

# SECURITY RECOMMENDATIONS FOR OMNIPCX OFFICE

---

This document provides the customer with the programming possibilities for maximum security against unauthorised persons from accessing the OmniPCX Office features such as Personal Assistant, remote configuration of a diversion to establish unauthorised outgoing calls.

---

## Revision History

|                              |                                                                                             |
|------------------------------|---------------------------------------------------------------------------------------------|
| Edition 1: February 17, 2009 | creation of the document                                                                    |
| Edition 2: June 5, 2009      | modification about VMUMaxTry noteworthy address                                             |
| Edition 3: December 11, 2009 | added information about DivRemCust noteworthy address                                       |
| Edition 4: January 26, 2011  | added weak password control, system password recommendations and Remote customization right |
| Edition 5: February 1, 2011  | VMUMaxTry added to R3.1                                                                     |
| Edition 6: April 21, 2011    | note about OMC Software download password added                                             |
| Edition 7: December 5, 2011  | complementary information about week password and system password security added            |
| Edition 8: May 24, 2013      | update 6 digit password, CallCorres noteworthy address and R910 new features added          |

## **Legal notice:**

Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent.  
All other trademarks are the property of their respective owners.  
The information presented is subject to change without notice.  
Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.  
Copyright © 2013 Alcatel-Lucent. All rights reserved.

## Table of contents

|                                                                                        |    |
|----------------------------------------------------------------------------------------|----|
| 1 Introduction.....                                                                    | 3  |
| 2 Overview .....                                                                       | 3  |
| 3 User Password management policy .....                                                | 4  |
| 4 System Password management policy .....                                              | 5  |
| 5 Software Security programming options .....                                          | 7  |
| 5.1 Programming possibilities for the different OmniPCX Office software releases ..... | 7  |
| 5.1.1 All Releases .....                                                               | 7  |
| 5.1.2 R110, R210 and above – User and System configuration .....                       | 7  |
| 5.1.3 R310 up to R910 – User Feature Right "Remote customization" .....                | 8  |
| 5.1.4 R310 up to R910 – Personal Assistant .....                                       | 8  |
| 5.1.5 R310 up to R910 – Password attempts.....                                         | 9  |
| 5.1.6 R710 up to R910 – Remote diversion customization .....                           | 9  |
| 5.1.7 R510 up to R910 – Callback feature in voicemail box .....                        | 10 |
| 6 Summary.....                                                                         | 11 |
| 6.1 Noteworthy addresses and system option .....                                       | 11 |
| 6.2 Passwords control and passwords check .....                                        | 11 |

## 1 Introduction

---

The purpose of this technical communication is to provide the customer with the programming possibilities for maximum security against unauthorised persons from accessing the OmniPCX Office features such as Personal Assistant, remote configuration of a diversion (since R700) to establish unauthorised outgoing calls. These features are protected with a password defined by the user.

This unique password is used to access to following features:

- Mailbox customization,
- Personal assistant customization,
- Password management,
- Nomadic mode configuration,
- Diversion activation,
- Remote substitution,
- Access to voicemail box,
- Connection of PIMphony to the OmniPCX,
- Lock the phone,
- My IC Web for Office,
- My IC Mobile.

## 2 Overview

---

Remote customization via a phone call to the OmniPCX Office can be used to configure e.g. the Personal Assistant in order to enable and define an external forwarding destination on the associated set.

The external caller has to know the exact remote access and Personal assistant process (i.e OmniPCX Office voice guides do not prompt for the actions required). The caller also has to know the extension number of the set and the password.

Once the Personal Assistant feature and an external forwarding destination have been enabled then an external caller to the Personal Assistant will be forwarded to the defined destination (trunk to trunk communication).

There are several OmniPCX Office programming options available to the installer to control the Personal Assistant from being forwarded to specified external destinations.

