem Namen auf, den Sie für den Dienst konfiguriert haben.

Verwandte Links

Überwachen des SSL VPN-Dienstes auf Seite 79
Beschreibungen der SysMonitor-Ausgaben auf Seite 85

Beschreibungen der SysMonitor-Ausgaben

Die folgende Tabelle enthält die Filter, die Sie in SysMonitor auswählen können, und beschreibt die Ausgaben, die jeder Filter generiert. Diese Informationen sind für Mitarbeiter des technischen Supports gedacht, um Probleme mit dem SSL VPN-Dienst beheben zu können.

Name	Beschreibung
Configuration (Konfiguration)	Zeigt Informationen dazu an, wann der SSL VPN-Dienst hinzugefügt, geändert oder gelöscht wurde.
Session (Sitzung)	Zeigt Informationen über den Status des SSL VPN-Dienstes an, z. B. ob der Tunnel in Betrieb oder im Ausweichbetrieb ist oder versucht, eine Verbindung aufzubauen. Wenn eine Verbindung für den SSL VPN-Dienst besteht, werden die mit AVG ausgehandelten SSL VPN-Tunnelparameter angezeigt.
SessionState (Sitzungsstatus)	Zeigt Informationen über den Status an, in dem ein Ereignis geschehen ist. Die definierten Zustände sind: Idle (Ruhend), Connecting (Verbindung wird aufgebaut), Connected (Verbunden), Disconnecting (Verbindung wird beendet), WaitingToStart (Auf Beginn wartend) und NeedsRestart (Neustart erforderlich).

Table continues…

Name	Beschreibung
Fsm	Wird für UDP-Verbindungen genutzt. UDP wird vom SSL VPN-Dienst nicht unterstützt, und es wird keine Ausgabe generiert.
Socks	Zeigt die SOCKS-Stack-Ereignisse an, die von den Signalisierungsnachrichten ausgelöst werden.
SocksState (Socks-Status)	Zeigt die internen Status des SOCKS-Stack an, wenn SOCKS5-Signalisierungsnachrichten verarbeitet werden.
Heartbeat	Zeigt Informationen darüber an, wann Heartbeat-Nachrichten gesendet und empfangen wurden.
Keepalive	Wird für UDP-Verbindungen genutzt. UDP wird vom SSL VPN-Dienst nicht unterstützt, und es wird keine Ausgabe generiert.
SignalingPktRx (SignalisierungsPktEmpfang)	Zeigt einen Byte-Stream von SOCKS-Signalisierungspaketen an, die von AVG empfangen wurden.
SignalingPktTx (SignalisierungsPktSendung)	Zeigt einen Byte-Stream von SOCKS-Signalisierungspaketen an, die an AVG gesendet wurden.
DataPktRx (Datenpaketempfang)	Zeigt eine Teilmenge des Datagramms an, die mit dem Datenpaket beginnt, die der SSL VPN-Tunnel von AVG empfangen und an das IP Office-System weitergegeben hat.
DataPktTx (Datenpaketsendung)	Zeigt eine Teilmenge des Datagramms an, die mit dem Datenpaket beginnt, die die SSL VPN-Tunnelschnittstelle an AVG gesendet hat.
TunnelInterface (Tunnelschnittstelle)	Zeigt Informationen über die Interaktionen zwischen der SSL VPN-Tunnelschnittstelle und dem IP Office-IP-Stack an.
TunnelRoutes (Tunnelrouten)	Zeigt Informationen über die Split-Tunneling-Routen an, die in IP Office installiert sind und aus der Routing-Tabelle des Produkts gelöscht wurden.

Verwandte Links

[Beheben von Problemen mit dem SSL VPN-Dienst](#) auf Seite 84

Kapitel 12: Wartung des SSL VPN-Dienstes

Dieser Abschnitt beschreibt die Aufgaben, die regelmäßig durchgeführt werden, nachdem der SSL VPN-Dienst konfiguriert und angebunden wurde.

Nutzen Sie die Informationen in diesem Abschnitt, um die folgenden Wartungsaufgaben durchzuführen:

- Deaktivieren und Aktivieren des Tunnels
- Ändern des Kennworts für das SSL VPN-Konto

Verwandte Links

Aktivieren und Deaktivieren des Dienstes auf Seite 87
Zurücksetzen des Kennworts auf Seite 93

Aktivieren und Deaktivieren des Dienstes

Nach der Konfiguration des SSL VPN-Dienstes können Sie die folgenden Oberflächen nutzen, um den Tunnel zu aktivieren oder zu deaktivieren.

- Manager
- System Status Application(SSA)
- Auf Avaya Tischtelefonen gewählte Funktionscodes
- Programmierbare Tasten auf unterstützten Avaya Tischtelefonen
- Eine auf Embedded Voicemail- oder Voicemail Pro-Systemen konfigurierte automatische Weitervermittlung
- Satzbasierte Verwaltung auf unterstützten Avaya Tischtelefonen

Die zur Verfügung stehenden Methoden hängen von dem verwendeten Betriebsmodus ab.

Die folgende Tabelle führt die Methoden auf, die in jedem Betriebsmodus unterstützt werden:

Methode	Betriebsmodus			
	Essential Edition	IP Office Server Edition	Erweiterungssystem Server Edition	Basic Edition
Manager	✔	✔	✔	—
SSA	✔	✔	✔	—
Auf Avaya Tischtelefonen gewählte Funktionscodes	✔	✔	✔	—
Programmierbare Tasten auf unterstützten Avaya Tischtelefonen	✔	✔	✔	—
Automatischer Weiterleitung auf Embedded Voicemail- oder Voicemail Pro-Systemen	✔	✔	✔	—
Satzbasierte Verwaltung	—	—	—	✔

Verwandte Links

Wartung des SSL VPN-Dienstes auf Seite 87
Aktivieren des Dienstes mit Manager auf Seite 88
Deaktivieren des Dienstes mit Manager auf Seite 89
Aktivieren des Dienstes mit SSA auf Seite 89
Deaktivieren des Dienstes mit SSA auf Seite 90
Aktivieren des Dienstes über einen Funktionscode auf Seite 90
Deaktivieren des Dienstes über einen Funktionscode auf Seite 91
Aktivieren und Deaktivieren des Dienstes mit satzbasierter Verwaltung auf Seite 91
Aktivieren und Deaktivieren des Dienstes mit programmierbaren Tasten auf Seite 92

Aktivieren des Dienstes mit Manager

Nutzen Sie diese Vorgehensweise, um den SSL VPN-Dienst über die Manager-Oberfläche zu aktivieren. Nutzen Sie zum Konfigurieren eines Server Edition-Systems den IP Office Manager for Server Edition-Modus.

Vor dem Beginn muss der SSL VPN-Dienst den Status „Im Ausweichbetrieb“ haben.

Vorgehensweise

1. Klicken Sie in der Navigationsliste mit der rechten Maustaste auf **Dienst**.

   Die Liste wird aufgeklappt und zeigt die Dienste an, die im System konfiguriert sind.
2. Wählen Sie den SSL VPN-Dienst aus, den Sie aktivieren möchten.
3. Wählen Sie die Registerkarte **Ausweichbetrieb**, und deaktivieren Sie die Option **Im Ausweichbetrieb**.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf das Symbol **Speichern**, um die Konfiguration zu speichern.

Verwandte Links

Aktivieren und Deaktivieren des Dienstes auf Seite 87

Deaktivieren des Dienstes mit Manager

Nutzen Sie diese Vorgehensweise, um den SSL VPN-Dienst über die Manager-Oberfläche zu deaktivieren. Nutzen Sie zum Konfigurieren eines Server Edition-Systems den IP Office Manager for Server Edition-Modus.

Vor dem Beginn muss der SSL VPN-Dienst den Status „Betriebsbereit“ haben.

Vorgehensweise

1. Klicken Sie in der Navigationsliste mit der rechten Maustaste auf **Dienst**.

   Die Liste wird aufgeklappt und zeigt die Dienste an, die im System konfiguriert sind.
2. Wählen Sie den SSL VPN-Dienst aus, den Sie deaktivieren möchten.
3. Wählen Sie die Registerkarte **Ausweichbetrieb**, und deaktivieren Sie die Option **Im Ausweichbetrieb**.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf das Symbol **Speichern**, um die Konfiguration zu speichern.

Verwandte Links

Aktivieren und Deaktivieren des Dienstes auf Seite 87

Aktivieren des Dienstes mit SSA

Nutzen Sie diese Vorgehensweise, um den SSL VPN-Dienst über die System Status Application (SSA)-Oberfläche zu aktivieren. Vor dem Beginn muss der SSL VPN-Dienst den Status „Im Ausweichbetrieb“ haben.

Vorgehensweise

1. Nutzen Sie eine der folgenden Methoden, um SSA zu starten:
   - Starten Sie SSA über die IP Office-Admin-DVD.
   - Wählen Sie **Start > Programs > IP Office > System Status**.

- Wählen Sie in Manager die Option **Datei > Erweitert > System Status**.

2. Wählen Sie in der Navigationsliste **IP-Netzanbindung > SSL VPN**.
3. Wählen Sie aus der Liste den SSL VPN-Dienst aus, den Sie aktivieren möchten.
4. Klicken Sie auf die Schaltfläche **Auf "Betriebsbereit" setzen**.

   Der Status wird in „Betriebsbereit“ geändert.

Verwandte Links

Aktivieren und Deaktivieren des Dienstes auf Seite 87

Deaktivieren des Dienstes mit SSA

Nutzen Sie diese Vorgehensweise, um den SSL VPN-Dienst über die System Status Application (SSA)-Oberfläche zu deaktivieren. Vor dem Beginn muss der SSL VPN-Dienst den Status „Betriebsbereit“ haben.

Vorgehensweise

1. Nutzen Sie eine der folgenden Methoden, um SSA zu starten:
   - Starten Sie SSA über die IP Office-Admin-DVD.
   - Wählen Sie **Start > Programs > IP Office > System Status**.
   - Wählen Sie in Manager oder IP Office Manager for Server Edition die Option **Datei > Erweitert > System Status**.
2. Wählen Sie in der Navigationsliste **IP-Netzanbindung > SSL VPN**.
3. Wählen Sie aus der Liste den SSL VPN-Dienst aus, den Sie aktivieren möchten.
4. Klicken Sie auf die Schaltfläche **Auf "Im Ausweichbetrieb" setzen**.

   Ein Bestätigungsdialogfeld wird angezeigt.
5. Klicken Sie auf **Ja**.

   Das System generiert einen Alarm, um zu bestätigen, dass der SSL VPN-Dienst deaktiviert ist.
6. Um den Alarm anzusehen, wählen Sie aus der Navigationsliste **Alarme > Dienst** aus.

   Die Warnung zeigt die folgende Meldung, gefolgt vom Namen des Dienstes, an: „SSL VPN außer Betrieb aufgrund geplanter Wartungsarbeiten“.

Verwandte Links

Aktivieren und Deaktivieren des Dienstes auf Seite 87

Aktivieren des Dienstes über einen Funktionscode

Nutzen Sie diese Vorgehensweise, um den SSL VPN-Dienst durch das Wählen eines Funktionscodes auf einem Tischtelefon zu aktivieren. Vor dem Beginn muss der SSL VPN-Dienst den Status „Im Ausweichbetrieb“ haben.

