



IP Office™ Platform 12.0

Verwalten von Avaya one-X Portal for IP Office

Hinweis

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

Haftungsausschluss für Dokumentation

„DOKUMENTATION“: Dies bezieht sich auf in Form verschiedener Medien veröffentlichten Informationen, die den Benutzern allgemein zugänglich gemacht werden; hierzu können Produktinformationen, Abonnement- oder Dienstleistungsbeschreibungen, Bedienungsanleitungen und Leistungsspezifikationen gehören. Der Begriff „Dokumentation“ schließt Marketingmaterialien nicht mit ein. Avaya haftet nur dann für Änderungen, Ergänzungen oder Streichungen der ursprünglich veröffentlichten Fassung dieser Dokumentation, wenn diese Änderungen, Ergänzungen und Streichungen von oder in ausdrücklichem Auftrag von Avaya vorgenommen wurden. Der Endnutzer erklärt sich einverstanden, Avaya sowie die Handlungsbevollmächtigten, Angestellten und Beschäftigten von Avaya im Falle von Forderungen, Rechtsstreitigkeiten, Ansprüchen und Urteilen auf der Grundlage von oder in Verbindung mit nachträglichen Änderungen, Ergänzungen oder Streichungen in dieser Dokumentation zu entschädigen und von jeglicher Haftung freizustellen, sofern diese Änderungen, Ergänzungen oder Streichungen vom Endnutzer vorgenommen worden sind.

Haftungsausschluss für Links

Avaya ist nicht verantwortlich für den Inhalt oder die Korrektheit verknüpfter Websites, auf welche auf dieser Website bzw. in dieser/n von Avaya bereitgestellten Dokumentation(en) verwiesen wird. Avaya haftet nicht für die Verlässlichkeit von auf diesen Websites enthaltenen Informationen, Aussagen oder Inhalten und unterstützt nicht notwendigerweise die Produkte, Dienstleistungen oder Informationen, die auf diesen beschrieben oder angeboten werden. Avaya garantiert nicht, dass diese Links jederzeit funktionieren und hat keinen Einfluss auf die Verfügbarkeit dieser Websites.

Garantie

Avaya gewährt eine eingeschränkte Gewährleistung für Hardware und Software von Avaya. Die Bedingungen der eingeschränkten Gewährleistung können Sie Ihrem mit Avaya geschlossenen Kaufvertrag entnehmen. Darüber hinaus stehen Avaya-Kunden und Dritten die Standard-Gewährleistungsbedingungen von Avaya sowie Informationen über den Support für dieses Produkt während der Gewährleistungszeit auf der Avaya-Support-Website <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> unter dem Link „Gewährleistung und Produktlebenszyklus“ bzw. auf einer von Avaya bekannt gegebenen Nachfolgersite zur Verfügung. Beachten Sie hierbei: Bei Erwerb des Produktes/der Produkte von einem Avaya-Channel Partner außerhalb der Vereinigten Staaten und Kanada wird die Gewährleistung von diesem Avaya-Channel Partner und nicht direkt von Avaya erbracht.

„Gehostete Dienste“: Dies bezeichnet das Abonnement eines von Avaya gehosteten 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](https://support.avaya.com/licenseinfo) UNTER DEM LINK „Avaya-Nutzungsbedingungen für gehostete Dienste“ ODER ETWAIGEN VON AVAYA BEKANNT GEGEBENEN NACHFOLGSEITEN ABRUFBAR UND GELTEN FÜR ALLE PERSONEN, DIE DEN GEHOSTETEN DIENST AUFRUFEN ODER NUTZEN. INDEM SIE DEN GEHOSTETEN DIENST AUFRUFEN ODER NUTZEN ODER ANDERE DAZU AUTORISIEREN, STIMMEN SIE IN IHREM NAMEN UND IM AUFTRAG IHRER ORGANISATION (IM NACHFOLGENDEN ENTWEDER „SIE“ ODER DER „ENDNUTZER“ BEZEICHNET) DEN NUTZUNGSBEDINGUNGEN ZU. WENN SIE DEN NUTZUNGSBEDINGUNGEN IM NAMEN EINES UNTERNEHMENS ODER EINER ANDEREN RECHTSPERSON ZUSTIMMEN, GARANTIEREN SIE, DASS SIE AUTORISIERT SIND, DIESE ENTITÄT AN DIE VORLIEGENDEN NUTZUNGSBEDINGUNGEN ZU BINDEN. WENN SIE DAZU NICHT BEFUGT SIND ODER SIE DIESEN NUTZUNGSBESTIMMUNGEN NICHT ZUSTIMMEN MÖCHTEN, DÜRFEN SIE AUF DEN GEHOSTETEN DIENST WEDER ZUGREIFEN NOCH IHN NUTZEN UND NIEMANDEN AUTORISIEREN, AUF DEN GEHOSTETEN DIENST ZUZUGREIFEN ODER IHN ZU NUTZEN.

Lizenzen

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

Copyright

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

Virtualisierung

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

Komponenten von Drittanbietern

Das Folgende gilt nur, wenn der H.264 (AVC)-Codec mit dem Produkt vertrieben wird. DIESES PRODUKT WIRD IM RAHMEN DER AVC-PATENT-PORTFOLIO-LIZENZ FÜR DEN PRIVATEN ODER ANDERWEITIG UNENTGELTLICHEN GEBRAUCH DURCH ENDKUNDEN LIZENZIERT. DIE LIZENZ GEWÄHRT (i) DIE CODIERUNG VON VIDEODATEN GEMÄSS DEM AVC-STANDARD („AVC-VIDEO“) UND/ODER (ii) DIE DECODIERUNG VON AVCVIDEODATEN, 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](http://www.mpegla.com).

Dienstanbieter

FOLGENDES GILT FÜR CODECS: WENN DER AVAYA CHANNEL PARTNER PRODUKTE HOSTET, DIE DIE CODECS H.264 ODER H.265 VERWENDEN BZW. IN DIE DIESE CODECS EINGEBETTET SIND, AKZEPTIERT UND BESTÄTIGT DER AVAYA CHANNEL PARTNER, DASS ER SELBST FÜR SÄMTLICHE LIZENZ-UND/ODER ANDERE GEBÜHREN IM ZUSAMMENHANG MIT DIESEN CODECS VERANTWORTLICH IST. DER H.264 (AVC)-CODEC WIRD IM RAHMEN DER AVC-PATENT-PORTFOLIO-LIZENZ FÜR DEN PRIVATEN ODER ANDERWEITIG NENTGELTLICHEN 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](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 Ausführungsrechte in dem Land oder Gebiet, in dem das Avaya-Produkt verwendet wird.

Gebührenbetrug verhindern

„Gebührenhinterziehung“ ist die unberechtigte Nutzung Ihres Telekommunikationssystems durch eine unberechtigte Partei (z.B. Personen, die keine Angestellten, Handlungsbevollmächtigten oder Auftragnehmer sind und die nicht im Auftrag Ihrer Firma arbeiten). Sie sollten sich darüber im Klaren sein, dass Gebührenbetrug in Verbindung mit Ihrem System möglich ist und gegebenenfalls zu erheblichen zusätzlichen Gebühren für Ihre Telekommunikationsdienste führen kann.

Avaya-Hilfe bei Gebührenbetrug

Wenn Sie vermuten, dass Sie durch Gebührenbetrug schikaniert werden und technische Unterstützung oder Unterstützung benötigen, wenden Sie sich bitte an Ihren Avaya-Vertriebsmitarbeiter.

Sicherheitsrisiken

Informationen zu den Avaya-Support-Richtlinien zur Sicherheit finden Sie im Bereich „Security Policies and Support“ unter <https://support.avaya.com/security>. Verdächtige Sicherheitsschwachstellen bei Avaya-Produkten werden gemäß AvayaProduct 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 Rechtserwirkung eine Lizenz oder ein sonstiges Recht bezüglich der Marken.

Avaya ist eine eingetragene Marke von Avaya LLC.

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

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

Herunterladen der Dokumentation

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

Avaya-Support kontaktieren

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

Inhaltsverzeichnis

1. one-X Portal for IP Office-Verwaltung	2.9 Hilfe und Support.....	51
1.1 Anmelden	51.2	51
1.2 Abmelden	51.3	51
2. Administrator-Menüs	3. Wartungsaufgaben	
2.1 Status	3.1 Neustarten des Dienstes.....	54
2.1.1 Dashboard	3.2 Konfiguration des Anrufprotokolls.....	55
2.1.2 Komponentenstatus	3.3 IP Office-Schalter.....	56
2.1.3 Status des IM-/Anwesenheitsservers.....	3.3.1 Hinzufügen eines weiteren IP Office-Systems.....	56
2.1.4 Ausfallsicherheit	3.3.2 Ändern von IP Office-Details.....	58
2.1.5 Letzte wichtige Ereignisse.....	3.3.3 Ausfallsicherheit	59
2.1.6 Aktive Sitzungen	3.4 Minianwendungen.....	62
2.1.7 Umgebung	3.4.1 Auslesen der URL einer Minianwendung.....	62
2.2 Konfiguration	3.4.2 Importieren von Minianwendungen.....	63
2.2.1 Anbieter	3.4.3 Exportieren von Minianwendungen.....	65
2.2.2 Benutzer	3.4.4 Hinzufügen einer externen Minianwendung.....	66
2.2.3 CSV	3.4.5 Bearbeitung einer externen Minianwendung.....	66
2.2.4 Marken	3.4.6 Aktivierung einer externen Minianwendung.....	67
2.2.5 IM/Anwesenheit	3.4.7 Deaktivierung einer externen Minianwendung.....	67
2.2.6 Exchange-Dienst	3.4.8 Löschen einer externen Minianwendung.....	67
2.2.7 SMTP-Konfiguration.....	3.5 Benutzer	68
2.2.8 Konferenzwahl	3.5.1 Hinzufügen/Löschen von Benutzern.....	68
2.2.9 Ausfallsicherheit	3.5.2 Bearbeiten von Benutzereinstellungen.....	68
2.2.10 Host-Domänenname.....	3.6 Verzeichnisse	70
2.2.11 Bereinigung von Konferenzen.....	3.6.1 Hinzufügen einer externen LDAP-Verzeichnisquelle	70
2.2.12 Zentrale CTI-Verbindung.....	3.6.2 Überprüfen des externen LDAP-Verzeichnisses	72
2.2.13 Clientversionen blockieren.....	3.6.3 Überprüfen und Aktualisieren des Systemverzeichnisses	73
2.3 Sicherheit	3.7 Aktualisieren/Herunterstufen.....	74
2.3.1 HTTP/HTTPS-Protokoll.....	3.7.1 Aktualisieren von one-X Portal for IP Office.....	74
2.3.2 TLS-Einstellungen	3.7.2 Downgraden von one-X Portal for IP Office.....	75
2.3.3 ESNA-Authentifizierung.....	3.7.3 Entfernen von one-X Portal for IP Office.....	76
2.3.4 Zertifikat	3.8 Sofortnachrichtenversand/Anwesenheit.....	78
2.4 Diagnose	3.8.1 IM Server-Konfiguration	79
2.4.1 Protokollierung konfigurieren.....	3.8.2 IM-Benutzerkonfiguration.....	81
2.4.2 Protokollanzeige	3.8.3 Starten des IM-Servers	81
2.4.3 Netzwerkrouuten	3.8.4 Durchsuchen des IM-Archivs.....	82
2.4.4 IP Office-Verbindungen.....	3.8.5 Exchange-Kalenderintegration.....	83
2.4.5 Datenbankintegrität.....	3.8.6 Aktivieren der XMPP-Administratorkonsole.....	84
2.4.6 Benutzerdatenüberprüfung.....	3.8.7 Aktivieren der IM-Archivierung.....	84
2.4.7 Anruf-/Konferenzplanung.....	3.8.8 Deaktivieren der IM-Archivierung.....	85
2.4.8 Konferenzen anzeigen.....	3.8.9 Deaktivieren der XMPP-Administratorkonsole.....	85
2.4.9 Speicherauszug erzeugen.....	3.9 Konferenzen	86
2.4.10 Thread-Abbild erzeugen.....	3.9.1 Anzeigen der Konferenzen.....	86
2.5 Verzeichnisintegration.....	3.9.2 Anzeigen geplanter Konferenzen.....	87
2.5.1 Verzeichnissynchronisierung.....	3.9.3 Löschen einer geplanten Konferenz.....	88
2.5.2 LDAP-Verzeichnissuche.....	3.9.4 Nachricht über Konferenzbenachrichtigungen.....	88
2.5.3 Systemverzeichnis	3.9.5 E-Mails der Konferenz.....	89
2.6 Konfiguration der Minianwendungen.....	3.9.6 Festlegen der Web Collaboration-URL.....	90
2.6.1 Externe Minianwendungsliste.....	3.10 Remote-Protokollierung.....	91
2.6.2 Importieren von Minianwendungen.....	3.11 Fehlerbehebung.....	95
2.6.3 Exportieren von Minianwendungen.....	3.12 Hinzufügen weiterer Administratoren.....	96
2.7 IM-Archiv	4. AFA-Menüs	
2.7.1 Archiv durchsuchen.....	4.1 Anmelden	98
2.8 Webkonferenzen	4.2 Systemstatus	99
2.8.1 Konferenzen überwachen.....	4.3 Konfiguration	99
	4.4 DB-Vorgänge	100

4.4.1 Sichern	100
4.4.2 Wiederherstellen	101
Index	103

Kapitel 1.

one-X Portal for IP Office-Verwaltung

1. one-X Portal for IP Office-Verwaltung

Neben dem normalen Betrieb durch den Endbenutzer wird die Weboberfläche von one-X Portal for IP Office auch für einige Verwaltungs- und Wartungsfunktionen verwendet. In dieser Dokumentation wird die Verwendung dieser Verwaltungsmenüs dargestellt.

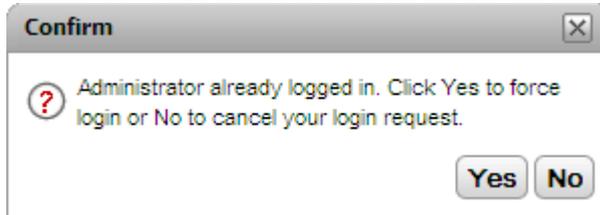
1.1 Anmelden

Der Zugriff auf die Administrationsmenüs für one-X Portal for IP Office erfolgt genauso wie der Benutzerzugriff über einen Webbrowser, wobei der URL jedoch **?admin=true** hinzugefügt wird. Es kann jeweils nur ein Benutzer als Administrator angemeldet sein.

- Standardmäßig verwenden Linux-basierte one-X Portal for IP Office-Server die **externe Authentifizierung**. Dies bedeutet, dass die Berechtigungen für die Portaladministration Sicherheitsbenutzern zugewiesen werden, die in der Sicherheitskonfiguration des IP Office-Diensts konfiguriert sind, der auf demselben Server ausgeführt wird. Standardmäßig ist dies der Benutzer **Administrator**, allerdings können auch zusätzliche Dienstbenutzer als Portaladministratoren konfiguriert werden.
- Wenn die externe Authentifizierung deaktiviert ist, verwendet das Portal sein eigenes lokales Administratorkonto auf die gleiche Weise wie für einen Windows-basierten Server (siehe unten).

So melden Sie sich an:

1. Geben Sie in Ihrem Webbrowser die URL mithilfe der Form **https://<Server-Name>:<Server-Port>/onexportal-admin.html** ein, wenn:
 - **<Server-Name>** ist der Name oder die IP-Adresse des one-X Portal for IP Office-Servers.
 - **<Server-Port>** ist die Portnummer, die von one-X Portal for IP Office verwendet wird. Diese ist entweder 9443 oder 8443 für HTTPS-Zugriff.
 - Sie können **http://** anstelle von **https://** und **8080** als den Port verwenden, wenn ein unsicherer Zugriff konfiguriert wurde. Siehe [Protokoll](#)³⁵.
 - Alternativ können Sie aus dem Anmeldemenü für normale Benutzer **Administrator-Login** auswählen.
2. Geben Sie den Namen und das Kennwort des one-X Portal for IP Office-Administrators ein, die bei der Installation konfiguriert wurden.
 - Falls bereits eine Sitzung als Administrator besteht, erscheint folgendes Feld mit einer Bestätigungsmeldung: Klicken Sie in der Bestätigungsmeldung auf **Ja**, um die Sitzung des angemeldeten Administrators zu beenden und sich mit Ihren Administrator-Zugangsdaten anzumelden.

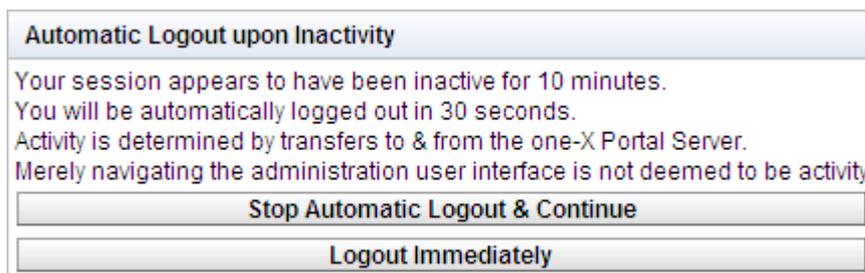


3. Klicken Sie auf **Anmelden**.

1.2 Abmelden

Die Option **Abmelden** oben rechts in den one-X Portal for IP Office-Administrationsmenüs dient zum Abmelden.

Neben einer manuellen Abmeldung werden Sie außerdem nach 10 Minuten gefragt, ob Sie angemeldet bleiben möchten. Bei Nichtbeantwortung werden Sie automatisch abgemeldet.



Kapitel 2.

Administrator-Menüs

2. Administrator-Menüs

Das Administrationsmenü von one-X Portal for IP Office bietet eine Reihe von Optionen für die Überwachung und Konfiguration der one-X Portal for IP Office-Anwendung.

Menü	Untermenü	Beschreibung
Status	Dashboard ¹⁴	Zeigt eine Übersicht des Serverstatus an.
	Komponentenstatus ¹⁵	Listet die letzte Statusänderung der Serverkomponenten auf.
	Status des IM-/Anwesenheitsservers ¹⁵	Zeigt den aktuellen Status der Serverkomponente für den Sofortnachrichtenversand an.
	Ausfallsicherheit ¹⁶	Zeigt den Status der Server in einer Ausfallsicherheitskonfiguration an. <i>(nur IP Office Server Edition)</i>
	Letzte wichtige Ereignisse ¹⁷	Zeigt die letzten 20 Ereignisse auf dem Server an.
	Aktive Sitzungen ¹⁸	Zeigt die Anzahl der Sitzungen an, die von one-X Portal for IP Office zwischengespeichert werden.
	Umgebung ¹⁸	Zeigt eine Übersicht des one-X Portal for IP Office-Server-PCs an.
Konfiguration	Anbieter ¹⁹	Dient zum Anzeigen und Bearbeiten der Anbieter.
	Benutzer ²⁴	Dient zum Anzeigen und Bearbeiten von one-X Portal for IP Office-Benutzereinstellungen.
	CSV ²⁵	Dient zum Exportieren von Benutzer- und Systemverzeichnis.
	Marken ²⁵	Dient zur Eingabe des Texts, der nach der Anmeldung eines Benutzers auf den one-X Portal for IP Office-Seiten angezeigt wird.
	IM/Anwesenheit ²⁶	Dient zur Überwachung des Status des IM-/Anwesenheitsservers als Administrator.
	Exchange-Dienst ²⁷	Dient zur Konfiguration des Exchange-Servers, um das Auslesen des Kalenders und der Anwesenheitsdaten von Benutzern zu ermöglichen.
	SMTP-Konfiguration ²⁸	Legen Sie die E-Mail-Informationen fest, die für E-Mail-Benachrichtigungen über Konferenzen verwendet werden.
	Konferenzeinwahl ²⁹	Geben Sie den festgesetzten Text für die Aufnahme in Benachrichtigungen über geplante Konferenzen ein.
	Ausfallsicherheit ³⁰	Wird auf einem IP Office Application Server verwendet, um festzulegen, ob das Portal Ausfallsicherheit unterstützt. <i>(nur IP Office Server Edition Select)</i>
	Host-Domänenname ³²	Legen Sie die URL fest, die für Web Collaboration-Konferenzen in Konferenzeinladungen verwendet wird.
	Bereinigung von Konferenzen ³²	Konfigurieren Sie, wie lange die Details einer Konferenz gespeichert werden sollen.
	Zentrale CTI-Verbindung ³³	Dient zum Konfigurieren, ob der Server automatisch Informationen über andere IP Office-System in einem Netzwerk erhält und diese unterstützt.
	Clientversionen blockieren ³⁵	Dient zum Konfigurieren bestimmter Versionen und Builds von Clients, die vom Server nicht unterstützt werden sollen.
Sicherheit	HTTP/HTTPS-Protokoll ³⁵	Legen Sie fest, ob der Server HTTPS oder HTTPS und HTTP verwendet.
	TLS-Einstellungen ³⁶	Konfigurieren Sie die Optionen für die Unterstützung von TLS.
	ESNA-Authentifizierung ³⁶	Legt die Adresse des ESNA-Servers fest, der zum Authentifizieren der Benutzeranmeldung mit einem ESNA-Konto verwendet werden soll.
Diagnose	Protokollierung konfigurieren ³⁷	Dient zum Konfigurieren der unterstützten Protokollierungsebene und -methode.

Menü	Untermenü	Beschreibung
	Protokollanzeige 	Dient zum Installieren und Starten von Chainsaw zum Anzeigen von Protokollen.
	Netzwerkrouen 	Dient zum Testen des IP-Verbindungspfads zu einer IP-Adresse.
	IP Office-Verbindungen 	Dient zum Testen des IP-Verbindungspfads zu IP Office.
	Datenbankintegrität 	Dient zum Testen der Datenbankstruktur.
	Benutzerdatenüberprüfung 	Dient zur Erkennung der möglichen Ursache von Fehlern bei der Benutzeranmeldung oder der Beschädigung von Benutzerdaten und zum Zurücksetzen der beschädigten Daten.
	Anruf- / Konferenzplanung 	Dient zum Löschen einer geplanten Konferenz.
	Konferenzen anzeigen 	Dient zum Anzeigen der Details von protokollierten und zukünftigen geplanten Konferenzen für alle Benutzer. Ermöglicht das Löschen und Ändern dieser Konferenzen.
	Speicherauszug erzeugen 	Erstellt einen Diagnosedatensatz der aktuellen Speichernutzung des Servers.
	Thread-Abbild erzeugen 	Erstellt einen Diagnosedatensatz der aktuellen Prozessor-Threads des Servers.
Verzeichnisintegration	Verzeichnissynchronisierung 	Erzwingt eine Aktualisierung des Systemverzeichnisses durch den Server.
	Systemverzeichnis 	Zeigt das one-X Portal for IP Office-Systemverzeichnis an.
	LDAP-Verzeichnissuche 	Zeigt das externe Verzeichnis an, für das der one-X Portal for IP Office-Server konfiguriert wurde.
Konfiguration der Minianwendungen	Liste externer Minianwendungen 	Die im System vorhandenen externen Minianwendungen werden aufgeführt.
	Externe Minianwendungen importieren 	Dient zum Import externer Minianwendungen.
	Externe Minianwendungen exportieren 	Dient zum Export externer Minianwendungen.
Webkonferenzen	Konferenzen überwachen 	Zeigt Informationen zu Web-Konferenzen an, die momentan auf dem Server stattfinden.
IM-Archiv	Archiv durchsuchen 	Dient zur Suche nach den IM-Konversationen zwischen den Systemkontakten.
Hilfe und Support	Hilfe 	Ruft die auf dem Server installierte Hilfe zu one-X Portal for IP Office auf.
	Unterstützung von Avaya 	Dient zum Aufrufen der Avaya-Support-Website für Avaya-Anwendungen.
	Info 	Zeigt Informationen zu der one-X Portal for IP Office-Version an.

Es ist wichtig zu wissen, dass die one-X Portal for IP Office-Administrationsmenüs als Offline-Editor fungieren. Innerhalb eines bestimmten Menüs werden Daten aus der Datenbank abgerufen (mit einem **GET**-Befehl), bearbeitet und dann an die Datenbank zurückgesendet (mit einem **PUT**-Befehl).

In jedem Menü kann durch Klicken auf die Symbole   eine kurze Beschreibung zu Funktion und Inhalt des Menüs ein-/ausgeblendet werden.

2.1 Status

In diesem Abschnitt können Sie den Status der verschiedenen Serverkomponenten anzeigen.

2.1.1 Dashboard

Das Menü „Dashboard“ enthält eine Übersicht des Serverstatus.

The screenshot shows the Avaya one-X Portal for IP Office dashboard. The top navigation bar includes the Avaya logo, the product name, and a user greeting: "Welcome Administrator | Help | Logout | Version: 11.0.4.0.0". The dashboard is divided into several sections:

- Health:** A sidebar menu with options like Dashboard, Component Status, IM/Presence Server Status, Key Recent Events, Active Sessions, and Environment.
- IP Office/Expansions:** A gauge showing "IP Office/Expansions Status" at 100%. A legend indicates: Available: 100% (1), Starting: 0% (0), Failed: 0% (0).
- Memory Status:** A gauge showing "Memory Status" at 26%. It also displays "JVM Max. Memory: 888.75 MB" and "JVM Allocated Memory: 358.11 MB".
- User Details:** A table showing "Logged In Users" (0) and "Total Users" (20). Below it, "Active Client Sessions" are shown as 13.
- IM/Presence Server:** A table showing "XMPP Domain Name" (rajaramse11) and "Status" (Available).

A note at the bottom states: "Note: Dashboard content will be updated automatically after every 40 seconds."

- **Status von IP Office/Erweiterungen**

Dieser Abschnitt enthält eine Übersicht über den Status der Verbindungen vom Portalserver zu den von diesem unterstützten IP Office-Systemen.

- **Status**

Dieser Abschnitt enthält eine Übersicht der Serverspeichernutzung.

- **Benutzerdetails**

Dieser Abschnitt enthält eine Übersicht über die Anzahl der konfigurierten und angemeldeten Benutzer. Des Weiteren wird die Anzahl der aktiven Sitzungen angezeigt, die Benutzer von Avaya Communicator for Web, Outlook-Plug-In, one-X Portal for IP Office umfassen.

- **IM/Anwesenheitsserver**

Dieser Abschnitt enthält eine Übersicht über den Status der XMPP-Komponente des Servers.

2.1.2 Komponentenstatus

Das Menü **Komponentenstatus** zeigt die zuletzt aufgezeichneten Statusänderungen jeder wesentlichen Komponente der one-X Portal for IP Office-Anwendung an.

- Für UCM-Server müssen ein CSTA-Hauptanbieter sowie zusätzlich ein CSTA-Anbieter für jedes unterstützte IP Office-System vorhanden sein. Dies gilt auch für Linux-Systeme, die ein IP Office Server Edition-Netzwerk unterstützen, aber den [zentralen CTI-Verbindungsmodus](#)^[33] nicht verwenden.
- Für einen Dienst in einem IP Office Server Edition-Netzwerk mit Verwendung des zentralen CTI-Verbindungsmodus darf nur ein DMSL-Anbieter für das primäre IP Office-System vorhanden sein. Außerdem muss ein CSTA-Anbieter für das primäre IP Office-System vorhanden sein, es sei denn, Portalausfallsicherheit wird verwendet; in diesem Fall muss auch ein CSTA-Anbieter für das sekundäre IP Office-System vorhanden sein.
- Falls LDAP verwendet wird, muss ein DSML LDAP-Anbieter vorhanden sein.

Health

▼ Component Status

► Description: Health of key one-X Portal for IP Office components

IP Address	Component Name	Status	
Filter	All	All	All

Apply Reset

Component Name	Status	Reported At	Additional Info.
DSML-Provider-1-ldap://ldap-server-ip-address...	Available	29 Jun 2017 09:10:01	
DSML-Provider-1-Master	Available	29 Jun 2017 09:10:48	TotalCount:Success:Failed:1:169.254.0.1:
DSML-Provider-1-169.254.0.1	Available	2 Jun 2017 11:11:17	Global resynchronization completed for IP Off...
CSTA-Provider-1-Master	Available	29 Jun 2017 09:18:42	Master Available
CSTA-Provider-1-169.254.0.1	Available	29 Jun 2017 09:18:42	Provider Ok
VOICEMAIL-Provider-169.254.0.2	Available	2 Jun 2017 10:49:34	Provider Up

Page 1 of 1 Displaying 1 to 6 of 6 Refresh

So zeigen Sie den Status der Komponente an:

1. Wählen Sie **Status** und dann **Komponentenstatus**.
2. Klicken Sie auf **Alle abrufen**, um die Statusdatensätze aus der one-X Portal for IP Office-Datenbank abzurufen.
3. Sie können die Datensätze mithilfe der Seitensteuerelemente durchsuchen.
4. Mit der Option **Löschen** können Sie den Statusdatensatz löschen. Dies hat keinen Einfluss auf die Komponente. Durch Benutzung der Kontrollkästchen und des Befehls **Ausgewählte löschen** können mehrere Datensätze gelöscht werden.

2.1.3 Status des IM-/Anwesenheitsservers

Dieses Menü zeigt den aktuellen Status des Sofortnachrichtenversand-Servers an, den one-X Portal for IP Office als Komponentendienst verwendet. Zahlreiche Wartungsverfahren im Hinblick auf IM und Anwesenheit finden Sie unter [Sofortnachrichtenversand](#)^[78].

Health

► Component Status

▼ IM/Presence server status

Component Name	Status	Reported At
IM/Presence Server	Available	29 Feb 2017 09:16

Refresh Start

2.1.4 Ausfallsicherheit

Dieses Menü wird auf den Portalservern im IP Office Server Edition Select-Netzwerk angezeigt. Es zeigt den aktuellen Status des Portals und des IP Office-Diensts auf den primären und sekundären Servern bei der Verwendung von [IP Office Server Edition-Resilienz](#) an.

The screenshot shows a web interface with a left-hand navigation menu and a main content area. The navigation menu includes 'Health', 'Configuration', and 'Security'. Under 'Health', there are links for 'Dashboard', 'Component Status', 'IM/Presence Server Status', 'Resiliency', 'Key Recent Events', 'Active Sessions', and 'Environment'. The main content area shows a breadcrumb trail: 'Dashboard' > 'Component Status' > 'IM/Presence Server Status' > 'Resiliency'. Below this is a table with the following data:

Resiliency Component	FQDN/IP Address	Status
Primary one-X Portal	stom1	Started
Secondary one-X Portal	192.168.0.182	Not Started / Reachable
Primary IP Office Connection	192.168.0.180	Connected Active
Secondary IP Office Connection	192.168.0.182	Connected Passive
Primary DB State	-	Started Active
Secondary DB State	-	Not Started / Reachable

Below the table is a 'Refresh' button.

