OpenScape Business

Tutorial

Measures against Toll Fraud

Version 1.0

About this Document

The descriptions in this document refer to OpenScape Business V2R2.

Disclaimer & Copyright

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of the contract. Availability and technical specifications are subject to change without notice.

Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

Document History

Date	Version	Changes / Remarks
2017-02-27	1.0	Initial creation

Table of Contents

1. Preface

The creation of hybrid systems through the combination of classical PBX systems with Voice over IP has also added to the specific security risks of the technologies used.

Many books, documents, guides and checklists address the threats and security issues in the TC / IT environment. Many of them show the basic threats and the countermeasures, but without any details about the actual systems and their settings.

For OpenScape Business, the security checklist describes all potential threats and the corresponding countermeasures for minimizing the risk. The checklist can be downloaded from the Unify Partner Portal. Only the consistent application of all the measures listed in the security checklist can optimally protect an OpenScape Business System and prevent damage to the operator.

Despite the availability of the security checklist, many OpenScape Business Systems are still not protected against attacks. Even a single successful attack can lead to a huge financial loss for the operator.

This document shows potential points of attack for toll-fraud as well as concrete countermeasures. It is intended to sensitize the operator and the administrator of the system to the issue and to allow the system to be specifically protected against fraud attempts.

The document does not replace the application of the security checklist.

2. Introduction

This document briefly presents the most frequently occurring attack scenarios for toll-fraud and the recommended countermeasures.

The use of standardized communication protocols allows attackers to execute attacks with corresponding SW tools without extensive knowledge of the system itself and to inflict damage if the interfaces are not adequately protected.

The use of communication software (SW) such as smartphones, unified communications or CTI clients on standard PCs, tablets or smartphone platforms provides access to internal system services such as voicemail or UC servers and thus makes it easier for attackers to take action when devices and communication SW are not sufficiently secured.

Access to unsecured system services such as voicemail or DISA ports or unlocked publicly-accessible telephones facilitates attacks and the unauthorized use of system features.

2.1. Toll Fraud Scenarios

Toll-fraud attacks are mostly performed on weekends when no one is in the company. Criminal hackers gain access via the telephone network or, depending on which telephone technology is used, also over the Internet. After successfully breaking into the telecommunications system (TC system) of the company, many short connections, e.g., to value-added service numbers, are established.

Too often, the perpetrators can cash in and hide behind short-lived PO Box companies in different parts of the world.

In most cases, toll-fraud occurs through call diversions, e.g., via:

- Access to insufficiently secured voice and AutoAttendant mailboxes
- Insufficiently secure phones and system interfaces
- Access to insufficiently secure DISA ports

2.2. General Protective Measures

In principle, only those subscribers, features and interfaces that are actually required by the operator of OpenScape Business should be enabled by the system administrator.

- Only the required number of subscribers must be set up in the system.
- Test subscribers, etc., must be removed from the system before handing it over to the operator.
- The authorizations for the use of features must be restricted individually to the required extent.
- The permissions for system subscribers, such as voicemail or DISA ports, etc., must be restricted to the required extent.
- Users must specifically change the default passwords for all the individual services such as voicemail, UC Client, etc., that they use and even for the telephone devices.
- Access to the system administration must be technically secured, and the factory default access data must be customized.
- The persons with access rights to the system administration must be restricted and named.
- Administration software must not remain on an unsecured PC.
- The first and second system device (in the configuration) must be secured physically and logically against unauthorized access.
- Remote access should only be set up or released when required.

- Remote access must be specially protected against unauthorized access using external security measures if required.

For newly delivered OpenScape Business systems with software versions greater than V2R2, only those interfaces which are required for the initial setup are open after the initial commissioning.

In the case of a SW upgrade from previous SW versions or a migration from HiPath 3000 to OpenScape Business, the existing system configuration and interface settings are retained. After any such upgrade or migration, these systems must be checked again for open interfaces and any possibly active default passwords and then secured if required

3. Toll Fraud via Voicemail and AutoAttendant Mailboxes

Voice and AutoAttendant mailboxes provide the ability to route calls to specific destinations from the mailbox. The forwarding destinations are configured by the user via the administration menu of the mailbox by entering DTMF characters. The call to the configuration menu is protected by an individual PIN. Depending on the Voicemail / AutoAttendant software used, the mailboxes are protected after the initial setup by a default PIN which is common to all users and should be changed by the user. Some systems force the user to change the PIN before the first use or when setting up the mailbox for the first time.

3.1. Attacks on Voice AutoAttendant Mailboxes

Attacks are particularly easy to launch if a voicemail box is enabled for outbound calls and the factory default password for voicemail boxes (e.g., "0000") was not changed or was changed to some easily guessed variant (such as "1234", for example).

This is exactly what many attackers look for when conducting large numbers of short test calls in the evenings or nights with their automated hacking software. Using the random principle, whole number blocks of companies are scanned for vulnerabilities. If the software is not blocked by a password or overcomes a hurdle that is too weak, the attack can begin immediately. However, in order to exploit the vulnerability to the maximum level, the attack often occurs only from the following Friday evening until Monday morning.

3.2. Measures to Protect the UC Suite Voicemail Box

In the UC Suite voicemail box, the attackers try to access the voicemail box via a telephone call and to enter the configuration menu of the mailbox by entering "#". If the access attempt succeeds, the attackers then try to manipulate and exploit the call or the callback destinations.

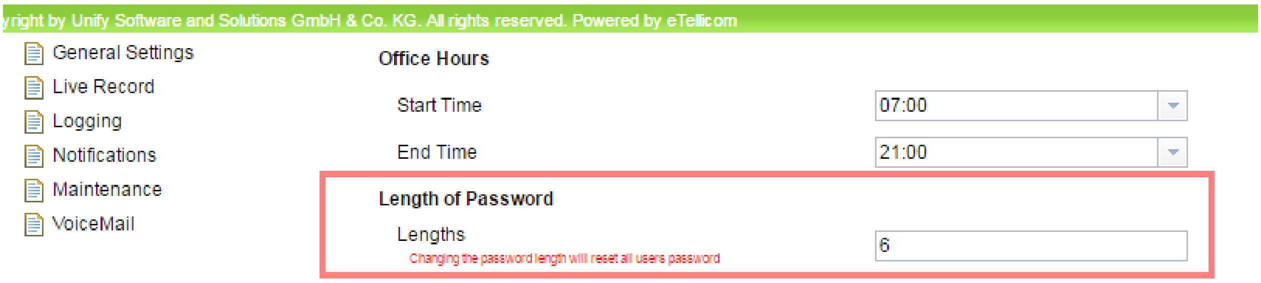
The configuration of the UC Suite Voicemail via the telephone interface (TUI) is protected by querying the subscriber number and the associated PIN. However, a UC Suite myPortal user can remove these protection measures to facilitate the voicemail query from "known phone numbers". Known call numbers are numbers entered by the UC Suite user in his or her myPortal client under the item "Personal data". In this context, it should be noted that attackers are able to fake the calling party number and spoof the UC Suite Voicemail with a “known” call number.

A general protection measure of the UC Suite Voicemail is to block access to the VM query / configuration and to disconnect the voicemail box when an invalid PIN is repeatedly entered. The block also affects the UC client of the user and can only be released by the system administrator.

In order to optimally protect the UC Suite voicemail box against attackers, the following measures must be taken, and the voicemail users must be instructed accordingly.