Voraussetzungen

Diese Funktion steht nur zur Verfügung, wenn der Systemadministrator im IP Office-System Funktionscodes konfiguriert hat. Weitere Informationen finden Sie unter Konfigurieren von Funktionscodes auf Seite 44. Vor dem Beginn müssen Sie die Nummer kennen, die der Systemadministrator im Funktionscode zur Identifikation des SSL VPN-Dienstes konfiguriert hat.

Vorgehensweise

Geben Sie auf einem mit dem IP Office-System verbundenen Tischtelefon ***775*x*1** ein. *x* steht hierbei für eine Instanz des SSL VPN-Dienstes und kann zwischen 1 und 9 liegen. Wenn der Systemadministrator den Funktionscode beispielsweise so konfiguriert hat, dass **1** den SSL VPN-Dienst identifiziert, dann müssen Sie ***77511** eingeben.

Die SSL VPN-Verbindung erhält den Status „Betriebsbereit“.

Verwandte Links

Aktivieren und Deaktivieren des Dienstes auf Seite 87

Deaktivieren des Dienstes über einen Funktionscode

Nutzen Sie diese Vorgehensweise, um den SSL VPN-Dienst durch das Wählen eines Funktionscodes auf einem Tischtelefon zu deaktivieren. Vor dem Beginn muss der SSL VPN-Dienst den Status „Betriebsbereit“ haben.

Voraussetzungen

Diese Funktion steht nur zur Verfügung, wenn der Systemadministrator im IP Office-System Funktionscodes konfiguriert hat. Weitere Informationen finden Sie unter Konfigurieren von Funktionscodes auf Seite 44. Vor dem Beginn müssen Sie die Nummer kennen, die der Systemadministrator im Funktionscode zur Identifikation des SSL VPN-Dienstes konfiguriert hat.

Vorgehensweise

Geben Sie auf einem mit dem IP Office-System verbundenen Tischtelefon ***775*x*0** ein. *x* steht hierbei für eine Instanz des SSL VPN-Dienstes und kann zwischen 1 und 9 liegen. Wenn der Systemadministrator den Funktionscode beispielsweise so konfiguriert hat, dass **1** den SSL VPN-Dienst identifiziert, dann müssen Sie ***77510** eingeben.

Die SSL VPN-Verbindung erhält den Status „Im Ausweichbetrieb“.

Verwandte Links

Aktivieren und Deaktivieren des Dienstes auf Seite 87

Aktivieren und Deaktivieren des Dienstes mit satzbasierter Verwaltung

Auf einigen Modellen von Avaya Telefonen können Sie Funktionstasten nutzen, um den SSL VPN-Dienst zu aktivieren und zu deaktivieren. Dieser Abschnitt bietet Informationen über diese Funktion und die Telefone, die sie unterstützen.

Voraussetzungen

Bevor die Funktion zur Verfügung steht, müssen für den Benutzer „Systemtelefonrechte“ konfiguriert werden. Informationen zum Einrichten von Systemtelefonrechten finden Sie in *IP Office Manager*.

Die Telefone müssen an einen der beiden ersten Ports auf der ersten Karte der IP500 V2-Plattform angeschlossen werden.

Informationen zu diesem Vorgang

Sie können Funktionstasten nutzen, um den SSL VPN-Dienst auf den folgenden Avaya Telefonen zu aktivieren und zu deaktivieren:

- ETR 18D- und ETR 34D-Tischtelefone
- Digitales Tischtelefon Modell 1416
- Digitales Tischtelefon Modell 1408
- Digitale Tischtelefone der Serie 9504
- Digitale Tischtelefone der Serie 9508
- Digitale Tischtelefone der Serien T7316 und 7316E
- Digitale Tischtelefone der Serien M7310 und 7324

Die folgende Vorgehensweise stellt eine allgemeine Anleitung dar, wie Sie auf diesen Telefonen auf die SSL VPN-Funktion zugreifen können. Detaillierte Informationen über die Menüoptionen finden Sie im Benutzerhandbuch Ihres Telefons.

Vorgehensweise

1. Welche Menüs Sie zum Zugriff auf die SSL VPN-Funktion benötigen, hängt vom Telefonmodell ab, das Sie verwenden. Nutzen Sie eine der folgenden Methoden, um auf die SSL VPN-Funktion zuzugreifen:
   - Wählen Sie **Admin > Systemverwaltung > Systemparameter**, und scrollen Sie zum SSL VPN-Dienst.
   - Wählen Sie **Admin > Funktion**, und scrollen Sie zum SSL VPN-Dienst.
   - Wählen Sie **Admin**, und drücken Sie auf **#775**, um auf das SSL VPN-Menü zuzugreifen.
2. Drücken Sie die entsprechende Funktionstaste, um den Dienst zu aktivieren oder zu deaktivieren.

Verwandte Links

Aktivieren und Deaktivieren des Dienstes auf Seite 87

Aktivieren und Deaktivieren des Dienstes mit programmierbaren Tasten

Einige Modelle der Avaya Telefone bieten programmierbare Tasten. Sie können diese Tasten als Schnellzugriff nutzen, damit Sie keinen Funktionscode eingeben oder durch Menüs auf der Telefonoberfläche navigieren müssen, um eine Funktion zu aktivieren. Ihr Systemadministrator kann eine programmierbare Taste konfigurieren, mit der Sie den SSL VPN-Dienst aktivieren und deaktivieren können.

Wenn Ihr Systemadministrator auf Ihrem Telefon eine programmierbare Taste für den SSL VPN-Dienst konfiguriert hat, wird neben der programmierbaren Taste auf Ihrem Telefon eine Beschriftung angezeigt.

Drücken Sie die Taste, um den SSL VPN-Dienst zu aktivieren (Betriebsbereit) und zu deaktivieren (Im Ausweichbetrieb).

Der Status des SSL VPN-Dienstes wird auf dem Telefon neben der Taste angezeigt. Die Art und Weise der Statusanzeige hängt vom Telefonmodell ab. Auf einigen Telefonen wird beispielsweise ein Symbol angezeigt, während andere Telefone für den Status einer Funktion LEDs verwenden. Wenn das Symbol oder die LED-Lichter angezeigt werden, ist der SSL VPN-Dienst aktiviert.

Wenn Sie auf die Taste drücken, um den SSL VPN-Dienst zu deaktivieren, wird das Symbol nicht mehr angezeigt, und die LED-Anzeige geht aus.

Verwandte Links

Aktivieren und Deaktivieren des Dienstes auf Seite 87

Zurücksetzen des Kennworts

Dieser Abschnitt beschreibt die Methoden, die Sie zum Zurücksetzen des Kennworts für den SSL VPN-Dienst verwenden können.

Es gibt zwei Methoden, um das Kennwort des SSL VPN-Dienst zurückzusetzen.

- Sie können das Kennwort in der On-Boarding-Datei ändern und neu importieren.
- Sie können das Kennwort über Manager ändern.

Bei beiden Methoden müssen Sie zusätzlich das Kennwort ändern, das auf dem RADIUS-Server für den SSL VPN-Dienst konfiguriert ist.

Verwandte Links

Wartung des SSL VPN-Dienstes auf Seite 87
Zurücksetzen des Kennworts über eine On-Boarding-Datei auf Seite 93
Zurücksetzen des Kennworts über Manager auf Seite 95

Zurücksetzen des Kennworts über eine On-Boarding-Datei

Nutzen Sie diese Vorgehensweise, wenn Sie den SSL VPN-Dienst bereits in einem IP Office-System konfiguriert haben und das Kennwort für den SSL VPN-Dienst ändern müssen.

Führen Sie diese Aktionen beim Kunden über die Avaya IP Office Web Manager-Oberfläche aus.

Voraussetzungen

Vor dem Beginn müssen Ihnen folgenden Informationen vorliegen:

- der SSL VPN-Dienstname
- der Kontoname, der verwendet wird, um den SSL VPN-Dienst beim Aufbau einer Verbindung mit AVG zu authentifizieren

Sie können System Status Application (SSA) verwenden, um den SSL VPN-Dienstnamen und den Kontonamen herauszufinden. Weitere Informationen finden Sie unter Anzeigen des Tunnel-Status auf Seite 79.

Darüber hinaus müssen Sie das Kennwort des SSL VPN-Dienstes auf dem RADIUS-Server zurücksetzen.

Vorgehensweise

1. Wählen Sie **Extras > On-Boarding**.

   Das Dialogfeld „On-Boarding“ wird angezeigt.

2. Klicken Sie auf **Ändern**.

   Ein Browser wird geöffnet und bringt Sie auf die Avaya Website.

3. Melden Sie sich an der Website an.

   Die Seite „IP Office Remote Connectivity / Password Management“ (Remote-Verbindungen / Passwortverwaltung) wird angezeigt.

4. Klicken Sie auf **Existing IP Office SSL VPN Remote Connectivity** (Bestehende IP Office SSL VPN-Remote-Verbindungen).

5. Wählen Sie **Password Reset** (Kennwort zurücksetzen).

   Der standardmäßige SSL VPN-Dienstname wird angezeigt.

6. Überprüfen Sie, ob der angezeigte Dienstname mit dem Namen des SSL VPN-Dienstes übereinstimmt, für den Sie das Kennwort zurücksetzen wollen. Wenn der standardmäßige Dienstname dem Namen nicht entspricht, geben Sie den korrekten Dienstnamen ein.

7. Geben Sie den Namen des SSL VPN-Kontos ein.

8. Klicken Sie auf **Submit** (Senden).

9. Wählen Sie aus, ob Sie die aktualisierte On-Boarding-Datei per E-Mail erhalten oder herunterladen möchten, und befolgen Sie die Anweisungen auf dem Bildschirm.

10. Sobald Sie die On-Boarding-Datei empfangen oder heruntergeladen haben, speichern Sie sie in Ihrem lokalen System.

11. Wechseln Sie in das Verzeichnis, in das Sie die On-Boarding-Datei gespeichert haben, und klicken Sie in der Web Manager-Oberfläche auf die Option **Hochladen**.

    Eine Nachricht bestätigt, dass die On-Boarding-Datei erfolgreich installiert wurde.

Weitere Schritte

Nachdem Sie das Kennwort zurückgesetzt haben, bestätigen Sie, dass der SSL VPN-Dienst wieder erfolgreich mit AVG verbunden ist, indem Sie die Vorgehensweise Anzeige des Tunnel-Status auf Seite 79 befolgen.

Verwandte Links

Zurücksetzen des Kennworts auf Seite 93

Zurücksetzen des Kennworts über Manager

Nutzen Sie diese Vorgehensweise, um das Kennwort des SSL VPN-Dienstes zu ändern. Führen Sie diese Aktionen beim Kunden über die Manager-Oberfläche aus. Nutzen Sie zum Konfigurieren eines Server Edition-Systems den IP Office Manager for Server Edition-Modus.

Voraussetzungen

Darüber hinaus müssen Sie das Kennwort des SSL VPN-Dienstes auf dem RADIUS-Server zurücksetzen.

