Alcatel·Lucent Enterprise

Technical Bulletin	Alcatel-Lucent OXO Connect

TC1143 ed.15 Release R2.0

Security Recommendations for OXO system

This document provides the customer with the Alcatel-Lucent Enterprise's recommendations for setting an optimal security against unauthorised uses or access to OXO Connect. This document also apply to OmniPCX Office RCE releases.
Remark : in the document, OXO system stands for OXO Connect and OmniPCX Office RCE

Revision History

Edition 11: November 24, 2014	Network Security chapter replaces Internet Security recommendations
Edition 12: April 16, 2015	Passwords and configuration enhancement in R10.1
Edition 13: August 21, 2015	User Passwords management update in R10.1MR
Edition 14: November 23, 2015	R10.2 : Enabling/disabling access to management or user application services
Edition 15: November 25, 2016	Update for OXO Connect R2.0 and OmniPCX Office RCE

Table of contents

1 Introduction

In the document, OXO system stands for OXO Connect and OXO Office RCE.

The purpose of this technical communication is to provide the customer with the Alcatel-Lucent Enterprise's recommendations for setting an optimal security on OXO system system's configuration and deployment.
OXO system provides multiple features that may be accessed from various locations, including remote sites or internet. Security measures and controls provided by our system allow controlling the access and use of these features while optimizing the security of the solution. Knowing however that telecommunication system cannot be entirely free from any risk of unauthorized use, it is highly critical that installer and user/system administrator provide diligent attention to system management and security recommendations of Alcatel-Lucent Enterprise to effectively reduce such risk.

It is installer's responsibility to carefully inform users/system administrators of the OXO system system's security features and ensure their awareness of the system vulnerabilities if the Alcatel-Lucent Enterprise's recommendations are not strictly and constantly followed.

System installer must also discuss with the user/system administrator the level of security it expects, advise the user/system administrator accordingly, and implement appropriate configurations to best customize the system to meet such security levels such as, but not limited to, to not activate Personal Assistant services or remote configuration of a diversion (since R700) if there is no current or anticipated need for it for the user/system administrator.

2 Access Control: Password policies

It is critical to consider appropriate security configuration when exposing OXO system services to external accesses, e.g. via the Internet. The access to OXO system user services are protected with a password to be defined and managed by the user in compliance with the policy set forth below.

This is a single password also used to access the 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 Office RCE,
- Lock the phone,
- My IC Web for Office,
- My IC Mobile / OpenTouch Conversation (OTCV).

2.1 User password management policy

Password creation and security is under the responsibility of the user/system Administrator. Installer must ensure that user/system Administrator is aware and understand that: (a) implementation, strict and constant compliance with a password management policy at least consistent with the recommendations set forth in this technical communication is key to protect the system from unauthorized usage; and (b) any person accessing the P.A (Personal Assistant) or DISA Transit (remote substitution) using a correct password shall be deemed to be an authorized user of the password. The OXO system system asks to the change the default password for each given Voice Mail when such Voice Mail is initialized.

Alcatel-Lucent Enterprise strongly recommends using the following rules for a good password management:

- change all default passwords to be new and strong passwords, in particular if you use any application linked to your OXO system telephone, such as Voice mail, Personal assistant or any external application which can connect via the WAN (i.e. My IC Mobile, PIMphony, etc.);
- regularly change their respective personal passwords;
- avoid the use of easy passwords such as 1234, 0000, the user's extension number, etc.;
- not to disclose passwords to other persons/colleagues; and
- Lock extensions when not being attended (i.e. holidays, night time, weekend, etc.);

Important

The system prevents the user input of easy 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 set of prevented easy passwords defined in the Omni PCX Office RCE has been extended. If a password input is considered easy by the OXO system or Omni PCX Office RCE, 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

(**for Release < R10.1MR**) As a reminder, after a swap with data saving from a previous version to any of the above mentioned versions, all passwords (including easy passwords if any have been used and existed at the time of the swap), will be automatically restored into the system. Therefore, it is the responsibility of the user/system Administrator to verify that Alcatel-Lucent Enterprise's recommendations for good password management are promptly implemented upon such swap, including change by user's agent of easy passwords.

Note

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

Note

Since R10.1 the installer will have to customize the default user password (See Expert Documentation for more details).

Note

When migrating from release ≤ R10.1 to R10.1MR, Easy passwords (subscriber passwords not in line with password policy of the system) are replaced with newly generated default subscriber password.

2.2 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 and the Web-Based Tool.

Alcatel-Lucent Enterprise strongly recommends using the following rules for a good password management:

- Regularly change the passwords.
- Implement company policy to regularly update all system passwords.
- Avoid the use of easy passwords with digits such as 12345678, 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, the name of your dog or your children, etc.
- Choose a different password for each connection level.
- Do not disclose passwords to other persons/colleagues.
- Do not 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 measures 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 this password syntax policy (controlled by the system) that requires a minimum of:

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

Since R10.0 (first version) Operator password has to follow this password syntax policy (controlled by the system) that requires:

- fixed length of 8 alphanumeric characters,
- at least one digit (e.g. "HelloYou" is rejected, "Hello123" is valid),
- at least two different characters (e.g. "11111111", "aaaaaaaa" are rejected),
- sequence of characters that are not in ascending or descending order (e.g. "12345678", "abcdefgh" are rejected),
- no special characters.

Note

Since R9.1 a new function to check if easy 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.

Note

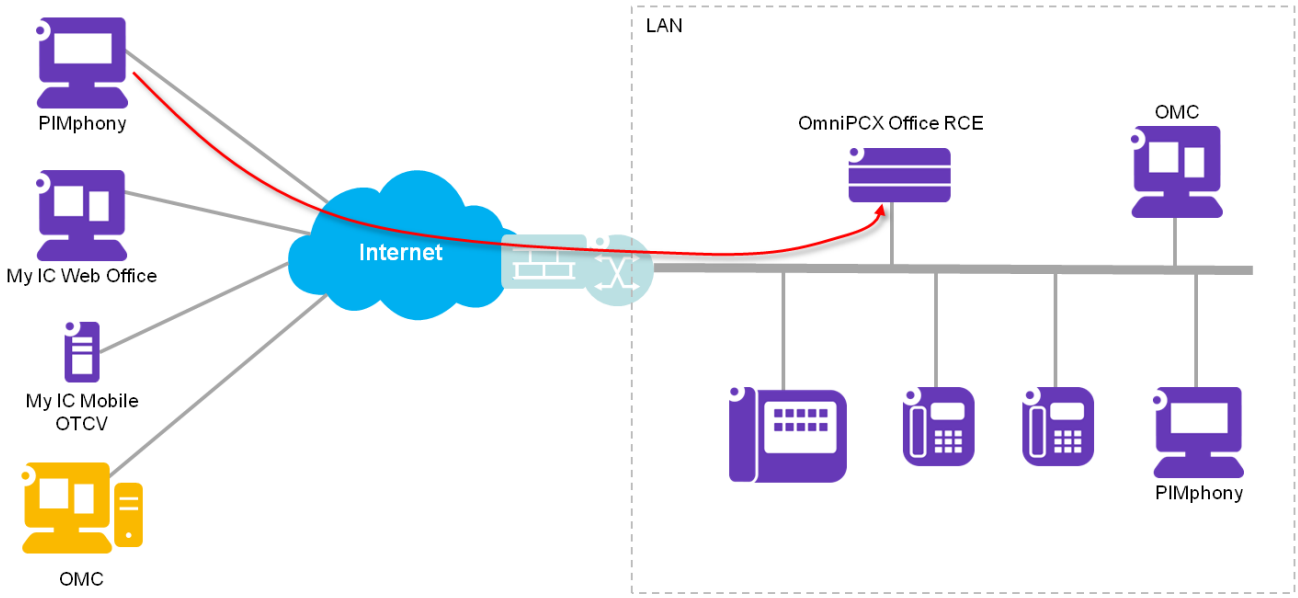
Since R10.1, it is mandatory to set all Management Passwords to non-default value during OMC connection. (See Expert Documentation for more details).