3.2.1. Setting the PIN length to at least 6 characters

The system administrator must set the length of the PIN to at least 6 characters in the UC Suite configuration. The higher the number of PIN characters, the better the protection.


yright by Unify Software and Solutions GmbH & Co. KG. All rights reserved. Powered by eTellicom
General Settings
Live Record
Logging
Notifications
Maintenance
VoiceMail

Office Hours

Start Time: 07:00

End Time: 21:00

Length of Password

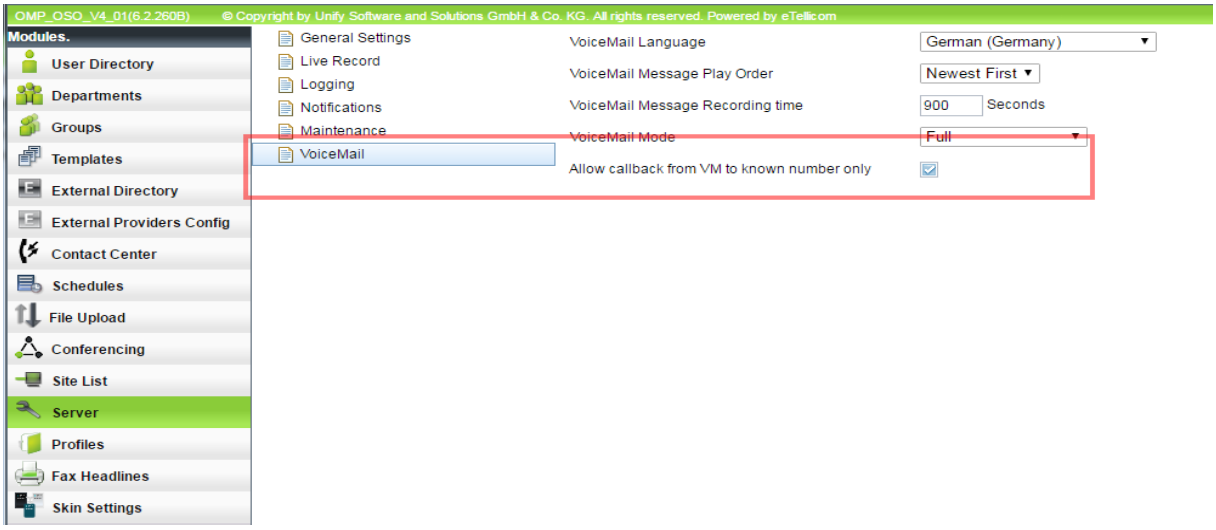
Lengths: 6

Changing the password length will reset all users password

Figure 1 UC-Suite: Configuring the PIN length of the voicemail box

3.2.2. Restricting callbacks from the voicemail box

The system administrator must specify in the system settings of the UC Suite that the voicemail box should allow callbacks to the caller only when the query call is made from a "known number".



VoiceMail Language: German (Germany)

VoiceMail Message Play Order: Newest First

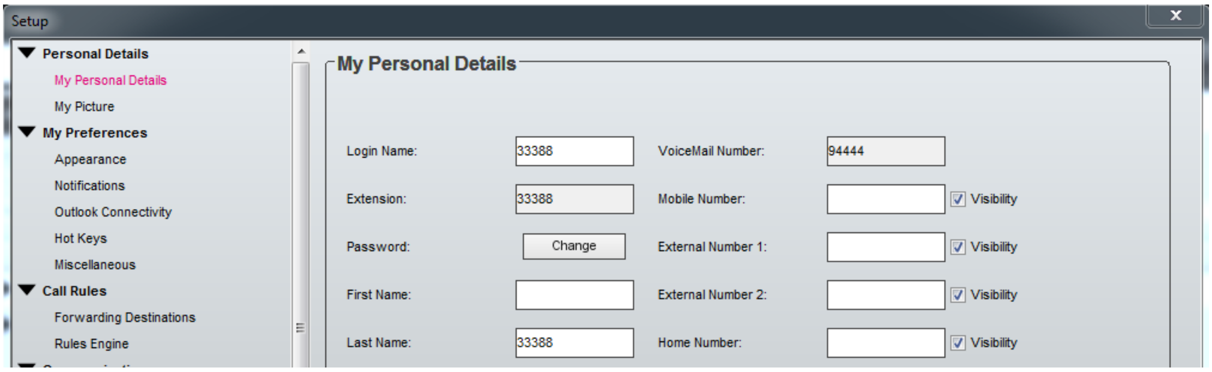
VoiceMail Message Recording time: 900 Seconds

VoiceMail Mode: Full

Allow callback from VM to known number only ☑

Figure 2 UC-Suite: Restricting the callback option

The UC-Suite user must be reminded that the call numbers in his or her personal data are regarded as a "known" numbers.



My Personal Details

Login Name:	33388	VoiceMail Number:	94444	
Extension:	33388	Mobile Number:		☑ Visibility
Password:	Change	External Number 1:		☑ Visibility
First Name:		External Number 2:		☑ Visibility
Last Name:	33388	Home Number:		☑ Visibility

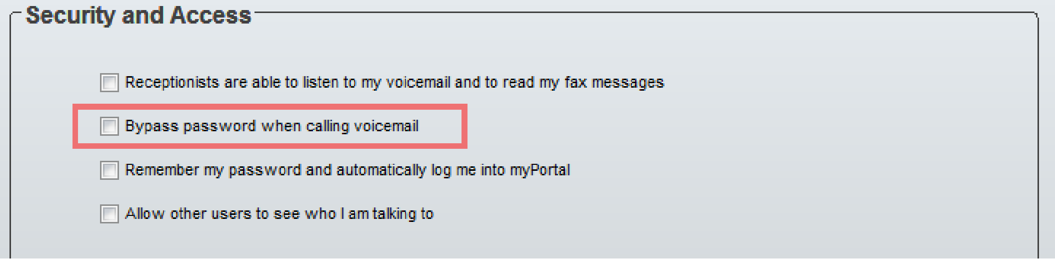
Figure 3UC-Suite: “Known” numbers

3.2.3. Assigning an individual PIN for voicemail box access

UC Suite uses a common PIN for accessing the voicemail box and for the UC Suite clients. When accessing the voicemail or the UC client for the first time, the user must change the default PIN "1234" assigned in the system. Users must be advised that they are required to use an individual "strong" PIN, which must not be divulged to third parties. For security reasons , strings of contiguous digits (e.g., 234567), repeated digits (e.g., 111111), or the extension number must not be used as a PIN.

3.2.4. Enforcing the PIN query

In the personal settings of the UC Client, the check box to "bypass the password" must not be set by the user. Otherwise, the PIN will not be requested on accessing the voicemail box from a "known number".



Security and Access

□ Receptionists are able to listen to my voicemail and to read my fax messages

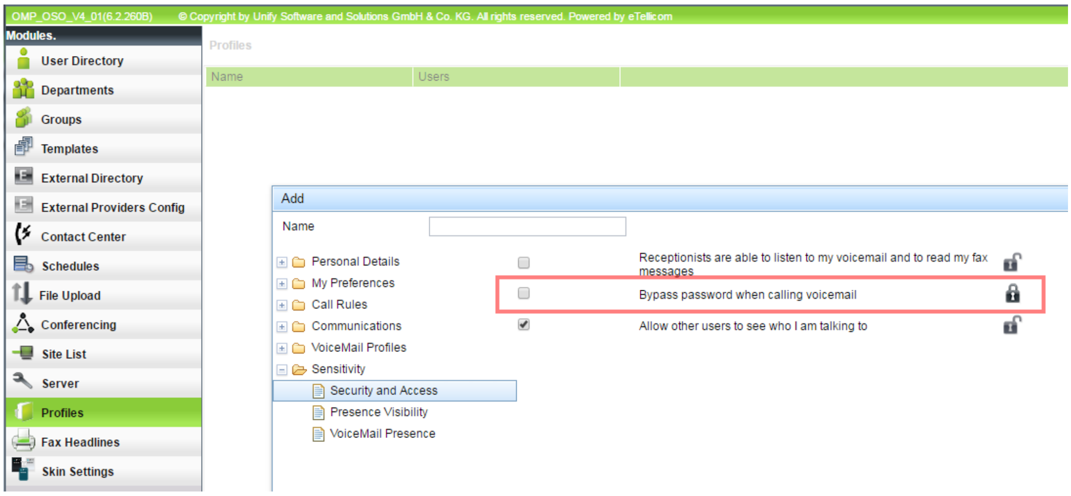
□ Bypass password when calling voicemail

□ Remember my password and automatically log me into myPortal

□ Allow other users to see who I am talking to

Figure 4 UC Suite: Enforcing the PIN query

This parameter can be assigned by the UC Suite Administrator to the UC Suite users via a policy in the UC Suite Server settings.