Der oben stehende Screenshot zeigt beispielsweise ein System, bei dem die primären und sekundären IP Office-Server ausgeführt werden und der primäre Portal-Server ebenfalls ausgeführt wird, aber der sekundäre Portaldienst noch nicht gestartet wurde. Wenn der Portaldienst gestartet wird, ändert sich der Status des sekundären Portal-Servers zu **Gestartet** und der Status der **sekundären DB** wird zu **Gestartet Passiv** geändert.

Die in der Statusanzeige verwendeten Begriffe haben die folgende Bedeutung. Die Begriffen können auch in Kombination verwendet werden:

- **Gestartet**
Der Dienst wird ausgeführt.
- **Gestoppt** oder **Nicht gestartet**
Der Dienst wird nicht ausgeführt.
- **Verbindung hergestellt**
Dieser Portal-Server verfügt über eine Verbindung zum Dienst.
- **Erreichbar**
Der Server, der den Dienst hostet, wurde erkannt, aber es besteht keine Verbindung, da der Dienst auf diesem Server noch nicht gestartet wurde.
- **Aktiv**
Der Dienst wird zurzeit für die Unterstützung von Portalbenutzern verwendet.
- **Passiv**
Der Dienst wird ausgeführt, wird aber derzeit nicht zur Unterstützung von Portalbenutzern verwendet.

2.1.5 Letzte wichtige Ereignisse

Das Menü **Letzte wichtige Ereignisse** zeigt die letzten 20 Ereignisse an, die von der one-X Portal for IP Office-Anwendung aufgezeichnet wurden. Dabei kann es sich um Aktionen handeln, die vom one-X Portal for IP Office-Dienst ausgeführt wurden, aber auch um Verwaltungsaktionen, wie Anmeldung/Abmeldung des Administrators, Änderung des Administrator Kennworts, Anbieteränderungen und Konfigurationswiederherstellungen.

Die Liste enthält nun die Anzahl der fehlgeschlagenen Anmeldeversuche, wenn mehr als 10 Versuche innerhalb von 5 Minuten fehlschlagen. Fehlgeschlagene Anmeldeversuche basieren auf dem Benutzernamen. Fehlgeschlagene Avaya Communicator-Anmeldungen werden nicht erfasst.

What Happened?	Significance	Reported At	Additional Info.
Extn1002	High	Jan 17, 2019 12:02:13 PM	Repeated login failures
Administrator	Low	Jan 17, 2019 11:56:40 AM	Administrator logged in
Extn1003	High	Jan 17, 2019 11:56:19 AM	Repeated login failures
Administrator	Low	Jan 17, 2019 11:54:22 AM	Administrator logged in
Administrator	Low	Jan 17, 2019 11:49:35 AM	Administrator logged in

Page 5 of 20 | Displaying 21 to 25 of 99 | Refresh

So zeigen Sie die letzten wichtigen Ereignisse an:

1. Wählen Sie **Status** und dann **Letzte wichtige Ereignisse**. Klicken Sie auf **Aktualisieren**.
2. Klicken Sie auf **Alle abrufen**, um die Ereignisdatensätze aus der one-X Portal for IP Office-Datenbank abzurufen.
3. Sie können die Datensätze mithilfe der Seitensteuerelemente durchsuchen.
4. Mit der Option **Löschen** können Sie den Statusdatensatz löschen. Dies hat keinen Einfluss auf die Komponente. Durch Benutzung der Kontrollkästchen und des Befehls **Ausgewählte löschen** können mehrere Datensätze gelöscht werden.

2.1.6 Aktive Sitzungen

Das Menü **Aktive Sitzungen** zeigt die Anzahl der aktuellen Sitzungen an, die mit dem one-X Portal for IP Office-Server verbunden sind.

User	Application
6	2

Extension	Application	Application Version	Login Time	IP Address	Is Active
1000	Avaya IP Office Plug-In	10.1.0.3.8	Jan 17, 2019 2:32:01 PM	148.147.100.14	Yes
1001	Avaya IP Office Plug-In	10.1.0.3.8	Jan 17, 2019 2:39:14 PM	148.147.100.12	Yes
1002	Avaya IP Office Plug-In	10.1.0.3.8	Jan 17, 2019 2:41:28 PM	148.147.206.105	Yes

So zeigen Sie die aktiven Sitzungen an:

1. Wählen Sie **Status** und dann **Aktive Sitzungen**.
2. Um die Details zu aktualisieren, klicken Sie auf **Aktualisieren**.

2.1.7 Umgebung

Das Menü **Umgebung** zeigt Informationen zum one-X Portal for IP Office-Server-PC an. Die verfügbaren Informationen sind abhängig vom Typ des Portal-Servers.

Server Details	Value
Version:	10.1.0.0.0 build 223
Build Date	May 15 2017
Operating System (OS)	Linux
OS Version	3.11.4-1.appscard.el6.i686
IP Addresses	[169.254.0.2, 192.168.0.201]
JVM Vendor/JVM Version	Oracle Corporation/1.7.0_75-mockbuild_2016_01_20_23_10-b00
JVM Architecture	i386

Resources Details	Value
Hard Disk Free	17.54GB
JVM Max. Memory	773.38MB
JVM Allocated Memory	424.73MB
JVM Free Memory	127.48MB

So zeigen Sie Informationen zur Umgebung an:

1. Wählen Sie **Status** und anschließend **Umgebung**.
2. Klicken Sie auf **Aktualisieren**.

2.2 Konfiguration

In diesem Abschnitt können Sie verschiedene Konfigurationsoptionen anzeigen und überprüfen.

2.2.1 Anbieter

Dieses Menü zeigt die auf dem one-X Portal for IP Office-Server konfigurierten Anbieter an. Im Menü **Anbieter** kann eingestellt werden, welche IP Office-Systeme und LDAP-Server den Anbietern zugewiesen werden.

Health

Configuration

[Providers](#)

[Users](#)

[CSV](#)

[Branding](#)

[IM/Presence](#)

[Exchange service](#)

[SMTP Configuration](#)

[Conference Dial-in](#)

[Host Domain Name](#)

[Conference Clean Up](#)

[Central CTI Link](#)

▼ Providers

► Description: Configure providers of services to applications

Provider Name

IP Address	User Name		
127.0.0.1	EnhTcpaService		
192.168.45.1	EnhTcpaService		

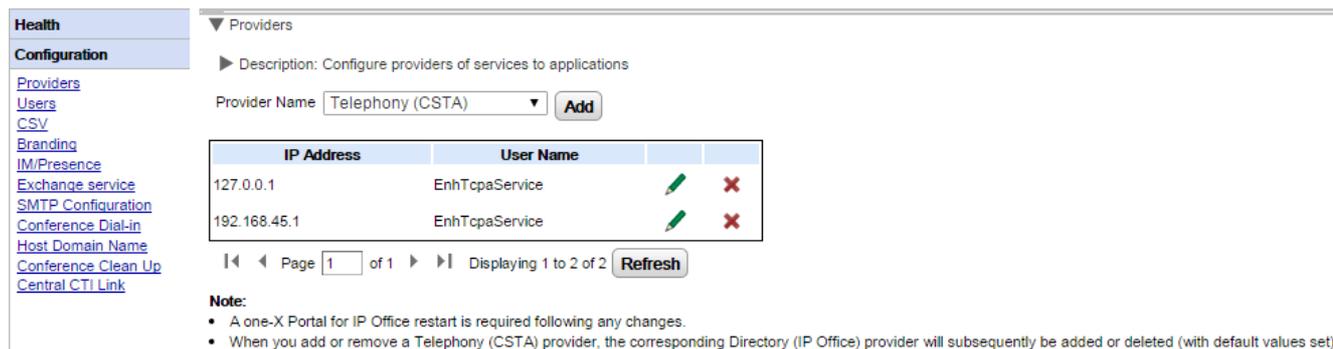
◀ Page of 1 ▶ Displaying 1 to 2 of 2

Note:

- A one-X Portal for IP Office restart is required following any changes.
- When you add or remove a Telephony (CSTA) provider, the corresponding Directory (IP Office) provider will subsequently be added or deleted (with default values set).

2.2.1.1 Telefonie-Anbieter (CSTA)

Die unten stehenden Einstellungen werden für einen CSTA-Telefonie-Anbieter angezeigt. Sie sollten nur geändert werden, wenn Sie mit der Installation und dem Betrieb von one-X Portal for IP Office vertraut sind.



Health

Configuration

Providers

Description: Configure providers of services to applications

Provider Name:

IP Address	User Name		
127.0.0.1	EnhTcpaService		
192.168.45.1	EnhTcpaService		

Page 1 of 1 | Displaying 1 to 2 of 2 |

Note:

- A one-X Portal for IP Office restart is required following any changes.
- When you add or remove a Telephony (CSTA) provider, the corresponding Directory (IP Office) provider will subsequently be added or deleted (with default values set).

Um einen neuen CSTA-Anbieter hinzuzufügen, klicken Sie auf **Hinzufügen**. Die Anbietereinstellungen werden angezeigt. Beachten Sie, dass beim Hinzufügen eines neuen CSTA-Anbieters automatisch auch ein neuer DMSL-Anbieter für die gleiche Adresse hinzugefügt wird. Das Hinzufügen eines neuen Anbieters ist nur in einem Netzwerk erforderlich, in dem keine [zentrale Konfiguration](#) verwendet wird.

Um einen vorhandenen CSTA-Anbieter zu bearbeiten, klicken Sie auf das Bearbeitungssymbol neben dem vorhandenen Eintrag. Die Anbietereinstellungen werden angezeigt. Zum Hinzufügen

Einstellungen für CSTA-Anbieter

Alle Änderungen an Anbietereinstellungen erfordern einen [Neustart des Portaldiensts](#).



Edit Telephony (CSTA)

This control enables you to add & delete the IP Office Unit(s) mapped to a provider.

IP Address	192.168.45.1
User Name	EnhTcpaService
Password	*****

- **IP-Adresse**
Die IP-Adresse des IP Office-Systems.
- **Benutzername**
Der Name des T CPA-Dienstbenutzers, der in den Sicherheitseinstellungen des IP Office-Systems konfiguriert ist. Der Standardbenutzer ist **EnhTcpaService**.
- **Kennwort**
Das für den T CPA-Dienstbenutzer festgelegte Kennwort.

2.2.1.2 Verzeichnis-Anbieter (IP Office)

Die unten stehenden Einstellungen werden für einen Verzeichnis-Anbieter (IP Office) angezeigt. Sie sollten nur geändert werden, wenn Sie mit der Installation und dem Betrieb von one-X Portal for IP Office vertraut sind.

Providers

Description: Configure providers of services to applications

Provider Name:

IP Address	User Name	Port number	Timeout	Secure Connection
127.0.0.1	EnhTcpaService	443	300	<input checked="" type="checkbox"/>
192.168.45.1	EnhTcpaService	443	300	<input checked="" type="checkbox"/>

Page 1 of 1 | Displaying 1 to 2 of 2 |

Note:

- A one-X Portal for IP Office restart is required following any changes.
- When you add or remove a Telephony (CSTA) provider, the corresponding Directory (IP Office) provider will subsequently be added or deleted (with default values set).

Um einen neuen Verzeichnis-Anbieter hinzuzufügen, verwenden Sie die Optionen zum Hinzufügen eines [CSTA-Anbieters](#). Um einen vorhandenen Anbieter zu bearbeiten, klicken Sie auf das Bearbeitungssymbol neben dem vorhandenen Eintrag.

Einstellungen für Verzeichnis-Anbieter

Alle Änderungen an Anbietereinstellungen erfordern einen [Neustart des Portaldienstes](#).

Edit Directory (IP-Office)

This control enables you to add & delete the IP Office Unit(s) mapped to a provider.

Note:

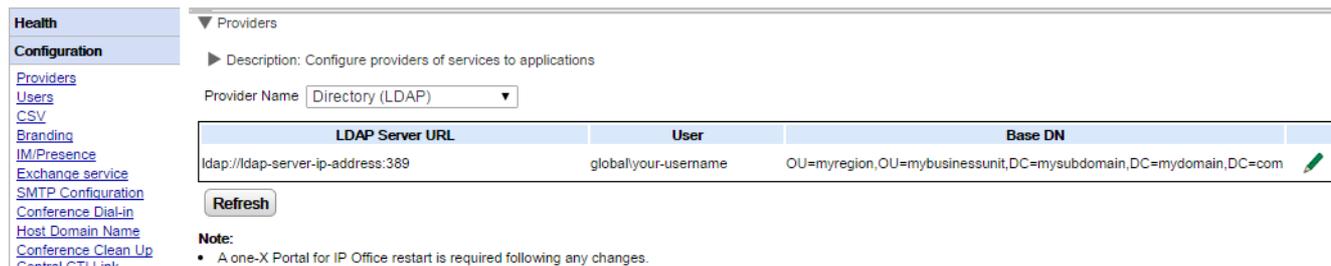
- Timeout value should be numeric and must be between 30 to 600

IP Address	<input type="text" value="127.0.0.1"/>
User Name	<input type="text" value="EnhTcpaService"/>
Password	<input type="password" value="....."/>
Port number	<input type="text" value="443"/>
Timeout	<input type="text" value="300"/>
Secure Connection	<input checked="" type="checkbox"/>

- IP-Adresse**
 Die IP-Adresse des IP Office-Systems.
- Benutzername**
 Der Name des TCPA-Dienstbenutzers, der in den Sicherheitseinstellungen des IP Office-Systems konfiguriert ist. Der Standardbenutzer ist **EnhTcpaService**.
- Kennwort**
 Das für den TCPA-Dienstbenutzer festgelegte Kennwort.
- Portnummer**
 Die Nummer des Ports, an dem das IP Office-System Verbindungen akzeptiert.
- Zeitlimit**
 Der Zeitlimitwert zwischen 30 und 600 Sekunden.
- Sichere Verbindung**
 Legen Sie diese Option für die Verbindung mit dem Verzeichnisdienst des Telefonssystems fest.

2.2.1.3 DSML (LDAP)-Anbieter

Die unten stehenden Einstellungen werden für einen **Verzeichnisanbieter (DSML LDAP)** angezeigt.



Providers

Description: Configure providers of services to applications

Provider Name: Directory (LDAP)

LDAP Server URL	User	Base DN
ldap://ldap-server-ip-address:389	globallyour-username	OU=myregion,OU=mybusinessunit,DC=mysubdomain,DC=mydomain,DC=com

Refresh

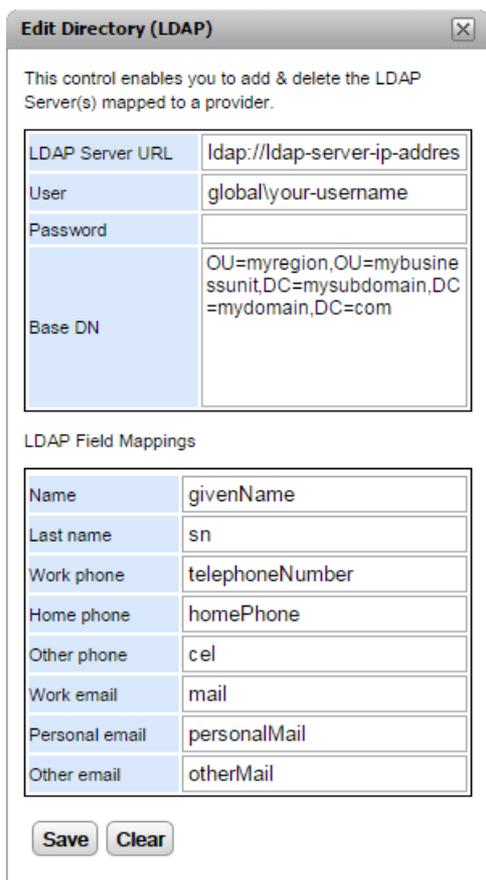
Note:

- A one-X Portal for IP Office restart is required following any changes.

Klicken Sie zum Bearbeiten des Anbieters auf das Bearbeitungssymbol .

Einstellungen für LDAP-Anbieter

Alle Änderungen an Anbietereinstellungen erfordern einen [Neustart des Portaldiensts](#) .



Edit Directory (LDAP)

This control enables you to add & delete the LDAP Server(s) mapped to a provider.

LDAP Server URL	ldap://ldap-server-ip-address
User	globallyour-username
Password	
Base DN	OU=myregion,OU=mybusinessunit,DC=mysubdomain,DC=mydomain,DC=com

LDAP Field Mappings

Name	givenName
Last name	sn
Work phone	telephoneNumber
Home phone	homePhone
Other phone	cel
Work email	mail
Personal email	personalMail
Other email	otherMail

Save Clear

2.2.1.4 Voicemail-Dienstanbieter

Die unten stehenden Einstellungen werden für einen **VoiceMailServer**-Anbieter angezeigt.

The screenshot displays the configuration interface for Voicemail Providers. On the left, a sidebar contains navigation links: Health, Configuration (selected), Providers, Users, CSV, Branding, IM/Presence, Exchange service, SMTP Configuration, Conference Dial-in, Host Domain Name, Conference Clean Up, and Central CTI Link. The main content area is titled 'Providers' and includes a description: 'Configure providers of services to applications'. Below this, there is a 'Provider Name' dropdown menu set to 'VoiceMailServer (VMPro)' and an 'Add' button. A table below shows the IP address '127.0.0.1' with edit and delete icons. At the bottom, there is a 'Note' section with a bullet point: 'A one-X Portal for IP Office restart is required following any changes.'

IP Address
127.0.0.1

Klicken Sie zum Bearbeiten des Anbieters auf das Bearbeitungssymbol .

Alle Änderungen an Anbietereinstellungen erfordern einen [Neustart des Portaldiensts](#)⁵⁴.

2.2.2 Benutzer

Im Menü **Benutzer** können Sie die Benutzer von IP Office sehen. Hier werden alle IP Office-Benutzer angezeigt und nicht nur diese, die für den one-X Portal for IP Office-Betrieb aktiviert wurden. Beachten Sie, dass der Portalserver während des normalen Betriebs seine Liste bekannter Benutzer nur alle fünf Minuten mit dem Telefonsystem neusynchronisiert.

Sie können einige der Benutzereinstellungen, die im one-X Portal for IP Office gespeichert sind, bearbeiten, siehe [Bearbeiten der Benutzereinstellungen](#). Sie können keine in IP Office gespeicherten Benutzereinstellungen bearbeiten.

ID	Name	Role	Actions
1	Administrator	ADMINISTRATOR	Edit
3	csta_provider_user	APPLICATION	Edit
4	dsm1_ipo_provider_user	APPLICATION	Edit
5	dsm1_ldap_provider_user	APPLICATION	Edit
41	Extn601	USER	Edit Clear Sessions
47	Extn602	USER	Edit Clear Sessions
48	Extn603	USER	Edit Clear Sessions
53	Extn604	USER	Edit Clear Sessions
42	Extn605	USER	Edit Clear Sessions
45	Extn606	USER	Edit Clear Sessions

So zeigen Sie Benutzer an:

1. Klicken Sie auf **Konfiguration**, und wählen Sie **Benutzer**.
2. Klicken Sie auf **Alle abrufen**.
3. Die Schaltfläche **Sitzungen löschen** neben einem Benutzer kann zum Trennen der Verbindung mit derzeit verbundenen Clients verwendet werden, die der Benutzer ausführt.

2.2.3 CSV

Über dieses Menü können Sie die vom one-X Portal for IP Office-Server verwendeten Benutzerinformationen und Systemtelefonbücher in .csv-Dateien exportieren.

Health	▶ Providers
Configuration	▶ Users
Providers	▼ CSV
Users	A control for exporting the user list and directory as a CSV file. CSV import is not supported. The exported filenames are hardcoded as exportUser.csv & exportDirectoryEntry.csv These get written to the underlying Tomcat/bin folder.
CSV	Export Configuration
Branding	▶ Branding
IM/Presence	▶ IM/Presence Server
Exchange service	▶ IM/Presence Exchange Service
SMTP Configuration	
Conference Dial-in	
Host Domain Name	
Conference Clean Up	
Central CTI Link	

So exportieren Sie:

1. Wählen Sie **Konfiguration** und dann **CSV**.
2. Klicken Sie auf **Konfiguration exportieren**.
3. Im Unterordner **/bin** des Anwendungsverzeichnis werden zwei Dateien erstellt. Bei Linux-basierten Servern entspricht der Standardpfad in etwa **/opt/Avaya/oneXportal/10.1.0_136//apache-tomcat/bin**.
 - **exportUser.csv**
 - **exportDirectoryEntry.csv**

2.2.4 Marken

Über dieses Menü können Sie Text eingeben, der dann auf den one-X Portal for IP Office-Seiten angezeigt wird, nachdem sich der Benutzer angemeldet hat.

Health	▶ Providers
Configuration	▶ Users
Providers	▶ CSV
Users	▼ Branding
CSV	A control for configure Branding Name so that it will shown at one-X Portal user login page. Maximum 40 characters allowed for Branding Name.
Branding	Branding Name <input type="text" value="MyBranding"/>
IM/Presence	<input type="button" value="Save"/> <input type="button" value="Refresh"/>
Exchange service	
SMTP Configuration	
Conference Dial-in	
Host Domain Name	

Der Text wird in der Titelleiste von one-X Portal for IP Office angezeigt (siehe unten).

 Office MyBranding	 Rajie(301) Available ▾ Help Logout Version:10.0.0.0 build 314 AVAYA
one-X Portal for IP Office	

2.2.5 IM/Anwesenheit

Das Portal enthält eine Komponente, die als Soforthrichten-(IM-)/Anwesenheitsserver fungiert. Der IM-/Anwesenheitsserver kann separat konfiguriert werden. Siehe [Soforthrichtenversand/Anwesenheit](#)^[78].

Server to Server Federation	<input checked="" type="checkbox"/>
Disconnect on Idle	<input type="checkbox"/>
Anyone can connect	<input checked="" type="checkbox"/>
Port number	5269
Idle timeout	3600
MyBuddy user name	mybuddy
XMPP Domain Name	server1.primary
Days to archive IMs	60

So konfigurieren Sie den IM-/Anwesenheitsserver:

1. Klicken Sie auf **Konfiguration** und wählen Sie **IM-/Anwesenheitsserver**.
2. Auswahl der erforderlichen Server-Einstellungen:

- **Server-Verbund**

Bei aktivierter Option kann der Anwesenheitsserver des Portals Anwesenheitsinformationen mit anderen Anwesenheitsservern austauschen.

- **Bei Leerlauf trennen**

Bei aktivierter Option werden Verbindungen zwischen Servern getrennt, wenn sie sich für den unter **Inaktivitäts-Zeitlimit** angegebenen Zeitraum im Leerlauf befinden.

- **Jede Verbindung möglich**

Jedem erlauben, sich mit IM-/Anwesenheitsdiensten zu verbinden.

- **Portnummer**

Diese ist auf **5269** festgelegt.

- **Inaktivitäts-Zeitlimit**

Dies ist das Zeitlimit in Sekunden, das bei aktivierter Option **Bei Leerlauf trennen** verwendet wird.

- **MyBuddy-Benutzername**

Dieses Feld ist auf **mybuddy** festgelegt. Der Wert ist gegebenenfalls erforderlich, wenn Anwesenheitsdetails in andere IM-/Anwesenheitsdienste integriert werden.

- **XMPP-Domänenname**

Hier wird der DNS-Domänenname festgelegt, der für IM-/Anwesenheitsfunktionen verwendet wird:

- Der XMPP-Domänenname sollte ein Domänenname sein, den der DNS auflösen kann. Sie können den XMPP-Domännennamen jederzeit festlegen. Der Domänenname muss über das Internet erreichbar sein, wenn Sie Anwesenheit außerhalb Ihres LAN verwenden wollen, z. B. mit one-X Mobile.
- Avaya empfiehlt, eine geteilte DNS zu verwenden, sodass der Servername außerhalb Ihres LAN in die öffentliche IP-Adresse der NAT oder der Firewall aufgelöst wird, während er innerhalb Ihres Netzwerks in die private IP-Adresse des LAN-Servers aufgelöst wird.
- Wenn Sie keinen auflösbaren DNS-Domännennamen einstellen können, können Sie die IP-Adresse des one-X Portal for IP Office-Servers ausschließlich für interne IM/Anwesenheit verwenden. In diesem Fall kann das one-X Portal for IP Office keine Verbindung zu Remote-Servern herstellen.
- Bei Linux-basierten Servern (IP Office Server Edition, IP Office Application Server und Unified Communications Module) müssen Sie die Websteuerungsmenüs des Servers verwenden, um deren Netzwerkeinstellungen zu konfigurieren, sodass der E-Mail-Link der automatischen Konfiguration den vollqualifizierten Domännennamen statt der IP-Adresse des Servers verwendet. Gehen Sie in Web Control zu EInstellungen > System > Hostname, um die Netzwerkeinstellungen zu ändern. Wenn Sie den Domännennamen auf eine andere Weise ändern, funktionieren die E-Mail-Links möglicherweise nicht richtig.
- **Tage für die Archivierung von IMs**
In diesem Feld wird festgelegt, wie lange der Server Nachrichten im IM-Archiv speichern soll, bevor sie gelöscht werden. Die Standardeinstellung lautet 182 Tage (6 Monate). Bei Bedarf können Sie mit der XMPP-Verwaltungskonsole die [IM-Archivierung deaktivieren](#)^[85]. Zum Ändern dieser Einstellung muss der IM-/Anwesenheitsserver verfügbar sein (siehe [Status des IM-/Anwesenheitsservers](#)^[15]).

3. Klicken Sie auf **Speichern**.

2.2.6 Exchange-Dienst

one-X Portal for IP Office kann auf dem Exchange-Server konfiguriert werden, um das Auslesen des Kalenders und der Anwesenheitsdaten von Benutzern zu ermöglichen.

Health	▶ Providers
Configuration	▶ Users
Providers	▶ CSV
Users	▶ Branding
CSV	▶ IM/Presence Server
Branding	▼ IM/Presence Exchange Service
IM/Presence	
Exchange service	
SMTP Configuration	
Conference Dial-in	
Host Domain Name	
Conference Clean Up	
Central CTI Link	

Exchange service account name	AvayaAdmin
Exchange service account password	●●●●●●●●
Exchange service Host	
Exchange Port number	6669
Exchange service proxy host	
Exchange proxy port	
Test Email Address (e.g. user@example.com)	

Note:

- Test email address is required for MS Exchange 2013 for validation purpose only.
- It is not possible to execute the batch file by placing it on the desktop. Please make sure that the batch file is not stored on the desktop.
- Save the file on any local drives, for example C drive. To download the file, right click on the link below and select "Save Link As...".

[Download Powershell script](#)

So konfigurieren Sie Exchange-Dienste:

1. Klicken Sie **Konfiguration** im linken Navigationsbalken.
2. Klicken Sie auf **Exchange-Dienst**.
 - a. Geben Sie **AvayaAdmin** in das Feld **Exchange-Dienst-Kontoname** ein. Vergewissern Sie sich, dass es sich bei diesem Namen um den gleichen Namen wie bei dem **AvayaAdmin**-Konto handelt, das Sie auf dem Exchange-Server erstellt haben.
 - b. Geben Sie das Kennwort ein, das für den **AvayaAdmin** als **Exchange-Dienst-Kontokennwort** festgelegt wurde.
 - c. Geben Sie als **Exchange-Dienst-Host** die IP-Adresse des Exchange-Dienst-Hosts ein.
 - d. Geben Sie in **Exchange-Portnummer** die Portnummer des Exchange-Dienstes ein.
 - e. Geben Sie den Domännennamen des Proxyservers, der für die Verbindung zum Exchange-Server genutzt wird, in **Exchange-Dienst-Proxyhost** ein.
 - f. Geben Sie die Portnummer des Proxyservers für den Exchange-Dienst in **Exchange-Proxyport** ein.
 - g. Legen Sie eine **Test-E-Mail-Adresse** mithilfe einer gültigen E-Mail-Adresse fest.
3. Klicken Sie auf **Exchange-Dienst-Konfiguration überprüfen**, um zu sehen, ob die eingegebenen Exchange-Daten korrekt sind.
4. Klicken Sie auf **Speichern**.

2.2.7 SMTP-Konfiguration

Die Konferenzeinladungen an Teilnehmer können sowohl über E-Mail als auch über den Sofortnachrichtenversand erfolgen. Für Benachrichtigungen über E-Mail müssen die E-Mail-Einstellungen der Konferenz wie folgt konfiguriert werden. Die E-Mail-Adresse jedes einzelnen Teilnehmers wird in der Telefonsystem-Konfiguration eingestellt.

Health

Configuration

- [Providers](#)
- [Users](#)
- [CSV](#)
- [Branding](#)
- [IM/Presence Server](#)
- [IM/Presence Exchange Service](#)
- [Conference Dial-in Information](#)
- SMTP Configuration**

Following SMTP configuration will be used to send emails for conference scheduling feature

Server Address	
Port number	25
Email From Address	
Use STARTTLS	<input type="checkbox"/>
Server Requires Authentication	<input type="checkbox"/>
User Name	
Password	

Note:

- *Default SMTP Port is 25

So stellen Sie den festgelegten Text der Konferenzbenachrichtigung ein:

1. Wählen Sie **Konfiguration** und dann **SMTP-Konfiguration**.
2. Legen Sie die Informationen der SMTP-E-Mail fest, die der Server verwenden soll:
 - **Serveradresse**
Die IP-Adresse des SMTP-Servers des Kunden.
 - **Portnummer**
Der SMTP-Abfrageport auf dem Server. Standardmäßig lautet er 25.
 - **E-Mail-Adresse des Absenders**
Dies ist die Adresse, die vom Server verwendet wird. Einige E-Mail-Server leiten nur Nachrichten von anerkannten Adressen oder Adressen in derselben Domäne weiter.
 - **STARTTLS verwenden**
Wählen Sie dieses Feld zur Aktivierung der TLS-/SSL-Verschlüsselung aus. Die Verschlüsselung ermöglicht die Voicemail-in-E-Mail-Integration bei Anbietern von gehosteten E-Mails, die SMTP nur auf Kommunikationswegen erlauben, die mehr Sicherheit bieten.
 - **Server erfordert Authentifizierung**
Wenn der Server ein Benutzerkonto benötigt, um E-Mails empfangen und versenden zu können, geben Sie die Einzelheiten eines Kontos ein, das auf diesem Server für die Verwendung durch IP Office konfiguriert wurde.
 - **Benutzername**
Der zu verwendende Kontoname, wenn „Server erfordert Authentifizierung“ ausgewählt ist.
 - **Kennwort**
Das zu verwendende Kontokennwort, wenn „Server erfordert Authentifizierung“ ausgewählt ist.
3. Klicken Sie auf **Speichern**.

