

# OpenScape Business

Tutorial

Maßnahmen gegen Gebührenbetrug

Version 1.0

## Über dieses Dokument

Die Beschreibungen in diesem Dokument beziehen sich auf OpenScape Business V2R2

## Disclaimer & Copyright

Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen und Leistungsmerkmale, die je nach Anwendungsfall nicht immer in der beschriebenen Form zutreffen oder sich durch Weiterentwicklung der Produkte ändern können. Eine Verpflichtung, die jeweiligen Merkmale zu gewährleisten besteht nur, sofern diese ausdrücklich vertraglich zugesichert wurden. Liefermöglichkeiten und technische Änderungen vorbehalten.

Unify, OpenScape, OpenStage und HiPath sind eingetragene Warenzeichen der Unify Software and Solutions GmbH & Co. KG. Alle anderen Marken-, Produkt- und Servicenamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

Alle Rechte vorbehalten.

© Unify Software and Solutions GmbH & Co. KG 2016

## Dokument Historie

Datum	Version	Änderungen / Bemerkungen
2017-02-13	1.0	Ersterstellung

## Inhaltsverzeichnis

1. Vorwort	5
2. Einführung	6
2.1. Gebührenbetrugsszenarien	6
2.2. Allgemeine Schutzmaßnahmen	6
3. Gebührenbetrug mittels Voicemail- und Autoattendant Mailboxen	8
3.1. Angriffe auf Voice- Autoattendant Mailboxen	8
3.2. Maßnahmen zum Schutz der UC Suite Voicemail Mailbox	8
3.2.1. Festsetzen der PIN Länge auf mindestens 6-Stellen	8
3.2.2. Einschränken von Rückrufen aus der VoiceMail Box	9
3.2.3. Vergabe von individuelle PIN für den Voicemail Mailbox Zugriff	10
3.2.4. Erzwingen der PIN Abfrage	10
3.2.5. Einschränken der Berechtigung für Anrufe aus der UC Suite Voicemail	11
3.3. Maßnahmen zum Schutz der UC-Smart Voicemail Mailbox	12
3.3.1. Vergabe einer „starken“ individuellen PIN	12
3.3.2. Einschränkung von Rückrufen aus der VoiceMail Box	12
3.3.3. Einschränken der Voicemail Erreichbarkeit von extern.	14
3.3.4. Vertraulichkeit der Voicemail Durchwahlnummern gewährleisten	15
3.3.5. Deaktivieren der Smart Voicemail Funktion.	15
3.3.6. Sicherung des AutoAttendant	15
3.4. Maßnahmen zum Schutz der Xpressions Compact Voicemail Mailbox	16
4. Gebührenbetrug mittels VoIP Endgeräte	17
4.1. Maßnahmen gegen Registrierung fremder SIP Endgeräte	17
4.1.1. Authentifizierung des SIP Endgeräts	17
4.1.2. Nutzung eines starken individuellen Kennworts für die Authentifizierung	18
4.1.3. Vergabe einer starken SIP User ID / Benutzernamen	18
4.1.4. Löschen von SIP Testanschlüssen	19
4.1.5. Löschen von nicht genutzten / überzähligen SIP Anschlüssen	19
4.1.6. Nutzung des internen SBC bei extern angeschalteten Endgeräten	19
4.1.7. Verwendung spezieller Ports für extern angeschaltete SIP Teilnehmer	19
4.2. Maßnahmen gegen Registrierung fremder System (HFA) Endgeräte	20
4.2.1. Authentifizierung des System (HFA) Endgeräts	20
4.2.2. Nutzung eines starken individuellen Kennworts für die Authentifizierung	20
4.2.3. Löschen von System (HFA) Testanschlüssen	20
4.2.4. Löschen von nicht genutzten / überzähligen System (HFA) Anschlüssen	20

4.2.5. Nutzung des internen SBC bei extern angeschalteten Endgeräten	20
4.2.6. Port Forwarding für extern angeschaltete System (HFA) Teilnehmer einrichten.	21
5. Gebührenbetrug mittels DISA Port	22
5.1. Angriffe auf den DISA Port	22
5.2. Maßnahmen gegen Angriffe auf den DISA Port bei OpenScape Business	22
5.2.1. Sperren bzw. keine Freigabe des DISA Ports	22
5.2.2. Restriktiver Umgang mit den Teilnehmer Flag „DISA Berechtigung	23
5.2.3. Ändern der Telefonschloss PIN für die „DISA Berechtigung“ Teilnehmer.	23
5.2.4. Sperren der DISA-Freigabe für Leitungen	24
5.2.5. Restriktiver Umgang mit der Publizierung des DISA Ports und DISA PIN	24
5.2.6. Sicherung des mobilen Telefon vor Fremdzugriff	24

# 1. Vorwort

Durch die Zusammenführung der klassischen TK-Anlage mit Voice over IP zu Hybrid Anlagen addieren sich auch die jeweils spezifischen Sicherheitsrisiken der verwendeten Technologien.

Viele Bücher, Dokumente, Leitfäden und Checklisten thematisieren die Bedrohungen und Sicherheitsfragen im TK / IT Umfeld. Viele davon zeigen die prinzipiellen Gefährdungen und die Gegenmaßnahmen ohne jedoch auf konkrete Systeme und deren Einstellungen einzugehen.

Für OpenScape Business beschreibt die Security Checkliste alle potentiellen Bedrohungen und die entsprechende Gegenmaßnahmen zur Risikominimierung. Die Checkliste kann über das Unify Partner Portal herunter geladen werden. Nur die konsequente Anwendung aller in der Security Checkliste aufgeführten Maßnahmen kann ein OpenScape Business System optimal schützen und Schäden vom Betreiber abwenden.

Trotz der Verfügbarkeit der Security Checkliste sind jedoch immer noch sehr viele OpenScape Business Systeme unzureichend gegen Angriffe gesichert. Bereits ein einziger erfolgreicher Angriff kann für den Betreiber zu einem großen finanziellen Schaden führen.

Dieses Dokument zeigt potentielle Angriffspunkte für Gebührenbetrug sowie konkrete Gegenmaßnahmen auf. Es soll dazu dienen, den Betreiber und den Administrator des Systems für das Thema zu sensibilisieren und es ihnen ermöglichen das System gezielt gegen Betrugsversuche abzusichern.

Das Dokument ersetzt nicht die Anwendung der Security Checkliste.

## 2. Einführung

Dieses Dokument stellt in kurzer Form die in der Praxis am häufigsten auftretenden Angriffsszenarien für einen Gebührenbetrug und die empfohlenen Gegenmaßnahmen dazu dar.

Die Verwendung standardisierter Kommunikationsprotokolle ermöglicht Angreifern auch ohne tiefgreifendes System Knowhow Angriffe mit entsprechenden SW Tools auszuführen und Schaden anzurichten, wenn die Schnittstellen nicht ausreichend geschützt sind.

Der Betrieb von Kommunikation Software (SW) wie Smartphones, Unified Communications oder CTI Clients auf Standard PC, Tablet oder Smartphone Plattformen und der darüber mögliche Zugang zu internen Systemdiensten wie Voicemail- oder UC- Server erleichtert den Angreifern die Attacken wenn die Geräte und die Kommunikation SW nicht ausreichend gesichert sind.

Auch der Zugang zu nicht gesicherten Systemdiensten wie Voicemail- oder Disa Ports oder zu nicht abgeschlossenen öffentlich zugänglichen Telefonen erleichtert Angreifern die unautorisierte Nutzung von Systemleistungsmerkmalen.