OMP_OSO_V4_01(6.2.260B) © Copyright by Unify Software and Solutions GmbH & Co. KG. All rights reserved. Powered by eTellicom

□ Receptionists are able to listen to my voicemail and to read my fax messages

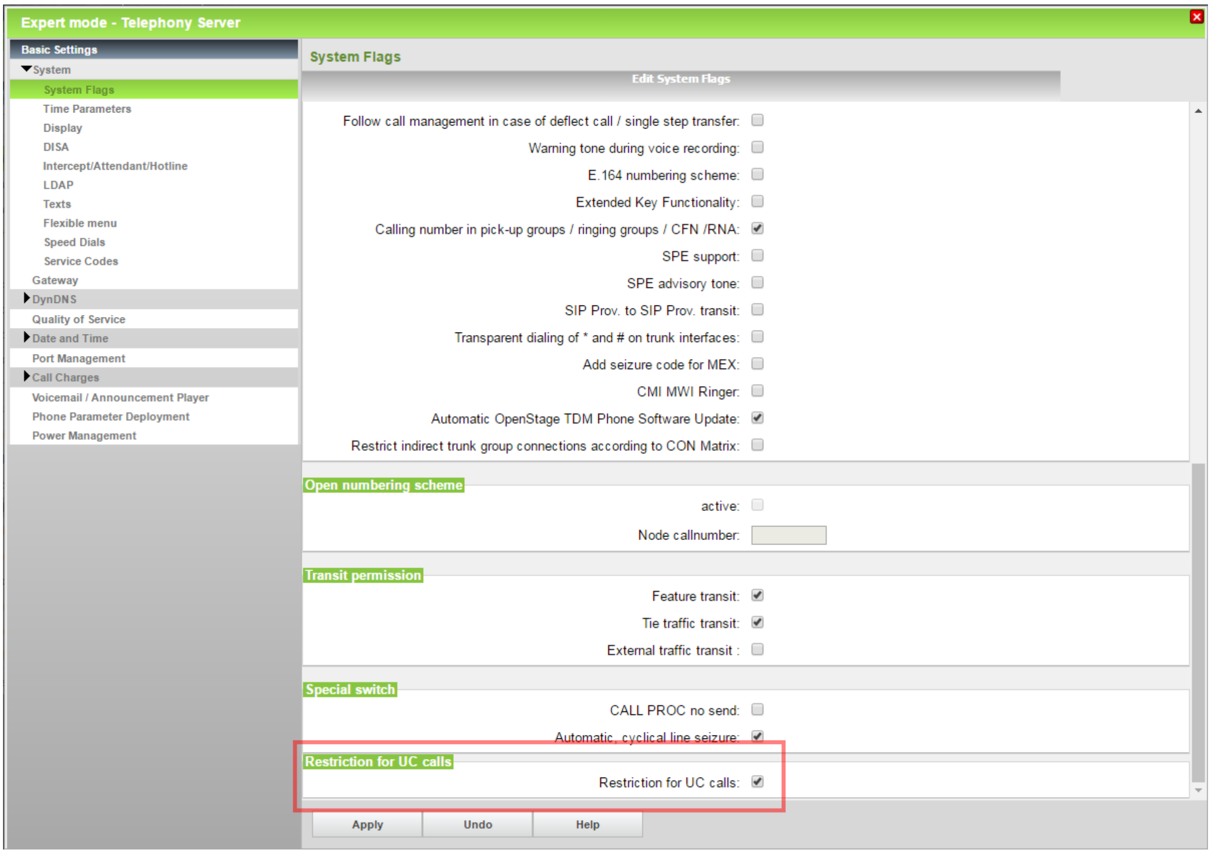
□ Bypass password when calling voicemail

☑ Allow other users to see who I am talking to

Figure 5 UC Suite: Defining the PIN policy

3.2.5. Restricting authorization for calls from the UC Suite voicemail

Via the system flag "Restrictions for UC calls", all calls initiated by the UC Suite application are checked before dialing to ensure that the corresponding UC user has the authorization for that call. This ensures that no higher-privileged calls can be routed from the voicemail box of a UC user than those that may be made by the UC user himself.



System Flags

Edit System Flags

Follow call management in case of deflect call / single step transfer: □
Warning tone during voice recording: □
E.164 numbering scheme: □
Extended Key Functionality: □
Calling number in pick-up groups / ringing groups / CFN /RNA: ☑
SPE support: □
SPE advisory tone: □
SIP Prov. to SIP Prov. transit: □
Transparent dialing of * and # on trunk interfaces: □
Add seizure code for MEX: □
CMI MWI Ringer: □
Automatic OpenStage TDM Phone Software Update: ☑
Restrict indirect trunk group connections according to CON Matrix: □

Open numbering scheme

active: □
Node callnumber:

Transit permission

Feature transit: ☑
Tie traffic transit: ☑
External traffic transit : □

Special switch

CALL PROC no send: □
Automatic, cyclical line seizure: ☑

Restriction for UC calls

Restriction for UC calls: ☑

Figure 6 UC Suite: Restricting the authorization for UC calls

3.3. Measures for Protecting the UC-Smart Voicemail Box

In the case of the UC Smart voicemail box, attackers may try to access the voicemail box via a telephone call and enter the configuration menu of the mailbox by entering a "#" to interrupt the prompt, followed by the mailbox number and PIN. If the access attempt succeeds, the attackers then try to manipulate and exploit the callback destination.

A general protection measure of the UC Smart Voicemail is that after the repeated input of an invalid PIN, access to the VM query / configuration is blocked, and the connection is disconnected. The lock can then only be released by the system administrator.

For the UC Smart Voicemail, please note that the behavior of the voicemail ports is different in OpenScape Business X and OpenScape Business S models and that some of the above measures against abuse are only available for use with the OpenScape Business X models. The differences are indicated explicitly in the text that follows.

3.3.1. Assigning a "strong" individual PIN

When setting up a voicemail box for the first time, the voicemail user is asked by the system to change his or her default PIN for the voicemail administration/query. OpenScape Business System supports the following PIN handling:

- The initial login must be made via the user's internal extension.
- The default PIN number of the mailboxes is "123456".
- The PIN length is set to 6digits.
- The following combinations are blocked by the system:
    - Strings of consecutive numbers (e.g., 234567)
    - More than 3 identical contiguous digits (e.g., 111111).

In addition, the voicemail user must also be instructed to use a "strong" individual PIN for access. It should be noted that:

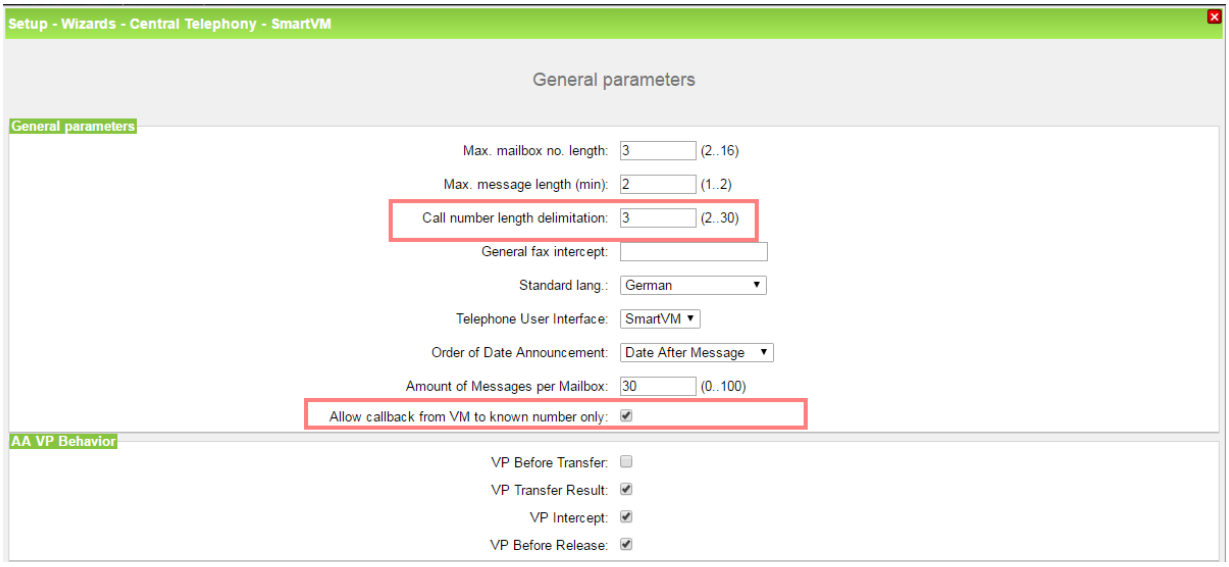
- The own extension number, even reversed, should not be part of the PIN
- No PINs that have already been used by other users should be used.
- The PIN should be changed at regular intervals.

