Administration and Configuration Guide TWP Version 4.1

AASTRA

Table of contents

6. Authentication methods 49

7. Users management 55

8. Directories and collaboration 67

1. Overview

1.1. Introduction

TWP Server is a gateway for business telephony.
Perfectly integrated into your computer's IT and telephony infrastructure, it significantly optimizes productivity and increases services for users. It enables all the PBX functions to be accessed through Web Service instructions. It enables you to centralize management for telephony functions.

1.2. Architecture

1.2.1. Introduction

The TWP architecture is composed of the following items:

- A server which acts as a gateway between the telephony world and the desktop IT world.
- A PBX or network with a TCP/IP access.
- Client sets (a computer and a telephone set associated with each user).

No applications need to be installed on the desktop PCs.
All types of telephone sets may be used: digital, analog, DECT, IP, "Soft Phone", etc. No modification of the workstation configuration is required.
Below is a list of external components which may benefit from TWP architecture:

- Customer databases
- Task applications
- Web applications
- Exchange or Lotus Notes base

- PBX database
- Mobile applications
- Microsoft components (Active Directory, domain controller, etc.)
- LDAP directory

1.2.2. Standard configuration

The TWP server connects telephone elements (PBX, telephone sets) with IT elements (data servers, users' PC).

1.3. Functionalities

1.3.1. Server

The TWP Server application is used to:

- Control the telephony using Web Services,
- Manage connections to other company directories (SQL, Exchange, LDAP, ODBC, Lotus),
- Manage the incoming and outgoing call logs for each user,
- Manage a reverse directory base,
- Manage directory access security,
- Define rights and services for user groups,
- Administer by remote (WEB),
- Manage the incident log.

1.3.2. Toolkit

TWP Toolkit is a development kit (API) based on Web Services. This kit lets you develop telephony functions completely transparently in your own applications. Specific documentation and tools are available on this CD-ROM.

1.3.3. Internet

TWP Internet lets you provide callback functions (double call transfer function).
Here are some examples of applications:

- "Call Back" buttons,
- E-mail message with automatic callback button,
- Telephony management for remote working

TWP Internet requires the development of Web applications, which means that you must have at least one TWP Toolkit license.

2. Server Installation

2.1. Configuration required

The configuration required depends on the number of users declared having access to the TWP services. For every configuration, you need a server with Windows Server 2008 R2 or Windows Server 2012.

2.1.1. Minimum configuration

- Before installing TWP, check that the server configuration respects the following conditions:
  - Operating system:
    - Windows 2008 Server (Standard, Enterprise, Web Edition versions)
    - Windows 2012 Server (Standard, Enterprise, Web Edition versions)

- Internet Information Services (IIS). IIS should be installed prior to TWP Server (See section below for Windows 2008 Server).

- Windows 2008 and 2012 Server requires an IIS configuration. The procedure is described in the appendix, Chapter 11.1.1.

2.1.2. Estimation of the storage volume required

The standard installation requires a minimum disk space of around 1 GB. However, the disk space required may increase significantly according to the number of users, the volume of the directories, the type of application installed and the site's activity.
A storage area of 40 GB will be enough in most cases; here are the rules to assess whether a greater storage area is required:

- A contact database (including all directories, private and public) with a total of between 250 000 and 500 000 entries, depending on the number of fields which are filled.

- The voice applications installed also increases the volume of data stored, at a rate of 2KB per second of voice recording

2.1.3. Environment

Rights: Administrator rights are required to install and operate the TWP Server.

Domain / Workgroup: There are two possibilities for integrating TWP Server into the company's network environment:

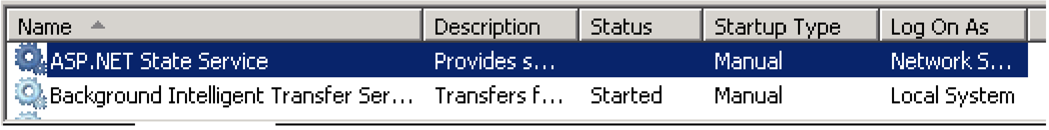
- Domain: In this case, the user rights are managed by the domain controller. The TWP Server must be registered in the domain.
- Workgroup: In this case, the users of each TWP client PC must be declared in the local database of TWP Server “Windows users”.

DHCP: The use of a fixed IP address is mandatory for the TWP Server.

2.2. First installation

***Caution**: Check that IIS is installed and configured before beginning the installation. If you are re-installing TWP, follow the indications in procedure 2.3 Server Update.*

***Caution**: Check also that the ASP.Net State Service is started before installing.*
It is possible from Windows Server 2012 SP1 or Windows Updates, this service is disabled. Reactivate it by right clicking on the service, choose Properties and then the Startup type to “Manual’, then do OK.
It will start anyway based on other services.



Name	Description	Status	Startup Type	Log On As
ASP.NET State Service	Provides s...		Manual	Network S...
Background Intelligent Transfer Ser...	Transfers f...	Started	Manual	Local System

Before launching the installation procedure you must connect as an administrator. Also check that the machine's name is definitive.

2.2.1. Unsupported applications

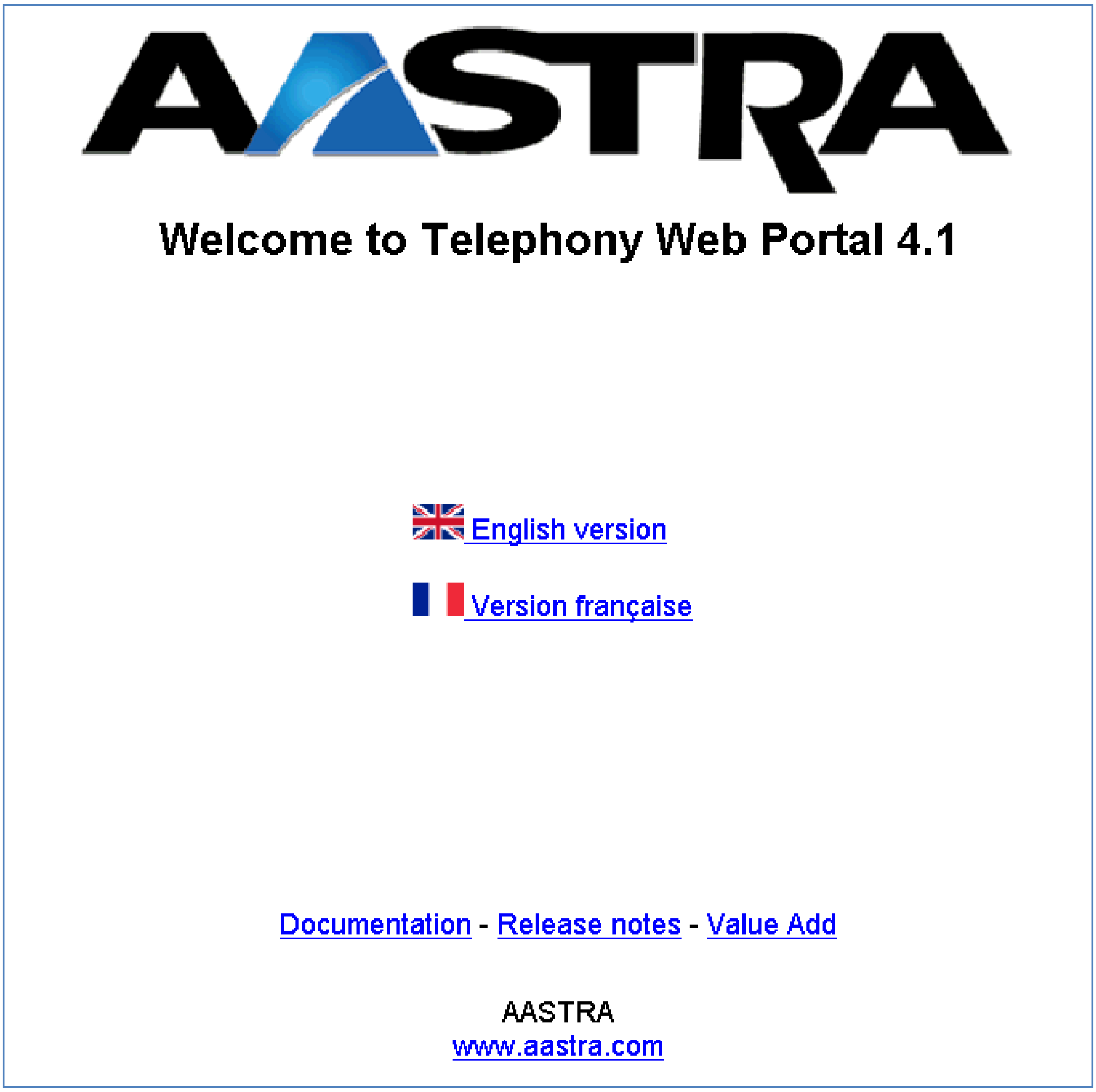
TWP Server is installed with several services which may conflict with already existing applications. Therefore, it is not advisable to have the following applications installed on the server receiving TWP Server:

- Install TWP server on a Primary Domain Controller
- Microsoft Exchange Server
- Any web server using port 80 (Apache server, etc.).

First uninstall these applications before going further with the installation.

2.2.2. Installation

Insert the Server CD-ROM or open the ISO file.
After a few seconds the screen below appears. If not, open the file autorun.html. The installation menu appears:



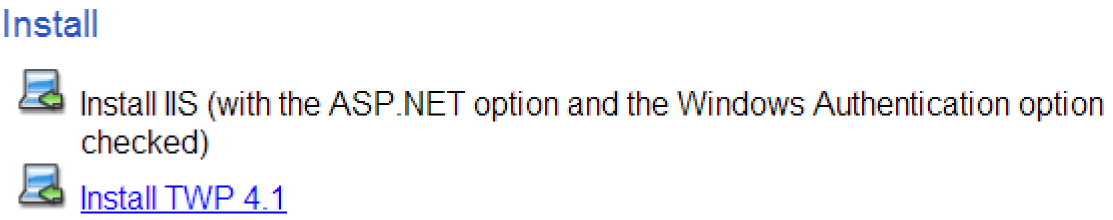
Welcome to Telephony Web Portal 4.1

English version

Version française

Documentation - Release notes - Value Add

AASTRA
www.aastra.com

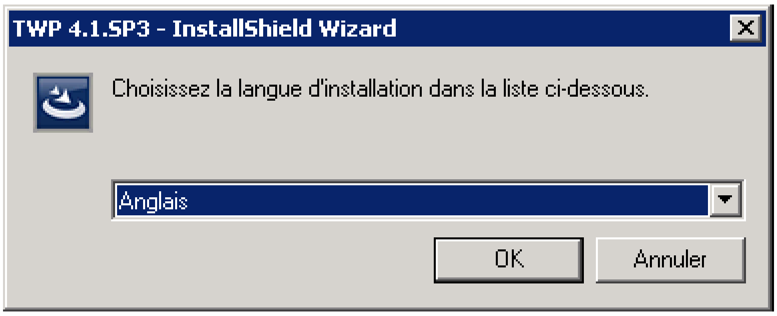


Install

Install IIS (with the ASP.NET option and the Windows Authentication option checked)

Install TWP 4.1

Choose the install option. Choose the language.

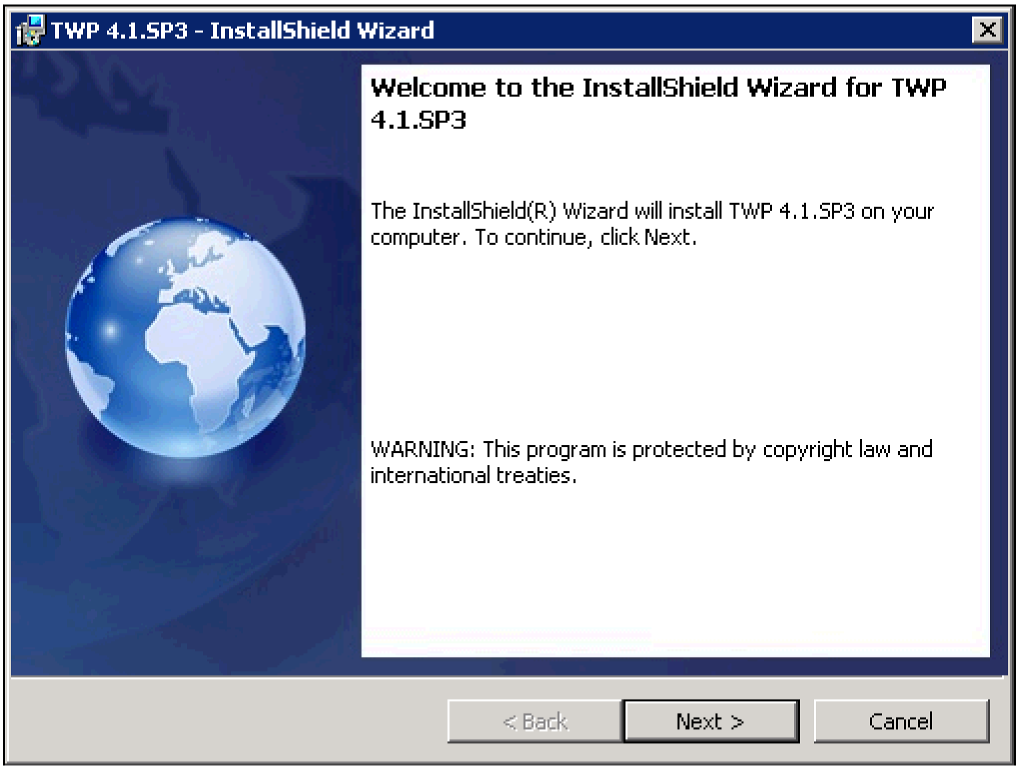


TWP 4.1.SP3 - InstallShield Wizard

Choisissez la langue d'installation dans la liste ci-dessous.

Anglais

Click on OK to install.



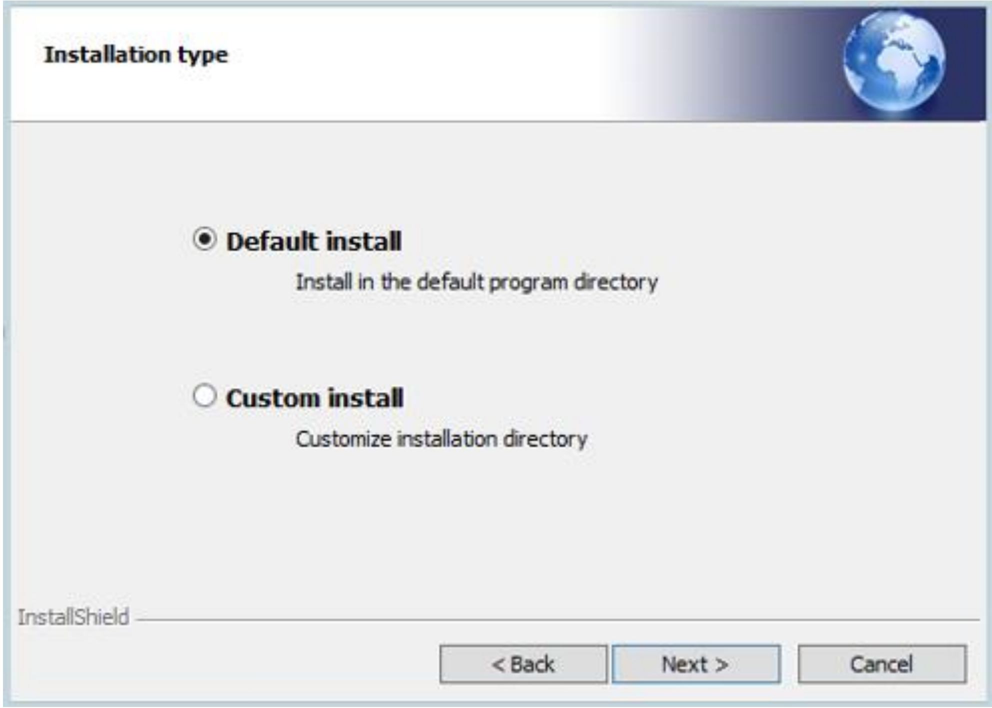
TWP 4.1.SP3 - InstallShield Wizard

Welcome to the InstallShield Wizard for TWP 4.1.SP3

The InstallShield(R) Wizard will install TWP 4.1.SP3 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Choose Next.



Installation type

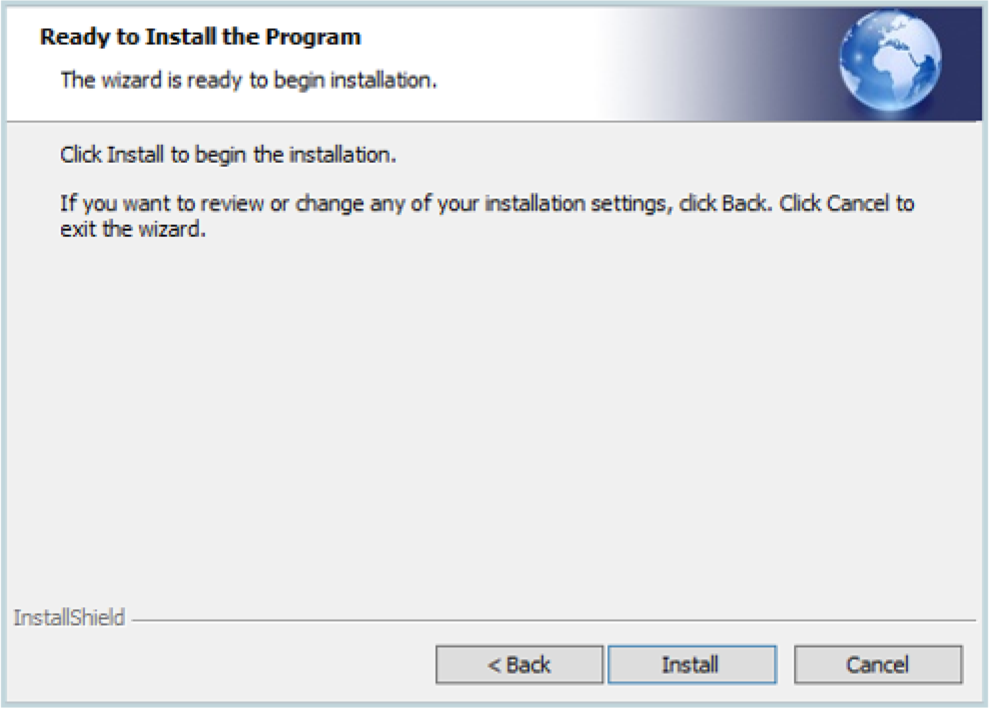
● Default install

Install in the default program directory

○ Custom install

Customize installation directory

Choose the default installation so that the application directory is in C:\Program Files…
Choose the custom installation to choose the directory.



Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Choose Install to continue and after that click finish to end the installation when it succeeds.

Now 2 icons are on the desktop:

- TWP Admin to access at the administration application
- TWP Caller to launch the application

2.3. Server update

2.3.1. Update from a version 4.1

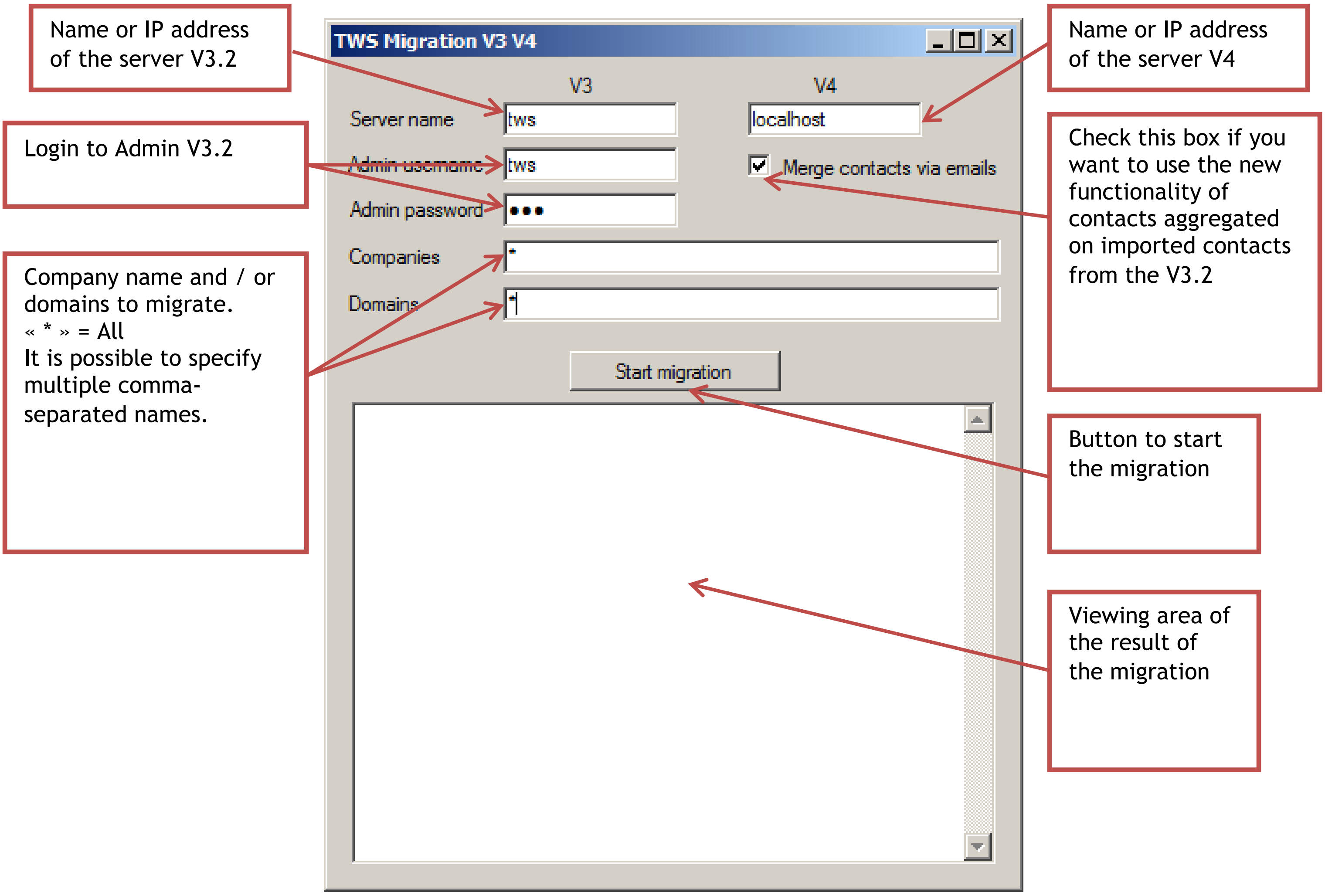
The CD-ROM provides the update from release 4.1.xxxx release 4.1.yyyy. Just follow the same procedure as the standard installation (chapter 2.2.2).

2.3.2. Update from a version 3.2

- Leave version 3.2 installed
- Install version 4.1 (see Chapter 2)
- Load the new license file in the Administration v4 (see chapter 3.3.1 and 3.3.2)
- Run the upgrade 3.2 to 4.1 tool (see next paragraph)
- Stop and disable all services of version 3.2

The upgrade tool is in the installation directory of TWP 4.1: “\TWS4\TWS_Tools\TWS_Migration_V3_V4“

Launch the EXE file named: “TWS_Migration_V3_V4.exe”.



TWS Migration V3 V4

	V3	V4
Server name	tws	localhost
Admin username	tws	☑ Merge contacts via emails
Admin password	●●●	
Companies	*	
Domains	*	

Name or IP address of the server V3.2

Login to Admin V3.2

Company name and / or domains to migrate.
« * » = All
It is possible to specify multiple comma-separated names.

Name or IP address of the server V4

Check this box if you want to use the new functionality of contacts aggregated on imported contacts from the V3.2

Button to start the migration

Viewing area of the result of the migration

When all fields of the configuration tool are filled, click "Start migration" button to begin the migration.
/!\ ATTENTION. All data on the V4 server will be deleted. The V3 server is not changed by this procedure.

Migrated data V3 include:

- Users of the administration
- Companies
- Domains
- The PBX links
- The bots groups
- The phone queues
- The collaboration servers
- The intercom groups
- Directories and Contacts
- The TWP users and their devices
- Groups
- Authorizations
- Contact lists
- The forward rules

Here is an example output of a correct migration:

```
------------- START --------------
Initialization...done
Dropping existing V4 databases...done
Authenticating on V3... done
Authenticating on V4... done
Creating admin users... 1 done
Creating applications... 20 done
Creating companies... 1 done
Creating domains... 1 done
Creating pbx links... 2 done
Creating directories... 7 done
Creating groups... 1 done
Creating users... 1 done
Creating bots groups... 1 done
Creating phone queues... 1 done
Creating scripts... 2 done
Creating collaboration servers... 0 done
Creating intercom groups... 0 done
Creating mail servers... 0 done
Creating SMS providers... 0 done
Creating Telenor links... 0 done
Creating callback groups... 0 done
Creating directory servers A5000... 1 done
Creating directory servers Intelligate... 0 done
Creating RCC connections... 0 done
Creating email configurations... 3 done
Creating authorizations... 14 done
Creating contacts... 3046 done
Indexing contacts... done
Set 'None' Authentication... Done
Importing user data...
1 users concerned
2 contacts lists done
6 personal contacts done
0 personal contacts not found
0 personal contacts failed
1 rules found
1 rules + 0 VM rules created
-------------- END ---------------
```

Note: Whatever the result of the migration from version 3.2, it will be useful:

- Restart the service TWS4$TWS_VTIXMLServices for the supervision of devices in intercom groups
- Configure as appropriate the devices of users in soft phone mode in the administration (see section 9.3)

2.3.3. Complete reinstallation

Before starting the installation, for security reasons, it is recommended to make a backup of the current configuration (see chapter 10.7).

Uninstalling

1. From the control panel start uninstalling Server
2. Delete all files in C:\Program files\tws4

Then reinstall as described in chapter 2.2.2.

3. Minimal server configuration

3.1. Company and domain

The TWP Server can be shared between companies, which are completely independent from each other.
Note: it is not possible to share resources between companies.

For each company, there is a concept of domain. A domain is a group of users who are in the same company with the same technical environment.
It is necessary to dispatch users to different domains when:

- They are not linked to the same IPBX system.
- They are not connected to the same email / calendar server.

Some information could be shared from one domain to another:

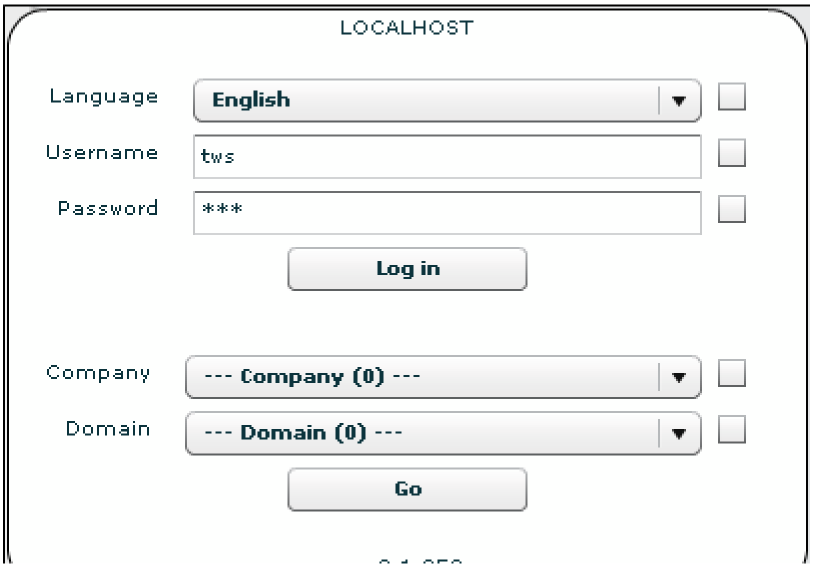
- Directories.
- Telephony presence.
- TWP status
- Calendar presence

3.2. Main steps to validate a standard installation

On TWP server desktop click the TWP_Admin shortcut. You should see the login form below in your browser.

To access the administration page, browse to the following URL:
http://servername/TWS3/TWS_Admin/TWS_Admin.HTML

The default user is "tws" and default password "tws".



LOCALHOST

Language: English ▼ □

Username: tws □

Password: *** □

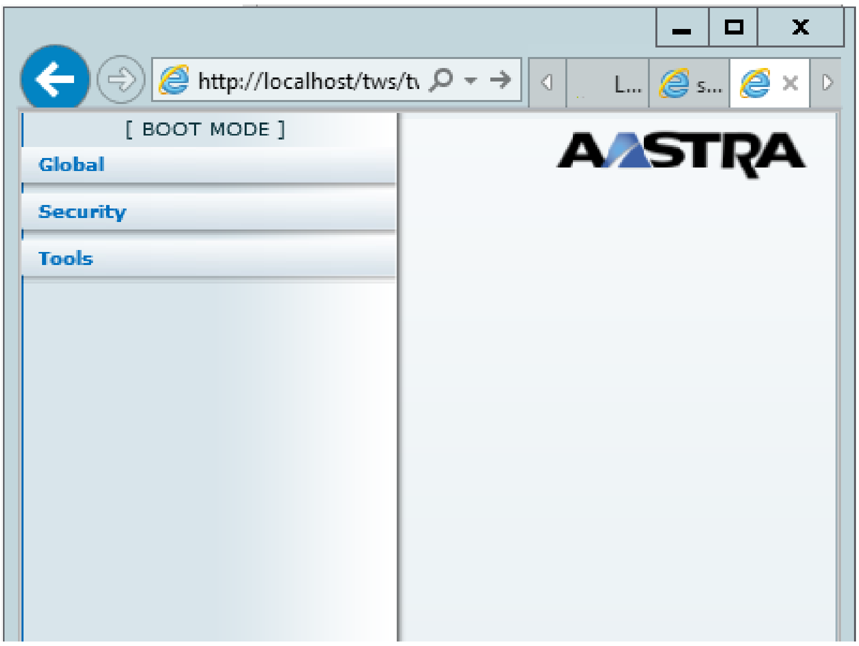
Log in

Company: --- Company (0) --- ▼ □

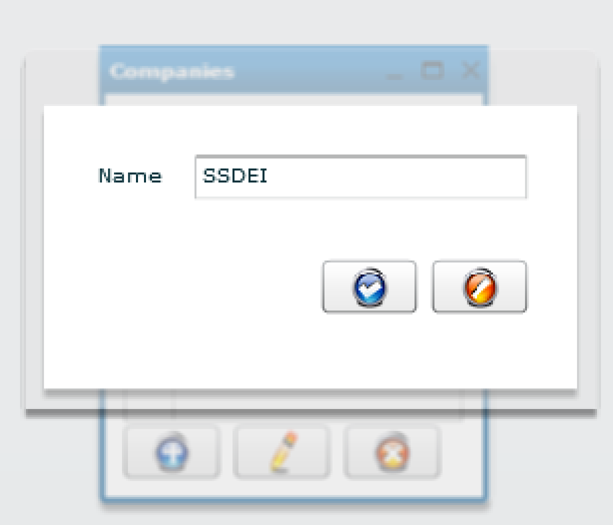
Domain: --- Domain (0) --- ▼ □

Go

Once user and password are entered, click go. You enter in "BOOT MODE".



You can now create your first company and domain.
To create a company, go to menu *Global / Companies* click on "+".

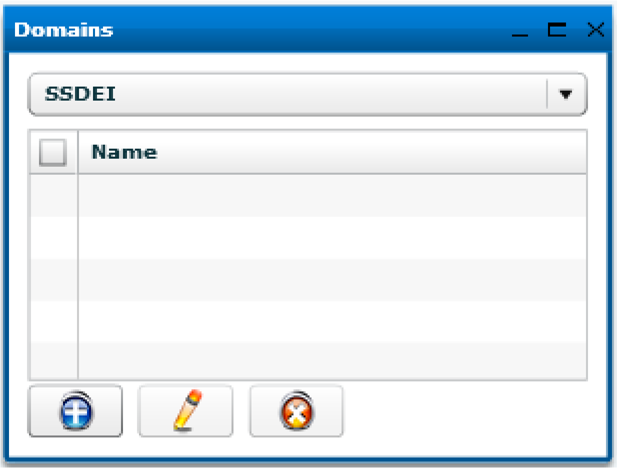


Name: SSDEI

Enter the company name and click on "*Save button*".

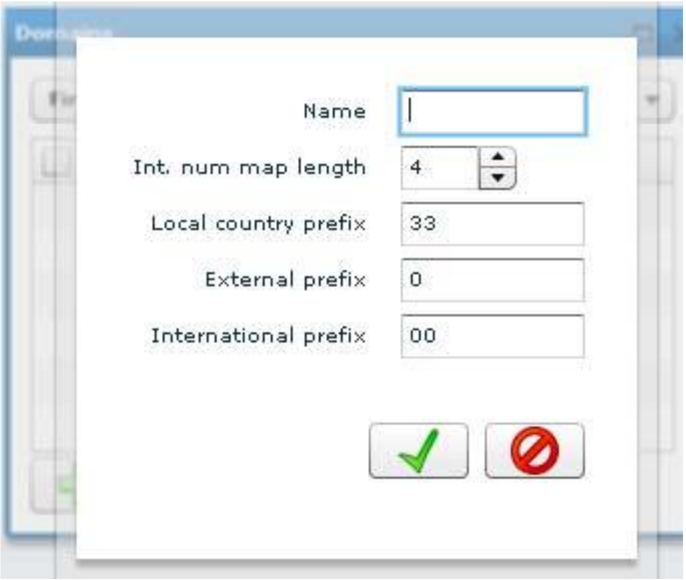
Note: Note that this company name will be in the applications in the users contact card configured later.

To create a domain on this company, select *Global / Domains*.
Note: If you create multiple domains and companies, please note that information can be shared between different domains but not between companies.



SSDEI

Select in the combo box the company in which you want to create your domain, and click on "+" button.



Name |

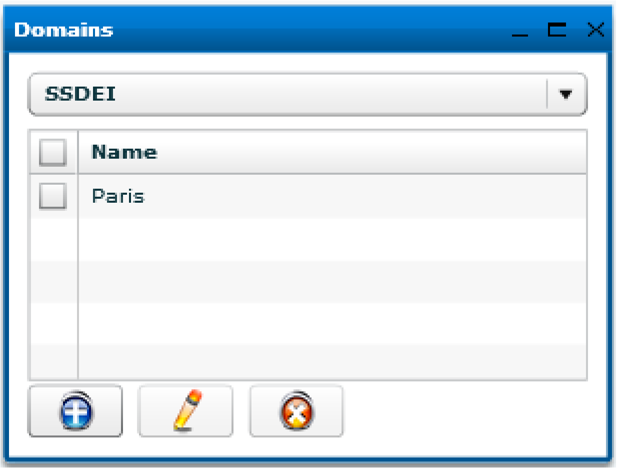
Int. num map length 4

Local country prefix 33

External prefix 0

International prefix 00

Enter the domain name and the numbering map length. This is the longest length of your internal phone number. Then click on “Save button”.



Domains

SSDEI

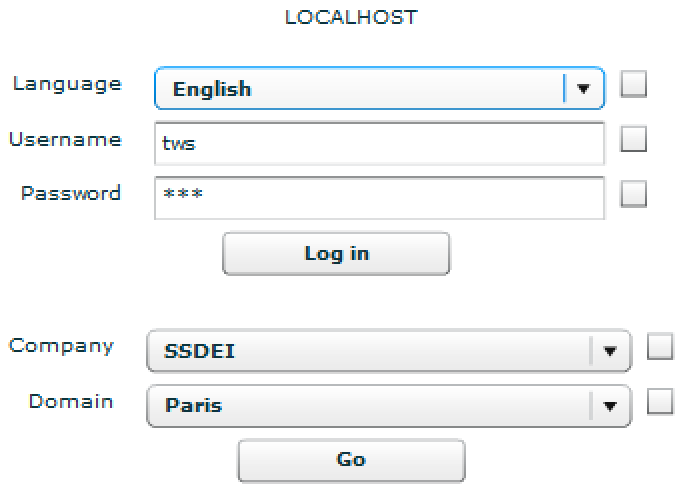
□	Name
□	Paris

Here we have created the domain “Paris” on company “SSDEI”.

Then click on log out button at the bottom of the page.

3.3. First domain configuration for standard installation

Select the company and the domain to configure.


LOCALHOST

Language: English □

Username: tws □

Password: *** □

Company: SSDEI □

Domain: Paris □

Click “go” to enter configuration.