### 2.1. Gebührenbetrugsszenarien

Meistens erfolgen die Gebührenbetrugs Angriffe am Wochenende, wenn niemand im Unternehmen ist. Kriminelle Hacker verschaffen sich Zugang über das Telefonnetz oder – je nachdem welche Telefontechnologie verwendet wird – auch über das Internet. Ist der Einbruch in das Telekommunikationssystem (TK-System) der Firma erst einmal gelungen, so werden automatisiert möglichst viele, kurze Verbindungen zu beispielsweise Mehrwertdienste-Nummern im Auslandsaufgebaut. Zu oft können die Täter tatsächlich abkassieren und verstecken sich hinter kurzlebigen Briefkastenfirmen in verschiedensten Teilen der Welt.

Gebührenbetrug findet in den meisten Fällen durch Rufumleitungen statt, z.B. über:

- den Zugriff auf unzureichend gesicherte Voice- und AutoAttendant Mailboxen
- unzureichend gesicherte Telefone und Systemschnittstellen
- den Zugriff auf unzureichend gesicherte DISA Ports

### 2.2. Allgemeine Schutzmaßnahmen

Prinzipiell dürfen nur die vom Betreiber benötigten Teilnehmer, Leistungsmerkmale und Schnittstellen in OpenScape Business freigeschaltet werden.

- Es dürfen nur so viele Teilnehmer wie benötigt im System eingerichtet werden.
- Testteilnehmer etc. sind vor der Übergabe des Systems an den Betreiber zu entfernen.
- Die Berechtigungen zur Nutzung von Leistungsmerkmalen müssen teilnehmerindividuell auf das benötigte Maß eingeschränkt werden.
- Die Berechtigungen für Systemteilnehmer wie Voicemail- oder DISA Ports etc. sind auf das benötigte Maß einzuschränken.
- Die Anwender müssen die Standardpasswörter für die von ihnen individuell genutzten Dienste wie z.B. Voicemail, UC Client oder auch für die Telefonendgeräte individuell ändern.
- Der Zugang zur Systemadministration muss technisch gesichert und die werksseitig eingestellten Zugangsdaten müssen individualisiert werden.
- Der Personenkreis mit Zugang zur Systemadministration muss eingeschränkt und benannt werden.
- Administrations SW darf nicht auf ungesicherten PC verbleiben.

- Das erste und zweite Systemendgerät (in der Konfiguration) müssen physikalisch und logisch gegen unbefugten Zugriff gesichert werden.
- Remote Zugänge sind nur dann einzurichten bzw. freizugeben, wenn sie benötigt werden.
- Remote Zugänge sind speziell ggf. über externe Sicherungsmaßnahmen gegen unbefugten Zugriff zu sichern.

Bei neu ausgelieferte OpenScape Business Systeme mit Software Ständen größer, gleich V2R2 sind nach der Erstinbetriebnahme nur die für die Ersteinrichtung erforderlichen Schnittstellen geöffnet.

Bei einem SW-Upgrade von vorhergehenden SW-Versionen bzw. bei migrierten HiPath 3000 Konfigurationen werden die jeweiligen Schnittstelleneinstellungen übernommen. Diese Systeme sind nach einem Upgrade / nach einer Migration hinsichtlich geöffneter Schnittstellen und aktiver Standard Passwörter zu überprüfen und ggf. abzusichern.

# 3. Gebührenbetrug mittels Voicemail- und Autoattendand Mailboxen

Voice- und Autoattendand Mailboxen bieten die Möglichkeit aus der Mailbox heraus Anrufe zu bestimmten Zielen weiterzuleiten. Die Weiterleitungsziele werden vom Anwender über das Administrationsmenü der Mailbox durch die Eingabe von DTMF Zeichen konfiguriert. Der Aufruf des Konfigurationsmenüs ist durch eine individuelle PIN geschützt. Abhängig von der verwendeten Voicemail / Autoattendand Software, sind die Mailboxen nach der Erstinbetriebnahme mit einer für alle Anwender einheitlichen PIN geschützt die vom Anwender geändert werden sollen. Einige Systeme zwingen den Anwender zur Neuvergabe einer PIN vor der ersten Nutzung bzw. beim erstmaligen Einrichten der Mailbox.

## 3.1. Angriffe auf Voice- Autoattendand Mailboxen

Besonders leicht ist es für die Angreifer, wenn bei den Mailboxen werksseitig voreingestellte Passwörter (z. B. »0000«) nicht geändert oder in zu leichte Varianten geändert wurden (z. B. »1234«) und aus diesen Boxen Verbindungen nach außen aufgebaut werden können.

Genau danach suchen viele der Angreifer und tätigen mit automatisierter Software abends und nachts massenhaft kurze Testanrufe. Nach dem Zufallsprinzip werden ganze Rufnummernblöcke von Unternehmen nach Schwachstellen durchsucht. Wenn die Software auf keine Passworthürde trifft oder eine zu schwache Hürde überwindet, kann der Angriff sofort beginnen. Um unentdeckt maximal abschöpfen zu können, erfolgt der Angriff jedoch oft erst ab dem folgenden Freitagabend bis montags früh.

## 3.2. Maßnahmen zum Schutz der UC Suite Voicemail Mailbox

Bei der UC Suite Voicemail Mailbox versuchen die Angreifer über einen Telefonanruf auf die Voicemail-Mailbox und durch die Eingabe von „#“ in das Konfigurationsmenü der Mailbox zu gelangen. Im Falle des erfolgreichen Zugriffs versuchen die Angreifer die Anrufziele, bzw. das Rückrufziel zu manipulieren und auszunutzen.

Die Konfiguration der UC Suite Voicemail über die Telefonschnittstelle (TUI) ist durch Abfrage der Teilnehmernummer und der zugehörigen PIN geschützt. Jedoch kann ein UC Suite myPortal Anwender diese Schutzmaßnahmen zur Erleichterung der Voicemail Abfrage durch „bekannte Rufnummern“ aufheben. Bekannte Rufnummer sind Rufnummern, die der UC Suite Anwender in seinem myPortal Client unter dem Punkt „Eigene Persönliche Daten“ eingetragen hat. In diesem Zusammenhang ist zu beachten, dass Angreifer in der Lage sind die Rufnummer des Rufenden Anschlusses (Calling Party Number) zu fälschen und der UC Suite Voicemail eine bekannte Rufnummer vorzutäuschen.

Eine generelle Schutzmaßnahme der UC Suite Voicemail ist, dass nach wiederholter Fehleingabe der PIN der Zugang zur VM Abfrage / Konfiguration gesperrt und die Verbindung getrennt wird. Die Sperrung wirkt sich auch auf den UC Client eines Anwenders aus und kann nur durch den Systemadministrator aufgehoben werden.

Um die UC Suite Voicemail Mailbox gegen Angreifer optimal zu schützen sind zusätzlich folgende Maßnahmen durchzuführen und die Voicemail Anwender sind entsprechend einzuweisen.

### 3.2.1. Festsetzen der PIN Länge auf mindestens 6-Stellen

Der Systemadministrator muss in der UC Suite Konfiguration die Länge der PIN auf mindestens 6 Stellen festlegen. Hierbei gilt je höher die Stellenzahl der PIN desto höher der Schutz.



Copyright by Unify Software and Solutions GmbH & Co. KG. All rights reserved. Powered by eTellicom

<b>Allgemeine Einstellungen</b>	<b>Bürozeiten</b>
Gespräch aufzeichnen	Startzeit: 08:00
Protokolle	Endezeit: 18:00
Benachrichtigungen	<b>Kennwortlänge</b>
Wartung	Längen: 6
Sprachnachrichten	<small>Durch Ändern der Passwörter werden die Passwörter aller Benutzer zurückgesetzt</small>
	<b>Rufnummer des Abwurfplatzes</b>
	Zielnummer:

Bild 1 UC-Suite: Länge Voicemail Mailbox PIN Länge

### 3.2.2. Einschränken von Rückrufen aus der VoiceMail Box

Der System Administrator muss in den Systemeinstellungen der UC Suite festlegen, dass die Voicemail Mailbox nur dann Rückrufe zum Anrufer zulässt wenn der Abfrage Anruf von einer „bekannten Rufnummer“ aus getätigt wird.