3.3.2. Restricting callback calls from the voicemail box

3.3.2.1. Limiting the call number length for outgoing connections

In the case of outgoing connections initiated by the Smart Voicemail, only numbers up to the specified length can be dialed. For longer call numbers, the connection setup fails. By default, the call number length limitation corresponds to the mailbox number length (internal call number length), so that only internal dialing is allowed. This limitation also applies to the numbers of AutoAttendant suffix dialing and AutoAttendant speed dialing.

The setting is made in the general parameters of the Smart Voicemail



Setup - Wizards - Central Telephony - SmartVM

General parameters

General parameters

Max. mailbox no. length:	3 (2..16)
Max. message length (min):	2 (1..2)
Call number length delimitation:	3 (2..30)
General fax intercept:	
Standard lang.:	German ▾
Telephone User Interface:	SmartVM ▾
Order of Date Announcement:	Date After Message ▾
Amount of Messages per Mailbox:	30 (0..100)
Allow callback from VM to known number only:	☑

AA VP Behavior

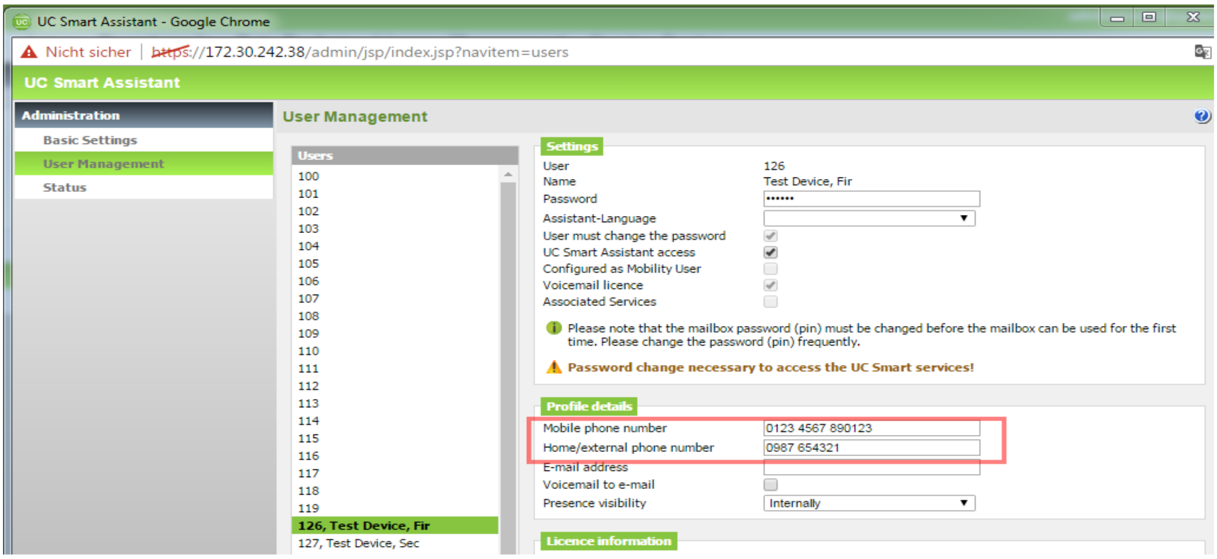
VP Before Transfer:	□
VP Transfer Result:	☑
VP Intercept:	☑
VP Before Release:	☑

Figure 7 UC Smart: Restricting the call number length for callback calls

3.3.2.2. Callbacks to known phone numbers only

Callbacks from the voicemail box can be restricted to known previously configured mobile or fixed network call numbers. The setting for this is also made in the general parameters of the Smart Voicemail.
If the flag "**Allow callback from VM to known number only**" is set, only callbacks to previously configured numbers can be made from the Smart Voicemail Box.

These numbers must be configured within OpenScape Business on a user-specific basis via the UC Smart Assistant (Setup → UC Smart → UC Smart).



UC Smart Assistant - Google Chrome
Nicht sicher | ~~https~~://172.30.242.38/admin/jsp/index.jsp?navitem=users
UC Smart Assistant
Administration
Basic Settings
User Management
Status

User Management

Users: 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

Settings

User	126
Name	Test Device, Fir
Password	••••••
Assistant-Language	▾
User must change the password	☑
UC Smart Assistant access	☑
Configured as Mobility User	□
Voicemail licence	☑
Associated Services	□

Please note that the mailbox password (pin) must be changed before the mailbox can be used for the first time. Please change the password (pin) frequently.

Password change necessary to access the UC Smart services!

Profile details

Mobile phone number	0123 4567 890123
Home/external phone number	0987 654321
E-mail address	
Voicemail to e-mail	□
Presence visibility	Internally ▾

Licence information

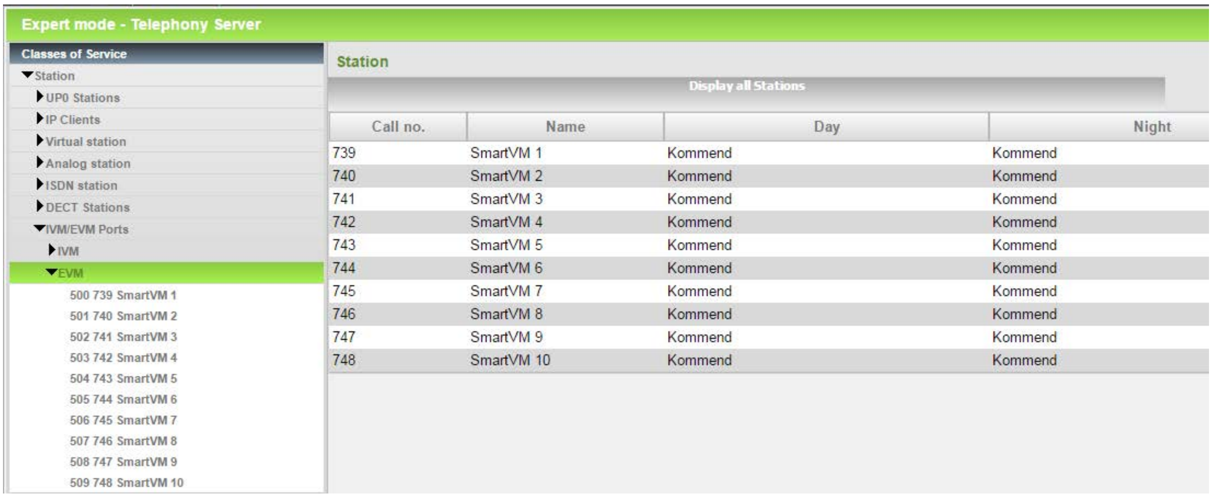
Figure 8 UC Smart: Restricting callbacks to known phone numbers only

Note:
This option is also available if UC Smart is not activated or if a Smart Voicemail user does not have a UC Smart license.

3.3.2.3. Restricting the class of service for outbound dialing (OpenScape Business X only)

A Class of Service (authorization) for outbound dialing can be assigned within the system for the Smart Voicemail internal ports. Following the initial startup of a system with Smart Voicemail, these ports are set to "outward restricted trunk access" (internal calls only).

This setting may have been modified, especially for updated or migrated systems. The Class of Service setting of the voicemail ports must therefore be checked and possibly corrected before an OpenScape Business system is handed over to the customer.



Call no.	Name	Day	Night
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

Figure 9 UC Smart: Restricting the class of service for outbound dialing (for X models only)

However, some features require a manual assignment of an unrestricted class of service (with direct trunk access). For example:

- Calling the sender of a voicemail
- Listening to voicemails by Mobility subscribers via callbacks
- Transfers to external destinations by the Company AutoAttendant

The subsequent assignment of an unrestricted Class of Service must always be discussed with the customer and properly documented.

Note:

The port-related COS restriction for outbound dialing from within the voicemail system is only available in OpenScape Business X models.

With OpenScape Business S, this mechanism cannot be used. Here, the restriction must always be made via the definition of callback destinations or the restriction of the call number length.

3.3.3. Restricting external voicemail accessibility

3.3.3.1. Deleting direct inward dialing numbers

The direct inward dialing (DID) number of the Smart Voicemail group should be deleted if no checking of the voicemail is required from an external location via the telephone user interface (TUI). The direct inward dialing numbers of the Smart Voicemail ports entered after an initial system setup must be deleted. They are not required for the normal operation of the Smart Voicemail.