3 Network Security: configuration for remote accesses

3.1 Internet access security

Internet access is usually provided to network equipments connected in a Local Area Networks (LAN) through an access router or Internet Access Device. Nowadays, this device systematically includes firewall functions to protect the LAN from external threats

The OXO system is not directly connected to the Internet but in the LAN. Remote access from the Internet to the OXO system usually goes through the Internet Access Device with firewall functions at the border of the LAN. Remote access may be required for end user applications (My IC Web for Office, My IC Mobile/OTCV, and PIMphony) and management applications (OMC, Web-Based Tool).

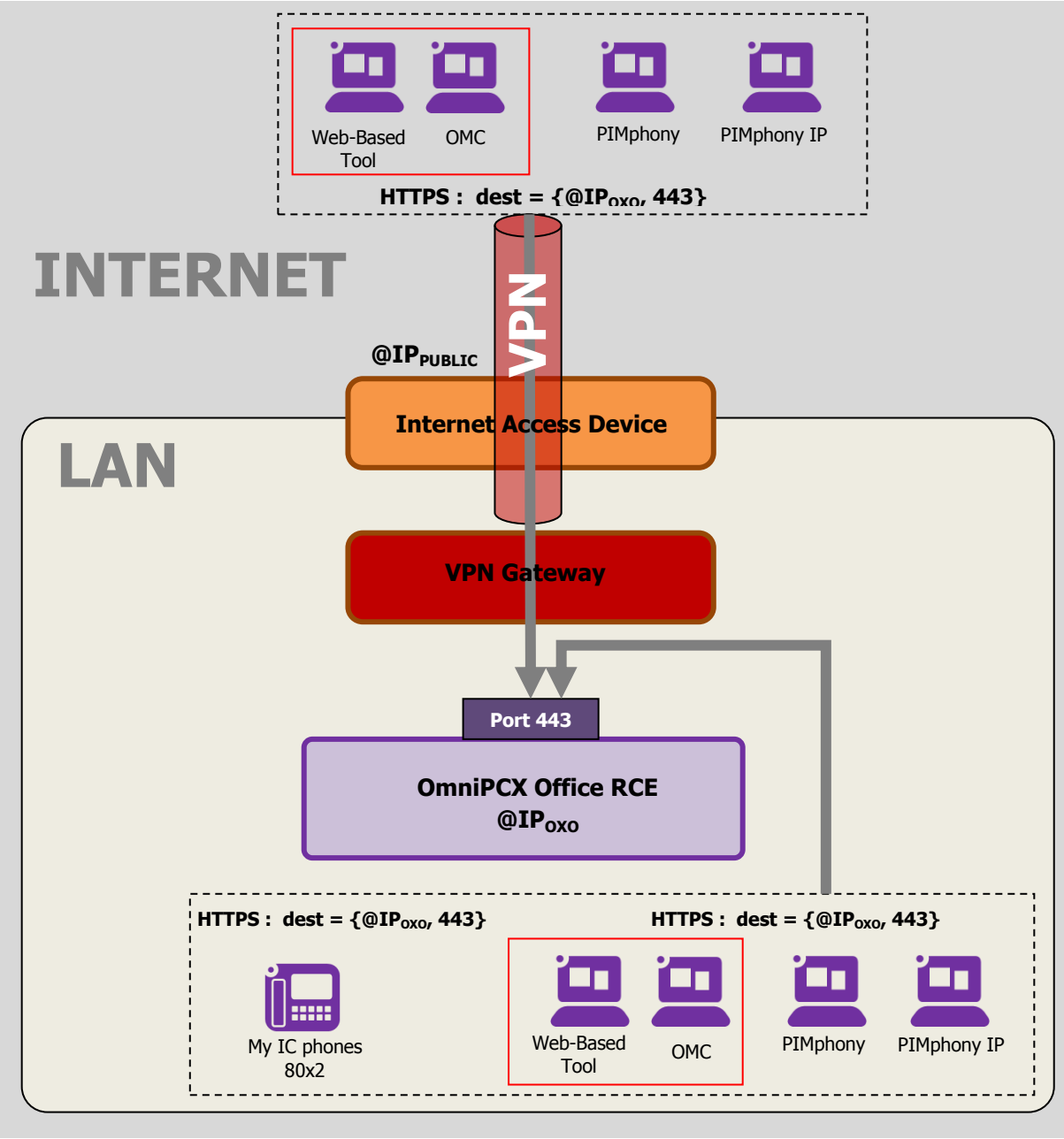


As a consequence, it is important to apply appropriate security measures in the firewall/Internet Access Device configuration to enable secured remote access to the OXO system server.

Remote access must be enabled only if required. If remote access is required, please apply carefully the recommendations of the next sections depending on the version of your product.

3.2 Remote access to OmniPCX Office RCE before R820

Before R820, a VPN connection is mandatory to allow remote access to OmniPCX Office RCE services between an application connecting from the Internet and the customer's LAN.
Note that VPN services are not provided by the OmniPCX Office RCE nor by the end user applications. The VPN connection requires additional software/equipments.
The security of such VPN solution is totally under the responsibility of the system's owner.