OMP\_OSQ\_V4\_01(6.2.260B) © Copyright by Unify Software and Solutions GmbH & Co. KG. All rights reserved. Powered by eTellicom

<b>Module:</b>	Allgemeine Einstellungen	VoiceMail-Sprache	German (Germany)
Benutzerverzeichnis	Gespräch aufzeichnen	Wiedergabereihenfolge für Sprachnachrichten	Neueste zuerst
Abteilungen	Protokolle	Aufzeichnungszeit Sprachnachricht	900 Sekunden
Gruppen	Benachrichtigungen	<b>VoiceMail-Modus</b>	Voll
Templates	Wartung	Rückruf von VM nur an bekannte Nummer zulassen	<input checked="" type="checkbox"/>
Externes Verzeichnis	<b>Sprachnachrichten</b>		
Externer Anbieter			
Contact Center			
Zeitpläne			
Datei-Upload			
Konferenzschaltung			
Standort-Liste			
Server			

Bild 2 UC-Suite: Einschränken der Rückrufoption

Der UC-Suite Anwender ist darauf hinzuweisen, dass die Rufnummern in seinen persönlichen Daten als “bekannte” Rufnummer angesehen werden.

Einrichtung

<b>▼ Persönliche Daten</b>	<b>Eigene persönliche Daten</b>	
Eigene persönliche Daten		
Eigenes Bild		
<b>▼ Meine Einstellungen</b>		
Darstellung		
Benachrichtigungen		
Outlook-Anbindung		
Abkürzungstasten		
Verschiedenes		
<b>▼ Anrufregeln</b>		
Anrufweiterleitungsziele		
Regelmodul		

Benutzername:	33388	VoiceMail-Rufnummer:	94444
Nebenstelle:	33388	Mobilrufnummer:	<input type="text"/> <input checked="" type="checkbox"/> Sichtbar
Kennwort:	<input type="text"/> <input type="button" value="Ändern"/>	Externe Rufnummer 1:	56789 <input checked="" type="checkbox"/> Sichtbar
Vorname:	User	Externe Rufnummer 2:	23456 <input checked="" type="checkbox"/> Sichtbar
Nachname:	33388	Private Rufnummer:	67898 <input checked="" type="checkbox"/> Sichtbar

Bild 3 UC-Suite: “Bekannte” Rufnummern

### 3.2.3. Vergabe von individuelle PIN für den Voicemail Mailbox Zugriff

Bei UC-Suite wird eine gemeinsame PIN für den Zugriff auf die Voicemail Mailbox und für die UC-Suite Clients verwendet. Bei erstmaligem Zugriff auf die Voicemail bzw. den UC-Client muss der Anwender die im System vergebene Default PIN „1234“ ändern. Der Anwender muss darauf hingewiesen werden, dass er eine individuelle „starke“ PIN verwenden muss und diese nicht an Dritte weitergegeben werden darf. Aufeinanderfolgende Ziffern (z.B. 234567), gleiche, zusammenhängenden Ziffern (z.B. 11111) oder die NST-Nr. dürfen aus Sicherheitsgründen als PIN nicht verwendet werden.

### 3.2.4. Erzwingen der PIN Abfrage

In den persönlichen Einstellungen des UC Client darf die Checkbox Überspringen der PIN Abfrage durch den Anwender nicht gesetzt werden. Ansonsten wird keine Prüfung der PIN beim Zugriff auf die Voicemail Mailbox vorgenommen, wenn von einer „bekannten Rufnummern“ aus angerufen wird.

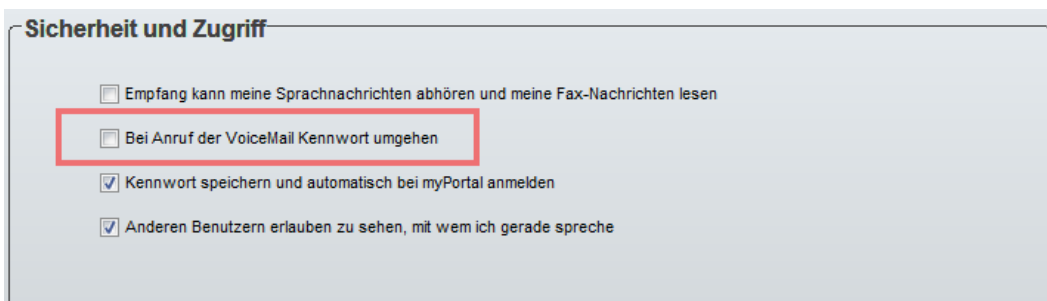


Bild 4 UC Suite: Erzwingen der PIN Abfrage

Dieser Parameter kann durch den UC-Suite Administrator den UC Suite Usern über eine Policy in den UC Suite Server Einstellungen fest zugewiesen werden.

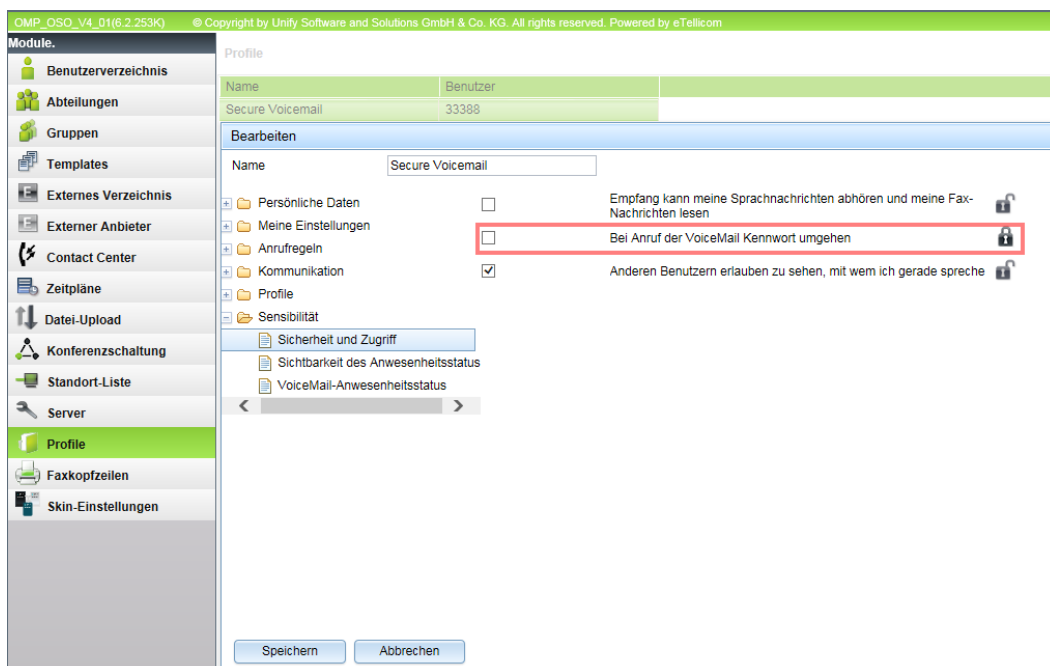


Bild 5 UC-Suite: Definition der PIN Policy

### 3.2.5. Einschränken der Berechtigung für Anrufe aus der UC Suite Voicemail

Über das Systemflag „Einschränkungen für UC-Anrufe“ wird für alle durch die UC-Suite Applikation initiierten Anrufe vor der Wahl geprüft, ob der zugehörige UC Benutzer die Berechtigung für diesen Anruf hat. Dadurch wird sichergestellt, dass aus der Voicemail Mailbox eines UC Users keine höher berechtigten Anrufe als durch den UC User selbst geführt werden können.