2.2.8 Konferenzeinwahl

Wenn der Benutzer eine Konferenz plant, sendet der Server den eingeladenen Teilnehmern über E-Mail und den Sofortnachrichtenversand eine Konferenzbenachrichtigung. Diese Benachrichtigung beinhaltet die Informationen zur Konferenz, die vom Benutzer eingestellt wurden (Brückennummer, Teilnehmercode). Außerdem kann sie den festgelegten Text enthalten, der über das Menü **Konferenzeinwahl** eingestellt wurde.

The screenshot shows the 'Configuration' menu in the Avaya Administrator. The 'Conference Dial-in Information' section is expanded, showing a text area for dial-in information. The text area contains the following text:

Dial-in

To access conferences, dial 01555 220637 if external or 637 if internal, and follow the prompts.

Below the text area are 'Save' and 'Clear' buttons. A 'Note' section provides an example of audio access numbers:

Note:
 Example
 Audio Access Numbers:

- Audio Bridge: <>
- Participation Code: <>
- Web Collaboration URL: https://abc.org:port/meeting

So stellen Sie den festgelegten Text der Konferenzbenachrichtigung ein:

1. Wählen Sie **Konfiguration** und dann **Konferenzeinwahl**.
2. Geben Sie den festgelegten Text ein, der in allen Konferenzbenachrichtigungen angezeigt werden sollte.
3. Klicken Sie auf **Speichern**.

2.2.9 Ausfallsicherheit

Dieses Menü ist auf Linux-basierten Portalservern verfügbar, die ein IP Office Server Edition Select-Netzwerk unterstützen. Es enthält weitere Einstellungen für den Portalserver, die für die Ausfallsicherheit des Portalserver erforderlich sind. Siehe [Ausfallsicherheit](#)^[59].

- Bei vorhandenen Nichtauswahlmodus-Systemen, die in den IP Office Server Edition Select-Modus gewechselt sind, müssen ggf. die Portaldienste neu gestartet werden, damit die Ausfallsicherheitseinstellungen verfügbar werden. Außerdem müssen die Portaldienste eventuell neu gestartet werden, nachdem die Portalresilienz in der IP Office-Systemkonfiguration erstmalig konfiguriert wurde.

Einstellungen für den primären Server

Auf dem primären Server werden folgende Einstellungen angezeigt:

The screenshot shows the configuration interface for the primary server. On the left is a navigation menu with categories: Health, Configuration, Security, Diagnostics, Directory Integration, Gadgets Configuration, and IM Archive. Under Configuration, various services are listed as links. The main area shows a tree view of configuration options: Providers, Users, CSV, Branding, IM/Presence Server, IM/Presence Exchange Service, SMTP Configuration, Conference Dial-in Information, and Resiliency. The Resiliency section is expanded to show 'Failover and Failback Controls'. In this section, 'Failover' is set to 'Enabled' with a 'Failover Now' button. 'Failover Detection Time' is set to '3 mins'. 'Failback' is set to 'Automatic'. At the bottom of this section are buttons for 'Save', 'Clear', 'Refresh', and 'Defaults'.

- **Failover**

Geben Sie an, ob der Server Failover unterstützen soll. Wenn diese Option aktiviert ist, sollte der Domänenname des sekundären Portalserver im Formular [Host-Domänenname](#)^[32] angegeben sein.

- **Jetzt Failover durchführen**

Mit diesem Steuerelement kann der Failover-Prozess manuell eingeleitet werden.

- **Failovererkennungzeit**

Mit dieser Option wird die Dauer in Minuten festgelegt, bevor ein Failover erfolgt, nachdem potenzielle Probleme festgestellt wurden. Mit der Standardeinstellung (drei Minuten) wird verhindert, dass bei normalen Wartungsneustarts von Diensten ein Failover durchgeführt wird.

- **Failback**

Mit dieser Option wird festgelegt, ob der Failback-Prozess automatisch eingeleitet werden sollte, sofern möglich. Wenn „Manuell“ eingestellt ist, ist ein Neustart der Portaldienste für den Abschluss des Failbacks erforderlich.

Einstellungen für den Anwendungsserver

Die Einstellungen werden auch auf einem Anwendungsserver angezeigt. Wenn dieser Server in einem IP Office Server Edition Select-Netzwerk verwendet wird, kann er als Portalserver für den primären oder sekundären Server fungieren und den eingebetteten Portaldienst auf diesem Server ersetzen.

Health

Configuration

[Providers](#)

[Users](#)

[CSV](#)

[Branding](#)

[IM/Presence](#)

[Exchange service](#)

[SMTP Configuration](#)

[Conference Dial-in](#)

[Resiliency](#)

[Host Domain Name](#)

[Conference Clean Up](#)

[Central CTI Link](#)

▶ Providers

▶ Users

▶ CSV

▶ Branding

▶ IM/Presence Server

▶ IM/Presence Exchange Service

▶ SMTP Configuration

▶ Conference Dial-in Information

▼ Resiliency

Resiliency Configuration

Enable Resiliency

This one-X Portal is: Secondary ▼

	FQDN	IP Address
Primary one-X Portal	apps	
Primary IP Office		
Secondary one-X Portal		
Secondary IP Office		

Note:

- Changes to Resiliency configuration require restarting both the Primary and Secondary Standalone Resilient one-X Portal servers.

- **Ausfallsicherheit aktivieren**

Aktiviert die Portal-Ausfallsicherheit und zeigt zusätzliche Felder an, die zum Definieren der Adressen der anderen Server in der Ausfallsicherheitskonfiguration und der Rollen der Server erforderlich sind. Wenn die Ausfallsicherheit nicht aktiviert ist, wird der Portaldienst auf dem sekundären Server automatisch angehalten und kann nicht manuell neu gestartet werden.

- **Dieses one-X Portal:**

Definieren Sie die Rolle dieses Servers.

- **Primärer Server**

Wählen Sie diese Option, wenn dieser Server als primärer Portalserver fungieren soll.

- **Sekundärer Server**

Wählen Sie diese Option, wenn dieser Server als Reserve-/Ausweich-Portalserver fungieren soll, falls der primäre Portalserver nicht verfügbar ist.

- **FQDN/IP-Adresse**

Geben Sie in dieser Tabelle die vollqualifizierten Domännennamen oder die IP-Adressen aller Portale und IP Office-Server in der Ausfallsicherheitskonfiguration ein.

2.2.10 Host-Domänenname

Im Menü **Konfiguration | Host-Domänenname** wird der Domänenname festgelegt, der für den Zugriff auf die Portalienste und zwischen Portalservern verwendet wird. Die Anzahl der erforderlichen Domänennamen hängt vom Typ des Portalservers ab.

Beachten Sie, dass nach dem Ändern der Domänennamen der Portaldienst neu gestartet werden muss, damit die Änderungen übernommen werden.

Primary Host Domain Name	primary.example.com
Secondary Host Domain Name	secondary.example.com
Web Collaboration Domain Name	webconf.example.com

Note:

- Web Collaboration Domain Name will be used to generate Conference Web Collaboration URL.
- **Changes to Domain Name configuration require one-X Portal server restart.**

2.2.11 Bereinigung von Konferenzen

Mithilfe dieses Menüs kann konfiguriert werden, wie viele Tage der Server Konferenzdetails speichern soll. Für Windows-basierte Server wird diese Option nicht unterstützt.

Enter number of days after the conferences are cleaned up:

2.2.12 Zentrale CTI-Verbindung

IP Office Server Edition-Portalserver können den zentralen CTI-Modus verwenden. In diesem Modus muss der Portaldienst nur mit einem Linux-basierten IP Office-System verbunden sein, um Dienste für alle Systeme im Netzwerk bereitzustellen. Hierzu zählt ein IP Office Application Server, der mit IP Office Server Edition verwendet wird.

- Diese Option ist für UCM-basierte Server und für einen IP Office Application Server, der einen IP500 V2 unterstützt, nicht verfügbar.

Im zentralen CTI-Modus stellt der Portaldienst automatisch Anrufdienste für alle IP Office-Systeme im Netzwerk bereit. Er ruft Systemverzeichniseinträge aus allen Systemen und automatisch Einträge zu Systemen ab, die im Netzwerk hinzugefügt oder entfernt wurden. Außerdem ruft der Portaldienst automatisch Informationen über den zentralen Voicemail-Server ab.

The screenshot shows the configuration page for 'Central CTI Link'. On the left is a navigation menu with categories: Health, Configuration, Security, Diagnostics, and Directory Integration. Under 'Configuration', several sub-items are listed, including 'Central CTI Link'. The main content area shows a tree view of configuration options: Providers, Users, CSV, Branding, IM/Presence Server, IM/Presence Exchange Service, SMTP Configuration, Conference Dial-in Information, Host Domain Name, Conference Clean Up, and Central CTI Link Configuration. Under 'Central CTI Link Configuration', there is a checkbox labeled 'Central CTI Link' which is checked. Below the checkbox is a 'Save' button.

- **Zentrale CTI-Verbindung**

Mit dieser Einstellung wird der zentrale CTI-Modus aktiviert bzw. deaktiviert. Beachten Sie, dass der one-X Portal for IP Office-Dienst neu gestartet werden muss, wenn diese Einstellung geändert wird.

- **Bei aktivierter Option:**

Wenn diese Einstellung aktiviert ist, verwendet der Portaldienst den zentralen CTI-Modus. Dies bedeutet Folgendes:

- Das Portal stellt nur mit einem IP Office-System eine Verbindung her. CSTA- und DSML-Anbieter werden nur für dieses System erstellt. Die Verbindungen mit diesem System werden jedoch genutzt, um Informationen über alle anderen IP Office-Systeme im Netzwerk abzurufen und Dienste für diese bereitzustellen.
- Mithilfe der Verbindung mit dem IP Office-System werden außerdem die Voicemail-Servereinstellungen ermittelt und der erforderliche Anbieter automatisch erstellt.
- Wenn zudem [IP Office Server Edition-Ausfallsicherheit](#) aktiviert ist, werden CSTA-Anbieter für das primäre und sekundäre IP Office-System erstellt.
- Jedes einzelne dem Portalserver bekannte IP Office-System wird nach wie vor im Menü [Komponentenstatus](#) angezeigt.
- Das Portal ruft IP Office-Serverinformationen und -Systemverzeichnisse vom primären IP Office-System ab.
- Datensätze des persönlichen Verzeichnisses werden nach wie vor vom IP Office-Hostsystem der einzelnen Benutzer abgerufen.

- **Bei deaktivierter Option:**

Wenn diese Einstellung nicht aktiviert ist, gilt Folgendes:

- CSTA- und DSML-Anbieter müssen für jedes IP Office-System im Netzwerk manuell konfiguriert werden. Dies geschieht während der Installation und/oder über das Menü [Anbieter](#). Der Voicemail-Anbieter wird jedoch automatisch anhand von Informationen aus dem verbundenen IP Office-System bereitgestellt.
- Dies ist die Standardeinstellung für Systeme, die auf IP Office Version 10 aktualisiert werden.

Automatische Bereitstellung

Auf Systemen, für die ein Upgrade von Version 9.1 durchgeführt wurde, wird die ursprüngliche Einstellung **Autom. Bereitstellung** angezeigt und diese Einstellung anstelle von **Zentrale CTI-Verbindung** verwendet. Wenn **Automatische Bereitstellung** aktiviert ist, wird der erste verbundene CSTA-Anbieter für die automatische Erstellung zusätzlicher Anbieter sowie zur Verwaltung von CSTA- und DSML-Anbietern für alle anderen Systeme im Netzwerk verwendet. In Version 10.0 wird zudem dem Voicemail-Anbieter automatisch anhand der Informationen aus dem Telefonsystem konfiguriert.

Systeme, auf denen **Autom. Bereitstellung** verwendet wird, können durch Klicken auf die Schaltfläche **In zentrale CTI-Verbindung konvertieren** für die Verwendung von **Zentrale CTI-Verbindung** konfiguriert werden. Dieser Prozess kann nicht rückgängig gemacht werden.



2.2.13 Clientversionen blockieren

Dieses Menü kann zum Erstellen einer Liste mit Clientversionen verwendet werden, die vom Portal-Server nicht unterstützt werden sollen. Dies kann durch Hinzufügen der Clientversion und des Builds zur Liste der blockierten Clients erfolgen.

Blockierte Clients können sich nicht anmelden. Bereits angemeldete Clients können bis zum Abmelden weiterhin verwendet werden.

Für jeden Client können maximal 15 Kombinationen aus Version und Build blockiert werden.

The screenshot shows the 'Block Client Versions' configuration page. The left sidebar contains a navigation menu with the following items: Health, Configuration (selected), Providers, Users, CSV, Branding, IM/Presence, Exchange service, SMTP Configuration, Conference Dial-in, Host Domain Name, Conference Clean Up, Central CTI Link, Block Client Versions, Security, Diagnostics, Directory Integration, Gadgets Configuration, and IM Archive. The main content area shows a tree view with 'Block Client Versions' expanded. Below it is a form with three input fields: 'Select client' (a dropdown menu showing 'Avaya Communicator'), 'Client version', and 'Client build number'. A 'Save' button is to the right of the build number field. Below the form is a table titled 'List of blocked Avaya Communicator versions' with one row containing '2.1.4.0', '299', and a red 'X' icon.

So fügen Sie einen neuen blockierten Client hinzu:

1. Verwenden Sie das Dropdown-Menü **Client auswählen**, um den Client auszuwählen.
2. Geben Sie die **Clientversion** und die **Clientbuild**nummer ein. Es müssen beide Werte festgelegt sein.
3. Klicken Sie auf **Speichern**.

So entfernen Sie einen blockierten Client:

1. Klicken Sie auf das Kreuzsymbol.

2.3 Sicherheit

2.3.1 HTTP/HTTPS-Protokoll

Der Server wird standardmäßig ausschließlich mit Unterstützung für verschlüsselten HTTPS-Zugriff installiert; dies bedeutet Port 9443 auf einem Linux-Server und Port 8443 auf einem Windows-Server. Dieses Menü kann auch zur Aktivierung von HTTP-Zugriff auf Port 8080 verwendet werden.

The screenshot shows the 'Protocol' configuration page. The left sidebar contains a navigation menu with the following items: Health, Configuration (selected), Security, HTTP/HTTPS Protocol, TLS Settings, and ESNA Authentication. The main content area shows a form titled 'Select protocol option' with two radio buttons: 'Secure Connection (HTTPS) Only' (selected) and 'Unsecure and Secure (HTTP and HTTPS)'. A 'Save' button is below the radio buttons. Below the form is a 'Note' section with two bullet points: 'HTTP is insecure and prone to eavesdropping attacks.' and 'Note: Changes to Secure Connection settings require one-X Portal server restart. The one-X Portal will NOT function till the service is restarted.'

2.3.2 TLS-Einstellungen

Das Portalserver unterstützt TLS-Verbindungen für Benutzer und Anwendungen. Dies kann auf TLS 1.2-Verbindungen eingeschränkt werden.

- **Nur TLS 1.2-Clients zulassen**

Bei Aktivierung dieser Option wird die vom Portalserver bereitgestellte TLS-Unterstützung auf TLS 1.2 beschränkt. Wenn diese Einstellung geändert wird, müssen Sie [den Portaldienst neu starten](#)^[54], damit die Änderung wirksam wird.

- Beachten Sie, dass die aktuellen Avaya Communicator-Clientanwendungen TLS 1.2 nicht unterstützen und daher keine Verbindung herstellen können, wenn diese Option aktiviert ist.

2.3.3 ESNA-Authentifizierung

Benutzer, die mithilfe eines ESNA-Kontos eine Verbindung herstellen, müssen anhand der eigenen ESNA-Server authentifiziert werden.

- **Server-URL**

In diesem Feld wird die URL für Benutzerauthentifizierungs-Anforderungen festgelegt, die an den ESNA-Server umgeleitet werden.

2.3.4 Zertifikat

Über dieses Menü kann das Portal ein Zertifikat für den verschlüsselten Zugriff importieren. Dies ist für Anwendungen erforderlich, die eine verschlüsselte TLS-Verbindung mit dem Portal verwenden möchten, z. B. Avaya Communicator.

2.4 Diagnose

Mithilfe dieses Abschnitts können Sie verschiedene Diagnoseprüfungen durchführen.

2.4.1 Protokollierung konfigurieren

one-X Portal for IP Office unterstützt eine große Bandbreite von Protokollausgabemethoden, bei denen die gewünschte Protokollebene ausgewählt werden kann.

- Hauptprotokollebene**
 Dieses Feld dient zur Auswahl der Mindestprotokollebene für Ereignisse oder ermöglicht das Deaktivieren der Protokollierung durch Auswahl von **AUS**.
- Protokollverzeichnis**
 Das Verzeichnis, in dem der Server die Protokolldateien speichert. Kann nicht geändert werden.
- Größe des Protokollverzeichnisses**
 Die aktuelle Gesamtgröße der Protokolldateien.
- Aktualisieren**
 Durch Klicken auf diese Schaltfläche werden die angezeigten Informationen aktualisiert.
- Standardeinstellungen**
 Durch Klicken auf diese Schaltfläche wird die Hauptprotokollebene auf den Standardwert zurückgesetzt. Die Standardeinstellung ist **FEHLER** ausgenommen für Unified Communications Module-Server; hier ist die Standardeinstellung **AUS**.
- Protokolldateibeschreibungen:**
 In dieser Tabelle werden die von den verschiedenen one-X Portal for IP Office-Komponenten verwendeten Protokolldateien aufgeführt.
 - Telefonie (CSTA):** *1XCSTAServiceRollingFile.log*
 In diesem Protokoll werden Telefonieinformationen erfasst. Dazu gehört das Abrufen von Benutzer- und Lizenzinformationen aus den IP Office-Systemen.
 - Verzeichnis (IP Office):** *1XIPODirServiceRollingFile.log*
 In diesem Protokoll werden IP Office-Verzeichnisinformationen erfasst.
 - Verzeichnis (LDAP):** *1XLDAPDirServiceRollingFile.log*
 In diesem Protokoll werden LDAP-Verzeichnisinformationen erfasst.
 - IM/Anwesenheit:** *1XSCSServicesRollingFile.log*
 In diesem Protokoll werden IM- und Anwesenheitsdaten zu IP Office erfasst.
 - Insgesamt:** *1XOverallRollingFile.log*
 Dies ist eine allgemeine Protokolldatei aller protokollierten Ereignistypen.

-
- **Darstellungsschicht:** *1XPresentationLayerRollingFile.log*
In diesem Protokoll werden Informationen zur Browseraktivität des Benutzers erfasst.
 - **Mid-Layer:** *1XMidLayerRollingFile.log*
In diesem Protokoll wird die Interaktion zwischen den verschiedenen one-X Portal for IP Office-Komponenten (einschließlich IP Office-Systemen) erfasst.
 - **Protokollarchivierungsregel**
Mit diesen Einstellungen können Sie konfigurieren, wie die Protokolldateiaufbewahrung vom Server gesteuert wird. Standardmäßig werden die letzten fünf Protokolldateien aufbewahrt.
 - **Protokollarchivierungsregel – nach Größe**
Wenn diese Option ausgewählt ist, wird anhand der Einstellung für die Anzahl der Protokolldateien bestimmt, welche Dateien aufbewahrt werden. Bei Beginn einer neuen Datei (wenn Dateien eine Größe von etwa 50 MB erreichen, werden sie automatisch umgeleitet) wird die älteste Datei automatisch gelöscht, wenn die Anzahl der aufzubewahrenden Dateien überschritten wurde.
 - **Anzahl der zu bewahrenden archivierten Protokolle**
Legt die Anzahl der aufzubewahrenden Dateien fest, sofern die Option **Protokollarchivierungsregel – nach Größe** ausgewählt wurde. Die Standardeinstellung ist fünf Dateien.
 - **Protokollarchivierungsregel – nach Zeit**
Wenn diese Option ausgewählt ist, wird anhand des Alters der Protokolldateien in Tagen bestimmt, welche Dateien aufbewahrt werden. Ältere Dateien werden automatisch gelöscht.
 - **Anzahl der Tage zur Bewahrung archivierter Protokolle**
Legt die Anzahl der Tage, die eine Protokolldatei aufzubewahren ist, fest, sofern die Option **Protokollarchivierungsregel – nach Zeit** ausgewählt wurde. Die Standardeinstellung ist fünf Tage.

2.4.2 Protokollanzeige

Neben der Protokollierung in Dateien können die von den one-X Portal for IP Office-Komponenten ausgegebenen Protokollmeldungen auch über eine Remote-Protokollierungsanwendung angezeigt werden, die das Log4j-Format unterstützt. Das Menü **Diagnose | Protokollanzeige** bietet Links zu Informationen zu den Eigenschaften und der [Installation von Apache Chainsaw](#)⁹¹⁾, einer geeigneten Protokollierungsanwendung.

Health	▶ Logging Configuration
Configuration	▼ Logging Viewer
Diagnosics	▶ Description: Remotely viewing logs.
Logging Configuration	More information about Apache Chainsaw.
Logging Viewer	Start Installation of Apache Chainsaw by Java Web Start
Network Routes	
IP Office Connections	▶ Network Routes
Database Integrity	

2.4.3 Netzwerkrouuten

Mit diesem Menü kann das Routing vom one-X Portal for IP Office-Server zu einer IP Office-Adresse getestet werden. Es verwendet TCP zu Port 7 (Echo-Dienst) an der Ziel-IP-Adresse. Beachten Sie, dass dies nicht bei IP Office-Steuereinheiten funktioniert. Für diese sollten stattdessen die [IP Office-Verbindungen](#)⁴⁰⁾ verwendet werden.

Health	▶ Logging Configuration
Configuration	▶ Logging Viewer
Diagnosics	▼ Network Routes
Logging Configuration	▶ Description: Simple 'ping-like' test of network routability
Logging Viewer	IP Address <input type="text" value="192.168.42.12"/> <input type="button" value="Check"/>
Network Routes	Result <input type="text" value="Reachable"/>
IP Office Connections	▶ URL Connection Test
Database Integrity	▶ Database Integrity

So überprüfen Sie eine Netzwerkroute:

1. Wählen Sie **Diagnose** und dann **Netzwerkrouuten**.
2. Geben Sie die **IP-Adresse** des Ziels ein und klicken Sie auf **Prüfen**.
3. Der one-X Portal for IP Office-Server meldet, ob das Ziel **Erreichbar** oder **Nicht erreichbar** ist.

2.4.4 IP Office-Verbindungen

Mit diesem Menü kann die Verbindung zwischen dem one-X Portal for IP Office-Server und einem bestimmten IP Office-System überprüft werden. Die Verbindungsprüfung erfolgt mithilfe der Standarderkennungsmethode, die von IP Office-Anwendungen wie IP Office Manager verwendet wird (Verbindung zu Port 50804 der IP Office-Steuerinheit).

So testen Sie die IP Office-Verbindung:

1. Wählen Sie **Diagnose** und dann **IP Office-Verbindungen**.
2. Geben Sie die **IP-Adresse** des IP Office-Zielsystems ein und klicken Sie auf **Prüfen**.
3. Wenn IP Office erreichbar ist, enthalten die Ergebnisse grundlegende Informationen zum IP Office-System.

2.4.5 Datenbankintegrität

Mit diesem Menü können Sie die Datenbankstruktur überprüfen. Wenn die Tabellen und Felder in der Datenbank den Erwartungen für die jeweilige Version von one-X Portal for IP Office entsprechen, wird das Ergebnis **Bestanden** zurückgegeben. Die Daten innerhalb der Felder werden jedoch nicht überprüft. Ist das Ergebnis **Fail** (Nicht bestanden), suchen Sie im Abschnitt [Fehlerbehebung](#) nach bekannten Fehlern und Lösungen.

2.4.6 Benutzerdatenüberprüfung

Die Gruppe „Administrator und Avaya Backbone Support“ kann mögliche Ursachen bei der Benutzeranmeldung oder bei Benutzerdaten ermitteln, und mit der Diagnosefunktion in one-X Portal for IP Office können die beschädigten Daten zurückgesetzt werden.

The screenshot shows the 'User Data Validation' section of the one-X Portal for IP Office. The interface includes a sidebar with navigation links (Health, Configuration, Diagnostics) and a main content area. The 'User Data Validation' section is active, displaying a form with a text input for 'Enter User Name' containing 'Extn5506' and a 'Validate' button. Below the form, there are three rows of validation results: 'Marked Deleted?' (No), 'UI Preferences' (Valid), 'CSTA Configuration' (Valid), and 'User Configuration' (Valid). Each row has a corresponding XML preview window showing the data. A 'Reset' button is located to the right of the XML preview windows.

So zeigen Sie die Benutzerdatenüberprüfung an:

1. Klicken Sie in der Administratorschnittstelle von one-X Portal for IP Office auf **Diagnose**.
2. Wählen Sie **Benutzerdatenüberprüfung**, um rechts das entsprechende Formular anzuzeigen.
3. **Geben Sie den Benutzernamen** des Benutzers ein, dessen Daten validiert werden sollen. Dieses Feld kann mit dem Dropdown-Menü automatisch vervollständigt werden.
4. Klicken Sie auf **Überprüfen**. Das System validiert bestimmte Felder der Benutzerdaten in der Datenbank und zeigt die Ergebnisse an. Die validierten Felder sind:
 - **Als gelöscht gekennzeichnet?:** Gibt an, ob der Benutzereintrag gelöscht ist oder nicht.
 - **UI-Einstellungen:** Gibt an, ob die UI-Einstellungsdaten gültig sind oder nicht mit der entsprechenden XML einhergehen. Eine **Rückstelltaste** wird bereitgestellt, mit der Daten bei Beschädigung zurückgesetzt werden können. Die UI-Einstellung wird als Standardeinstellung neu gespeichert. Der Benutzer muss sich erneut bei one-X Portal for IP Office anmelden.
 - **CSTA-Konfiguration:** Gibt an, ob die CSTA-Konfiguration gültig ist oder nicht mit der entsprechenden XML einhergeht.
 - **Benutzerkonfiguration:** Gibt an, ob die Benutzerkonfiguration gültig ist oder nicht mit der entsprechenden XML einhergeht.

2.4.7 Anruf-/Konferenzplanung

Sie können eine zukünftige geplante Konferenz löschen. Wenn es sich dabei um eine wiederholte Konferenz handelt, werden alle Termine der Konferenz gelöscht.

Health	▶ Logging Configuration
Configuration	▶ Logging Viewer
Security	▶ Network Routes (Not for IP Offices)
Diagnostics	▶ IP Office Connections
Logging Configuration	▶ Database Integrity
Logging Viewer	▶ User data validation
Network Routes	▼ Call/Conference Scheduling
IP Office Connections	Enter Scheduled Conference ID to delete: <input type="text"/> <input type="button" value="Delete"/>
Database Integrity	Delete scheduled conference with subject: <input type="text"/> with host extension*: <input type="text"/> <input type="button" value="Delete"/>
User data validation	
Call/Conference Sched	
View Conferences	

So löschen Sie geplante Konferenzen:

1. Klicken Sie auf **Diagnosen** und wählen Sie **Anruf-/Konferenzplanung**.
2. Geben Sie die Host-Nebenstelle und ein Thema ein. Wenn Sie das Thema leer lassen, werden alle vom Host geplanten Konferenzen gelöscht.
3. Klicken Sie auf **Löschen**.

2.4.8 Konferenzen anzeigen

Dieses Menü zeigt den Kalender für geplante Konferenzen an, ähnlich dem Kalender, den Einzelbenutzer von one-X Portal for IP Office sehen und verwenden. Der Unterschied besteht darin, dass die geplanten Konferenzen für alle Benutzer angezeigt werden. Sie können mit diesem Menü eine geplante Konferenz löschen und die Details zukünftiger Konferenzen ändern.

Health	▶ Logging Configuration
Configuration	▶ Logging Viewer
Security	▶ Network Routes (Not for IP Offices)
Diagnostics	▶ IP Office Connections
Logging Configuration	▶ Database Integrity
Logging Viewer	▶ User data validation
Network Routes	▶ Call/Conference Scheduling
IP Office Connections	▼ View Conferences
Database Integrity	
User data validation	
Call/Conference Sched	
View Conferences	

New
 Historic
 All
 Non-Recurring
 Recurring

Host	Subject	Bridge Details	Date	Start Time	End Time	
212	Daily Meeting	Bridge:212	September 22, 2015	8:30 PM	9:00 PM	
212	Team Meeting	Bridge:212	September 22, 2015	6:00 PM	6:30 PM	

⏪
◀ Page 1 of 1 ▶
⏩

2.4.9 Speicherauszug erzeugen

Zur Diagnostizierung von Problemen muss Avaya einen Speicherauszug anfordern. Mit diesem Menü wird eine Speicherauszug-Protokolldatei für den aktuellen Betriebszustand des Servers erstellt. Der Dateiname beruht auf dem Datum und der Uhrzeit und weist die Endung **.hprof** auf.

Auf Linux-basierten Servern werden alle bestehenden Speicherauszugsdateien in den Protokolldateien berücksichtigt, die über die Web-Steuerungs-/Plattformansichtsmenüs (**Protokolle | Herunterladen**) des Servers heruntergeladen werden können.

2.4.10 Thread-Abbild erzeugen

Zur Diagnostizierung von Problemen muss Avaya ein Thread-Abbild anfordern. Mit diesem Menü wird eine Thread-Abbild-Protokolldatei für den aktuellen Betriebszustand des Servers erstellt. Der Dateiname setzt sich aus **onex_thread_dump** plus Datum und Uhrzeit und der Dateierdung **.log** zusammen.

Auf Linux-basierten Servern werden alle bestehenden Speicherauszugsdateien in den Protokolldateien berücksichtigt, die über die Web-Steuerungs-/Plattformansichtsmenüs (**Protokolle | Herunterladen**) des Servers heruntergeladen werden können.

2.5 Verzeichnisintegration

In diesem Abschnitt können Sie die Integration des Servers mit den verwendeten Verzeichnissen anzeigen und überprüfen.

2.5.1 Verzeichnissynchronisierung

Bei normalem Betrieb aktualisiert der one-X Portal for IP Office-Server die Einträge etwa alle 300 Sekunden. Über dieses Menü kann auch eine Aktualisierung des Systemverzeichnisses und der IP Office-Benutzer erzwungen werden.