3.3.3.2. Changing the default direct inward dialing numbers

If direct inward dialing numbers need to be assigned for external access to the Smart Voicemail group or ports, the default DID numbers must be changed.

3.3.4. Ensuring the confidentiality of the voicemail DID numbers

The Smart Voicemail group or port DID number should not be publicly disclosed.

3.3.5. Disabling the Smart Voicemail feature

The Smart Voicemail functionality is basically active in the system after the initial setup. If no Smart Voicemail or AutoAttendant function is used in the system, the Smart Voicemail must be disabled..

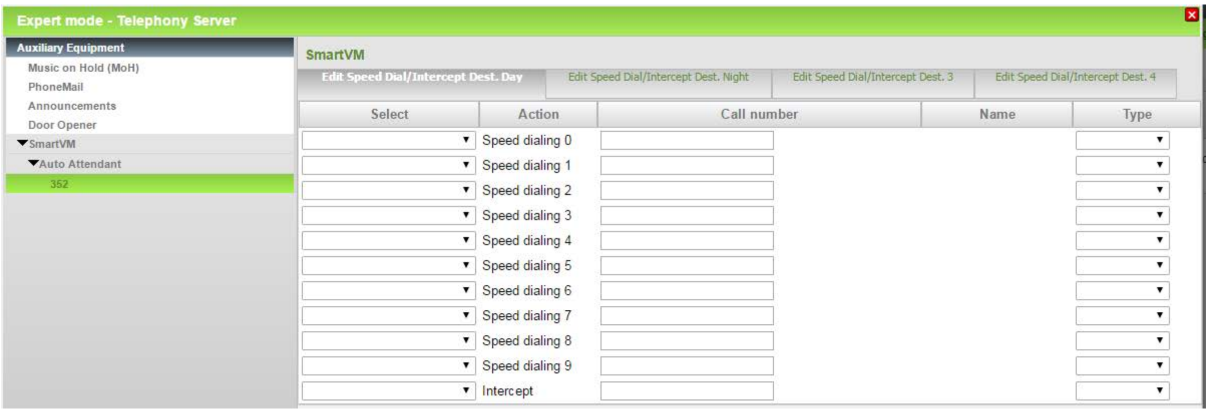
3.3.6. Securing the AutoAttendant

3.3.6.1. Call number length limitation for outgoing calls from the AutoAttendant

The values for the call number length limitation set in the general parameters of the Smart Voicemail also apply to AutoAttendant suffix dialing and AutoAttendant speed dialing

3.3.6.2. Restricting the class of service for outbound dialing (OpenScape Business X only)

The internal ports of the AutoAttendants can be assigned a restricted class of service in the system.


Expert mode - Telephony Server
Auxiliary Equipment
Music on Hold (MoH)
PhoneMail
Announcements
Door Opener
SmartVM
Auto Attendant
352
SmartVM
Edit Speed Dial/Intercept Dest. Day
Edit Speed Dial/Intercept Dest. Night
Edit Speed Dial/Intercept Dest. 3
Edit Speed Dial/Intercept Dest. 4

Select	Action	Call number	Name	Type
▾	Speed dialing 0			▾
▾	Speed dialing 1			▾
▾	Speed dialing 2			▾
▾	Speed dialing 3			▾
▾	Speed dialing 4			▾
▾	Speed dialing 5			▾
▾	Speed dialing 6			▾
▾	Speed dialing 7			▾
▾	Speed dialing 8			▾
▾	Speed dialing 9			▾
▾	Intercept			▾

3.4. Measures for Protecting the Xpressions Compact Voicemail Box

The Xpressions Compact solution is no longer available in the current Unify portfolio and is no longer supported with corrections / updates by Unify. Consequently, it is recommended to replace Xpressions Compact with the UC Suite application.

Customers who want to continue using Xpressions Compact in OpenScape Business should be advised of the existing security risks.

As a general protection against toll-fraud attacks using Xpressions Compact, it is recommended that a restricted class of service (with “outward restricted trunk access”) be assigned to the voicemail ports used by Xpressions Compact within OpenScape Business.

4. Toll Fraud through VoIP Devices

To perpetrate toll fraud via VoIP, attackers exploit the standardization of Internet protocols to register external SIP or system devices as internal stations of the system. They then establish connections from these devices to any phone numbers.

The registration attempts are automated by systematically scanning the connections of VoIP PBX systems for IP terminals. The primary goal here is to find devices without authentication or devices with default or easy-to-guess passwords. After a successful registration, connections are automatically made to external phone numbers.

The successful registration of a foreign device as an internal station is difficult to detect. The stations are generally detected only during the call cost accounting, e.g., through unusually high call charges, the dialed destination numbers or the number of calls.

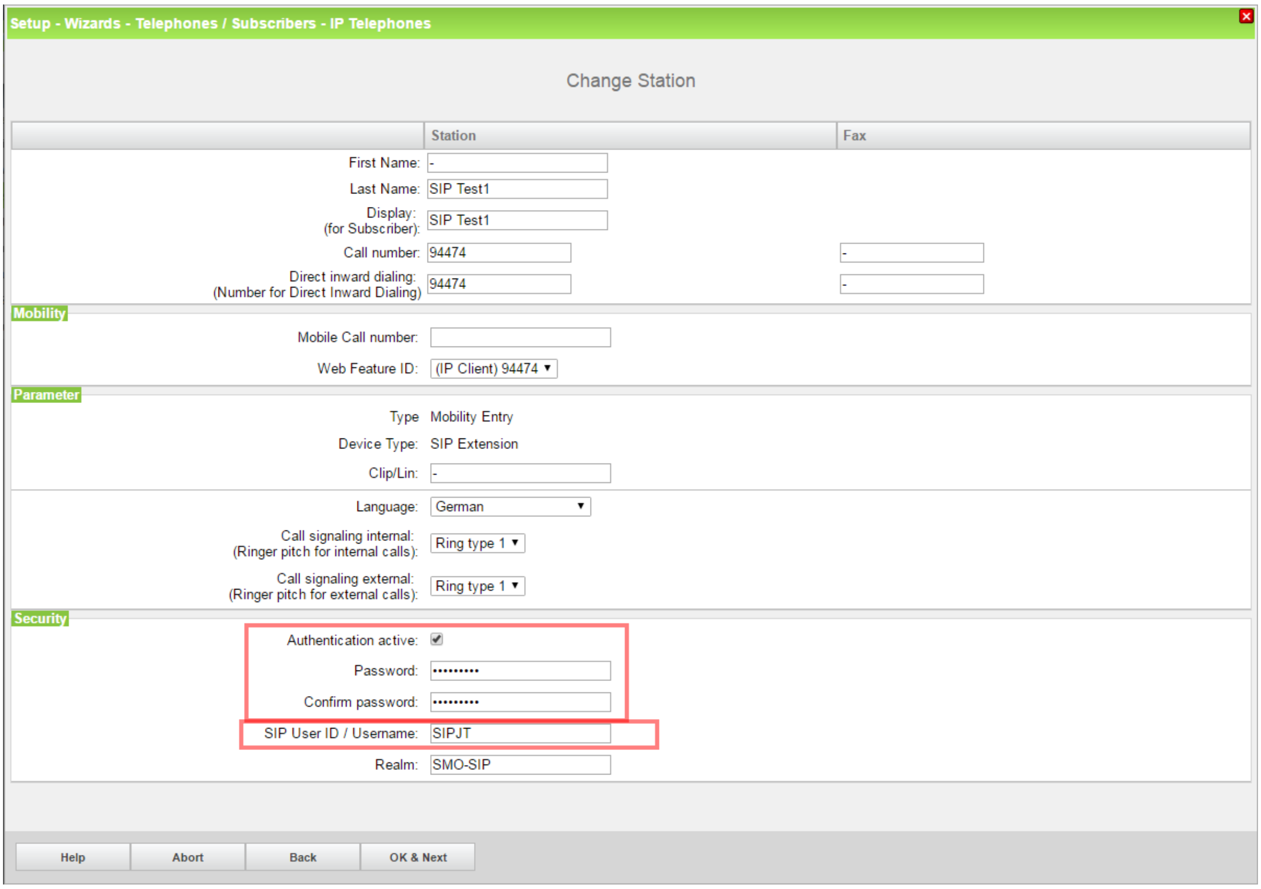
Some ITSPs block the connection if the costs exceed certain limits within a defined time period. In most cases, however, substantial damage has already occurred by the time the abuse is detected.