**Experten-Modus - Telephonie**

**Grundeinstellungen**

- ▼ System
  - System Flags**
  - Zeitparameter
  - Display
  - DISA
  - Abwurf/VPL/Hotline
  - LDAP
  - Texte
  - Flexible Menüs
  - Kurzwahlziele
  - Servicekennzahlen
  - Gateway
- DynDNS
- Quality of Service
- Datum und Uhrzeit
- Port-Verwaltung
- Gebühren
  - Wiedergabegerät für Sprachnachrichten/Ansagen
  - Telefonparameter-Bereitstellung
  - Power Management

**System Flags**

System Flags ändern

Knoten-Rufnummer bei Voice Mail:	<input type="checkbox"/>
Anrufübernahme nach Wiederanruf:	<input type="checkbox"/>
Einstellbare CLIP:	<input checked="" type="checkbox"/>
Anruferliste beim Zienteilnehmer im Falle Umleitung MULAP:	<input type="checkbox"/>
Rufweitschaltung nach Deflect call / Single step transfer:	<input type="checkbox"/>
Ermittlung des Ziels über Rufzielliste beim Deflect call / Single step transfer:	<input type="checkbox"/>
Hinweiston während Sprachaufzeichnung:	<input type="checkbox"/>
E.164 Nummerierung:	<input type="checkbox"/>
Erweiterte Schlüsselfunktionen:	<input type="checkbox"/>
A-Rufnummer in AUN-Gruppen / Rufzusaltung / Umleitungsziel / RWS-Ziel:	<input checked="" type="checkbox"/>
SPE Unterstützung:	<input type="checkbox"/>
SPE Advisory Ton:	<input type="checkbox"/>
SIP Prov. zu SIP Prov. transit:	<input type="checkbox"/>
Wahl von * und # auf Leitungsschnittstellen:	<input type="checkbox"/>
Richtungskennzahl für MEX hinzufügen:	<input type="checkbox"/>
CMI MWI Hinweiston:	<input type="checkbox"/>
Automatisches Software-Update für OpenStage TDM-Telefone:	<input checked="" type="checkbox"/>
Indirekte Richtungsverbindungen gemäß VBZ-Matrix einschränken:	<input type="checkbox"/>

**offene Nummerierung**

aktiv: ☐

Knoten-Rufnummer:

**Transiterlaubnis**

Leistungsmerkmal Transit: ☒

Transit Durchwahl Quer: ☒

Transit Durchwahl Amt: ☐

**Schalter Spezial**

CALL PROC nicht senden: ☐

Autom. zykl. Leitungsbelegung: ☒

**Einschränkung für UC-Anrufe**

Einschränkung für UC-Anrufe: ☒

Übernehmen Rückgängig Hilfe

Bild 6 UC-Suite: Einschränken der Berechtigung für UC-Anrufe

### 3.3. Maßnahmen zum Schutz der UC-Smart Voicemail Mailbox

Bei der UC-Smart Voicemail Mailbox versuchen die Angreifer über einen Telefonanruf auf die Voicemail-Mailbox und durch Unterbrechen der Ansage durch Eingabe von „#“ und anschließender Eingabe von Mailbox Nr. und PIN, zu gelangen. Im Falle des erfolgreichen Zugriffs versuchen die Angreifer das Rückrufziel wie folgt zu manipulieren und auszunutzen.

Eine generelle Schutzmaßnahme der UC-Smart Voicemail ist, dass nach wiederholter Fehleingabe der PIN der Zugang zur VM Abfrage / Konfiguration gesperrt und die Verbindung getrennt wird. Die Sperrung kann nur durch den Systemadministrator aufgehoben werden.

Bei der UC-Smart Voicemail ist zu beachten, dass das Verhalten der Voicemail Ports in OpenScape Business X und OpenScape Business S Modellen unterschiedlich ist und dass einige der genannten Maßnahmen gegen Missbrauch nur bei OpenScape Business X Modellen zur Verfügung stehen. Hierauf wird im folgenden Text gesondert hingewiesen.

#### 3.3.1. Vergabe einer „starken“ individuellen PIN

Der Voicemail Anwender wird bei der ersten Einrichtung seiner Voicemail Box vom System aufgefordert seine Default PIN für die Voicemail- Verwaltung /Abfrage zu ändern. Beim PIN Handling unterstützt das OpenScape Business System wie folgt:

- Der Erstlogin muss über die Interne Nebenstelle des Anwenders erfolgen.
- Die Default die PIN-Nr. der Mailboxen lautet „123456“,
- Die PIN Länge ist fest definiert auf 6 Stellen.
- Die Verwendung folgender Kombinationen wird von System geblockt :
  - Zahlenketten (z.B. 234567)
  - mehr als 3 gleichen, zusammenhängenden Ziffern (z.B. 111111).

Der Voicemail Anwender muss darüber hinaus angewiesen werden, dass er eine „starke“ individuelle PIN für den Zugang verwenden muss. Er ist darauf hinzuweisen, dass:

- die eigenen Nebenstellen Nummer, auch nicht rückwärts notiert, nicht Bestandteil der PIN sein soll
- keine PINs verwendet werden sollen, die bereits von anderen Anwendern genutzt werden.
- Die PIN in regelmäßigen Abständen verändert werden soll.

#### 3.3.2. Einschränkung von Rückrufen aus der VoiceMail Box

##### 3.3.2.1. Rufnummernlängenbegrenzung für gehende Verbindungen

Bei gehenden Verbindungen, die von der Smart Voicemail eingeleitet werden können nur Rufnummern bis zur angegebenen Länge gewählt werden. Bei längeren Rufnummern unterbleibt der Verbindungsaufbau. Im Standard entspricht die Rufnummernlängenbegrenzung der Mailbox-Rufnummernlänge (interne Rufnummernlänge), so dass nur eine Internwahl erlaubt ist. Diese Begrenzung gilt auch für die Rufnummern der AutoAttendant Nachwahl und AutoAttendant Kurzwahl

Die Einstellung erfolgt in den allgemeinen Parametern der Smart Voicemail

Einrichtung - Wizards - Zentrale Telephonie - SmartVM

allgemeine Parameter

allgemeine Parameter

maximale Mailbox-Nummerlänge: 3 (2..16)

Max. Nachrichtenlänge (Min.): 2 (1..2)

Rufnummernlängenbegrenzung: 3 (2..30)

Allgemeines Fax-Abwurfziel:

Standardsprache: Deutsch

Telephone User Interface (TUI): SmartVM

Reihenfolge der Datumsansage: Datum nach Nachricht

Anzahl der Nachrichten pro Mailbox: 30 (0..100)

Rückruf von VM nur an bekannte Nummer zulassen: ☒

AA-VP-Verhalten

VP vor Übergabe: ☐

VP-Übergabe-Ergebnis: ☒

VP-Abwurf: ☒

VP vor Trennen: ☒

Bild 7 UC-Smart Einschränkung von Rückrufen

### 3.3.2.2. Rückrufe ausschließlich zu bekannten Rufnummern.

Rückrufe aus der Voicemail Box können auf bekannte zuvor eingerichtete Mobil- bzw. Festnetzzrufnummer eingeschränkt werden. Die Einstellung erfolgt ebenfalls in den allgemeinen Parametern der Smart Voicemail. Wenn das Flag „Rückruf von VM nur an bekannte Rufnummern zulassen“ gesetzt ist, können aus der Smart Voicemail Box nur Rückrufe zu zuvor konfigurierten Rufnummern getätigt werden.

Dieser Rufnummer müssen innerhalb von OpenScape Business über den UC-Smart Assistent anwenderspezifisch konfiguriert werden. (Einrichtung → UC-Smart → UC-Smart).

UC Smart Assistant

Administration

Benutzerverwaltung

Benutzer

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

126, Test Device, Fir

127, Test Device, Sec

Einstellungen

Benutzer 126

Name Test Device, Fir

Passwort \*\*\*\*\*

Assistant-Sprache

Anwender muss neues Passwort vergeben ☒

Zugriff auf UC Smart Assistant ☒

Konfiguriert als Mobility-Teilnehmer ☐

Voicemail-Lizenz ☒

Assoziierte Dienste ☐

Vor der ersten Bedienung des Voicemail-Systems muss die PIN (Codenummer) der jeweiligen Mailbox geändert werden. Aus Sicherheitsgründen wird empfohlen, die PIN in regelmäßigen Abständen zu ändern.