### 3 User Password management policy

---

Password creation and security is the responsibility of the user/system Administrator or Installer. Therefore, if somebody is accessing the P.A (Personal Assistant) or DISA Transit (remote substitution) using a correct password then it is deemed that he/she is an authorized user of the password.

This functionality is a security feature and is not viewed as a product defect or limitation.

The following are the Alcatel-Lucent recommendations for good password management:

- Implement company policy to regularly update all user passwords.
- Ask the users to regularly change their passwords.
- Avoid the use of simple passwords such as 1234, 1111, 0000, etc...
- User is forced by the OmniPCX Office system to change the default password when initialising their Voice mail.
- Do not disclose passwords to other persons/colleagues etc.
- Lock extensions when not being attended (i.e. holidays, night time, weekend etc...).



#### Important

---

The system prevents the user input of weak passwords since R410/065.001, R510/059.001, R610/047.001, R710/052.007, R800/030.002, R810/045.003, R820/026.007, R900/033.002 and R910/021.001.

Since R800/043.001 and R810/047.001 the range of passwords defined in the Omni PCX Office to be weak has been increased. If a password input is considered as weak by the OmniPCX Office then the message "Invalid input" will be played.

---



#### Important

---

Since R820/026.007, R900/033.002 and R910/021.001 the system can be configured to use a 6 digits password for the users. New systems will start with 6 digits and migrated systems will keep the 4 digits passwords but at each OMC connection a message will pop-up with a recommendation to switch to 6 digits.

---



#### Note

---

After a swap with data saving, from a previous version to one mentioned above, if weak passwords have been used they will be restored into the system. In such cases it is the responsibility of the user/system Administrator or Installer to verify that our recommendations for good password management are applied.

---



#### Note

---

Since R9.1 new functions to check if weak password are used and to reset the passwords of users having a weak password have been introduced (See Expert Documentation for more details).

---

## 4 System Password management policy

Similar rules have to be applied to the different passwords allowing an OMC connection to the system. It is recommended to change the default **Installer** password for OMC Expert, **Administrator** password for OMC EasyPlus and **Operator** password for OMC Easy. Remember these passwords can also be used from the MMC-Station.

The following are the Alcatel-Lucent recommendations for good password management:

- Implement company policy to regularly update all system passwords.
- Regularly change the passwords.
- Avoid the use of simple passwords such as 12345678, 11111111, 00000000 etc...
- Never choose a word from everyday language. Attackers can use special dictionary cracking software to retrieve these.
- Never choose a word that is closely related to you: your company name, your name, your wife's maiden name, the name of your dog or your children, your favourite hobby, etc...
- Choose a different password for each connection level.
- Do not disclose passwords to other persons/colleagues etc.
- Never write down your password (or store it on your computer). The first thing an attacker will do is rummage through your belongings.



### Warning

The same rules have to be applied to the OMC **Software download** session password. Default password is same as default Installer level, but downloading session has a specific password which can be modified with OMC Expert.



### Note

Complementary security can be achieved by enabling the "Callback / Authorized Callers" feature in OMC "Network Management Control". This will give full control of who is authorized to connect to the system (for more details read Expert Documentation).

Since R9.1 (first version) all the management passwords (except Operator) have to follow new rules (controlled by the system) and requires now a minimum of:

- one uppercase letter (A-Z),
- one lowercase letter (a-z),
- one numeric character (0-9),
- fixed length of 8 characters,
- no special characters.

**Note**

---

Since R9.1 a new function to check if weak or default passwords are used has been introduced (See Expert Documentation for more details).

---

**Important**

---

Since R9.0 when you request an Installer password reset through a Service Request it is mandatory to provide us either the CPU Serial Number and MAC Address or the CPU id.

---

## 5 Software Security programming options

There are many OmniPCX Office programming options, which when configured correctly provide the customers system with the maximum Security.