Apart from the registration of devices via the Internet, it should be noted that additional devices could also be introduced within the customer LAN in order to establish unauthorized connections.

4.1. Measures against the Registration of Third-Party SIP Devices

4.1.1. Authentication of SIP stations

When setting up SIP stations in OpenScape Business, the "Authentication active" flag must be set. This flag enforces authentication via the user name and password during the registration request from SIP stations.



Setup - Wizards - Telephones / Subscribers - IP Telephones

Change Station

	Station	Fax
First Name:	-	
Last Name:	SIP Test1	
Display: (for Subscriber):	SIP Test1	
Call number:	94474	-
Direct inward dialing: (Number for Direct Inward Dialing)	94474	-
Mobility		
Mobile Call number:		
Web Feature ID:	(IP Client) 94474	
Parameter		
Type	Mobility Entry	
Device Type:	SIP Extension	
Clip/Lin:	-	
Language:	German	
Call signaling internal: (Ringer pitch for internal calls):	Ring type 1	
Call signaling external: (Ringer pitch for external calls):	Ring type 1	
Security		
Authentication active:	☑	
Password:	•••••••••	
Confirm password:	•••••••••	
SIP User ID / Username:	SIPJT	
Realm:	SMO-SIP	

Figure 10 Setting up authentication for SIP stations

4.1.2. Using a strong individual password for authentication

A strong and unique device-specific password must be assigned for the authentication of SIP stations. The password must also be entered in the SIP terminal.

Note:
The operation of a SIP terminal without authentication or with a trivial or default password is tantamount to gross negligence.

4.1.3. Assigning a strong SIP User ID / User Name

Among other things, a SIP user ID is used for the registration of SIP stations. A SIP User ID that cannot be easily guessed must be selected in the SIP station configuration. It should never be just the call number of the subscriber. Even the default prefix selected by the system should be customized.

4.1.4. Deleting SIP test connections

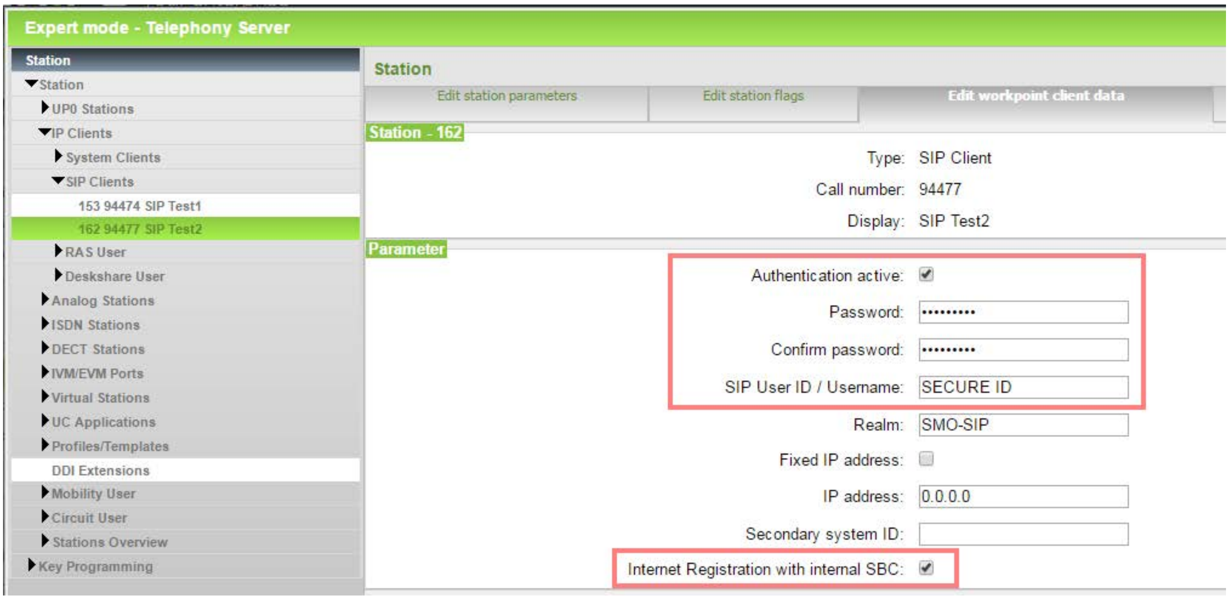
In some cases, it is necessary to set up test connections for the configuration / management of SIP stations within OpenScape Business. These connections must be deleted before handing the system over to the customer or, if they have to remain, be provided with authentication and passwords.

4.1.5. Deleting unused / surplus SIP stations

All SIP stations that are not currently required in the system should essentially be deleted.

4.1.6. Using the internal SBC with externally connected devices

For SIP stations that are connected to OpenScape Business via the Internet (SIP Device@Home), the flag "Internet Registration with internal SBC" must be set.



Station - 162

Type: SIP Client
Call number: 94477
Display: SIP Test2

Parameter

Authentication active: ☑
Password: •••••••••
Confirm password: •••••••••
SIP User ID / Username: SECURE ID
Realm: SMO-SIP
Fixed IP address: □
IP address: 0.0.0.0
Secondary system ID:
Internet Registration with internal SBC: ☑

Figure 11 Setting up external SIP stations via SBC

To set the flag, the check box "Authentication active" and the assignment of a password are mandatory and must be enabled.

The flag enables the integrated Session Border Controller (SBC) of OpenScape Business. The SBC recognizes this subscriber and blocks registration attempts by other external SIP subscribers via the Internet.

4.1.7. Using special ports for externally connected SIP stations

The signaling of a SIP connection via TCP / UDP occurs via the default port 5060. For connections secured with TLS, the default port 5061 is used.

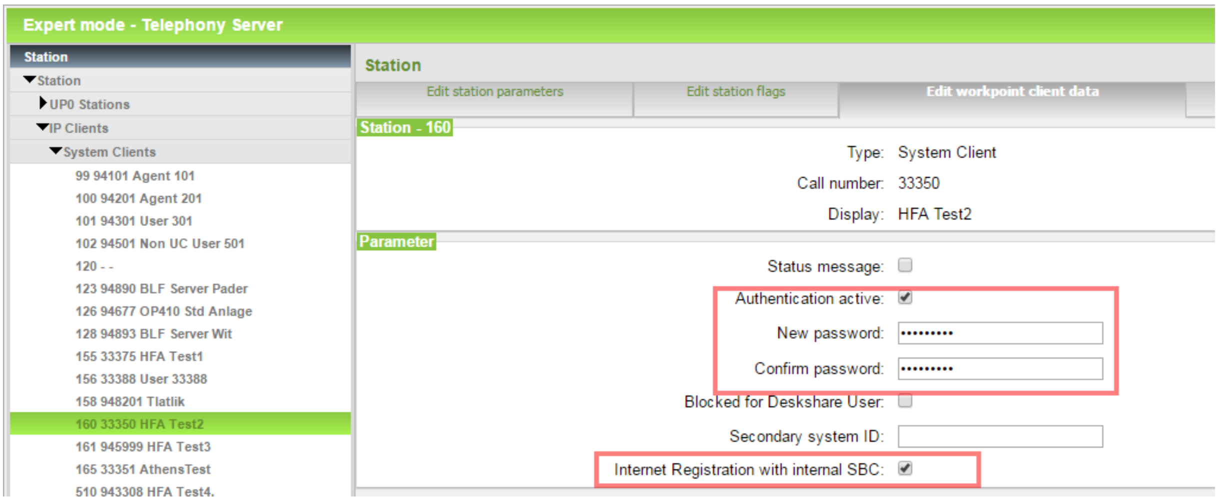
For the connection of external SIP stations to OpenScape Business, it is recommended that a UDP connection via port 5070 be used instead of the default port 5060. For connections secured with TLS, port 5062 should be used.

This requires an adaptation of the port and possibly the type of protocol (UDP) in the SIP devices. In the company (office) router, port forwarding must then be additionally configured from the external port 5070 to the internal port 5060 (UDP only).
For a TLS-secured connection, the external port 5062 must be routed to the internal port 5062. (Note: This specification is correct, since 5061 is used elsewhere in the system).