Vorgehensweise

1. Wählen Sie in der Navigationsliste **Dienst**.
2. Wählen Sie den Namen des SSL VPN-Dienstes aus.
3. Wählen Sie die Registerkarte **Sitzung**, und geben Sie das neue Kennwort für das SSL VPN-Servicekonto in das Feld **Kontokennwort** ein.
4. Geben Sie das Kennwort erneut in das Feld **Kennwort bestätigen** ein.
5. Klicken Sie auf **OK**.
6. Klicken Sie auf das Symbol **Speichern**, um die Konfiguration zu speichern.

Verwandte Links

Zurücksetzen des Kennworts auf Seite 93

Kapitel 13: Anhang A: AVG-Schnelleinrichtungsassistent – Beispiel

Laden Sie zum Starten des Assistenten ein neues AVG-Image. Wenn die Eingabeaufforderung `localhost login:` auf der Konsole angezeigt wird, melden Sie sich als Benutzer „admin“ mit dem Kennwort „admin“ an. Das Assistentenmenü wird geöffnet. Wählen Sie `new` und befolgen Sie die Anweisungen.

Konfigurieren der AVG-Schnittstellen

```
localhost login: admin
Password:
Alteon iSD SSL
Hardware platform: 3050-VM
Software version: 10.0.1.0

------------------------------------------------------------
[Setup Menu]
      join        - Join an existing cluster
      new         - Initialize host as a new installation
      boot        - Boot menu
      info        - Information menu
      exit        - Exit  [global command, always available]

>> Setup# new

Setup will guide you through the initial configuration.
```

```
Enter port number for the management interface [1-4]: 1
Enter IP address for this machine (on management interface): 172.16.1.5
Enter network mask [255.255.255.0]:
Enter VLAN tag id (or zero for no VLAN) [0]:
Setup a two armed configuration (yes/no) [yes]:
Enter port number for the traffic interface [1-4]: 2
Enter IP address for this machine (on traffic interface): 10.136.66.195
Enter network mask [255.255.255.0]:
Enter VLAN tag id (or zero for no VLAN) [0]:
Enter default gateway IP address (on the traffic interface): 10.136.66.1
Enter the Management IP (MIP) address: 172.16.1.6
Making sure the MIP does not exist...ok
Trying to contact gateway...ok
```

Konfigurieren der selbstsignierten Zertifikate

```
Enter a timezone or 'UTC' or 'select' [select]: UTC
Enter the current date (YYYY-MM-DD) [2014-11-20]:
Enter the current time (HH:MM:SS) [23:54:18]:
Enter NTP server address (or blank to skip):
Enter DNS server address: 198.152.7.12
   Enabled SSH (allow CLI access).
Enter a password for the "admin" user:
Re-enter to confirm:
Run VPN quick setup wizard [yes]:
Enter VPN Portal IP address: 10.136.66.196
   Using VPN device without an Alteon switch.
   Using empty DNS search list.
   Creating HTTP to HTTPS redirect server.
   Enabling HTTPS BBI on port 443.
Use self-signed certificate (yes/no) [yes]:
!!!The combined length of the following parameters may not exceed 225 bytes!!!
Country Name (2 letter code): ca
State or Province Name (full name): on
Locality Name (eg, city): ottawa
Organization Name (eg, company): smec
Organizational Unit Name (eg, section):
Common Name (eg, your name or your server's hostname): testavg
Email Address:
Subject alternative name (blank or comma separated list of
URI:<uri>, DNS:<fqdn>, IP:<ip-address>, otherName:<string>, email:<email-address
>):
Valid for days [2556 (7 years)]:
Key size (512/1024/2048/4096) [2048]:
```

Option 1: Konfigurieren eines lokalen IP-Pools

```
Use RADIUS authentication server (yes/no) [yes]: no
   Using LOCAL authentication.
Enter Lower IP address in pool range: 172.30.0.1
Enter Upper IP address in pool range: 172.30.255.254
Enter Network mask for the pool range [255.255.255.0]: 255.255.0.0
```

Option 2: Konfigurieren des RADIUS-Servers

```
Use RADIUS authentication server (yes/no) [yes]:
Use generic RADIUS server configuration parameters (yes/no) [yes]:
Enter RADIUS server IP address: 172.16.1.2
Enter shared secret:
Re-enter to confirm:
```

Konfigurieren des Dienstagenten-Subnetzes

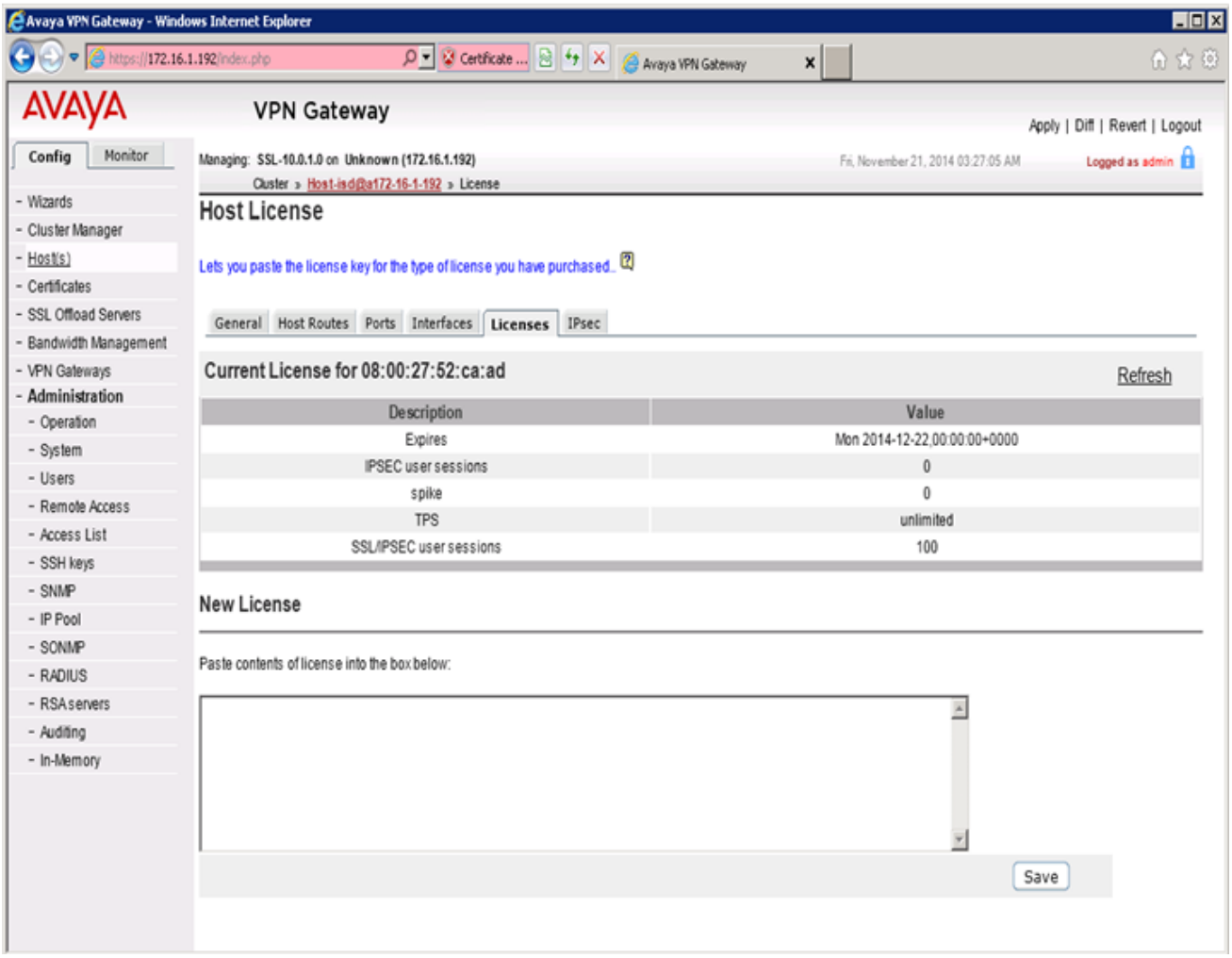
Hinweis:

Befindet sich der Dienstagent im selben Subnetz wie die AVG-Hostschnittstelle, beispielsweise 172.16.1.0 und Netzmaske 255.255.255.0, erhalten Sie eine Eingabeaufforderung für das Gateway, selbst wenn es weder konfiguriert wurde noch genutzt wird. Verfügt das Hostschnittstellen-Subnetz über ein Standard-Gateway, verwenden Sie diese Gateway-IP-Adresse (z. B. 172.16.1.1). Andernfalls geben Sie die Subnetz-Adresse erneut ein (z. B. 172.16.1.0).

```
Enter intranet network address: 172.17.1.0
Enter intranet network mask [255.255.255.0]:
Enter intranet gateway: 172.16.1.1
   Enabling network attributes.
   Enabling NetDirect.
   Enabling Split Tunnel Mode.
   Set splittun based on intranet network.
   Added a static route with intranet network.
   Creating empty portal linkset 'base-links'.
   Creating group 'trusted' with secure access.
   Creating network access rule to allow only intranet network for group 'truste
d'.
   Asigning portal linkset 'base-links' to group 'trusted'.
   Creating group 'ipoffice' with secure access.
   Creating network access rule to allow only intranet network for group 'ipoffi
ce'.
   Asigning portal linkset 'base-links' to group 'ipoffice'.
Initializing system.....
```