- **Mit IP Office-Verzeichnissen neusynchronisieren**
Fordert eine Aktualisierung der Systemverzeichnis-Einträge an, die in den Konfigurationen der IP Office-Systeme gespeichert sind. Die Einträge im **Systemverzeichnis** können auch über die Option [Verzeichnisintegration | Systemverzeichnis](#)⁴⁶⁾ angezeigt und überprüft werden.

2.5.2 LDAP-Verzeichnissuche

Mit dieser Option können Sie das externe Verzeichnis auf dieselben Weise durchsuchen wie one-X Portal for IP Office-Benutzer. Dies gibt Ihnen die Möglichkeit, die Funktion des [LDAP-Anbieters](#)⁷⁰⁾ zu testen.

So durchsuchen Sie das LDAP-Verzeichnis:

1. Wählen Sie **Verzeichnisintegration**.
2. Wählen Sie **LDAP-Verzeichnissuche**.

3. Geben Sie einen Namen oder eine Nummer ein, für den bzw. für die es einen Eintrag im externen Verzeichnis gibt, und klicken Sie auf **Suchen**. Ist die Suche erfolgreich, werden die Ergebnisse unter dem Suchfeld angezeigt.

The screenshot shows the 'LDAP Directory Search' section of the administrator menu. On the left is a navigation sidebar with categories: Health, Configuration, Security, Diagnostics, and Directory Integration. Under 'Directory Integration', there are links for 'Directory Synchronization', 'System Directory', and 'LDAP Directory Search'. The main content area has a search input field with the placeholder text 'Enter a name or number' and a 'Search' button. Below the search field is a large empty box with the text 'Enter search text to find contacts'. At the bottom of the page, there is a pagination control showing 'Page' followed by a small empty box and navigation arrows.

2.5.3 Systemverzeichnis

Diese Option zeigt Ihnen das Systemverzeichnis in derselben Weise an, wie es one-X Portal for IP Office-Benutzern angezeigt wird. Sie können das Verzeichnis genauso durchsuchen wie bei Verwendung des one-X Portal for IP Office-Clients.

Mithilfe dieses Menüs können Sie überprüfen, ob das Verzeichnis erwartungsgemäß aussieht und Benutzer-, Gruppen- und Verzeichniseinträge aus jedem unterstützten IP Office-System enthält.

- **Hinweis:** Das System zeigt keine Sammelanschlüsse an, die in der Konfiguration des Telefonsystems als „Außerhalb des Verzeichnisses“ festgelegt sind.

Der one-X Portal for IP Office-Server aktualisiert die Einträge im System- und persönlichen Verzeichnis etwa alle 300 Sekunden. Mit der Option [Verzeichnissynchronisierung](#)^[44] können Sie eine Aktualisierung erzwingen.

- Bei einigen Verzeichniskontakten zeigt one-X Portal for IP Office den aktuellen Kontaktstatus mithilfe verschiedener Symbole an. Bei Kontakten mit mehreren Telefonnummern beruht der Status auf der Dienstnummer.

Status	Symbol	Beschreibung
Verfügbar		Normaler Status für einen Benutzer, bei dem der Status des aktiven Dienstanschlusses angezeigt wird.
Besetzt		Normaler Status für einen Benutzer, von dessen Dienstanschluss aus gerade ein Gespräch geführt wird.
Nicht stören		Der Benutzer hat die Funktion Nicht stören eingestellt. Anrufe an den Benutzer werden an Voicemail weitergeleitet (falls aktiviert), oder es ertönt ein Besetztzeichen, sofern Sie nicht in der Liste Ausnahmenummern für „Nicht stören“ des Benutzers eingetragen sind.
Abgemeldet		Der Benutzer hat sich von seinem Telefon abgemeldet. Anrufe an den Benutzer gehen höchstwahrscheinlich an Voicemail (falls verfügbar).
Sonstige		Dieses Symbol wird verwendet, wenn der Status nicht bekannt ist bzw. nicht bekannt sein darf, z. B. externe Nummern.
Klingeln		Dieses Symbol wird für einen internen Kontakt verwendet, von dem gerade ein Anruf eingeht.

Hinzufügen und Bearbeiten von Portalkontakten

Mit dem Symbol können Sie einen neuen Systemverzeichnis-Kontakt hinzufügen. Beachten Sie, dass auf diese Weise hinzugefügte Kontakte nur von one-X Portal for IP Office gespeichert werden, und sie sind somit von Benutzern nur über one-X Portal for IP Office erreichbar. Für diese Kontakte können bei Bedarf mehrere Telefonnummern und E-Mail-Adressen konfiguriert werden.

Zum Löschen von Kontakten, die auf diese Weise hinzugefügt wurden, klicken Sie auf den jeweiligen Kontakt, und wählen das Löschsymbol aus.

2.6 Konfiguration der Minianwendungen

Als Administrator von one-X Portal for IP Office können Sie im System eine Liste externer Minianwendungen konfigurieren. Sie können die Minianwendungen freischalten, bearbeiten oder löschen, die der Benutzer von one-X Portal for IP Office hinzufügen kann. Der Benutzer von one-X Portal for IP Office kann nur die externen Minianwendungen hinzufügen, die der Administrator freigeschaltet hat.

2.6.1 Externe Minianwendungsliste

Alle externen Minianwendungen, die im System vorhanden sind, werden in der **Liste externer Minianwendungen** aufgeführt. Standardmäßig sind keine externen Minianwendungen auf dem one-X Portal for IP Office konfiguriert. Als Administrator können Sie für den Benutzer [eine externe Minianwendung hinzufügen](#)^[63] oder [externe Minianwendungen importieren](#)^[63].

2.6.2 Importieren von Minianwendungen

Sie können externe Minianwendungen als XML-Datei importieren. Benutzer können diese Minianwendungen dann wählen. Siehe [Importieren von Kontakten](#)^[63].



So importieren Sie eine Datei einer Minianwendung:

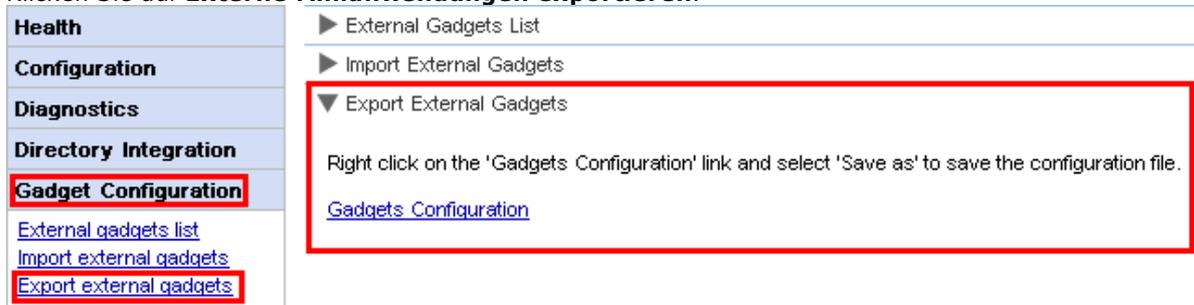
1. Klicken Sie auf **Konfiguration der Minianwendungen** und wählen Sie **Externe Minianwendungen importieren**.
2. Klicken Sie auf **Datei auswählen**, um die Konfigurationsdatei zu suchen und auszuwählen.
3. Klicken Sie auf **Hochladen**. Das System lädt die XML-Datei hoch zum one-X Portal for IP Office.
4. Klicken Sie auf **Importieren**, um die Minianwendung eines Drittanbieters der *Liste externer Minianwendungen* hinzuzufügen.
5. Bei der nächsten Anmeldung des Benutzers im one-X Portal for IP Office kann der Benutzer die Minianwendung eines Drittanbieters dem Portal hinzufügen.

2.6.3 Exportieren von Minianwendungen

Die vorhandenen Einstellungen für externe Minianwendungen in one-X Portal for IP Office können als Konfigurationsdatei exportiert werden. Die Konfigurationsdatei ist im XML-Format. Die Konfigurationsdatei enthält Informationen über die Parameter der Minianwendungen. Sie können diese Zusammenstellung von Minianwendungen zum one-X Portal for IP Office eines anderen Benutzers hinzufügen, indem Sie die gespeicherte Konfigurationsdatei [importieren](#)⁶³.

So exportieren Sie eine Minianwendung von Drittanbietern:

1. Klicken Sie im linken Navigationsfenster auf **Konfiguration der Minianwendungen**.
2. Klicken Sie auf **Externe Minianwendungen exportieren**.



3. Klicken Sie mit der rechten Maustaste auf den Link **Konfiguration der Minianwendungen**.
4. Wählen Sie **Speichern unter**, um die Konfigurationsdatei zu speichern.

2.7 IM-Archiv

Als Administrator von one-X Portal for IP Office können Sie die IM-Konversationen aller Benutzer durchsuchen. Siehe [Aktivieren/Deaktivieren der IM-Archivierung](#)^[78].

2.7.1 Archiv durchsuchen

Sie können nach IM-Gesprächen zwischen Benutzern und zwischen System und Benutzer suchen. Alle Felder im Suchfeld sind optional. Die Anzahl der Tage, für die der Server IM-Nachrichten archiviert, wird mit der Einstellung [Tage für die Archivierung von IMs](#)^[79] festgelegt.

<ul style="list-style-type: none"> Health Configuration Security Diagnostics Directory Integration Gadgets Configuration Web Conferences IM Archive Search Archive 	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Participants <input type="text" value="Extn210"/> Start <input type="text" value=""/> Keywords <input type="text"/></p> <p><input type="text"/> End <input type="text"/></p> <p><input type="button" value="Search"/> <input type="button" value="Clear"/> <input type="button" value="Export"/></p> </div>																
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Participants</th> <th style="width: 30%;">Start</th> <th style="width: 10%;">Count</th> <th style="width: 30%;"></th> </tr> </thead> <tbody> <tr> <td>Extn210 mybuddy</td> <td>Aug 15, 2014 12:00 PM</td> <td>4</td> <td></td> </tr> <tr style="background-color: #e0e0e0;"> <td>Extn210 Extn211</td> <td>Aug 15, 2014 8:05 AM</td> <td>2</td> <td></td> </tr> <tr> <td>Extn210 everyone</td> <td>Aug 14, 2014 2:13 PM</td> <td>1</td> <td></td> </tr> </tbody> </table> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Participants: Extn210, Extn211</p> <p>Date: Aug 15, 2014 8:05 AM</p> <p>Keyword:</p> <p>7:59 Extn210 : Morning. How are the updates going?</p> <p>8:5 Extn211 : Okay now we have the system running. Tell you how far we got at the end of today.</p> </div>	Participants	Start	Count		Extn210 mybuddy	Aug 15, 2014 12:00 PM	4		Extn210 Extn211	Aug 15, 2014 8:05 AM	2		Extn210 everyone	Aug 14, 2014 2:13 PM	1	
Participants	Start	Count															
Extn210 mybuddy	Aug 15, 2014 12:00 PM	4															
Extn210 Extn211	Aug 15, 2014 8:05 AM	2															
Extn210 everyone	Aug 14, 2014 2:13 PM	1															

So durchsuchen Sie das IM-Archiv:

1. Wählen Sie im linken Teilfenster das **IM-Archiv** aus.
2. Klicken Sie auf **Archiv durchsuchen**.
3. Geben Sie die Suchkriterien ein, und klicken Sie auf „Suchen“.

Feld	Beschreibung
Teilnehmer	Geben Sie den Namen des Teilnehmers der IM-Unterhaltung ein.
Stichwörter	Geben Sie Stichwörter aus der IM-Unterhaltung ein.
Starten	Wählen Sie das Datum aus, ab dem Unterhaltungen aufgelistet werden sollen. Wenn Sie kein Datum auswählen, beginnt die Anzeige bei der frühesten vom System gespeicherten Unterhaltungen.
Ende	Wählen Sie das Datum aus, bis zu dem Unterhaltungen aufgelistet werden sollen. Wenn Sie kein Datum auswählen, werden alle Unterhaltungen bis zur letzten Unterhaltung angezeigt.

4. Klicken Sie auf die Unterhaltung, die Sie öffnen möchten. Die Unterhaltung wird angezeigt.

2.9 Hilfe und Support

Hilfe | Hilfe

Enthält Links zu der one-X Portal for IP Office-Benutzerhilfe und zu diesem Dokument als Hilfestellung.

Hilfe | Unterstützung von Avaya

Lädt einen Link zur Avaya Support-Webseite (<http://support.avaya.com>).

Hilfe | Info

Zeigt grundlegende Versionsinformationen zur one-X Portal for IP Office-Installation an.

Health	▶ Help
Configuration	▶ Avaya Support
Security	▼ About
Diagnostics	Avaya one-X Portal for IP Office Copyright 2015 Avaya Inc. All Rights Reserved.
Directory Integration	Version: 10.0.0.0.0 build 259
Gadgets Configuration	
IM Archive	
Web Conferences	
Help & Support	
Help	Links to the licences of the third-party software components used in one-X Portal for IP Office.
Avaya Support	H2 1.0.75 License
About	GWT 1.5.3 License
	GWT Rocket 0.56 License
	Apache Tomcat 6 License
	Apache Log4j 1.2.15 License

Kapitel 3.

Wartungsaufgaben

3. Wartungsaufgaben

3.1 Neustarten des Dienstes

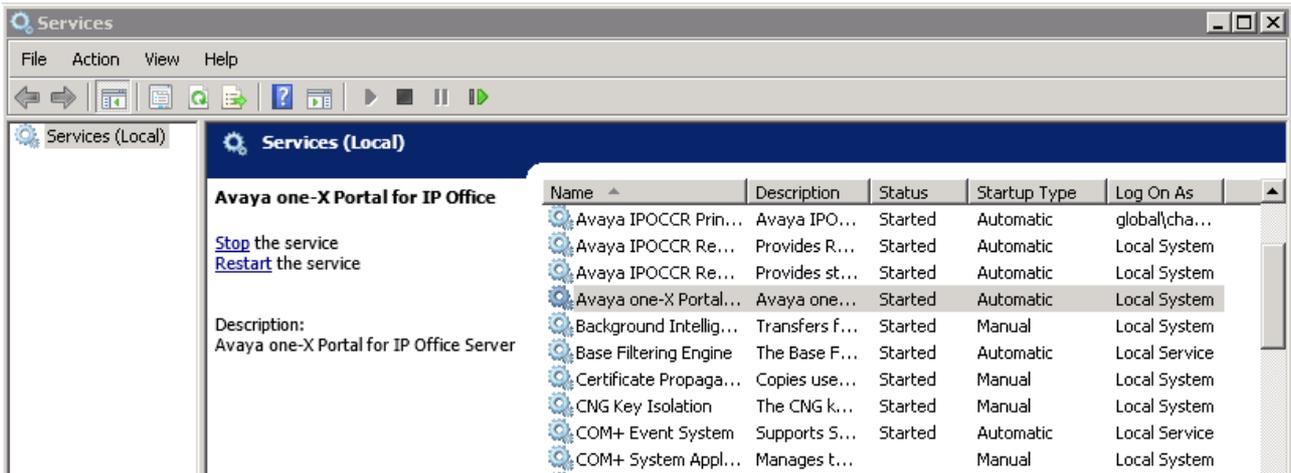
Der one-X Portal for IP Office-Dienst kann auf mehrere Weise beendet und neu gestartet werden.

Über die Administratormenüs

Sie können im oberen Bereich der Administratormenüs auf das Symbol  klicken, um den Portaldienst neu zu starten. Dieses Symbol wird automatisch angezeigt, wenn Sie Änderungen vornehmen, die einen Neustart erfordern.

Windows-basierter Server

Die one-X Portal for IP Office-Anwendung wird als Dienst namens Avaya one-X Portal installiert. Sie kann über das Standardelement „Dienste“ der Windows-Systemsteuerung gestartet und beendet werden.



Beachten Sie, dass der Avaya one-X Portal-Dienst nach dem Starten oder Neustarten bis zu 15 Minuten braucht, bis er voll funktionsfähig ist, auch wenn er als gestartet angezeigt wird. Der Fortschritt kann u. a. mit dem Windows Task-Manager überwacht werden. Beim Starten von one-X Portal for IP Office wächst die **Auslagerungsdatei** gewöhnlich allmählich auf ungefähr 2.3 GB an, bevor one-X Portal for IP Office vollends gestartet ist.

- **Kein Dienst!**

Wenn der Dienst nicht verfügbar ist, liegt dies wahrscheinlich an einem Port-Konflikt oder einem Java-Problem. Siehe [Fehlerbehebung](#).

Linux-basierter Server

1. Wählen Sie über die Web-Verwaltungsmenüs für den Server **Lösung**.
2. Klicken Sie auf das Symbol , und wählen Sie **Plattformansicht**.
3. In der Plattformansicht wird der Status des one-X Portal-Dienstes auf der Registerkarte **System** angezeigt. Klicken Sie zum Stoppen des Dienstes auf **Stopp** oder **Stopp erzwingen**. Klicken Sie zum Starten des Dienstes auf **Start**.

3.2 Konfiguration des Anrufprotokolls

Das von one-X Portal for IP Office angezeigte Benutzeranrufprotokoll wird als Teil der Benutzereinstellungen im Telefonsystem gespeichert. Es werden bis zu 30 Datensätze gespeichert und alte Datensätze werden durch neue ersetzt, wenn die Grenze erreicht wurde. Bei wiederholten Anrufen an dieselbe bzw. von derselben Nummer wird der vorhandene Datensatz jedoch aktualisiert und die Anzahl der Anrufe im Datensatz erhöht.

Bei eingehenden Anrufen werden standardmäßig lediglich persönliche Anrufe (nicht zum Sammelanschluss gehörend) an den Benutzer, die dieser angenommen hat oder die nicht angenommen wurden, in das Anrufprotokoll aufgenommen.

- **Verpasste Anrufe**
Anrufe, die nicht vom Benutzer, sondern von Voicemail oder einer anderen Nebenstelle entgegengenommen werden, werden normalerweise nicht als verpasste Anrufe protokolliert. Um die Protokollierung verpasster Anrufe zu aktivieren, sollte die systemweite Einstellung **Verpasste Anrufe, die bei der Übergabe beantwortet wurden, protokollieren (System | Telefonie | Anrufprotokoll)** in der Telefonsystem-Konfiguration des IP Office aktiviert sein.
- **Entgangene Sammelanschlussanrufe**
Standardmäßig werden nur die vom Benutzer entgegengenommenen Sammelanschlussanrufe protokolliert. Um die Protokollierung verpasster Hunt-Gruppen-Anrufe zu aktivieren, sollte die systemweite Einstellung **Verpasste Hunt-Gruppen-Anrufe protokollieren** ebenfalls in der Telefonsystem-Konfiguration des IP Office aktiviert sein. Der Benutzer muss ebenfalls in den Telefonsystemen mit den Hunt-Gruppen, für die das Anrufprotokoll verpasste Anrufe enthalten kann (**Benutzer | Telefonie | Anrufprotokoll**), konfiguriert sein.
- **Automatisches Löschen**
Alte Anrufrdatensätze werden automatisch gelöscht, wenn die Kapazität des Anrufprotokolls erreicht wurde und ein neues Anrufprotokoll hinzugefügt werden muss. Außerdem können Sie über die Telefonsystem-Konfiguration das Telefonesystem so konfigurieren, dass es Protokolleinträge nach einem festgesetzten Zeitraum löscht. Wählen Sie **Einträge löschen nach (Benutzer | Telefonie | Anrufprotokoll)**.

Verlauf des Telefongesprächs.

Wenn der Benutzer ein Telefon der 1400, 1600, 9500 oder 9600 Serie mit einer **Anrufprotokoll**- oder einer **Verlauf**-Taste, oder ein Telefon der M- oder T-Serie verwendet, wird standardmäßig das gleiche Anrufprotokoll wie auf dem Portal auf dem Telefon angezeigt. Sie können das Anrufprotokoll dann über das Telefon oder das one-X Portal for IP Office verwenden und bearbeiten. Beide werden parallel geändert.

Für Benutzer, die ein anderes Telefonmodell mit einem integrierten Anrufprotokoll verwenden, wird das Anrufprotokoll durch das Telefon gespeichert und stimmt daher nicht zwangsweise mit dem im one-X Portal for IP Office angezeigten Anrufprotokoll überein. Über one-X Portal for IP Office getätigte Anrufe werden z. B. nicht im Anrufprotokoll des Telefons angezeigt und umgekehrt.

In beiden Fällen ist das one-X-Anrufprotokoll auf die Anzeige von 255 Datensätzen beschränkt.

3.3 IP Office-Schalter

3.3.1 Hinzufügen eines weiteren IP Office-Systems

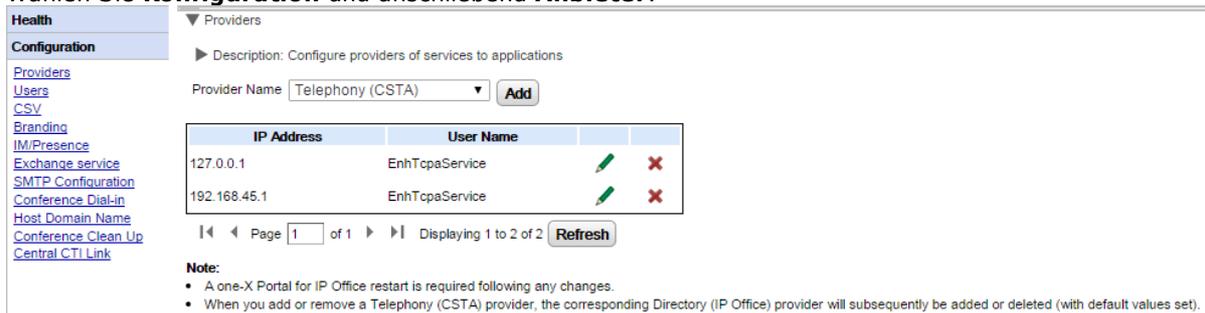
Zum Hinzufügen eines weiteren IP Office-Systems innerhalb des Small Community Networks muss dem Telefonie-Anbieter (CSTA) und dem Verzeichnisanbieter (IP Office) die IP-Adresse des Systems zugewiesen werden.

- **Automatische Bereitstellung/zentraler CTI-Modus**^[33]
Ein Linux-basierter Potalsserver, der ein IP Office Server Edition-Netzwerk unterstützt, kann vom primären IP Office-System über andere IP Office-Systeme im Netzwerk und auf dem Voicemail-Server informiert werden. Es werden dann vom ihm automatisch die entsprechenden Anbieter für diese anderen Systeme hinzugefügt oder entfernt. Dies erfolgt mit der Einstellung **Zentrale CTI-Verbindung**, die in neuen Installationen standardmäßig aktiviert ist. Wenn sie aktiviert ist, müssen Anbieter für zusätzliche IP Office-Systeme nicht manuell konfiguriert werden. Im zentralen CTI-Modus gilt Folgendes:
 - Wenn keine Ausfallsicherheit verwendet wird, benötigt der Server nur einen DMSL-Anbieter für das primäre IP Office-System.
 - Wenn Ausfallsicherheit verwendet wird, benötigt der Server nur einen DMSL-Anbieter für das primäre und sekundäre IP Office-System.
 - Der Server benötigt nur einen CSTA-Anbieter für das primäre IP Office-System, es sei denn, Portalausfallsicherheit wird verwendet; in diesem Fall muss auch ein CSTA-Anbieter für das sekundäre IP Office-System vorhanden sein.

So fügen Sie ein weiteres IP Office-System hinzu::

- **Achtung**
Für diesen Prozess müssen Sie den **Portaldienst neu starten**^[54], damit die Änderungen übernommen werden. Das Portal ist während des Neustarts möglicherweise bis zu 15 Minuten lang nicht für Benutzer verfügbar.
1. Vor dem Hinzufügen eines weiteren IP Office-Systems zur one-X Portal for IP Office-Konfiguration:
 - Überprüfen Sie, ob IP Office mit den Sicherheitseinstellungen für den Betrieb von one-X Portal for IP Office konfiguriert wurde.
 - Überprüfen Sie, ob IP Office für one-X Portal for IP Office lizenziert ist.
 - Überprüfen Sie, ob mindestens ein Benutzer auf dem IP Office-System für one-X Portal for IP Office aktiviert ist.
 2. **Melden Sie sich als Administrator an**^[9].
 3. Überprüfen Sie, ob das IP Office-System über den one-X Portal for IP Office-Server angezeigt werden kann.
 - a. Wählen Sie **Diagnose** und dann **IP Office-Verbindungen**.
 - b. Geben Sie die **IP-Adresse** des IP Office-Zielsystems ein und klicken Sie auf **Prüfen**.
 - c. Wenn IP Office erreichbar ist, enthalten die Ergebnisse grundlegende Informationen zum IP Office-System.

4. Wählen Sie **Konfiguration** und anschließend **Anbieter**.



Providers

Description: Configure providers of services to applications

Provider Name:

IP Address	User Name		
127.0.0.1	EnhTcpcService		
192.168.45.1	EnhTcpcService		

Page 1 of 1 | Displaying 1 to 2 of 2 |

Note:

- A one-X Portal for IP Office restart is required following any changes.
- When you add or remove a Telephony (CSTA) provider, the corresponding Directory (IP Office) provider will subsequently be added or deleted (with default values set).

5. Klicken Sie auf **Hinzufügen**.



Edit Telephony (CSTA)

This control enables you to add & delete the IP Office Unit(s) mapped to a provider.

IP Address	192.168.45.1
User Name	EnhTcpcService
Password	*****

6. Geben Sie die **IP-Adresse** des neuen IP Office-Systems ein.

7. Geben Sie unter **Benutzername** und **Kennwort** einen Benutzernamen und ein Kennwort ein, der/das mit dem im IP Office-System konfigurierten TCPA-Sicherheitsbenutzer übereinstimmt.
8. Klicken Sie auf **Speichern**.
9. [Starten Sie den Avaya one-X Portal-Dienst neu](#)⁵⁴. Sobald der Dienst vollständig neu gestartet ist, melden Sie sich wieder bei den Administrationsmenüs an.
10. Wählen Sie **Status** und dann **Komponentenstatus**.
11. Klicken Sie auf **Alle abrufen**. Neue CSTA- und DSML-Komponenten für die IP-Adresse des neu hinzugefügten IP Office-Systems sollten eingeschlossen sein. Der Status dieser Komponenten sollte verfügbar sein.
12. Wählen Sie **Verzeichnisintegration**. Überprüfen Sie, ob die Benutzer des neuen IP Office-Systems aufgelistet werden. Falls nicht, wählen Sie **Telefonbuchsynchronisierung | Neusynchronisierung mit IP Office-Telefonbüchern erzwingen** und warten 5 Minuten.
13. Wählen Sie **Konfiguration** und anschließend **Benutzer**. Klicken Sie auf **Alle abrufen**. Überprüfen Sie, ob die Benutzer des neuen IP Office-Systems aufgelistet werden.

3.3.2 Ändern von IP Office-Details

Wenn die Details (IP-Adresse, Benutzername oder Kennwort des T CPA-Dienstes) eines zugewiesenen IP Office-Systems geändert werden, müssen die IP Office-Einstellungen in den one-X Portal for IP Office-Anbietern entsprechend aktualisiert werden.

- **Achtung**
Für diesen Prozess müssen Sie den [Portaldienst neu starten](#)⁵⁴, damit die Änderungen übernommen werden. Das Portal ist während des Neustarts möglicherweise bis zu 15 Minuten lang nicht für Benutzer verfügbar.

So ändern Sie die Details von IP Office:

1. [Melden Sie sich als Administrator an](#)⁹.
2. Wenn sich die IP-Adresse des IP Office-Systems geändert hat, überprüfen Sie, ob das IP Office-System über den one-X Portal for IP Office-Server angezeigt werden kann.
 - a. Wählen Sie **Diagnose** und dann **IP Office-Verbindungen**.
 - b. Geben Sie die **IP-Adresse** des IP Office-Zielsystems ein und klicken Sie auf **Prüfen**.
 - c. Wenn IP Office erreichbar ist, enthalten die Ergebnisse grundlegende Informationen zum IP Office-System.
3. Wählen Sie **Konfiguration** und anschließend **Anbieter**.

Providers

Description: Configure providers of services to applications

Provider Name:

IP Address	User Name		
127.0.0.1	EnhTcpaService		
192.168.45.1	EnhTcpaService		

Page 1 of 1 | Displaying 1 to 2 of 2 |

Note:

- A one-X Portal for IP Office restart is required following any changes.
- When you add or remove a Telephony (CSTA) provider, the corresponding Directory (IP Office) provider will subsequently be added or deleted (with default values set).

4. Klicken Sie auf das Symbol neben dem vorhandenen CSTA-Anbieter, dem das IP Office-System zugewiesen wurde.

Edit Telephony (CSTA)

This control enables you to add & delete the IP Office Unit(s) mapped to a provider.

IP Address	192.168.45.1
User Name	EnhTcpaService
Password	*****

5. Bearbeiten Sie die angezeigten Details, um sie den neuen Einstellungen des IP Office-Systems anzupassen, und klicken Sie dann auf **Speichern**.
6. Starten Sie den [Portaldienst](#)⁵⁴ neu.

3.3.3 Ausfallsicherheit

Bei IP Office Version 10 und höher wird der Portaldienst standardmäßig auch auf dem sekundären IP Office Server Edition-Server installiert. So kann dieser sekundäre Server als Portalserver für Benutzer fungieren, wenn der primäre Server aus irgendeinem Grund nicht verfügbar ist.

- Portalausfallsicherheit wird im IP Office Server Edition Select-Modus unterstützt. Portalausfallsicherheit kann auch konfiguriert werden, wenn ein IP Office Application Server anstelle des Portaldiensts des primären oder sekundären Servers verwendet wird.
 - Bei vorhandenen Nichtauswahlmodus-Systemen, die in den IP Office Server Edition Select-Modus gewechselt sind, müssen ggf. die Portaldienste neu gestartet werden, damit die Ausfallsicherheitseinstellungen verfügbar werden. Außerdem müssen die Portaldienste eventuell neu gestartet werden, nachdem die Portalresilienz in der IP Office-Systemkonfiguration erstmalig konfiguriert wurde.
- Ausfallsicherheit wird nur zwischen dem primären und sekundären Server unterstützt, wenn auf diesen die gleiche Version der Portalsoftware ausgeführt wird.
- Während des normalen Betriebs (beide Server sind in Betrieb und miteinander verbunden) werden Änderungen, die von Benutzern und Administratoren am primären Server vorgenommen werden, automatisch mit dem sekundären Server synchronisiert. Jedoch werden Änderungen, die während eines Failovers an einem der Server vorgenommen werden, nicht synchronisiert, und diese gehen möglicherweise verloren, wenn der normale Betrieb der Server wiederaufgenommen wird.
 - Geplante Konferenzen sind davon zurzeit ausgenommen. Konferenzen, die auf dem primären Server geplant sind, finden während des Failover-Betriebs nicht statt. Konferenzen, die auf dem sekundären Server geplant sind, gehen beim Failback verloren.
- In der Plattformsicht (Web-Steuerung) des jeweiligen Servers:
 - wird der aktive Portalserver als „Verfügbar“ (grünes Symbol) angezeigt.
 - wird der passive Portalserver mit dem Status „Startet“ (orangefarbenes Symbol) angezeigt.
- Portalclientanwendungen wie one-X Portal Call Assistant werden nicht automatisch umgeleitet. Der Benutzer muss die Adresse des sekundären Servers eingeben, um sich anzumelden.