4.2. Measures against the Registration of Third-Party System (HFA) Devices

4.2.1. Authenticating system (HFA) devices

When setting up system (HFA) stations in OpenScape Business, the flag "Authentication active" must be set. This flag enforces authentication using a password during the registration request of HFA devices and prevents third-party devices from easily registering at OpenScape Business via the LAN or the Internet.



Type: System Client
Call number: 33350
Display: HFA Test2

Status message: □
Authentication active: ☑
New password: •••••••••
Confirm password: •••••••••
Blocked for Deskshare User: □
Secondary system ID:
Internet Registration with internal SBC: ☑

Figure 12 Setting up external system devices with authentication

4.2.2. Using a strong individual password for authentication

A strong and unique device-specific password must be assigned for the authentication of system (HFA) devices. This increases the security against guessing the password.

Note:
The password must be entered both in the system configuration as well as the system (HFA) devices.

4.2.3. Deleting system (HFA) test connections

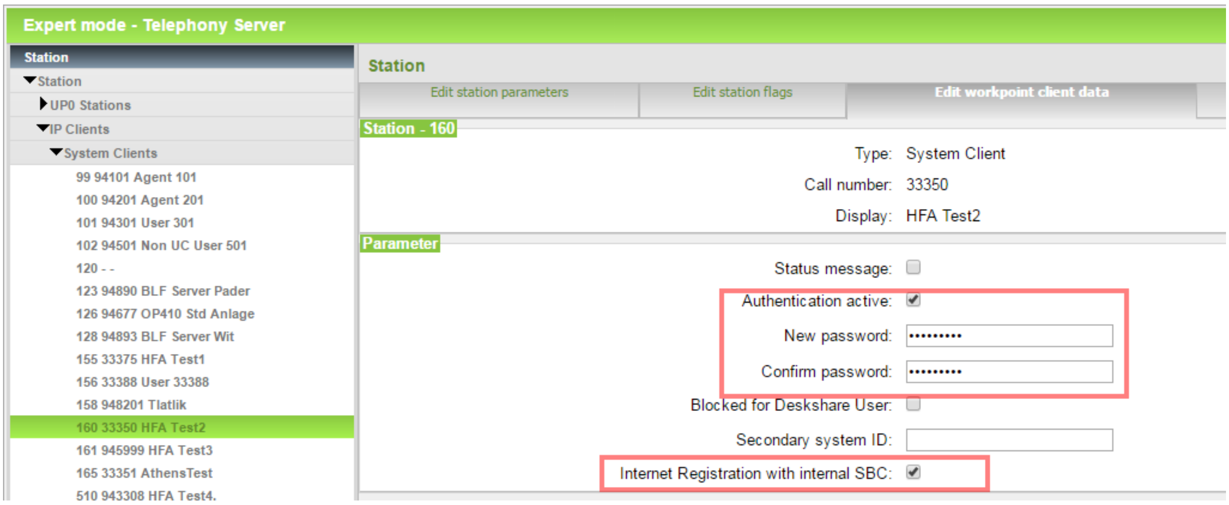
In some cases, it is necessary to set up test connections for the configuration / management of system (HFA) devices within OpenScape Business.
These connections must be deleted before handing the system over to the customer or, if they have to remain, be provided with authentication and passwords.

4.2.4. Deleting unused / surplus system (HFA) connections

All system (HFA) stations that are currently not required in the system should essentially be deleted.

4.2.5. Using the internal SBC with externally connected devices

For system (HFA) stations that are connected to OpenScape Business via the Internet (feature: System Device@Home), the flag "Internet Registration with internal SBC" must be set.



Type: System Client
Call number: 33350
Display: HFA Test2

Status message: □
Authentication active: ☑
New password: •••••••••
Confirm password: •••••••••
Blocked for Deskshare User: □
Secondary system ID:
Internet Registration with internal SBC: ☑

Figure 13 Setting up SBC for external system devices

To set the flag, the check box "Authentication active" and the assignment of a password are mandatory and must be enabled.

The flag enables the integrated Session Border Controller (SBC) of OpenScape Business. With the activation, ports 4062 and 4063 are used for communication with external system (HFA) stations.
The use of different ports enables the integrated SBC to differentiate between external stations and internal system (HFA) stations and block unauthenticated registrations.

4.2.6. Setting up port forwarding for externally connected system (HFA) stations.

To establish the connection to external system (HFA) stations, ports 4062 and 4063 are used with TLS encryption.

In order to avoid having to change the default ports used by the external system (HFA) devices in each of these devices, port forwarding must be configured in the company (office) router from the external port 4060 to the internal port 4062 (TCP/UDP) for normal connections, and from the external port 4061 to the internal port 4063 for TLS-encrypted connections.

5. Toll Fraud through DISA Port

OpenScape Business offers a DISA port for the implementation of various Mobility features within OpenScape Business. The function can be addressed within OpenScape Business via two different signaling pathways.

- **Signaling via DTMF control**
  Here, the control is performed via DTMF tones in the voice channel.
  External subscribers dial into the system via the DISA port and run associated services in the system from their devices by entering feature codes. By entering phone numbers, even connections to internal or external stations are set up via the system.
  Before the system allows the execution of services via the DISA port, the external user has to provide authentication via the DISA PIN. The check for the DISA pin occurs either after a timeout or after entering "#".
  Note:
  Checking the DISA PIN is skipped if the number of the calling external subscriber is assigned to a Mobility station within the system.
- **Signaling via the Web Services Interface (only for myPortal to go)**
  Here, the information for controlling the port is transmitted in the data channel using HTPP(S).

5.1. Attacks on the DISA Port

Attacks on DISA ports generally occur in the same manner as attacks on voicemail ports by automatically calling the DISA phone number and trying PIN combinations. Upon receiving a positive acknowledgment, the attacker then either connects directly to external destinations or programs further call forwarding destinations in the system in order to establish additional connections to external destinations.

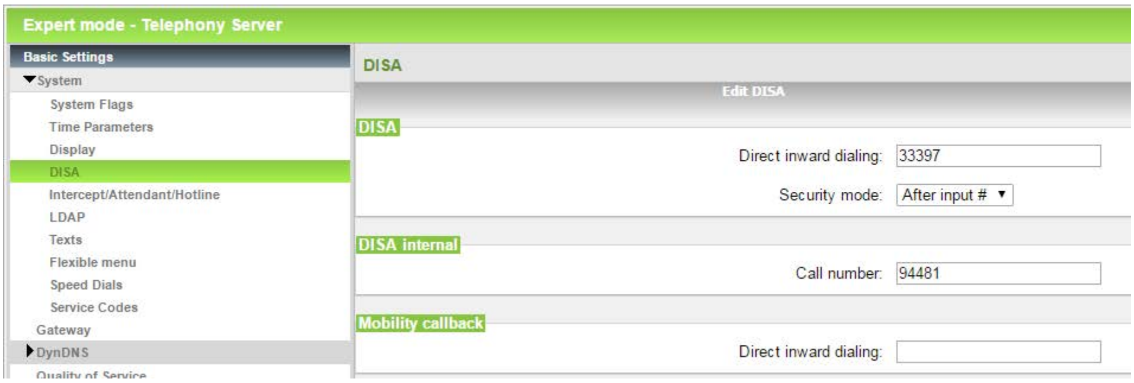
DISA port attacks are easier for attackers if they become aware of the DISA port number and possibly also the subscriber who is internally assigned to the DISA port.

The attack is greatly facilitated if the attacker gains access to the mobile phone of a mobile subscriber registered in the system.

5.2. Measures against Attacks on the DISA Port with OpenScape Business

5.2.1. Blocking or not releasing the DISA port

If no DISA number is entered in the system configuration (Basic Settings → System → DISA) or if the existing number is deleted, the DISA port is blocked.