### 5.1 Programming possibilities for the different OmniPCX Office software releases

#### 5.1.1 All Releases

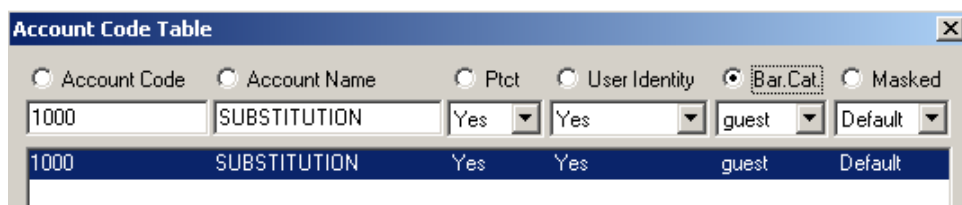


By default all external break out calls from the Personal Assistant and User Voicemail box are subject to the User Barring traffic sharing tables and User Features Rights of its associated physical extension.

However, it is possible to change this mechanism so that the call is subject to the barring traffic sharing tables of the VMU ports, which are used by the Personal Assistant to make the break out call.

This mechanism change can be achieved by removing all Account codes table entries having a "Guest" barring category.

The default system Account code table has such a 'Guest' barring category - see following:



| Account Code | Account Name | Pct | User Identity | Bar.Cat. | Masked  |
|--------------|--------------|-----|---------------|----------|---------|
| 1000         | SUBSTITUTION | Yes | Yes           | guest    | Default |
| 1000         | SUBSTITUTION | Yes | Yes           | guest    | Default |

#### 5.1.2 R110, R210 and above – User and System configuration

Disabling the following features prevents an incoming caller from break-out, either by manual transfer or diversion

- Users per user Feature Right – Join incoming and outgoing
- Feature Design – Part 2 – Transfer to external
- Feature Design – Part 2 – Transfer Ext/Ext by on hook
- User per user Barring and traffic sharing (depending on above description)
- System Joining

### 5.1.3 R310 up to R910 – User Feature Right "Remote customization"

Remote customization right can now be controlled on a per user basis: Subscriber – Feature – Part 2 – "Remote customization". This feature disables the personal options menu (option 9) from the voice mailbox.



This feature is available since R310/060.001, R410/065.001, R510/059.001, R610/047.001, R710/069.001, R800/030.002, R810/045.003, R820/026.007, R900/033.002 and R910/021.001. By default this feature is disable and option 9 (personal options) is not available.



It is mandatory to use OMC 800/21.1b or above. This feature is not available in OMC R711.



**It is strongly recommended to upgrade the systems to latest version of each release**

### 5.1.4 R310 up to R910 – Personal Assistant

Noteworthy Address called **PerAssAlwd** has been introduced in R310/055.001, R410/056.001, R510/035.001, R610/012.001, R7.0, R7.1, R8.0, R8.1, R9.0 and R9.1 since first version.

This flag can be used to enable/disable the Personal Assistant on the system.



Since R410/064.001, R510/058.001, R610/033.001, R700/026.001, R710/022.001, R800/030.002, R810/045.003, R820/026.007, R900/033.002 and R910/021.001 the default value of the noteworthy addresses for personal assistant is: 00H (personal assistant disable by default).



In R310 the default value of the noteworthy addresses for personal assistant is: **01H** (personal assistant enable by default).



After a swap with data saving, from a previous e.g. R6.x or R7.x version, to R610/033.001 or R710/022.001, it is necessary to enable the Personal Assistant if the feature was used by the end customer before.



**It is strongly recommended to upgrade the systems to latest version of each release**



### 5.1.5 R310 up to R910 – Password attempts

Noteworthy Address called **VMUMaxTry** has been introduced in R310/060.001, R410/064.001, R510/058.001, R610/015.001, R7.0, R7.1, R8.0, R8.1, R8.2, R9.0 and R9.1 since first version. This flag is used to limit the maximum incorrect voicemail password retries attempts




---

Since R310/060.001, R410/064.001, R510/058.001, R610/033.001, R700/026.001, R710/022.001, R800/030.002, R810/045.003, R820/026.007, R900/033.002 and R910/021.001 the default value is **03H** (3 attempts max by default).