Bei konfigurierter Portalausfallsicherheit gilt Folgendes:

- **Bei Ausfall des Portals auf dem primären Server**
Wenn der Portaldienst des primären Servers aus irgendeinem Grund gestoppt wird, wird automatisch der Portaldienst auf dem sekundären Server verfügbar.
 - Benutzer, die beim Portal auf dem primären Server angemeldet waren, können sich auf dem sekundären Server erneut anmelden.
 - Wenn der primäre IP Office-Dienst noch ausgeführt wird, werden diese Portalbenutzer automatisch umgeleitet.
 - Wenn der Benutzer nicht zuvor auf den sekundären Portalserver zugegriffen hat, muss er das Sicherheitszertifikat akzeptieren oder eine Ausnahme erstellen. Hierdurch wird die automatische Verbindungswiederherstellung unterbrochen.
 - Das Gleiche gilt für Benutzer, die bei einem der Portal-Clients, z. B. dem Outlook-Plug-In, angemeldet waren.
 - Neue Benutzer, die sich anmelden möchten, müssen die Adresse des sekundären Servers verwenden.
- **Bei einem IP Office-Ausfall auf dem primären Server:**
Wenn der IP Office-Dienst auf dem primären Server aus irgendeinem Grund gestoppt wird, werden die Portaldienste automatisch an den sekundären Server übertragen, wie oben beschrieben.
 - Wenn die IP Office-Kerneinheit nicht in Betrieb ist, können Benutzer, die zu dieser Kerneinheit gehören, persönliche Kontakte in der Portal-Minianwendung „Verzeichnis“ nicht aktualisieren oder löschen.
- **Bei Netzwerkausfall:**
Wenn die Netzwerkverbindung zwischen primärem und sekundärem Server aus irgendeinem Grund unterbrochen wird, werden beide Portalserver aktiv, und Benutzer können sich anmelden. Auch hier werden Änderungen an Benutzer- und Administratoreinstellungen, die auf dem sekundären Portalserver vorgenommen werden, bei Wiederherstellung der Netzwerkverbindung nicht auf den primären Server kopiert. Dies wird als „eigenständiger Modus“ bezeichnet.
- **Bei Wiederherstellung des Portals auf dem primären Servers:**
Wenn der Portaldienst auf dem primären Server wieder verfügbar ist, können sich Benutzer nicht länger beim Portaldienst auf dem sekundären Server anmelden.
 - Benutzer, die beim Portal auf dem sekundären Server angemeldet waren, werden automatisch umgeleitet und können sich auf dem primären Server erneut anmelden.
 - Benutzer, die bei einem der Portal-Clients wie z. B. dem Outlook-Plug-in angemeldet waren, werden automatisch mit dem primären Server verbunden.

-
- Neue Benutzer, die sich anmelden möchten, werden zum primären Server umgeleitet.
 - **Bei IP Office-Wiederherstellung auf dem primären Server:**
Wenn der IP Office-Dienst auf dem primären Server wieder verfügbar ist, wird der Portaldienst nur noch auf dem primären Server unterstützt, wie oben beschrieben.

So konfigurieren Sie Ausfallsicherheit:**1. Aktivieren des zentralen CTI-Verbindungsmodus**

Beide Portalserver müssen für die Verwendung des zentralen CTI-Verbindungsmodus konfiguriert sein. Dies ist die Standardeinstellung für eine neue Installation; für vorhandene Systeme, die auf IP Office Version 10 oder höher aktualisiert werden, muss die Einstellung jedoch manuell aktiviert werden.

- a. Der zentrale CTI-Verbindungsmodus wird über das Menü **Zentrale CTI-Verbindung** ³³ aktiviert.
- b. Wenn die Einstellungen geändert wird, ist ein Neustart des Portaldiensts erforderlich, damit die Änderung wirksam wird.
- c. Die Einstellung muss sowohl auf dem primären als auch auf dem sekundären Server aktiviert werden.

2. Aktivieren der Ausfallsicherheit des Portalservers

Die Ausfallsicherheit des primären Portalservers muss seine Menüs für die **Ausfallsicherheitskonfiguration** ³⁰ konfiguriert werden.

3. Neustarten der Portaldienste

Wenn Änderungen in den vorstehenden Schritten vorgenommen werden.

4. Aktivieren der Portalsicherung auf Netzwerkamtsleitungen

Für die SCN-Amtsleitungen zwischen dem primären und sekundären IP Office-Server muss die Einstellung für Portalsicherung aktiviert werden.

- a. Laden Sie mithilfe von IP Office Manager die Konfiguration aus den IP Office Server Edition IP Office-Systemen.
- b. Suchen Sie in den Einstellungen des primären Systems die IP Office-Leitung vom primären zum sekundären IP Office-System.
- c. Überprüfen Sie auf der Registerkarte **Leitung** unter **SCN-Ausfallsicherheitsoptionen**, ob **Unterstützt Ausfallsicherheit** und **Reservesystem für mein one-X Portal** aktiviert sind.
- d. Speichern Sie die Konfigurationsänderungen.

3.4 Minianwendungen

3.4.1 Auslesen der URL einer Minianwendung

Google bietet eine Auswahl von Minianwendungen an, die Sie Ihrer Webseite hinzufügen können.

Beispiel: So finden Sie die URL einer Google-Minianwendung:

1. Eine Liste der von Google angebotenen Minianwendungen finden Sie unter:
<http://www.google.com/ig/directory?synd=open>
2. Wählen Sie die Minianwendung aus, die Sie Ihrer Webseite hinzufügen möchten.
3. Klicken Sie auf **Ihrer Webseite hinzufügen**.
4. Klicken Sie auf **Code anzeigen**. Das System zeigt einen ähnlichen String wie den unten stehenden an. Der Text zwischen den Anführungszeichen („ ") stellt die URL der Minianwendung dar:

```
<script src="http://www.gmodules.com/ig/ifr?  
url=http://www.donalobrien.net/apps/google/currency.xml&up_def_from=USD&up_def_to=EUR&  
synd=open&w=320&h=170&title=Currency+Converter&border=%23ffffff%7C0px%  
2C1px+solid+%2382CAFA%7C0px%2C2px+solid+%23BDEDFE%7C0px%2C3px+solid+%  
23E0FFF&output=js"></script>
```

3.4.2 Importieren von Minianwendungen

Minianwendungen von Drittanbietern können dem one-X Portal for IP Office mithilfe einer XML-Datei hinzugefügt werden. Sie können maximal 50 Minianwendungen auf einmal hochladen. Die Dateigröße darf 2 MB nicht überschreiten.

Die nachfolgenden Parameter müssen für jede Minianwendung angegeben werden:

- URL der Minianwendung - die Quelle der Minianwendung und deren Inhalt
- Minianwendungsname - wird auf der Titelleiste der Minianwendung angezeigt
- Symbolleistensymbole für die Minianwendung. Es wird empfohlen, für alle in gadgets.xml spezifizierten Minianwendungen Symbolleisten-Symbole zur Verfügung zu stellen.
- Texte der Minianwendungs-Symbolleiste (Quickinfo-Text und der Text, der unterhalb des Symbolleisten-Symbols erscheint).

Beispiel einer Minianwendungsdatei im XML-Format:

```
<GadgetsConfigurationImpl>
<gadgetRecords>
<entry>
<key>1</key>
<value>
<categorys>1</categorys>
<categorys>2</categorys>
<created>2012-08-10</created>
<defaultToolbarIcon />
<downToolbarIcon />
<deleted />
<enable>true</enable>
<external>true</external>
<height>300</height>
<id>1</id>
<localizedName><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry
Birds</en_US><en_GB>Angry Birds</en_GB><de>Angry Birds</de><fr>Angry Birds</fr><it>Angry
Birds</it><nl>Angry Birds</nl><es>Angry Birds</es><pt_BR>Angry Birds</pt_BR><ru>Angry
Birds</ru><zh>Angry Birds</zh></names></localizedName>
<name>Angry Birds</name>
<toolbarText><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry
Birds</en_US><en_GB>Angry Birds</en_GB><de>Angry Birds</de><fr>Angry Birds</fr><it>Angry
Birds</it><nl>Angry Birds</nl><es>Angry Birds</es><pt_BR>Angry Birds</pt_BR><ru>Angry
Birds</ru><zh>Angry Birds</zh></names></toolbarText>
<tooltip><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry
Birds</en_US><en_GB>Angry Birds</en_GB><de>Angry Birds</de><fr>Angry Birds</fr><it>Angry
Birds</it><nl>Angry Birds</nl><es>Angry Birds</es><pt_BR>Angry Birds</pt_BR><ru>Angry
Birds</ru><zh>Angry Birds</zh></names></tooltip>
<url>http://www.gmodules.com/ig/ifr?
url=http://www.forumforyou.it/google_gadget_angry_birds.xml&synd=open&w=820&h=680&title
=Angry+Birds&border=%23ffffff%7C3px%2C1px+solid+%23999999&output=js</url>
</value>
</entry>
</gadgetRecords>
</GadgetsConfigurationImpl>
```

Hinweis: Achten Sie in der .xml-Datei auf Folgendes:

1. Im Element <entry></entry> muss jede Minianwendung enthalten sein.
2. Das Element <key></key> muss eindeutig sein und es muss übereinstimmen mit <id></id>. Dieses ist eine spezifische Minianwendungs-ID, die für interne Zwecke verwendet wird.
3. Das Element <value></value> sollte Informationen zur Minianwendung enthalten.
4. Das Element <categorys></categorys> gibt an, zu welcher Kategorie die Minianwendung gehört. Die IDs und Codes für die Kategorien lauten wie folgt:

Code	Kategorie
1	ALLE

2	KOMMUNIKATION
3	TOOLS
4	PRODUKTIVITÄT
5	FINANCE
6	TECHNOLOGIE
7	ZOHO

5. Details anderer Elemente:

Element	Beschreibung
<erstellt>	Das Datum, an dem die Datei erstellt wurde.
<defaultToolBarIcon>	Zur Angabe des standardmäßigen Symbolleisten-Symbols, das das System anzeigt, wenn die Minianwendung minimiert ist. Das System zeigt das Symbol auf der Symbolleiste des Benutzers an.
<downToolBarIcon>	Zur Angabe der Symbolleiste, die das System anzeigt, wenn der Benutzer auf das Minianwendungen-Symbol klickt.
<Aktivieren>	Geben Sie den Wert mit „Wahr“ an, wenn Sie möchten, dass der Benutzer die Minianwendung sehen kann.
<extern>	Setzen Sie bei allen externen Minianwendungen den Wert auf „Wahr“.
<Höhe>	Gibt die Höhe der Minianwendung in Pixeln an.
<ID>	ID der Minianwendung.
<localizedName>	Legt für jedes Gebietsschema den lokalisierten Namen fest.
<Name>	Geben Sie der Minianwendung einen eindeutigen Namen.
<toolbarText>	Der Text, den das System in der Minianwendungen-Symbolleiste anzeigt.
<tooltip>	Der Text, den das System als QuickInfo zur Minianwendung anzeigt.
<URL>	Die URL der Minianwendung. Für weitere Informationen siehe Die URL einer externen Minianwendung holen – Beispiel

Hinweis: Entspricht die Konfigurationsdatei nicht den oben genannten Kriterien, werden entsprechende Fehlermeldungen angezeigt.

So importieren Sie eine Datei einer Minianwendung:

1. Klicken Sie im linken Navigationsfenster auf **Konfiguration der Minianwendungen**.
2. Klicken Sie auf **Externe Minianwendungen importieren**.
3. Klicken Sie auf **Datei auswählen**, um die Konfigurationsdatei zu suchen und auszuwählen.
4. Klicken Sie auf **Hochladen**. Das System lädt die XML-Datei hoch zum one-X Portal for IP Office.
5. Klicken Sie auf **Importieren**, um die Minianwendung eines Drittanbieters der *Liste externer Minianwendungen* hinzuzufügen.



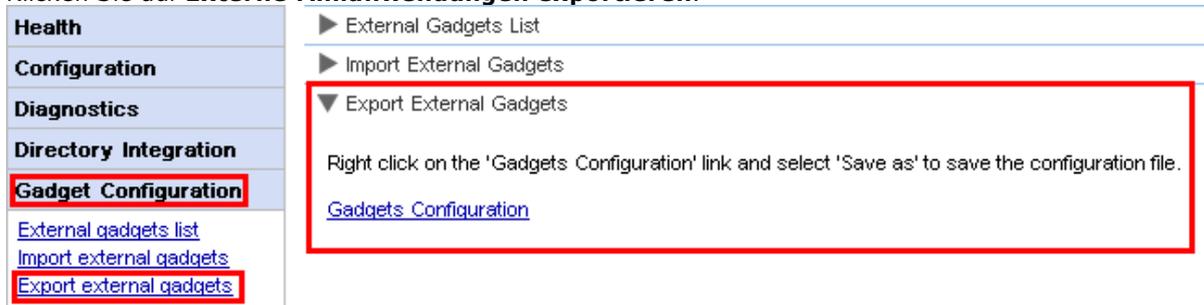
6. Bei der nächsten Anmeldung des Benutzers im one-X Portal for IP Office kann der Benutzer die Minianwendung eines Drittanbieters dem Portal hinzufügen.

3.4.3 Exportieren von Minianwendungen

Die vorhandenen Einstellungen für externe Minianwendungen in one-X Portal for IP Office können als Konfigurationsdatei exportiert werden. Die Konfigurationsdatei ist im XML-Format. Die Konfigurationsdatei enthält Informationen über die Parameter der Minianwendungen. Sie können diese Zusammenstellung von Minianwendungen zum one-X Portal for IP Office eines anderen Benutzers hinzufügen, indem Sie die gespeicherte Konfigurationsdatei [importieren](#)⁶³.

So exportieren Sie eine Minianwendung von Drittanbietern:

1. Klicken Sie im linken Navigationsfenster auf **Konfiguration der Minianwendungen**.
2. Klicken Sie auf **Externe Minianwendungen exportieren**.



3. Klicken Sie mit der rechten Maustaste auf den Link **Konfiguration der Minianwendungen**.
4. Wählen Sie **Speichern unter**, um die Konfigurationsdatei zu speichern.

3.4.4 Hinzufügen einer externen Minianwendung

Um eine einzelne Minianwendung hinzuzufügen, brauchen Sie deren URL. Weiterführende Informationen zum Erhalt der Minianwendungs-URLs finden Sie unter [Auslesen der URL einer externen Minianwendung – Beispiel](#).

Um eine externe Minianwendung hinzuzufügen:

1. Klicken Sie im linken Navigationsfenster auf **Konfiguration der Minianwendungen**.
2. Klicken Sie auf **Liste externer Minianwendungen**.
3. Klicken Sie auf **Hinzufügen**. Das System zeigt das **Minianwendung hinzufügen**-Dialogfeld an.
4. Fügen Sie die Details der Minianwendung (siehe unten) hinzu, und klicken Sie auf **Speichern**. Das System aktualisiert die externe Minianwendung, die Sie zur one-X Portal for IP Office-Datenbank hinzugefügt haben.

Felder für die Minianwendung

Feldname	Beschreibung
Name der Minianwendung	Das System gibt den Namen in der Titelleiste der Minianwendung wieder, den Sie in diesem Feld festlegen. Stellen Sie sicher, dass der Name der Minianwendung das Limit von 50 Zeichen nicht überschreitet.
URL der Minianwendung	Enthält die URL der Minianwendung. Die URL, die Sie angeben, sollte der folgenden Norm für URLs entsprechen http://www.w3.org/Addressing/URL/url-spec.txt . Das System nutzt die von Ihnen bestimmte URL, um die Minianwendung anzuzeigen.
Lokalisierter Name der Minianwendung	Das System gibt den lokalisierten Namen, den Sie in diesem Feld bestimmen, auf der Titelleiste der Minianwendung an. Das System zeigt den lokalisierten Namen nur an, wenn der Benutzer von one-X Portal for IP Office während dem Anmeldevorgang eine Sprache angibt.
Beschriftung des Symbolleistensymbols	Das System zeigt den Text, den Sie in diesem Feld bestimmen, als Beschriftung der Minianwendung in der Symbolleiste an. Wenn Sie den Text nicht bestimmen, zeigt das System den gesamten Namen der Minianwendung an.
Symbolleistensymbol Tool-Hilfetext	Das System zeigt den Tool-Hilfetext an, den Sie in diesem Feld für die Minianwendung festlegen, wenn der Benutzer den Mauszeiger auf dem Minianwendungssymbol in der Symbolleiste hält.
Symbolleistensymbol	Das System gibt in der Symbolleiste das Symbol an, das Sie in diesem Feld festlegen. Vergewissern Sie sich, dass der Bildtyp ausschließlich png, gif oder jpeg ist, die Abmessungen des Bildes 37*37 Pixel betragen und die maximale Größe 10 Kb nicht überschreitet. Wenn Sie kein Symbol bestimmen, zeigt das System das Standardsymbol an.
Symbolleistensymbol bei Mausklick	Das System zeigt das Symbol, das in diesem Feld festgelegt wurde an, wenn Sie das Symbol in der Symbolleiste anklicken. Vergewissern Sie sich, dass der Bildtyp ausschließlich png, gif oder jpeg ist, die Abmessungen des Bildes 37*37 Pixel betragen und die maximale Größe 10 Kb nicht überschreitet.
Aktiviert	Das System aktiviert die Minianwendung für alle Benutzer von one-X Portal for IP Office.
Höhe der Minianwendung	Das System gibt die Höhe der Minianwendung bis zu der Höhe an, die Sie in diesem Feld festlegen. Die Standardhöhe des Minianwendungsfensters ist auf 300 Pixel in diesem Feld eingestellt. Sie können die Höhe des Minianwendungsfensters nur festlegen, wenn Sie eine Minianwendung hinzufügen. Sie können die Höhe der Minianwendung nicht mehr verändern, nachdem Sie eine Minianwendung hinzugefügt haben.

3.4.5 Bearbeitung einer externen Minianwendung

Sie können die Details einer Minianwendung, wie z. B. den Namen, die URL, den Text, der in der Symbolleiste erscheint, den Hilfetext, das Symbol, das in der Symbolleiste angezeigt wird und das Symbol, das bei einem Mausklick erscheint, bearbeiten.

So bearbeiten Sie eine externe Minianwendung:

1. Klicken Sie im linken Navigationsfenster auf **Konfiguration der Minianwendungen**.
2. Klicken Sie auf **Liste externer Minianwendungen**.
3. Klicken Sie auf **Alle abrufen**. Das System zeigt eine Liste aller externen Minianwendungen, die im System verfügbar sind.

4. Klicken Sie auf **Bearbeiten**, um die Details der Minianwendung zu bearbeiten. Das System zeigt ein **Minianwendung bearbeiten**-Dialogfenster an.
5. Siehe [Hinzufügen einer externen Minianwendung](#) für Informationen zu den Feldern der Minianwendungen. Nehmen Sie die von Ihnen gewünschten Änderungen vor, und klicken Sie auf **Speichern**.
6. Klicken Sie auf **Ausgewählte ablegen**. Das System aktualisiert die externen Minianwendungen, die von Ihnen bearbeitet wurden, in der one-X Portal for IP Office -Datenbank.

3.4.6 Aktivierung einer externen Minianwendung

Wenn Sie eine Minianwendung aktivieren, können alle Benutzer von one-X Portal for IP Office diese Minianwendung verwenden.

So aktivieren Sie eine externe Minianwendung:

1. Klicken Sie im linken Navigationsfenster auf **Konfiguration der Minianwendungen**.
2. Klicken Sie auf **Liste externer Minianwendungen**.
3. Klicken Sie auf **Alle abrufen**. Das System zeigt eine Liste aller externen Minianwendungen, die im System verfügbar sind.
4. Aktivieren Sie die Minianwendung, die der Benutzer von one-X Portal for IP Office zum one-X Portal for IP Office-Fenster hinzufügen kann.
5. Klicken Sie auf **Ausgewählte ablegen**. Das System aktualisiert die externen Minianwendungen, die von Ihnen aktiviert wurden, in der one-X Portal for IP Office -Datenbank.

3.4.7 Deaktivierung einer externen Minianwendung

Wenn Sie eine Minianwendung deaktivieren, können Benutzer von one-X Portal for IP Office diese Minianwendung nicht dem one-X Portal for IP Office-Fenster hinzufügen. Wenn Sie eine Minianwendung deaktivieren, die von den Benutzern bereits dem one-X Portal for IP Office-Fenster hinzugefügt wurde, zeigt das System diese nicht an, wenn die Benutzer sich das nächste Mal anmelden.

So deaktivieren Sie eine externe Minianwendung:

1. Klicken Sie im linken Navigationsfenster auf **Konfiguration der Minianwendungen**.
2. Klicken Sie auf **Liste externer Minianwendungen**.
3. Klicken Sie auf **Alle abrufen**. Das System zeigt eine Liste aller externen Minianwendungen, die im System verfügbar sind.
4. Deaktivieren Sie die Minianwendung, von der Sie nicht wollen, dass Benutzer von one-X Portal for IP Office sie dem Fenster one-X Portal for IP Office hinzufügen.
5. Klicken Sie auf **Ausgewählte ablegen**. Das System aktualisiert die von Ihnen deaktivierten Minianwendungen in der one-X Portal for IP Office -Datenbank.

3.4.8 Löschen einer externen Minianwendung

So löschen Sie eine externe Minianwendung:

1. Klicken Sie im linken Navigationsfenster auf **Konfiguration der Minianwendungen**.
2. Klicken Sie auf **Liste externer Minianwendungen**.
3. Klicken Sie auf **Alle abrufen**. Das System zeigt eine Liste aller externen Minianwendungen, die im System verfügbar sind.
4. Wählen Sie die Minianwendung aus, die Sie löschen möchten.
5. Klicken Sie auf **Löschen**.
6. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie diese Minianwendung löschen möchten. Das System aktualisiert die externen Minianwendungen, die Sie in der one-X Portal for IP Office-Datenbank gelöscht haben.

3.5 Benutzer

3.5.1 Hinzufügen/Löschen von Benutzern

Der one-X Portal for IP Office™-Server wird mit den Benutzern synchronisiert, die auf den IP Office-Systemen vorhanden sind. Benutzer werden über die IP Office-Konfiguration hinzugefügt oder entfernt.

Änderungen an Benutzern auf den IP Office-Systemen werden innerhalb von one-X Portal for IP Office und anderen Avaya-Clients, z. B. Mobility, Avaya Communicator u. a., nach zehn Minuten Synchronisierungszeit aktualisiert. Die Benutzer sollten auch nach der Synchronisierung angemeldet sein.

3.5.2 Bearbeiten von Benutzereinstellungen

Sie können die Administrationsmenüs des Portals für die Anzeige und Bearbeitung einer Vielzahl von Einstellungen verwenden.

So bearbeiten Sie Benutzereinstellungen:

1. Wählen Sie **Konfiguration** und anschließend **Benutzer**.
2. Klicken Sie auf **Alle abrufen** und durchsuchen Sie die Benutzer.
3. Klicken Sie auf die Schaltfläche **Bearbeiten** neben dem Benutzer, den Sie bearbeiten möchten. Die Einstellungen der Benutzerkonfiguration werden angezeigt.

User Editor	
ID	13
Name	Extn101
Unique Identifier	B7462000CEEC11DB80
Display Name	Extn101
Password
Password Hash	7B295DC8FA34A5BE93
User Role	User
User Configuration Type Selector	Select
User Configuration Type Specific Editor	
User Role Configuration	<input checked="" type="radio"/> User <input type="radio"/> Manager
Created	2013-05-14 01:29:06.160
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

4. Wählen Sie mithilfe der **Benutzertypenauswahl** die Benutzereinstellungen aus, die Sie anzeigen/bearbeiten möchten. Bearbeiten Sie die Einstellungen gegebenenfalls.
 - **Popup-Fenster**
Zeigt den Link für das Herunterladen der Installationssoftware des Desktop-Clients an, die für one-X Portal Call Assistant und Outlook Plug-in verwendet wird.
 - **Parkbereich**
Ermöglicht die Konfiguration der Parkbereichnummern, die den Parktasten des Benutzers zugeordnet sind.
 - **Brückennummer**
Ermöglicht die Konfiguration der Brückennummer des Benutzers für dessen persönliche Einwahlkonferenzen.
 - **Telecommuter-Modus**
Ermöglicht dem Benutzer die Auswahl des Telecommute-Modus und die Konfiguration seiner Festnetz-/Mobilnummer, die bei Aktivierung des Modus verwendet wird.
 - **IM-/Anwesenheitskonfiguration**
Ermöglicht die Konfiguration der IM-/Anwesenheitseinstellungen des Benutzers. Beachten Sie, dass der Benutzer dennoch die Benachrichtigungen während der eigenen one-X Portal for IP Office-Sitzung aktivieren muss.
5. Klicken Sie auf **Speichern**.
6. Um die bearbeiteten Einstellungen in die one-X Portal for IP Office-Datenbank zu übernehmen, aktivieren Sie das Kontrollkästchen neben dem Benutzer und klicken auf **Ausgewählte ablegen**.

So bearbeiten Sie eine große Anzahl an Benutzereinstellungen zur gleichen Zeit:

1. Wählen Sie **Konfiguration** und anschließend **Benutzer**.
2. Klicken Sie auf **Alle abrufen** und durchsuchen Sie die Benutzer.
3. Aktivieren Sie das Kontrollkästchen neben jedem Benutzer, den Sie bearbeiten möchten.
4. Klicken Sie auf **Massenbearbeitung**.



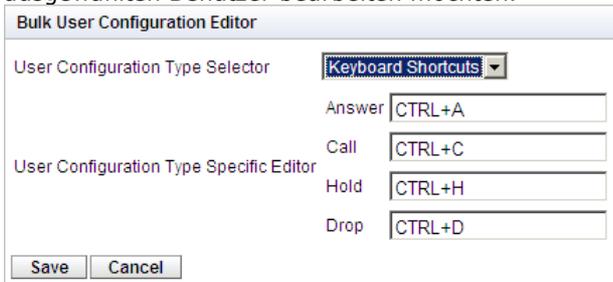
Bulk User Configuration Editor

User Configuration Type Selector: Select

User Configuration Type Specific Editor: Some User Configuration

Save Cancel

5. Wählen Sie mithilfe der **Benutzertypenauswahl** die Benutzerkonfigurationseinstellungen aus, die Sie für alle ausgewählten Benutzer bearbeiten möchten.



Bulk User Configuration Editor

User Configuration Type Selector: Keyboard Shortcuts

User Configuration Type Specific Editor:

Answer: CTRL+A

Call: CTRL+C

Hold: CTRL+H

Drop: CTRL+D

Save Cancel

6. Wenn Sie mit der Bearbeitung fertig sind, klicken Sie auf **Speichern**.
7. Aktivieren Sie das Kontrollkästchen neben jedem bearbeiteten Benutzer und klicken Sie auf **Ausgewählte ablegen**, um die Änderungen an die one-X Portal for IP Office-Datenbank zurückzusenden.

3.6 Verzeichnisse

3.6.1 Hinzufügen einer externen LDAP-Verzeichnisquelle

Während der Installation wird standardmäßig ein LDAP-Anbieter erstellt, aber nicht für die Verbindung mit einem LDAP-Server konfiguriert (es sei denn „Erweiterte Installation“ wird ausgewählt und die LDAP-Anbiereinstellungen werden geändert). Mit dem unten stehenden Verfahren werden die LDAP-Anbiereinstellungen geändert, um die LDAP-Funktion zuzulassen.

Die LDAP-Funktion kann über die Option [Verzeichnisintegration | LDAP-Verzeichnissuche](#)^[44] in den Administrationsmenüs getestet werden.

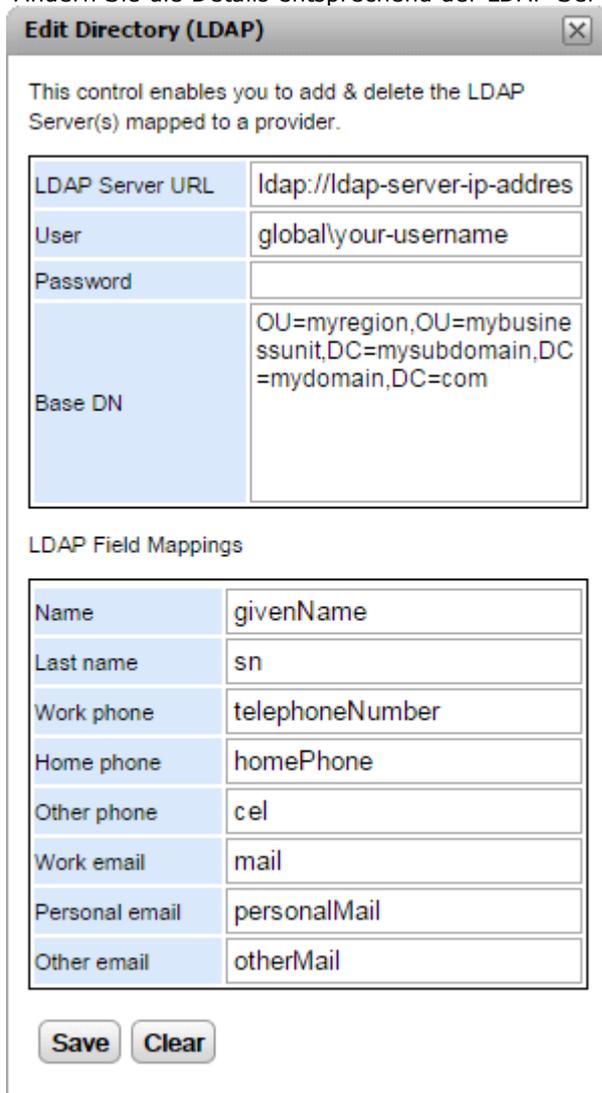
Im Gegensatz zur LDAP-Unterstützung in IP Office importiert der one-X Portal for IP Office-Server keine Datensätze aus der LDAP-Quelle, um diese dann als Verzeichnis zu verwenden. Stattdessen verwendet der one-X Portal for IP Office-Server die LDAP-Quelleneinstellungen, um die Datensätze der LDAP-Quelle online zu durchsuchen, sobald ein one-X Portal for IP Office-Benutzer Zeichen in die Registerkarte „Externes Verzeichnis“ der Minianwendung „Verzeichnis“ eingibt. Daher muss der one-X Portal for IP Office-Server seine LDAP-Datensätze nicht regelmäßig aktualisieren.