3.3 Remote access to OmniPCX Office RCE R820 and later

For R820 and above remote services via Internet are possible but require following these security principles: Note again that OXO system is connected to the LAN and not directly to the Internet. The system differentiates connections originated from the Internet from the LAN based on the ports addressed on the OXO system itself:

- Ports 443 and 10443 are dedicated to connections from the LAN,
- Port 50443 is dedicated to connections from the Internet and it applies adapted access control policies

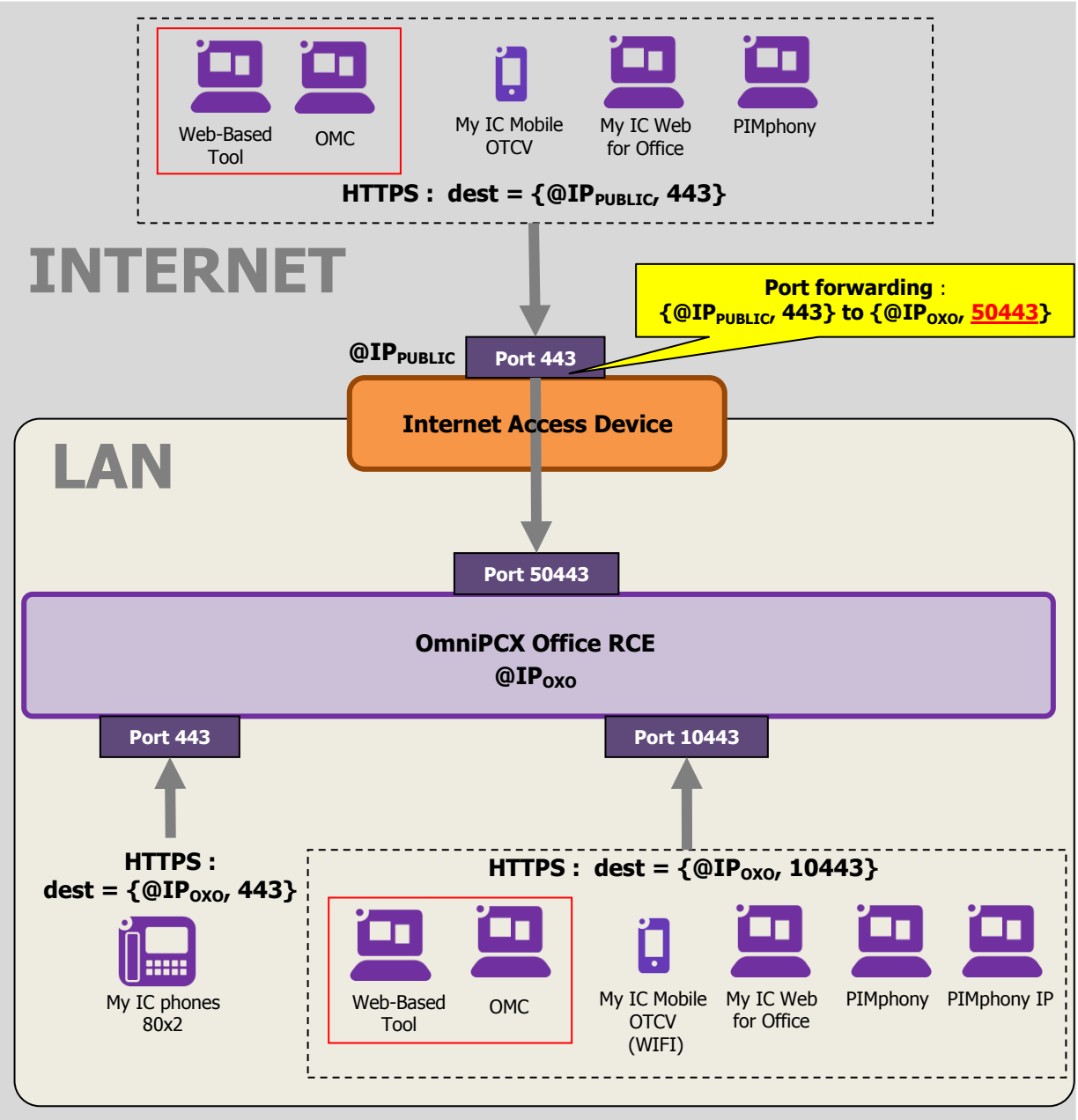


Fig. 1 : OmniPCX Office RCE R820

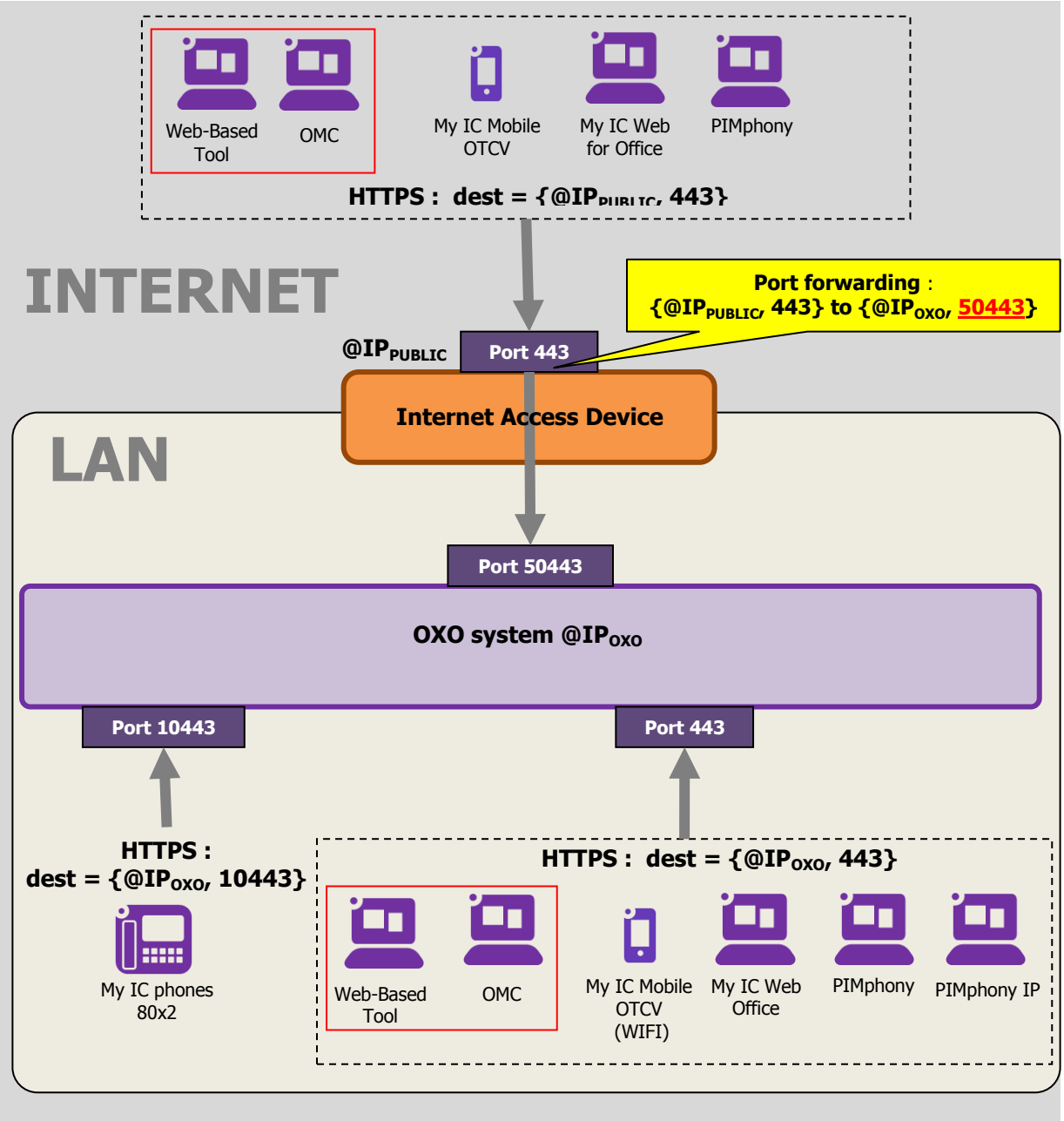


Fig. 2 : OmniPCX Office RCE R900 and later

Any remote access from the Internet is received on the public interface of the Internet Access Device that forwards the received traffic to the OXO system in the LAN.