Hinzufügen der SSL VPN-Lizenz

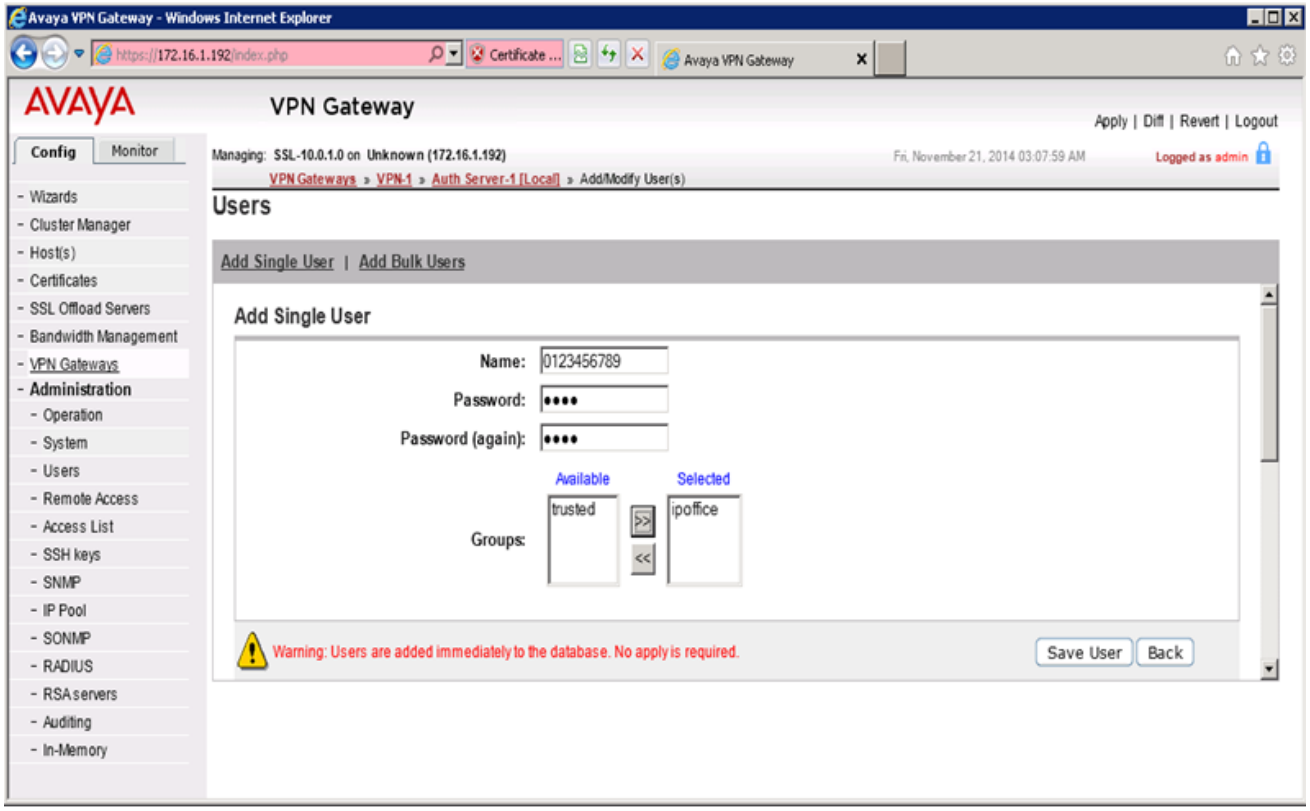
Melden Sie sich bei der AVG-Benutzeroberfläche an, um eine Lizenz hinzufügen.



Hinzufügen eines Benutzers

Damit ist die Konfiguration abgeschlossen.

Sofern Sie Option 1, „Konfigurieren eines lokalen IP-Pools“, verwendet haben, können Sie jetzt Benutzer der lokalen AVG-Datenbank hinzufügen. Benutzer müssen Teil der Gruppe **ipoffice** sein.



Kapitel 14: Anhang B: Änderung des Standard-AVG für SSL VPN (mit Bildschirmfotos)

Nach Ausführung der Konfigurationsassistenten für Schnelleinstellung und Net Direct muss die Standardkonfiguration geändert werden, um eine SSL VPN-Verbindung mit einem IP Office-System zu unterstützen.

Nutzen Sie zum Durchführen der Aktionen die browserbasierte Oberfläche (Browser-Based Interface, BBI) von AVG. Siehe *Avaya VPN Gateway BBI Application Guide* (BBI-Anwendungsleitfaden).

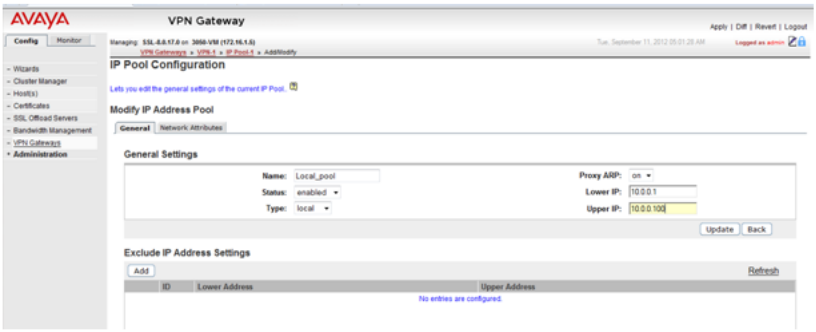
Voraussetzungen

Vergewissern Sie sich, dass das im AVG konfigurierte Standard-Gateway auf ICMP-Anfragen antwortet. Falls das Standard-Gateway nicht auf ICMP-Anfragen reagiert, kann das AVG keine VPN-Dienste bereitstellen.

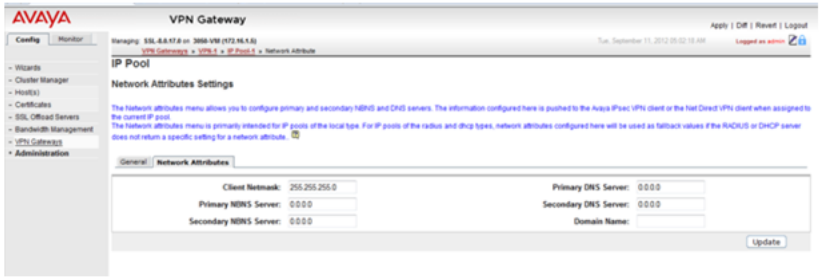
Vorgehensweise

1. Melden Sie sich als Administrator bei der BBI des AVG an.
2. Wählen Sie im linken Navigationsfenster die Registerkarte **Config** (Konfig.) und dann **VPN Gateway** > **VPN1** > **IP Pool**.
3. Das Standard-VPN aus der grundlegenden AVG-Konfiguration hat eventuell bereits einen lokalen Pool. Falls nicht, müssen Sie dem Standard-VPN einen lokalen Pool hinzufügen. Fügen Sie dem Standard-VPN auf der Seite **Add new IP Address Pool** (Neuen IP-Adressenpool hinzufügen) einen lokalen Pool hinzu.

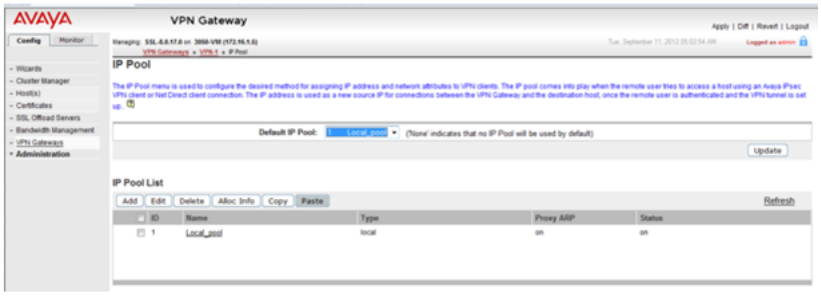
4. Überprüfen Sie auf der Seite **Modify IP Address Pool** (IP-Adressenpool ändern), ob die Werte in den Feldern **Lower IP** (Untere IP) und **Upper IP** (Obere IP) mit den Werten übereinstimmen, die mit dem Net Direct-Konfigurationsassistenten eingestellt wurden.



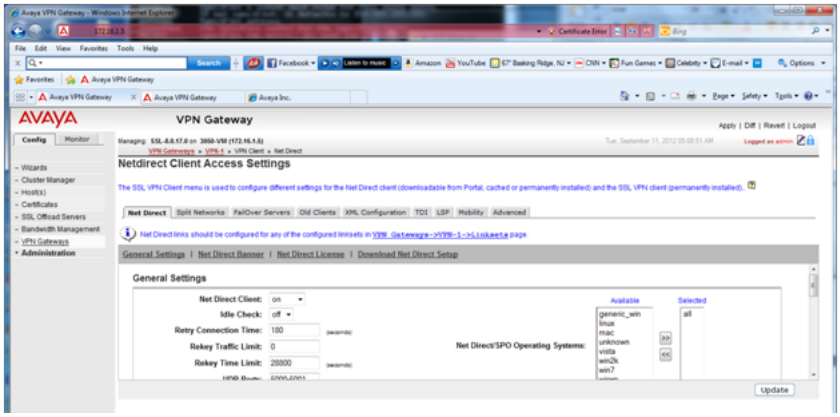
5. Wählen Sie auf der Seite **IP Pool** > **Network Attributes Settings** (IP-Pool > Netzwerkattributeinstellungen) die Registerkarte **Network Attributes** (Netzwerkattribute), und geben Sie die Werte für Ihr Netzwerk ein.



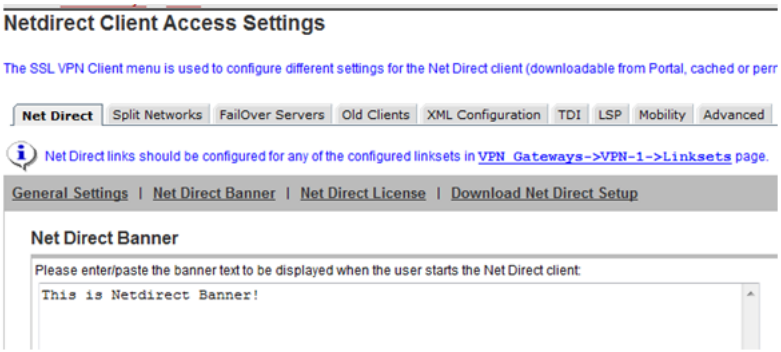
6. Stellen Sie auf der Seite **IP Pool** (IP-Pool) den in Schritt 3 erstellten lokalen Pool als **Default IP Pool** (Standard-IP-Pool) ein.



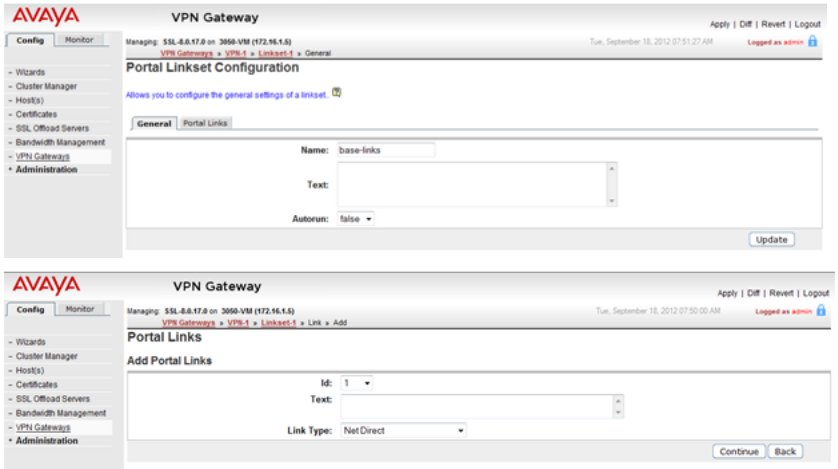
7. Überprüfen Sie auf der Seite**Net Direct Client Access Settings** (Zugangseinstellungen Net Direct Client) die mit dem Net-Direct-Konfigurationsassistenten vorgenommenen Einstellungen.
    a. Vergewissern Sie sich, dass **Idle Check** (Inaktivitätsprüfung) auf **off** (aus) gestellt ist.



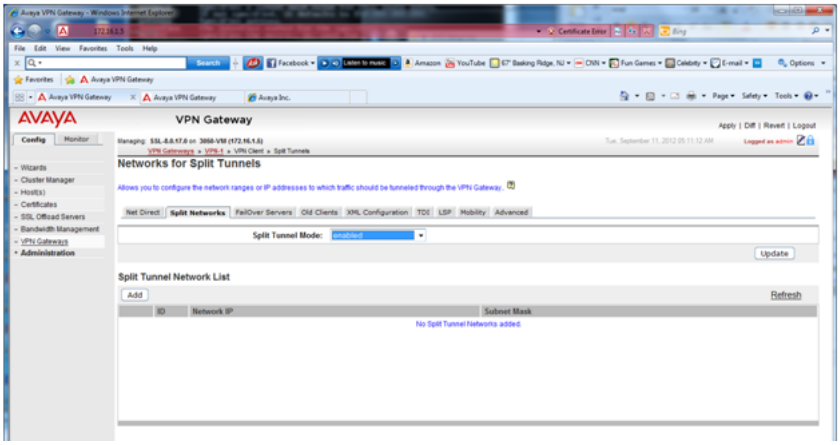
b. Vergewissern Sie sich, dass das Net Direct-Banner eingestellt ist.