- **Achtung**

Für diesen Prozess müssen Sie den [Portaldienst neu starten](#)^[54], damit die Änderungen übernommen werden. Das Portal ist während des Neustarts möglicherweise bis zu 15 Minuten lang nicht für Benutzer verfügbar.

So fügen Sie ein externes LDAP-Verzeichnis hinzu:

1. Melden Sie sich als Administrator an.
2. Wählen Sie **Konfiguration** und anschließend **Anbieter**.
3. Wählen Sie aus der Dropdown-Liste **Anbietername** die Option **Verzeichnis (LDAP)** aus.
4. Klicken Sie auf das Symbol  neben dem LDAP-Anbieter.
5. Ändern Sie die Details entsprechend der LDAP-Serverquelle, die Sie verwenden möchten.



LDAP Server URL	ldap://ldap-server-ip-address
User	globallyour-username
Password	
Base DN	OU=myregion,OU=mybusinessunit,DC=mysubdomain,DC=mydomain,DC=com

LDAP Field Mappings

Name	givenName
Last name	sn
Work phone	telephoneNumber
Home phone	homePhone
Other phone	cel
Work email	mail
Personal email	personalMail
Other email	otherMail

Save Clear

- **URL des LDAP-Servers**

Die URL der LDAP-Verzeichnisquelle, z. B. *ldap://ldap.beispiel.com*.

- **Benutzer/Kennwort**

Benutzername und Kennwort für den Zugriff auf den LDAP-Server.

- **Basis-DN**

Auch **Such-Basis** genannt. Definiert, welche Datensätze in der LDAP-Quelle für Suchen verwendet werden sollten. Der LDAP-Serveradministrator gibt eine geeignete Zeichenfolge ein, z. B. *ou=benutzer,dc=global,dc=beispiel,ddc=com*.

- **LDAP-Feldzuweisungen**

Die Feldnamen (links) entsprechen den Feldern, die im one-X Portal for IP Office-Verzeichnis angezeigt werden. Geben Sie für jedes Feld in den Datensätzen der LDAP-Quelle den Namen des übereinstimmenden Felds ein.

6. Klicken Sie auf **Speichern**.

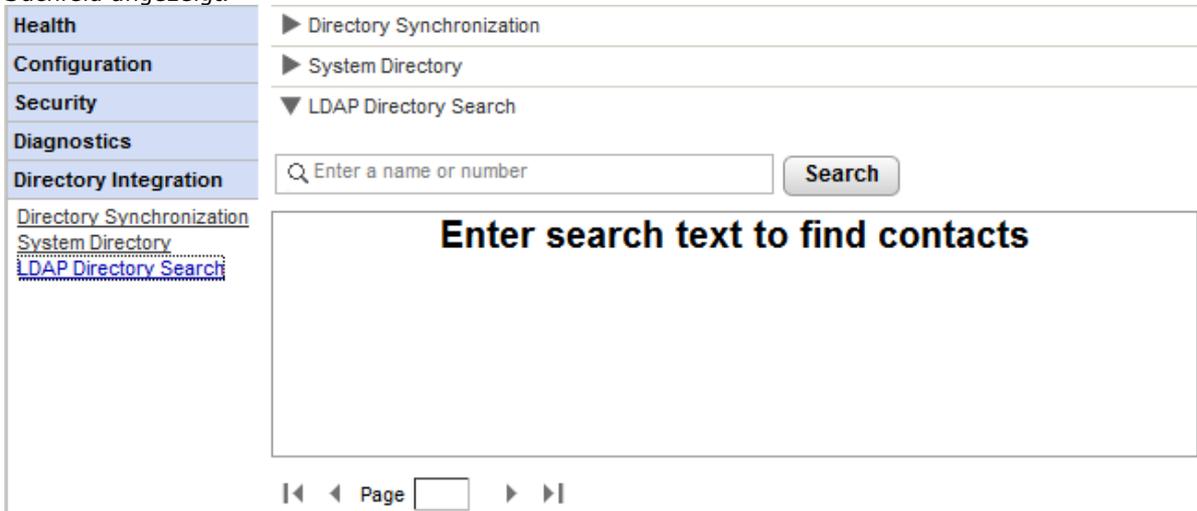
7. [Starten Sie den Avaya one-X Portal-Dienst neu](#)⁵⁴.

3.6.2 Überprüfen des externen LDAP-Verzeichnisses

Wenn Sie eine externe LDAP-Verzeichnisquelle konfiguriert haben, können Sie den Zugriff von one-X Portal for IP Office auf diese Quelle über die Administrationsmenüs testen.

So überprüfen Sie das LDAP-Verzeichnis:

1. Wählen Sie **Verzeichnisintegration**.
2. Wählen Sie **LDAP-Verzeichnissuche**.
3. Geben Sie einen Namen oder eine Nummer ein, für den bzw. für die es einen Eintrag im externen Verzeichnis gibt, und klicken Sie auf **Suchen**. Ist die Suche erfolgreich, werden die Ergebnisse unter dem Suchfeld angezeigt.



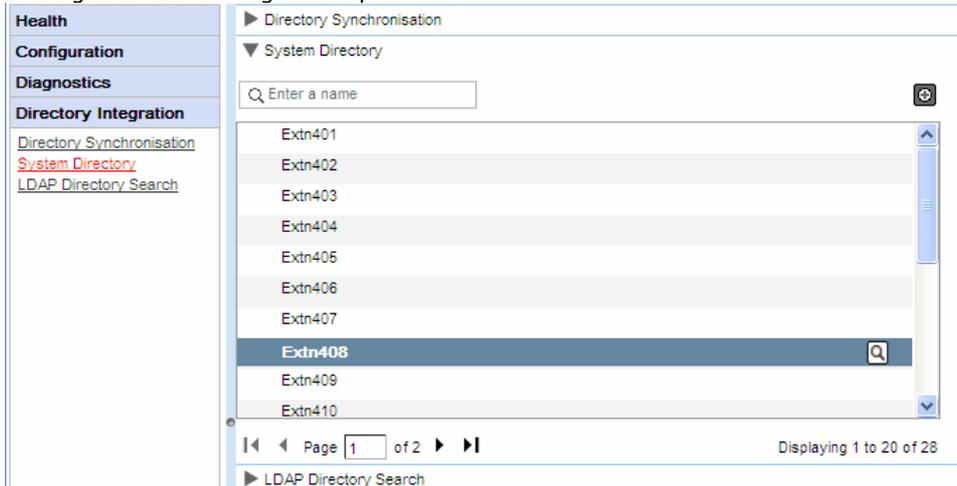
3.6.3 Überprüfen und Aktualisieren des Systemverzeichnisses

Das Systemverzeichnis, das one-X Portal for IP Office-Benutzern angezeigt wird, ist eine Kombination aus Benutzer-, Gruppen- und Verzeichniseinträgen aus allen IP Office-Systemen, für deren Betrieb one-X Portal for IP Office konfiguriert wurde.

Standardmäßig aktualisiert one-X Portal for IP Office die Einträge im Systemverzeichnis etwa alle 300 Sekunden. Über die one-X Portal for IP Office-Administrationsmenüs können Sie das Systemverzeichnis anzeigen und eine Aktualisierung erzwingen.

So überprüfen Sie das Systemverzeichnis:

1. Wählen Sie **Verzeichnisintegration**.
2. Wählen Sie **Systemverzeichnis**. Das aktuelle Systemverzeichnis wird angezeigt. Überprüfen Sie, ob die Einträge den Erwartungen entsprechen.



3. Wenn Sie eine Aktualisierung für erforderlich halten, wählen Sie **Verzeichnissynchronisierung**.



4. Klicken Sie auf **Neusynchronisierung aller IP Office-Verzeichnisse erzwingen**.

3.7 Aktualisieren/Herunterstufen

Das in diesem Abschnitt beschriebene Verfahren gilt nur für Windows-basierte Server.

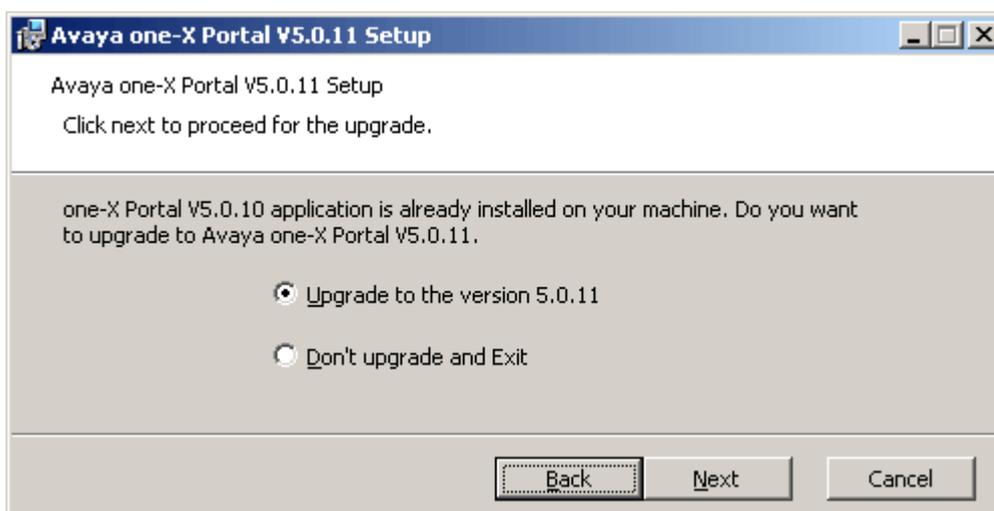
3.7.1 Aktualisieren von one-X Portal for IP Office

Lesen Sie vor dem Upgrade von one-X Portal for IP Office auf Windows-Basis unbedingt das technische Merkblatt von Avaya IP Office zu der one-X Portal for IP Office-Softwareversion, die Sie installieren möchten bzw. in der es enthalten war. Das technische Merkblatt enthält Einzelheiten zu besonderen Anforderungen und zusätzlichen Schritten, die in dieser Dokumentation nicht aufgeführt werden.

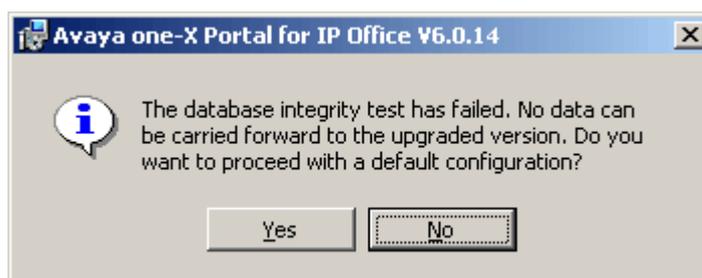
Wenn one-X Portal for IP Office bereits auf einem Server-PC installiert ist und die Installationsdatei für eine neuere Version ausgeführt wird, wird die vorhandene Version erkannt und Sie werden gefragt, ob Sie sie aktualisieren möchten. Wenn Sie sich für ein Upgrade entscheiden, erfolgt dieser Vorgang ähnlich wie bei einer normalen Softwareinstallation, wobei einige Installationsoptionen allerdings grau unterlegt sind, da die vorhandenen Einstellungen nicht geändert werden können.

- **Achtung**

Für diesen Prozess müssen Sie den [Portaldienst neu starten](#)⁵⁴⁾, damit die Änderungen übernommen werden. Das Portal ist während des Neustarts möglicherweise bis zu 15 Minuten lang nicht für Benutzer verfügbar.



- Wenn ein Upgrade der bestehenden one-X Portal for IP Office-Datenbank nicht möglich ist, wird ein Warnhinweis angezeigt. Wenn Sie „Ja“ auswählen, wird die bestehende Datenbank durch eine Standard-Datenbank ersetzt. Wenn Sie „Nein“ auswählen, müssen Sie das Installationsprogramm erneut ausführen, um ein [Downgrade](#)⁷⁵⁾ auf eine mit der Datenbank kompatible Version von one-X Portal for IP Office durchzuführen.



Während des Upgrade-Vorgangs wird eine Sicherungsdatei erstellt (backup.sql). Dies ist keine vollständige Sicherung des one-X Portal for IP Office-Systems und sollte nicht zur Wiederherstellung von Einstellungen verwendet werden.

3.7.2 Downgraden von one-X Portal for IP Office

Wenn die Windows-basierte one-X Portal for IP Office-Anwendungssoftware mit einem [Upgrade](#)^[74] aktualisiert wurde, kann sie mit einem Downgrade auch wieder auf die ursprünglich installierte Version heruntergestuft werden.

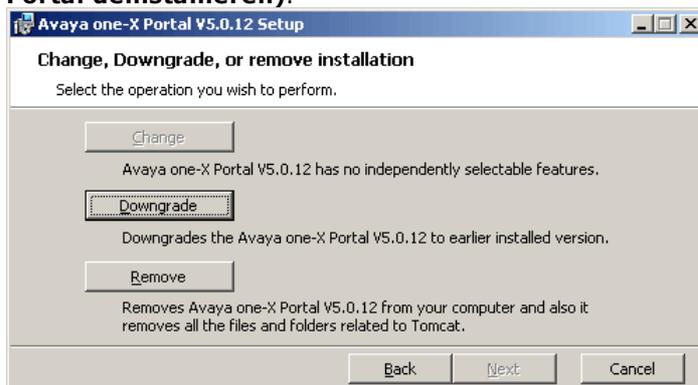
- **Hinweis:** Die Installation von one-X Portal for IP Office sowie das letzte Upgrade auf one-X Portal for IP Office werden in der Windows-Systemsteuerung in der Liste **Software** aufgeführt. Beachten Sie jedoch, dass bei der Deinstallation einer dieser Versionen die gesamte Anwendung entfernt wird.

Lesen Sie vor dem Downgrade von one-X Portal for IP Office unbedingt das technische Merkblatt von Avaya IP Office zu den one-X Portal for IP Office-Softwareversionen. Das technische Merkblatt enthält Einzelheiten zu besonderen Anforderungen und zusätzlichen Schritten, die in dieser Dokumentation nicht aufgeführt werden.

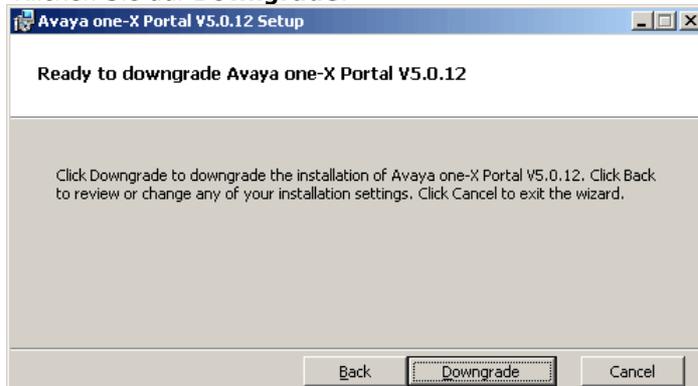
- **Achtung**
Für diesen Prozess müssen Sie den [Portaldienst neu starten](#)^[54], damit die Änderungen übernommen werden. Das Portal ist während des Neustarts möglicherweise bis zu 15 Minuten lang nicht für Benutzer verfügbar.

So stufen Sie one-X Portal for IP Office herunter:

1. Wählen Sie **Start | Alle Programme | IP Office | one-X Portal | Uninstall one-X Portal (one-X Portal deinstallieren)**.



2. Klicken Sie auf **Downgrade**.



3. Nachdem das Downgrade durchgeführt wurde, muss Avaya one-X Portal [manuell neu gestartet](#)^[54] werden.

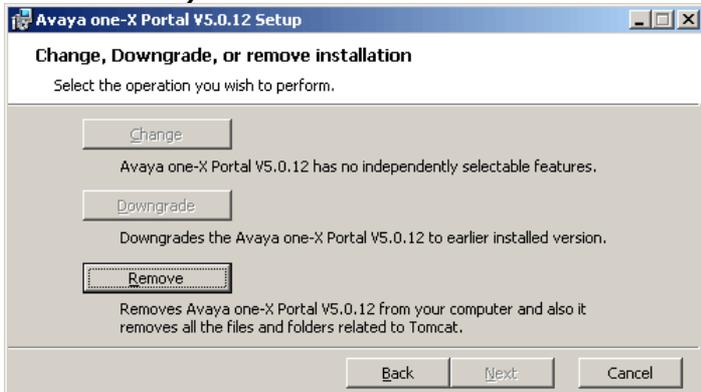
3.7.3 Entfernen von one-X Portal for IP Office

Zum Entfernen der one-X Portal for IP Office-Anwendung von einem Windows-Server stehen zwei Methoden zur Verfügung.

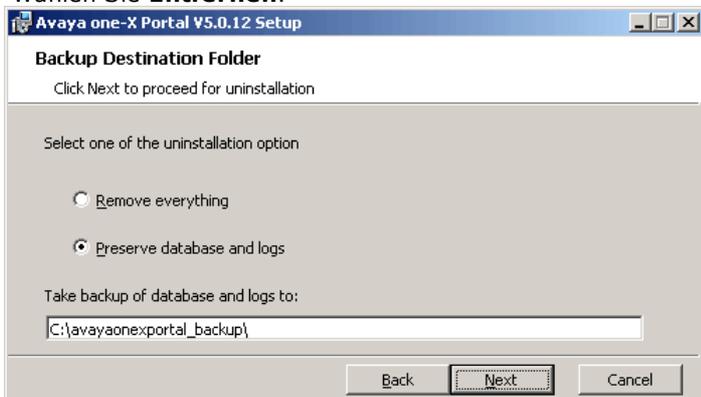
So deinstallieren Sie one-X Portal for IP Office:

Bei dieser Methode kann ausgewählt werden, ob Sicherungen der Datenbank- und Protokolldateien beibehalten werden sollen.

1. Wählen Sie **Start | Alle Programme | IP Office | one-X Portal | Uninstall one-X Portal (one-X Portal deinstallieren)**.



2. Wählen Sie **Entfernen**.



3. Klicken Sie auf **Next** (Weiter).



4. Klicken Sie auf **Entfernen**, um mit dem Entfernen der Dateien zu beginnen.

So entfernen Sie one-X Portal for IP Office über die Systemsteuerung von Windows:

Die Option **Software** in der Windows-Systemsteuerung kann ebenfalls zum Entfernen von one-X Portal for IP Office verwendet werden. Bei dieser Methode werden automatisch Sicherungskopien der Datenbank und der Protokolldateien im Ordner **c:\avayaonexpportal_backup** erstellt.

1. Öffnen Sie die Windows-Systemsteuerung.
2. Wählen Sie **Software**.
3. Wählen Sie **one-X Portal** und klicken Sie dann auf **Entfernen**.

- Wenn one-X Portal for IP Office irgendwann aktualisiert wurde, ist sowohl für die ursprüngliche one-X Portal for IP Office-Installation als auch für das letzte Upgrade ein Programmeintrag vorhanden. Wählen Sie die Upgrade-Installation, und klicken Sie dann auf „Entfernen“. Dadurch werden sowohl die Upgrade- als auch die ursprüngliche Installation entfernt.

3.8 Sofortnachrichtenversand/Anwesenheit

Der one-X Portal for IP Office-Server enthält eine XMPP-Serverkomponente, die standardmäßig aktiviert ist. Mithilfe dieses Servers können Benutzer einander Sofortnachrichten senden und ihre IM-Anwesenheit teilen.

Die Archivierung von Sofortnachrichten ist ebenfalls standardmäßig aktiviert, sodass Sie die vorherigen Nachrichten eines Benutzers durchsuchen können.

- [IM Server-Konfiguration](#)⁷⁹
- [Starten des IM-Servers](#)⁸¹
- [Durchsuchen des IM-Archivs](#)⁸²
- [Festlegen der Dauer der IM-Archivierung](#)⁷⁹
- [Exchange-Kalenderintegration](#)⁸³

So deaktivieren Sie die IM-Archivierung:

1. [Aktivieren der Administratorkonsole des XMPP-Servers](#)⁸⁴
2. [Deaktivieren der IM-Archivierungseinstellungen anhand des XMPP-Servers](#)⁸⁵
3. [Deaktivieren der Administratorkonsole des XMPP-Servers](#)⁸⁵

So aktivieren Sie die IM-Archivierung:

1. [Aktivieren der Administratorkonsole des XMPP-Servers](#)⁸⁴
2. [Aktivieren der IM-Archivierungseinstellungen anhand des XMPP-Servers](#)⁸⁴
3. [Deaktivieren der Administratorkonsole des XMPP-Servers](#)⁸⁵

Änderungen am XMPP-Standardvorgang

Vor IP Office Version 9.1 verfügte jedes IP Office-System über eine XMPP-Standardgruppe, in der jeder IP Office-Benutzer als Mitglied enthalten war. Daher konnte jeder Benutzer automatisch die IM-Anwesenheit anderer Benutzer sehen.

Für IP Office Version 9.1 ist dies nicht länger zutreffend. Der Austausch von IM/Anwesenheit zwischen Benutzern erfordert die manuelle Konfiguration von XMPP-Gruppen mit diesen Benutzern in der IP Office-Systemkonfiguration (weitere Informationen finden Sie in der Hilfe oder Dokumentation zu IP Office Manager).

3.8.1 IM Server-Konfiguration

Das Portal enthält eine Komponente, die als Sofortnachrichten-(IM-)/Anwesenheitsserver fungiert. Der IM-/Anwesenheitsserver kann separat konfiguriert werden. Siehe [Sofortnachrichtenversand/Anwesenheit](#)^[78].

Configuration	
Providers	► Users
Users	► CSV
CSV	► Branding
Branding	▼ IM/Presence Server
IM/Presence	Server to Server Federation <input checked="" type="checkbox"/>
Exchange service	Disconnect on Idle <input type="checkbox"/>
SMTP Configuration	Anyone can connect <input checked="" type="checkbox"/>
Conference Dial-in	Port number <input type="text" value="5269"/>
Host Domain Name	Idle timeout <input type="text" value="3600"/>
Conference Clean Up	MyBuddy user name <input type="text" value="mybuddy"/>
Central CTI Link	XMPP Domain Name <input type="text" value="server1.primary"/>
	Days to archive IMs <input type="text" value="60"/>
	<input type="button" value="Save"/> <input type="button" value="Clear"/> <input type="button" value="Refresh"/>

So konfigurieren Sie den IM-/Anwesenheitsserver:

1. Klicken Sie auf **Konfiguration** und wählen Sie **IM-/Anwesenheitsserver**.
2. Auswahl der erforderlichen Server-Einstellungen:

- **Server-Verbund**

Bei aktivierter Option kann der Anwesenheitsserver des Portals Anwesenheitsinformationen mit anderen Anwesenheitsservern austauschen.

- **Bei Leerlauf trennen**

Bei aktivierter Option werden Verbindungen zwischen Servern getrennt, wenn sie sich für den unter **Inaktivitäts-Zeitlimit** angegebenen Zeitraum im Leerlauf befinden.

- **Jede Verbindung möglich**

Jedem erlauben, sich mit IM-/Anwesenheitsdiensten zu verbinden.

- **Portnummer**

Diese ist auf **5269** festgelegt.

- **Inaktivitäts-Zeitlimit**

Dies ist das Zeitlimit in Sekunden, das bei aktivierter Option **Bei Leerlauf trennen** verwendet wird.

- **MyBuddy-Benutzername**

Dieses Feld ist auf **mybuddy** festgelegt. Der Wert ist gegebenenfalls erforderlich, wenn Anwesenheitsdetails in andere IM-/Anwesenheitsdienste integriert werden.

- **XMPP-Domänenname**

Hier wird der DNS-Domänenname festgelegt, der für IM-/Anwesenheitsfunktionen verwendet wird:

- Der XMPP-Domänenname sollte ein Domänenname sein, den der DNS auflösen kann. Sie können den XMPP-Domännennamen jederzeit festlegen. Der Domänenname muss über das Internet erreichbar sein, wenn Sie Anwesenheit außerhalb Ihres LAN verwenden wollen, z. B. mit one-X Mobile.
- Avaya empfiehlt, eine geteilte DNS zu verwenden, sodass der Servername außerhalb Ihres LAN in die öffentliche IP-Adresse der NAT oder der Firewall aufgelöst wird, während er innerhalb Ihres Netzwerks in die private IP-Adresse des LAN-Servers aufgelöst wird.
- Wenn Sie keinen auflösbaren DNS-Domännennamen einstellen können, können Sie die IP-Adresse des one-X Portal for IP Office-Servers ausschließlich für interne IM/Anwesenheit verwenden. In diesem Fall kann das one-X Portal for IP Office keine Verbindung zu Remote-Servern herstellen.
- Bei Linux-basierten Servern (IP Office Server Edition, IP Office Application Server und Unified Communications Module) müssen Sie die Websteuerungsmenüs des Servers verwenden, um deren Netzwerkeinstellungen zu konfigurieren, sodass der E-Mail-Link der automatischen Konfiguration den vollqualifizierten Domännennamen statt der IP-Adresse des Servers verwendet. Gehen Sie in Web Control zu EInstellungen > System > Hostname, um die Netzwerkeinstellungen zu ändern. Wenn Sie den Domännennamen auf eine andere Weise ändern, funktionieren die E-Mail-Links möglicherweise nicht richtig.
- **Tage für die Archivierung von IMs**
In diesem Feld wird festgelegt, wie lange der Server Nachrichten im IM-Archiv speichern soll, bevor sie gelöscht werden. Die Standardeinstellung lautet 182 Tage (6 Monate). Bei Bedarf können Sie mit der XMPP-Verwaltungskonsole die [IM-Archivierung deaktivieren](#)^[85]. Zum Ändern dieser Einstellung muss der IM-/Anwesenheitsserver verfügbar sein (siehe [Status des IM-/Anwesenheitsservers](#)^[15]).

3. Klicken Sie auf **Speichern**.

3.8.2 IM-Benutzerkonfiguration

Damit für zwei IP Office-Benutzer der Anwesenheitsstatus des jeweils anderen Benutzers angezeigt wird und sie Sofortnachrichten austauschen können, müssen sie Mitglieder derselben XMPP-Gruppe in der IP Office-Systemkonfiguration sein. Jeder Benutzer kann einer oder mehreren XMPP-Gruppen angehören.

Wenn ein neuer IP Office-Benutzer in einer einzelnen Aktion (Benutzer hinzufügen, neuen Benutzer zu XMPP-Gruppe hinzufügen, Konfiguration speichern) hinzugefügt wird, wird der Benutzer nicht in der Portalansicht der XMPP-Gruppe angezeigt. Zum Beheben des Problems kann die XMPP-Gruppenkonfiguration geändert oder der Portaldienst neu gestartet werden.

Um dies zu vermeiden, sollten Sie zwischen jeder Aktion die Konfiguration speichern (Benutzer hinzufügen, Konfiguration speichern, neuen Benutzer zu XMPP-Gruppe hinzufügen, Konfiguration speichern).

3.8.3 Starten des IM-Servers

Sie können den Status des IM-/Anwesenheitsservers über das Menü [Status des IM-/Anwesenheitsservers](#)¹⁵ überprüfen. Ist der IM-/Anwesenheitsserver nicht in betrieb, können Sie den Service anhand der nachfolgenden Vorgehensweise starten.

So starten Sie den IM- /Anwesenheitsserver:

1. Wählen Sie **Status**.
2. Wählen Sie **Status des IM-/Anwesenheitsservers**. Das System zeigt den Status des IM-/Anwesenheitsservers an.

The screenshot shows the 'Health' section of the IP Office interface. On the left is a navigation menu with links: Dashboard, Component Status, IM/Presence server status, Key Recent Events, Active Sessions, and Environment. The main content area shows 'Component Status' expanded to 'IM/Presence server status'. Below this is a table with the following data:

Component Name	Status	Reported At
IM/Presence Server	Stopped	29 May 2015 09:16

Below the table are two buttons: 'Refresh' and 'Start'.

3. Klicken Sie auf **Start**.
 - Ist die Datenbank beschädigt, zeigt das System „Die Datenbank des IM-/Anwesenheitsservers ist beschädigt und muss wiederhergestellt werden. Möchten Sie sie wiederherstellen?“ an.
 - Um die Datenbank wiederherzustellen und den IM-/Anwesenheitsserver zu starten, klicken Sie auf **Ja**. Die Datenbank wird aus dem Sicherungsordner wiederhergestellt. Das System führt alle acht Stunden eine automatische Sicherung der Datenbank durch. Sie können den IM/Anwesenheitsserver nicht starten, ohne die beschädigte Datenbank wiederherzustellen.
 - Wenn Sie auf **Nein** klicken. Das System zeigt die folgende Nachricht an: „Der IM-/Anwesenheitsserver kann nicht mit einer beschädigten Datenbank gestartet werden. Die IM-/Anwesenheitsfunktionen stehen nicht zur Verfügung.“.

3.8.4 Durchsuchen des IM-Archivs

Sie können nach IM-Gesprächen zwischen Benutzern und zwischen System und Benutzer suchen. Alle Felder im Suchfeld sind optional. Die Anzahl der Tage, für die der Server IM-Nachrichten archiviert, wird mit der Einstellung [Tage für die Archivierung von IMs](#) festgelegt.