Der Anwender muss das Passwort ändern, um die UC Smart Dienste nutzen zu können!

Profildetails

Mobile Rufnummer 0123 4567 890123

Private/externe Rufnummer 0987 654321

Email-Adresse

Voicemail an Email ☐

Sichtbarkeit Präsenzstatus Intern sichtbar

Lizenzierungsinformationen

Bild 8 UC-Smart Rückruf ausschliesslich zu bekannten Rufnummern

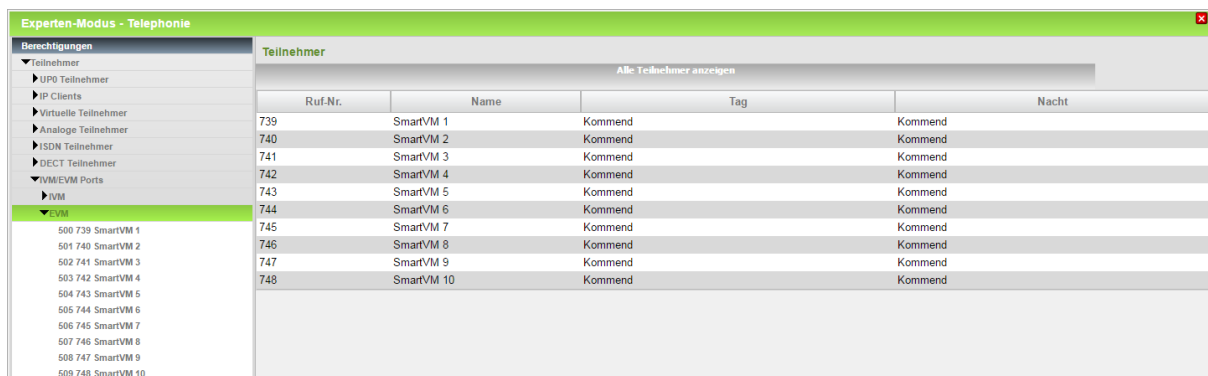
Hinweis:

Diese Möglichkeit steht auch dann zur Verfügung wenn UC-Smart nicht aktiviert wurde bzw. ein Smart Voicemail Teilnehmer keine UC-Smart Lizenz hat.

### 3.3.2.3. Einschränkung der Berechtigung für die gehende Wahl (nur OpenScape Business X)

Für die internen Ports der Smart Voicemail kann im System eine Berechtigung für die gehende Wahl vergeben werden. Nach der Erstinbetriebnahme eines Systems mit Smart Voicemail sind diese Ports nur halbamtsberechtigt.

Insbesondere bei upgedateten oder migrierten Systemen kann die Einstellung verändert worden sein. Die Berechtigungseinstellung der Voicemail Ports ist daher bei einer Übergabe eines OpenScape Business System an den Kunden zu überprüfen und ggf. zu korrigieren.



Ruf-Nr.	Name	Tag	Nacht
739	SmartVM 1	Kommend	Kommend
740	SmartVM 2	Kommend	Kommend
741	SmartVM 3	Kommend	Kommend
742	SmartVM 4	Kommend	Kommend
743	SmartVM 5	Kommend	Kommend
744	SmartVM 6	Kommend	Kommend
745	SmartVM 7	Kommend	Kommend
746	SmartVM 8	Kommend	Kommend
747	SmartVM 9	Kommend	Kommend
748	SmartVM 10	Kommend	Kommend

Bild 9 UC Smart Einschränken der Berechtigung für gehende Wahl (nur bei X Systemen)

Einige Leistungsmerkmale erfordern jedoch eine manuelle Zuweisung einer amtsberechtigten Berechtigungsgruppe:

- Absender einer Sprachnachricht anrufen
- Abhören von Sprachnachrichten durch Mobility-Teilnehmer via Rückruf
- Übergeben zu externem Ziel durch Company AutoAttendant

Eine nachträgliche Zuweisung einer Amtsberechtigung ist immer mit dem Kunden abzusprechen und zu dokumentieren.

Hinweis:

Die portbezogene Berechtigungseinschränkung für die gehende Wahl aus der Voicemail heraus, steht ausschließlich in OpenScape Business X Modellen zur Verfügung.

Bei OpenScape Business S kann dieser Mechanismus nicht verwendet werden. Hier muss die Einschränkung immer über die Definition von Rückrufzielen bzw. über die Einschränkung der Rufnummernlänge erfolgen.

### 3.3.3. Einschränken der Voicemail Erreichbarkeit von extern.

#### 3.3.3.1. Löschen der Durchwahlnummern

Die Durchwahlnummer der Smart Voicemail Gruppe ist zu löschen, wenn keine Abfrage der Voicemail von extern über das Telefon User Interface (TUI) erfolgen soll. Die nach einer Erstinbetriebnahme eingetragene Durchwahlnummern der Smart Voicemail Ports sind zu löschen. Die Durchwahlnummern werden für die normale Funktion der Smart Voicemail nicht benötigt.

#### 3.3.3.2. Änderung der Default Durchwahlnummern

Wenn Durchwahlrufnummern für die externe Erreichbarkeit der Smart Voicemail Gruppe oder Ports vergeben werden müssen, sind die Default Durchwahlrufnummern zu verändern.

### 3.3.4. Vertraulichkeit der Voicemail Durchwahlnummern gewährleisten

Die Smart Voicemail Gruppe oder Port Durchwahlnummer sollten nicht allgemein veröffentlicht werden.

### 3.3.5. Deaktivieren der Smart Voicemail Funktion.

Die Smart Voicemail Funktion ist nach der Erstinbetriebnahme im System prinzipiell aktiv.

Wenn keine Smart Voicemail oder Auto Attendant Funktion im System genutzt wird, ist die Smart Voicemail zu deaktivieren.

### 3.3.6. Sicherung des AutoAttendant

#### 3.3.6.1. Rufnummernlängenbegrenzung für gehende Verbindungen aus dem Auto Attendant

Die in den allgemeinen Parametern der Smart Voicemail eingestellten Werte für die Rufnummernlängenbegrenzung gilt auch für die AutoAttendant Nachwahl und AutoAttendant Kurzwahl

#### 3.3.6.2. Einschränkung der Berechtigung für die gehende Wahl (nur OpenScape Business X)

Für die internen Ports des AutoAttendants kann im System eine Berechtigung für die gehende Wahl vergeben werden.

Auswählen	Aktion	Rufnummer	Name	Typ
	Kurzwahl 0			
	Kurzwahl 1			
	Kurzwahl 2			
	Kurzwahl 3			
	Kurzwahl 4			
	Kurzwahl 5			
	Kurzwahl 6			
	Kurzwahl 7			
	Kurzwahl 8			
	Kurzwahl 9			
	Abwurf			

### 3.4. Maßnahmen zum Schutz der Xpressions Compact Voicemail Mailbox

Die Xpressions Compact Lösung ist im aktuellen Unify Portfolio nicht mehr verfügbar. Sie wird durch Unify nicht mehr mit Korrekturen / Updates versorgt. Aus den vorgenannten Gründen wird empfohlen Xpressions Compact durch die UC Suite Applikation zu ersetzen.

Sollte ein Kunde weiterhin den Einsatz von Xpressions Compact in OpenScape Business wünschen, so ist er auf die bestehenden Sicherheitsrisiken hinzuweisen.

Als allgemeiner Schutz gegen Gebührenbetrug mittels Xpressions Compact wird empfohlen, die von Xpressions Compact verwendeten Voicemail Ports innerhalb von OpenScape Business der Berechtigungsklasse „Halbamt“ zuzuweisen.