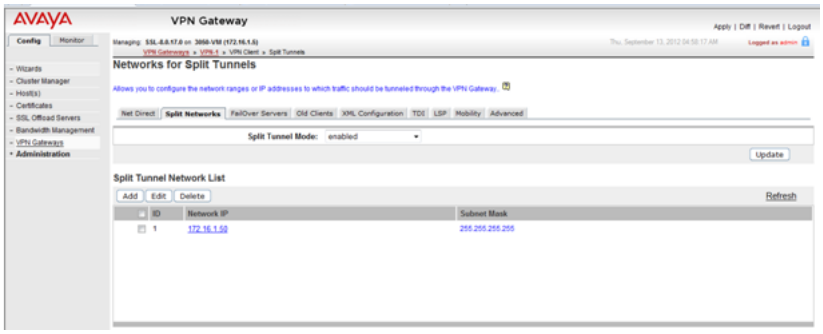
8. Stellen Sie die Portalverbindung für den Aufruf des Net Direct-Clients ein. Wählen Sie auf der Seite **Portal Linkset Configuration** (Konfiguration Portalverbindungen) die Registerkarte **Portal Link** (Portalverbindung). Wählen Sie **Net Direct** im Feld **Verbindungstyp**.



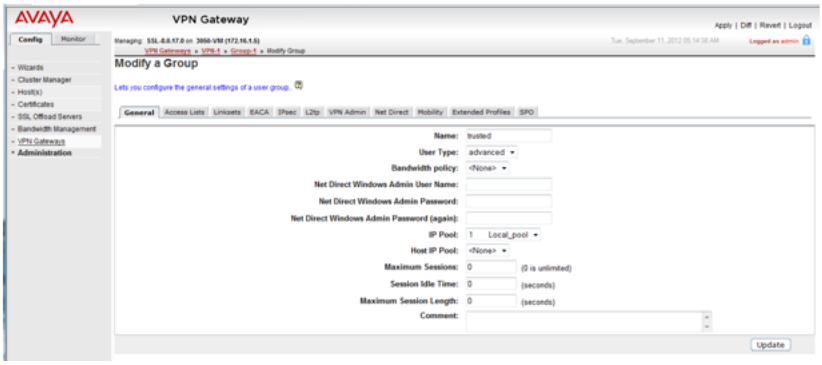
9. Auf der Seite **Networks for Split Tunnels** (Netzwerke für aufgeteilte Tunnel):
   a. Stellen Sie **Split Tunnel Mode** (Aufgeteilter Tunnelmodus) auf **Aktiviert.**



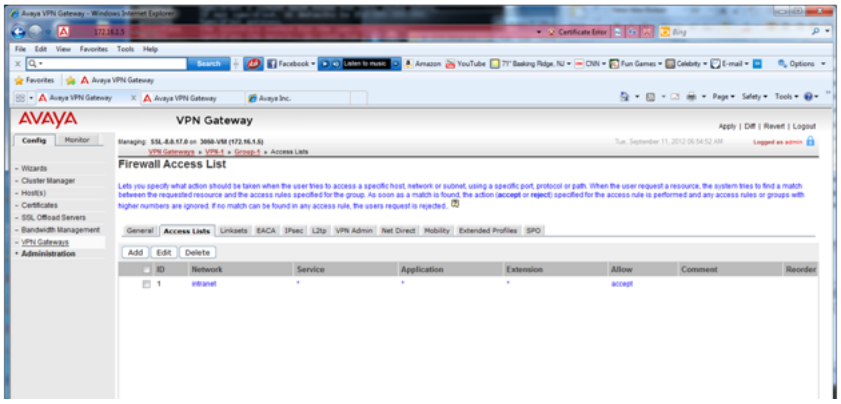
b. Stellen Sie die aufgeteilten Tunnelrouten so ein, dass der Dienstagent im privaten Netzwerk erreicht wird.



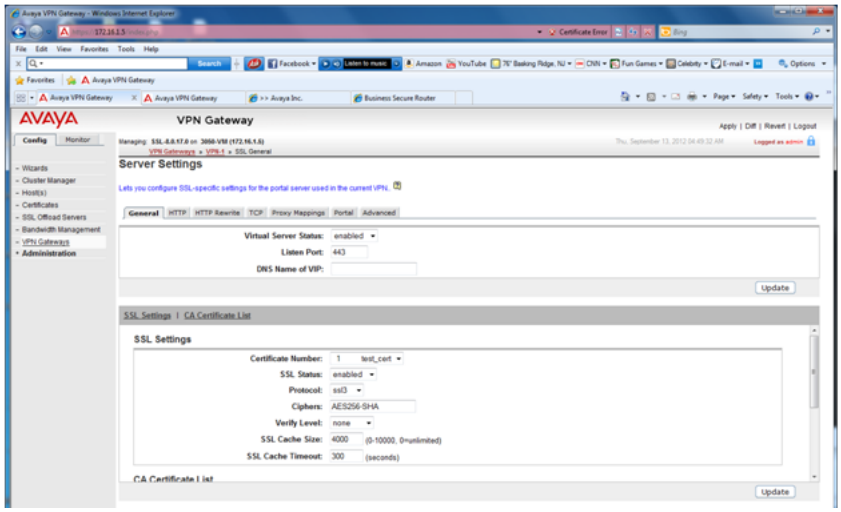
10. Für VPN1: Rufen Sie die Gruppenseite auf, und wählen Sie **Group1** (Gruppe1). Stellen Sie auf der Seite **Modify a Group** (Gruppe ändern) als IP-Pool den in Schritt 3 erstellten lokalen Pool ein.



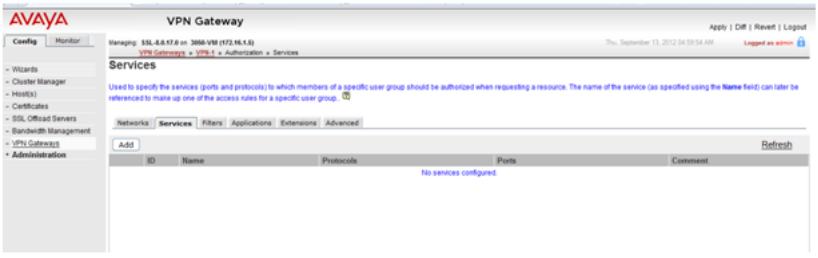
11. Rufen Sie die Seite **VPN1** > **Group1** > **Access Lists** (VPN1 > Gruppe1 > Zugriffslisten) auf. Erstellen Sie auf der **Firewall Access List** (Firewall-Zugriffsliste) eine Zugriffsregel, falls eine solche nicht standardmäßig erstellt wurde.



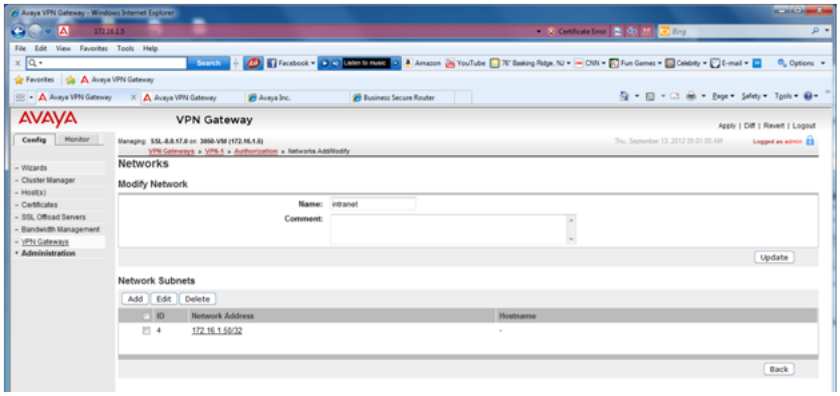
12. Rufen Sie die Seite **VPN1** > **SSL** auf. Stellen Sie auf der Seite **Server Settings** (Servereinstellungen) unter **SSL Settings** (SSL-Einstellungen) für die **Ciphers** (Chiffren) den Wert **AES256-SHA** ein, um eine sichere Verschlüsselung zu erhalten.



13. Rufen Sie die Seite **VPN1** > **Autorisierung** > **Dienste** auf. Entfernen Sie alle in der Standardkonfiguration eingestellten Dienste, da sie von SSL VPN nicht benötigt werden.



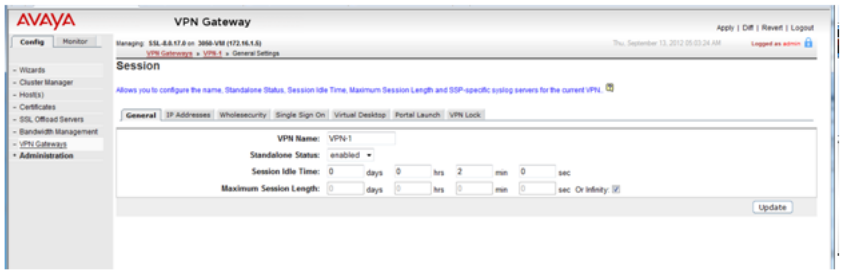
14. Rufen Sie die Seite **VPN1** > **Autorisierung** > **Networks (Netzwerke)** auf. Stellen Sie das Autorisierungsnetzwerksubnetz ein, auf das in einer der unter **VPN1** > **Group1** > **Access Lists** (VPN1 > Gruppe1 > Zugriffslisten) eingerichteten Zugriffsregeln verwiesen wird.



Hinweis:

Diese Einstellung steuert die wechselseitige Kommunikation über den SSL-VPN-Tunnel. Damit die Kommunikation aktiviert wird, muss eine Liste mit erlaubten „Intranet“-Netzwerken angegeben werden. Die Inter-VPN-Client-Kommunikation ist standardmäßig gesperrt.

15. Rufen Sie die Seite **VPN1** > **Allgemeine Einstellungen** > **Sitzung** auf. Stellen Sie die **Session Idle Time** (Inaktive Zeit der Sitzung) auf 2 Minuten ein.