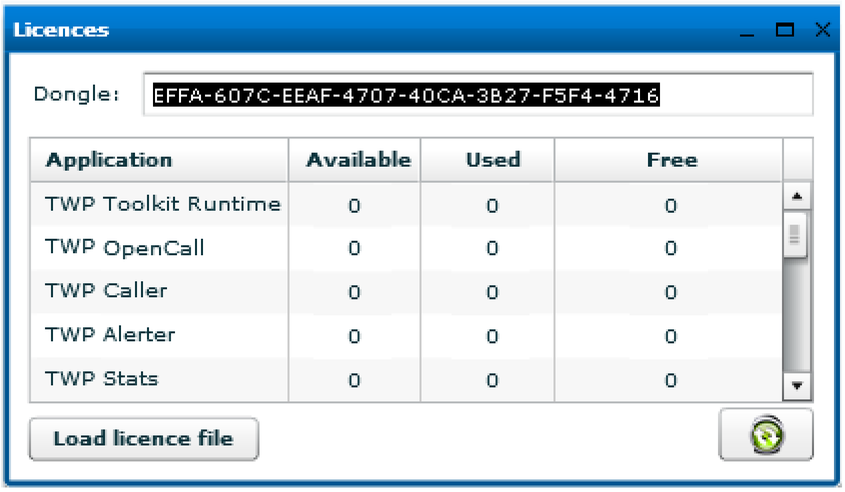
3.3.1. Installing licenses key file

If you do not have a license file, follow the steps below:

Get the Dongle id

Select *Security / Licenses* menu then copy the Dongle id which appears as follows:

<u>**Attention:**</u> For virtual machines, set the MAC address of the machine before retrieving the Dongle id.



Dongle: EFFA-607C-EEAF-4707-40CA-3B27-F5F4-4716

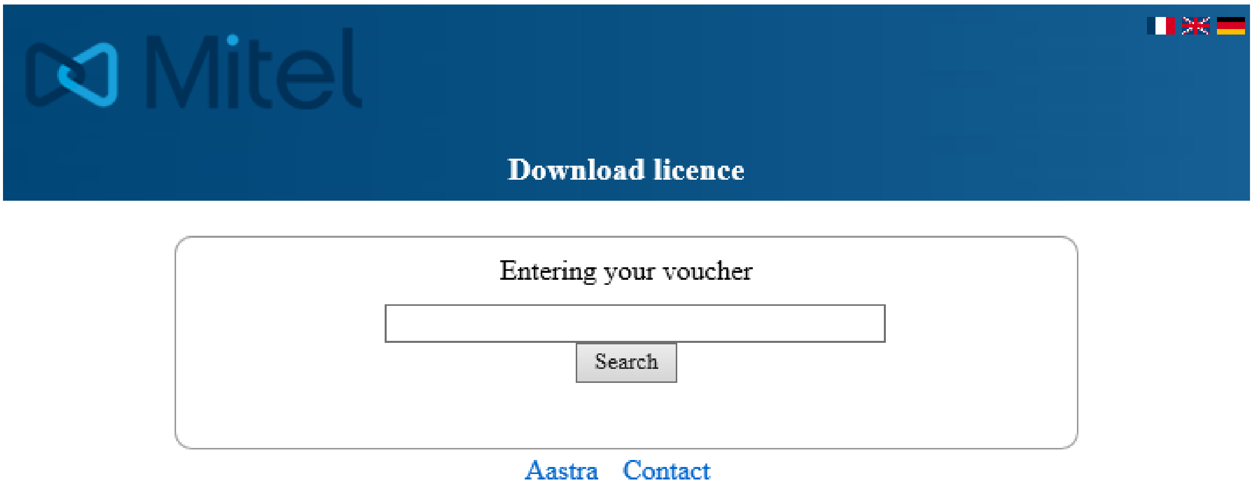
Application	Available	Used	Free
TWP Toolkit Runtime	0	0	0
TWP OpenCall	0	0	0
TWP Caller	0	0	0
TWP Alerter	0	0	0
TWP Stats	0	0	0

If no Dongle id appears on this licenses form, check if the Windows TWS4$TWS_WebServices service is started. If it is not, start the service and try again. Otherwise, contact your support.

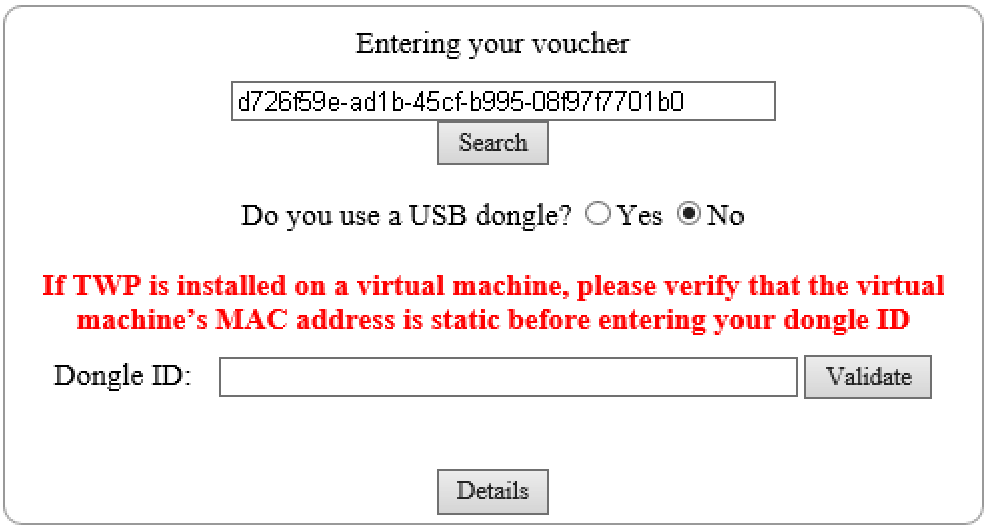
Retrieve the license certificate

Go to the following URL and enter your voucher received by email at the specified location.

http://register.algoria.fr/Licences/aastra.aspx



If your voucher is not yet associated with a Dongle id, you must first enter your Dongle id recovered from the administration, then click "Validate".



Entering your voucher

d726f59e-ad1b-45cf-b995-08f97f7701b0

Do you use a USB dongle? ○ Yes ● No

If TWP is installed on a virtual machine, please verify that the virtual machine's MAC address is static before entering your dongle ID

Dongle ID:

When your voucher is associated with your Dongle id, you can retrieve your license by:

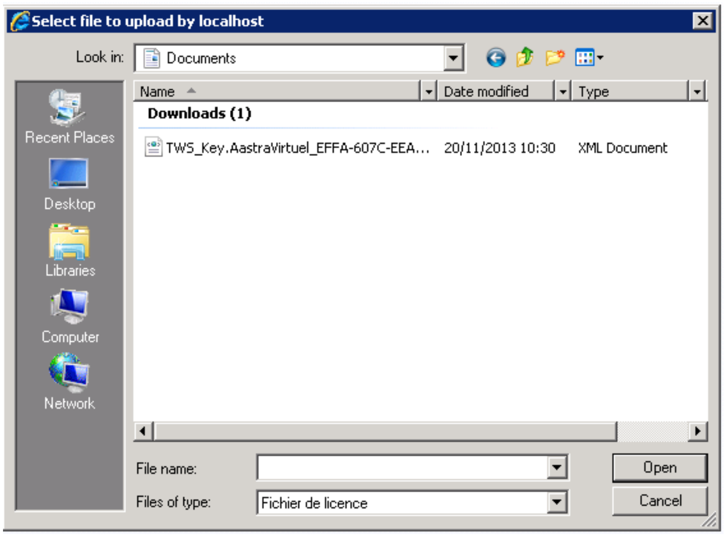
- Direct download by clicking on the "Get License" button
- By email by checking the box "For mail", indicating your email address and then clicking the "Get License" button.

You can access your order details by clicking on the "Details" button.

If you do not have a license file, contact your support.

3.3.2. Install the license file

In the administration, select the *Security / licenses* menu. Click on "Load license file" and select the file. Licenses ordered by the customer appear on the window after loading the file.



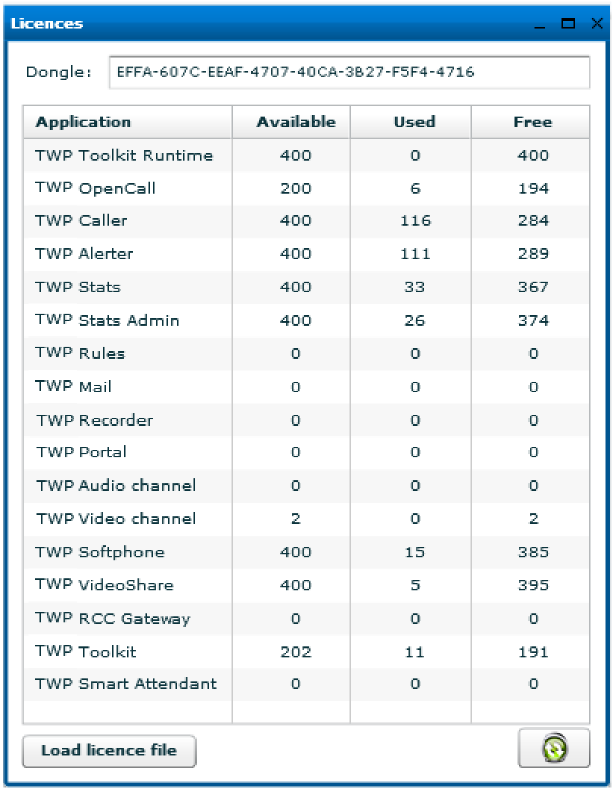
Downloads (1)

TWS_Key.AastraVirtuel_EFFA-607C-EEA... 20/11/2013 10:30 XML Document

File name:

Files of type: Fichier de licence

If no Dongle id appears on this licenses form, check if the Windows TWS4$TWS_WebServices service is started. If it is not, start the service and try again. Otherwise, contact your support.



Dongle: EFFA-607C-EEAF-4707-40CA-3B27-F5F4-4716

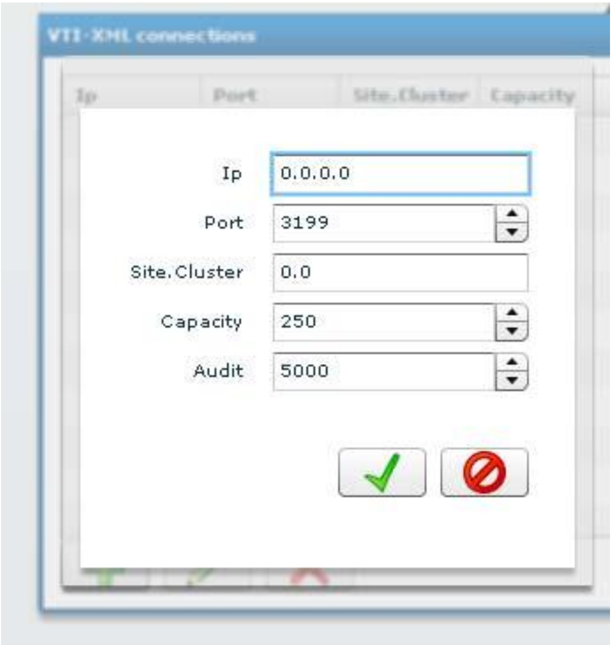
Application	Available	Used	Free
TWP Toolkit Runtime	400	0	400
TWP OpenCall	200	6	194
TWP Caller	400	116	284
TWP Alerter	400	111	289
TWP Stats	400	33	367
TWP Stats Admin	400	26	374
TWP Rules	0	0	0
TWP Mail	0	0	0
TWP Recorder	0	0	0
TWP Portal	0	0	0
TWP Audio channel	0	0	0
TWP Video channel	2	0	2
TWP Softphone	400	15	385
TWP VideoShare	400	5	395
TWP RCC Gateway	0	0	0
TWP Toolkit	202	11	191
TWP Smart Attendant	0	0	0

3.3.3. Create a PBX link

Configure a VTIXML link

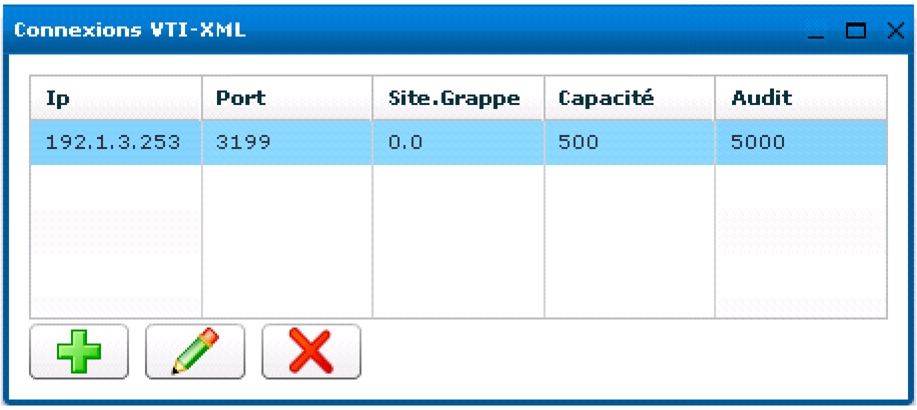
Select the *Connections / VTI-XML Connections* menu. Click on the "+" button and configure your link.

Fill with the IP address of your PBX, the default port is 3199 for VTIXML (never change this value).
It is possible to configure multiple links VTIXML under a multi-site/multi-node architecture, in this case it is important to mention the information *Site.Cluster*. Then set the number of maximum supported connections on each link.



Ip: 0.0.0.0
Port: 3199
Site.Cluster: 0.0
Capacity: 250
Audit: 5000

Click on the “Save” button.



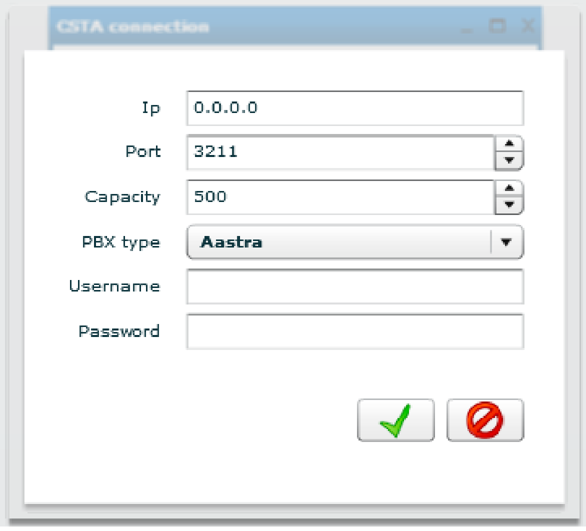
Ip	Port	Site.Grappe	Capacité	Audit
192.1.3.253	3199	0.0	500	5000

***Information:** You must restart the VTI-XML service if you have made changes.*

Configure a CSTA link

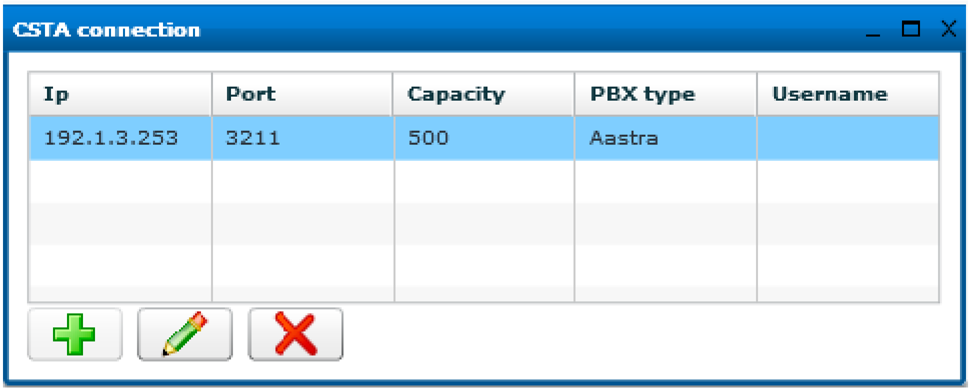
Select the *Connections / CSTA Connection* menu. Click on the "+" button and configure your link.

Fill with the IP address of your PBX, the default port for CSTA depends on the PBX type, set the username and password in case it is needed and the PBX type selected.



Ip	0.0.0.0
Port	3211
Capacity	500
PBX type	Aastra
Username	
Password	

Click on “Save” button.

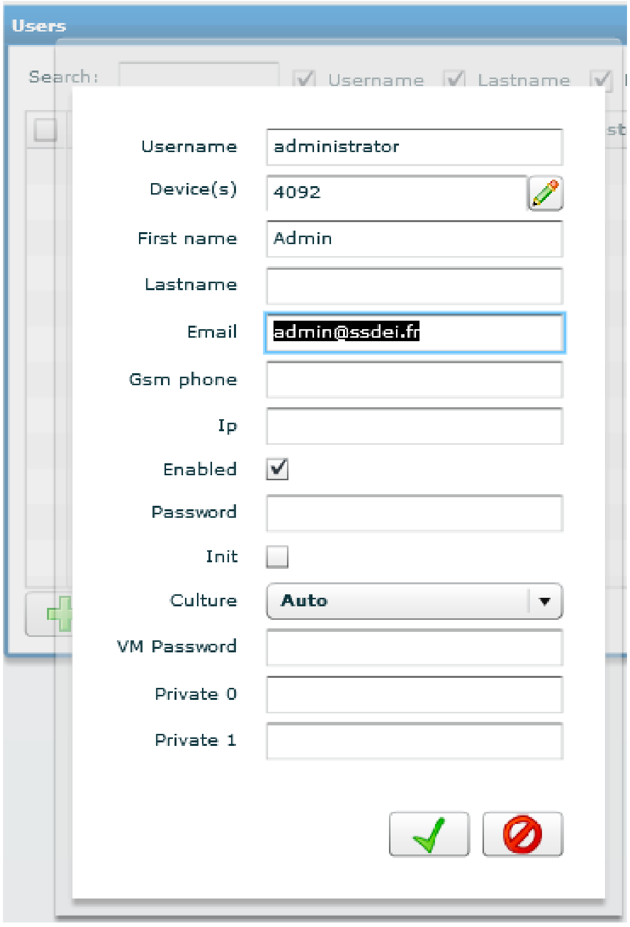


Ip	Port	Capacity	PBX type	Username
192.1.3.253	3211	500	Aastra	

Information: *You must restart the CSTA service if you have made changes.*

3.3.4. Create your first user

Select the *Users* / *Users* menu then click on "+".

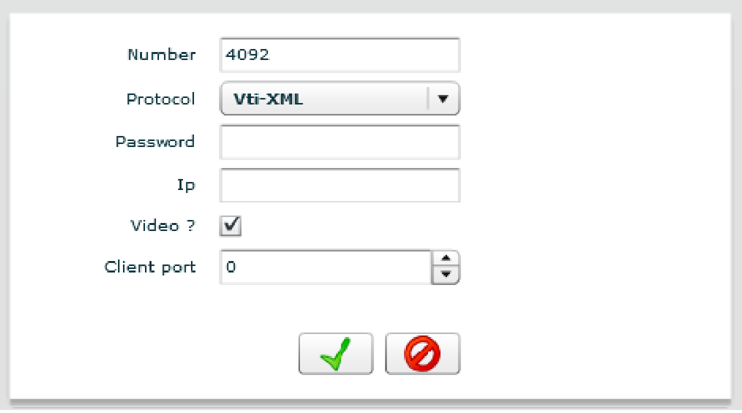


Username	administrator
Device(s)	4092
First name	Admin
Lastname	
Email	admin@ssdei.fr
Gsm phone	
Ip	
Enabled	☑
Password	
Init	□
Culture	Auto
VM Password	
Private 0	
Private 1	

- *User name*: If the Windows authentication is used, the user name must be the Windows login of the user on the domain. Otherwise, it is the login TWP the user must enter to authenticate.
- *First name* – *Last name* – *Gsm phone*: information displayed in the contact card of the user and available for application search feature.
- *Email*: the email address of the user is used by several TWP applications, for the management Calendar Presence status, unified voicemail and private contacts in particular. Verify that the email addresses are correct.
- *Ip*: not fill anything. The IP address can be used for an authentication process.
- *Enabled*: Enable or disable a user
- *Password*: If the authentication process selected for the user is TWP then this password field must be filled.
- Culture: sets the language selected by default in user applications.
- *VM Password* is the PBX voicemail password.

Fields of the device object of a user.

- *Number*: Number of the device.
- *Protocol*: depending of the PBX: VTIXML- CSTA....
- *Password*: Not used on CSTA protocol but important for the VTIXML protocol
- *IP*: Optional, used for Recorder
- *Video*: Enable or not the video point to point for the user

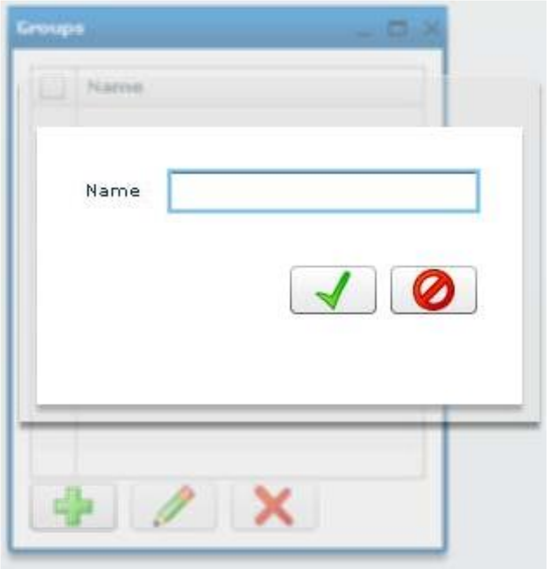


Number	4092
Protocol	Vti-XML
Password	
Ip	
Video ?	☑
Client port	0

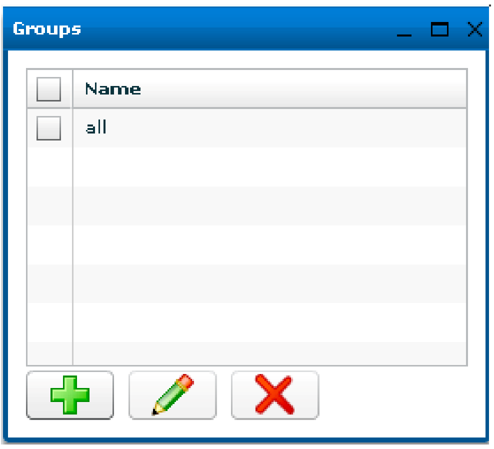
Save the device information and the user one too to ensure that any changes are taken into account.

3.3.5. Create your first users group

Select *Users / Groups* menu and click on “+”.

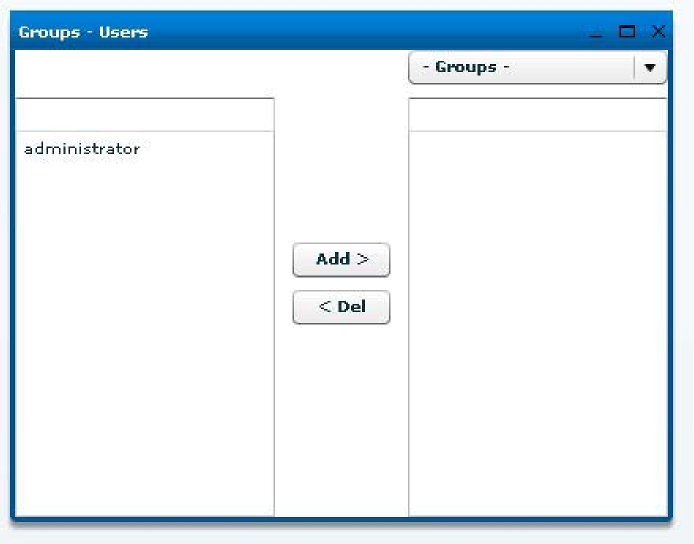


Enter a name for this new group: "All" for example and save.

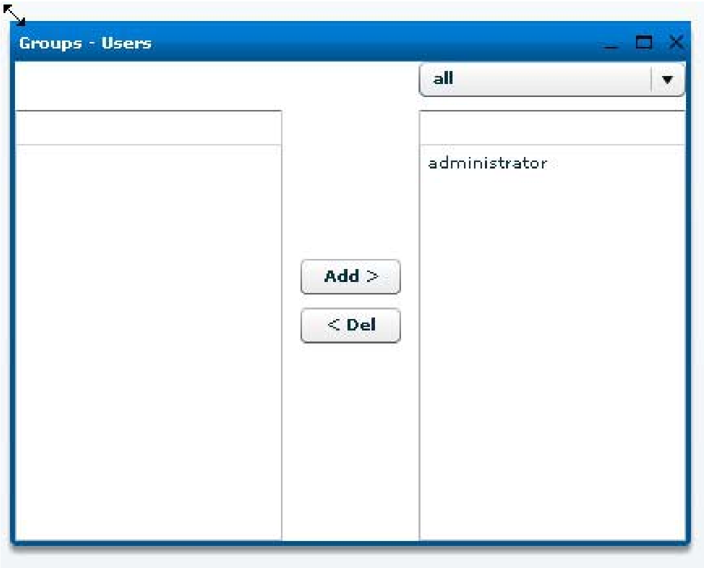


3.3.6. Add your first user in a group

Select *Users / Groups - Users* menu.

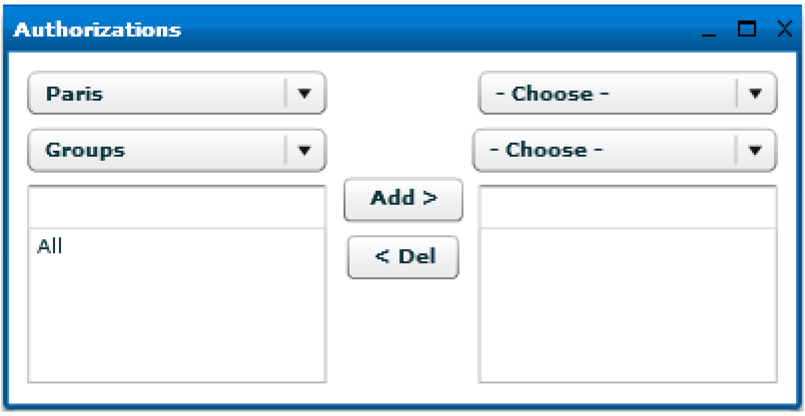


Select the group “all” from the list box. Add the user in the group: select the name of the user and click on *Add*.



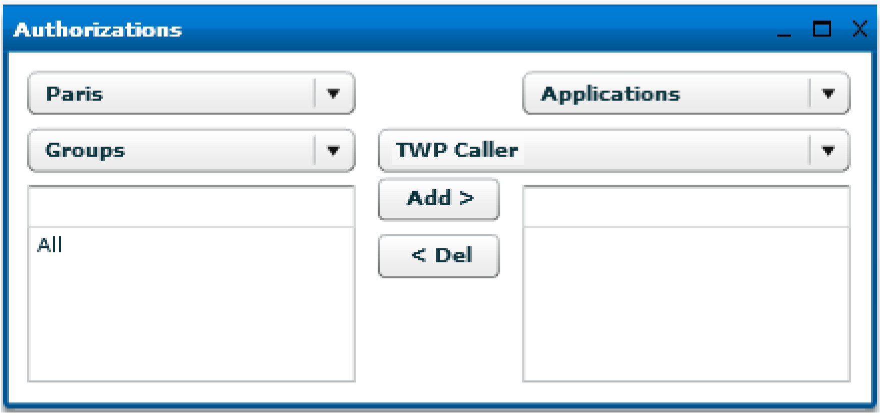
3.3.7. Providing authorization to Caller application

Select the *Users / Authorizations* menu.



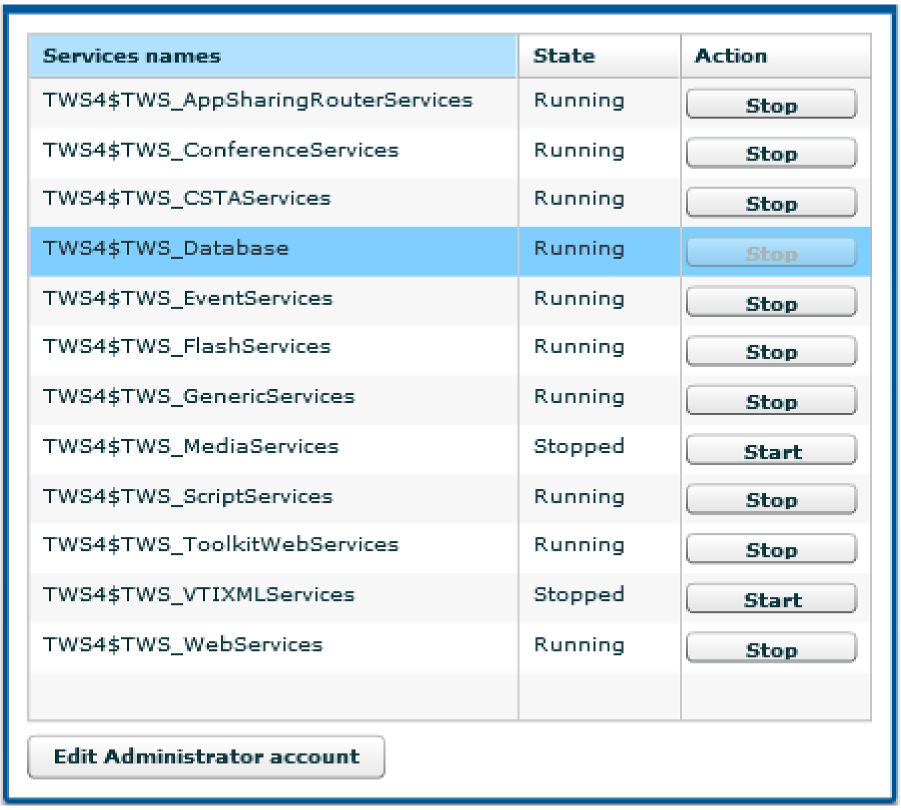
In the upper right list box, select *Applications*. In the bottom right list box select TWP Caller.

Select the group "All" and click on "*Add*". All users of this group will be granted to user TWP Caller.



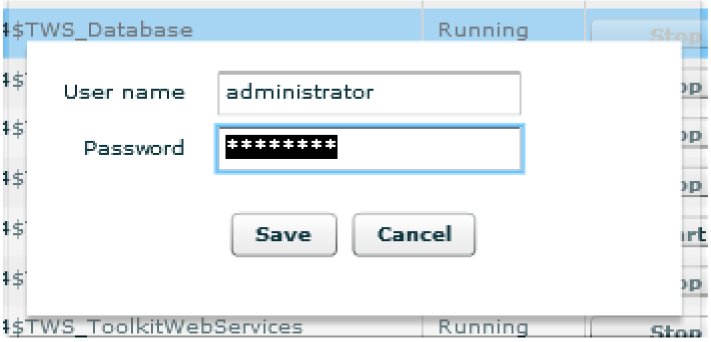
3.3.8. Starting Services

Select *Tools / TWP Services* menu.



Services names	State	Action
TWS4$TWS_AppSharingRouterServices	Running	Stop
TWS4$TWS_ConferenceServices	Running	Stop
TWS4$TWS_CSTAServices	Running	Stop
TWS4$TWS_Database	Running	Stop
TWS4$TWS_EventServices	Running	Stop
TWS4$TWS_FlashServices	Running	Stop
TWS4$TWS_GenericServices	Running	Stop
TWS4$TWS_MediaServices	Stopped	Start
TWS4$TWS_ScriptServices	Running	Stop
TWS4$TWS_ToolkitWebServices	Running	Stop
TWS4$TWS_VTIXMLServices	Stopped	Start
TWS4$TWS_WebServices	Running	Stop

Click on "Edit administrator account" button: you must enter the information of the local administrator of the machine to start and stop Windows services from this screen.



User name: administrator

Password: ********

Click on "Save" button.

- Start TWS4$TWS_Database
- Start TWS4$TWS_GenericServices, the other services will be started automatically

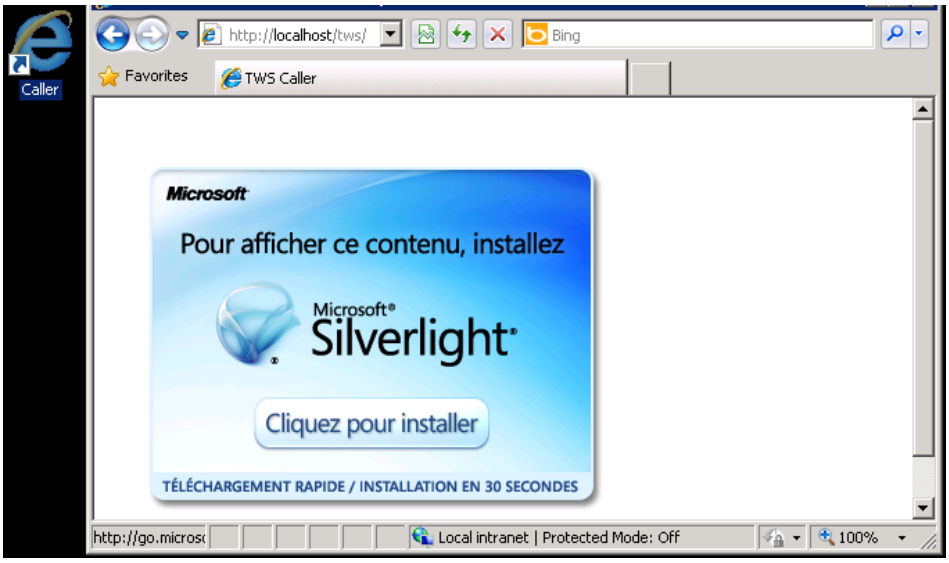
3.3.9. Testing the Caller application

There is 2 ways to install the application in user session:

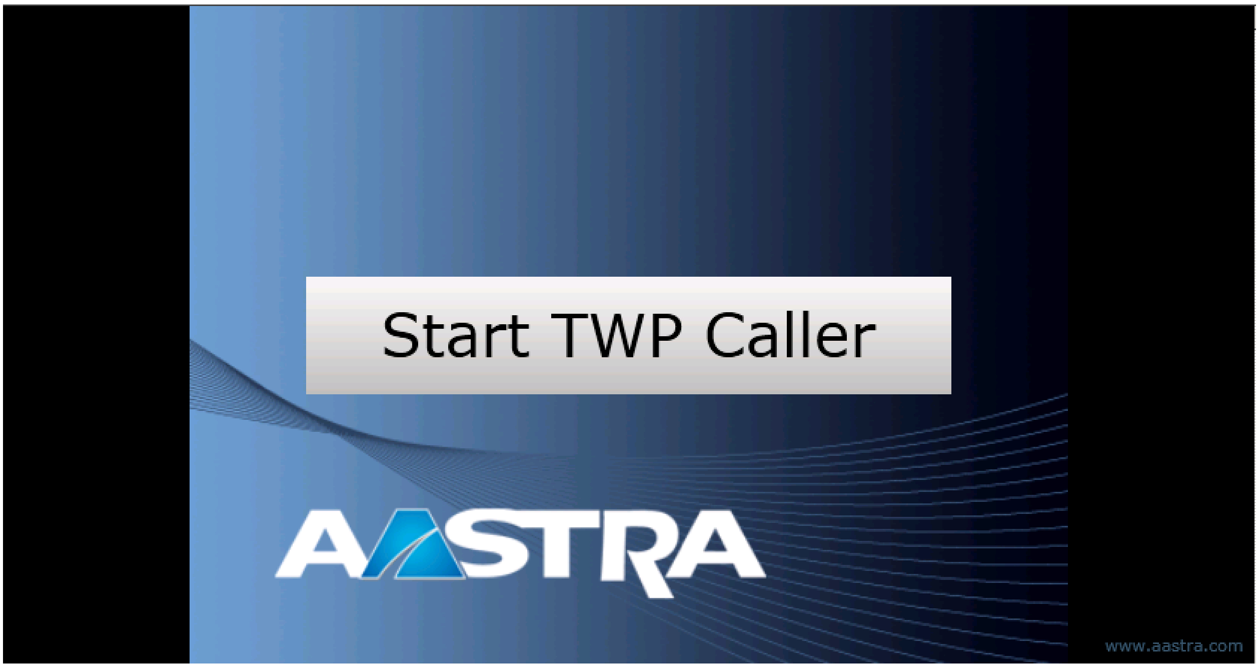
- TWP_Launcher.msi: This installation tool automatically or manually deploy TWP _Caller in Windows user sessions.
  However, there is no automatic installation of Microsoft Silverlight. It must be installed beforehand.
  The TWP _Launcher.pdf documentation is reserved to the description of this installation tool.