## 4. Gebührenbetrug mittels VoIP Endgeräte

Beim Gebührenbetrug über VoIP nutzen Angreifer die Standardisierung der Internet Protokolle aus, um externe SIP oder System Endgeräte als systeminterne Teilnehmer zu registrieren. Anschließend bauen sie von diesen Endgeräten aus Verbindungen zu beliebigen Rufnummern auf.

Die Registrierungsversuche laufen automatisiert ab, wobei die Anschlüsse von VoIP TK-Anlagen systematisch auf IP-Endgeräte hin gescannt werden. Vorrangig wird dabei nach Endgeräten ohne Authentifizierung bzw. nach Endgeräten mit Standard- oder leicht zu erratendem Passwort gesucht. Nach erfolgreicher Registrierung werden automatisiert Verbindungen zu externen Rufnummern aufgebaut.

Die erfolgreiche Registrierung eines fremden Endgeräts als interner Teilnehmer ist schwierig zu erkennen. Die Teilnehmer fallen in der Regel erst in einer Gesprächskostenabrechnung z.B. durch hohe Gesprächskosten, durch die gewählten Zielrufnummern oder durch die Anzahl der Gespräche auf.

Einige ITSP sperren den Anschluss, wenn die Kosten innerhalb eines Zeitraumes bestimmte Grenzen überschreiten. In den meisten Fällen ist aber bis zum Erkennen des Missbrauchs bereits ein großer Schaden entstanden.

Neben der Registrierung von Endgeräten über das Internet ist zu beachten, dass auch innerhalb des Kunden LAN zusätzliche Endgeräte eingebracht werden können, um nicht autorisierte Verbindungen aufzubauen.

### 4.1. Maßnahmen gegen Registrierung fremder SIP Endgeräte

#### 4.1.1. Authentifizierung des SIP Endgeräts

Bei der Einrichtung von SIP Teilnehmer in OpenScape Business ist das Flag „Authentifizierung aktiv“ zu setzen. Dieser Flag erzwingt die Authentifizierung mittels Benutzername und Passwort bei der Registrierungsanfrage von SIP Endgeräten.

Einrichtung - Wizards - Endgeräte / Teilnehmer - IP-Endgeräte	
Teilnehmer ändern	
Teilnehmer	
Vorname:	SIP
Nachname:	Teilnehmer
Anzeigen: (für den Teilnehmer):	Teilnehmer, SIP
Rufnummer:	131
Durchwahl: (Nummer zur direkten Durchwahl)	131
Mobility	
Mobile Rufnummer:	-
Web Feature ID:	Keine ▼
Parameter	
Typ	SIP Client ▼
Endgeräte Typ:	SIP Extension
Clip/Lin:	-
Stationstyp:	Standard ▼
Sprache:	Deutsch ▼
Rufsignalisierung intern: (Klang des Ruftons bei internen Anrufen):	Rufart 1 ▼
Rufsignalisierung extern: (Klang des Ruftons bei externen Anrufen):	Rufart 1 ▼
Sicherheit	
Authentifizierung aktiv:	<input checked="" type="checkbox"/>
Kennwort:	.....
Kennwort bestätigen:	.....
SIP User ID / Benutzername:	SIP-131
Realm:	SMO-SIP

Bild 10 Authentifizierung bei SIP Teilnehmern einrichten

#### 4.1.2. Nutzung eines starken individuellen Kennworts für die Authentifizierung

Für die Authentifizierung von SIP Endgeräten muss ein starkes, geräteindividuelles Kennwort vergeben werden. Das Kennwort ist ebenfalls im SIP Endgerätes einzutragen.

Hinweis:

Der Betrieb eines SIP Endgeräts ohne Authentifizierung bzw. mit trivialem bzw. default Kennwort ist grob fahrlässig.

#### 4.1.3. Vergabe einer starken SIP User ID / Benutzernamen

Für die Registrierung von SIP Endgeräten wird unter anderem eine SIP user ID verwendet. Die SIP User ID muss in der SIP Teilnehmerkonfiguration so gewählt werden, dass sie nicht leicht erraten werden kann. Sie darf auf keinem Fall nur aus der Rufnummer des Teilnehmers bestehen. Auch der vom System gewählte Default Präfix sollte kundenspezifisch geändert werden.

#### 4.1.4. Löschen von SIP Testanschlüssen

In einigen Fällen ist es erforderlich Testanschlüsse zur Einrichtung / Verwaltung von SIP Endgeräten innerhalb von OpenScape Business einzurichten. Diese Anschlüsse sind vor eine Kundenübergabe des Systems zu löschen oder falls sie bestehen bleiben müssen, mit Authentifizierung und Kennwort zu versehen.

#### 4.1.5. Löschen von nicht genutzten / überzähligen SIP Anschlüssen

Alle SIP Teilnehmer, die im System aktuell nicht benötigt werden, sind grundsätzlich zu löschen.

#### 4.1.6. Nutzung des internen SBC bei extern angeschalteten Endgeräten

Für SIP Teilnehmer, die über das Internet an OpenScape Business angeschaltet werden (SIP Device@Home), muss das Flag „Internet Registrierung mit internem SBC“ gesetzt werden.

The screenshot shows the 'Experten-Modus - Telephonie' interface. On the left, a sidebar contains a tree view with 'Teilnehmer' expanded, showing sub-items like 'UP0-Teilnehmer', 'IP Clients', 'System Clients', 'SIP Clients', and '31 131 Teilnehmer, SIP'. The main area displays the configuration for 'Teilnehmer - 31'. It has three tabs: 'Teilnehmer-Parameter ändern', 'Teilnehmer-Flags ändern', and 'Workpointclient Daten ändern'. The 'Teilnehmer-Parameter ändern' tab is active. It shows the following configuration: 'Typ: SIP Client', 'Rufnummer: 131', and 'Anzeigen: Teilnehmer, SIP'. Below this is the 'Parameter' section with the following fields: 'Authentifizierung aktiv:' (checked), 'Kennwort:' (empty), 'Kennwort bestätigen:' (empty), 'SIP User ID / Benutzername: SIP-131', 'Realm: SMO-SIP', 'Feste IP Adresse verwenden:' (unchecked), 'IP Adresse: 0.0.0.0', and 'ID des Sekundärsystems:' (empty). A red box highlights the 'Internet-Registrierung mit internem SBC:' checkbox, which is checked.

Bild 11 Externe SIP Endgeräte über SBC einrichten

Um das Flag setzen zu können ist die Aktivierung des Flags „Authentifizierung aktiv“ und eine Kennwortvergabe Voraussetzung.

Das Flag aktiviert den integrierten Session Border Controller (SBC) von Open Scape Business. Der SBC erkennt diesen Teilnehmer und blockt Registrierungsversuche von anderen externen SIP Teilnehmern über das Internet.

#### 4.1.7. Verwendung spezieller Ports für extern angeschaltete SIP Teilnehmer

Die Signalisierung einer SIP Verbindung über TCP / UDP erfolgt über den Standard Port 5060. Bei TLS gesicherten Verbindungen wird im Default der Port 5061 verwendet.

Für die Anschaltung von externen SIP Teilnehmer an OpenScape Business wird empfohlen eine UDP Verbindung über den Port 5070 und nicht den Standard Port 5060 zu verwenden. Für TLS gesicherte Anschaltung ist der Port 5062 zu verwenden.

In den SIP Endgeräten ist hierzu eine Anpassung des Ports und ggf des Protokolltyps (UDP) erforderlich. Im Company (Office) Router muss dann zusätzlich ein Port Forwarding von extern 5070 auf intern 5060 (nur UDP) einzurichten. Für eine TLS gesicherte Verbindung ist der externe Port 5062 auf den internen Port 5062 zu routen. (Hinweis: Diese Angabe ist richtig, da 5061 im System anderweitig genutzt wird).