---




---

No information related to remote access status is provided and the behaviour of remote access remains the same, even after blocking.

If the remote access is blocked before the third attempt (e.g. VMUMaxTry is set to 01), a malicious call will nevertheless be able to process the second and third try. Those attempts will get the prompt "xxxx is not your correct password", followed by "good-by" message and call release.

Even if the remote access is already blocked before the first malicious try, the same process (3 tries and call release) will be performed.

---




---

**It is strongly recommended to upgrade the systems to latest version of each release**

---

### 5.1.6 R710 up to R910 – Remote diversion customization

Noteworthy Address called **DivRemCust** has been introduced in R710/028.001, R8.0, R8.1, R8.2, R9.0 and R9.1 since first version. This flag is used to enable or disable the feature "remote diversion customization".




---

Since R710/028.001, R800/030.002, R810/045.003, R820/026.007, R900/033.002 and R910/021.00 the default value is 00H (feature not available in the voice mailbox customization menu).

---




---

**It is strongly recommended to upgrade the systems to latest version of each release**

---

### 5.1.7 R510 up to R910 – Callback feature in voicemail box

Noteworthy Address called **CallCorres** has been introduced in R510/064.001, R610/052.001, R710/097.001, R820/045.001, R900/037.001 and R910 since first version. This flag is used to enable or disable the feature "callback" (option 3) when consulting a message left on the voicemail box.



#### Important

---

Default value is country dependant (00H feature not available in the voice mailbox menu, 01H feature is available in the voice mailbox menu).

---



#### Warning

---

**It is strongly recommended to upgrade the systems to latest version of each release**

---

## 6 Summary

### 6.1 Noteworthy addresses and system option

|                  | VMUMaxTry                         | VMUMaxTry   | PerAssAlwd        | PerAssAlwd                        | DivRemcust                         | Callcorres                        | User Feature<br>"Remote<br>customization" |
|------------------|-----------------------------------|-------------|-------------------|-----------------------------------|------------------------------------|-----------------------------------|-------------------------------------------|
| default<br>value | 20<br>(old value)                 | 03          | 01<br>(old value) | 00                                | 00                                 | country<br>dependent              | disabled                                  |
| R3.1             | <i>not available</i> <sup>1</sup> | 310/060.001 | 310/055.001       | <i>not available</i> <sup>1</sup> | <i>not applicable</i> <sup>2</sup> | <i>not available</i> <sup>1</sup> | 310/060.001                               |
| R4.1             | <i>not available</i> <sup>1</sup> | 410/064.001 | 410/056.001       | 410/064.001                       | <i>not applicable</i> <sup>2</sup> | <i>not available</i> <sup>1</sup> | 410/065.001                               |
| R5.1             | <i>not available</i> <sup>1</sup> | 510/058.001 | 510/035.001       | 510/058.001                       | <i>not applicable</i> <sup>2</sup> | 510/064.001                       | 510/059.001                               |
| R6.1             | 610/015.003                       | 610/033.001 | 610/012.001       | 610/031.001                       | <i>not applicable</i> <sup>2</sup> | 610/052.001                       | 610/047.001                               |
| R7.0             | 700/012.005                       | 700/026.001 | 700/012.005       | 700/026.001                       | <i>in R710</i>                     | <i>in R710</i>                    | <i>in R710</i>                            |
| R7.1             |                                   | 710/022.001 |                   | 710/022.001                       | 710/028.001                        | 710/097.001                       | 710/069.001                               |
| R8.0             |                                   | 800/030.002 |                   | 800/030.002                       | 800/030.002                        | <i>in R820</i>                    | 800/030.002                               |
| R8.1             |                                   | 810/045.003 |                   | 810/045.003                       | 810/045.003                        | <i>in R820</i>                    | 810/045.003                               |
| R8.2             |                                   | 820/026.007 |                   | 820/026.007                       | 820/026.007                        | 820/045.001                       | 820/026.007                               |
| R9.0             |                                   | 900/033.002 |                   | 900/033.002                       | 900/033.002                        | 900/037.001                       | 900/033.002                               |
| R9.1             |                                   | 910/021.001 |                   | 910/021.001                       | 910/021.001                        | 910/021.001                       | 910/021.001                               |

1: *Not available* means that the noteworthy address is not available or that the indicated default value is not used in this release.