- Installation via the URL http://servername/tws/ on different browsers compatible with Silverlight.
  (See compatibility table: https://www.microsoft.com/getsilverlight/get-started/install/default.aspx)
  Windows 10: The installation may be done via Internet Explorer which is installed by default.
  Mac OS: The installation may be done via Safari through a configuration (see the TWS user documentation) or Mozilla Firefox.

Click on the "TWP Caller" link on the desktop of the server. This page is opened.



This allows you to install Silverlight. If it is installed, just refresh the page to start TWP Caller.



The application should start and you should see your user name and your extension number in the title bar.

You are now ready to test and make your first call with TWP Caller. (See user guide of TWP Caller)

4. A5000 link

4.1. General

In order to control the subscriber telephony functions, the TWP server establishes CTI supervision links with the NeXspan or A5000 PBX multisite. Depending on the subscribers and the intended usage, there may be two types of protocol: CSTA (standard ECMA) and VTI-XML (AASTRA proprietary).

TWP may establish a CSTA link and several VTI-XML links at the same time with a multisite PBX per domain. Each link multiplexes the supervision of several subscribers. Each link is limited in the maximum number of permanent supervisions according to its type and the characteristics of the PBX connection.

***Caution**: Consult the LCI AASTRA MATRA TELECOM to find the technical constraints related to the link capacities, according to the NeXspan/A5000 software releases as well as their interface boards.*

In order to be able to serve a large number of users, TWP implements a multiple VTI-XML link mechanism which enables to cumulate each capacity.

***Caution**: Only one link is enough when the total number of VTI-XML subscribers supervised does not exceed the capacity of a link and the architecture is monosite or multisite / mono center.*

Several links must be created when the total number of VTI-XML subscribers supervised exceeds the capacity of a link or the architecture is multisite / multi center.

The algorithm for allocating subscriber supervisions to the VTI-XML links operates according to several modes:

- Explicit mode: for each link, the administrator designates cluster sites for which the subscribers must be supervised by this link.
    - If several explicit links are possible for a given cluster site, TWP distributes the supervisions by filling the least loaded links first
    - If all the explicit links are saturated, the supervisions overflow to other links by filling the least loaded links first
- Implicit mode: When the cluster site is not associated explicitly with a link, TWP distributes the supervisions by filling the least loaded links first.

These two modes may be combined: a part of the cluster sites is associated explicitly with a link and the rest is associated dynamically.

Each link is defined mainly by:

- The IP address of the connection site
- The cluster site(s) associated explicitly with the link
- The maximum capacity of the link

It is mandatory to define the CSTA link for the call forwarding feature.
The CSTA server configured on the PBX must be only dedicated to the link with the TWP server.

4.2. Starting services

The configuration of the different links must respect the following engineering principles:

- The capacity of a link must not exceed the maximum capacity of the connection site (cf. LCI AASTRA)
- The list of cluster sites on the link must contain at least the cluster site of the connection site
- At least one link must be created in each center of a multi-center.
- It is recommended that you create a link to each cluster site with an IP board which supports VTI-XML
- The allocation of the cluster sites must favor a "shortest IP path" routing
- In the case of a supervision "transit site", the allocation of cluster sites must favor the sites which have the highest connection capacity.

Before you configure the different links you are recommended to fill in a table which enables the link and the subscriber's cluster site to be associated clearly.

		Link 0	Link 1	Link 2
Center		1	2	3
Site		1.1	2.1	3.1
Capacity		500	250	200
IP Address		IP address 1	IP address 2	IP address 3
Site	**Center**			
1.*	1	500		
2.*	2		250	
3.*	3			100
4.*	3			100

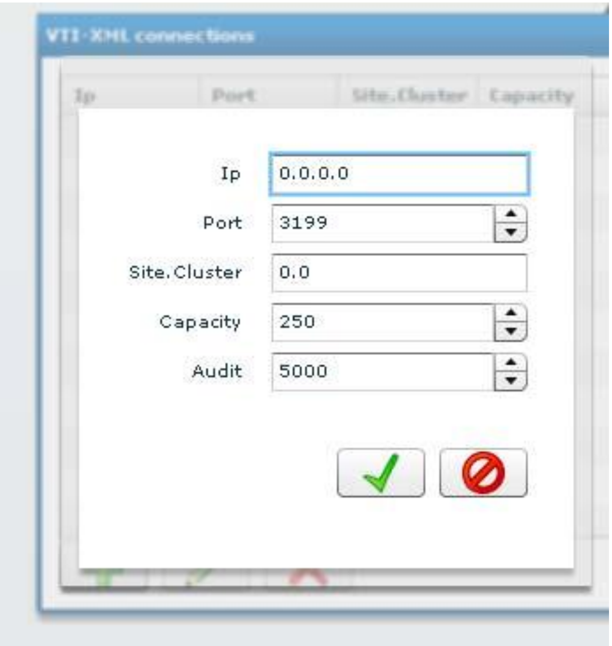
Here we see that:

- Each center has a link
- Sites 1, 2 and 3 are supervised with the "shortest IP path"
- Link 2 which is connected to site 3 enables the supervision of sites 3 and 4 to be routed.

The menu "provider state" and "device state" are used to verify the allocation of the cluster sites with the supervisions (see 9.4. and 9.5.).

Create a VTIXML link

VTIXML link is used to monitor any device type except I2052.
Select *Connection / VTI-XML Connections* menu, then click on "+" button.



Ip	0.0.0.0
Port	3199
Site.Cluster	0.0
Capacity	250
Audit	5000

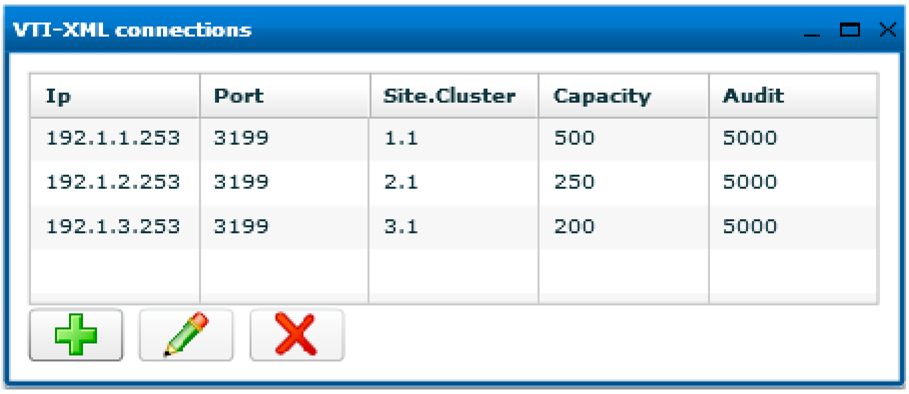
By default you only need to fill in:

- the IP address of the IPBX,
- the Site.Cluster if you want to create more than one link
- the capacity (see LCI).

Click on "save" button.

***Information:** You must restart the VTI-XML service if you make any changes.*

In the case of a multi-site architecture and the creation of several VTI links, here is an example:



Ip	Port	Site.Cluster	Capacity	Audit
192.1.1.253	3199	1.1	500	5000
192.1.2.253	3199	2.1	250	5000
192.1.3.253	3199	3.1	200	5000

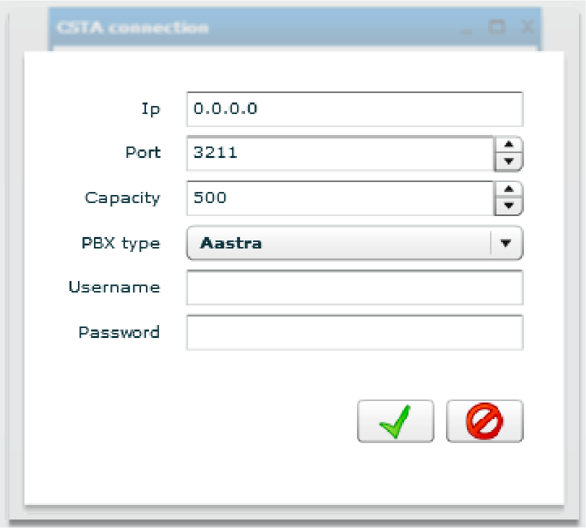
After restarting the service, you can check the status of connections created and device supervision (see 9.4. Connections state and 9.5. Devices state).

4.3. CSTA link

CSTA link is used to manage simple forward rules (see Caller user guide), or I2052 phone with a TWP Caller.

Note: Only one CSTA link is allowed by domain.

Select the *Connections / CSTA Connection* menu then click on "+" button.



Ip	0.0.0.0
Port	3211
Capacity	500
PBX type	Aastra
Username	
Password	

By default, you only need to fill in:

- the IP address of the IPBX,
- the CSTA port (the default is 3211 in non-delimited mode): this port must be unique in a multisite and dedicated to only one application (see Aastra specification for CSTA link)
- the PBX type “A5000”
- the capacity (see LCI)
- Username/Password are not used in this case

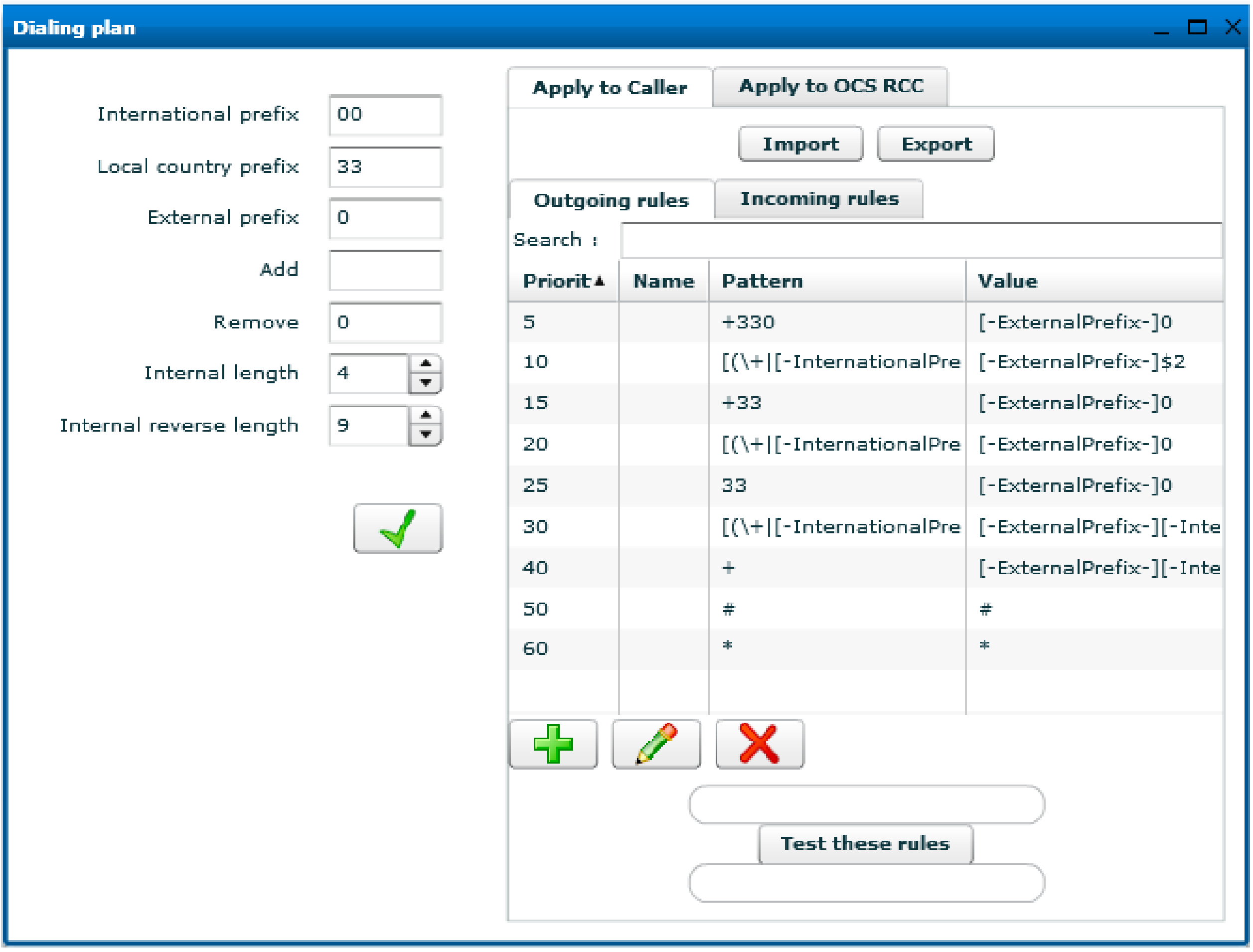
Click on “save” button.
***Information**: You must restart the CSTA service if you make any changes.*

5. Dialing plan management

Management of the numbering plan allows you to define rules for processing numbers:

- Dialed or found in directories to make them good to call (for example, deleting the "+" for the numbers in international format)
- Received in the reverse directory search

Select *Telephony/Dialing plan* menu.



Dialing plan

International prefix	00
Local country prefix	33
External prefix	0
Add	
Remove	0
Internal length	4
Internal reverse length	9

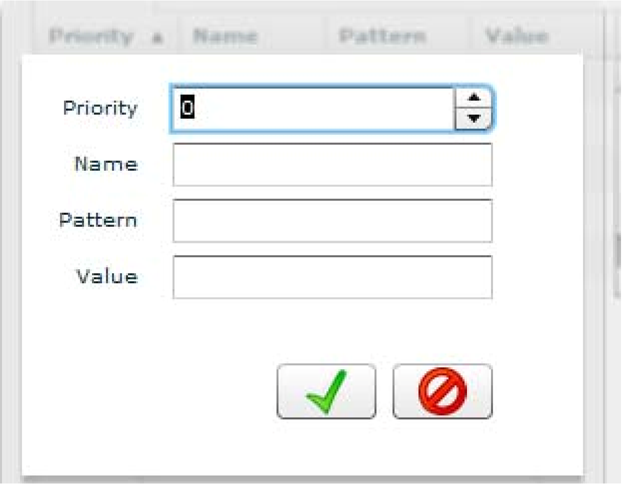
Priorit▲	Name	Pattern	Value
5		+330	[-ExternalPrefix-]0
10		[(\+|[-InternationalPre	[-ExternalPrefix-]$2
15		+33	[-ExternalPrefix-]0
20		[(\+|[-InternationalPre	[-ExternalPrefix-]0
25		33	[-ExternalPrefix-]0
30		[(\+|[-InternationalPre	[-ExternalPrefix-][-Inte
40		+	[-ExternalPrefix-][-Inte
50		#	#
60		*	*

On the left part you define the global rules.

- International prefix: prefix used for international calls.
- Local country prefix: International prefix for the installation country, e.g. 33 for France.
- External prefix: prefix used to make an external communication. (prefix to access to the public network)
- Add: characters set to add to incoming calls.
- Remove: characters set to remove from incoming calls.
- Internal length: is the maximum length of your internal phone number.
- Internal reverse length: is the length used to resolve incoming call.

On the right part you define specific rules for your dialing plan (by default some standard rules are created).

To add a specific rules to your installation click on "+" button and this window will open.



Priority 0
Name
Pattern
Value

- Priority: is the priority of the rules, the rules are tested from the lowest priority to the highest, the first one found is played.
- Pattern: character string to be replaced
- Value: character string which replaces the pattern

For example:

The "+" character will be replaced by "00".
The string "361" will be replaced by "361".

The rules are processed in order, from top to bottom. As soon as a rule is taken into account, the following rules are ignored.
The patterns are searched only at the beginning of the string.

5.1. Standard rules

The included standard rules are:

- Any non-numerical character is deleted, except for +, #, * when they are the first character
- "+33(0": is transformed into 00 (therefore +33 (0) 123456789 becomes 00123456789)
- "+330" : is transformed into 00
- "#": is transformed into "#" (therefore no transformation, used for facilities).
- "*": is transformed into "*" (therefore no transformation, also used for facilities).

Particular cases: Any number which begins with the international prefix + the national code (i.e. 0033 or +33) will be replaced by the network prefix + national code ("+33155171889" will become "00155171889’).

5.2. Dialing transformation

The dialing transformation algorithm is as follows: the first operation involves detecting whether a rule is applicable:

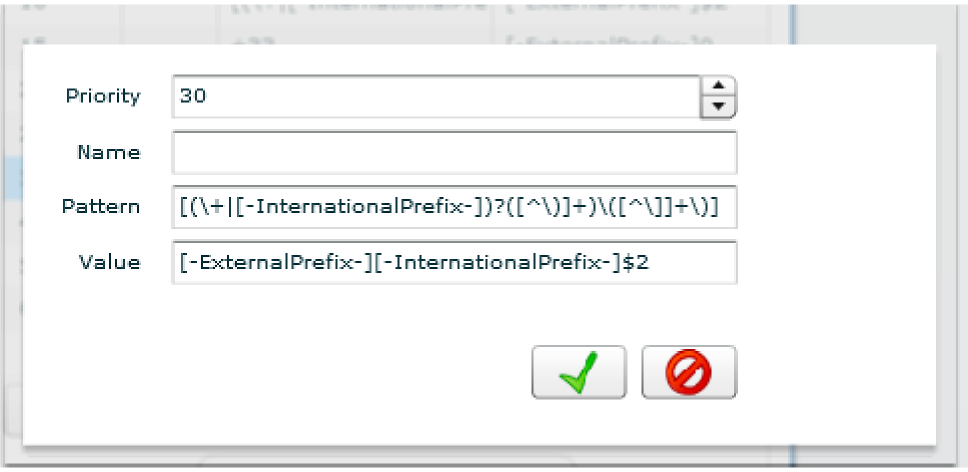
Two case

- No rule is found. In this case, if the number is larger than the length of the dialing plan, the external network prefix is added; otherwise, the number is returned as it is.
- A rule is applicable, two cases are possible:
    - The number starts with a “+”. The transformation is applied then the network prefix is added if necessary. For example: +3912334477 -> 0 00 3912334477
    - The number does not start with a “+”. Only the dialing transformation is applied. For example: if we have the rule: pattern = 3611 value = 03611, the dialing of 3611 will become 03611 but the external network prefix will not be added in this case.

5.3. Extended rules

It is possible to define rules based on regular expressions.

In the screen shot above, the rule (which has a priority of 30) is a regular expression:



Priority	30
Name	
Pattern	[(\+|[-InternationalPrefix-])?([^\)]+)\([^\]]+\)]
Value	[-ExternalPrefix-][-InternationalPrefix-]$2

This rule turns +42(0)141906666 into 00042141906666. It adds the international prefix and external prefix and removes the national prefix if necessary.

Model details:

```
[(\+|[-InternationalPrefix-])?([^\)]+)\([^\]]+\)]
```

The model's square brackets informs that it is a regular expression.

```
[(\+|[-InternationalPrefix-])?([^\)]+)\([^\]]+\)]-> 42(0)141906666
```

The '+', a special character used in regular expressions, is preceded by a '\' to show that the expression will search for a '+' in the string. The '?' indicates that the expression will search for one or zero '+'. The rule thus treats numbers such as +42(0) and 42(0) etc...

```
[(\+|[-InternationalPrefix-])?([^\)]+)\([^\]]+\)] -> 42(0)141906666
```

[-InternationalPrefix-] represents the numbers of the international prefix mentioned in the left column. The term look this value to copy this in the result.

```
[(\+|[-InternationalPrefix-])?([^\)]+)\([^\]]+\)] -> 42141906666
```

The characters '(' and ')', special characters used in regular expressions, are preceded by a '\' to indicate that the expression will specifically search for '(' and ')'.

Details of the value: [-ExternalPrefix-][-InternationalPrefix-]$2

'$2' will be replaced by the captured value (see Model details above). In our example, our rule replaces +42(0) by 00042.

For more details on regular expressions:
http://msdn.microsoft.com/fr-fr/library/hs600312(VS.80).aspx

Dialing plan test:

You can check your numbering translation rules as follows:

Enter a number in the box above the "test these rules" button. After the click, the converted number is displayed in the lower box. This is the number that will be sent to the IPBX.

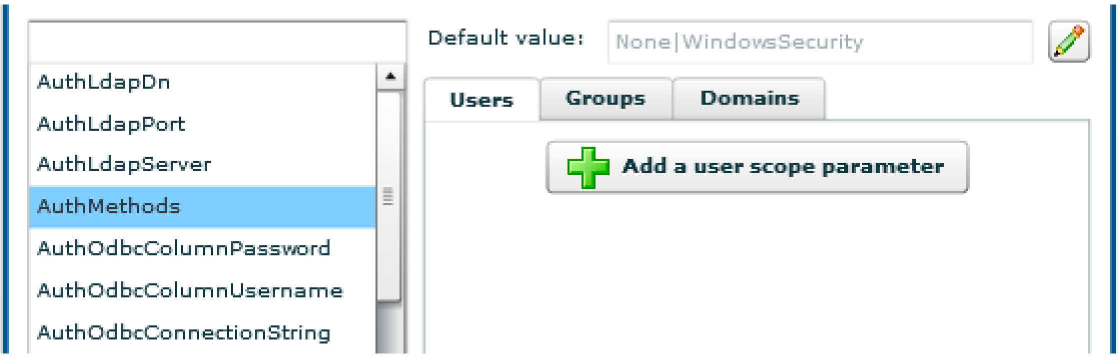
6. Authentication methods

6.1. Configuration

Users are created manually or imported from a database, they must be authenticated when using applications. There are several authentication methods with TWP that can be configured in the administration:

- *Windows* authentication: application parameter value "*WindowsSecurity*"
- *LDAP* authentication: application parameter value "*LDAP*"
- TWP authentication: application parameter value "*TWS*"
- *None* authentication: application parameter value "*None*"

To change or apply an authentication method to a user, group of users or an entire domain, go to the administration, the *Applications / Applications parameters* menu then choose TWP *Server*. Find "*AuthMethods*".


AuthLdapDn
AuthLdapPort
AuthLdapServer
AuthMethods
AuthOdbcColumnPassword
AuthOdbcColumnUsername
AuthOdbcConnectionString

Default value: None|WindowsSecurity

It is possible to enter different values separated by "|". In the example above, all users can both run the Caller application, automatically authenticated from their Windows sessions or by specifying the user name on the login window.

6.2. Windows authentication

This is the historical authentication system on TWP solution. Authentication is carried out via the Windows accounts of users.

6.2.1. Prerequisites: with domain controller

At the launch of the Caller application or the use of authenticated web services, there is no authentication pop-up that appears in this mode.

- On the domain controller all users of the company must have an account
- The TWP server must be in the same Windows domain as the user accounts.
- The user must log on its Windows session with a login / password that is its identifier on the domain.
- In the administration, TWP user names must be identical to the names of domain users.

6.2.2. Prerequisites: without domain controller

Without the pop-up authentication:

- Users and server must be in the same Workgroup (Windows workgroup).
- You must declare the same user names on the server in the user manager window as on the client machines (Windows users) and in the administration.
- Users must log onto their machine with their local account (which is the same as what is set on the server and the administration) and not with administrator account.
- **Attention**: If the user changes his password locally (on the client machine) it must also change in the user's manager on the server TWP.

With the pop-up authentication:

- Users are declared on the server (Windows users).
- The user must enter his login / password each time he launches the Caller application or uses authenticated web services.
- The user can connect as they see fit on their local machine (in this kind of architecture in general, user can be administrator of the machine).

6.3. LDAP authentication

The authentication is done via LDAP user accounts.

Prerequisites:

- Users must all be reported on one (or more) LDAP server.
- The LDAP server must be accessible from the TWP server:
  To configure the LDAP server connection information, go to the administration, the *Applications / Applications parameters* menu, choose TWP *Server*. You must fill in the following fields.
  Note that the values can be indicated for a user or a group or domain
    - *AuthLdapServer*: IP address of the LDAP server
    - *AuthLdapPort*: connection port.
    - *AuthLdapDn*: Where to point in the LDAP tree. The default value is "?". "?" is replaced by the user name. It is possible to enter other values as « `OU=PARIS, DC=SSDEI, DC=local, CN=?` »

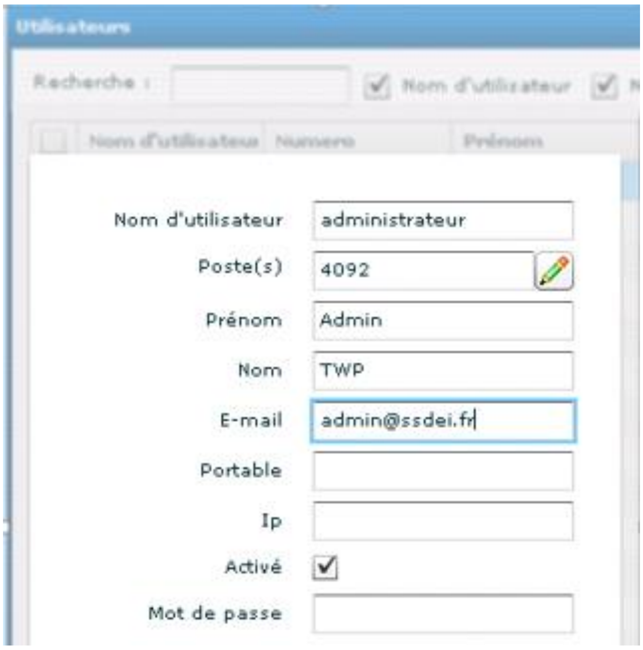
- The user name must be present with or without "*AuthLdapDn*" in the LDAP server.
- The password for the user is the same as in the LDAP server.
- At the first connection with the Caller application, an authentication pop-up (TWP) appears, the user enters his login / password. If the user checks the "save" button the pop-up box does not reappear. If he wants to change the user name, it can uncheck the automatic login feature in the *General* menu in the preferences tab.

6.4. TWP Authentication

The authentication is performed directly on the server using the user name and password provided in the administration.

Prerequisites:

- Neither need a domain nor a WorkGroup. No matter how the user connects to the session.
- Users can be created manually or by the import of various directory in the administration.
- Each user must have a password and it must be entered manually by the administrator
  To complete the password of the user login, go to the administration, the *Users / Users* menu. Edit a user and modify the value of “*password*”.



Nom d'utilisateur	administrateur
Poste(s)	4092
Prénom	Admin
Nom	TWP
E-mail	admin@ssdei.fr
Portable	
Ip	
Activé	☑
Mot de passe	

- When connecting the user must fill in the same password that the administrator has assigned to him.
- At the first connection with the Caller application, an authentication pop-up (TWP) appears, the user enters his login / password. If the user checks the "save" button the pop-up box does not reappear. If he wants to change the user name, it can uncheck the automatic login feature in the *General* menu in the preferences tab.

6.5. No authentication

The authentication is performed directly on the server through the user name.

Prerequisites:

- Neither need a domain nor a WorkGroup. No matter how the user connects to the session.
- Users can be created manually or by the import of various directory in the administration.
- When connecting the user must fill in his user name.
- At the first connection with the Caller application, an authentication pop-up (TWP) appears, the user enters his login / password. If the user checks the "save" button the pop-up box does not reappear. If he wants to change the user name, it can uncheck the automatic login feature in the *General* menu in the preferences tab.

7. Users management

Users can be created manually or imported from databases.

7.1. Creating user manually

See chapter 3.3.4.

7.2. Importing users

In TWP, you can synchronize your users with an external database. This will help you to create a large number of TWP users in very short time.

To import users, select *Users / Import Users* menu and click “+” button.

There is 3 types of imports:

- LDAP
- Active Directory
- A5000 INT

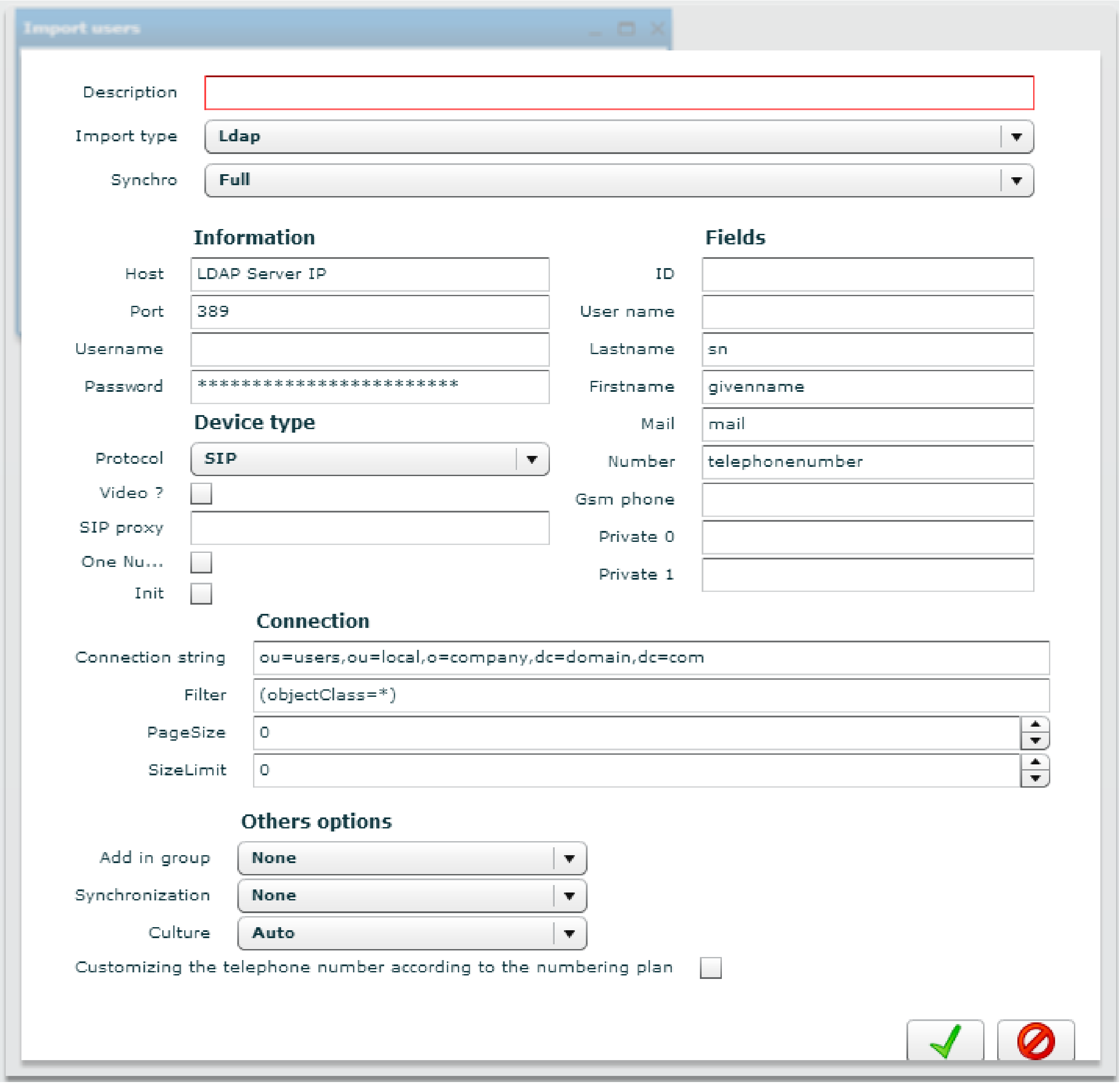
Note: The import process is one way only from the external directory to the TWP user’s directory.

There are also different synchronization types:

- Full: Insert, update and delete. Create new users, update existing users and delete non-existent users.
- Insert, update and disable: Create new users, update existing users and disable non-existent users.
- Insert, update: Create new users and update existing
- Update: update only the existing users

7.2.1. Import users from LDAP

From the dropdown list 'Import type' select "*LDAP*".



Import users

Description	
Import type	Ldap
Synchro	Full

Information

Host	LDAP Server IP
Port	389
Username	
Password	************************

Device type

Protocol	SIP
Video ?	□
SIP proxy	
One Nu...	□
Init	□

Fields

ID	
User name	
Lastname	sn
Firstname	givenname
Mail	mail
Number	telephonenumber
Gsm phone	
Private 0	
Private 1	

Connection

Connection string	ou=users,ou=local,o=company,dc=domain,dc=com
Filter	(objectClass=*)
PageSize	0
SizeLimit	0

Others options

Add in group	None
Synchronization	None
Culture	Auto
Customizing the telephone number according to the numbering plan	□

All standards fields are pre filled. You need to set:

Required information:

Information:

- Description: a description of the import link
- Host: Ip address of the LDAP server
- Port: 389, the default port for LDAP connection
- Username / Password: credential for the LDAP connection

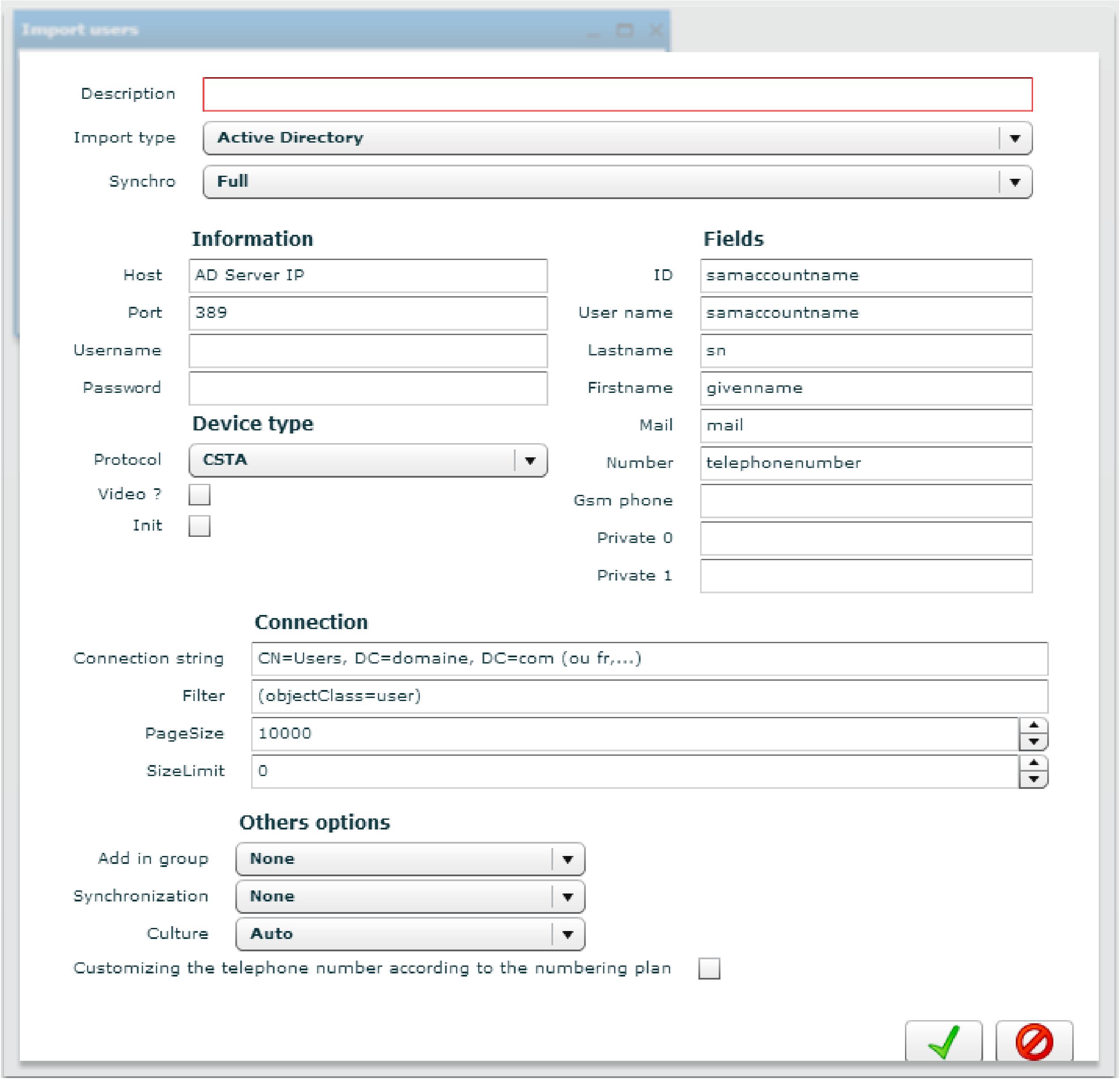
Fields: Map LDAP fields and TWP fields: depend of the LDAP schema.

Connections:

- Connection string: Base DN of your connection
- Filter: LDAP filter for the search request

7.2.2. Import users from Active Directory

In the import type list box, select "*Active Directory*".



Import users

Description:

Import type: Active Directory ▾

Synchro: Full ▾

Information

Host: AD Server IP

Port: 389

Username:

Password:

Device type

Protocol: CSTA ▾

Video ? □

Init □

Fields

ID: samaccountname

User name: samaccountname

Lastname: sn

Firstname: givenname

Mail: mail

Number: telephonenumber

Gsm phone:

Private 0:

Private 1:

Connection

Connection string: CN=Users, DC=domaine, DC=com (ou fr,...)