## 4.2. Maßnahmen gegen Registrierung fremder System (HFA) Endgeräte

### 4.2.1. Authentifizierung des System (HFA) Endgeräts

Bei der Einrichtung von System (HFA) Teilnehmer in OpenScape Business ist das Flag „Authentifizierung aktiv“ zu setzen. Dieser Flag erzwingt die Authentifizierung mittels eines Passwortes bei der Registrierungsanfrage von HFA Endgeräten und verhindert, dass sich fremde Endgeräte über LAN oder Internet einfach an OpenScape Business registrieren können.

The screenshot displays the 'Expert mode - Telephony Server' configuration window. On the left is a navigation tree with categories like Station, IP Clients, Analog Stations, and DDI Extensions. The 'Station' section is expanded, showing 'Station - 46'. The main area contains configuration options for this station. Under the 'Parameter' tab, several settings are visible: 'Status message' (unchecked), 'Authentication active' (checked), 'New password' (masked with dots), 'Confirm password' (masked with dots), 'Blocked for Deskshare User' (unchecked), 'Secondary system ID' (empty field), and 'Internet Registration with internal SBC' (checked). Red boxes highlight the 'Authentication active' checkbox, the password fields, and the 'Internet Registration with internal SBC' checkbox.

Bild 12 Externes SystemEndgeräte mit Authentifizierung einrichten

### 4.2.2. Nutzung eines starken individuellen Kennworts für die Authentifizierung

Für die Authentifizierung von System (HFA) Endgeräten muss ein starkes, geräteindividuelles Kennwort vergeben werden, dieses erhöht die Sicherheit gegen ein Erraten des Kennwortes.

Hinweis:

Das Kennwort ist sowohl in der System Konfiguration als auch im System (HFA) Endgeräte einzutragen.

### 4.2.3. Löschen von System (HFA) Testanschlüssen

In einigen Fällen ist es erforderlich Testanschlüsse zur Einrichtung / Verwaltung von System (HFA) Endgeräten innerhalb von OpenScape Business einzurichten.

Diese Anschlüsse sind vor eine Kundenübergabe des Systems zu löschen oder falls sie bestehen bleiben müssen, mit Authentifizierung und Kennwort zu versehen.

### 4.2.4. Löschen von nicht genutzten / überzähligen System (HFA) Anschlüssen

Alle System (HFA) Teilnehmer, die im System aktuell nicht benötigt werden, sind grundsätzlich zu löschen.

### 4.2.5. Nutzung des internen SBC bei extern angeschalteten Endgeräten

Für System (HFA) Teilnehmer, die über das Internet an OpenScape Business angeschaltet werden (Leistungsmerkmal: System Device@Home), muss das Flag „Internet Registrierung mit internem SBC“ gesetzt werden.

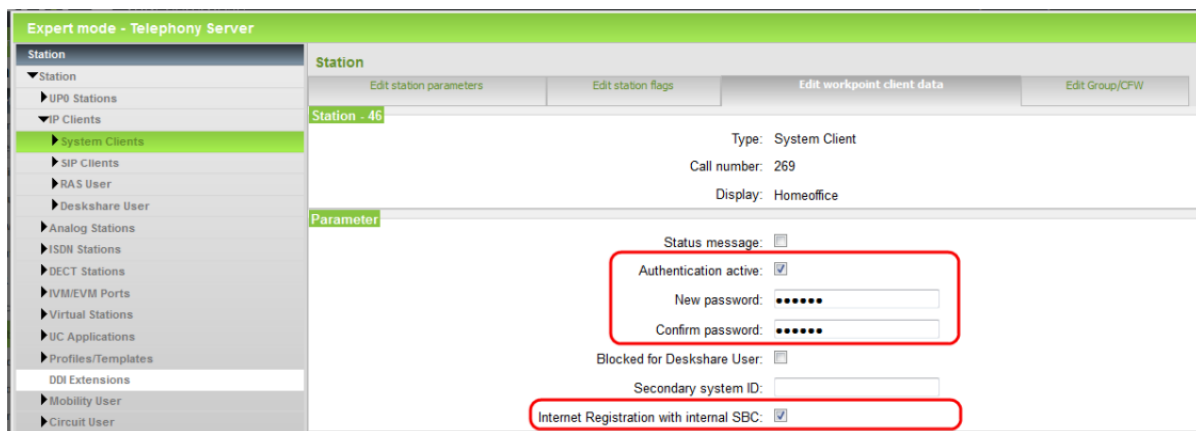


Bild 13 SBC für externes SystemEndgerät einrichten

Um das Flag setzen zu können ist die Aktivierung des Flags „Authentifizierung aktiv“ und eine Kennwortvergabe Voraussetzung.

Das Flag aktiviert den integrierten Session Border Controller (SBC) von Open Scape Business. Mit der Aktivierung werden die Ports 4062 und 4063 für die Kommunikation mit externen System (HFA) Teilnehmern verwendet. Durch die Verwendung unterschiedlicher Ports kann der integrierte SBC externe Teilnehmer von internen System (HFA) Teilnehmer unterscheiden und nicht authentifizierte Registrierungen blocken.

#### 4.2.6. Port Forwarding für extern angeschaltete System (HFA) Teilnehmer einrichten.

Für den Verbindungsaufbau zu externen System (HFA) Teilnehmern werden die Ports 4062 bzw. 4063 bei TLS Verschlüsselung verwendet.

Damit die von den externen System (HFA) Endgeräten verwendeten Standardports in den Endgeräten nicht verändert werden müssen, ist im Company (Office) Router ein Port Forwarding vom externen Port 4060 auf den internen Port 4062 (TCP / UDP) für normale Verbindungen, sowie vom externen Port 4061 auf den internen Ports 4063 bei TLS verschlüsselten Verbindungen einzurichten.

# 5. Gebührenbetrug mittels DISA Port

OpenScape Business bietet einen DISA Port zur Realisierung verschiedener Mobility Leistungsmerkmale innerhalb von OpenScape Business. Die Funktion kann innerhalb von OpenScape Business über zwei unterschiedliche Signalisierungswege angesprochen werden.

- **Signalisierung über DTMF Steuerung**  
Hierbei wird die Steuerung mittels DTMF Tönen im Sprachkanal durchgeführt.  
Externe Teilnehmer wählen sich über den DISA Port in das System ein und führen von ihrem Endgerät durch die Eingabe von Feature Codes assoziierten Dienste im System aus. Durch die Eingabe von Rufnummern werden über das System auch Verbindungen zu internen oder externen Verbindungen aufgebaut.  
Bevor das System die Ausführung von Diensten über den DISA Port erlaubt, muss sich der externe Teilnehmer über die DISA PIN authentifizieren. Die Prüfung auf die DISA Pin erfolgt entweder nach einem Timeout oder nach der Eingabe von „#“.  
Hinweis:  
Die Prüfung der DISA PIN wird übersprungen, wenn die Rufnummer des rufenden externen Teilnehmers innerhalb des Systems einem Mobility Teilnehmer zugeordnet ist.
- **Signalisierung über das Web Services Interface (nur bei myPortal to Go)**  
Hierbei wird die Information zu Steuerung des Ports mittels HTTP(S) im Datenkanal übertragen.

## 5.1. Angriffe auf den DISA Port

Angriffe auf DISA Ports erfolgen prinzipiell in der gleichen Art und Weise wie Angriffe auf Voicemail Ports durch automatisches Anrufen der DISA Rufnummer und durch ausprobieren von PIN Kombinationen. Bei positiver Quittung baut der Angreifer dann entweder direkt Verbindungen zu externen Zielen auf oder programmiert weitere Anrufumleitungen im System um noch zusätzliche Verbindungen zu externen Zielen aufbauen zu können.

DISA Port Angriffe werden dem Angreifer erleichtert, wenn er Kenntnis über die DISA Port Rufnummer und ggf. auch über die dem DISA Port intern zugeordneten Teilnehmer erlangt.