Kapitel 15: Anhang C: Konfiguration der RADIUS-Authentifizierung (mit Bildschirmfotos)

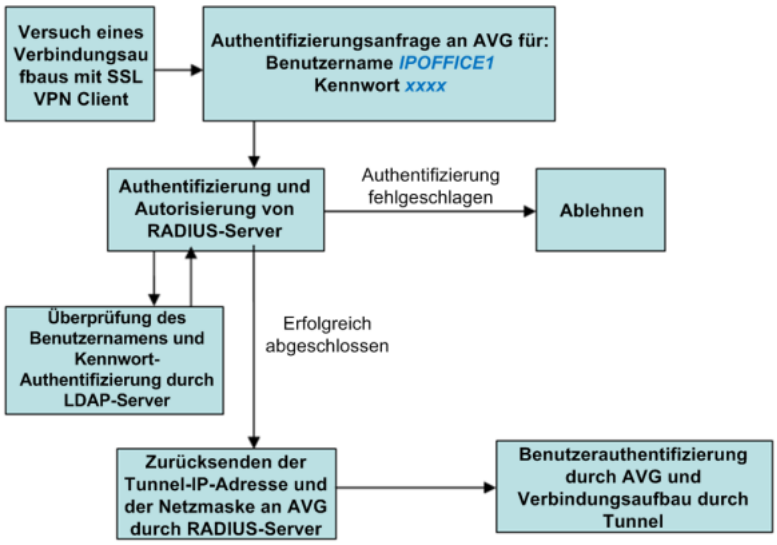
Der Hauptvorteil der RADIUS-Authentifizierung besteht darin, dass der SSL VPN-Dienst immer die gleiche Tunnel-IP-Adresse zugewiesen bekommt.

Zur Konfiguration der RADIUS-Authentifizierung müssen Sie einen RADIUS-Server installieren. Avaya empfiehlt die Avaya Identity Engine für einen Radius-Server. Informationen und Software zum Herunterladen finden Sie unter http://support.avaya.com.

RADIUS-Protokollauthentifizierungsinformationen wie Daten von Benutzerkonten und SSL VPN-Tunneldaten wie IP-Adresse und Netzmaske müssen in einer Datenbank gespeichert werden. Es gibt zwei mögliche Optionen:

- Verwenden Sie die lokale Datenbank der Identity Engine zur Speicherung der Benutzerdaten und Bereitstellung von Durchsuchungs-, Authentifizierungs- und Autorisierungsdiensten. Diese Option kann bei einer kleinen Anzahl von Benutzern verwendet werden. Bei der Identity Engine ist die Anzahl der Benutzer stark eingeschränkt. Den exakten Wert finden Sie in der Dokumentation.
- Verwenden Sie einen LDAP-Server für die Speicherung der Anmeldedaten und SSL VPN-Tunneldaten für Durchsuchungs- und Authentifizierungsdienste. Diese Option kann bei Bereitstellungsszenarien mit einer großen Anzahl von Benutzern eingesetzt werden.

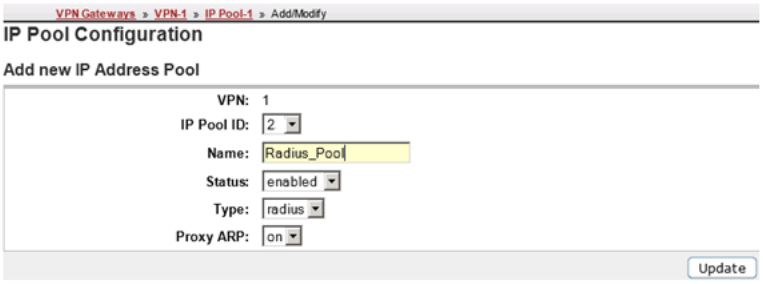
Die Dokumentation zum Radius-Server für die Avaya Identity Engine enthält Konfigurationsoptionen für LDAP-Servers verschiedener Hersteller, die bei der Installation hilfreich sind. Die RADIUS-Authentifizierung mittels LDAP-Server wird in der folgenden Abbildung veranschaulicht. Bitte beachten Sie, dass in dieser RADIUS-Serverkonfiguration bei diesem Verfahren kein LDAP-Server erforderlich ist.



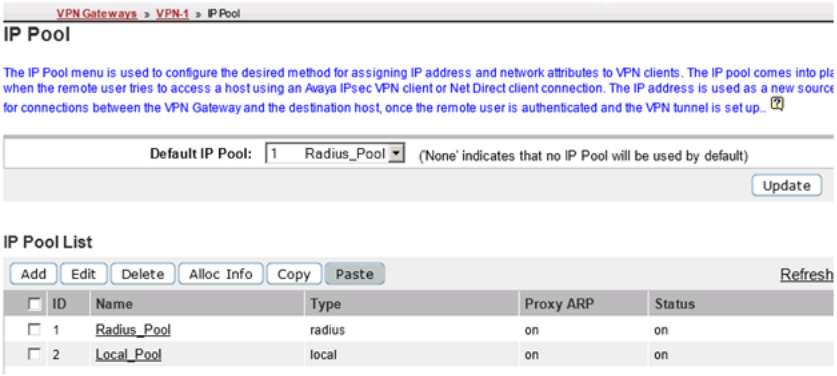
Dieses Verfahren behandelt die manuellen Schritte für die Konfiguration der RADIUS-Authentifizierung. Alternativ können Sie die Authentifizierung auch mit dem AVG-Authentifizierungsassistenten konfigurieren.

Vorgehensweise

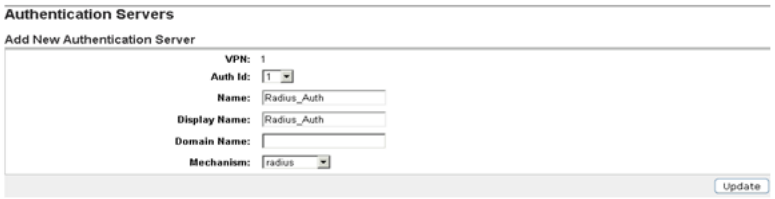
1. Melden Sie sich als Administrator bei der BBI des AVG an.
2. Fügen Sie auf der Seite **IP Pool Configuration** (IP-Pool-Konfiguration) einen neuen IP-Adressen-Pool für die RADIUS-Authentifizierung hinzu.



3. Stellen Sie auf der Seite **IP Pool** (IP-Pool) den in Schritt 2 erstellten IP-Adressen-Pool für die RADIUS-Authentifizierung als **Default IP Pool** (Standard-IP-Pool) ein.



4. Ändern Sie das VPN. Füllen Sie auf der Seite **Authentication Servers** > **Add New Authentication Server** (Authentifizierungsserver > Neuen Authentifizierungsserver hinzufügen) die Felder für den RADIUS-Server aus.



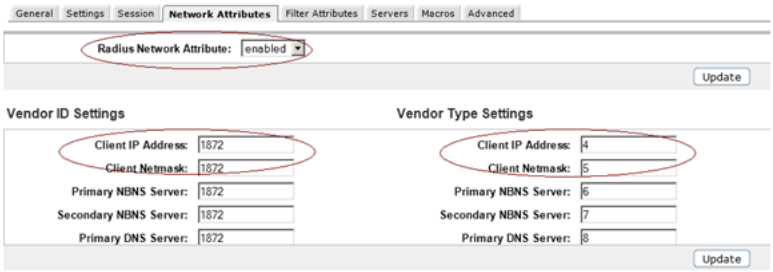
5. Konfigurieren Sie die Einstellungen des RADIUS-Authentifizierungsservers. Bitte beachten Sie, dass Hersteller-ID 1872 mit dem Hersteller Alteon verknüpft ist und das AVG bestimmt. Wählen Sie die Registerkarte **Einstellungen**, und füllen Sie die folgenden Felder aus.
   - **Vendor ID (Hersteller-ID): 1872**
   - **Vendor Type (Herstellertyp): 1**
   - **Zeitüberschreitung: 10**
   - **Vendor Id for VPN Id (Hersteller-ID für VPN-ID): 1872**
   - **Vendor Type for VPN Id (Herstellertyp für VPN-ID): 3**

6. Konfigurieren Sie die RADIUS-Netzwerkattribute. Füllen Sie auf der Registerkarte **Network Attributes** (Netzwerkattribute) die folgenden Felder aus.

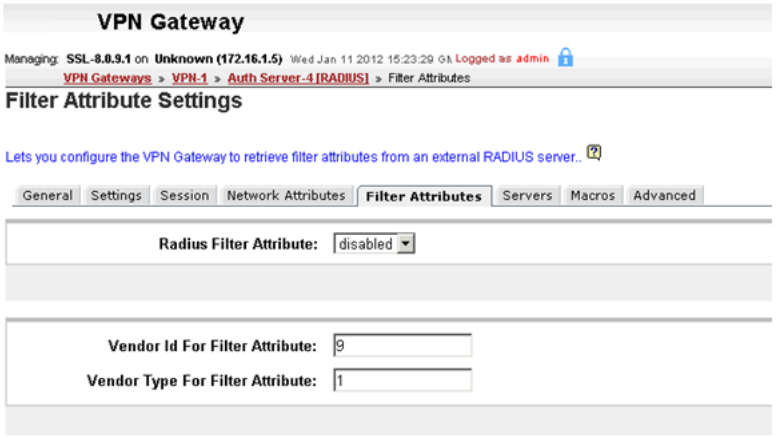
Vendor ID Settings (Einstellungen Hersteller-ID)	Vendor Type Settings (Einstellungen Herstellertyp)
Client IP Address (IP-Adresse des Clients): 1872	Client IP Address (IP-Adresse des Clients): 4
Client Netmask (Netzmaske des Clients): 1872	Client Netmask (Netzmaske des Clients): 5

Table continues…

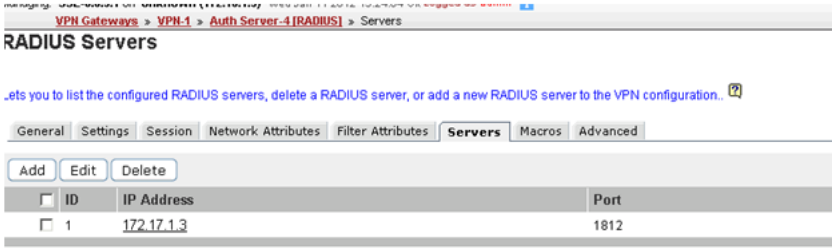
Vendor ID Settings (Einstellungen Hersteller-ID)	Vendor Type Settings (Einstellungen Herstellertyp)
Primary NBNS Server (Primärer NBNS-Server): 1872	Primary NBNS Server (Primärer NBNS-Server): 6
Secondary NBNS Server (Sekundärer NBNS-Server): 1872	Secondary NBNS Server (Sekundärer NBNS-Server): 7
Primary DNS Server (Primärer DNS-Server): 1872	Primary DNS Server (Primärer DNS-Server): 8



7. Konfigurieren Sie die Filterattribute. Füllen Sie auf der Registerkarte „Filter Attributes“ (Filterattribute) die folgenden Felder aus>.
   - **Radius filter attribute (Radius-Filterattribut): Deaktiviert**
   - **Vendor Id for Filter Attribute (Hersteller-ID für Filterattribut): 9**
   - **Vendor Type for Filter Attribute (Herstellertyp für Filterattribut): 1**

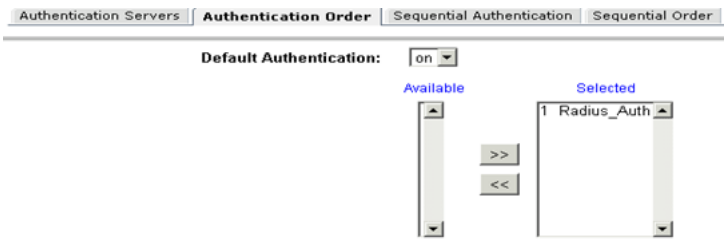


8. Geben Sie die Adresse des Radius-Servers an. Wählen Sie die Registerkarte **Server** auf der Seite **RADIUS Servers** (RADIUS-Server).