<ul style="list-style-type: none"> Health Configuration Security Diagnostics Directory Integration Gadgets Configuration Web Conferences IM Archive Search Archive 	<div style="display: flex; justify-content: space-between;"> <div> Participants <input type="text" value="Extn210"/> <input type="text"/> </div> <div> Start <input type="text"/> End <input type="text"/> </div> <div> Keywords <input type="text"/> </div> </div> <div style="margin-top: 10px;"> <input type="button" value="Search"/> <input type="button" value="Clear"/> <input type="button" value="Export"/> </div>																											
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Participants</th> <th style="width: 30%;">Start</th> <th style="width: 10%;">Count</th> </tr> </thead> <tbody> <tr> <td>Extn210 mybuddy</td> <td>Aug 15, 2014 12:00 PM</td> <td>4</td> </tr> <tr style="background-color: #e0e0e0;"> <td>Extn210 Extn211</td> <td>Aug 15, 2014 8:05 AM</td> <td>2</td> </tr> <tr> <td>Extn210 everyone</td> <td>Aug 14, 2014 2:13 PM</td> <td>1</td> </tr> </tbody> </table> <div style="margin-top: 10px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2">Participants:</td> <td>Extn210, Extn211</td> </tr> <tr> <td colspan="2">Date:</td> <td>Aug 15, 2014 8:05 AM</td> </tr> <tr> <td colspan="3">Keyword:</td> </tr> <tr> <td style="width: 10%;">7:59</td> <td style="width: 10%;">Extn210 :</td> <td>Morning. How are the updates going?</td> </tr> <tr> <td>8:5</td> <td>Extn211 :</td> <td>Okay now we have the system running. Tell you how far we got at the end of today.</td> </tr> </table> </div>	Participants	Start	Count	Extn210 mybuddy	Aug 15, 2014 12:00 PM	4	Extn210 Extn211	Aug 15, 2014 8:05 AM	2	Extn210 everyone	Aug 14, 2014 2:13 PM	1	Participants:		Extn210, Extn211	Date:		Aug 15, 2014 8:05 AM	Keyword:			7:59	Extn210 :	Morning. How are the updates going?	8:5	Extn211 :	Okay now we have the system running. Tell you how far we got at the end of today.
Participants	Start	Count																										
Extn210 mybuddy	Aug 15, 2014 12:00 PM	4																										
Extn210 Extn211	Aug 15, 2014 8:05 AM	2																										
Extn210 everyone	Aug 14, 2014 2:13 PM	1																										
Participants:		Extn210, Extn211																										
Date:		Aug 15, 2014 8:05 AM																										
Keyword:																												
7:59	Extn210 :	Morning. How are the updates going?																										
8:5	Extn211 :	Okay now we have the system running. Tell you how far we got at the end of today.																										

So durchsuchen Sie das IM-Archiv:

1. Wählen Sie im linken Teilfenster das **IM-Archiv** aus.
2. Klicken Sie auf **Archiv durchsuchen**.
3. Geben Sie die Suchkriterien ein, und klicken Sie auf „Suchen“.

Feld	Beschreibung
Teilnehmer	Geben Sie den Namen des Teilnehmers der IM-Unterhaltung ein.
Stichwörter	Geben Sie Stichwörter aus der IM-Unterhaltung ein.
Starten	Wählen Sie das Datum aus, ab dem Unterhaltungen aufgelistet werden sollen. Wenn Sie kein Datum auswählen, beginnt die Anzeige bei der frühesten vom System gespeicherten Unterhaltungen.
Ende	Wählen Sie das Datum aus, bis zu dem Unterhaltungen aufgelistet werden sollen. Wenn Sie kein Datum auswählen, werden alle Unterhaltungen bis zur letzten Unterhaltung angezeigt.

4. Klicken Sie auf die Unterhaltung, die Sie öffnen möchten. Die Unterhaltung wird angezeigt.

3.8.5 Exchange-Kalenderintegration

one-X Portal for IP Office kann auf dem Exchange-Server konfiguriert werden, um das Auslesen des Kalenders und der Anwesenheitsdaten von Benutzern zu ermöglichen.

Health	▶ Providers
Configuration	▶ Users
Providers	▶ CSV
Users	▶ Branding
CSV	▶ IM/Presence Server
Branding	▼ IM/Presence Exchange Service
IM/Presence	
Exchange service	
SMTP Configuration	
Conference Dial-in	
Host Domain Name	
Conference Clean Up	
Central CTI Link	

Exchange service account name	AvayaAdmin
Exchange service account password	●●●●●●●●
Exchange service Host	
Exchange Port number	6669
Exchange service proxy host	
Exchange proxy port	
Test Email Address (e.g. user@example.com)	

Note:

- Test email address is required for MS Exchange 2013 for validation purpose only.
- It is not possible to execute the batch file by placing it on the desktop. Please make sure that the batch file is not stored on the desktop.
- Save the file on any local drives, for example C drive. To download the file, right click on the link below and select "Save Link As...".

[Download Powershell script](#)

So konfigurieren Sie Exchange-Dienste:

1. Klicken Sie **Konfiguration** im linken Navigationsbalken.
2. Klicken Sie auf **Exchange-Dienst**.
 - a. Geben Sie **AvayaAdmin** in das Feld **Exchange-Dienst-Kontoname** ein. Vergewissern Sie sich, dass es sich bei diesem Namen um den gleichen Namen wie bei dem **AvayaAdmin**-Konto handelt, das Sie auf dem Exchange-Server erstellt haben.
 - b. Geben Sie das Kennwort ein, das für den **AvayaAdmin** als **Exchange-Dienst-Kontokennwort** festgelegt wurde.
 - c. Geben Sie als **Exchange-Dienst-Host** die IP-Adresse des Exchange-Dienst-Hosts ein.
 - d. Geben Sie in **Exchange-Portnummer** die Portnummer des Exchange-Dienstes ein.
 - e. Geben Sie den Domännennamen des Proxyserver, der für die Verbindung zum Exchange-Server genutzt wird, in **Exchange-Dienst-Proxyhost** ein.
 - f. Geben Sie die Portnummer des Proxyserver für den Exchange-Dienst in **Exchange-Proxyport** ein.
 - g. Legen Sie eine **Test-E-Mail-Adresse** mithilfe einer gültigen E-Mail-Adresse fest.
3. Klicken Sie auf **Exchange-Dienst-Konfiguration überprüfen**, um zu sehen, ob die eingegebenen Exchange-Daten korrekt sind.
4. Klicken Sie auf **Speichern**.

3.8.6 Aktivieren der XMPP-Administratorkonsole

Aus Sicherheitsgründen ist die XMPP-Administratorkonsole nicht standardmäßig aktiviert. Wenn sie für die Wartung oder Fehlersuche aktiviert ist, müssen Sie anschließend [die Administratorkonsole wieder deaktivieren](#)⁸⁵.

So aktivieren Sie die Administratorkonsole: (Linux)

1. Melden Sie sich als root-User an.
2. Geben Sie Folgendes ein: `cd /opt/Avaya/oneXportal/openfire/bin`
3. Geben Sie an der Eingabeaufforderung Folgendes ein: `sh AdminConsoleManager.sh enable`
4. Geben Sie zum Neustarten des Dienstes Folgendes ein: `service onexportal restart`

So aktivieren Sie die Administratorkonsole: (Windows)

1. Gehen Sie zur Eingabeaufforderung.
2. Navigieren Sie zu dem Verzeichnis, in dem one-X Portal for IP Office installiert ist, z. B. „`cd C:\Program Files\Avaya\oneXportal`“.
 - **Hinweis:** Der Installationspfad wird sich bei einer 32-bit- und einer 64-bit-Installation unterscheiden.
3. Geben Sie Folgendes ein: `cd \openfire\bin`
4. Geben Sie an der Eingabeaufforderung Folgendes ein: `AdminConsoleManager.bat enable`
5. Starten Sie Avaya one-X Portal neu.

3.8.7 Aktivieren der IM-Archivierung

So aktivieren Sie die IM-Archivierungseinstellungen im XMPP-Server:

1. [Aktivieren der XMPP-Administratorkonsole](#)⁸⁴.
2. Öffnen Sie die Administratorkonsole in einem Browser, indem Sie `http://<Server-IP-Adresse>:9094` eingeben.
3. Melden Sie sich mit dem Benutzernamen und Kennwort **admin** an.
4. Klicken Sie auf die Registerkarte **Server**.
5. Klicken Sie auf die Registerkarte **Archivierung**.
6. Wählen Sie im linken Teilfenster **Archivierungseinstellungen** aus.
7. Aktivieren Sie die folgenden Kontrollkästchen:
 - **Archivierung des Gesprächsstatus**
 - **Archivieren der Einzelgespräche**
 - **Archivieren der Gruppengespräche**
8. Klicken Sie auf die Schaltfläche **Einstellungen aktualisieren**. Das System speichert die Einstellungen und zeigt die nachfolgende Nachricht an: *Die Archiveinstellungen wurden gespeichert.*
9. [Deaktivieren der XMPP-Administratorkonsole](#)⁸⁵.

3.8.8 Deaktivieren der IM-Archivierung

So deaktivieren Sie die IM-Archivierung:

1. [Aktivieren der XMPP-Administratorkonsole](#)⁸⁴.
2. Öffnen Sie die Administratorkonsole in einem Browser, indem Sie `http://<Server-IP-Adresse>:9094` eingeben.
3. Melden Sie sich mit dem Benutzernamen und Kennwort **admin** an.
4. Klicken Sie auf die Registerkarte **Server**.
5. Klicken Sie auf die Registerkarte **Archivierung**.
6. Wählen Sie im linken Teilfenster **Archivierungseinstellungen** aus.
7. Deaktivieren Sie die folgenden Kontrollkästchen:
 - **Archivierung des Gesprächsstatus**
 - **Archivieren der Einzelgespräche**
 - **Archivieren der Gruppengespräche**
8. Klicken Sie auf die Schaltfläche **Einstellungen aktualisieren**. Das System speichert die Einstellungen und zeigt die nachfolgende Nachricht an: *Die Archiveinstellungen wurden gespeichert.*
9. [Deaktivieren der Administratorkonsole](#)⁸⁵.

3.8.9 Deaktivieren der XMPP-Administratorkonsole

Aus Sicherheitsgründen ist die XMPP-Administratorkonsole nicht standardmäßig aktiviert. Wenn die Administratorkonsole für die Wartung oder Fehlersuche aktiviert ist, müssen Sie sie anschließend wieder deaktivieren.

So deaktivieren Sie die Administratorkonsole: (Linux)

1. Melden Sie sich als root-User an.
2. Geben Sie Folgendes ein: `cd /opt/Avaya/oneXportal/openfire/bin`
3. Geben Sie an der Eingabeaufforderung Folgendes ein: `sh AdminConsoleManager.sh disable`
4. Geben Sie zum Neustarten des Dienstes Folgendes ein: `service onexportal restart`

So deaktivieren Sie die Administratorkonsole: (Windows)

1. Gehen Sie zur Eingabeaufforderung.
2. Navigieren Sie zu dem Verzeichnis, in dem one-X Portal for IP Office installiert ist, z. B. „`cd C:\Program Files\Avaya\oneXportal`“.
 - **Hinweis:** Der Installationspfad wird sich bei einer 32-bit- und einer 64-bit-Installation unterscheiden.
3. Geben Sie Folgendes ein: `cd \openfire\bin`
4. Geben Sie an der Eingabeaufforderung Folgendes ein: `AdminConsoleManager.bat disable`
5. Starten Sie Avaya one-X Portal neu.

3.9 Konferenzen

Das Portal kann eine Komponente enthalten, die Support für Konferenzfunktionen bietet. Bei diesen handelt es sich um Konferenzplanung und Web Collaboration-Sitzungen, die parallel zu den Konferenzen stattfinden.

3.9.1 Anzeigen der Konferenzen

Anhand dieses Menüs können Sie die Details zu allen auf dem Server gehosteten Web Collaboration-Konferenzen anzeigen. Es listet die Mitglieder der Konferenz auf, wann sie zuletzt teilgenommen haben und die Art ihrer Teilnahme (Moderator, Audiokonferenz-Mitglied, Webkonferenz-Mitglied). Dieses Menü wird auf dem Unified Communications Module-Server nicht unterstützt.

Health	Host	User Name	Extension	Join Time	Leave Time			
Configuration	▲ Peter Power							
Security		 Peter Power	239	Jul 23, 2014 4:19 PM				
Diagnostics		 Gary Guest	5555555	Jul 23, 2014 4:22 PM				
Directory Integration	▲ Lync01(230)							
Gadgets Configuration		 Lync01	230	Jul 23, 2014 4:20 PM				
Web Conferences		 Getrude Guest	666666	Jul 23, 2014 4:23 PM				
Monitor Conferences								

So zeigen Sie aktuelle Konferenzen an:

1. Wählen Sie **Webkonferenzen** und dann **Konferenzen überwachen**.
2. Die aktuellen Webkonferenzen werden aufgelistet
3. Klicken Sie auf den **Host**, um die Konferenz zu erweitern und die Informationen der Teilnehmer anzuzeigen.

3.9.2 Anzeigen geplanter Konferenzen

Dieses Menü zeigt den Kalender für geplante Konferenzen an, ähnlich dem Kalender, den Einzelbenutzer von one-X Portal for IP Office sehen und verwenden. Der Unterschied besteht darin, dass die geplanten Konferenzen für alle Benutzer angezeigt werden. Sie können mit diesem Menü eine geplante Konferenz löschen und die Details zukünftiger Konferenzen ändern.

Health	▶ Logging Configuration
Configuration	▶ Logging Viewer
Security	▶ Network Routes (Not for IP Offices)
Diagnostics	▶ IP Office Connections
Logging Configuration	▶ Database Integrity
Logging Viewer	▶ User data validation
Network Routes	▶ Call/Conference Scheduling
IP Office Connections	▼ View Conferences
Database Integrity	
User data validation	
Call/Conference Sched	
View Conferences	

New
 Historic
 All
 Non-Recurring
 Recurring

Host	Subject	Bridge Details	Date	Start Time	End Time	
212	Daily Meeting	Bridge:212	September 22, 2015	8:30 PM	9:00 PM	
212	Team Meeting	Bridge:212	September 22, 2015	6:00 PM	6:30 PM	

⏪
◀ Page 1 of 1 ▶
⏩

3.9.3 Löschen einer geplanten Konferenz

Sie können eine zukünftige geplante Konferenz löschen. Wenn es sich dabei um eine wiederholte Konferenz handelt, werden alle Termine der Konferenz gelöscht.

So löschen Sie geplante Konferenzen:

1. Klicken Sie auf **Diagnosen** und wählen Sie **Anruf-/Konferenzplanung**.
2. Geben Sie die Host-Nebenstelle und ein Thema ein. Wenn Sie das Thema leer lassen, werden alle vom Host geplanten Konferenzen gelöscht.
3. Klicken Sie auf **Löschen**.

3.9.4 Nachricht über Konferenzbenachrichtigungen

Wenn der Benutzer eine Konferenz plant, sendet der Server den eingeladenen Teilnehmern über E-Mail und den Sofortnachrichtenversand eine Konferenzbenachrichtigung. Diese Benachrichtigung beinhaltet die Informationen zur Konferenz, die vom Benutzer eingestellt wurden (Brückenummer, Teilnehmercode). Außerdem kann sie den festgelegten Text enthalten, der über das Menü **Konferenzeinwahl** eingestellt wurde.

So stellen Sie den festgelegten Text der Konferenzbenachrichtigung ein:

1. Wählen Sie **Konfiguration** und dann **Konferenzeinwahl**.
2. Geben Sie den festgelegten Text ein, der in allen Konferenzbenachrichtigungen angezeigt werden sollte.
3. Klicken Sie auf **Speichern**.

3.9.5 E-Mails der Konferenz

Die Konferenzeinladungen an Teilnehmer können sowohl über E-Mail als auch über den Sofortnachrichtenversand erfolgen. Für Benachrichtigungen über E-Mail müssen die E-Mail-Einstellungen der Konferenz wie folgt konfiguriert werden. Die E-Mail-Adresse jedes einzelnen Teilnehmers wird in der Telefonsystem-Konfiguration eingestellt.

Health	▶ Providers
Configuration	▶ Users
Providers	▶ CSV
Users	▶ Branding
CSV	▶ IM/Presence Server
Branding	▶ IM/Presence Exchange Service
IM/Presence	▶ Conference Dial-in Information
Exchange service	▼ SMTP Configuration
SMTP Configuration	Following SMTP configuration will be used to send emails for conference scheduling feature
Conference Dial-in	Server Address
Host Domain Name	Port number
Conference Clean Up	Email From Address
Central CTI Link	Use STARTTLS
	Server Requires Authentication
	User Name
	Password
	<input type="button" value="Save"/> <input type="button" value="Clear"/> <input type="button" value="Refresh"/>
	Note: • *Default SMTP Port is 25

So stellen Sie den festgelegten Text der Konferenzbenachrichtigung ein:

- Wählen Sie **Konfiguration** und dann **SMTP-Konfiguration**.
- Legen Sie die Informationen der SMTP-E-Mail fest, die der Server verwenden soll:
 - **Serveradresse**
Die IP-Adresse des SMTP-Servers des Kunden.
 - **Portnummer**
Der SMTP-Abfrageport auf dem Server. Standardmäßig lautet er 25.
 - **E-Mail-Adresse des Absenders**
Dies ist die Adresse, die vom Server verwendet wird. Einige E-Mail-Server leiten nur Nachrichten von anerkannten Adressen oder Adressen in derselben Domäne weiter.
 - **STARTTLS verwenden**
Wählen Sie dieses Feld zur Aktivierung der TLS-/SSL-Verschlüsselung aus. Die Verschlüsselung ermöglicht die Voicemail-in-E-Mail-Integration bei Anbietern von gehosteten E-Mails, die SMTP nur auf Kommunikationswegen erlauben, die mehr Sicherheit bieten.
 - **Server erfordert Authentifizierung**
Wenn der Server ein Benutzerkonto benötigt, um E-Mails empfangen und versenden zu können, geben Sie die Einzelheiten eines Kontos ein, das auf diesem Server für die Verwendung durch IP Office konfiguriert wurde.
 - **Benutzername**
Der zu verwendende Kontoname, wenn „Server erfordert Authentifizierung“ ausgewählt ist.
 - **Kennwort**
Das zu verwendende Kontokennwort, wenn „Server erfordert Authentifizierung“ ausgewählt ist.
- Klicken Sie auf **Speichern**.

3.9.6 Festlegen der Web Collaboration-URL

Im Menü **Konfiguration | Host-Domänenname** wird der Domänenname festgelegt, der für den Zugriff auf die Portalienste und zwischen Portalservern verwendet wird. Die Anzahl der erforderlichen Domännennamen hängt vom Typ des Portalservers ab.

Beachten Sie, dass nach dem Ändern der Domännennamen der Portaldienst neu gestartet werden muss, damit die Änderungen übernommen werden.

The screenshot shows the configuration page for 'Host Domain Name'. On the left is a navigation menu with categories: Health, Configuration, Security, Diagnostics, Directory Integration, Gadgets Configuration, and IM Archive. Under 'Configuration', several links are listed, including 'Host Domain Name'. The main content area shows a tree view of configuration options, with 'Host Domain Name' expanded. Below this, a table contains the following entries:

Primary Host Domain Name	primary.example.com
Secondary Host Domain Name	secondary.example.com
Web Collaboration Domain Name	webconf.example.com

Below the table, a 'Note' section contains the following information:

Note:

- Web Collaboration Domain Name will be used to generate Conference Web Collaboration URL.
- **Changes to Domain Name configuration require one-X Portal server restart.**

At the bottom of the configuration area are three buttons: 'Save', 'Clear', and 'Refresh'.

3.10 Remote-Protokollierung

Der one-X Portal for IP Office-Server kann so konfiguriert werden, dass Protokollierungsanwendungen eine Verbindung zu Port 4560 herstellen können, um eine Protokollausgabe zu erfassen. Die Ausgabe erfolgt im Log4j-Format. Die Administratorschnittstelle des one-X Portal for IP Office-Servers enthält Links zur Installation von Apache Chainsaw.

Für diesen Vorgang wird vorausgesetzt, dass der PC, über den er erfolgt, über eine Internet-Verbindung verfügt. Ist dies nicht der Fall, kann Apache Chainsaw gemäß den Anweisungen auf der Apache Chainsaw-Website (<http://logging.apache.org/chainsaw>) heruntergeladen und installiert werden.

1. Wählen Sie **Diagnose** und dann **Protokollierung konfigurieren**.

The screenshot shows the 'Logging Configuration' section of the Apache Chainsaw web interface. On the left is a navigation menu with 'Diagnostics' selected. The main content area is titled 'Logging Configuration' and includes the following sections:

- Master Logging Level:** A dropdown menu set to 'ALL'. Text below: 'Set the threshold above which logging events are sent to logging targets. Choose ALL for 'log everything', choose OFF to 'disable logging'.'
- Logging Targets(Rolling Log Files):** Text: 'Rolling log files grow to a max. 10 MB, then a new one is started. The oldest rolling log is removed when the max. of 5 is reached. Rolling log files reflect the master logging level.' Below is a table:

Enabled	Name	Level	File Path
<input checked="" type="checkbox"/>	Overall	ALL	../logs/1XOverallRollingFile.log
<input checked="" type="checkbox"/>	Presentation Layer	ALL	../logs/1XPresentationLayerRollingFile.log
<input checked="" type="checkbox"/>	Mid-Layer	ALL	../logs/1XMidLayerRollingFile.log
<input checked="" type="checkbox"/>	Telephony (CSTA)	ALL	../logs/1XCSTAServiceRollingFile.log
<input checked="" type="checkbox"/>	Directory (IP-Office)	ALL	../logs/1XIPODirServiceRollingFile.log
<input checked="" type="checkbox"/>	Directory (LDAP)	ALL	../logs/1XLDAPDirServiceRollingFile.log

- Logging Targets(Server and Network):** A checkbox for 'Socket Receiver(required for remote log viewing)' is checked and labeled 'Enabled'.

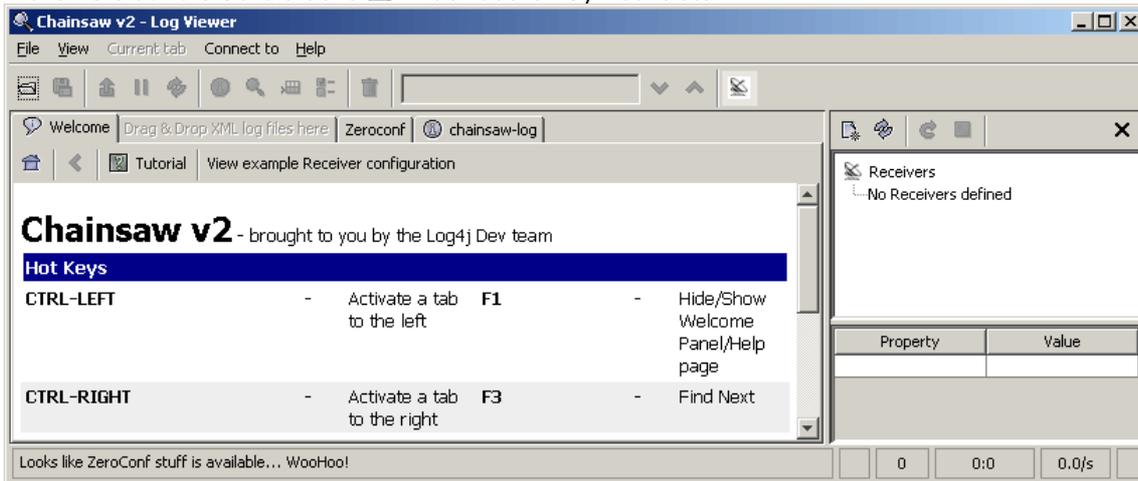
2. Wählen Sie **Protokollierung der Ziele**, und überprüfen Sie, ob **Empfängerkanal** aktiviert ist.
3. Wählen Sie **Protokollanzeige**.

The screenshot shows the 'Logging Viewer' section of the Apache Chainsaw web interface. The left navigation menu has 'Diagnostics' selected. The main content area is titled 'Logging Viewer' and includes:

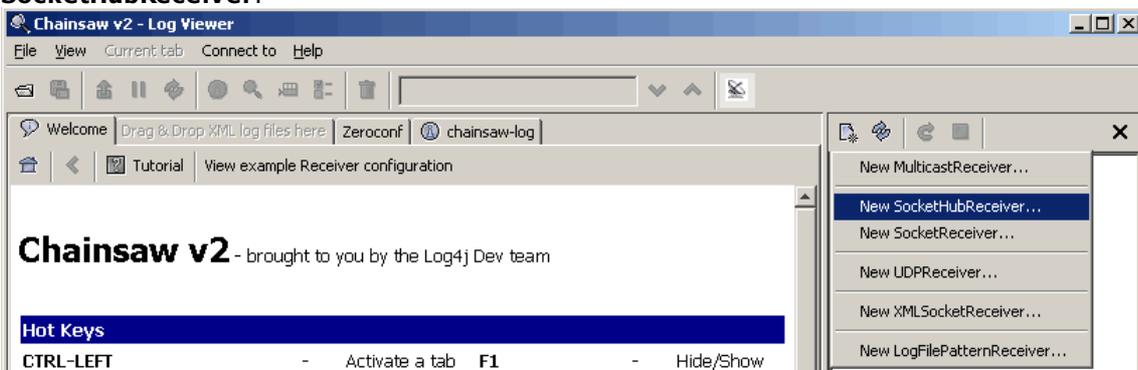
- A description: 'Remotely viewing logs.' and links for 'More information about Apache Chainsaw.' and 'Start Installation of Apache Chainsaw by Java Web Start'.
- A list of expandable sections: 'Network Routes (Not for IP Offices)', 'IP Office Connections', 'Database Integrity', and 'User Data Validation'.

4. Klicken Sie auf **Installation von Apache Chainsaw mit Java Web Start starten**.
5. Download und Installation von Chainsaw erfolgen weitgehend automatisch. Chainsaw wird gestartet. Wenn die Meldung **Warning: You have no Receivers defined...** angezeigt wird, wählen Sie **I'm fine thanks, don't worry** und **Don't show me this again** und klicken auf **OK**.

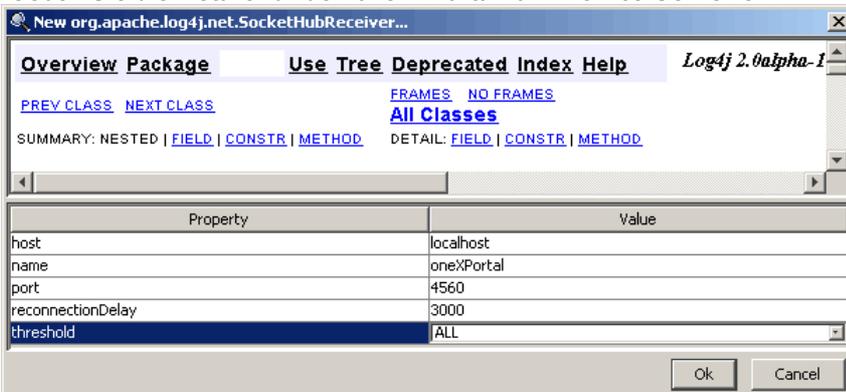
6. Das Teilfenster **Empfänger** sollte auf der rechten Seite angezeigt werden. Sollte dies nicht der Fall sein, klicken Sie auf die Schaltfläche  in der oberen Symbolleiste.



7. Klicken Sie im Bereich „Receivers“ auf das Symbol „New Receiver“  und wählen Sie **New SocketHubReceiver**.

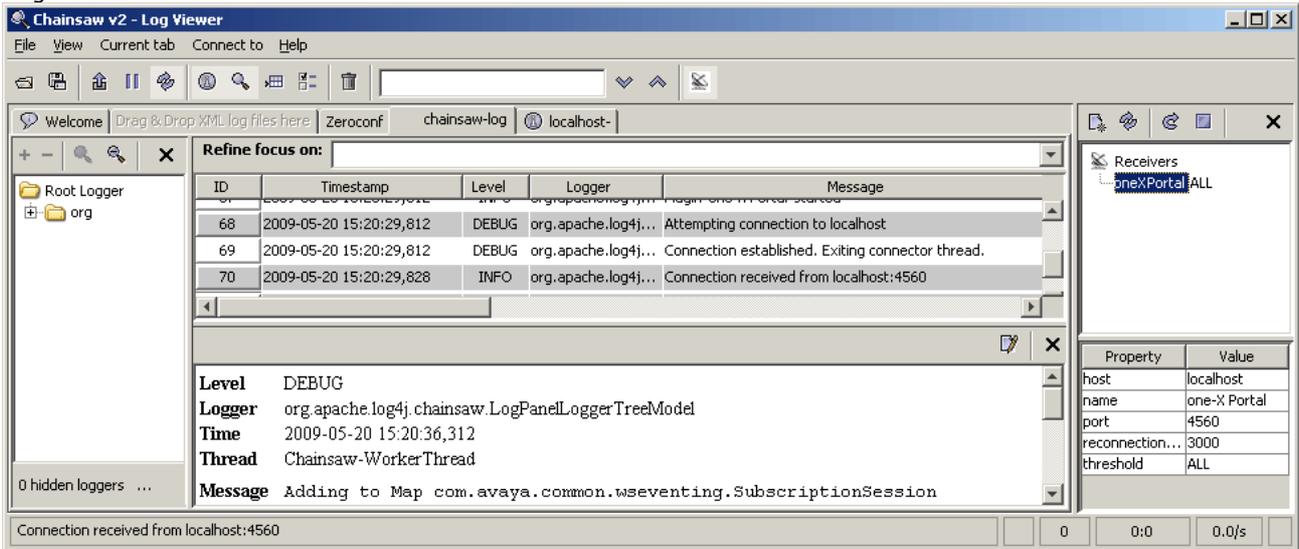


8. Geben Sie die Details für den one-X Portal for IP Office-Server ein.

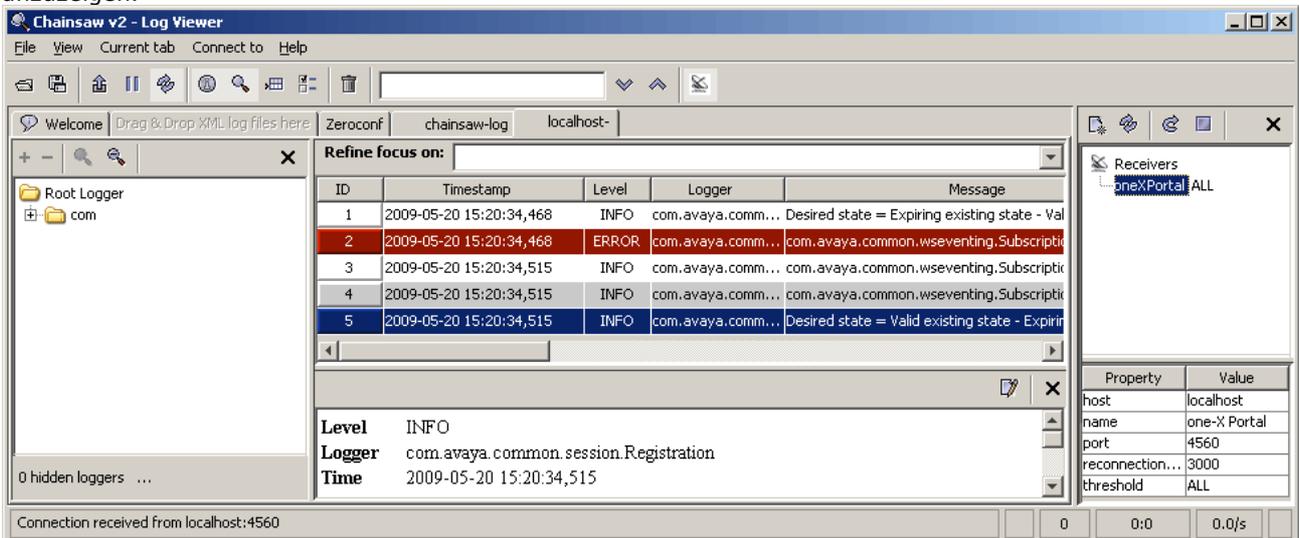


host	Dieses Feld legt die Adresse des one-X Portal for IP Office-Servers fest. In dem oben stehenden Beispiel wird Chainsaw auf dem one-X Portal for IP Office-Server-PC ausgeführt.
name	Dieses Feld dient nur zu Anzeigezwecken. Geben Sie einen Namen für den Empfängereintrag in Chainsaw ein.
port	Setzen Sie dieses Feld auf 4560. Dies ist der Port, an den one-X Portal for IP Office Protokoll Datensätze zur Erfassung durch Protokollierungsanwendungen ausgibt.
reconnectionDelay	Dieses Feld legt fest, wie lang (in Millisekunden) der Empfänger warten soll, wenn er den Verdacht hat, dass die Verbindung verloren gegangen ist, bevor er einen neuen Verbindungsversuch unternimmt.
threshold	Dieses Feld legt fest, welche Protokollmeldungen empfangen werden sollen, kann aber auch auf „Alle“ oder „Aus“ gesetzt werden.