Filter: (objectClass=user)

PageSize: 10000

SizeLimit: 0

Others options

Add in group: None ▾

Synchronization: None ▾

Culture: Auto ▾

Customizing the telephone number according to the numbering plan □

All standards fields are pre filled. You need to set:

Required information:

Information:

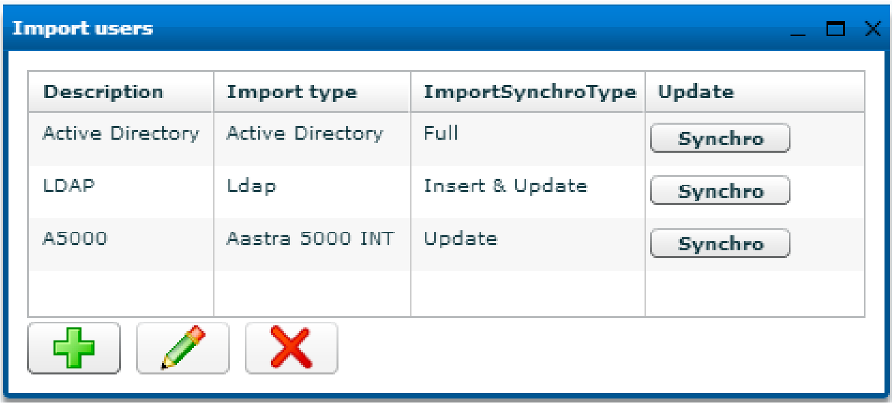
- Description: a description of the import link
- Host: IP address of the DC server
- Port: 389, the default port for DC connection
- Username / Password: credential for the DC connection

Fields: Standard AD fields are pre-filled, you can add private fields schema.

Connections:

- Connection string: Base DN of your DC connection
- Filter: LDAP filter for the search request

7.2.3. User Import window



Description	Import type	ImportSynchroType	Update
Active Directory	Active Directory	Full	Synchro
LDAP	Ldap	Insert & Update	Synchro
A5000	Aastra 5000 INT	Update	Synchro

➕ Create a new user import

✎ Edit an import

❌ Delete an import

To enable synchronization, click the corresponding button "*Synchro*".

Once the sync is complete, a report is issued and the result is visible. If you drag the mouse in the results, the details of the timing display:

- Created: number of new users added.
- Updated: number of new users updated.
- Ignored: number of failures. Users are ignored if they don't have a telephone number.

Attention: The user import is linked to TWS4$TWS_WebServices service, it must always be started. If the service is stopped, it is impossible to synchronize.

7.2.4. Authorization for viewing contacts

To access the contact sheets of imported users, it is essential to give rights to the directory associated with this import (see chapter 7.4.2.).

7.3. Group management

General management

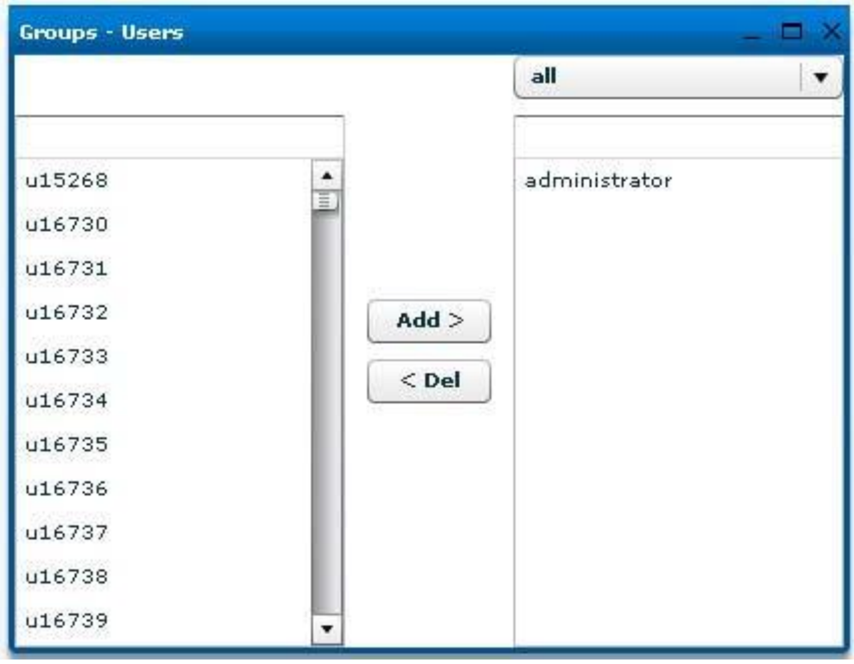
Choose the *Users / Groups* menu.

The groups are containers which are used to group together users who have common characteristics. These groups will then be used to define access to applications, services, logs, etc.

To create groups, see *chapter 3.3.5*.

User management

Choose the *Users / Groups-Users*. This menu is used to define the users included in the groups defined in the last menu.



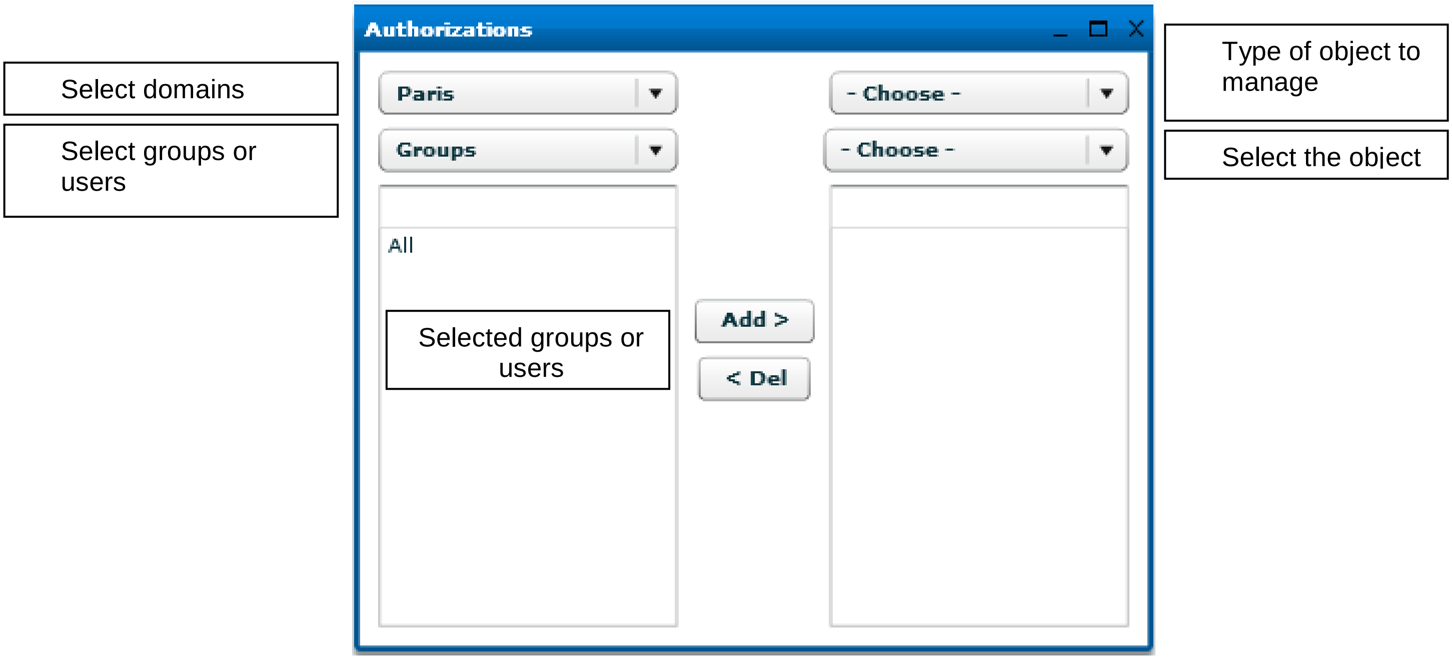
From the upper right combo box, you can select the group to manage. On the left list box, you can see all users that are not already in the selected group. The left upper list box gives you the facility to filter users.

To add a user in a group:

- Select the group on the upper right combo box
- Select one (or more users with ctrl key) and click ”Add>”

7.4. Authorization management

The *Users / Authorizations* is the central interface used to manage all object, user or group rights on the server.



Select domains

Select groups or users

Selected groups or users

Type of object to manage

Select the object

To give rights to a user or user group to an object (applications, directories, ...), proceed as follows:

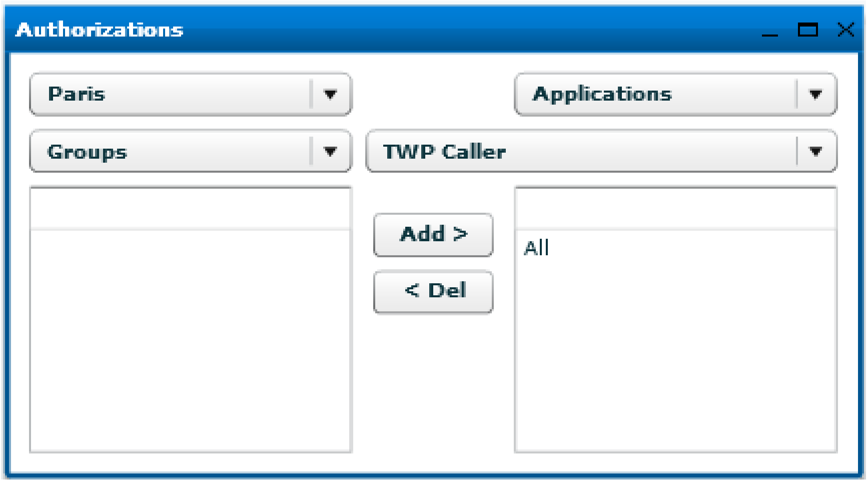
1. The list at the top right, select the type of object to manage
2. Directly below, select the object in question
3. From the list in the top left, select the domain to which the user or user group belongs. The domain of the session is selected by default.
4. The list below select the *users* or *groups*. All users or groups of users in the domain will appears.
5. Then simply select the user or group to the left and click the *Add* button to give him the rights to the object.

***Attention:** Only permissions on Statistics and Records objects are differently manage.*
That is to say, the point 2. rather select the user who will have the rights to Statistics/Records of other users instead of selecting the Statistics/Records object of himself. This will also allow in point 5. to give a single user rights visualizations on Statistics / Records of a group of users.

7.4.1. Applications authorization

The example below shows the authorization for Caller application.

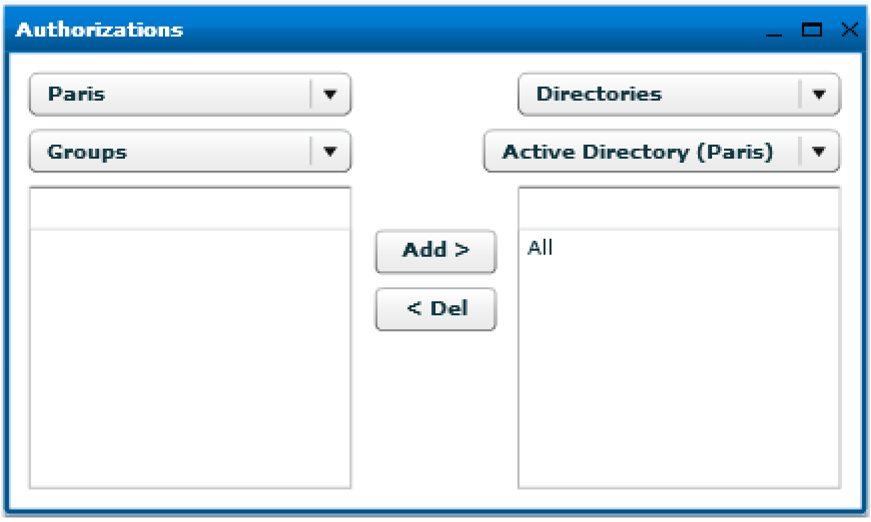
All users in the groups “All” can execute the Caller application.
Any authorization to an application automatically consume a corresponding number of licenses.



7.4.2. Directories authorization

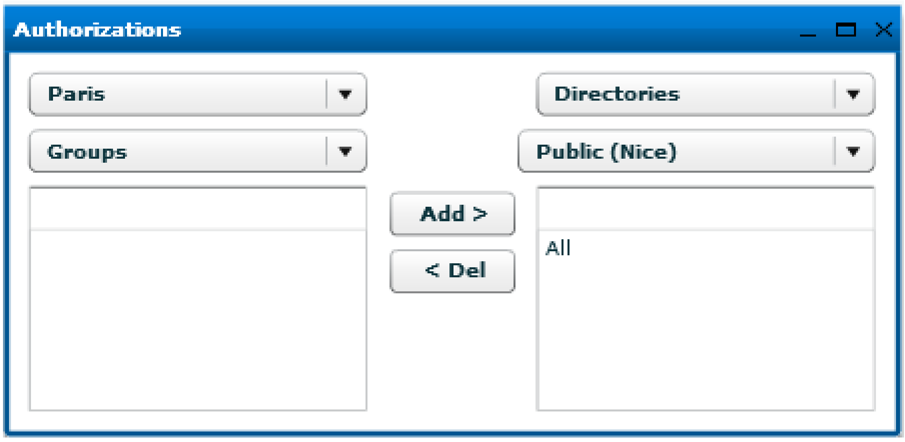
The example below shows the authorization for directory Active Directory (which is the directory created previously by the user import) on the domain Paris.

The group “All” on the domain Paris has the right to see the Active Directory of the domain “Paris”.



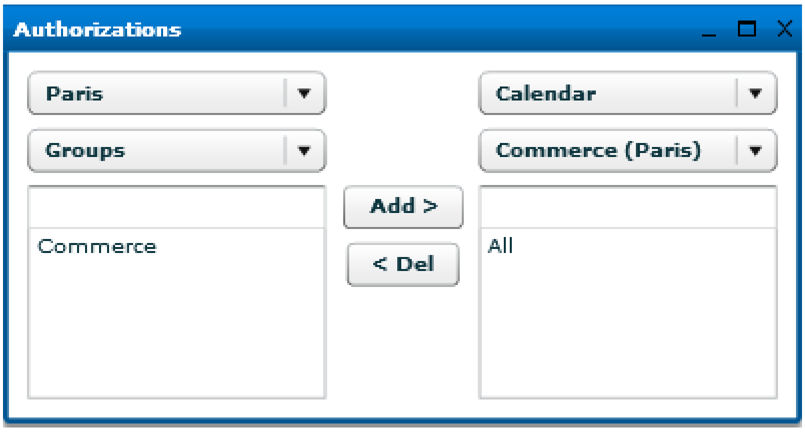
Note: Directories can be shared between domains.

Below is an example of multi-domain authorization. All users in the group “All” on the domain “Paris” have the right to see the directory “Public” on the domain “Nice”.



7.4.3. Calendars authorization

To allow a user to see the events of another user's calendar, go to the *Users / Authorizations* menu. In the example below, the group “All” is allowed to see the calendar events of group “Commerce” of the same domain “Paris”.



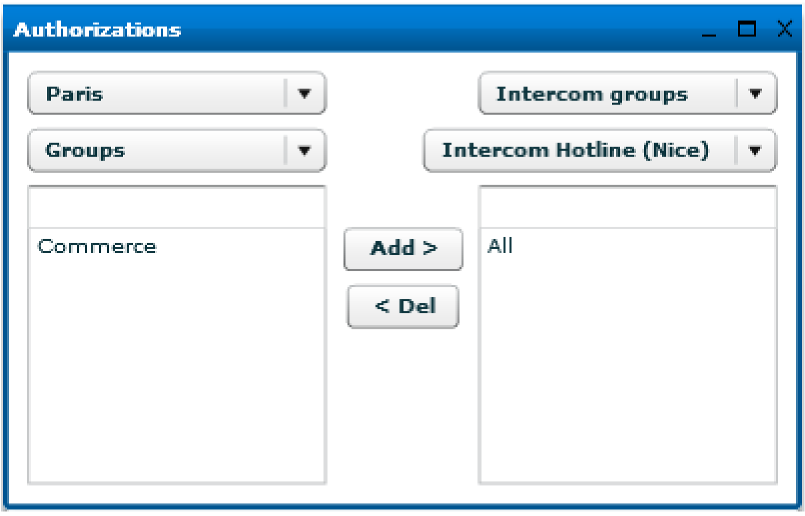
Select *Calendar* in the type of objects, then select users groups who want to share their calendar. Finally select the group or user who will get these calendar events and click on “Add”.

Note: Note that calendar events can also be shared between domains.

7.4.4. Intercom group authorization

The example below shows the authorization for the intercom group “Intercom Hotline” on the domain “Nice”.

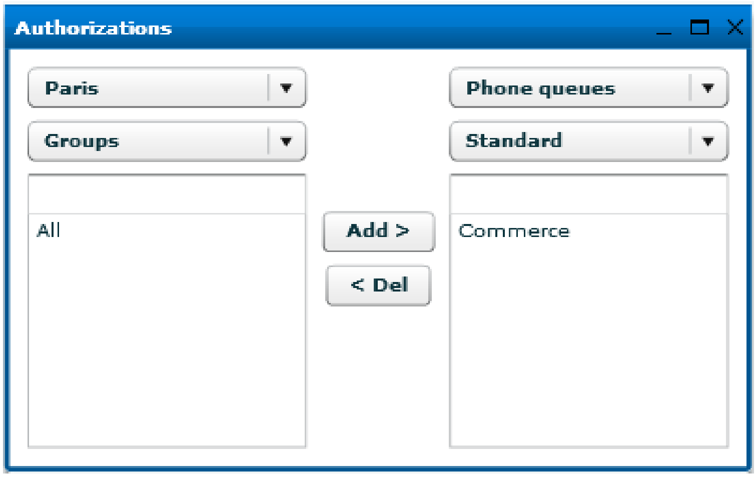
All users in the group “All” on the domain “Paris” have the right to see telephony presence of user devices managed by the group intercom "Intercom Hotline" on the domain "Nice".



Note: Note that intercom groups can also be shared between domains.

7.4.5. Phone queues authorization

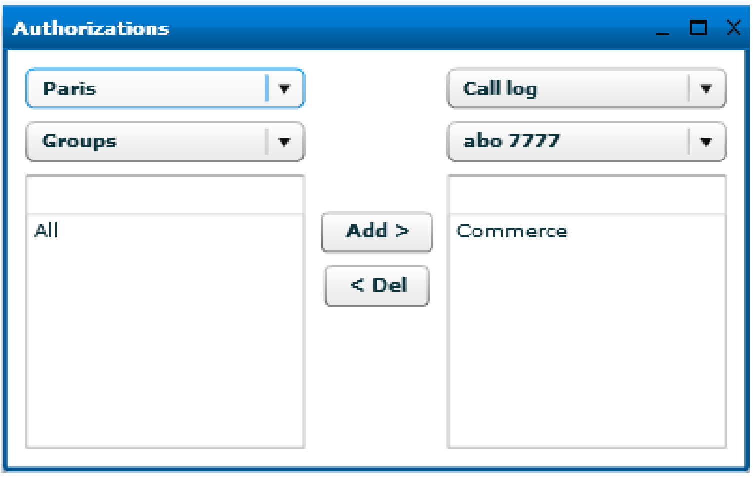
All users of the group “Commerce” of the domain “Paris” have the rights to see calls in the phone queue “Standard”.



Note: The phone queues can’t be shared between domains.

7.4.6. Call log authorization

All user of group “Commerce” of the domain “Paris” have the rights to see the call logs of user “abo 7777”.



Authorizations

Paris

Groups

All

Call log

abo 7777

Commerce

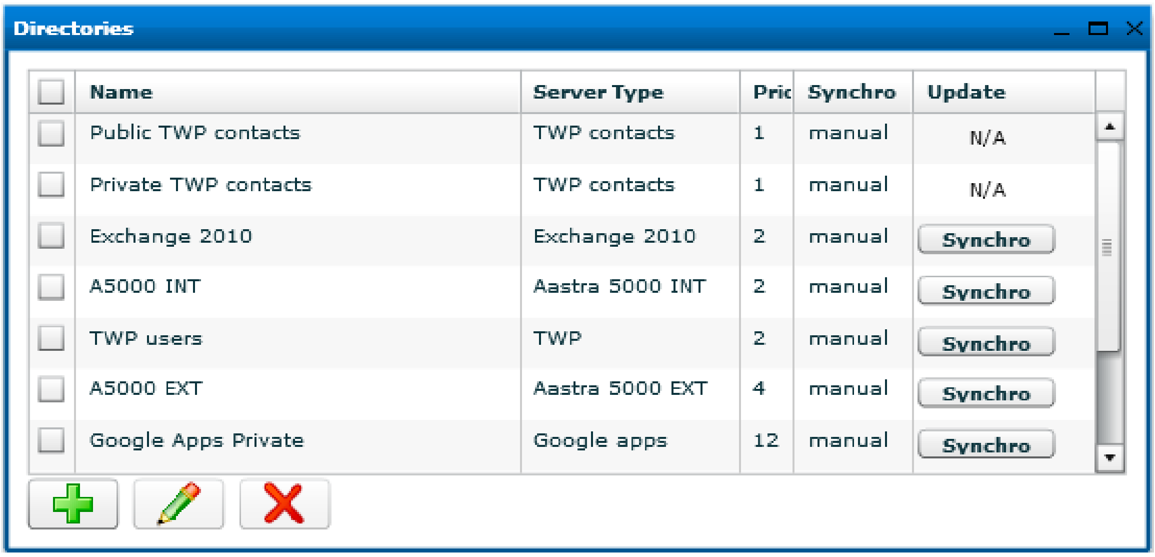
Note: The call logs can't be shared between domains.

8. Directories and collaboration

8.1. General

In the administration go to menu *IT Management* then *Directories*.

A window is opened and it contains several directories already created.



Directories

□	Name	Server Type	Pric	Synchro	Update
□	Public TWP contacts	TWP contacts	1	manual	N/A
□	Private TWP contacts	TWP contacts	1	manual	N/A
□	Exchange 2010	Exchange 2010	2	manual	Synchro
□	A5000 INT	Aastra 5000 INT	2	manual	Synchro
□	TWP users	TWP	2	manual	Synchro
□	A5000 EXT	Aastra 5000 EXT	4	manual	Synchro
□	Google Apps Private	Google apps	12	manual	Synchro

To create a directory, click on “+” button.

The creation of a directory is done in 3 steps:

- Connector tab: creation of the directory connector
- Fields tab: filling in the fields
- Synchronization tab: Configuration of the synchronization mechanism

Connector tab:

You need to fill in some information in this window directory depending on the connector directory you create.

Name: description of the directory

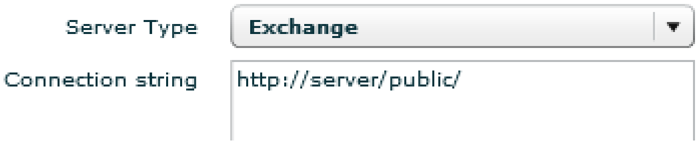
Directory type: Enable or disable a directory

- *Sample / Draft*: Disable the directory, it will not synchronize.
- TWP: The directory is public.
- *Private*: The directory is private.

Priority: This value determines the priority of directories which TWP connected simultaneously. TWP display information about incoming / outgoing calls from the directory with the lowest number of priority.

Example: A contact exists in Exchange, SQL and LDAP directories, all reported on TWP Server. If contact information are displayed with TWP Alerter, information from the directory with the lowest number of priority will be displayed (identity, society, link to customers profile...).

Server type:



Server Type: Exchange

Connection string: http://server/public/

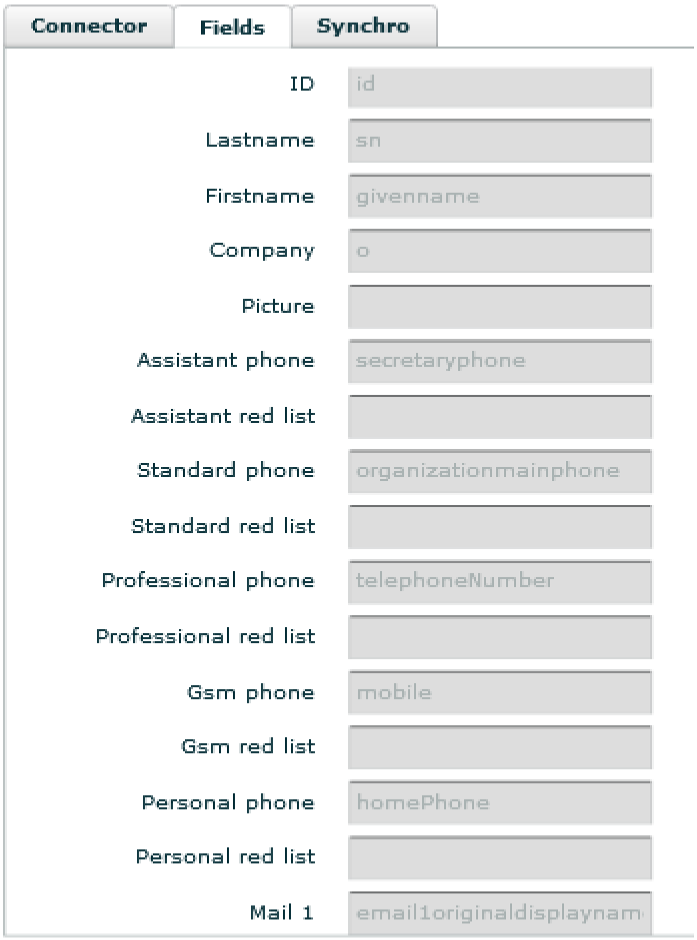
The directory connector can be configured for:

- *Exchange* : MS Exchange server 2003 / 2007 /2010
- *LOTUS* : Lotus domino server version 7.5 / 8
- *LDAP* : All LDAP server
- *ODBC* : ODBC databases
- *OLE DB* : OLE DB databases
- *SQL* : SQL databases server
- TWP : TWP users directories

The remaining fields are used to create a directory connector according to the type of directory connector.

Fields tab:

The fields below match the names of directory fields.
These fields are used to map internal TWP directory fields to the external directory.



ID	id
Lastname	sn
Firstname	givenname
Company	o
Picture	
Assistant phone	secretaryphone
Assistant red list	
Standard phone	organizationmainphone
Standard red list	
Professional phone	telephoneNumber
Professional red list	
Gsm phone	mobile
Gsm red list	
Personal phone	homePhone
Personal red list	
Mail 1	email1originaldisplaynam

Adding options

It is possible to add options to the fields directories, add a Pipe "| " after the field name and a letter that corresponds to the option to run.

Example: « `Surname|u` »

Options:

- ***a***: converts the field value in mailing address and allows the user to click on the resulting link to directly search on a mapping website.
  Note: The URL mapping website is configurable in the administration menu *Applications / Application parameters* / TWP *Caller*, find « *MapServiceURL* ».
- ***h***: hash the value
- ***i***: make invisible the field value in the contact information card in the Caller application. This field remains available in the Alerter application.
- ***l***: put all in lowercase
- ***m***: turn the first letter capitalized, followed by lower case

- ***u***: put all in uppercase
- ***p***: allows you to add items to the value of the field
    - Format: `p::[value]{0}::[Regexp]`
    - Example: `PhoneNumber|p::9{0}::^[0-9]{4}$`
        - « `PhoneNumber` »: field name that will be synchronized
        - « `::` »: separator
        - « `p` »: option name
        - « `9{0}` »: the number 9 will be added at the beginning of the value of PhoneNumber
({0} represents the value synchronized and can be placed anywhere in this expression)
        - « `^[0-9]{4}$` » is a regular expression that checks if the value matches a 4-digit number. (optional)

To add more than one option, you must separate them with a comma ",".

Example: « `Surname|h,u,p::9{0}::^[0-9]{4}$` »

Synchro tab:

See next chapter 8.2.

8.2. Directory synchronization - Merging contacts – Specific fields

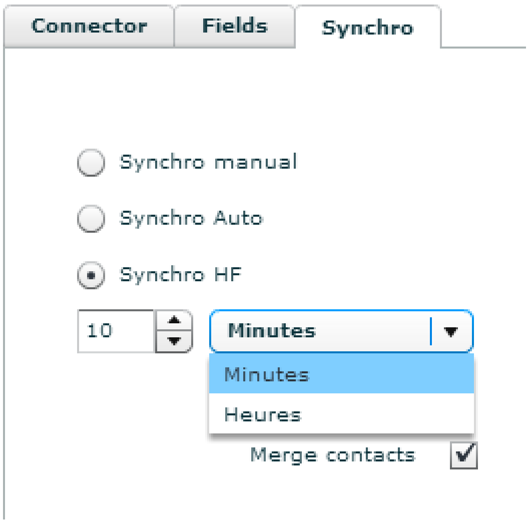
8.2.1. Directory synchronization

There are three types of directory synchronization:

- *Manual*: to synchronize a directory, click the *Synchro* button in the window that lists the directories.
- *Automatic*: to enable synchronization every day at a pre-set time.

  To configure time synchronization, select *Applications / Applications parameters* menu > *System settings*, search for *timeSynchronizationDirectories* (Expert Mode) and change the default value.

  Attention: the correct format is: HH:MM
- *Synchro HF*: High frequency allows you to enable regular synchronization. You can choose a number of minutes or hours.



○ Synchro manual

○ Synchro Auto

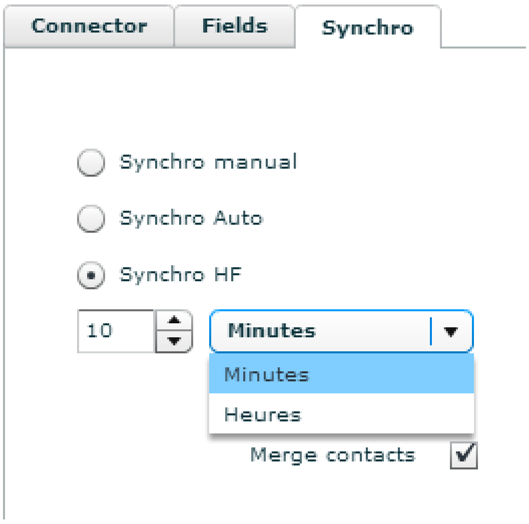
● Synchro HF

10 Minutes

Merge contacts ☑

8.2.2. Merging contacts

In the Synchronization tab, it is possible for a directory to check the box allowing the system to merge the information of his contacts with those from other directories contacts which also have the box checked.



○ Synchro manual

○ Synchro Auto

● Synchro HF

10 Minutes

Merge contacts ☑

The fusion of information between contacts is based on the ***email*** *address.*

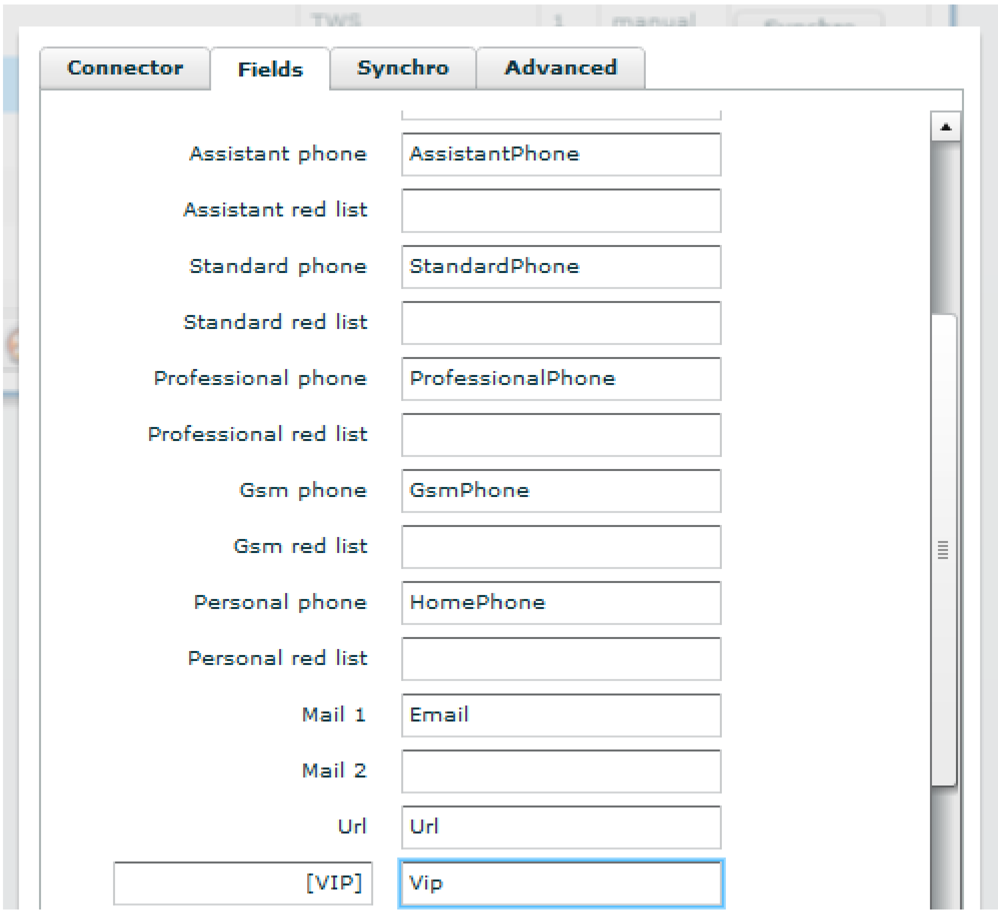
Indeed, if two or more contacts (from all directories) have the same email address, their different information will be merged and presented in a single directory profile.

For example, if users configured in the administration have email addresses, merging information of these will automatically be done with others directories if the "*Merge contacts*" box is checked for the directories in question.
The advantage of this feature is to allow these users to see in the same contact card of one of their colleagues, informations from other directories not available from the TWP list of usersTWP.

8.2.3. Specific Fields : VIP Contact

To activate the VIP contact view in the applications, Caller, Alerter and Smart Attendant, configure the directory source as explained below :

In the name of a private field of the directory you need to put the wording `[VIP]` and match the field name of your external directory (see print screen below) :



Assistant phone: AssistantPhone
Assistant red list:
Standard phone: StandardPhone
Standard red list:
Professional phone: ProfessionalPhone
Professional red list:
Gsm phone: GsmPhone
Gsm red list:
Personal phone: HomePhone
Personal red list:
Mail 1: Email
Mail 2:
Url: Url
[VIP]: Vip

Here, the field of your directory is called "Vip". If the VIP field of your directory is filled, the contact will be seen as a VIP contact and the field contents will be displayed during an incoming call (in a call queue or a direct call).

8.2.4. Specific Fields : red list

The red list system does not display the phone number of a contact in applications, but only the name of this contact.
This feature is efficient if the user does not see the number from his physical telephone: so for the Softphone or other device linked to the PBX red list (in this last case, the PBX directory is configured in administration).