2: *Not applicable* means that the noteworthy address doesn't exist in this release because the feature on which it is applicable doesn't exist in this release

Version in blue means that it is the first version of this release

### 6.2 Passwords control and passwords check

|      | User password<br>control<br>(system) | Management<br>password control<br>(system) | User, Management and<br>Admin SIP Phone<br>passwords check<br>(system)<br>AutoPwdChk | OMC user password check<br>and reset<br>(only with OMC910/14.1b<br>and above) <sup>2</sup> |
|------|--------------------------------------|--------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| R3.1 | <i>not available</i> <sup>1</sup>    | <i>not available</i> <sup>1</sup>          | <i>not available</i> <sup>1</sup>                                                    | yes                                                                                        |
| R4.1 | 410/064.001                          | <i>not available</i> <sup>1</sup>          | <i>not available</i> <sup>1</sup>                                                    | yes                                                                                        |
| R5.1 | 510/058.001                          | <i>not available</i> <sup>1</sup>          | <i>not available</i> <sup>1</sup>                                                    | yes                                                                                        |
| R6.1 | 610/047.001                          | <i>not available</i> <sup>1</sup>          | <i>not available</i> <sup>1</sup>                                                    | yes                                                                                        |
| R7.0 | <i>not available</i> <sup>1</sup>    | <i>not available</i> <sup>1</sup>          | <i>not available</i> <sup>1</sup>                                                    | yes                                                                                        |
| R7.1 | 710/057.007                          | <i>not available</i> <sup>1</sup>          | <i>not available</i> <sup>1</sup>                                                    | yes                                                                                        |
| R8.0 | 800/030.002                          | <i>not available</i> <sup>1</sup>          | <i>not available</i> <sup>1</sup>                                                    | yes                                                                                        |
| R8.1 | 810/045.003                          | <i>not available</i> <sup>1</sup>          | <i>not available</i> <sup>1</sup>                                                    | yes                                                                                        |
| R8.2 | 820/026.007                          | <i>not available</i> <sup>1</sup>          | <i>not available</i> <sup>1</sup>                                                    | yes                                                                                        |
| R9.0 | 900/033.002                          | <i>not available</i> <sup>1</sup>          | <i>not available</i> <sup>1</sup>                                                    | yes                                                                                        |
| R9.1 | 910/021.001                          | 910/021.001                                | 910/021.001                                                                          | yes                                                                                        |

1: *Not available* means that the feature doesn't exist in this release

2: OMC user password check and reset will work on all releases

Version in blue means that it is the first version of this release

### Follow us on Facebook and Twitter

Stay tuned on our Facebook and Twitter channels where we inform you about:

- New software releases
- New technical communications
- AAPP InterWorking Reports
- Newsletter
- Etc.



[twitter.com/ALUEnterpriseCare](https://twitter.com/ALUEnterpriseCare)



[facebook.com/ALECustomerCare](https://facebook.com/ALECustomerCare)

### Submitting a Service Request

Please connect to our eService application at:

<https://businessportal.alcatel-lucent.com/alugesdp/faces/gesdp/customerSupport/CustomerSupport.jspx>

Before submitting a Service Request, make sure that:

- In case a Third-Party application is involved, that application has been certified via the AAPP
- You have read through the Release Notes which lists new features available, system requirements, restrictions etc. available in the [Technical Knowledge Base](#)
- You have read through the Troubleshooting Guides and Technical Bulletins relative to this subject available in the [Technical Knowledge Base](#)

- END OF DOCUMENT -

---