Applications connecting from the Internet to the OXO system must use the HTTPS protocol. The default destination port used by the applications is the standard HTTPS port 443. In some cases another port may have to be used: see next section for explanation.

Port forwarding must be configured at the Internet Access Device to forward incoming traffic received on the public port 443 to the port 50443 of the OXO system :

Forward {@IP$_{PUBLIC}$, port 443} to {@IP$_{OXO}$, port **50443**}


Warning

Security rules:

- For remote access from the Internet forwarded to the OXO system, the destination port at the OXO system must always be port 50443.
- Never forward any traffic from the Internet to another port of the OXO system than port 50443, except those explicitly required for the activation of IP trunking services.
- Never forward any traffic from the Internet to ports 443 or 10443.


Note

My IC Phone terminal uses the port 443 on OXO in LAN on release 820. It then uses the port 10443 on OXO in LAN on all releases above 820.


Note

A VPN based connection can still be used in this topology for remote applications (see section 3.2).


Important

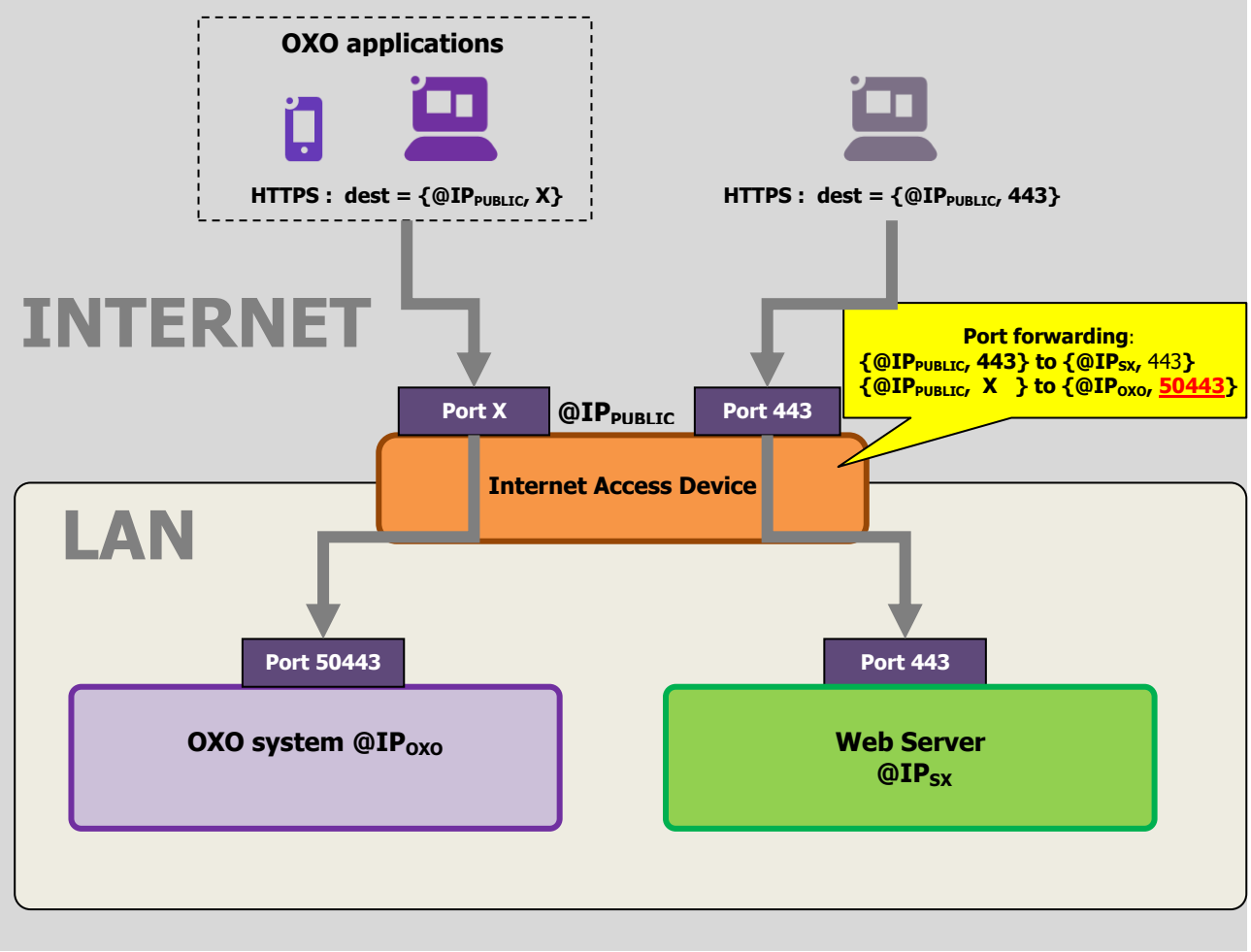
In case of remote connection, the VPN based solution is the only supported case for PIMphony IP.

3.4 Remote access to OXO system if public port 443 is already used

It is assumed that there is only one public IP address allocated to the Internet Access Device.
If another HTTPS server (e.g. web server) is connected to the LAN in addition to the OXO system, different ports at the Internet Access Device must be used to address each server from the Internet. One port can still be the standard HTTPS port 443. The other port can be any unused port of the Internet Access Device.
Note again that the destination port used by the applications connecting to the OXO system from the Internet is not a port of the OXO system, but a port at the public interface of the Internet Access Device. Any traffic

received on this public port is then forwarded by the Internet Access Device to the local port 50443 of the OXO system in LAN.