To configure whether to display some synchronized contact numbers, you have to fill in the specific field "red list" linked to the type of number to hide (or not), with the field name of the external database containing the following values:

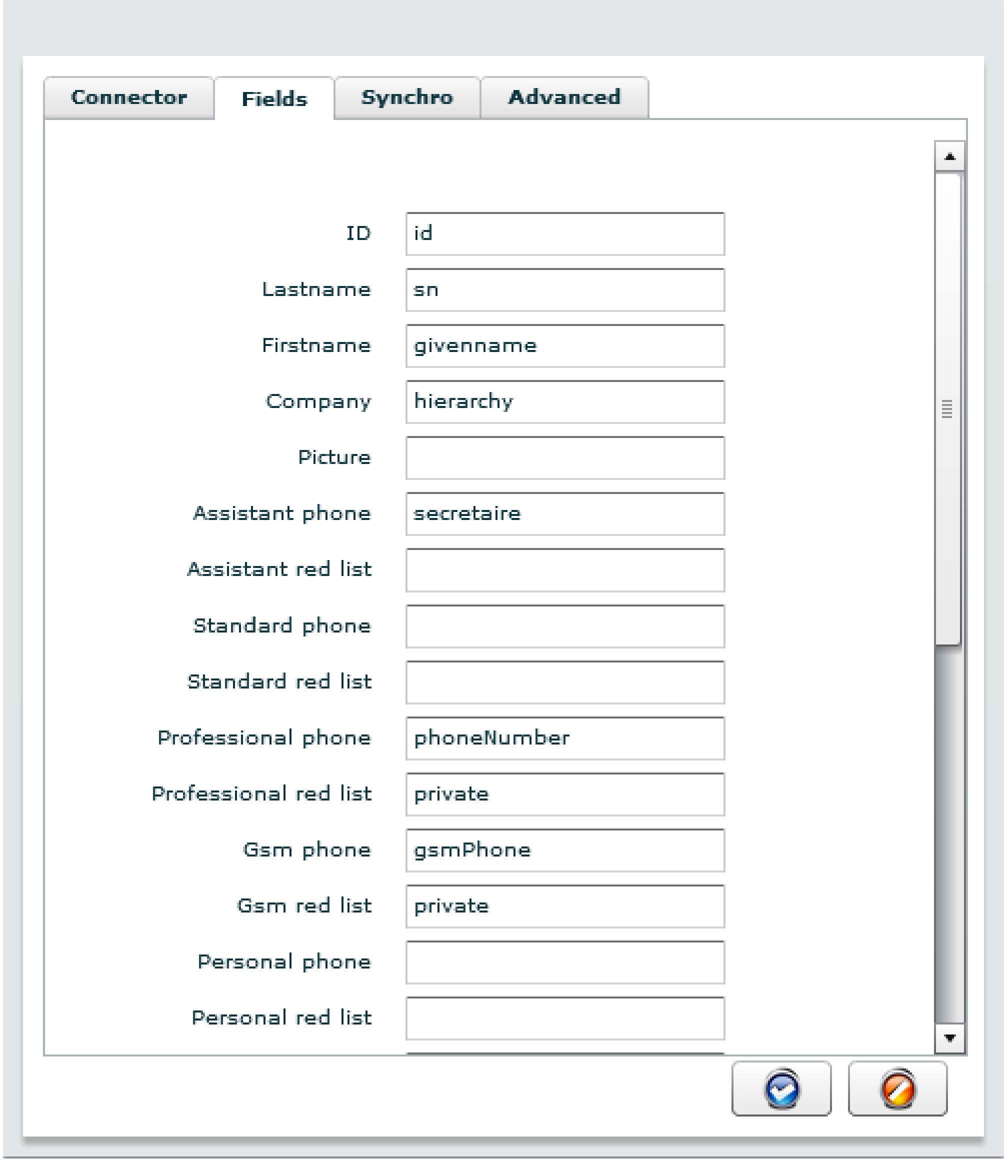
- To hide the contact phone number, the value must be one of the following: “*1*” or “*true*” or “*yes*” or “*y*” or “*lr*” or “*rf*”
- To display the contact phone number, the value must be not one of the given above.

Example : A database contains the following information.

id	sn	givenname	hierarchy	secretaire	phoneNumber	gsmPhone	private
1	Francis	Dupont	Compta		6660		0
2	Noa	Hollande	Direction	4694	4594	0601020304	1

...							

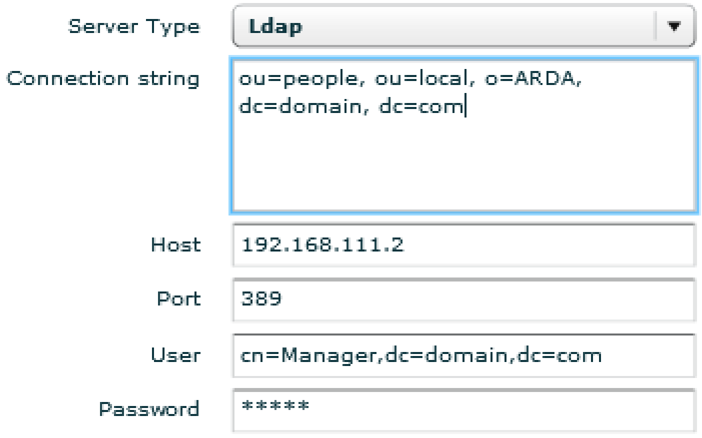
Here is how to set so that the numbers of the contact "Noa Hollande" (excluding Assistant phone) are not displayed:



ID	id
Lastname	sn
Firstname	givenname
Company	hierarchy
Picture	
Assistant phone	secretaire
Assistant red list	
Standard phone	
Standard red list	
Professional phone	phoneNumber
Professional red list	private
Gsm phone	gsmPhone
Gsm red list	private
Personal phone	
Personal red list	

8.3. Creating an LDAP connector

The connection to an LDAP directory server is defined as follows.



Server Type: Ldap

Connection string: ou=people, ou=local, o=ARDA, dc=domain, dc=com

Host: 192.168.111.2

Port: 389

User: cn=Manager,dc=domain,dc=com

Password: *****

Connector tab:

The following fields are required:

- **Connection string**: DN base of the connector
  Example: `ou=people, ou=local, o=ARDA, dc=domain, dc=com`
- **Host**: IP Address or LDAP server name.
- **Port:** LDAP server port. (389 per default)
- **Name**: User name with reading access to the database
- **Password**: Password.

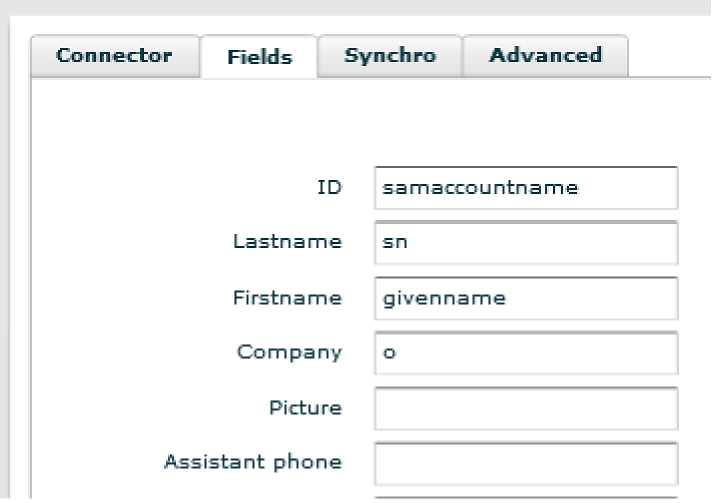
Remark: To validate the connection information and the LDAP schema, we recommend to use a tool such as LDAP Admin (http://www.ldapadmin.org/).

Fields tab:

In fields tab, you must fill in the LDAP fields' name.

Attention: You must fill in these names in lower case. We recommend to use the tool LDAP Admin to find the field names.

Here below is an example of fields in people type schema:

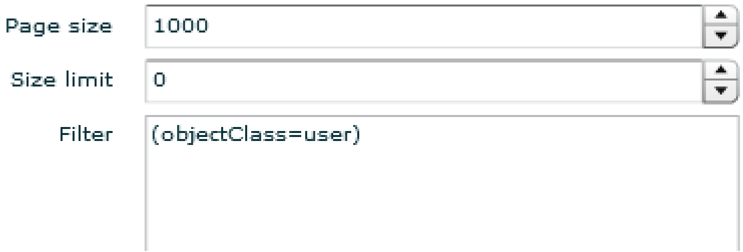


ID: samaccountname
Lastname: sn
Firstname: givenname
Company: o
Picture:
Assistant phone:

Advanced tab:

In this tab you can add advanced settings for the LDAP connection.

- Page size: number of rows loaded for a query
- Size limit: maximum number of rows loaded by the LDAP server
- Filter: LDAP filter applied to the search query.



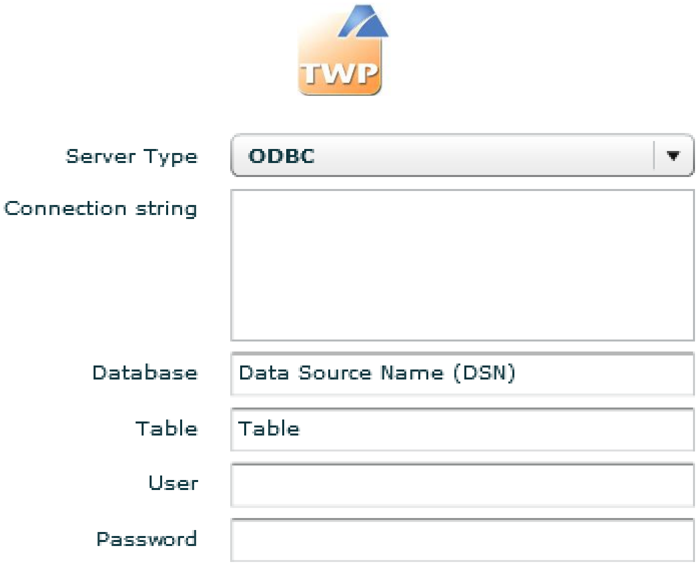
Page size: 1000
Size limit: 0
Filter: (objectClass=user)

Save the data and do a manual synchronization to test if the connector is correct.

Remark: Don't forget about giving rights to corresponding directories for users to access them.

8.4. Creating an ODBC directory

In the *IT management / Directories*, to create a new ODBC connector, click on the "+" button and select ODBC as server type:



Server Type: ODBC

Connection string:

Database: Data Source Name (DSN)

Table: Table

User:

Password:

8.4.1. Connector

There are 2 ways to create an ODBC connection. Note that regardless of the ODBC type you must install the drivers corresponding to the database on which you want to connect.

ODBC System connection:

In this case you must create an ODBC connector system using the Windows Control Panel.

ODBC sources supported by the server must be defined in 32-bit. On a 64-bit server adbcad32.exe program should be used, find it in this directory C:\Windows\SysWOW64.

When the ODBC system source is defined, you can:

- Either set in the field *Connection string*: DSN=Windows_ODBC_source_name.
- Or define the field *Database*, the name of your Windows ODBC source name.

Table: fill in the table name in which TWP need to get information.

TWP ODBC connection:

It is also possible to define a connection string directly, in this case it is not useful to define an ODBC source system using the control panel.

Below are some examples of connection strings:

MySQL:

```
Driver={mySQL};Server=myServerAddress;Port=3306;Option=131072;Stmt=;Database=myDataBase;User=myUsername;Password=myPassword;
```

AS/400:

```
Driver={Client Access ODBC Driver (32-bit)};System=my_system_name;Uid=myUsername;Pwd=myPassword;
```

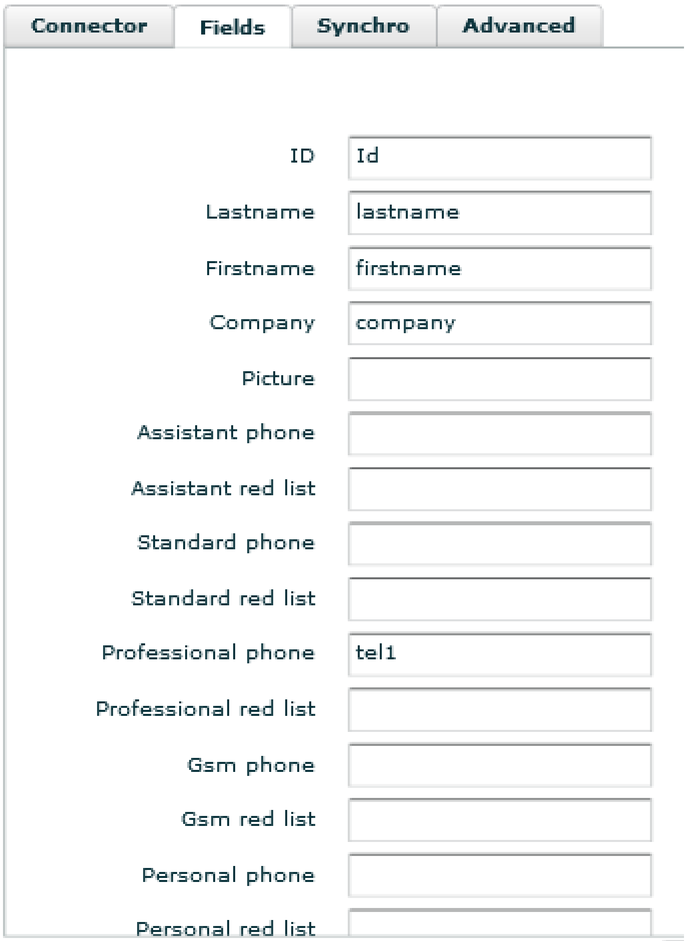
Excel: `Driver= {Microsoft Excel Driver (*.xls)};Dbq=C:\Annuaires\Annuaire.xls;`

Table: fill in the table name in which TWP need to get information.

8.4.2. Fields

Attention: *For an ODBC connection linked to an Excel, CSV file, avoid name columns (fields) containing special characters, punctuation or other spaces to not have errors when attempting to synchronize directories in question.*

Below is a sample configuration of the correspondence between the fields of TWP directory and fields from an Excel or CSV file (the first line of the file represents the fields).

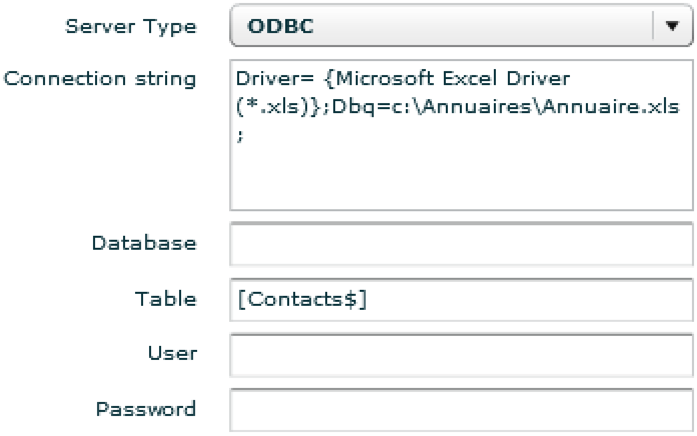


ID	Id
Lastname	lastname
Firstname	firstname
Company	company
Picture	
Assistant phone	
Assistant red list	
Standard phone	
Standard red list	
Professional phone	tel1
Professional red list	
Gsm phone	
Gsm red list	
Personal phone	
Personal red list	

Note: Among the fields to match, the ID field is important in updating distinct contact records that will be present in applications. It will also enable these applications to bind other information to the same contact card whatever the update by a new directory synchronization.

8.4.3. ODBC connectors models

Excel directory example:

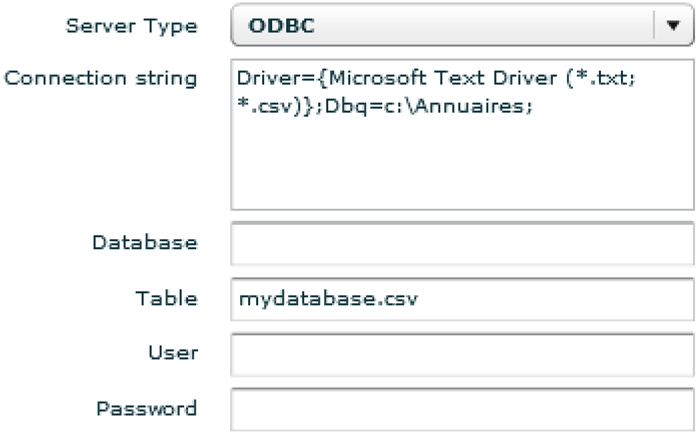


Server Type	ODBC ▼
Connection string	Driver= {Microsoft Excel Driver (*.xls)};Dbq=c:\Annuaires\Annuaire.xls ;
Database	
Table	[Contacts$]
User	
Password	

Connection string: `Driver= {Microsoft Excel Driver (*.xls)};Dbq=c:\Annuaires\Annuaire.xls;`

Table: `[Contacts$]` Name of the Excel file sheet « Contacts » containing the data (Don't forget the $ at the end between brackets).

CSV directory example:

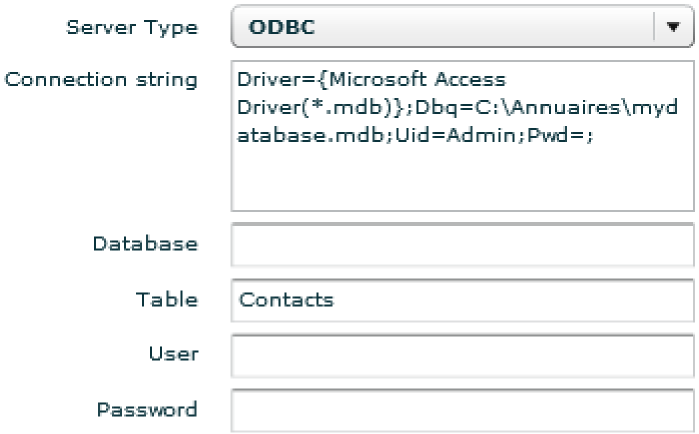


Server Type	ODBC ▼
Connection string	Driver={Microsoft Text Driver (*.txt; *.csv)};Dbq=c:\Annuaires;
Database	
Table	mydatabase.csv
User	
Password	

Connection string: `Driver={Microsoft Text Driver (*.txt; *.csv)};Dbq=c:\Annuaires;`
Table: mydatabase.csv (CSV file name)

Attention: the file name must not contains special character.

Access directory example:



Server Type	ODBC
Connection string	Driver={Microsoft Access Driver(*.mdb)};Dbq=C:\Annuaires\mydatabase.mdb;Uid=Admin;Pwd=;
Database	
Table	Contacts
User	
Password	

Connection string:

```
Driver={Microsoft Access
Driver(*.mdb)};Dbq=C:\Annuaires\mydatabase.mdb;Uid=Admin;Pwd=;
```

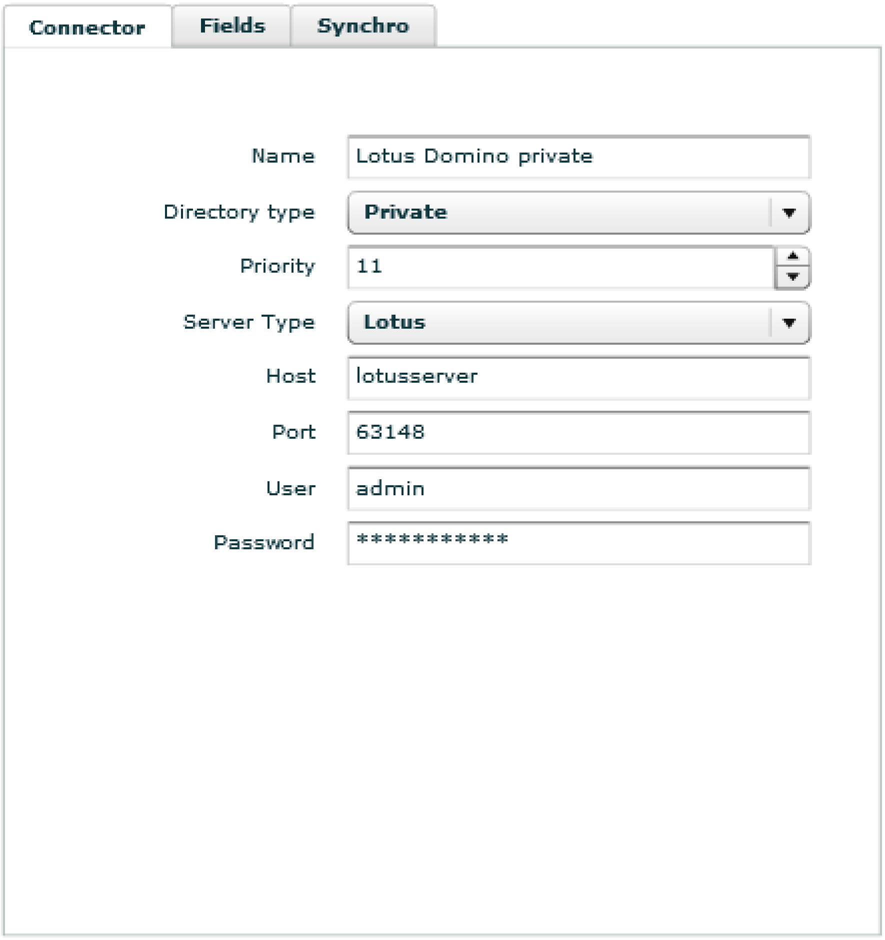
Table: Contacts

8.5. Lotus connector configuration

8.5.1. Configuration of public Lotus connector

The configuration of public Lotus directory is similar to an LDAP directory. See chapter 8.3 LDAP Connector.

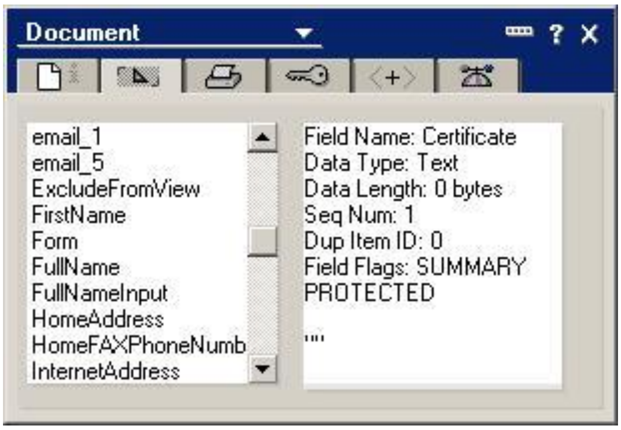
8.5.2. Configuration of private Lotus connector



Name: Lotus Domino private
Directory type: Private
Priority: 11
Server Type: Lotus
Host: lotusserver
Port: 63148
User: admin
Password: ***********

- **Host:** IP address or name of the Lotus server
- **Port:** Lotus server port (port per default: 63148)
- **User:** Lotus administrator name
- **Password:** Password of the Lotus administrator

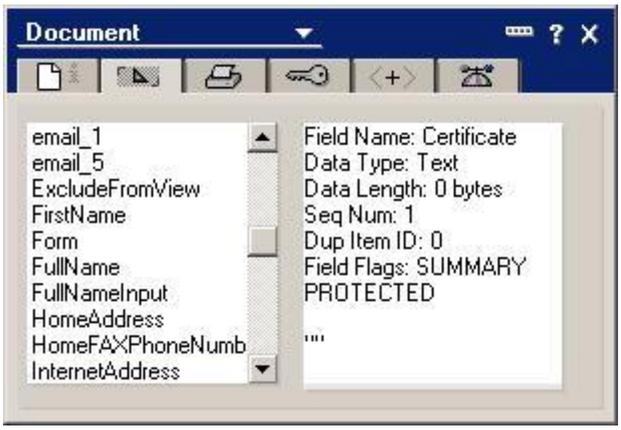
To find the required fields in the fields tab: in Lotus Notes, select a contact, right-click and select *Properties*, in the second section, you will find the list of fields to use.



email_1
email_5
ExcludeFromView
FirstName
Form
FullName
FullNameInput
HomeAddress
HomeFAXPhoneNumb
InternetAddress

Field Name: Certificate
Data Type: Text
Data Length: 0 bytes
Seq Num: 1
Dup Item ID: 0
Field Flags: SUMMARY PROTECTED

""



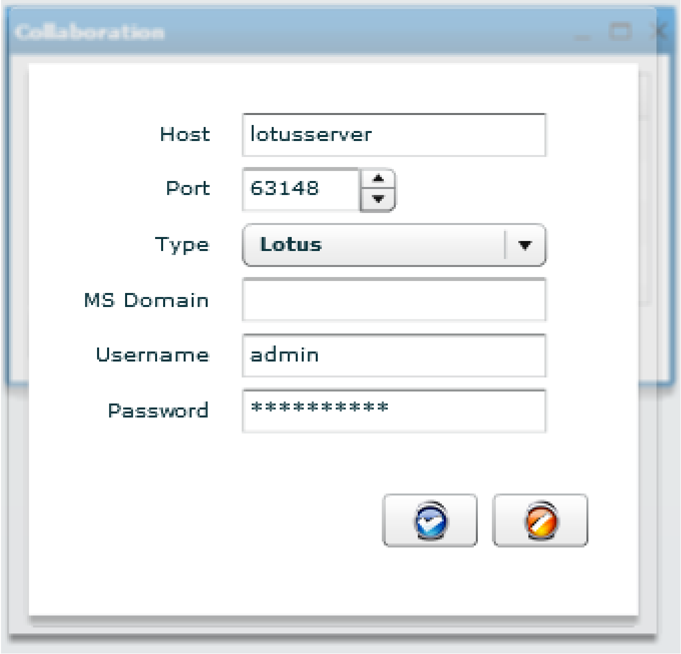
email_1
email_5
ExcludeFromView
FirstName
Form
FullName
FullNameInput
HomeAddress
HomeFAXPhoneNumb
InternetAddress

Field Name: Certificate
Data Type: Text
Data Length: 0 bytes
Seq Num: 1
Dup Item ID: 0
Field Flags: SUMMARY PROTECTED

""

8.5.3. Calendar connector

Open "*IT Management*" then "*Collaboration*", then click on "+" button.



Host lotusserver

Port 63148

Type Lotus

MS Domain

Username admin

Password **********

Define the IP 'address or the Lotus Domino server name.

Define the ID and the password to use to connect to the Domino server. This user must have reading access to all TWP users calendar.

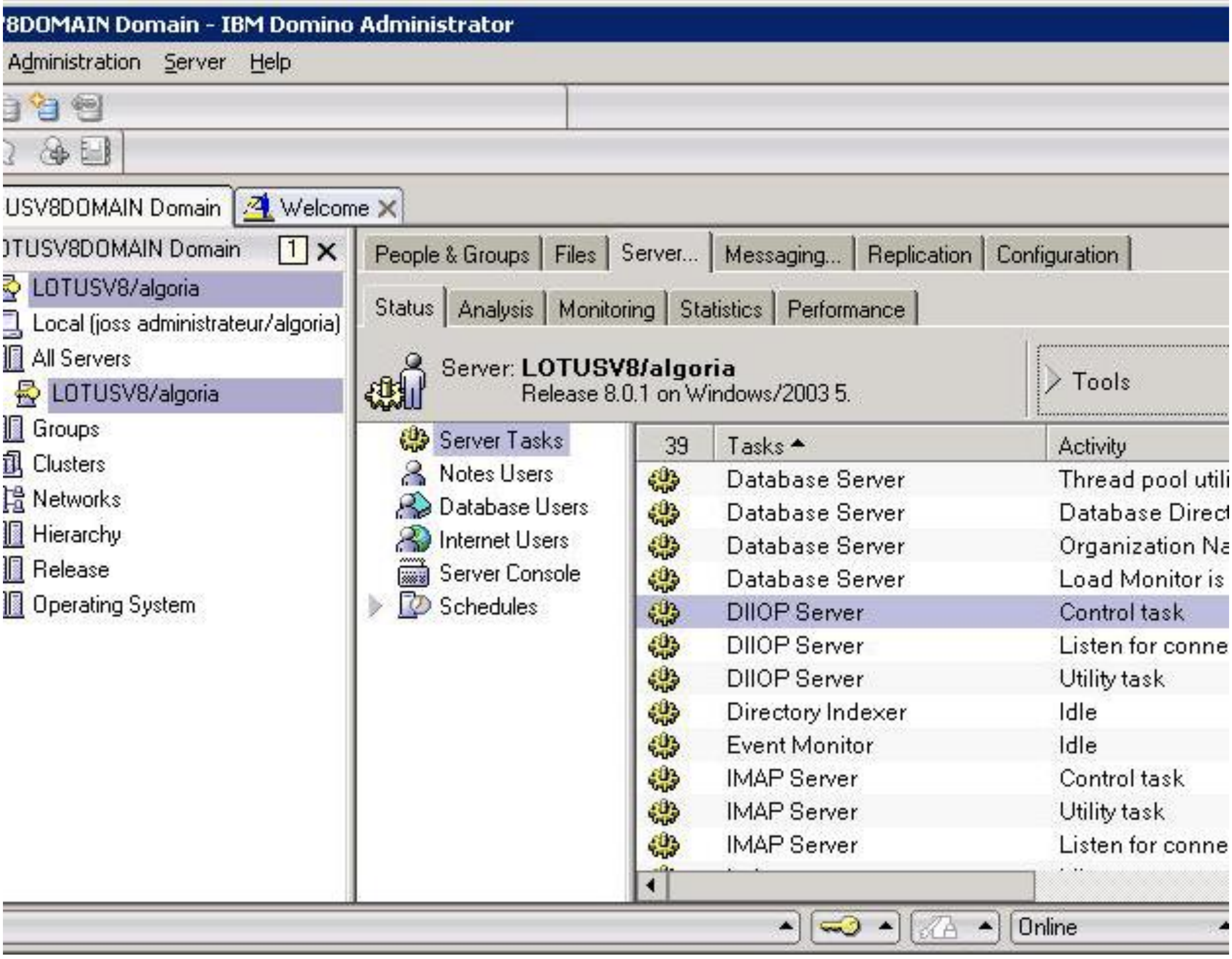
In order to be able to see the calendar presence of a user, make sure that the user mail address entered in the Email field of the user edit form is a valid address.

8.5.4. Configuration of the Lotus server

The Domino Server 8.0.1 version or higher are supported:

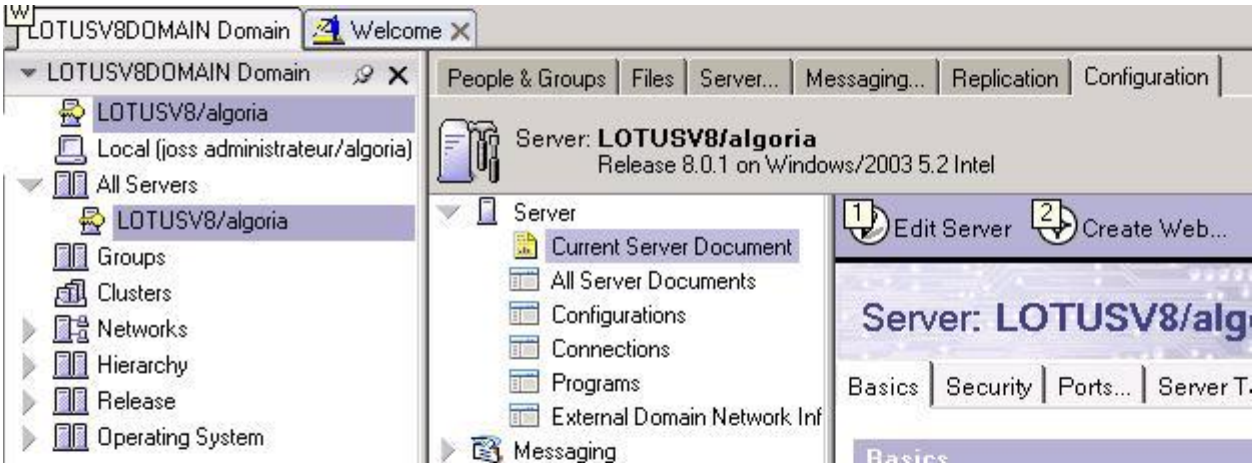
DIIOP Configuration: DIIOP is used by directory connector.

To check if the service is enabled, go to the section *Administration Server/Status* and find the *DIIOP* service:

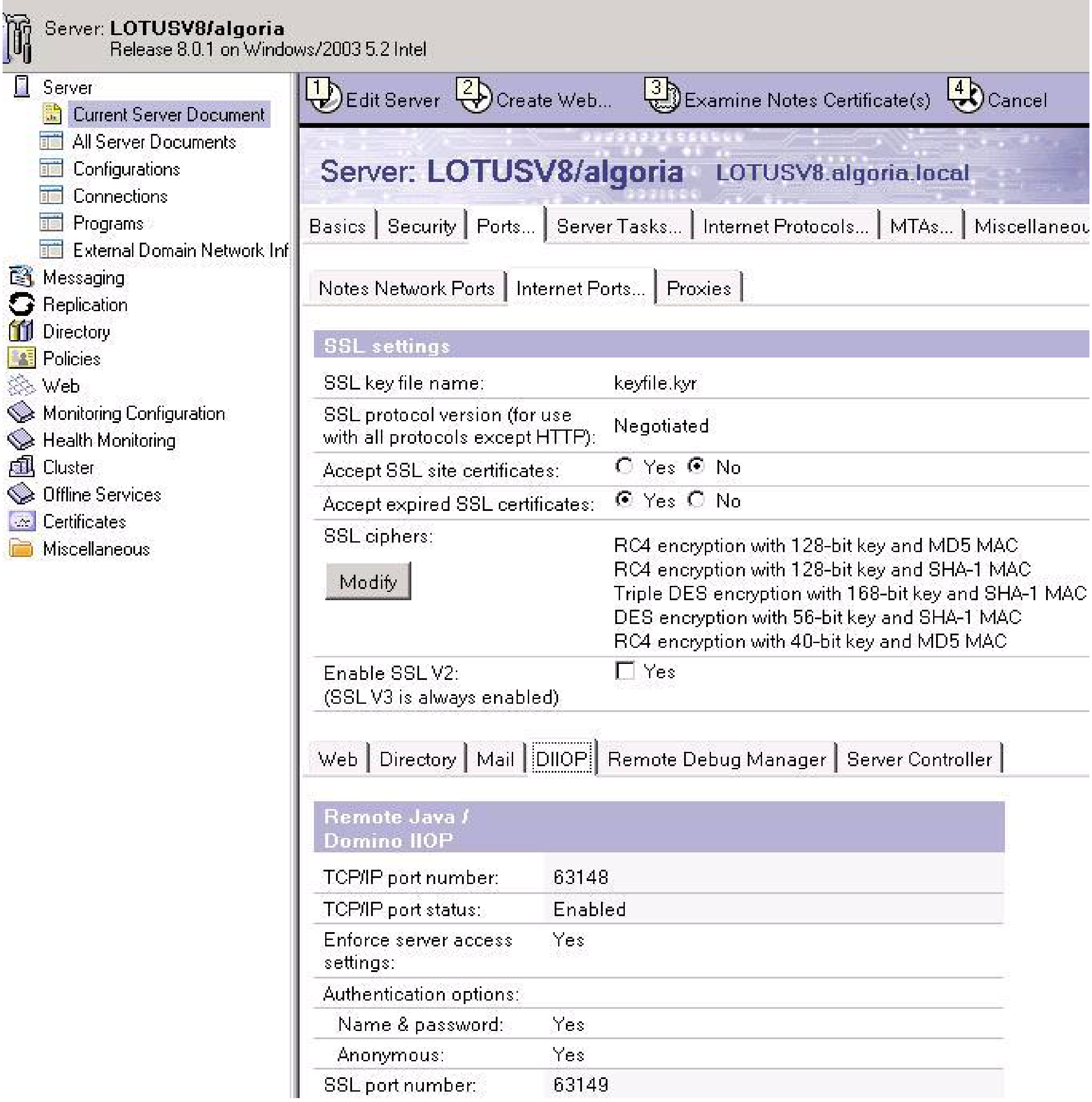


39	Tasks	Activity
	Database Server	Thread pool utili
	Database Server	Database Direct
	Database Server	Organization Na
	Database Server	Load Monitor is
	DIIOP Server	Control task
	DIIOP Server	Listen for conne
	DIIOP Server	Utility task
	Directory Indexer	Idle
	Event Monitor	Idle
	IMAP Server	Control task
	IMAP Server	Utility task
	IMAP Server	Listen for conne

Select the section *Configuration* and *Current server Document*.