Stark erleichtert wird es dem Angreifer, wenn er Zugriff auf das Mobiltelefon eines im System registrierten Mobilteilnehmers erlangt hat.

## 5.2. Maßnahmen gegen Angriffe auf den DISA Port bei OpenScape Business

### 5.2.1. Sperren bzw. keine Freigabe des DISA Ports

Wird in der Systemkonfiguration (Grundeinstellungen → System → DISA) keine DISA Rufnummer eingetragen bzw. wird diese gelöscht ist der DISA Port gesperrt.

The screenshot shows the 'Experten-Modus - Telephonie' configuration window. On the left is a sidebar with 'Grundeinstellungen' expanded, showing a tree view with 'System' selected. The main area is titled 'DISA' and contains several sections: 'DISA' with a 'Disa ändern' button, 'DISA intern' with a 'Durchwahl:' field containing '33397' and a 'Sicherheits Modus:' dropdown set to 'Nach Zeit', and 'Mobility callback' with a 'Rufnummer:' field containing '94481' and a 'Durchwahl:' field.

Bild 14 Freigabe des DISA Ports

### 5.2.2. Restriktiver Umgang mit den Teilnehmer Flag „DISA Berechtigung

Das Flag „DISA Berechtigung“ darf nur für die Teilnehmern gesetzt sein, die auch für die Ausführung der DISA-Funktionen vorgesehen sind. Das Flag ist bei Erstinbetriebnahme nicht gesetzt. Bei Migrationen / Ugrades ist es zu überprüfen.

**Experten-Modus - Telephonie**

**Teilnehmer**

- ▼ Teilnehmer
  - ▶ UP0-Teilnehmer
  - ▼ IP Clients
    - ▶ System Clients
    - ▶ SIP Clients
    - ▶ RAS User
    - ▶ Deskshare User
    - ▶ Analoge Teilnehmer
    - ▶ ISDN Teilnehmer
    - ▶ DECT-Teilnehmer
    - ▶ IVM/EVM Ports
    - ▶ Virtuelle Teilnehmer
    - ▶ UC Applications
    - ▶ Profile/Vorlagen
    - Durchwahl Rufnummern
    - ▶ Mobility Teilnehmer
    - ▶ Circuit Teilnehmer
    - ▶ Teilnehmerübersicht
    - ▶ Tastenprogrammierung

**Teilnehmer - 156**

Typ: System Client  
Rufnummer: 33388  
Anzeigen: User 33388

**Teilnehmer-Flags**

- Auswahlberechtigung ein: ☐
- Anrufschutz durchbrechen: ☐
- AUL extern erlaubt: ☒
- Direktansprecherschutz aus: ☒
- Disa Berechtigung: ☐**
- Transit schalten durch Auflegen: ☐
- Codeschloss zurücksetzen: ☐
- Zugriff für Fangen: ☐
- Eintrag in Telefonbuch: ☒
- Editieren der Wahl: ☐
- Keine Rufzusaltung bei besetzt: ☐
- Call Supervisor: ☐
- Assoziierte Wahl/Dienste: ☒**
- Anklopfschutz ein: ☐

Bild 15 Sperren DISA Berechtigung für Teilnehmer

Hinweise:

Mobility Teilnehmer benötigen keine DISA-Berechtigung zur Ausführung obiger Leistungsmerkmale.

Das Flag assoziierte Wahl Dienste beeinflusst die DISA Funktionalität nicht wenn für den Teilnehmer das Flag „DISA Berechtigung“ gesetzt ist

### 5.2.3. Ändern der Telefonschloss PIN für die „DISA Berechtigung“ Teilnehmer.

Die Telefonschloss PIN der „DISA berechtigten“ Teilnehmer muss von Standardwert „00000“ in eine „starke“ PIN geändert werden. Wenn den „DISA berechtigten“ Teilnehmern physikalische Endgeräten zugewiesen sind ist das Personal entsprechend einzuweisen.

Hinweis:

Die Authentifizierung mittels DISA PIN und die Abfrage des Flag „DISA Berechtigung“ entfällt, wenn eine, einem Mobility Teilnehmer zugeordnete Rufnummer, von extern auf die DISA-Durchwahlnummer anruft.

#### 5.2.4. Sperren der DISA-Freigabe für Leitungen

Für jede ISDN oder VoIP Leitung ist für DISA Tag/Nacht der Eintrag „kein“ in den Leitungsparametern einzustellen, um die Leitung für die Benutzung von DISA zu sperren. Bei Erstinbetriebnahme ist der Wert auf „kein“ gesetzt. Bei Upgrade / Migration ist der Wert zu prüfen und ggf. anzupassen.

The screenshot shows the 'Experten-Modus - Telephonie' interface. On the left, a tree view under 'Leitungen/Vernetzung' shows the selection path: 'Leitungen' > 'STMD3' > 'Box: 2, Slot: 15' > 'Port 1 No Port' > '15-1-71'. The main area is titled 'Leitungen' and 'Leitung ändern'. It displays the following configuration for 'Leitung: 71':

- Box/Slot/Port/Leitung: STMD3 2-15-1-1
- Kennzahl: (empty field)
- Richtung: keine (dropdown)
- Rufzuordnung Leitung: (empty field)
- Tag Ruf-Nr.: 94000 Master SAPP (dropdown)
- Nacht Ruf-Nr.: 94000 Master SAPP (dropdown)
- DISA Tag/Nacht: Kein (dropdown, highlighted with a red box)**
- CMI flags:**
  - Echokompensationsglied: ☐
  - Echounterdrückung: ☒
  - Künstliches Echo: ☒
- Circuit-Flags:**
  - Anrufpriorität/Sofortton Anklopfen: ☐

Bild 16 Sperren DISA Berechtigung für Leitungen

#### 5.2.5. Restriktiver Umgang mit der Publizierung des DISA Ports und DISA PIN

Informationen über die DISA Port Nummer und den zugordneten „DISA Teilnehmer“ und DISA PIN sind nur den Personen mitzuteilen, die den DISA Port nutzen sollen. Keine Veröffentlichung des DISA Ports z.B. in internen Telefonbüchern etc.

#### 5.2.6. Sicherung des mobilen Telefon vor Fremdzugriff

Mobiltelefone, die mobilen Teilnehmer im System zugewiesen sind, müssen mit geeigneten Mitteln gegen Fremdzugriff bzw. ausspähen von Daten geschützt werden um die DISA Port Einwahlp Parameter und ggf. die UC user Login Parameter geheimzuhalten.



## Abbildungsverzeichnis

Bild 1	UC-Suite: Länge Voicemail Mailbox PIN Länge .....	9
Bild 2	UC-Suite: Einschränken der Rückrufoption .....	9
Bild 3	UC-Suite: "Bekannte" Rufnummern .....	9
Bild 4	UC Suite: Erzwingen der PIN Abfrage .....	10
Bild 5	UC-Suite: Definition der PIN Policy .....	10
Bild 6	UC-Suite: Einschränken der Berechtigung für UC-Anrufe .....	11
Bild 7	UC-Smart Einschränkung von Rückrufen .....	13
Bild 8	UC-Smart Rückruf ausschliesslich zu bekannten Rufnummern .....	13
Bild 9	UC Smart Einschränken der Berechtigung für gegenseitige Wahl (nur bei X Systemen) .....	14
Bild 10	Authentifizierung bei SIP Teilnehmern einrichten .....	18
Bild 11	Externe SIP Endgeräte über SBC einrichten .....	19
Bild 12	Externes SystemEndgeräte mit Authentifizierung einrichten .....	20
Bild 13	SBC für externes SystemEndgerät einrichten .....	21
Bild 14	Freigabe des DISA Ports .....	23
Bild 15	Sperrung DISA Berechtigung für Teilnehmer .....	23
Bild 16	Sperrung DISA Berechtigung für Leitungen .....	24