9. Klicken Sie auf **Hinzufügen**, und geben Sie auf der Seite **Modify RADIUS Server** (RADIUS-Server ändern) die IP-Adresse des RADIUS-Servers und den gemeinsamen geheimen Schlüssel an.

10. Geben Sie auf der Registerkarte **Authentication Order** (Authentifizierungsreihenfolge) die gewünschte Reihenfolge für die Authentifizierungsmethoden an.



Kapitel 16: Anhang D: AVG-Konfigurationseinstellungen

```
[Main Menu]       info       - Information menu       stats      -
Statistics menu       cfg        - Configuration menu       boot
     - Boot menu       maint      - Maintenance menu       diff
    - Show pending config changes   [global command]       apply
    - Apply pending config changes  [global command]       revert
    - Revert pending config changes [global command]       paste
    - Restore saved config with key [global command]       help
    - Show command help             [global command]       exit
    - Exit  [global command, always available]

>> Main# cfg

------------------------------------------------------------
[Configuration Menu]
      ssl        - SSL offload menu
      cert       - Certificate menu
      vpn        - VPN menu
      test       - Create test vpn, portal and certificate
      quick      - Quick vpn setup wizard
      sys        - System-wide parameter menu
      lang       - Language support
      bwm        - Bandwidth management menu
      log        - logging system menu
      ptcfg      - Backup configuration to TFTP/FTP/SCP/SFTP server
      gtcfg      - Restore configuration from TFTP/FTP/SCP/SFTP server
      dump       - Dump configuration on screen for copy-and-paste

>> Configuration# dump
Dump private/secret keys (yes/no) [no]:
Collecting data, please wait...
/*
/*
/* Alteon iSD SSL
/* Configuration dump taken Tue Sep 18 08:40:50 EDT 2012
/* Hardware Platform: 3050-VM
/* Software Version: 8.0.17.0
/* Uptime:  8 days 3 hours 59 minutes
/* IP Address: 172.16.1.4
/* Hardware Address: 00:0c:29:e0:d8:73
/* Disk space:   config         10110  386513  3 %
  user_content   32832  6015488  1 %

/*
/*
/cfg/.
/cfg/ssl/.
/cfg/ssl/server 1/.
        name "Redirect to VPN 1"
        vips 216.13.56.91
```

```
        standalone off
        port "80 (http)"
        rip 0.0.0.0
        rport 81
        type http
        proxy on
        loopback on
        fastfin off
        ena enabled
/cfg/ssl/server 1/trace/.
/cfg/ssl/server 1/ssl/.
        cert 1
        cachesize 4000
        cachettl 5m
        renegotiate legacy
        protocol ssl3
        verify none
        log none
        verifylog none
        ciphers ALL:-EXPORT:-LOW!ADH
        ena disabled
/cfg/ssl/server 1/tcp/.
        cwrite 15m
        ckeep 15m
        swrite 15m
        sconnect 30s
        csendbuf auto
        crecbuf auto
        ssendbuf auto
        srecbuf 6000
/cfg/ssl/server 1/http/.
        httpsredir on
        redirect on
        downstatus unavailable
        securecookie off
        certcard off
        cookieonce off
        sslheader on
        sslxheader off
        sslsidheader off
        addxfor off
        addvia on
        addxisd off
        addfront off
        addbeassl off
        addbeacli off
        addclicert off
        addnostore off
        nocachehdr off
        compress off
        cmsie on
        rhost off
        maxrcount 40
        maxline 16384
        urlobscure off
        sessionhdr off
/cfg/ssl/server 1/http/redirmap/.
/cfg/ssl/server 1/http/dynheader/.
/cfg/ssl/server 1/http/rewrite/.
        paramtag none
        urldeferattr on
        rewrite off
        ciphers HIGH:MEDIUM
        response iSD
        URI "/cgi-bin/weakcipher"
```

```
/cfg/ssl/server 1/http/auth/.
        mode basic
        realm Xnet
        proxy off
        ena disabled
/cfg/ssl/server 1/dns/.
/cfg/ssl/server 1/adv/.
/cfg/ssl/server 1/adv/pool/.
        timeout 15s
        ena disabled
/cfg/ssl/server 1/adv/traflog/.
        protocol bsd
        sysloghost 0.0.0.0
        udpport 514
        priority info
        facility local4
        ena disabled
/cfg/ssl/server 1/adv/loadbalancing/.
        type all
        persistence none
        metric hash
        health auto
        interval 10s
        grace on
        ena disabled
/cfg/ssl/server 1/adv/loadbalancing/script/.
/cfg/ssl/server 1/adv/loadbalancing/remotessl/.
        protocol ssl3
        ciphers ALL
/cfg/ssl/server 1/adv/loadbalancing/remotessl/verify/.
        verify none
/cfg/ssl/server 1/adv/sslconnect/.
        protocol ssl3
        cachemode on
        ciphers EXP-RC4-MD5:ALL!DH
        ena disabled
/cfg/ssl/server 1/adv/sslconnect/verify/.
        verify none
/cfg/cert 1/.
        name test_cert
        cert
-----BEGIN CERTIFICATE-----
MIIEejCCA+OgAwIBAgIJAODDyCE7V9E3MA0GCSqGSIb3DQEBBAUAMIG/MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEQMA4GA1UEBxMHVGVzdGluZzEo
MCYGA1UEChMfVGVzdCBJbmMuIDEgMDQ6Mzc6MjEgMjAxMi0wOS0xMDESMBAGA1UE
CxMJdGVzdCBkZXB0MSAwHgYDVQQDExd3d3cuZHVtbXlzc2x0ZXN0aW5nLmNvbTEp
MCcGCSqGSIb3DQEJARYadGVzdGVyQGR1bW15c3NsdGVzdGluZy5jb20wHhcNMTIw
OTEwMDgzNzIyWhcNMTMwOTEwMDgzNzIyWjCBvzELMAkGA1UEBhMCVVMxEzARBgNV
BAgTCkNhbGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoTH1Rlc3Qg
SW5jLiAxIDA0OjM3OjIxIDIwMTItMDktMTAxEjAQBgNVBAsTCXRlc3QgZGVwdDEg
MB4GA1UEAxMXd3d3LmR1bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG9w0BCQEW
GnRlc3RlckBkdW1teXNzbHRlc3RpbmcuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQCyw80A6VzNwFRpizR9iWJnvZziAgwJZBmI7V2QjtQD+7tMwZA1mNZf
JohYRRS24WGOerGJd3YtAkQHv3yWSo6NiQ5X0Ng8ou4wvg7nlhsqSjeReSn7RUPV
Jl7L45MySiLI5iKWH2j+i1NxLfLbtkqO7+RVAlM3lL4T0Lsjg4RiswIDAQABo4IB
ejCCAXYwDAYDVR0TBAUwAwEB/zARBglghkgBhvhCAQEEBAMCAkQwMgYJYIZIAYb4
QgENBCUWI0FsdGVvbi9Ob3J0ZWwgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1Ud
DgQWBBSGR0w74d4NpcyEeYyLayjiBtRc9DCB9AYDVR0jBIHsMIHpgBSGR0w74d4N
pcyEeYyLayjiBtRc9KGBxaSBwjCBvzELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNh
bGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoTH1Rlc3QgSW5jLiAx
IDA0OjM3OjIxIDIwMTItMDktMTAxEjAQBgNVBAsTCXRlc3QgZGVwdDEgMB4GA1UE
AxMXd3d3LmR1bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG9w0BCQEWGnRlc3Rl
ckBkdW1teXNzbHRlc3RpbmcuY29tggkA4MPIITtX0TcwCQYDVR0SBAIwADANBgkq
hkiG9w0BAQQFAAOBgQAMw7vnW4aWgwQZEpjWEYxzRkbAD1+vWYbtdNix9kPtHzWu
e5Fr9c4iuzSHW6cC8natTQc+8iAUNjokBpZ2PT62mENRsNjfj2Ov3/OzXuUYtwkt
```

```
OtOCddd5gM1DL6ovxM4k59VLkDYdn5p0kwknSAGHJyoUjQ3g7XWGAOffJy+Wbw==
-----END CERTIFICATE-----
...
/cfg/cert 1/revoke/.
/cfg/cert 1/revoke/automatic/.
        anonymous false
        interval 1d
        verify off
        ena disabled
/cfg/vpn 1/.
        name VPN-1
        ips 216.13.56.91
        standalone on
        hostippool false
/cfg/vpn 1/aaa/.
        idlettl 2m
        sessionttl infinity
        authorder 1
        defauth on
        defippool 1
/cfg/vpn 1/aaa/tg/.
        ena disabled
        recheck 15m
        action teardown
        details on
        runonce off
        logmode off
        loglevel info
        bypass off
/cfg/vpn 1/aaa/tg/agent/.
        timeout 2s
        minver 0.0.0.0
/cfg/vpn 1/aaa/nap/.
        autorem false
/cfg/vpn 1/aaa/nap/probation/.
        ena false
/cfg/vpn 1/aaa/nap/servers/.
/cfg/vpn 1/aaa/nap/shvs/.
        add 311 128 wshv
        add 40082 0 nshv
/cfg/vpn 1/aaa/nap/wshv/.
        firewall on
        autoupdate on
/cfg/vpn 1/aaa/nap/wshv/virus/.
        enabled false
/cfg/vpn 1/aaa/nap/wshv/spyware/.
        enabled false
/cfg/vpn 1/aaa/nap/wshv/secupdates/.
        enabled false
/cfg/vpn 1/aaa/wholesec/.
        ena false
/cfg/vpn 1/aaa/auth 1/.
        type local
        name local
/cfg/vpn 1/aaa/auth 1/local/.
        pwdage 0
        expirewarn 15
/cfg/vpn 1/aaa/auth 1/adv/.
/cfg/vpn 1/aaa/seqauth/.
        ena false
        copyuser off
        usesecond off
        retries 3
/cfg/vpn 1/aaa/network 1/.
        name intranet
```

```
/cfg/vpn 1/aaa/network 1/subnet 4/.
        net 172.16.1.50
        mask 255.255.255.255
/cfg/vpn 1/aaa/group 1/.
        name trusted
        restrict 0
        usertype advanced
        idlettl 0
        sessionttl 0
        ippool 1
/cfg/vpn 1/aaa/group 1/access 1/.
        network intranet
        service *
        appspec *
        extspec *
        action accept
/cfg/vpn 1/aaa/group 1/linkset/.
        add base-links
/cfg/vpn 1/aaa/group 1/l2tp/.
/cfg/vpn 1/aaa/group 1/ipsec/.
/cfg/vpn 1/aaa/ssodomains/.
/cfg/vpn 1/aaa/ssoheaders/.
/cfg/vpn 1/aaa/radacct/.
        ena false
/cfg/vpn 1/aaa/radacct/servers/.
/cfg/vpn 1/aaa/radacct/vpnattribute/.
        vendorid "1872 (alteon)"
        vendortype 3
/cfg/vpn 1/aaa/adv/.
/cfg/vpn 1/aaa/adv/unmatchgrp/.
        ena disabled
/cfg/vpn 1/server/.
        port "443 (https)"
        loopback on
        fastfin off
        ena enabled
/cfg/vpn 1/server/trace/.
/cfg/vpn 1/server/ssl/.
        cert 1
        cachesize 4000
        cachettl 5m
        renegotiate legacy
        protocol ssl3
        log none
        verifylog none
        ciphers AES256-SHA
        verify none
        ena enabled
/cfg/vpn 1/server/tcp/.
        cwrite 15m
        ckeep 15m
        skeep 2m
        sinterval 1m
        swrite 15m
        sconnect 30s
        csendbuf auto
        crecbuf auto
        ssendbuf auto
        srecbuf 6000
/cfg/vpn 1/server/http/.
        downstatus unavailable
        securecookie on
        certcard off
        cookieonce off
        sslheader off
```

```
        sslxheader off
        sslsidheader off
        addxfor off
        addvia on
        addxisd off
        addclicert off
        addnostore on
        nocachehdr off
        compress off
        allowimage on
        allowdoc off
        allowscript off
        allowica on
        cmsie on
        maxrcount 40
        maxline 16384
        urlobscure off
        sessionhdr off
/cfg/vpn 1/server/http/rewrite/.
        paramtag none
        urldeferattr on