You must now determine whether the DIIOP ports are configured:



Server: **LOTUSV8/algoria**
Release 8.0.1 on Windows/2003 5.2 Intel

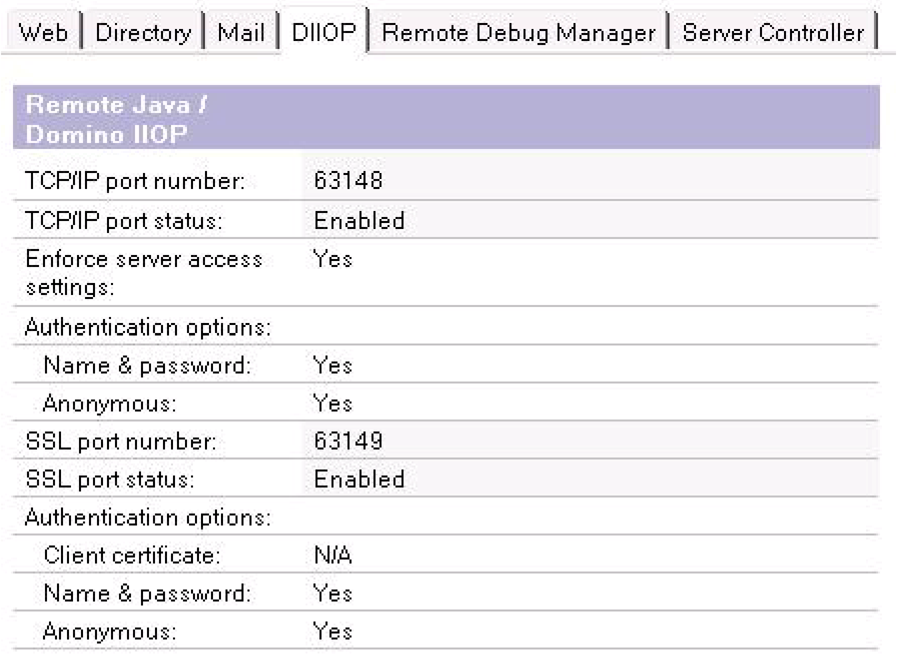
Server: LOTUSV8/algoria LOTUSV8.algoria.local

SSL settings

SSL key file name:	keyfile.kyr
SSL protocol version (for use with all protocols except HTTP):	Negotiated
Accept SSL site certificates:	○ Yes ● No
Accept expired SSL certificates:	● Yes ○ No
SSL ciphers:	RC4 encryption with 128-bit key and MD5 MAC RC4 encryption with 128-bit key and SHA-1 MAC Triple DES encryption with 168-bit key and SHA-1 MAC DES encryption with 56-bit key and SHA-1 MAC RC4 encryption with 40-bit key and MD5 MAC
Enable SSL V2: (SSL V3 is always enabled)	□ Yes

Remote Java / Domino IIOP

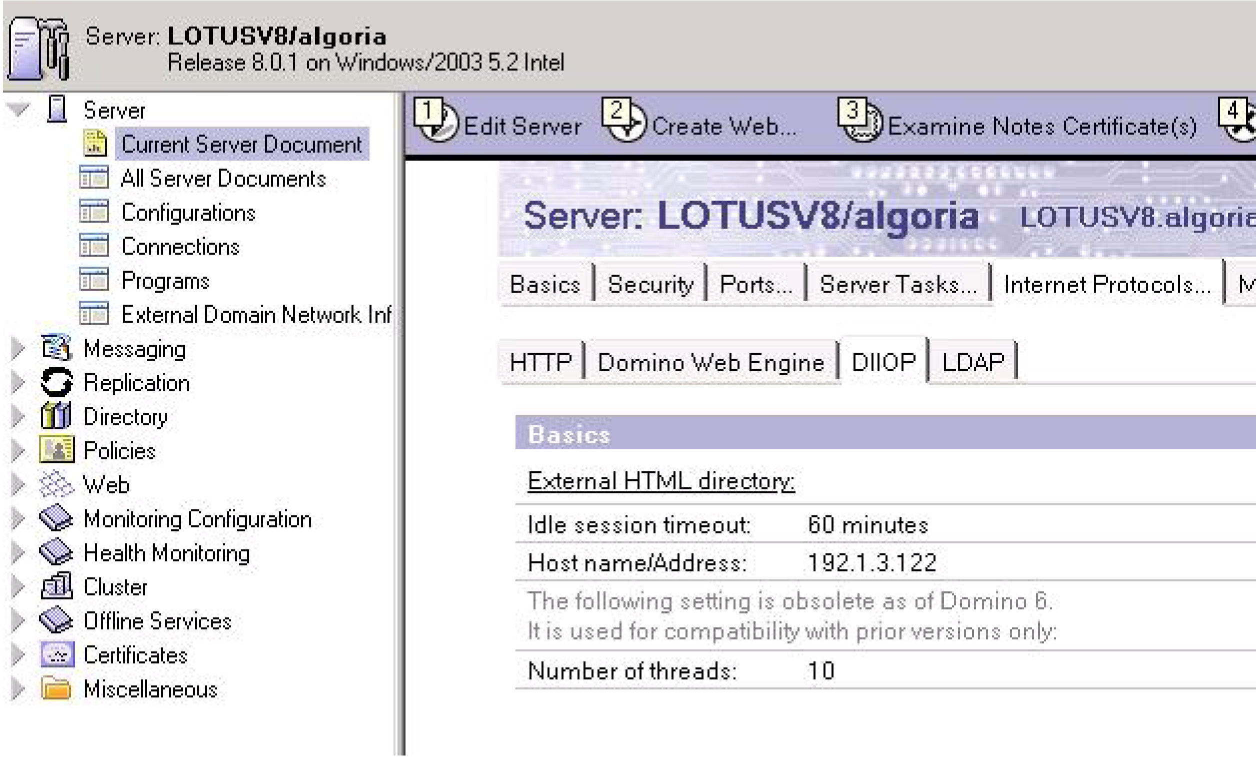
TCP/IP port number:	63148
TCP/IP port status:	Enabled
Enforce server access settings:	Yes
Authentication options:	
Name & password:	Yes
Anonymous:	Yes
SSL port number:	63149



Remote Java / Domino IIOP

TCP/IP port number:	63148
TCP/IP port status:	Enabled
Enforce server access settings:	Yes
Authentication options:	
Name & password:	Yes
Anonymous:	Yes
SSL port number:	63149
SSL port status:	Enabled
Authentication options:	
Client certificate:	N/A
Name & password:	Yes
Anonymous:	Yes

Verify that the IP address field is filled:



Basics

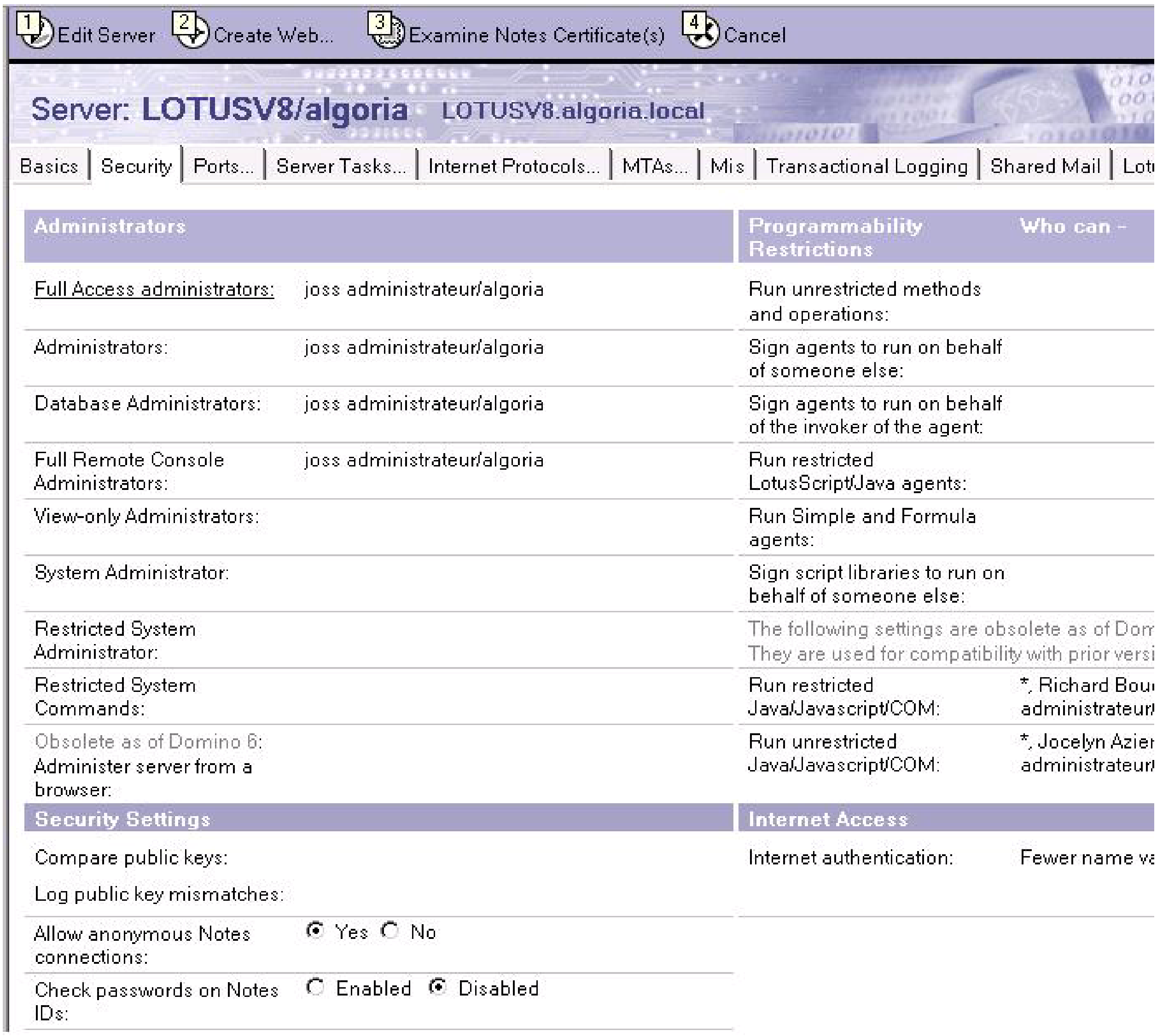
External HTML directory:

Idle session timeout:	60 minutes
Host name/Address:	192.1.3.122

The following setting is obsolete as of Domino 6.
It is used for compatibility with prior versions only:

Number of threads:	10

In the *Security* tab, you must add the Java options to users:

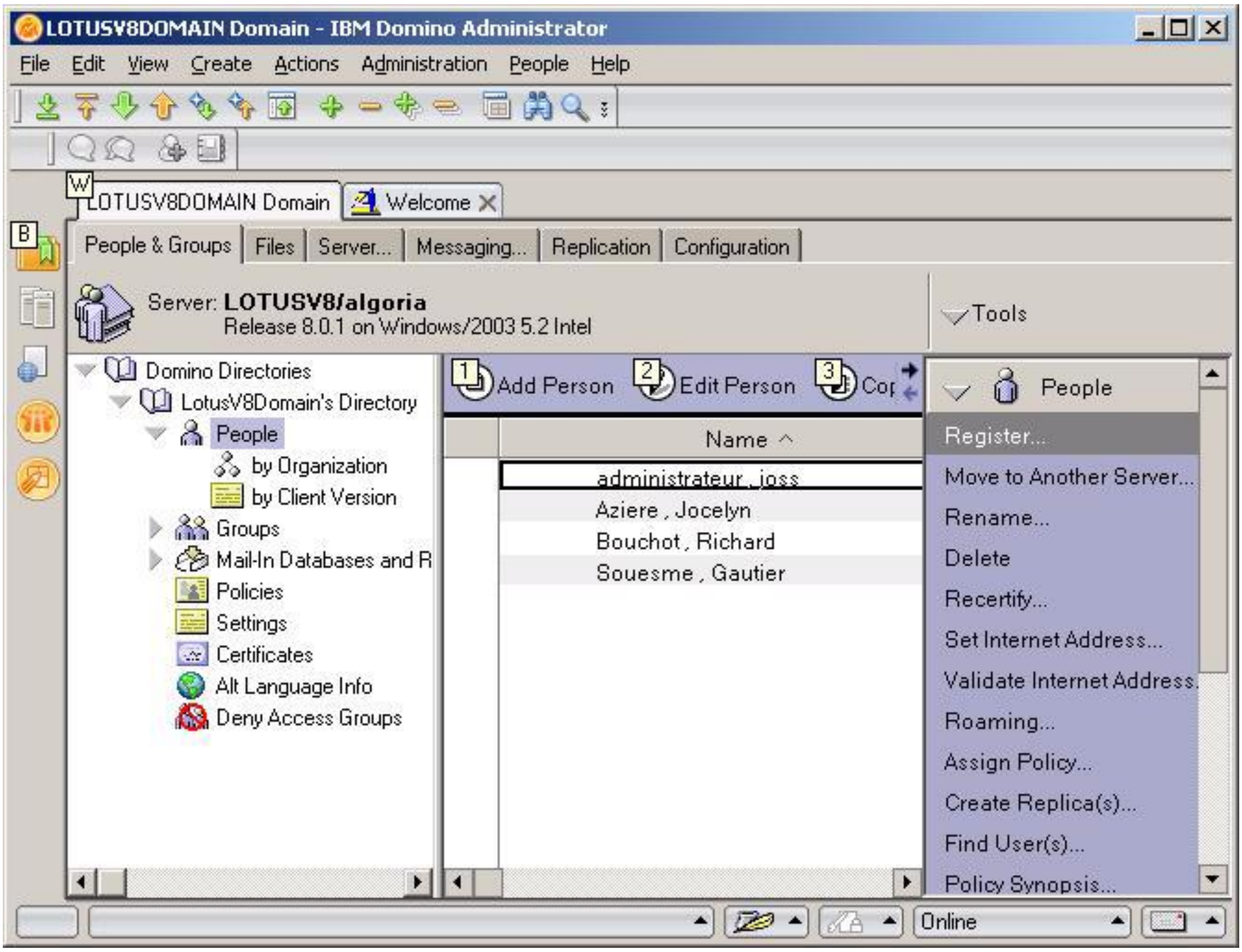


Server: LOTUSV8/algoria LOTUSV8.algoria.local

Administrators		Programmability Restrictions	Who can –
Full Access administrators:	joss administrateur/algoria	Run unrestricted methods and operations:	
Administrators:	joss administrateur/algoria	Sign agents to run on behalf of someone else:	
Database Administrators:	joss administrateur/algoria	Sign agents to run on behalf of the invoker of the agent:	
Full Remote Console Administrators:	joss administrateur/algoria	Run restricted LotusScript/Java agents:	
View-only Administrators:		Run Simple and Formula agents:	
System Administrator:		Sign script libraries to run on behalf of someone else:	
Restricted System Administrator:		The following settings are obsolete as of Dom They are used for compatibility with prior versi	
Restricted System Commands:		Run restricted Java/Javascript/COM:	*, Richard Bou administrateur/
Obsolete as of Domino 6: Administer server from a browser:		Run unrestricted Java/Javascript/COM:	*, Jocelyn Azier administrateur/
Security Settings		**Internet Access**	
Compare public keys:		Internet authentication:	Fewer name va
Log public key mismatches:			
Allow anonymous Notes connections:	● Yes ○ No		
Check passwords on Notes IDs:	○ Enabled ● Disabled		

Create and configure the Lotus user:

To create a new user, click on "*Register*":

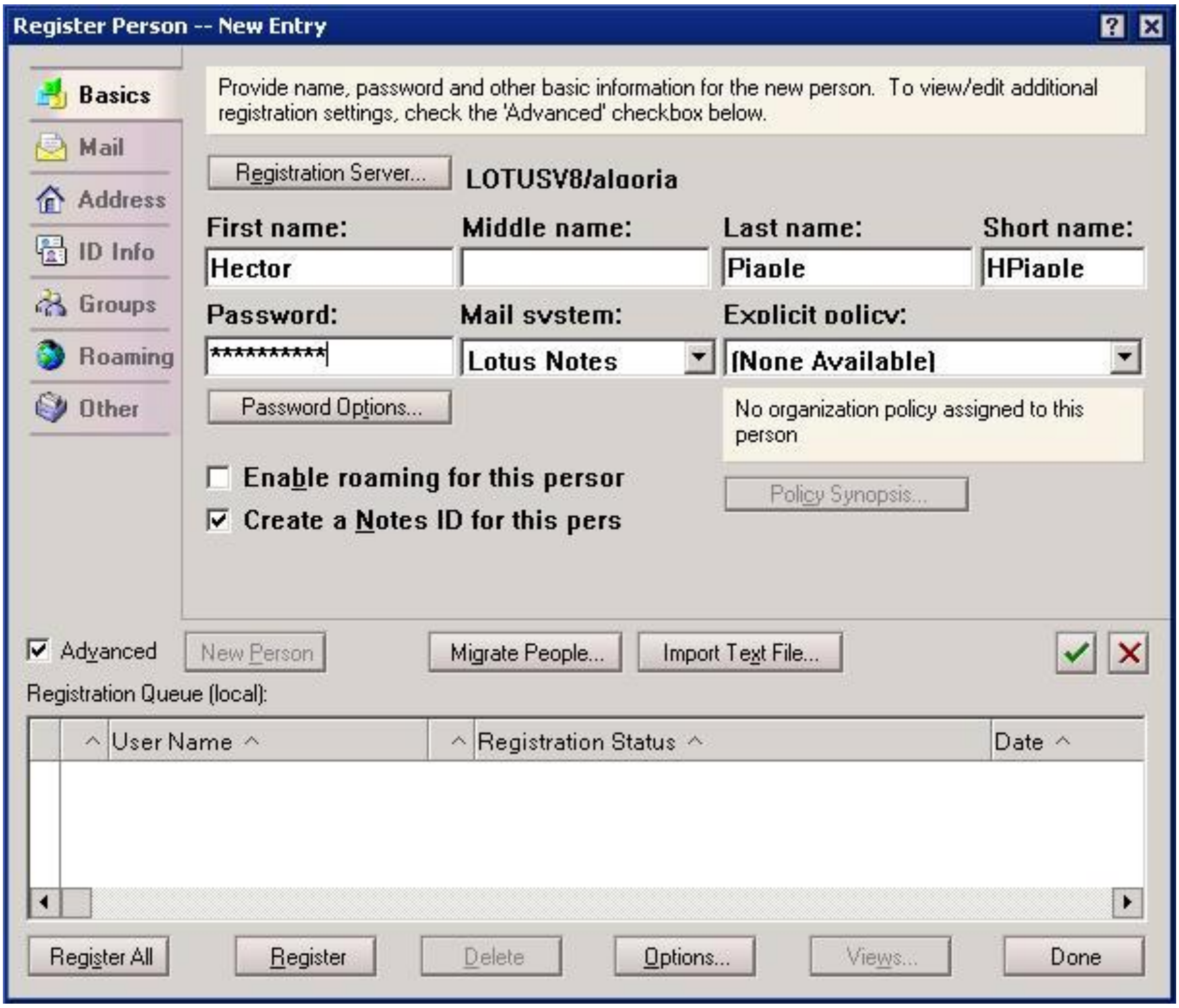


Server: LOTUSV8/algoria
Release 8.0.1 on Windows/2003 5.2 Intel

Name
administrateur , joss
Aziere , Jocelyn
Bouchot , Richard
Souesme , Gautier

Fill in the required fields.

Attention: *The short name must be the same as TWP user name.*



Register Person -- New Entry

Provide name, password and other basic information for the new person. To view/edit additional registration settings, check the 'Advanced' checkbox below.

Registration Server... LOTUSV8/algoria

First name: Hector

Middle name:

Last name: Piaple

Short name: HPiaple

Password: ***********

Mail system: Lotus Notes

Explicit policy: [None Available]

No organization policy assigned to this person

□ Enable roaming for this persor

☑ Create a Notes ID for this pers

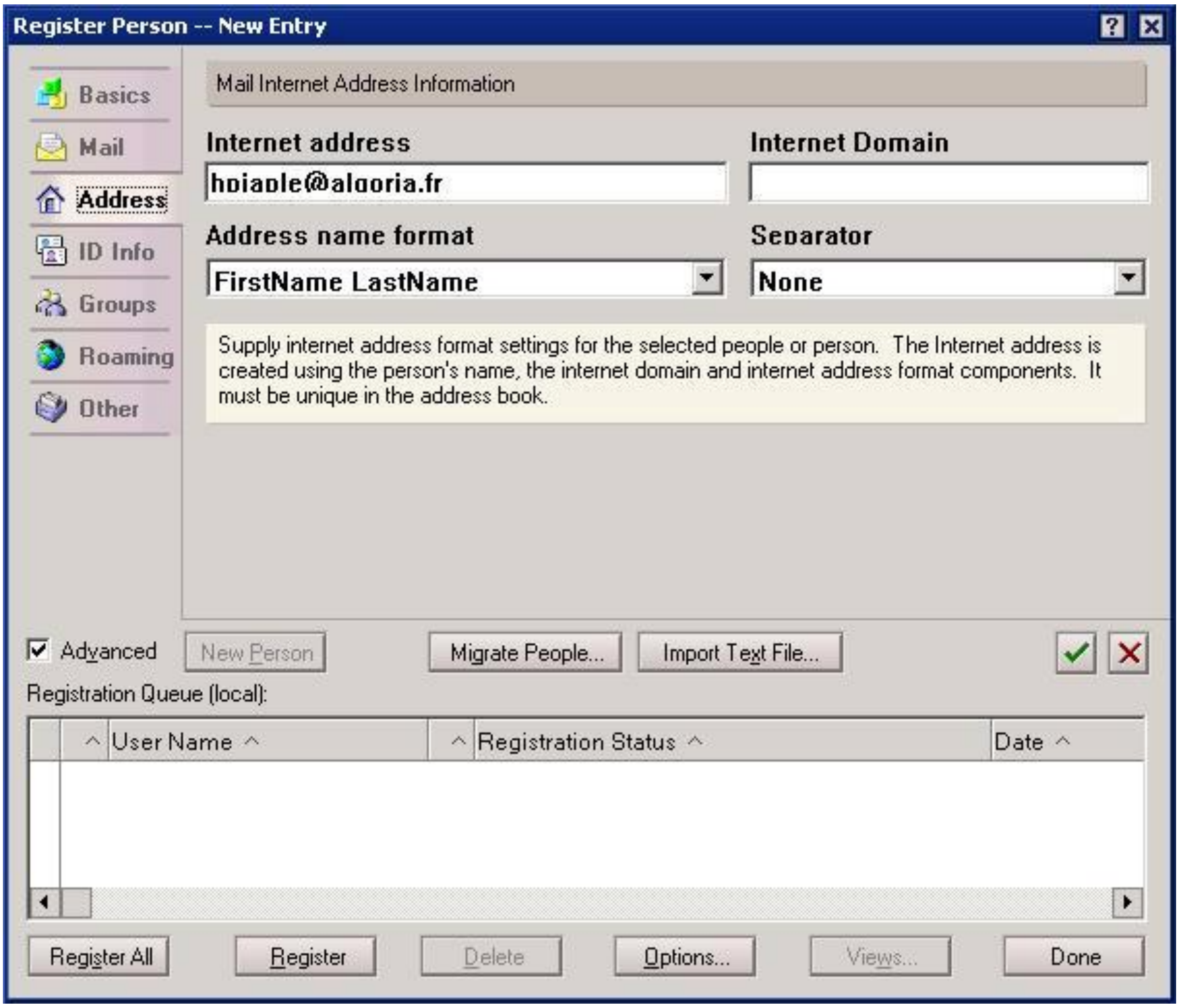
☑ Advanced

Registration Queue (local):

User Name	Registration Status	Date

Select the Address section. In Internet address, enter the email address of the user. Complete all required fields.

Attention: *This email address must be the same as that entered in TWP.*



Register Person -- New Entry

Mail Internet Address Information

Internet address: hpiaple@algoria.fr

Internet Domain:

Address name format: FirstName LastName

Separator: None

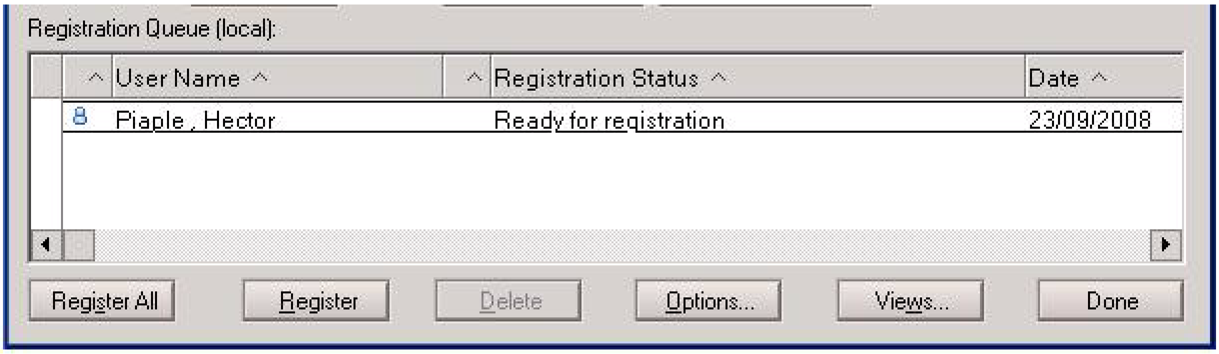
Supply internet address format settings for the selected people or person. The Internet address is created using the person's name, the internet domain and internet address format components. It must be unique in the address book.

☑ Advanced

Registration Queue (local):

User Name	Registration Status	Date

Once all your contacts have been created, click on “Register all”.



Registration Queue (local):

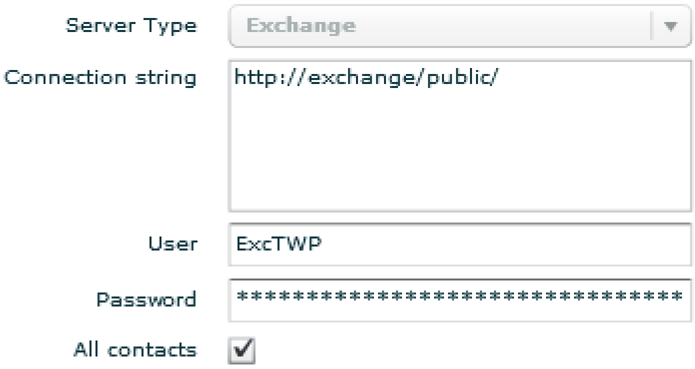
User Name	Registration Status	Date
Piaple , Hector	Ready for registration	23/09/2008

8.6. Directories / Calendar MS Exchange 2003/2007

8.6.1. Creating a public directory connector

Connecting to an Exchange server directory is defined as follows.

<u>Connector tab:</u>



Server Type	Exchange ▾
Connection string	http://exchange/public/
User	ExcTWP
Password	********************************
All contacts	☑

Directory type:

- *Public contacts*: select TWP for a connection to public directories.
- *Private contacts of users*: Select **Private** for a connection to private contact of the Exchange user.

Attention: Make sure the email address of the user is entered in the Email field in the edit user form and it is the same as its Exchange email address.

Server type: Exchange.

Connection string: This is the URL that opens the Exchange directory, TWP supports HTTP and HTTPS URLs. Exchange 2007 uses HTTPS by default .
The URL is usually: http://exchangeservername/public.

User / password: The login is used by TWP to connect to the Exchange server.

- *Public contacts*: This account must have the rights to read and write on the Exchange directory.
- *Private contacts of users*: This account must have read permissions on private contacts of the user mailbox.

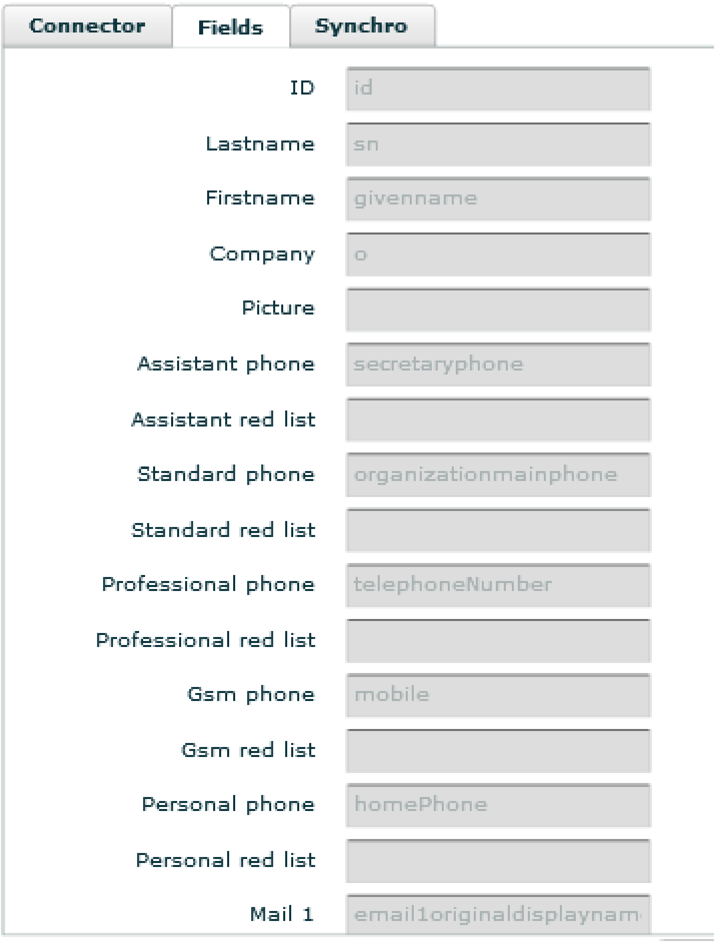
All contacts: If “All contacts” box is checked, it will allow to search contacts in sub-folders / directories.

If you want to limit syncing contacts to a directory, add the name of the directory at the end of the connection URL, for example: “http://192.168.0.1/public/commerce” and uncheck the "All Contacts" box.

Attention: Also make sure that the permissions are set correctly, see chapter 7.4.2.

<u>Fields tab:</u>

For Exchange directories, the fields are pre-filled.



ID	id
Lastname	sn
Firstname	givenname
Company	o
Picture	
Assistant phone	secretaryphone
Assistant red list	
Standard phone	organizationmainphone
Standard red list	
Professional phone	telephoneNumber
Professional red list	
Gsm phone	mobile
Gsm red list	
Personal phone	homePhone
Personal red list	
Mail 1	email1originaldisplaynam

However, you can add fields to the private field’s cells. 10 private fields can be used, from *Private 0 (Private0) to 9 (Private9)*. These fields can be configured manually.

See below examples of Exchange fields that could be used:

- givenName = last name
- sn = name
- o = company
- secretaryphone = assistant phone number
- mobile = mobile number
- homePhone = home phone number
- organizationmainphone = standard phone number
- account
- authorig
- bday = birthday date

- businesshomepage = company web page (URL)
- callbackphone
- customerid
- departement
- email1
- email2
- email3
- employeenumber

- facsimiletelephonenumber = fax number
- ftpsite
- homeCity = employee city
- homeCountry = employee country
- homefax
- homephone2
- telephonenumber2
- office2telephonenumber
- othermobile
- otherTelephone
- pager

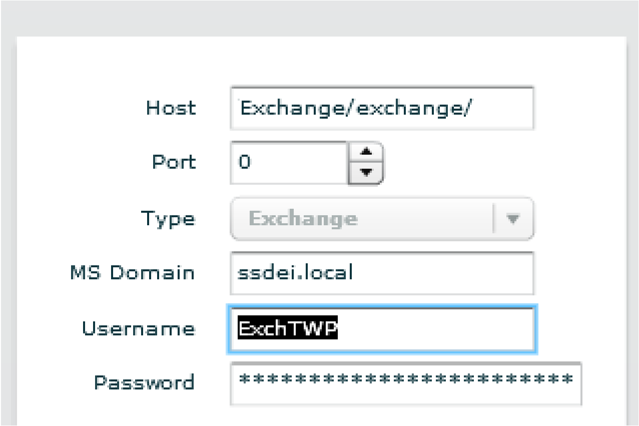
All fields are accessible at this address:
http://msdn.microsoft.com/en-us/library/office/aa563261(v=exchg.80).aspx

Information: Always set the prefix urn:schemas:contacts: in case the single field does not work. E.g. urn:schemas:contacts:mobile

8.6.2. Calendar connector

TWP allows users to see the events of other TWP user’s calendar from their contact list and in the directory search (see user guide TWP Caller).

In the administration menu, open "*IT Management*" then "*Collaboration*", then click on “+”.



Host: Exchange/exchange/

Port: 0

Type: Exchange

MS Domain: ssdei.local

Username: ExchTWP

Password: ************************

It is possible to define more than one link.

Set the URL of your Exchange server depending on the configuration of your server: http://server_exchange/exchange/ or https://server_exchange/exchange/.

Set the username and password to use to connect to the Exchange server: this user must have the rights to read TWP users' calendars.

Attention: In order to be able to see the calendar events of a TWP user, make sure that the email entered in the Email field in edit user form is their email address Exchange.

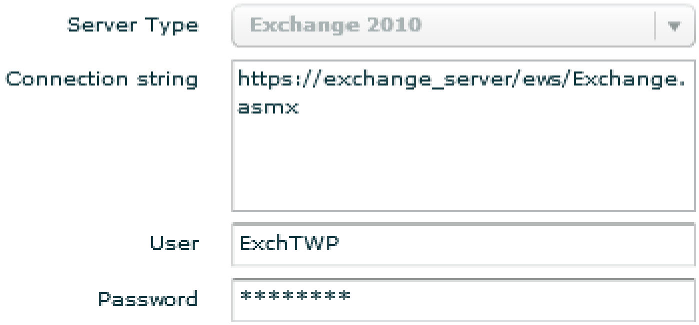
Attention: Also make sure that the permissions are set correctly, see chapter 7.4.3.

8.7. Directories / Calendar MS Exchange 2010 / Office 365

8.7.1. Create a public / private connector

Connecting to an Exchange server or Office 365 online directory is defined as follows.

Connector tab:



Server Type: Exchange 2010

Connection string: https://exchange_server/ews/Exchange.asmx

User: ExchTWP

Password: ********

Directory type:

- *Public contacts*: select TWP for a connection to public directories. **(only Exchange 2010)**
- *Private contacts of users*: Select **Private** for a connection to private contact of the Exchange user.

Attention: Make sure the email address of the user is entered in the Email field in the edit user form and it is the same as its Exchange email address.

Server type: Exchange 2010. ***(Even for a connection to Office 365)***

Connection string: This is the URL that entitles access to Exchange Web Services to get contacts.
The URL for Exchange 2010 is usually: https://exchangeservername/ews/exchange.asmx.
For Office 365, the URL is: https://outlook.office365.com/ews/Exchange.asmx.

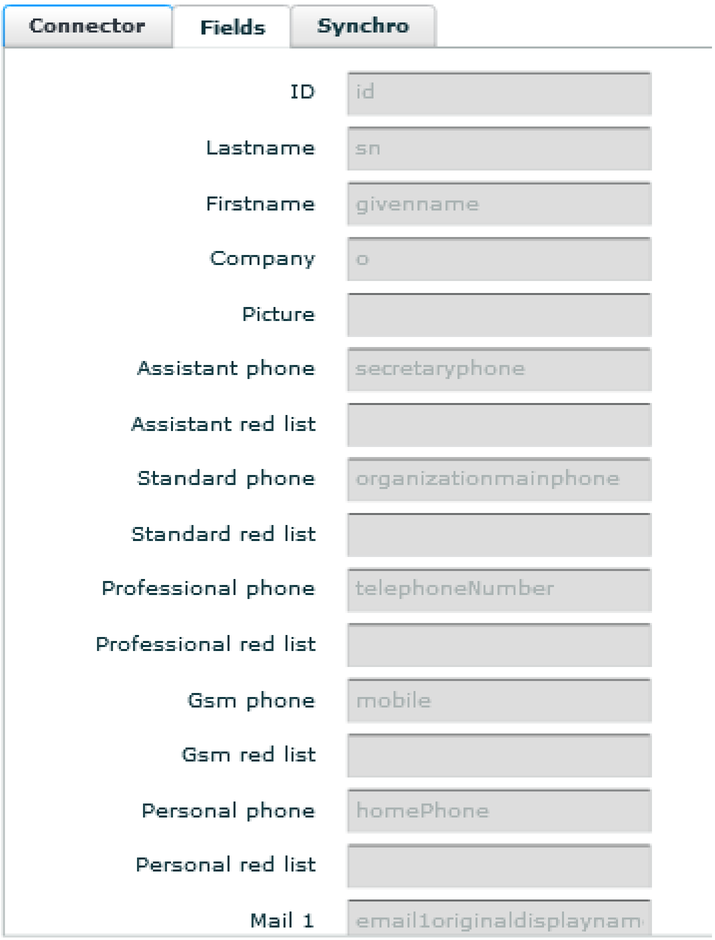
User / password: The login is used by TWP to connect to the Exchange server.

- *Public contacts* ***(only Exchange 2010)***: This account must have the rights to read on the Exchange directories.
- *Private contacts of users*: There is different ways to allow the connection. See section 8.7.5.

Attention: Make sure that the permissions are set correctly, see chapter 7.4.2.

Fields tab:

For Exchange directories, the fields are pre-filled.



ID	id
Lastname	sn
Firstname	givenname
Company	o
Picture	
Assistant phone	secretaryphone
Assistant red list	
Standard phone	organizationmainphone
Standard red list	
Professional phone	telephoneNumber
Professional red list	
Gsm phone	mobile
Gsm red list	
Personal phone	homePhone
Personal red list	
Mail 1	email1originaldisplaynam

However, you can add fields to the private field's cells. 10 private fields can be used, from *Private 0 (Private0) to* 9 *(Private9)*. These fields can be configured manually.