DISA

Direct inward dialing: 33397

Security mode: After input #

DISA internal

Call number: 94481

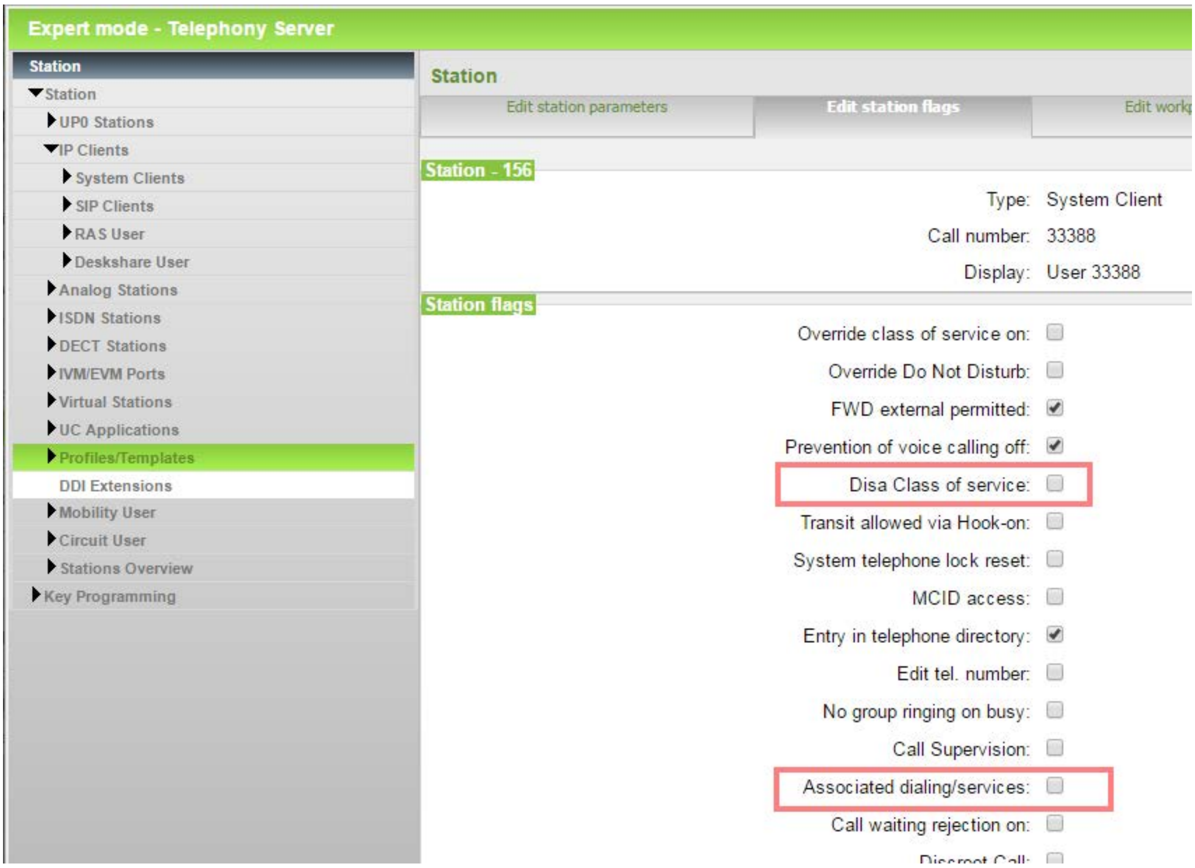
Mobility callback

Direct inward dialing:

Figure 14 Releasing the DISA port

5.2.2. Restrictive handling of the "DISA Class of Service" station flag

The "DISA Class of Service" flag should be set only for those subscribers for whom the execution of DISA functions is actually intended. The flag is not set at the initial startup. It must always be double-checked after a migration/ugrade.



Station - 156

Type: System Client

Call number: 33388

Display: User 33388

Station flags

Override class of service on: □

Override Do Not Disturb: □

FWD external permitted: ☑

Prevention of voice calling off: ☑

Disa Class of service: □

Transit allowed via Hook-on: □

System telephone lock reset: □

MCID access: □

Entry in telephone directory: ☑

Edit tel. number: □

No group ringing on busy: □

Call Supervision: □

Associated dialing/services: □

Call waiting rejection on: □

Discreet Call: □

Figure 15 Blocking the DISA class of service for subscribers

Notes:
Mobility stations do not require any DISA class of service to execute the above features.

The flag "Associated dialing/services" does not affect the DISA functionality if the flag "DISA Class of Service" is set for the subscriber.

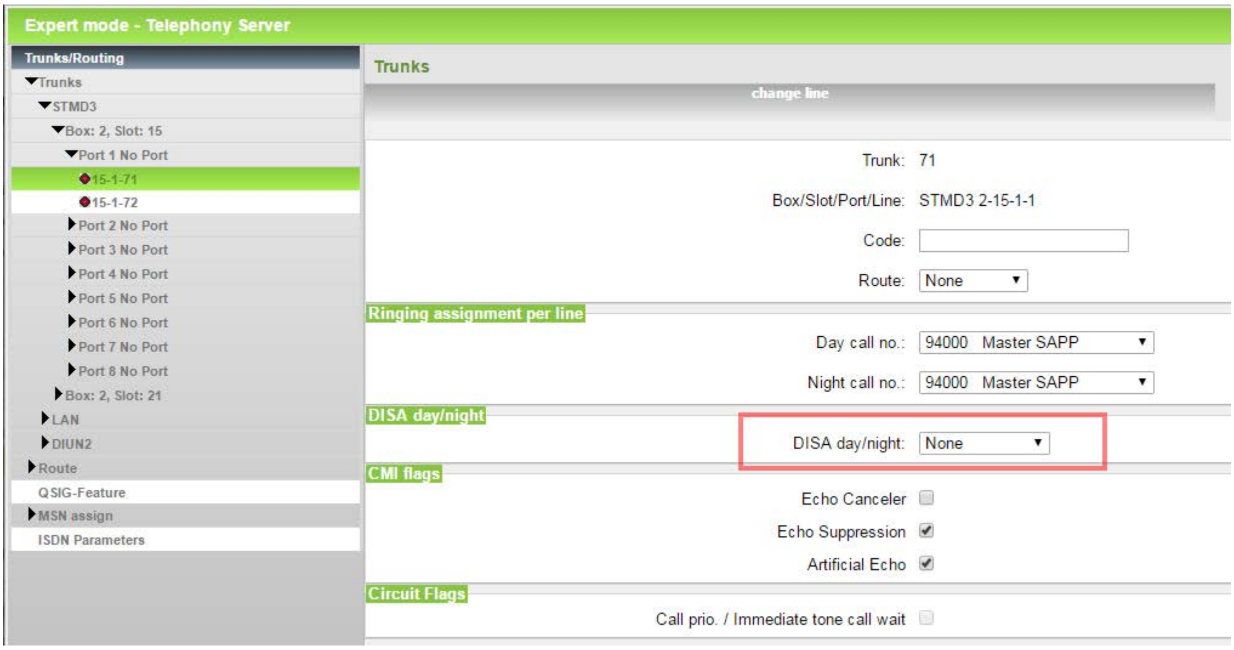
5.2.3. Changing the phone lock PIN for "DISA class of service" subscribers.

Thephone lock PIN of the "DISA class of service" subscribers must be changed from the default "00000" to a "strong" PIN. If physical devices have been assigned to the "DISA class of service" subscribers, the staff must be advised accordingly.

Note:
The authentication using the DISA PIN and the checking of the "DISA Class of Service" flag do not occur on receiving an external call to the DISA DID number from a number that was assigned to a Mobility station.

5.2.4. Locking the DISA release for lines

For each ISDN or VoIP line, the value "None" must be set in the line parameters for "DISA day/night" in order to lock the line for the use of DISA. The value is set to "None" at the initial startup. It must always be double-checked again and possibly adapted if required following any upgrade/migration.



Trunks

Trunk: 71
Box/Slot/Port/Line: STMD3 2-15-1-1
Code:
Route: None

Ringing assignment per line

Day call no.: 94000 Master SAPP
Night call no.: 94000 Master SAPP

DISA day/night

DISA day/night: None

CMI flags

Echo Canceler □
Echo Suppression ☑
Artificial Echo ☑

Circuit Flags

Call prio. / Immediate tone call wait □

Figure 16 Blocking the DISA class of service for lines

5.2.5. Restrictive dealing with the publication of the DISA port and DISA PIN

Information on the DISA port number and the assigned "DISA stations" and the DISA PIN should only be communicated to the individuals who will actually be using the DISA port. There should, for example, be no publication of the DISA port in internal phone books, etc.

5.2.6. Securing a mobile phone against unauthorized access

Mobile phones assigned to mobile subscribers in the system must be protected by appropriate means against unauthorized access or data espionage in order to keep the DISA dial-in parameters and possibly the UC user login parameters secret.

List of Figures

unify Harmonize your enterprise

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products.
An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

Availability and technical specifications are subject to change without notice.