Example:



Generic configuration:

- To connect to the OXO system from the Internet, use destination address {@IP_{PUBLIC}, port X}
- To connect to the web server from the Internet, use destination address {@IP_{PUBLIC}, port 443}

Port forwarding must be configured accordingly at the Internet Access Device:

- Forward {@IP_{PUBLIC}, port X} to {@IP_{OXO}, port 50443}
- Forward {@IP_{PUBLIC}, port 443} to {@IP_{SX}, port 443}

Warning

Security rules:

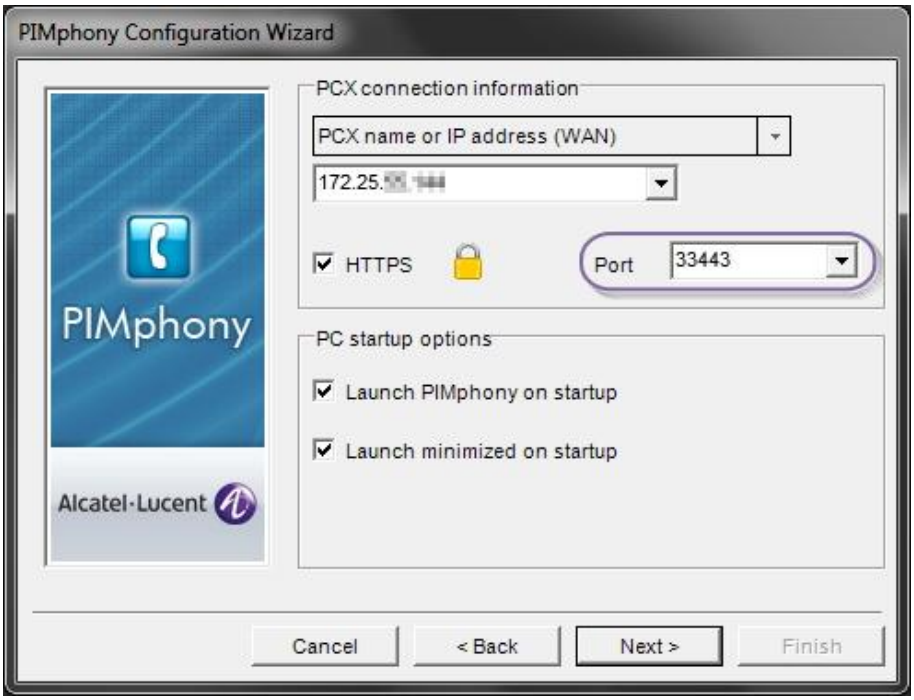
- For remote access from the Internet forwarded to the OXO system, the destination port at the OXO system must always be port 50443.
- Never forward any traffic from the Internet to another port of the OXO system than port 50443, except those explicitly required for the activation of IP trunking services.
- Never forward any traffic from the Internet to ports 443 or 10443.

3.4.1 End user application configuration of connecting port

If another destination public port than the standard HTTPS port 443 is used on the Internet Access Device, it must be then configured as the new destination port for each end user application.
Note that you may use any unused port of the Internet Access Device. The same port should be used for all applications.

3.4.1.1 PIMphony

For PIMphony (PIMphony associated to a physical set of the OXO system) the destination port used for remote connection must be defined in the Configuration Wizard:

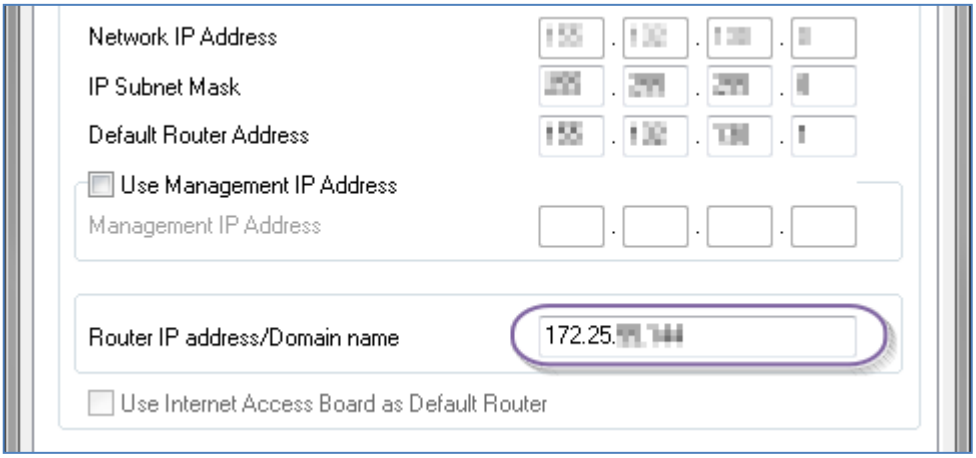


3.4.1.2 My IC Mobile / OpenTouch Conversation (OTCV)

The public URL used by the application to connect from the Internet is defined in the application's configuration file. By default the destination port is 443. To use another port it must be configured with noteworthy address "**ExtHttpsPo**".

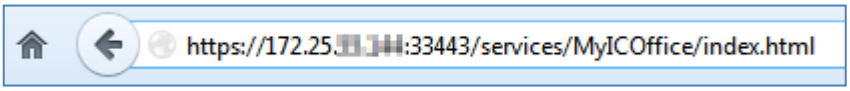
For example if you use port 33443 ExtHttpsPo has to be set to 82 A3 (Hex)

The public URL or IP address is defined in OMC \ Hardware & Limits → LAN configuration → Router IP address/Domain name



3.4.1.3 My IC Web for Office

My IC Web for Office is a web application: the destination port can be defined in the web browser.

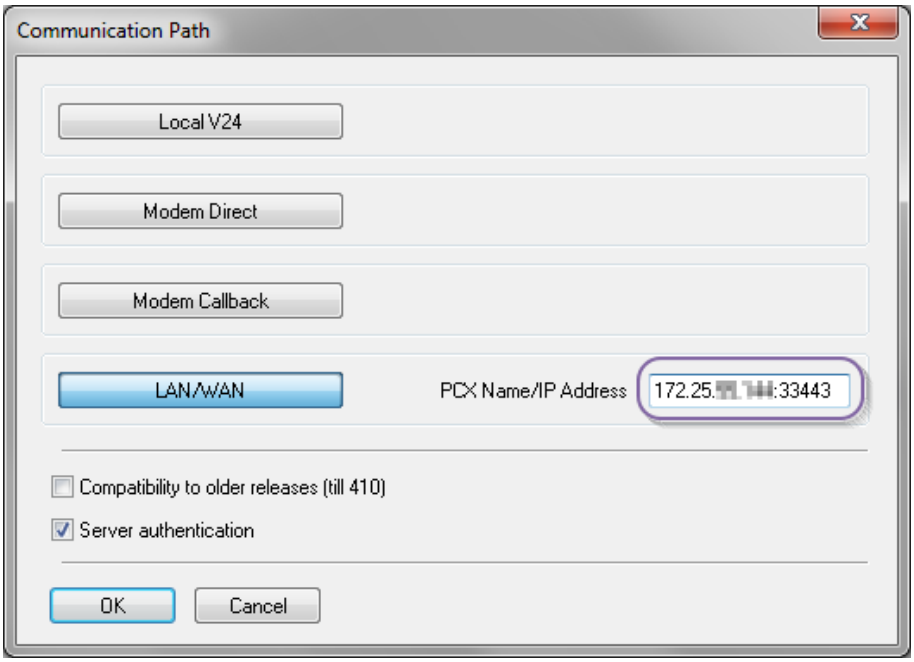


3.4.2 Management application configuration of connecting port

If another destination public port than the standard HTTPS port 443 is used on the Internet Access Device, it must be then configured as the new destination port for each management application.
Note that you may use any unused port of the Internet Access Device. The same port should be used for all applications.