See below examples of Exchange fields that could be used:

- AssistantName
- AssistantPhone
- Birthday
- BusinessAddress
- BusinessAddressCity
- BusinessAddressCountry
- BusinessAddressPostalCode
- BusinessAddressState
- BusinessAddressStreet
- BusinessFax
- BusinessHomePage
- BusinessPhone
- BusinessPhone2
- CallbackPhone
- CarPhone
- Categories
- Children
- Comment
- Companies
- CompanyName
- CompanyPhone

- CompleteName
- ConversationId
- CreatedTime
- Culture
- Department
- DisplayName
- EffectiveRights
- Email1Address
- Email1DisplayAs
- Email1DisplayName
- Email1Type
- Email2Address
- Email2DisplayAs
- Email2DisplayName
- Email2Type
- Email3Address
- Email3DisplayAs
- Email3DisplayName
- Email3Type
- EntryId
- Gender
- Generation
- GivenName
- HasAttachments
- HasPicture
- HomeAddress
- HomeAddressCity
- HomeAddressCountry
- HomeAddressPostalCode
- HomeAddressState
- HomeAddressStreet
- HomeFax
- HomePhone
- HomePhone2
- Id
- Importance
- Initials
- InstantMessengerAddress1
- InstantMessengerAddress2
- InstantMessengerAddress3
- IsAssociated
- IsHidden
- ItemClass
- ItemId
- JobTitle
- LastModifiedTime
- LastModifierName
- Manager
- MiddleName
- Mileage
- MimeContent
- MobilePhone
- Nickname
- OfficeLocation
- OtherAddress
- OtherAddressCity
- OtherAddressCountry

- OtherAddressPostalCode
- OtherAddressState
- OtherAddressStreet
- OtherFax
- OtherPhone
- Pager
- ParentId
- PrimaryPhone
- Profession
- RadioPhone
- SearchKey
- SelectedMailingAddress
- Sensitivity
- Size
- SpouseName
- Subject
- Surname
- Title
- WeddingAnniversary

All fields are accessible at this address:
http://msdn.microsoft.com/en-us/library/office/aa581315(v=exchg.140).aspx

8.7.2. Tip Exchange 2010: connecting to a selection of public folder(s)

In the connection string of an Exchange 2010 connector, it is possible to sync only selected folders.
Format of a connection string with a selection of folders:
https://exchange_server/ews/Exchange.asmx|public|folder1,folder2/subfolder1/subfolder2,...

Attention: It is important to be careful of the folder tree and the case sensitive. Several files can be filled by separating them with a comma ",". Subfolders are separated from the parent folders by "/".

Example: https://exchange_server/ews/Exchange.asmx|public|General/Algo Distributors/Export,General/Algo suppliers

8.7.3. Tip Office 365: private directory goes public

To allow users to view the same contacts from a single connector to Office 365, you can configure it in public.
This connector will synchronize private contacts of a single user but all users authorized will access.
The information to enter are below:

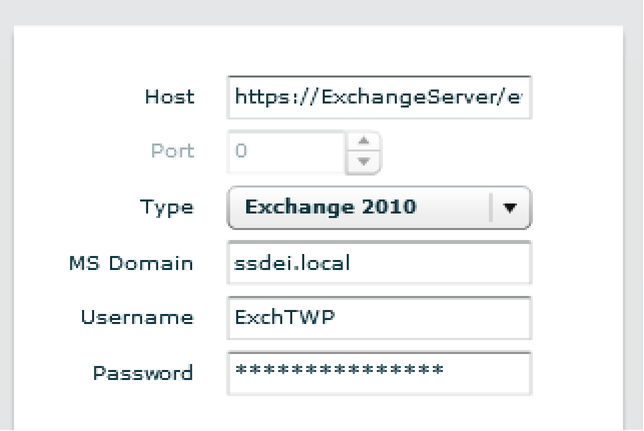
Directory type: TWS

Server type: Exchange 2010
Connection string: https://outlook.office365.com/ews/Exchange.asmx|user
User: email account to sync

8.7.4. Calendar connector

TWP allows users to see the events of other TWP user's calendar from their contact list and in the directory search (see user guide TWP Caller).

In the administration menu, open "*IT Management*" then "*Collaboration*", then click on "+".



Host: https://ExchangeServer/e
Port: 0
Type: Exchange 2010
MS Domain: ssdei.local
Username: ExchTWP
Password: ***************

It is possible to define more than one link.

Set the URL of your Exchange server: https://server_exchange/ews/Exchange.asmx

Set the username and password to use to connect to the Exchange server: this user must have the rights to read TWP users' calendars.

Attention: In order to be able to see the calendar events of a TWP user, make sure that the email entered in the Email field in edit user form is their email address Exchange.

Attention: Also make sure that the permissions are set correctly, see chapter 7.4.3.

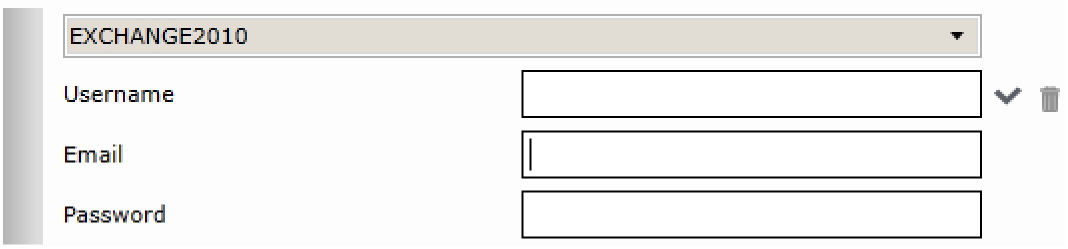
8.7.5. Accounts for private connectors

To allow the connectors to get the private contacts and calendar appointments of Exchange 2010 or Office 365 users, it is possible to define different ways to login:

- *Exchange/Office 365 account having access to the user's inbox (see chapter 8.7.6)*: This account must have read permission on private contacts and calendar of the user mailbox.

- *Exchange/Office 365 account with no special privileges*: each user can add Viewer authorization in their mail client Outlook for the account in question.

- *Exchange/Office 365 account for collaboration*: to fill directly in the Caller Application (*Preferences menu*, *Contact*, *Collaboration*).



EXCHANGE2010

Username

Email

Password

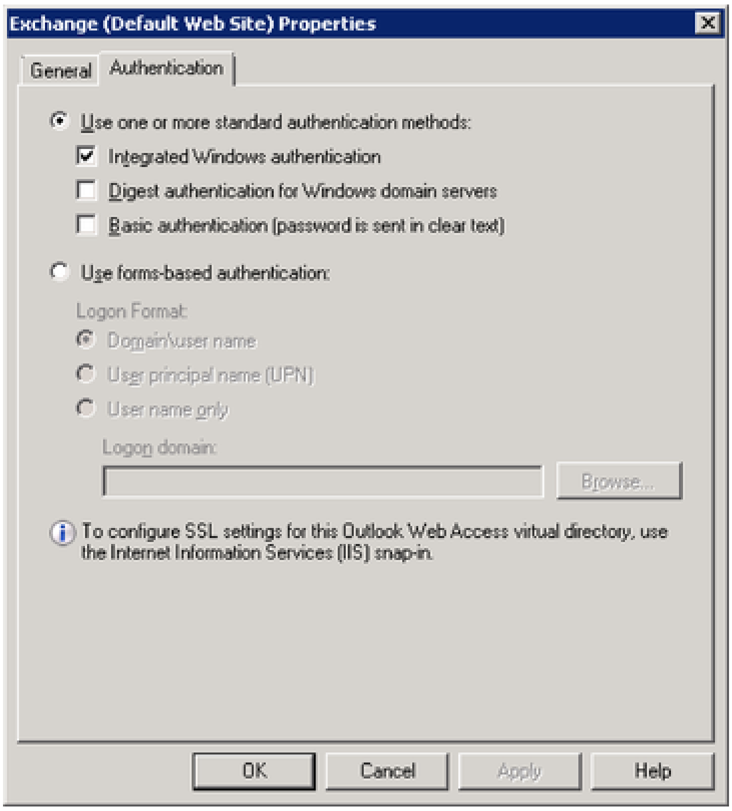
  - *Username* : Name of the user who is allowed to read the contents of the mailbox (can be the same as the email)
  - *Email* : email account to sync
  - *Password* : Account password to sync

8.7.6. Configuration of Exchange server: Access to users' mailboxes (private contacts and calendar)

Configuration of the authentication type

The server uses the NTLM authentication with "Integrated Windows Authentication" or "Basic authentication" modes.
After changing authentication type, the exchange server must restart.
In the Exchange Management Console, Microsoft Exchange -> Server Configuration -> Mailbox -> Tab WebDAV, double click on:

- Exchange (Default Web Site) and check “Integrated Window authentication" or "Basic authentication" box in “Authentication” tab.



Exchange (Default Web Site) Properties

● Use one or more standard authentication methods:

☑ Integrated Windows authentication

□ Digest authentication for Windows domain servers

□ Basic authentication (password is sent in clear text)

○ Use forms-based authentication:

Logon Format:

● Domain\user name

○ User principal name (UPN)

○ User name only

Logon domain:

To configure SSL settings for this Outlook Web Access virtual directory, use the Internet Information Services (IIS) snap-in.

- Exchweb (Default Web Site) and check “Integrated Window authentication" or "Basic authentication" box in “Authentication” tab.

- Public (Default Web Site) and check “Integrated Window authentication" or "Basic authentication" box in “Authentication” tab.

Configuration of access rights

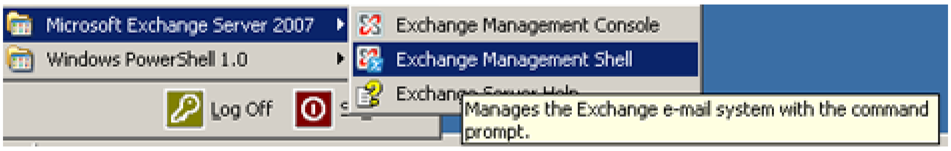
2 possible solutions

1. Give access rights on all Exchange server mailboxes
2. Give access rights from MS Outlook

Solution 1: Give “Receive-As” rights on all Exchange server mailboxes

First you must declare a user with a dedicated Exchange mailbox.
Then use the Management Shell to give read permissions on all the boxes for that particular user:

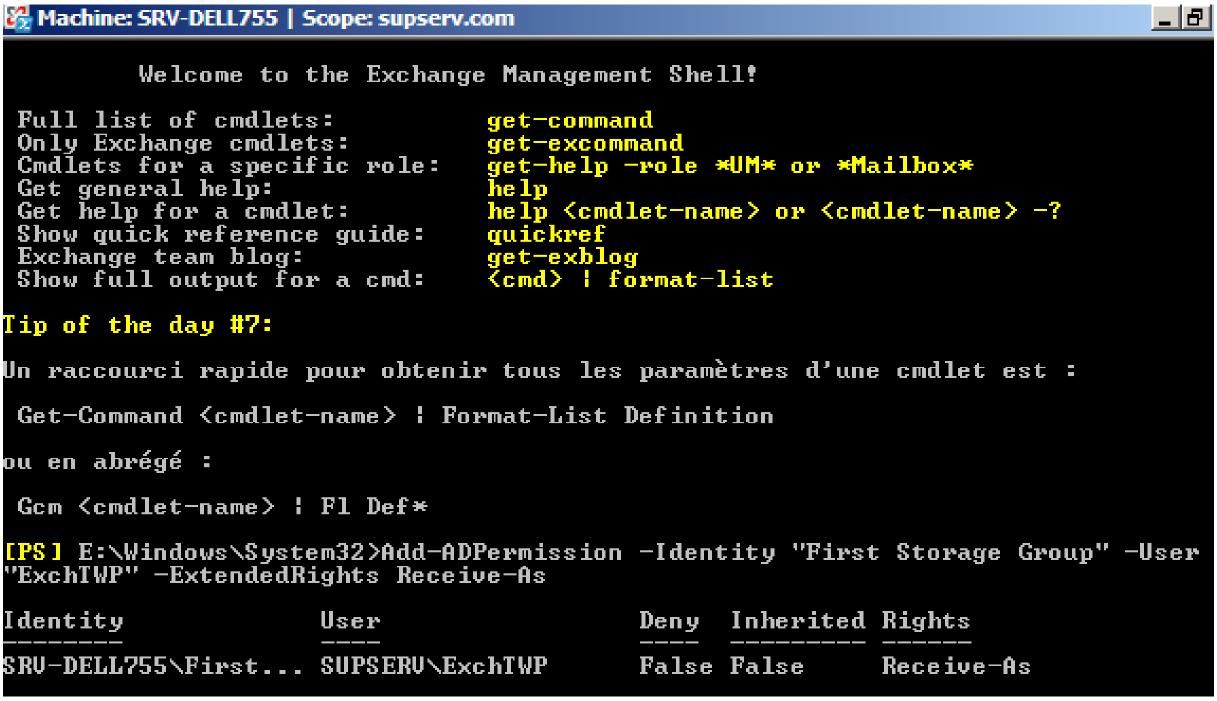
Click on “Start” → “All programs” → “Microsoft Exchange Server…” → “Exchange Management Shell”.


Microsoft Exchange Server 2007
Windows PowerShell 1.0
Log Off
Exchange Management Console
Exchange Management Shell
Exchange Server Help
Manages the Exchange e-mail system with the command prompt.

To give “Receive-As” rights on all boxes:

```
Add-ADPermission -Identity "Mailbox Store" -User "Trusted User" -ExtendedRights
Receive-As
```

Replace "Mailbox Store" with the name of exchange database ("First Storage Group" in below example) and "Trusted User" with the name of the dedicated user (“ExchTWP” in the example).



```
         Welcome to the Exchange Management Shell!

 Full list of cmdlets:          get-command
 Only Exchange cmdlets:         get-excommand
 Cmdlets for a specific role:   get-help -role *UM* or *Mailbox*
 Get general help:              help
 Get help for a cmdlet:         help <cmdlet-name> or <cmdlet-name> -?
 Show quick reference guide:    quickref
 Exchange team blog:            get-exblog
 Show full output for a cmd:    <cmd> | format-list

Tip of the day #7:

Un raccourci rapide pour obtenir tous les paramètres d’une cmdlet est :

 Get-Command <cmdlet-name> | Format-List Definition

ou en abrégé :

 Gcm <cmdlet-name> | Fl Def*

[PS] E:\Windows\System32>Add-ADPermission -Identity "First Storage Group" -User
"ExchTWP" -ExtendedRights Receive-As

Identity              User                Deny  Inherited Rights
--------              ----                ----  --------- ------
SRV-DELL755\First...  SUPSERV\ExchTWP     False False     Receive-As
```

To verify the rights granted, execute the following command:

```
Get-ADPermission -Identity "Mailbox Store" -User "Trusted User"
```

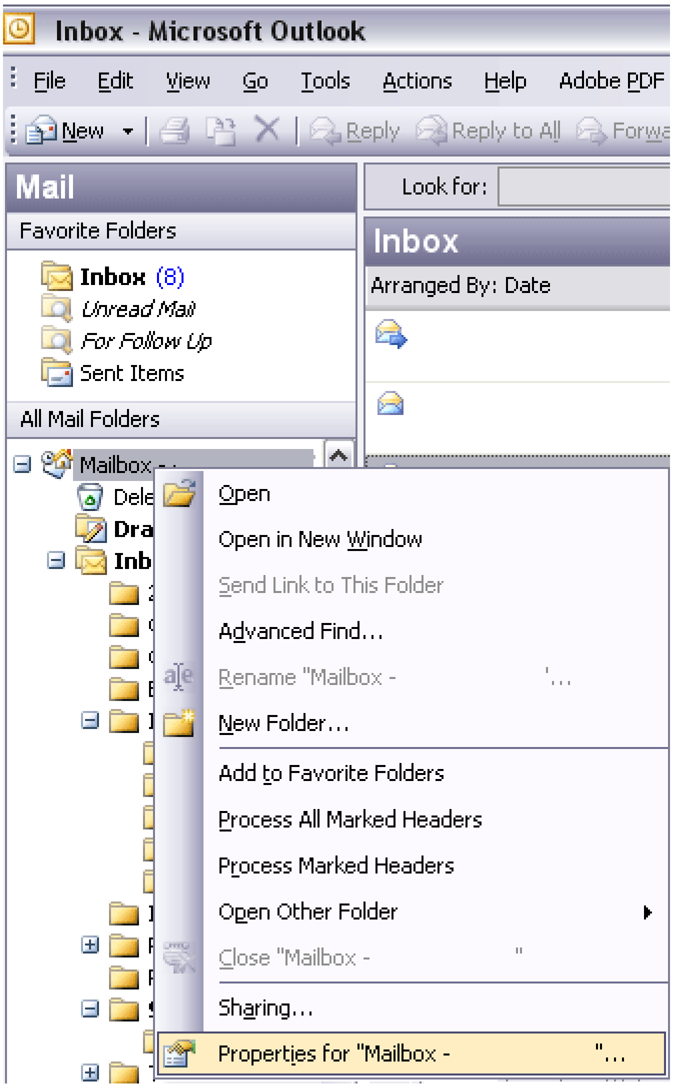
To remove the "Receive-As" rights, execute the following command:

```
Remove-ADPermission -Identity "Mailbox Store" -User "Trusted User" -ExtendedRights
Receive-As
```

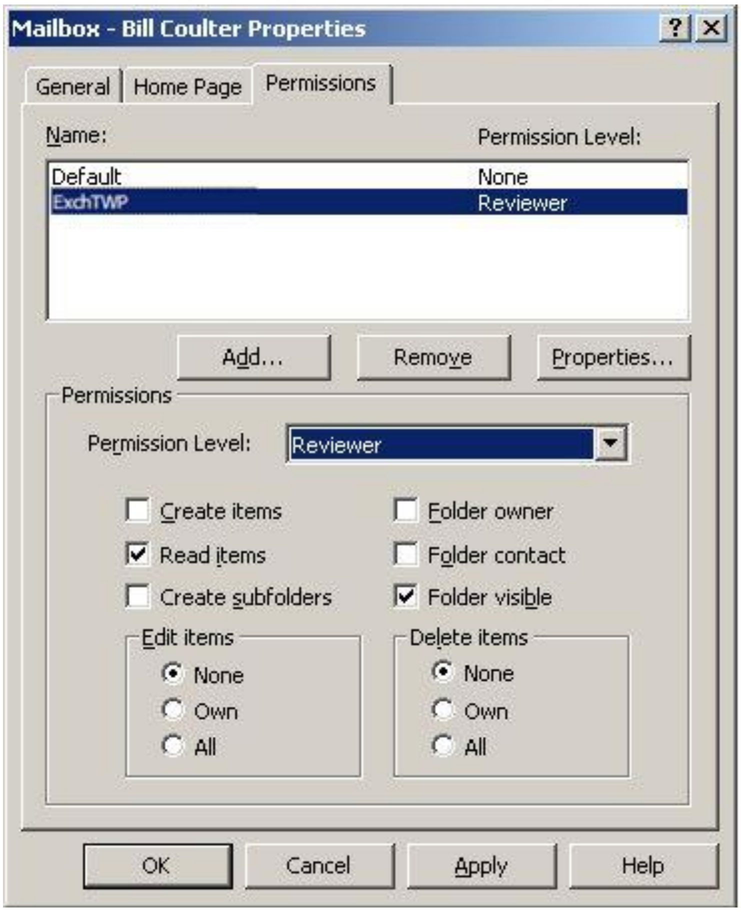
Note: it takes a few minutes so that the rights are taken into account, or the service can be restarted ("Microsoft Exchange Information Store").

Solution 2: Give rights from MS Outlook

From Outlook, select “Inbox”, right click and select *properties*.



Give the Reviewer rights to the dedicated user (“ExchTWP” in the example).



Name:	Permission Level:
Default	None
ExchTWP	Reviewer

Permissions

Permission Level: Reviewer

☐ Create items ☐ Folder owner

☑ Read items ☐ Folder contact

☐ Create subfolders ☑ Folder visible

Edit items: ● None ○ Own ○ All

Delete items: ● None ○ Own ○ All

Also to share his calendar, do the same configuration on the Calendar tab.

8.8. Outlook Add-In Client

The Outlook add-in client lets users to recover directly via their Caller their private contacts Outlook connected to Exchange or not.

8.8.1. Prerequisites

Compatible systems

- Windows Server 2012 / Windows Server 2012 R2
- Windows Server 2008 / Windows Server 2008 R2
- Windows Server 2003
- Windows 8
- Windows 7
- Windows Vista
- Windows XP

Necessary applications

- Microsoft .Net Framework 4.0 Full package
- Having launched once the Caller Application
- Compatible Microsoft Outlook versions:
    - Microsoft Outlook 2013
    - Microsoft Outlook 2010
    - Microsoft Outlook 2007 (partially)

      Attention: With Microsoft Outlook 2007, no display of the synchronization button is present in Microsoft Outlook. Only the automatic synchronization of contacts at the start of Microsoft Outlook is available.
- The TWP Server versions compatible are the versions *greater or equal than 4.1.1341*.

Protocols and Ports

The AddInOutlook need to access to the TWP server through the following list of ports:

- Link to web services: HTTP port *8000*.

8.8.2. Installation

Install the application

In the DVD, look for AddInOutlook. Run the file *setup.exe*. Follow the installation window, and click the "next" button to move from one stage to another. Installation takes about 1 to 2 minutes.

What is installed with this package:

- TWS_AddInOutlook

8.8.3. Configuration

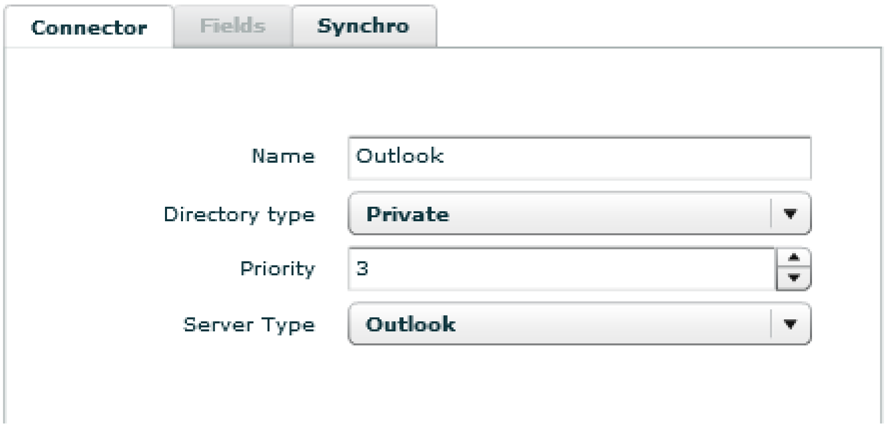
TWP Server

1. *Creating the Outlook directory*

The TWP server version must be 4.1.1341 or higher.

You must create an Outlook directory in administration server by clicking the "+" button in the menu *IT Management / Directories*:

- Put the name you want.
- Choose "Private" value as directory type.
- Select the priority you want (more the priority is low, more the directory will be at the top priority for name resolution ...).
- And select the server type "*Outlook*" then save your directory.



Name: Outlook

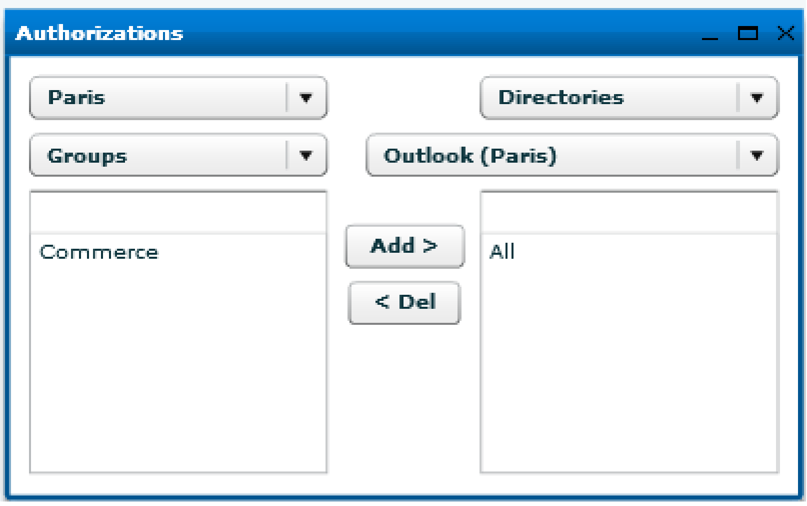
Directory type: Private

Priority: 3

Server Type: Outlook

2. *Allow access to the Outlook directory*

So that the AddInOutlook can copy private Outlook contacts in the server database, you must allow users who installed the AddInOutlook to use the Outlook directory (see below).



Paris

Groups

Commerce

Directories

Outlook (Paris)

All

Here all users in the user group "All" have the rights to use the Outlook directory of the domain Paris.

Attention: You must allow users and user groups to the Outlook directory of their domains. In the example above the "All" group is part of the domain "Paris".

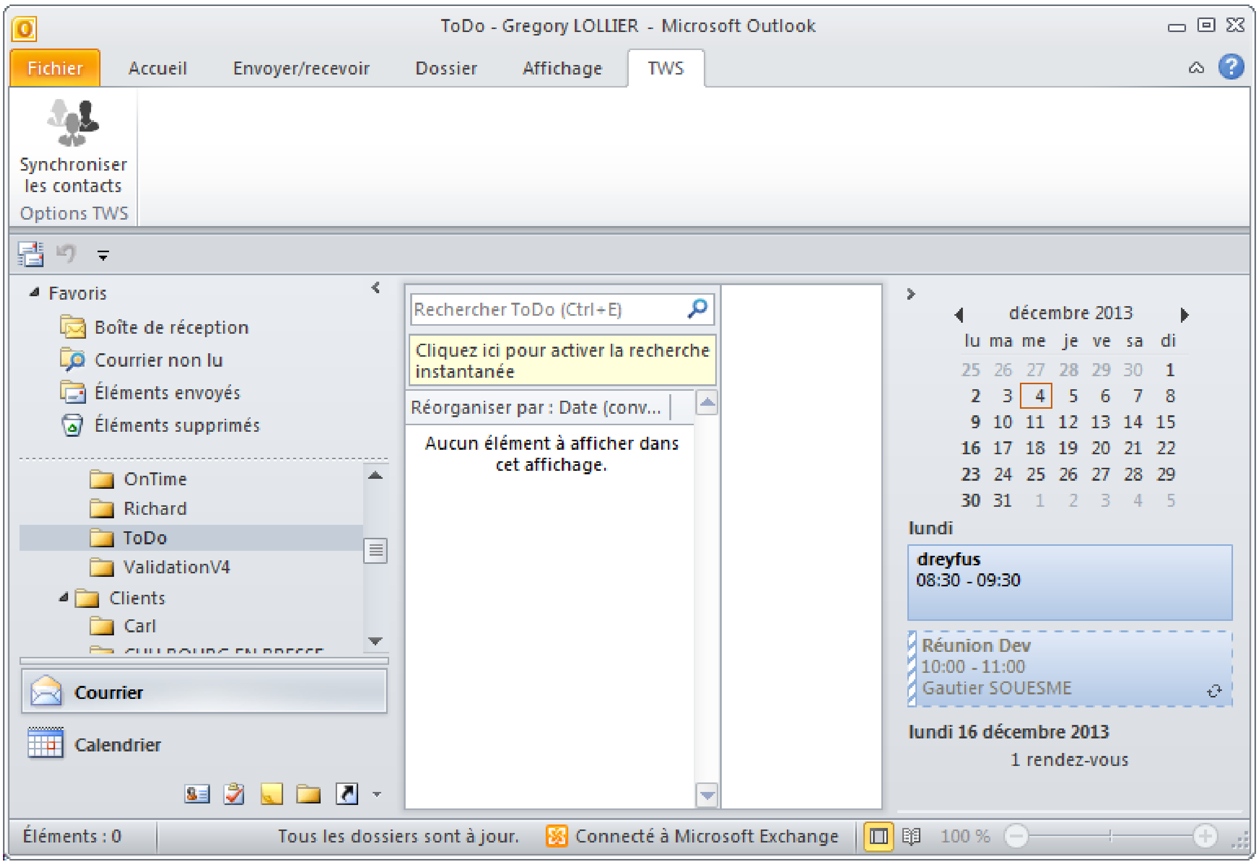
3. Identification

The identification of the user, to which Microsoft Outlook contacts will be synchronized, is done through the Caller application. You must at least have started once your Caller application after the installation of the AddInOutlook.

8.8.4. Using

Users who installed the AddInOutlook, will see (after restarting Microsoft Outlook) a new tab named "TWP". In this tab, users will find a button to synchronize their private Microsoft Outlook contacts. Every click on this button synchronize your contacts to the TWP server.

Also, synchronizing contacts is done automatically each time you restart Microsoft Outlook.



8.8.5. Maintenance

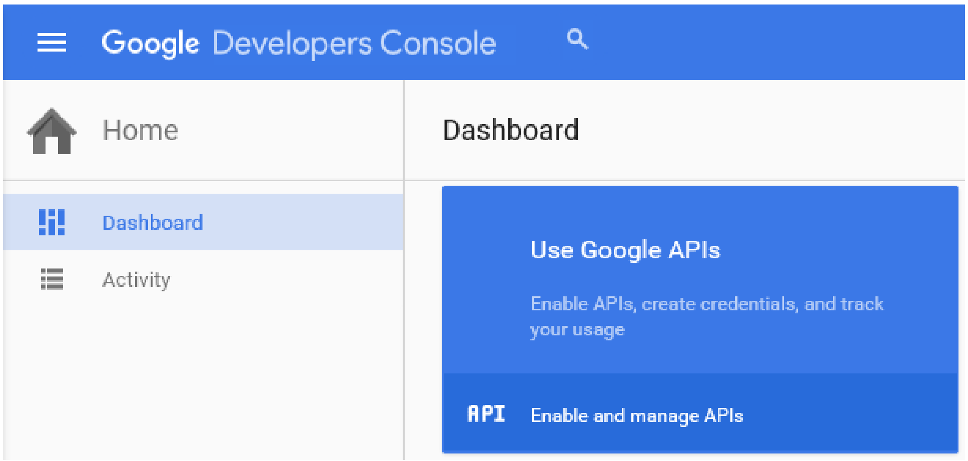
The AddInOutlook application logs in Log_AddInOutlook.txt file in the temporary files on the computer that is running Microsoft Outlook.

8.9. Google Apps Integration

8.9.1. Google Apps Account Setup

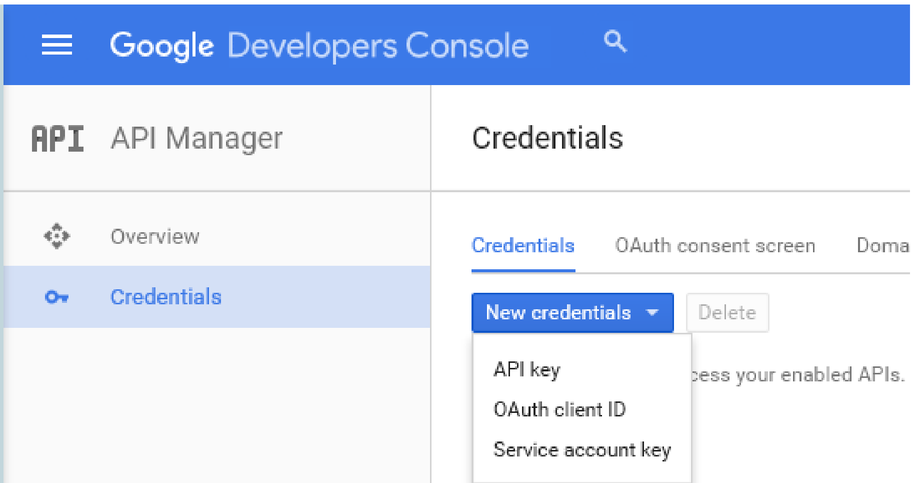
Creating a Google Apps new project

Go to: https://console.developers.google.com/project and create a new project. Open this project and then go to "*Use Google APIs*" then "*Credentials*".

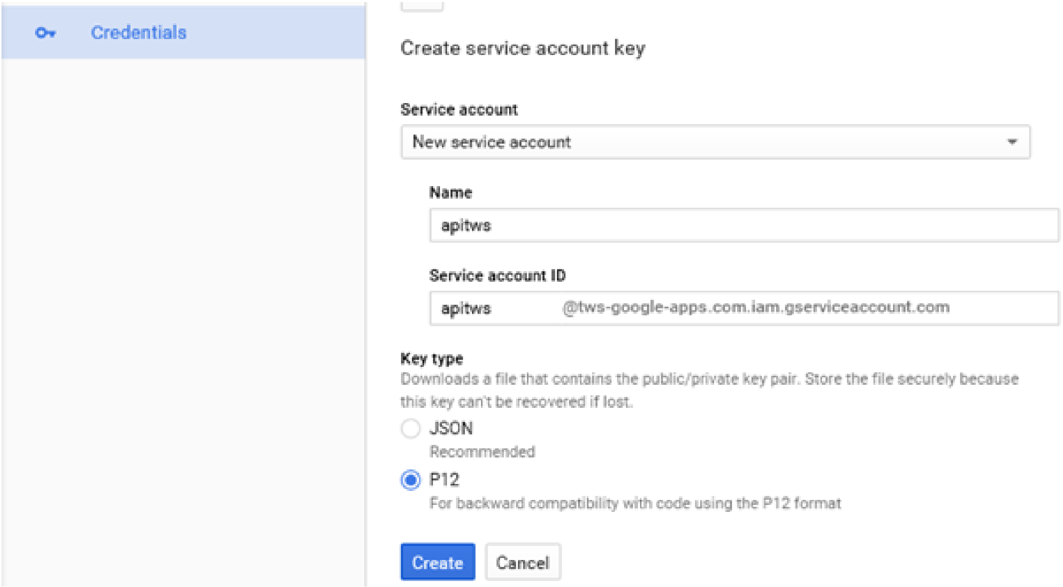

Google Developers Console
Home
Dashboard
Dashboard
Activity
Use Google APIs
Enable APIs, create credentials, and track your usage
API
Enable and manage APIs

Creating a Service account key

In "*Credentials*" and then "*Credentials*" tab, create the new credentials. Choose "*Service account key*".



Then choose "*New Service Account*" and enter a name for this account. Here is "*apitws*". Then select "*P12*" and do "*Create*".



Create service account key

Service account: New service account

Name: apitws

Service account ID: apitws @tws-google-apps.com.iam.gserviceaccount.com

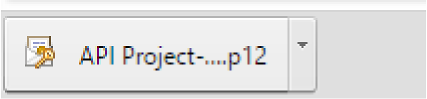
Key type

Downloads a file that contains the public/private key pair. Store the file securely because this key can't be recovered if lost.

○ JSON
Recommended

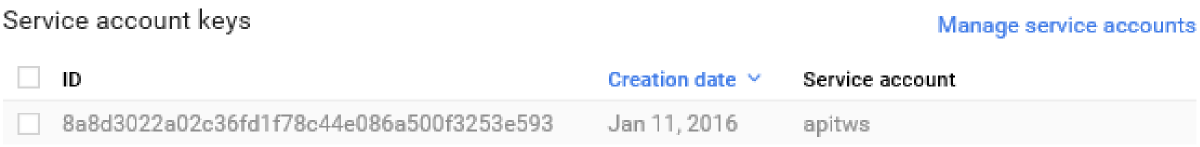
● P12
For backward compatibility with code using the P12 format

The browser will offer to download a *P12 file*. Save this file on your computer.



API Project-....p12

The service account key is created.