        rewrite off
        ciphers HIGH:MEDIUM
        response iSD
        URI "/cgi-bin/weakcipher"
/cfg/vpn 1/server/proxymap/.
/cfg/vpn 1/server/portal/.
        wipecookies on
        cookiedb on
        resetcookie off
        persistent off
/cfg/vpn 1/server/portal/urlrewrite/.
        rewrite on
        jrewrite on
        cssrewrite on
        gziprewrite on
        ena enabled
/cfg/vpn 1/server/adv/.
/cfg/vpn 1/server/adv/traflog/.
        protocol bsd
        sysloghost 0.0.0.0
        udpport 514
        priority info
        facility local4
        ena disabled
/cfg/vpn 1/server/adv/sslconnect/.
        protocol ssl23
        cachemode on
        ciphers EXP-RC4-MD5:ALL!DH
/cfg/vpn 1/server/adv/sslconnect/verify/.
        verify none
/cfg/vpn 1/l2tp/.
        ena disabled
        cert unset
        authorder mschapv2,pap
        groupmatch true
/cfg/vpn 1/ipsec/.
        ena disabled
        cert unset
        groupmatch true
        groupbind off
/cfg/vpn 1/ipsec/sys/.
/cfg/vpn 1/ipsec/sys/failover/.
        primary 0.0.0.0
        secondary 0.0.0.0
```

```
        tertiary 0.0.0.0
/cfg/vpn 1/ipsec/sys/nat-t/.
        udpport 10001
        portswitch off
        ena false
/cfg/vpn 1/ippool 1/.
        type local
        name Local_pool
        lowerip 10.0.0.1
        upperip 10.0.0.100
        proxyarp on
        ena enabled
/cfg/vpn 1/ippool 1/exclude/.
/cfg/vpn 1/ippool 1/netattr/.
        netmask 255.255.255.0
        primnbns 0.0.0.0
        secnbns 0.0.0.0
        primdns 0.0.0.0
        secdns 0.0.0.0
/cfg/vpn 1/portal/.
        logintext
This is a configurable text.
...
        seclogtext
This is a configurable text.
...
        iconmode fancy
        linktext

...
        linkurl on
        punblock off
        linkcols 2
        linkwidth 100%
        companyname "Avaya Inc."
        smbworkgrp WORKGROUP
        autojre on
        applet on
        wiper on
        rsaauto off
        ieclear on
        citrix off
        clientauth off
        trustsite off
/cfg/vpn 1/portal/colors/.
        color1 #ececec
        color2 #ececec
        color3 #cc0000
        color4 #cc0000
/cfg/vpn 1/portal/content/.
        ena disabled
/cfg/vpn 1/portal/faccess/.
        ena disabled
        ipsecmode native
        contip 0.0.0.0
        portalmsg
From this page you can gain full network access. This
requires that Net Direct is enabled or
that you have either Avaya's IPSEC client (version 4.89 or better)
and/or SSL-VPN (TDI version 1.1 or better) client installed. If the Net Direct
installable client is installed it will be used if Net Direct is enabled.
Note: Your browser must support Java. If not download SUN's
J2SE JRE from
class="white_link" href="javascript:download_jre()">www.java.com.
Remember: You can only access resources on the network as defined by
```

```
your access rights. Contact your network operator if you are
dissatisfied with your current access rights.
...
appletmsg
The quest for full network access has started._The outcome of the quest will be indicated
in the progress bar and console window below.
...
/cfg/vpn 1/portal/lang/.
        setlang en
/cfg/vpn 1/portal/lang/beconv/.
/cfg/vpn 1/portal/whitelist/.
        ena disabled
/cfg/vpn 1/portal/whitelist/domains/.
/cfg/vpn 1/portal/blacklist/.
        ena disabled
/cfg/vpn 1/portal/blacklist/domains/.
/cfg/vpn 1/portal/usertype/.
/cfg/vpn 1/portal/usertype/novice/.
        sysinfo off
/cfg/vpn 1/linkset 1/.
        name base-links
        autorun false
/cfg/vpn 1/linkset 1/link 1/.
        href <netdirect>
        NetdirectFlag off
        type netdirect
/cfg/vpn 1/linkset 1/link 1/netdirect/.
/cfg/vpn 1/vdesktop/.
        ena off
        prelogon off
        always off
        force off
        switch off
        secure off
        persist off
        filesep off
        remdisk off
        print off
        netshare off
        cryptlevel 128
        timeout 5
        conncntrl off
/cfg/vpn 1/vdesktop/mcd/.
        ena disabled
        keylogger off
        scrscrap off
        acntcreate off
/cfg/vpn 1/vdesktop/mcd/vkeyboard/.
        ena disabled
/cfg/vpn 1/sslclient/.
        ippool off
        netdirect on
        caching off
        ndbanner
This is Netdirect Banner!
...
ndlicense
END USER LICENSE AGREEMENT
FOR AVAYA VPN CLIENT
This Software License Agreement ('Agreement') is between you, ('User') and Avaya
Corporation and its subsidiaries and affiliates ('Avaya').  PLEASE READ THE FOLLOWING
CAREFULLY.
BY CLICKING ON THE 'YES' BUTTON OR USING THIS SOFTWARE, YOU ('USER') ARE CONSENTING TO BE
BOUND BY THIS AGREEMENT BETWEEN YOURSELF AND AVAYA.  IF YOU DO NOT AGREE TO BE BOUND BY
THIS AGREEMENT, CLICK 'NO' AND DO NOT USE THIS SOFTWARE.
```

```
LICENSE GRANT: This Agreement shall govern the licensing of Avaya and Avaya licensor's
software and the accompanying user manuals, on line help services, Avaya Web Site and
other instructions (collectively, the 'Software') provided or made available to User.
The Software includes client software, which resides on the computers of User, to access
Sublicensor's networks (the 'Client Software').  The Software provided under this License
is proprietary to Avaya and to third parties from whom Avaya has acquired license
rights.  This Software was licensed in conjunction with the purchase of a 'Avaya VPN
Gateway' or other Avaya VPN device, that will give the User access to the Sublicensor's
purchaser's network and may only be used for this purpose by you.  User is hereby granted
a nonexclusive object code only license to use the Software under the following terms:
- User shall use the Software only in conjunction with the Avaya VPN Gateway or other
Avaya VPN device with which the Software was distributed.
- User may make one copy of the Software only for safekeeping (archives) or backup
purposes.
- User may not modify, translate, adapt, decompile, disassemble, decrypt, extract,
or otherwise reverse engineer or attempt to discover the source code and techniques
incorporated in the Software.  User may not create derivative works based on the Software
or any trade secret or proprietary information of Avaya.
- Title to Software shall not pass to User.
- User shall not provide, or otherwise make available, any Software, in whole or in part,
in any form, to any third party, nor shall User sublicense, rent or lease the Software.
- Upon termination or breach of this Agreement, or in the event that the Avaya device
with which it was distributed is no longer in use, User will immediately cease use of
and destroy all copies of the Software and  return the Software to Avaya or certify as
to such destruction to Avaya that is has been destroyed. Avaya and Third-party owners
from whom Avaya has acquired license rights to material that is incorporated into the
Software shall have the right to enforce the provisions of this Agreement against User.
IN NO EVENT SHALL AVAYA OR ITS  AGENTS, SUPPLIERS, MANUFACTURERS OR DISTRIBUTORS BE
LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF
BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR DATA, DAMAGES
BASED ON ANY THIRD PARTY CLAIM,  OR, OR ANY OTHER PECUNIARY LOSS ARISING OUT OF THE USE
OR INABILITY TO USE THE SOFTWARE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY
OF SUCH DAMAGES.  SOME JURISDICTIONS DO NOT ALLOW THESE LIMITATIONS OR EXCLUSIONS AND IN
SUCH EVENT THEY MAY NOT APPLY.
User agrees to comply with all export restrictions regarding the Software, and shall not
export, directly or indirectly, any Software or related technical data or information
without first obtaining any required export licenses or other governmental approvals. THE
SOFTWARE IS PROVIDED 'AS IS' WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS
OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF
USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH USER.  Avaya is not obligated to User
to provide support of any kind for the Software, and in the event it chooses to do
so, such support is subject to the terms of this Agreement.  Some jurisdictions do not
allow exclusion of implied warranties and, in such event, the above exclusions may not
apply. If User is the United States Government, the following paragraph shall apply:
All Software provided hereunder is commercial computer software and commercial computer
software documentation, as applicable, and in the event Software is licensed for or
on behalf of the United States Government, the respective rights to the Software is
governed by Avaya standard commercial license in accordance with U.S. Federal Regulations
at 48 C.F.R. Sections 12.212 (for non-DoD entities) and  48 C.F.R. 227.7202 (for DoD
entities). Software contains trade secrets and copyrighted material and User agrees to
treat the Software as confidential information using a reasonable standard of care.  User
shall not remove or obscure any copyright, patent, trademark, trade secret, or similar
intellectual property or restricted rights notice within or affixed to any Software and
shall reproduce and affix such notices on any backup copy of software. User may terminate
this Agreement at any time.  Avaya may terminate this Agreement if User fails to comply
with any of its terms.  This Agreement is the complete and exclusive agreement between
the parties hereto regarding its subject matter, and shall be governed solely by the laws
of the state of New York, without regard to its rules governing conflicts of law.
...
          oslist all
        udpports 5000-5001
        rekeytraf 0
        rekeytime 8h
        portalbind on
```

```
        idlecheck off
        keepalive 0
        recncttime 3m
        clampmss on
        splittun enabled
        tdiclient off
        lspclient off
        oldclients false
/cfg/vp
```

Index

Special Characters

A

B

D

E

F

I

K

M

N

O

P

R

S

T

U

V

W

Z