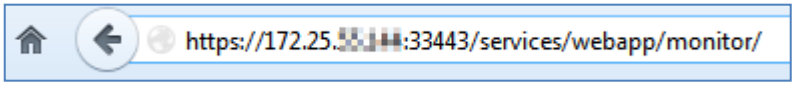
3.4.2.1 OMC

By default the destination port is 443.
The destination port can be defined with the system's host name / IP address in the connection popup window:



3.4.2.2 Web-Based Tool

Web-Based Tool is a web application: the destination port can be defined in the web browser.



4 System security programming options

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

4.1 All Releases – Account code table

Important

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:

4.2 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

4.3 R310 up to current Release – User Feature Right "Remote customization"

Remote customization right can 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.


Important

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.


Note

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


Warning

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

4.4 R310 up to current Release – 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.


Important

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).


Reminder

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


Note

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.


Warning

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

4.5 R310 up to current Release – 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

Important

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).

Note

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.

Warning

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

4.6 R710 up to current Release – 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".

Important

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).

Warning

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

4.7 R510 up to current Release – Callback feature in voicemail box / user feature right "Callback in VM Consultation"

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).

Note

Since R10.1, the new user feature right "Callback in VM Consultation", disabled by default, allows to forbid/authorize callback for each user (in OMC: Users/Base stations List - Details - Features - Feature Rights Part 3).

That means that the CallCorres noteworthy address cannot be used anymore. When upgrading from R10.0 or lower to R10.1 or higher, the Callback in VM Consultation option is disabled for all users, regardless of the value configured for the CallCorres noteworthy address.

Warning

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

4.8 Since R820 – User feature right "WAN API Access"

This user feature right was introduced in R820, it's also available in all newer software releases and versions. "WAN API Access" is a user feature right that permits to enable or disable WAN access on a user by user basis for requests coming from the WAN on OXO systemport 50443.
WAN access can be disabled /enabled via OMC: Users/Base stations List - Details - Features - Feature Right Part 1 – "WAN API Access".

Important

Only enable WAN access for a user in case that the user needs an application, such as My IC Web Office or PIMphony via a WAN access connection. It is strongly recommended to configure in accordance with Chapter 3 if you allow WAN access to the OXO systemand its users.

Warning

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

4.9 Since R820 – Feature to forbid any LAN/WAN connections

The noteworthy address called **ExtLnkClsd** has been introduced in R8.2 since first version. This flag permits to forbid all connection to the OXO system from the WAN and the LAN, except OMC which is still allowed under respect of recommendation given in the chapters above.

Important

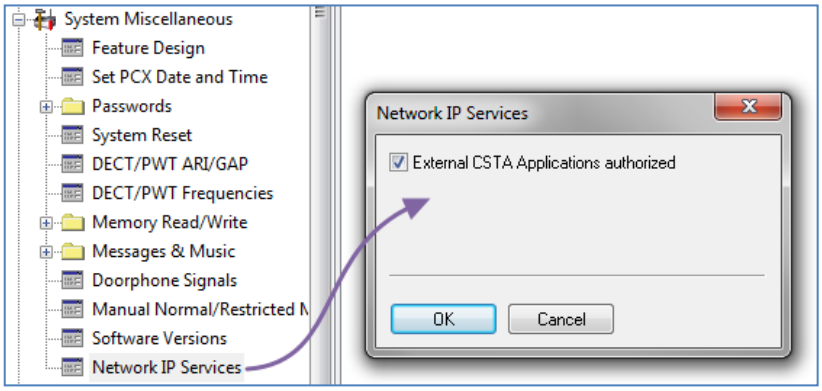
By default all connections are opened, **ExtLnkClsd** = 00. To close the current opened connections the flag has to be set to 01, a reboot is mandatory.

Warning

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

4.10 Since R820 – External CSTA Applications access control

Since R820, access for external CSTA applications connecting to OXO can be enabled / disabled through a configuration flag in OMC.



Reminder

From R8.2 up to R9.2 the default value for External CSTA applications access control to OXO is country dependant.

Important

From R10.0, the default value for External CSTA applications access control to OXO is disabled by default for all targets.

Note

During the migration from OXO release < R10.0 to R10.0, the access configured (enabled or disabled) for external CSTA applications in the earlier release is restored to R10.0. For example, if the access for external CSTA applications connecting to OXO is enabled in earlier release then the access is restored as enabled in R10.0 after migration.

Warning

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

4.11 Since R10.0 – Certificate management

The certificate management is improved in R10.0 by allowing the import of custom certificates signed by external authorities, the creation of a local certification authority and the management of a trust store.
The trust store contains well known certification authorities and can be populated with additional certificates by installer.

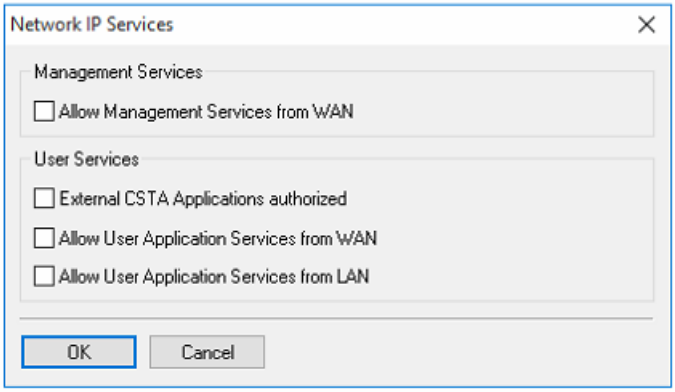
The security is also enhanced in OMC, which now provides strong authentication of the server certificate. Certificates are managed through the Web-Based Tool. From R10.2 signature algorithm of dynamic certificate and local CA certificate of OXO is changed from "SHA1- with RSA Encryption" protocol to "SHA256-with RSA Encryption" protocol.

For a detailed description please read Expert Documentation chapter 13 - Security / Certificate management.

4.12 Since R10.2 : Access control to management services and user services

In OMC, under the category system miscellaneous -> Network IP services, three new options are included to enable/disable the following categories :

- Management services from WAN
- User application services from WAN
- User application services from LAN



- Allow Management Services from WAN : In case of fresh installation of R10.2, this option is disabled by default, resulting that management services are not allowed in WAN. In case of migration from release <= R10.1 to R10.2, the management services from WAN is allowed by default. So it is up to the installer to disable them, if necessary.