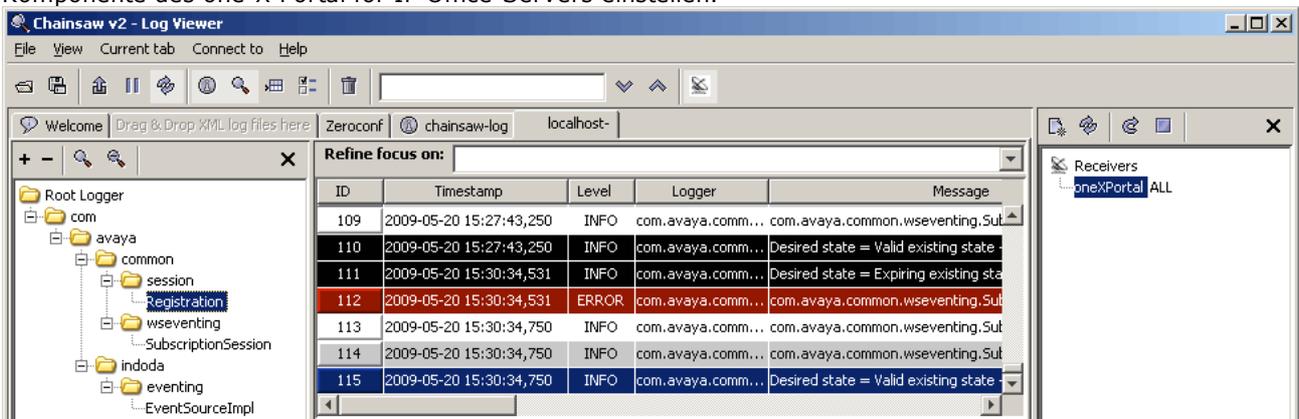
- Wenn Sie die Felder ausgefüllt haben, klicken Sie auf OK. Nach einigen Sekunden sollte der Empfänger starten und eine Verbindung zum one-X Portal for IP Office-Server herstellen. Der Vorgang wird in Form von Protokollereignissen auf der Chainsaw-Protokollregisterkarte angezeigt und erscheint nach Beendigung als neue Registerkarte.



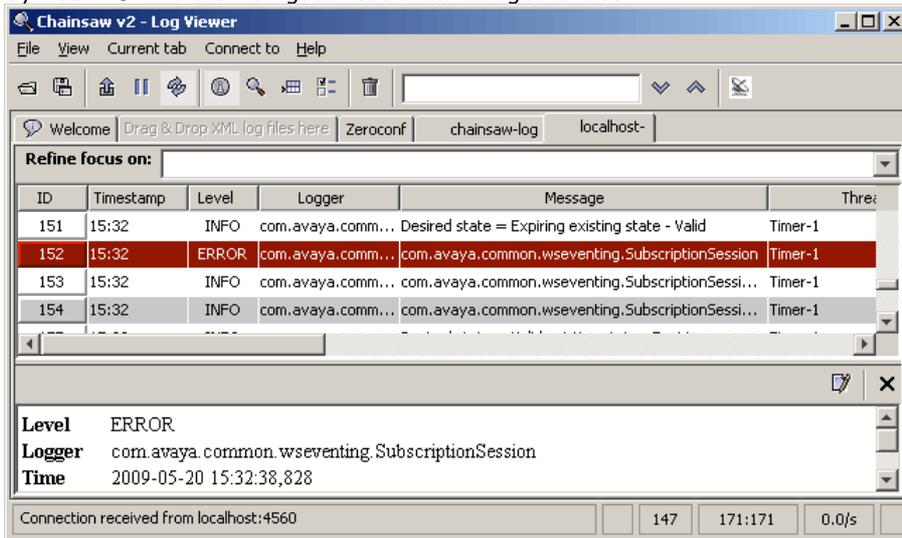
- Klicken Sie auf die neue Empfängerregisterkarte, um die one-X Portal for IP Office-Protokoll Datensätze anzuzeigen.



- Mithilfe der Navigationsstruktur auf der linken Seite können Sie die Protokollanzeige auf eine bestimmte Komponente des one-X Portal for IP Office-Servers einstellen.



12. Klicken Sie auf das Empfängersymbol , um den Empfängerbereich auszublenden. Durch Klicken auf das Symbol  wird die Navigationsstruktur ausgeblendet.



3.11 Fehlerbehebung

Nichtübereinstimmende Versionen

Symptome	<ul style="list-style-type: none"> • Die Integritätsprüfung der Datenbank⁷⁶ schlägt fehl. • Beim Starten von one-X Portal for IP Office wird auf der Anmeldeseite die vorherige Version angezeigt, die sich von der Version unterscheidet, die im Windows-Menü (Start Programme IP Office Avaya one-X Portal for IP Office VX.XXdeinstallieren) angezeigt wird.
Ursache	Normalerweise hält das Installationsprogramm von one-X Portal for IP Office alle Tomcat-Webserver, die mit einer früheren Version von one-X Portal for IP Office verknüpft sind, automatisch an. Manchmal kommt es jedoch vor, dass es den Tomcat-Server nicht anhalten kann, aber dennoch meldet, dass der Installationsvorgang erfolgreich abgeschlossen wurde. Dies führt dazu, dass auf unterschiedlichen Komponenten unterschiedliche Versionen angegeben werden.
Lösung	<ol style="list-style-type: none"> 1. Entfernen Sie one-X Portal for IP Office⁷⁶. 2. Löschen Sie den one-X Portal for IP Office-Anwendungsordner manuell (standardmäßig C:\Programme (x86)\Avaya\onexportal). Sie müssen einen Neustart des Servers durchführen, wenn der Ordner als gesperrt aufgeführt wird. 3. Installieren Sie die neue Version von one-X Portal for IP Office.

one-X Portal for IP Office startet nicht

Symptome	<ul style="list-style-type: none"> • one-X Portal for IP Office lässt sich nicht starten. • Prorun-Fehler erscheint in den Tomcat-Server-Protokolldateien. • Andere Java-Anwendungen lassen sich auf dem Server nicht ausführen (zum Beispiel die IP Office System Status Application).
Lösung	<ol style="list-style-type: none"> 1. Prüfen Sie auf einen Port-Konflikt. Falls ein solcher existiert, entfernen Sie die Anwendung oder installieren Sie one-X Portal for IP Office und nutzen Sie einen anderen Port. 2. Entfernen Sie Java über die Option Software in der Windows-Systemsteuerung. 3. Entfernen Sie one-X Portal for IP Office⁷⁶. 4. Installieren Sie one-X Portal for IP Office.

3.12 Hinzufügen weiterer Administratoren

- Standardmäßig verwenden Linux-basierte one-X Portal for IP Office-Server die **externe Authentifizierung**. Dies bedeutet, dass die Berechtigungen für die Portaladministration Sicherheitsbenutzern zugewiesen werden, die in der Sicherheitskonfiguration des IP Office-Diensts konfiguriert sind, der auf demselben Server ausgeführt wird. Standardmäßig ist dies der Benutzer **Administrator**, allerdings können auch zusätzliche Dienstbenutzer als Portaladministratoren konfiguriert werden.
- Wenn die externe Authentifizierung deaktiviert ist, verwendet das Portal sein eigenes lokales Administratorkonto auf die gleiche Weise wie für einen Windows-basierten Server (siehe unten).

Das folgende Verfahren veranschaulicht das Konfigurieren von Berechtigungen zur Portaladministration für zusätzliche Sicherheitsdienstbenutzer. Jeder Benutzer des IP Office Service ist Mitglied von einer oder mehreren Berechtigungsgruppen. Durch die Einstellungen der Berechtigungsgruppen wird festgelegt, wozu der Dienstbenutzer Berechtigungen hat, einschließlich des Zugriffslevels auf den one-X Portal for IP Office-Server.

Anzeigen und Anpassen der Einstellungen der Berechtigungsgruppen:

1. Wählen Sie in IP Office Manager **Datei | Erweitert | Sicherheitseinstellungen**.
2. Wählen Sie das IP Office-System, und klicken Sie auf **OK**.
3. Geben Sie den Namen und das Kennwort für den Zugriff auf die Sicherheitseinstellungen des IP Office-Systems ein.
4. Wählen Sie  **Berechtigungsgruppen**.
5. Wählen Sie die Registerkarte **Extern**. In dieser Registerkarte sind die Einstellungen zum Zugriffslevel auf das Portal, das den Mitgliedern einer Berechtigungsgruppe gewährt wird, eingeschlossen.
 - **One-X Portal-Administrator**
Zugriff auf die Administratormenüs des Portals.
 - **One-X Portal-Superbenutzer**
Zugriff auf die AFA-Menüs des Portals.
6. Wählen Sie eine Berechtigungsgruppe in der Liste aus, um die Zugriffsberechtigungsebene der Gruppe anzuzeigen.
7. Sollten Sie Änderungen vornehmen, klicken Sie auf **OK**.
8. Klicken Sie auf , um Ihre Änderungen zu speichern.

So ändern Sie die Zugehörigkeit eines Dienstbenutzers zu einer Berechtigungsgruppe:

1. Wählen Sie in IP Office Manager **Datei | Erweitert | Sicherheitseinstellungen**.
2. Wählen Sie das IP Office-System, und klicken Sie auf **OK**.
3. Geben Sie den Namen und das Kennwort für den Zugriff auf die Sicherheitseinstellungen des IP Office-Systems ein.
4. Wählen Sie  **Dienstbenutzer**.
5. Wählen Sie den Dienstbenutzer aus. Die Details zeigen die Berechtigungsgruppe an, bei welcher der Benutzer Mitglied ist.

Kapitel 4.

AFA-Menüs

4. AFA-Menüs

one-X Portal for IP Office unterstützt eine Reihe von Menüs zum Sichern und Wiederherstellen von one-X Portal for IP Office-Konfigurationseinstellungen. Diese bieten die Möglichkeit, beim Sichern und Wiederherstellen den one-X Portal for IP Office-Server, einen FTP-Server oder den eigenen Browser-PC als Ziel für die Sicherungsdateien zu verwenden.

Außerdem sollen die Menüs Sicherungen und Wiederherstellungen zwischen alten und neuen Installationen von one-X Portal for IP Office auf einem neuen Server ermöglichen. Dies wird jedoch nicht für Sicherungen und Wiederherstellungen zwischen verschiedenen Versionen von one-X Portal for IP Office unterstützt (z. B. von 6.1 auf 7.0).

Der Zugriff auf erweiterte Menüs zum Sichern und Wiederherstellen wird über ein anderes Benutzerkonto als das Administratorkonto gesteuert.

- **Linux-basierte Server**

Bei Portalen, die auf einem Linux-basierten Server ausgeführt werden, kann das Portal in die Sicherungs- und Wiederherstellungsfunktionen, die durch die Web-Management-Menüs des Linux-Servers bereitgestellt werden, eingefügt werden. Zu diesen Optionen gehört die Sicherung in einem HTTP-Server. HTTPS- und SFTP-Server und geplante Sicherungsvorgänge.

4.1 Anmelden

Es kann jeweils nur ein Benutzer als Superuser angemeldet sein.

- Standardmäßig verwenden Linux-basierte one-X Portal for IP Office-Server die **externe Authentifizierung**. Dies bedeutet, dass die Berechtigungen für die Portaladministration Sicherheitsbenutzern zugewiesen werden, die in der Sicherheitskonfiguration des IP Office-Diensts konfiguriert sind, der auf demselben Server ausgeführt wird. Standardmäßig ist dies der Benutzer **Administrator**, allerdings können auch zusätzliche Dienstbenutzer als Portaladministratoren konfiguriert werden.
- Wenn die externe Authentifizierung deaktiviert ist, verwendet das Portal sein eigenes lokales Administratorkonto auf die gleiche Weise wie für einen Windows-basierten Server (siehe unten).

So melden Sie sich an:

1. Geben Sie die Browser-Adresse **<http://<Server-Name>:<Server-Port>/onexportal-afa.html>** ein, wobei gilt:
 - **<Server-Name>** ist der Name oder die IP-Adresse des one-X Portal for IP Office-Servers.
 - **<Server-Port>** ist die Portnummer, die von one-X Portal for IP Office verwendet wird. Diese ist entweder 9443 oder 8443 für HTTPS-Zugriff.
 - Sie können **http://** anstelle von **https://** und **8080** als den Port verwenden, wenn ein unsicherer Zugriff konfiguriert wurde. Siehe [Protokoll](#)^[35].
 - Alternativ können Sie aus dem Anmeldemenü für normale Benutzer **AFA-Login** auswählen.
2. Geben Sie im Anmeldemenü das Kennwort ein:
 - Auf einem Linux-basierten Server geben Sie das Kennwort eines IP Office-Sicherheitsbenutzers ein, der für den Zugriff als [one-X Portal-Superuser konfiguriert ist](#)^[96]. Standardmäßig ist dies der Benutzer **Administrator**.
 - Auf einem Windows-basierten Server geben Sie den Namen **Superuser** und das zugehörige Kennwort ein.
 - Nutzen Sie das Standardkennwort, wenn Sie sich das erste Mal anmelden **MyFirstLogin1_0**. Nachdem Sie sich angemeldet haben, werden Sie zur Eingabe eines neuen Kennworts für das **Superuser**-Konto und weiterer Informationen aufgefordert.
 - **Anzeigename**
Geben Sie einen Namen ein, der in den Menüs von one-X Portal for IP Office angezeigt werden soll.
 - **Kennwort/Kennwort bestätigen**
Geben Sie ein Kennwort ein, das für den künftigen **Superuser**-Zugriff verwendet werden soll. Dieses Kennwort wird auf Windows- und Linux-basierten Servern verwendet, die nicht die **externe Authentifizierung** nutzen.

4.2 Systemstatus

Dieses Menü gibt Ihnen einen Überblick über die vorherige Nutzung der Superuser-Menüs. Außerdem ermöglicht es ein Rollback für den letzten Wiederherstellungsvorgang.

System status			
	Backup Name	File Size in Bytes	Backup Date Time
Last Backup Taken	OneX-DB-Bkp	29882	2010-08-03-11.33.25
	Backup Name	File Size in Bytes	Restore Date Time
Last Restore Done	OneX-DB-Bkp-2010-08-03-	29898	2010-08-03-11.38.32
			<input type="button" value="Undo Last Restore"/>
Local Server Total Space	149	GB	
Local Server Free Space	91	GB	

- Letzte Sicherung**
 Dieser Abschnitt enthält Einzelheiten zur letzten Sicherung, die über das Menü „Sicherung“ ausgeführt wurde. Die Sicherungsdatei ist eine ZIP-Datei, deren Dateiname aus der **Bezeichnung der Sicherung** und **Sicherungsdatum/-uhrzeit** zusammengesetzt ist. Beispiel: **OneX-DB-Bkp-2010-08-03-11.33.25.zip**.
- Letzte Wiederherstellung**
 Dieser Abschnitt enthält Einzelheiten zum letzten Wiederherstellungsvorgang. Uhrzeit und Datum der Wiederherstellung sowie der Name der dazu verwendeten Datei werden angezeigt. Mit dem Steuerelement „Letzte Wiederherstellung rückgängig machen“ kann ein Rollback für die Wiederherstellungsaktion ausgeführt werden.
- Gesamtspeicherplatz lokaler Server**
 Zeigt den ungefähren Gesamtspeicherplatz auf dem one-X Portal for IP Office-Server an.
- Freier Speicherplatz auf lokalem Server**
 Zeigt den ungefähren freien Speicherplatz auf dem one-X Portal for IP Office-Server an.

4.3 Konfiguration

Dieses Menü dient zum Festlegen der grundlegenden Einstellungen für den **Superuser**-Zugriff.

System Status	
Configuration	Edit
Edit	
DB Operations	
	<p>Password Complexity Requirements:</p> <ol style="list-style-type: none"> 1. Minimum Password length supported is 8 2. The password characters must include characters from at least 2 of the 'complexity rules' listed below. For example a mix of lower case and upper case. In addition, three or more repeated characters of the same case are not allowed. <ol style="list-style-type: none"> a. Lower-case alphabetic characters. b. Upper-case alphabetic characters. c. Numeric characters. d. Non-alphanumeric characters (for example # or *).
	Super User Name <input type="text" value="Superuser"/> Display Name <input type="text" value="Superuser"/> Password <input type="password" value="....."/> Confirm Password <input type="password" value="....."/>
	<input type="button" value="Save"/> <input type="button" value="Clear"/>

- Superuser-Name**
 Dies ist ein feststehender Name, der nicht geändert werden kann.
 - Anzeigenname**
 Geben Sie einen Namen ein, der in den Menüs von one-X Portal for IP Office angezeigt werden soll.
 - Kennwort/Kennwort bestätigen**
 Geben Sie ein Kennwort ein, das für den künftigen **Superuser**-Zugriff verwendet werden soll. Dieses Kennwort wird auf Windows- und Linux-basierten Servern verwendet, die nicht die **externe Authentifizierung** nutzen.

4.4 DB-Vorgänge

Diese Menüs dienen zum Erstellen von Sicherungsdateien und zum Wiederherstellen der Einstellungen aus einer vorherigen Sicherungsdatei.

4.4.1 Sichern

Dieses Menü dient zum Erstellen von Sicherungsdateien.

System Status

Configuration

DB Operations

Backup

Restore

Backup

Backup Name

Note: Server timestamp at time of taking backup will be appended to the backup name, e.g. OneX-DB-Bkp-2010-01-18-12.50.24.zip

Backup To

Local Server FTP Local Drive

Server IP Address

Port

User Name Password

Backup

- **Sicherungsname**
Dieser Name wird für die ZIP-Sicherungsdateien verwendet. Datum und Uhrzeit der Sicherung werden dem Dateinamen ebenfalls hinzugefügt. Beispiel: **OneX-DB-Bkp-2010-08-03-11.33.25.zip**.
- **Sicherung auf**
Diese Einstellung dient zum Auswählen des Ziels für die Sicherungsdatei.
- **Lokaler Server**
Bei Auswahl dieser Option wird die Sicherungsdatei im **Sicherungsordner** erstellt.
- **FTP**
Bei Auswahl dieser Option wird die Sicherungsdatei zeitweilig im **Sicherungsordner** erstellt. Anschließend wird sie an die angegebene FTP-Serveradresse gesendet.
- **Lokales Laufwerk**
Bei Auswahl dieser Option wird die Sicherungsdatei zeitweilig im **Sicherungsordner** erstellt. Anschließend wird sie vom Browser zum Herunterladen angeboten.
- **FTP-Einstellungen**
Wenn als Ziel der Sicherungsdatei **FTP** festgelegt ist, werden die folgenden Einstellungen verwendet.
- **Server-IP-Adresse**
Die Adresse des FTP-Servers, einschließlich Dateipfad.
- **Port**
Der FTP-Port auf dem Server. Normalerweise ist standardmäßig Port 21 eingestellt.
- **Benutzername/Kennwort**
Benutzername und Kennwort für den Dateizugriff auf dem angegebenen FTP-Server.
- **Sicherung**
Über diese Schaltfläche wird eine Sicherung mit den oben stehenden Einstellungen gestartet.

4.4.2 Wiederherstellen

Über dieses Menü kann eine vorherige Sicherungsdatei ausgewählt und für einen Wiederherstellungsvorgang verwendet werden. Bevor die Wiederherstellung erfolgt, wird eine Sicherung der aktuellen Konfiguration erstellt und im **Sicherungsordner** gespeichert. Diese kann mit dem Steuerelement **Letzte Wiederherstellung rückgängig machen** verwendet werden. Eine Wiederherstellung ist nur von einer Sicherung der gleichen one-X Portal for IP Office-Version aus möglich.

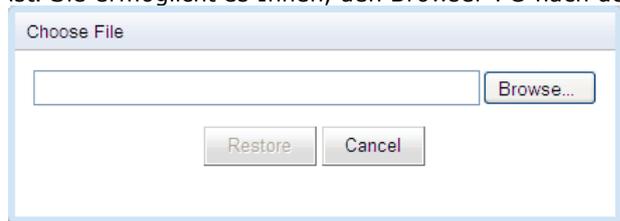
- Wiederherstellen von**
 Diese Einstellung dient zum Auswählen des Ziels, aus dem die vorherige Sicherungsdatei ausgewählt werden soll.
- Lokaler Server**
 Bei Auswahl dieser Option wird die Sicherungsdatei für die Wiederherstellung im konfigurierten **Sicherungsordner** ausgewählt.
- FTP**
 Bei Auswahl dieser Option wird die Sicherungsdatei für die Wiederherstellung unter der angegebenen FTP-Serveradresse ausgewählt.
- Lokales Laufwerk**
 Bei Auswahl dieser Option wird die Sicherungsdatei für die Wiederherstellung mithilfe eines Dateisuchmenüs auf dem Browser-PC ausgewählt.
- FTP-Einstellungen**
 Wenn als Ziel der Sicherungsdatei **FTP** festgelegt ist, werden die folgenden Einstellungen verwendet.
- Server-IP-Adresse**
 Die Adresse des FTP-Servers, einschließlich Dateipfad.
- Port**
 Der FTP-Port auf dem Server. Normalerweise ist standardmäßig Port 21 eingestellt.
- Benutzername/Kennwort**
 Benutzername und Kennwort für den Dateizugriff auf dem angegebenen FTP-Server.
- Verfügbare Sicherungen anzeigen**
 Diese Schaltfläche wird angezeigt, wenn die Option **Wiederherstellen von** auf **Lokaler Server** oder **FTP** festgelegt ist. Wenn Sie darauf klicken, wird eine Liste der verfügbaren Sicherungsdatei am ausgewählten Speicherort angezeigt. Wählen Sie eine Datei, und klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsvorgang zu starten.

Select	Backup Folder	Backup Name	File Size in Bytes	Backup Date Time
<input type="radio"/>	C:\Backups	OneX-DB-Bkp-2010-08-03-11.32.55.zip	29898	Tue Aug 03 19:32:55 GMT+100 2010
<input type="radio"/>	C:\Backups	OneX-DB-Bkp-2010-08-03-11.33.25.zip	29882	Tue Aug 03 19:33:25 GMT+100 2010
<input type="radio"/>	C:\Backups	OneX-DB-Bkp-2010-08-03-11.45.58.zip	29866	Tue Aug 03 19:45:59 GMT+100 2010

Restore Cancel

- **Datei auswählen**

Diese Schaltfläche ist verfügbar, wenn die Option **Wiederherstellen von** auf **Lokales Laufwerk** festgelegt ist. Sie ermöglicht es Ihnen, den Browser-PC nach der Sicherungsdatei zu durchsuchen.



Index

4

4560 91

A

Abmelden 9

Administrator

Hilfe 51

Name 9

Administratorsitzung außer Kraft setzen 9

Aktive Sitzungen 12, 18

Aktivieren

Externe Minianwendung 67

Anbieter 12

Ansicht 19

CSTA (IP Office) 20

DSML (IP Office) 21

DSML (LDAP) 22

Verzeichnis (DSML IP Office) 21

Verzeichnis (DSML LDAP) 22

Voicemail 23

Zuweisen 19

Anmelden 9

Fehlgeschlagen 17

Anrufprotokoll 68

Ansicht

Komponentenstatus 15

Konferenz 50

Letzte wichtige Ereignisse 17

Anwesenheit 68

Exchange 27, 83

Konfiguration 79

Status 81

Anzeigen

Anbieter 19

Apache

Chainsaw 39, 91

Archiv

IM-Sitzungen 78

Audiokonferenz 50

Ausnahmen 68

Automatische Abmeldung 9

B

Basis-DN 70

Bearbeiten

Benutzereinstellungen 24, 68

IP Office-Einstellungen 58

Massenbearbeitung 68

Minianwendung 66

Benutzer 12

Aktiv 18

Ansicht 24

Datenüberprüfung 41

Einstellungen bearbeiten 24, 68

Exportieren 25

Hilfe 51

Hinzufügen 68

Löschen 68

Massenbearbeitung 68

Neusynch 44, 73

Blockieren von Clients 35

Blockierte Clients 35

C

Chainsaw 39, 91

CSTA 20

CSTA (IP Office)-Anbieter 20

CSV 12, 25

D

Datenbank

Integritätsprüfung 40

Prüfen 40

Datenbankintegrität 12

Datenüberprüfung 41

Deinstallation 76

Deinstallieren 76

Diagnose 12

Datenbankintegrität 40

IP Office-Verbindungen 40

Netzwerkrouen 39

Protokollanzeige 39, 91

Protokollierung konfigurieren 37, 91

Verbindungen 40

Dienst

Neustart 54

Dienst neu starten 54

Dienst starten 54

DND-Ausnahmen 68

Domänenname

XMPP-Domänenname 79

Downgrade 75

DSML (IP Office)-Anbieter 21

DSML (LDAP)-Anbieter 22

E

Echo 39

Einstellungen

Massenbearbeitung 68

Entfernen

Benutzer 68

IP Office 58

one-X Portal for IP Office 76

Ereignisse 17

Erreichbar 39

Exchange 27, 83

exportDirectoryEntry.csv 25

Exportieren

Minianwendungen 48, 65

exportUser.csv 25

Externes Verzeichnis

Suchen 44, 72

F

Fehlgeschlagene Anmeldungen 17

Feldzuweisung 22, 70

H

Hauptprotokollebene 37

Hilfe 12

Hilfe 51

Info 51

Unterstützung von Avaya 51

Hinzufügen

Benutzer 68

IP Office 56

LDAP 70

Minianwendung 66

I

IM

Archivieren 78

Konfiguration 79

IM

Sitzungen durchsuchen 49, 82
Status 81

Importieren

Minianwendungen 63

Info 12**Integrität** 40**IP Office**

CSTA-Anbieter 20
Verbindungen 12
Verzeichnisanbieter 21

J

Java Web Start 91

Jeder kann sich verbinden. 79

K

Kalender 27, 83

Kennwort 9

Komponentenstatus 12, 15

Konferenz 50

Konfiguration 12

Anbieter 19
Anwesenheit 79
Benutzer 24
CSV 25
Exportieren 25
IM 79
Marken 25
Massenbearbeitung 68

Konfiguration exportieren 25

L

LDAP 72

Anbieter 22
Verzeichnissuche 12, 44, 72
Zuweisen 70

Letzte Ereignisse 17

Letzte wichtige Ereignisse 12, 17

Log4j-Format 91

Löschen

Benutzer 68
IP Office 58
Minianwendung 67

M

Marken 25

Massenbearbeitung 24, 68

Benutzer 68

Minianwendung

Aktivieren 67
Bearbeiten 66
Deaktivieren 67
Exportieren 48, 65
Importieren 63
Löschen 67
URL 62

Minianwendungen

Auflisten der externen Minianwendungen 47

Monitor 50

N

Nachrichten 68

Netzwerkrouen 12, 39

Neusynchronisierung 44, 73

Neusynchronisierung erzwingen 44, 73

Nicht erreichbar 39

P

Parkbereiche 68

Persönliches Verzeichnis 68

Ping-Test 39

Port

4560 91
7 39

Protokolldateien 37

Protokollierung 91

Ebene 37
Konfiguration 12
Viewer 12, 91
Ziele 37

Protokollierung konfigurieren 91

R

Remote-Protokollierung 91

Rollende Protokolldateien 37

Routen 39

Ruhedauer vor Zeitabschaltung. 79

S

Server

Informationen 18
Version 18

Sicherungen 12

Sitzungen 18

Sitzungszähler zurücksetzen 9

Socket-Empfänger 37, 91

Sofortige Abmeldung 9

Status 12, 15

Aktive Sitzungen 18
Anwesenheit 81
IM 81
Komponente 15
Komponentenstatus 15
Letzte wichtige Ereignisse 17
Umgebung 18

Such-Basis 70

Suche

IM-Sitzungen 49, 82

Suchen

LDAP 44, 72
Systemverzeichnis 46, 73

Synchronisation 44, 73

Systemsteuerung 76

Systemverzeichnis 12

Exportieren 25
Neusynch 44, 73
Verzeichnissuche 46, 73

T

Tastenkombinationen 68

TCP-Port 7 39

Teilnehmer 50

Test

Externes Verzeichnis 44, 72
IP Office-Verbindung 40
LDAP-Verzeichnis 44, 72
Netzwerkroute 39
Systemverzeichnis 46, 73

Trennung im Leerlauf. 79

U

Umgebung 12

Unterstützung von Avaya 12

Upgrade 74

V

Version 18

Verzeichnis

Exportieren 25

Neusynch 44, 73

Verzeichnis (DSML IP Office) 21

Verzeichnis (DSML LDAP) 22

Verzeichnisintegration 12

LDAP 44, 72

Systemverzeichnis 46, 73

Verzeichnissynchronisierung 44, 73

Verzeichnissuche

LDAP 44, 72

Systemverzeichnis 46, 73

Verzeichnissynchronisierung 12

Voicemail

Anbieter 23

Voicemail-Nachrichten 68

W

Webkonferenz 50

X

XMPP-Domänenname 79

Z

Zuweisen

Anbieter 19

IP Office 56, 58

IP Office (CSTA) 20

IP Office (Verzeichnis) 21

LDAP-Anbieter 22

Voicemail-Dienstanbieter 23