- Allow User Application Services from WAN : In case of fresh installation of R10.2, this option is disabled by default, resulting that end user applications are not allowed from WAN.
  In case of migration from release <= R10.1 to R10.2 :

Before migration (<= OXO R10.1)	After migration (OXO R10.2)
ExtLnkClsd = 0	User Application Services from WAN : Not allowed
ExtLnkClsd = 1	User Application Services from WAN : Allowed

  When "Allow User application services from WAN" is disabled, "WAN API Access" right for each subscriber has no effect.
  When "Allow User application services from WAN" is enabled, "WAN API Access" right for each subscriber has to be enabled to allow WAN access for the corresponding subscriber.
- Allow User Application Services from LAN : In case of fresh installation of R10.2, this option is enabled by default, resulting that user applications are allowed in LAN.
  In case of migration from release <= R10.1 to R10.2 **:**

Before migration (<= OXO R10.1)	After migration (OXO R10.2)
ExtLnkClsd = 0	User Application Services from LAN : Not allowed
ExtLnkClsd = 1	User Application Services from LAN : Allowed

Important

- After changing the configuration in OMC to enable/ disable "Allow Management services from WAN" and/or "Allow User application services from WAN" and/or "Allow User application services from LAN" options, the OmniPCX Office RCE **goes for warm reset** to make these changes into effect.
- Noteworthy address ExtLnkClsd is no more used in R10.2 (it is still present in the list but without any effect) The options "Allow User application services from WAN" and "Allow User application services from LAN" have to be used instead
- WAN/LAN access : see section 3.3 Remote access to OmniPCX Office RCE R820 and later

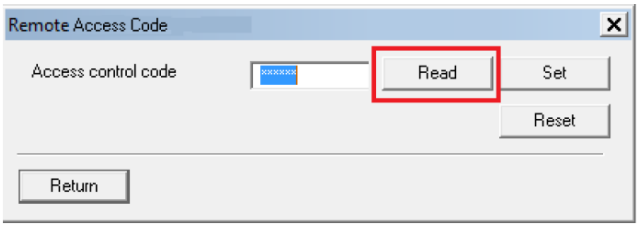
4.13 Since R10.3

4.13.1 Random Access control Code generation for Remote Access

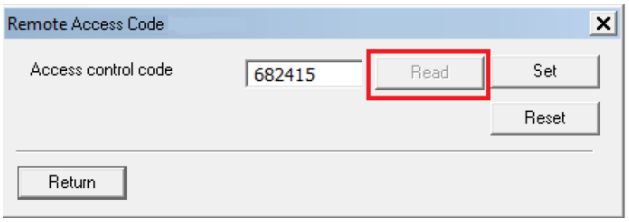
From OXO R10.3, "Access control code" has system generated random value by default after fresh installation of OXO. This "Access control code" is used for following Remote access services and is global to the system :

- Remote Substitution
- Remote access to Voice Mail

By default this "Access control code" is a 6 digit random value defined automatically by the system.
The system administrator and Installer can modify or delete the "Access control code" (0 to 16 digits).
The previous label in OMC "Remote Substitution Password" is renamed as "Remote Access code".
In OMC, "System Miscellaneous->Passwords->Remote Access Code" window, new "Read" option is provided to read "Access control code" as shown below.



On press of "Read", OMC will prompt for OMC current session password. After successful authentication of OMC session, the access control code is visible as shown in below figure.



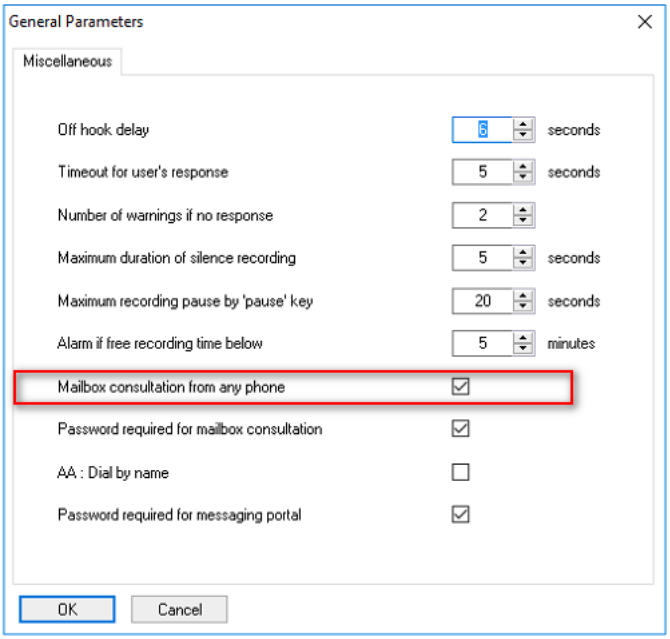
Warning Do not empty the Access control code field. Please keep the generated password or define a personalized password.

4.13.2 Voice mail consultation

4.13.2.1 Voice mail local consultation

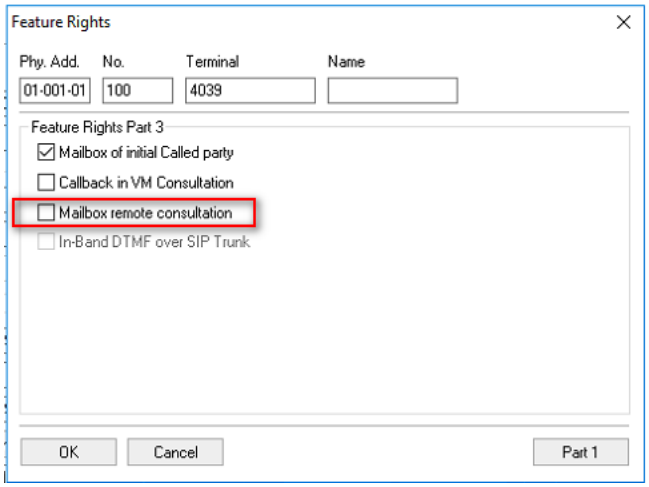
From OXO R10.3, the "Mailbox consultation" option is renamed as "Mailbox consultation from any phone". Enabling or disabling the option "Mailbox consultation from any phone" controls Voice Mail access from Local user phone. By default "Mailbox consultation from any phone" is enabled and consulting a handset's mailbox from another handset is authorized.
See menu OMC->Voice Processing->General Parameters

Warning When this option is disabled, consultation of the mailbox is possible only from the user's phone and not from another phone.



4.13.2.2 Voice mail remote consultation

From R10.3, to allow or deny explicitly remote consultation of voice mailbox over telephone network for each user, a new feature right "Mailbox remote consultation" is introduced in OMC->Subscribers/Base Stations List->Subscriber"s Details->Features and it is disabled by default.



If "Mailbox remote consultation" feature right is not enabled, external incoming call to voice mail will be rerouted to AA after playing the newly introduced pre-defined voice prompt "Remote access to voice mail is currently disabled".

Warning

If AA is not available :

- When External call is redirected to AA, call will be routed to Attendant group.
- When Local call is redirected to AA, call will be released

4.13.2.3 Summary table

Below table shows the behavior of Local and Remote access to VM with different configuration of "Mailbox Consultation from any phone" and "Mailbox Remote consultation".

Mailbox consultation from any phone	Mailbox Remote consultation	Local Access to VM	Remote Access to VM
Enabled	Enabled	Yes	Yes
Enabled	Disabled	Yes	No
Disabled	Enabled	No	Yes
Disabled	Disabled	No	No

Warning

- Voice Mail consultation over LAN/WAN using WS API is not controlled by the options "Mailbox Consultation from any phone" and "Mailbox Remote consultation".

4.13.3 Remote access to the general mailbox

New noteworthy address "RmAcGenMbx" is added to control the remote access to general mailbox:

- 00 : general mailbox remote consultation is not allowed – default value
- 01 : general mailbox remote consultation allowed.

5 System Security Programming Summary

5.1 Noteworthy addresses and system option

5.1.1 Global system options

	VMUMaxTry	VMUMaxTry	PerAssAlwd	PerAssAlwd	DivRemcust	Callcorres
default value	20 (old value)	03	01 (old value)	00	00	country dependent
R3.1	*not available*[1]	310/060.001	310/055.001	*not availabe*[1]	*not applicable*[2]	*not availabe*[1]
R4.1	*not available*[1]	410/064.001	410/056.001	410/064.001	*not applicable*[2]	*not availabe*[1]
R5.1	*not available*[1]	510/058.001	510/035.001	510/058.001	*not applicable*[2]	510/064.001
R6.1	610/015.003	610/033.001	610/012.001	610/031.001	*not applicable*[2]	610/052.001
R7.0	700/012.005	700/026.001	700/012.005	700/026.001	*in R710*	*in R710*
R7.1		710/022.001		710/022.001	710/028.001	710/097.001
R8.0		800/030.002		800/030.002	800/030.002	*in R820*
R8.1		810/045.003		810/045.003	810/045.003	*in R820*
R8.2		820/026.007		820/026.007	820/026.007	820/045.001
R9.0		900/033.002		900/033.002	900/033.002	900/037.001
R9.1		910/021.001		910/021.001	910/021.001	910/021.001
R9.2		All		All	All	All
R10.0		All		All	All	All
R10.1		All		All	All	Replaced by user feature right
R10.2		All		All	All	Replaced by user feature right
R10.3		All		All	All	Replaced by user feature right
OXO Connect R2.0		All		All	All	Replaced by user feature right

	ExtLnkClsd	External CSTA Applications access control
default value	disabled	country dependent in R8.2 to R9.2 Disabled in R10.0
R3.1=>R7.1	*not availabe*[1]	*not availabe*[1]
R8.0	*in R820*	*not availabe*[1]
R8.1	*in R820*	*not availabe*[1]
R8.2=>R10.1	All	All
R10.2	Without effect	All
R10.3	Without effect	All
OXO Connect R2.0	Without effect	All

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
3: *Without effect* means that still present in noteworthy address list but no more used
Version in blue means that it is the first version of this release

5.1.2 User Features

	User Feature "Remote customization"	User Feature "WAN API Access"	User Feature "Callback in VM Consultation"
default value	disabled	Disabled	*not available*[1]
R3.1	310/060.001	*not available*[1]	*not available*[1]
R4.1	410/065.001	*not available*[1]	*not available*[1]
R5.1	510/059.001	*not available*[1]	*not available*[1]
R6.1	610/047.001	*not available*[1]	*not available*[1]
R7.0	*in R710*	*not available*[1]	*not available*[1]
R7.1	710/069.001	*not available*[1]	*not available*[1]
R8.0	800/030.002	*in R820*	*not available*[1]
R8.1	810/045.003	*in R820*	*not available*[1]
R8.2	820/026.007	All	*not available*[1]
R9.0	900/033.002	All	*not available*[1]
R9.1	910/021.001	All	*not available*[1]
R9.2	All	All	*not available*[1]
R10.0	All	All	*not available*[1]
R10.1	All	All	All
R10.2	All	All	All
R10.3	All	All	All
OXO Connect R2.0	All	All	All

1: *Not available* means that the option is not available or that the indicated default value is not used in this release.
2: *Not applicable* means that the option 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

5.2 Passwords control and passwords check

	User password control (system)	Management password control (system)	User, Management and Admin SIP Phone passwords check (system) AutoPwdChk	OMC user password check and reset (only with OMC910/14.1b and above)[2]	Mandatory set of non-default value for user/management passwords
R3.1	*not available*[1]	*not available*[1]	*not available*[1]	yes	*not available*[1]
R4.1	410/064.001	*not available*[1]	*not available*[1]	yes	*not available*[1]
R5.1	510/058.001	*not available*[1]	*not available*[1]	yes	*not available*[1]
R6.1	610/047.001	*not available*[1]	*not available*[1]	yes	*not available*[1]
R7.0	*not available*[1]	*not available*[1]	*not available*[1]	yes	*not available*[1]
R7.1	710/057.007	*not available*[1]	*not available*[1]	yes	*not available*[1]
R8.0	800/030.002	*not available*[1]	*not available*[1]	yes	*not available*[1]
R8.1	810/045.003	*not available*[1]	*not available*[1]	yes	*not available*[1]
R8.2	820/026.007	*not available*[1]	*not available*[1]	yes	*not available*[1]
R9.0	900/033.002	*not available*[1]	*not available*[1]	yes	*not available*[1]
R9.1	910/021.001	910/021.001	910/021.001	yes	*not available*[1]
R9.2	All	All	All	yes	*not available*[1]
R10.0	All	All	All	yes	*not available*[1]
R10.1	All	All	All	Yes	Yes
R10.2	All	All	All	Yes	Yes
R10.3	All	All	All	Yes	Yes
OXO Connect R2.0	All	All	All	Yes	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

Connect with us on Facebook and Twitter for the latest:

- Software releases
- Technical communications
- AAPP InterWorking reports
- Newsletters

…and much more!


twitter.com/ALUE_Care


facebook.com/ALECustomerCare

Submitting a Service Request

Please connect to our eService Request application.

Before submitting a Service Request, please be sure:

- The application has been certified via the AAPP if a third party application is involved.
- You have read the release notes that list new features, system requirements, restrictions, and more, and are available in the Technical Documentation Library.
- You have read through the related troubleshooting guides and technical bulletins available in the Technical Documentation Library.
- You have read through the self-service information on commonly asked support questions and known issues and workarounds available in the Technical Knowledge Center.

- END OF DOCUMENT -