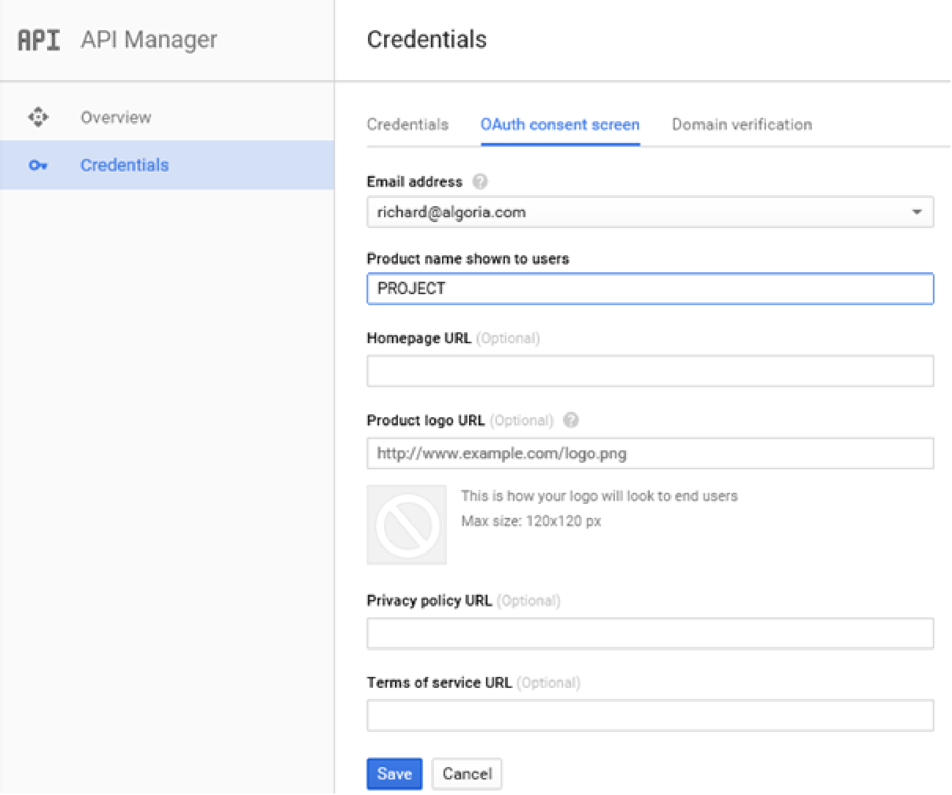


Service account keys

□	ID	Creation date	Service account
□	8a8d3022a02c36fd1f78c44e086a500f3253e593	Jan 11, 2016	apitws

Creating a Client ID associated with the service account key

Before creating the client ID, you must enter a product name. In the menu "Credentials" and the "OAuth consent Screen" tab, enter a product name as below:



Email address: richard@algoria.com

Product name shown to users: PROJECT

Homepage URL (Optional)

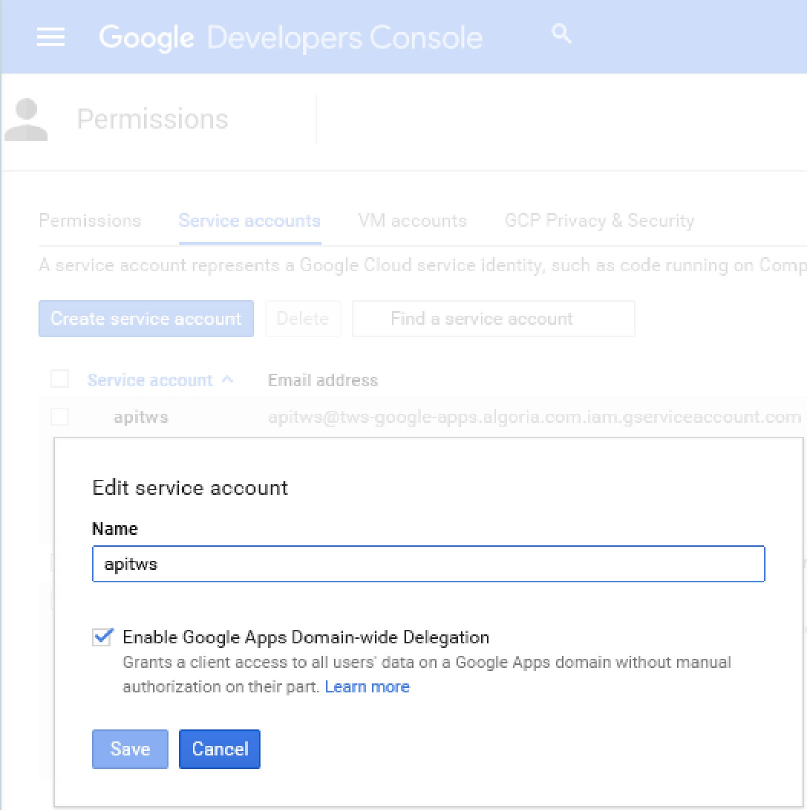
Product logo URL (Optional): http://www.example.com/logo.png

Privacy policy URL (Optional)

Terms of service URL (Optional)

Then in the "*Credentials*" menu and the "*Credentials*" tab, click "*Manage Service Accounts*" under "*Service Account Keys*". Select the account created and at the right the button allows you to edit the account.

Check the "*Enable Google Apps Domain-wide Delegation*" box and save.



A service account represents a Google Cloud service identity, such as code running on Comp

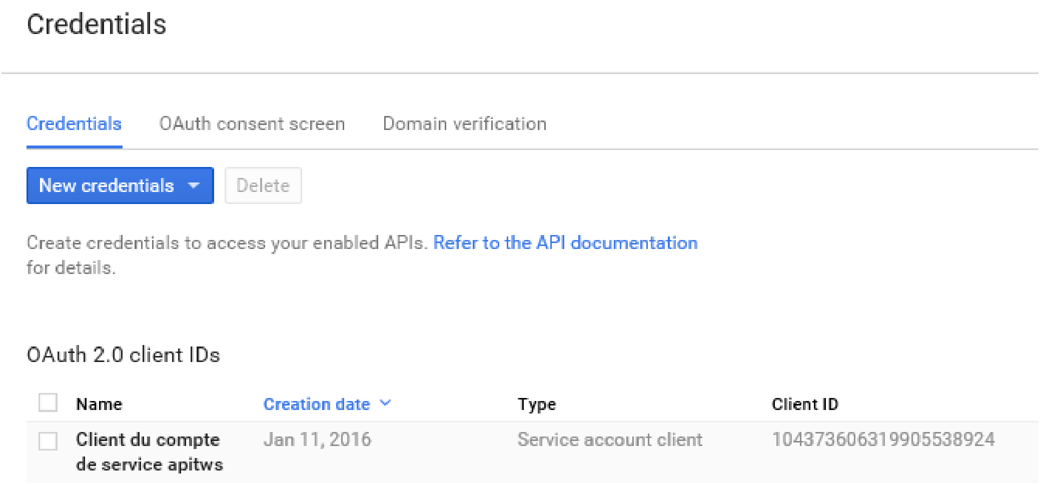
Service account	Email address
apitws	apitws@tws-google-apps.algoria.com.iam.gserviceaccount.com

Edit service account

Name: apitws

☑ Enable Google Apps Domain-wide Delegation
Grants a client access to all users' data on a Google Apps domain without manual authorization on their part. Learn more

Thus, a new client ID was created. This will be used to access the data and APIs. Remember that "*Client ID*".



Credentials

Credentials | OAuth consent screen | Domain verification

New credentials ▾ | Delete

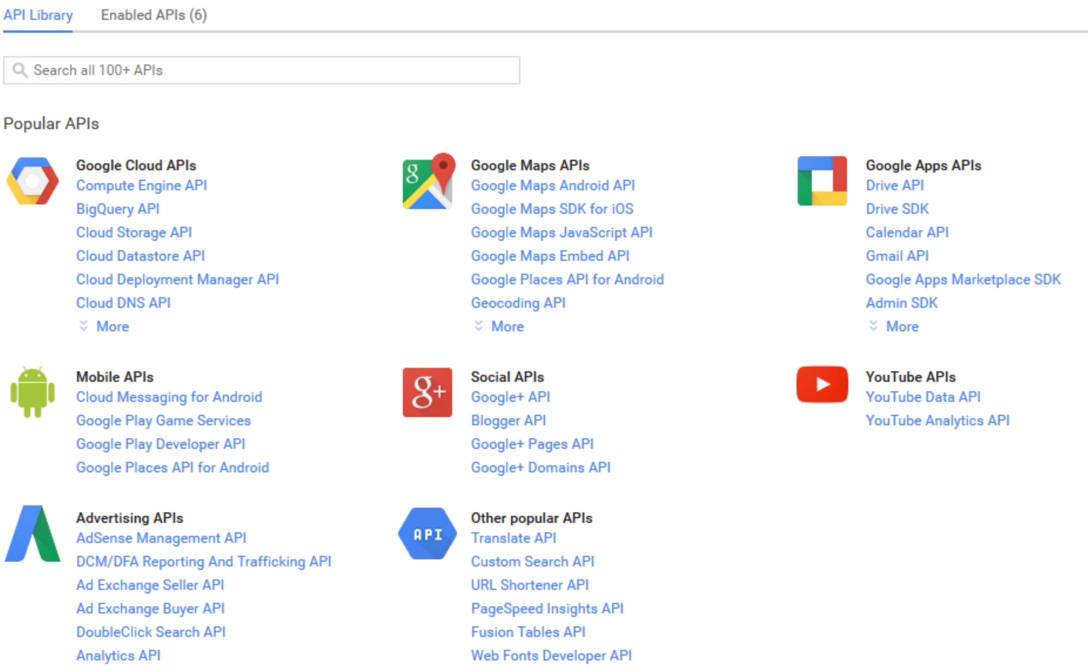
Create credentials to access your enabled APIs. Refer to the API documentation for details.

OAuth 2.0 client IDs

□	Name	Creation date ⌄	Type	Client ID
□	Client du compte de service apitws	Jan 11, 2016	Service account client	104373606319905538924

8.9.2. Activate your APIs

Open the "*Overview*" menu, "*API Library*" tab and in the "*Google Apps APIs*" section you will find the 2 APIs to enable.



API Library | Enabled APIs (6)

Search all 100+ APIs

Popular APIs

Google Cloud APIs
- Compute Engine API
- BigQuery API
- Cloud Storage API
- Cloud Datastore API
- Cloud Deployment Manager API
- Cloud DNS API
- More

Google Maps APIs
- Google Maps Android API
- Google Maps SDK for iOS
- Google Maps JavaScript API
- Google Maps Embed API
- Google Places API for Android
- Geocoding API
- More

Google Apps APIs
- Drive API
- Drive SDK
- Calendar API
- Gmail API
- Google Apps Marketplace SDK
- Admin SDK
- More

Mobile APIs
- Cloud Messaging for Android
- Google Play Game Services
- Google Play Developer API
- Google Places API for Android

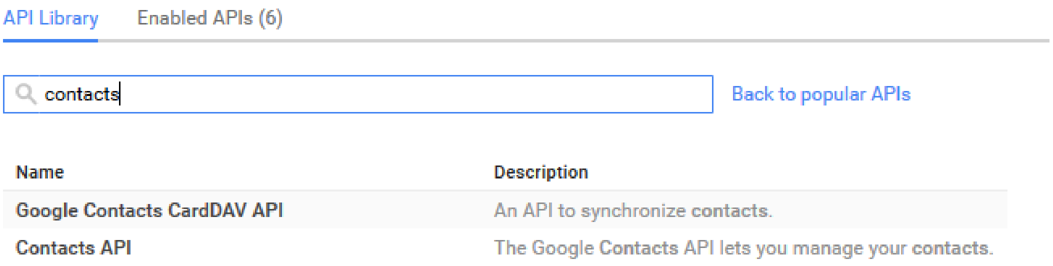
Social APIs
- Google+ API
- Blogger API
- Google+ Pages API
- Google+ Domains API

YouTube APIs
- YouTube Data API
- YouTube Analytics API

Advertising APIs
- AdSense Management API
- DCM/DFA Reporting And Trafficking API
- Ad Exchange Seller API
- Ad Exchange Buyer API
- DoubleClick Search API
- Analytics API

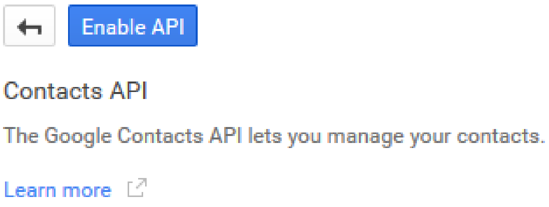
Other popular APIs
- Translate API
- Custom Search API
- URL Shortener API
- PageSpeed Insights API
- Fusion Tables API
- Web Fonts Developer API

In the search box, you can search for “*Contacts*”.



Name	Description
Google Contacts CardDAV API	An API to synchronize contacts.
Contacts API	The Google Contacts API lets you manage your contacts.

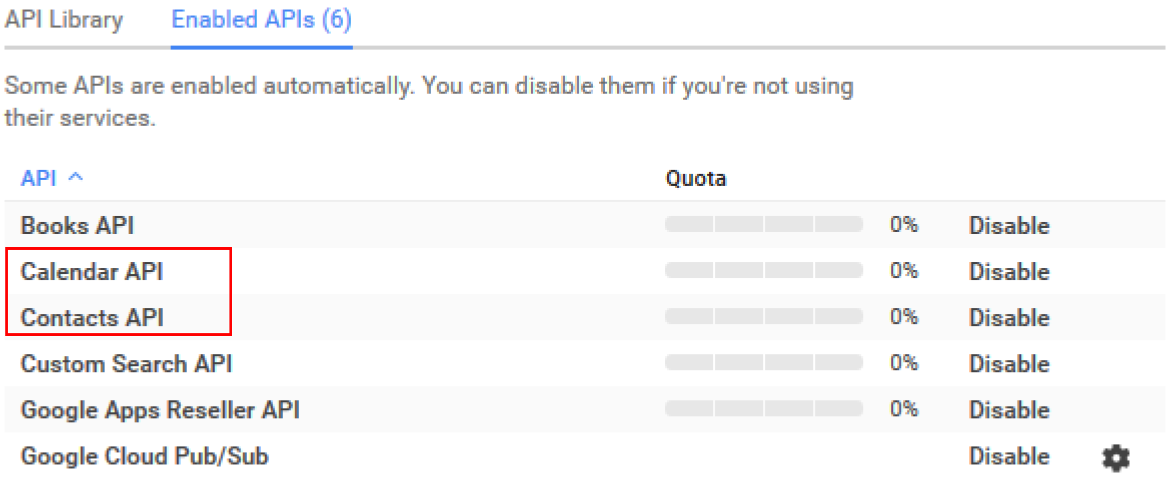
Select "*Contacts API*" and Enable API.



Contacts API

The Google Contacts API lets you manage your contacts.

Do the same again for the « *Calendars* » API.
When finished, select the “*Enabled APIs*” menu to check that your APIs are active.

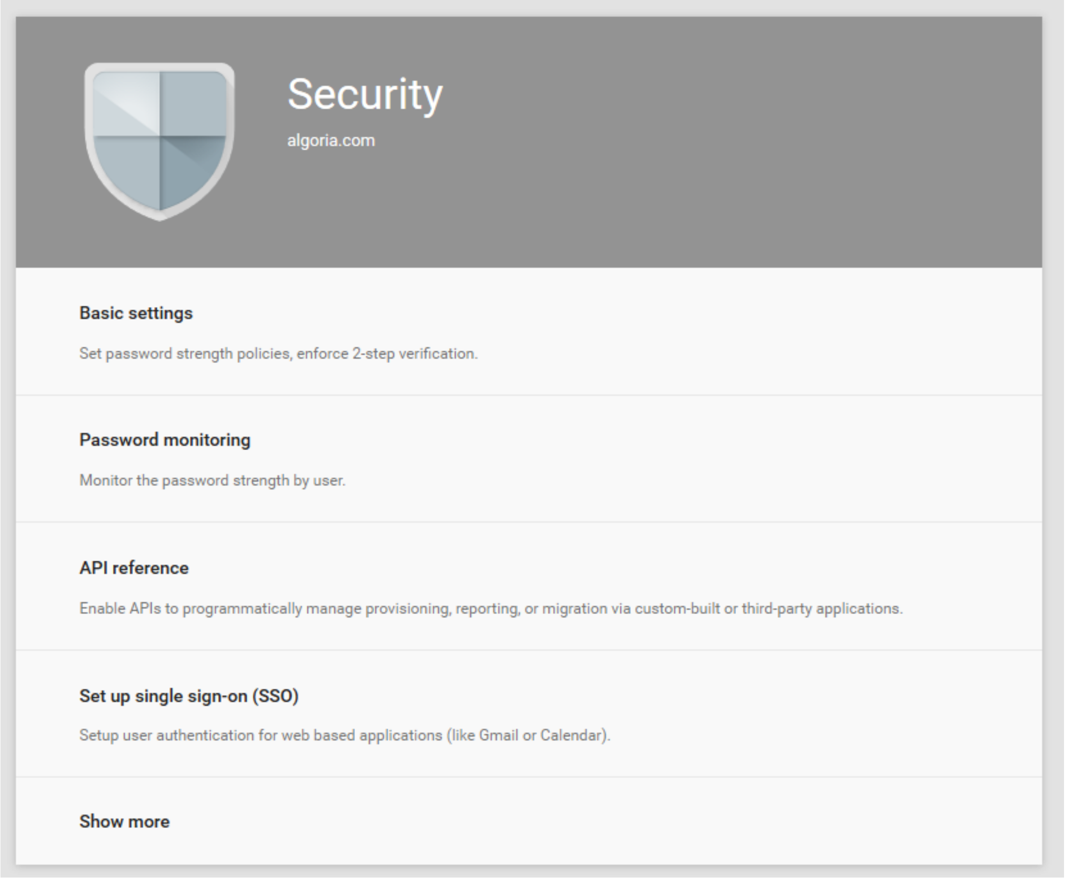


Some APIs are enabled automatically. You can disable them if you're not using their services.

API ^	Quota		
Books API	0%	Disable	
Calendar API	0%	Disable	
Contacts API	0%	Disable	
Custom Search API	0%	Disable	
Google Apps Reseller API	0%	Disable	
Google Cloud Pub/Sub		Disable	⚙

8.9.3. Authorize APIs

Go to: https://www.google.fr/intx/fr/work/apps/business/ . Connect you to your domain Google Apps and select Administration console.
Open the “*Security*” menu and click on “*Show more*”.



Security

algoria.com

Basic settings

Set password strength policies, enforce 2-step verification.

Password monitoring

Monitor the password strength by user.

API reference

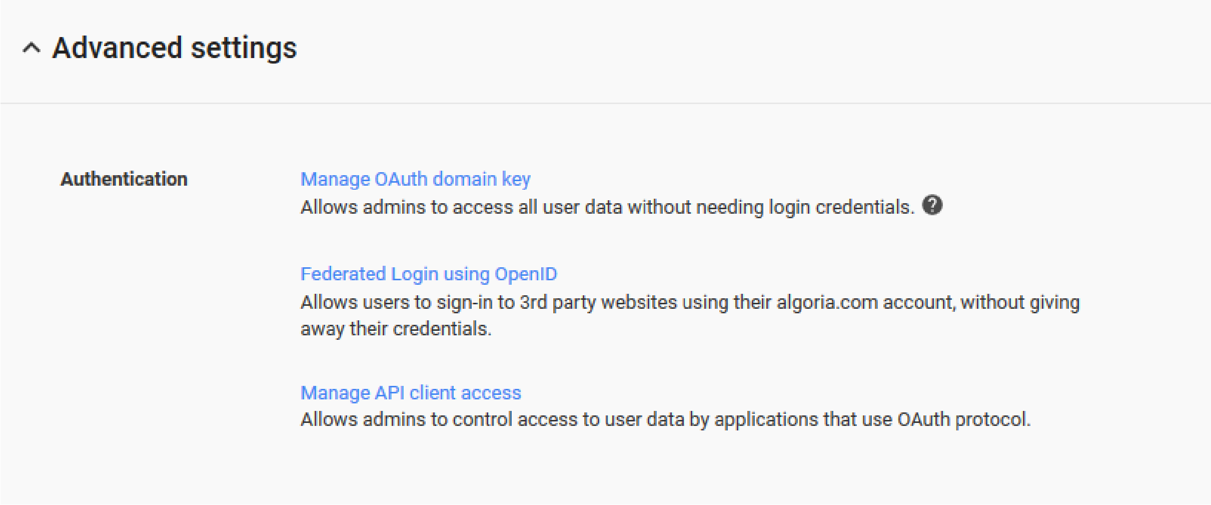
Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.

Set up single sign-on (SSO)

Setup user authentication for web based applications (like Gmail or Calendar).

Show more

Open “*Advanced settings*” and click “*Manage API client access*”.



Advanced settings

Authentication

Manage OAuth domain key

Allows admins to access all user data without needing login credentials.

Federated Login using OpenID

Allows users to sign-in to 3rd party websites using their algoria.com account, without giving away their credentials.

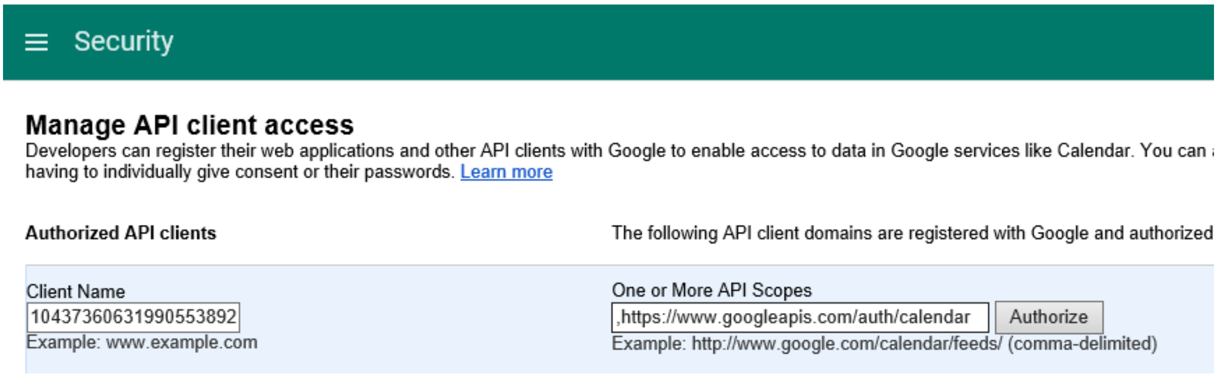
Manage API client access

Allows admins to control access to user data by applications that use OAuth protocol.

Now you must save the Web applications to access data services.

Find your "*CLIENT ID*" created previously and fill "*Customer Name*" (see chap. *Creating a customer ID associated with the service account key*). Then in the "*One or more API scopes*" complete the following URL separated by commas, as shown below:

https://www.google.com/calendar/feeds/,https://www.google.com/m8/feeds/,https://www.googleapis.com/auth/calendar



Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can
having to individually give consent or their passwords. Learn more

Authorized API clients

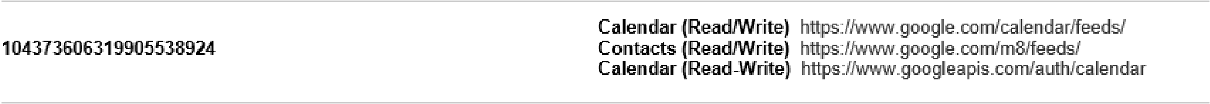
The following API client domains are registered with Google and authorized

Client Name
10437360631990553892
Example: www.example.com

One or More API Scopes
,https://www.googleapis.com/auth/calendar

Example: http://www.google.com/calendar/feeds/ (comma-delimited)

Then click on “*Authorize*”.



104373606319905538924	**Calendar (Read/Write)**	https://www.google.com/calendar/feeds/
	Contacts (Read/Write)	https://www.google.com/m8/feeds/
	Calendar (Read-Write)	https://www.googleapis.com/auth/calendar

Your Google Apps account is configured correctly.

8.9.4. Configuring connectors in TWP

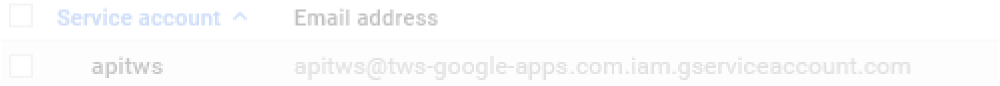
Prerequisites

TWP can communicate with Google Apps with:

- The email address previously configured in the Google service account
- The *P12* file
- The domain name you use in Google Apps

Configuration

Rename *P12* file this way: « *api-google-[Username].p12* »
The [Username] matches the name of the user present in the e-mail address of the Google Apps developer account.



□	Service account ^	Email address
□	apitws	apitws@tws-google-apps.com.iam.gserviceaccount.com

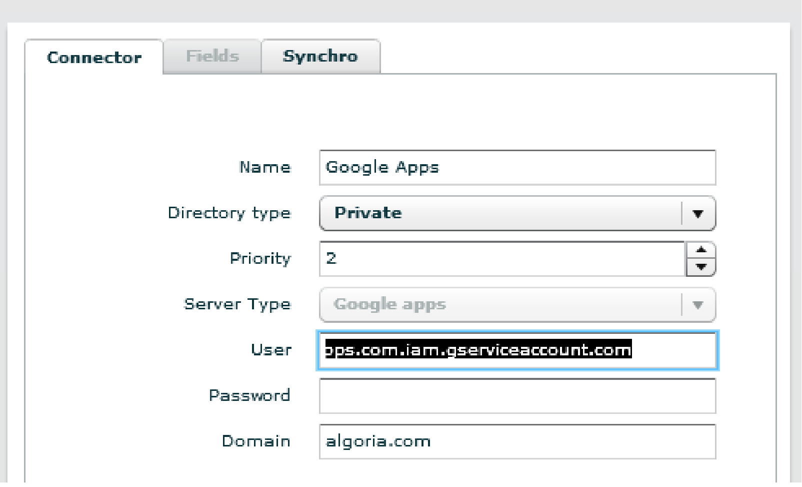
Ex:
Email: apitws@tws-google-apps.com.iam.gserviceaccount.com
Name of the user: apitws
File name: ***api-google-apitws.p12***

Then copy the file in the directory [InstallTWP]\TWS4\TWS_Web\TWS_Config.

TWP can synchronize the directory and Google Apps calendars. To do that, the email address of the TWP user should match the email address of the Google Apps user.

8.9.5. Creating a private directory

In the TWP administration, create a new directory with *Google Apps* as the server type and *private* as the directory type and name it as you want.

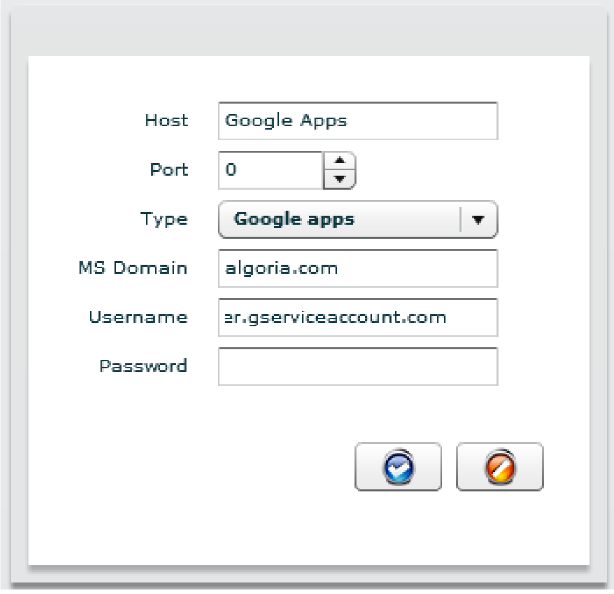


Name: Google Apps
Directory type: Private
Priority: 2
Server Type: Google apps
User: pps.com.iam.gserviceaccount.com
Password:
Domain: algoria.com

In the *User* field, enter the full email address.
In the *Domain* field, enter the name of your domain.
The password field is not used.
Save and you can start synchronizing.

8.9.6. Creating a calendar connector

In the TWP administration, create a new collaboration connector of Google Apps.



Host: Google Apps
Port: 0
Type: Google apps
MS Domain: algoria.com
Username: er.gserviceaccount.com
Password:

Choose the type Google Apps.

In the *User* field, enter the full email address.
In the *domain* field, enter the name of your domain.

The password field is not used.
The Host field is not used. You can use this field to name the connector.

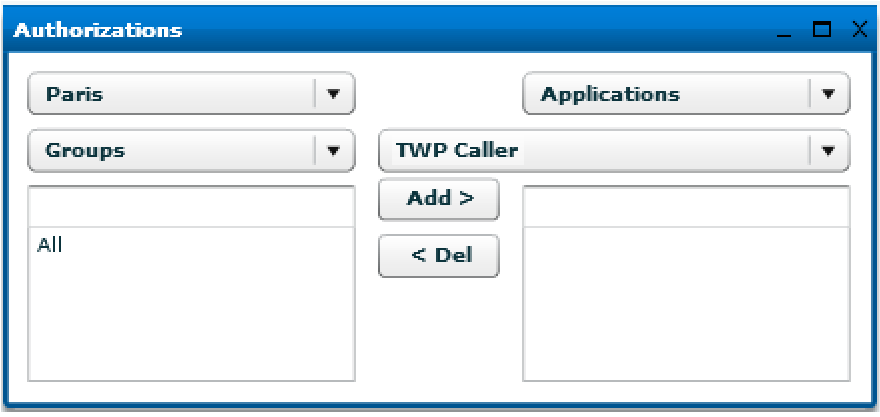
9. Configuration of applications

9.1 Configuration of Caller application

The Caller application is the basic building block of TWP applications. It contains many features that add value to the routine use of the telephony business. Among these features, some requires a minimum of configuration:

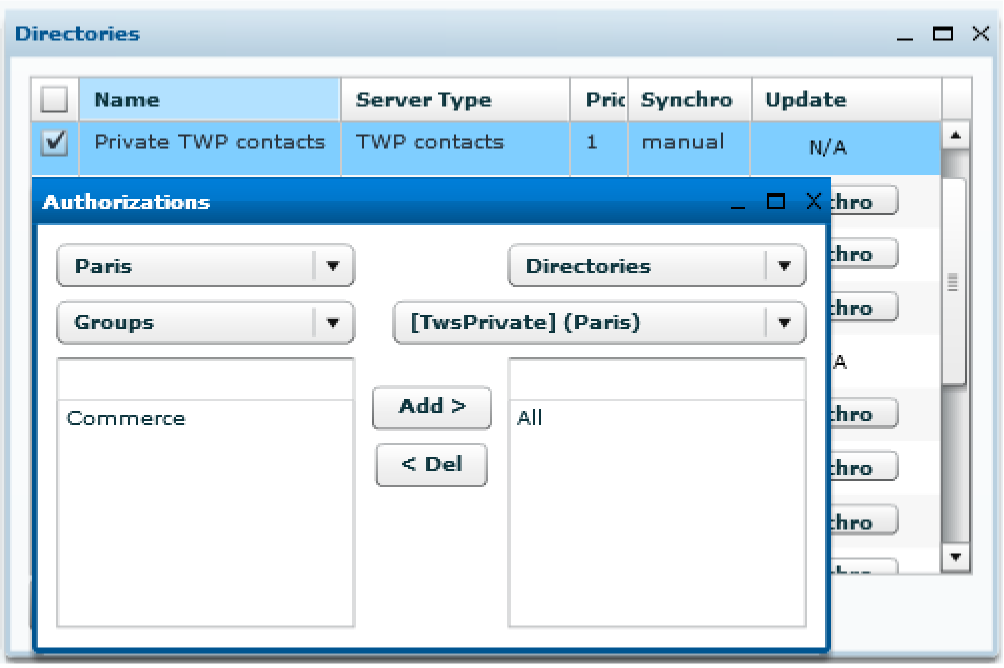
- multi-directories search,
- contacts list,
- Telephony presence of contacts,
- Calendar events of contacts,
- TWP presence of contacts,
- text chat, video and application sharing point to point (with one contact)
- sharing information : notes, notifications, call logs
- rules for call forwarding
- new voice messages (PBX A5000)
- e-mail alert while a missed call

Every user has these features with the Caller application and it consumes a license.
To give rights to the Caller application, go to the administration, *Users / Authorizations* menu, choose at top right list Applications then TWP Caller below. Select the user group or the user at the left and click on the "Add>" button.



9.1.1. Private contacts

With the Caller application, users can create their own private contacts. These are visible only in their Caller.
For this, just verify that the user in question does have rights to the directory *[TwsPrivate]*. Access to *Users / Authorizations* menu and *IT Management / Directories* is necessary.



Directories

☐	Name	Server Type	Pric	Synchro	Update
☑	Private TWP contacts	TWP contacts	1	manual	N/A

Authorizations

Paris ▾

Groups ▾

Directories ▾

[TwsPrivate] (Paris) ▾

Commerce

All

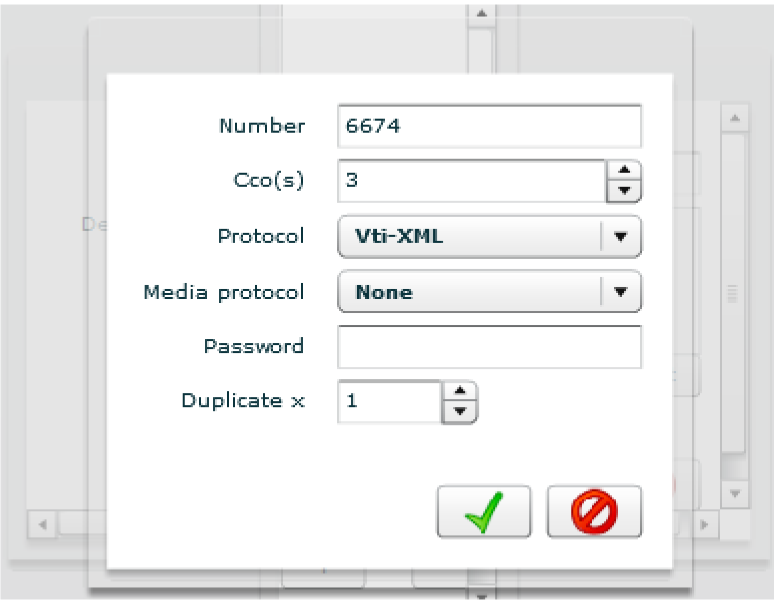
9.1.2. Telephony presence - Intercom

To have the telephony presence of contacts (with internal phone numbers) - equivalent to supervision key on a physical phone - it is absolutely necessary to configure Intercom groups specific to TWP.

1. **Create a TWP Intercom group:**

   There are several ways to create an Intercom group:

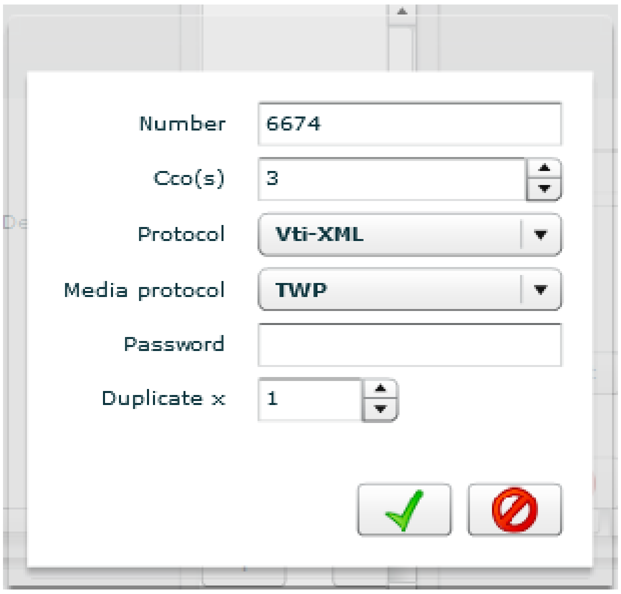
- *From existing physical extension:* you already have one or more devices that contain the supervision keys of other devices which status must be visible, then these numbers can be listed to create an intercom group. Access



Number 6674
Cco(s) 3
Protocol Vti-XML
Media protocol None
Password
Duplicate x 1

Number: First number of devices list.
Protocol: choose the protocol of the device supervision.
Media protocol: in the case of an existing physical extension, select *None*.
Password: password of the device, useful for the supervision.
Duplicate x: Number of the device in the list. If the number is 6674 and you specified 2 then 6674 and 6675 will be created.

- *From virtual device*: create in your PBX a virtual device linked to no physical extension (for example VTIXML/IP device for A5000 PBX). On this device, create the supervision keys of other devices which status must be visible. Then fill in the number of this virtual device in the configuration of the Intercom group.



Number 6674

Cco(s) 3

Protocol Vti-XML

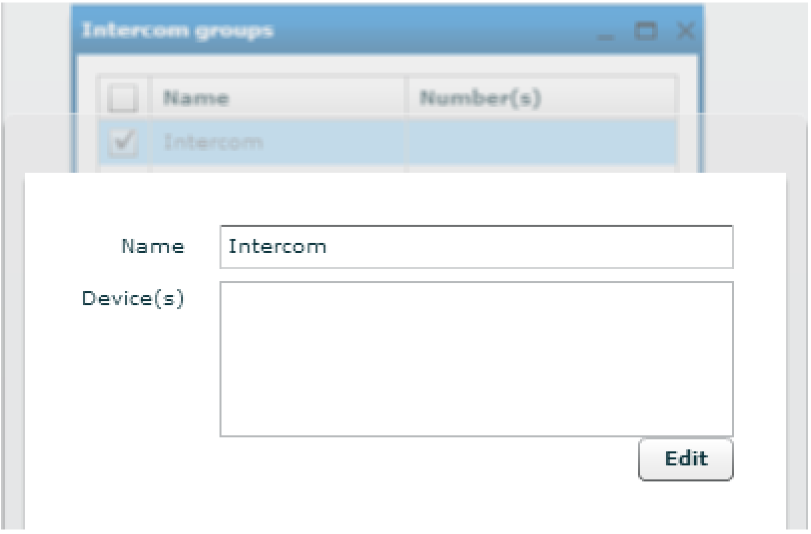
Media protocol TWP

Password

Duplicate x 1

Number: First number of devices list.
Protocol: choose the protocol of the device supervision.
Media protocol: in the case of a virtual device, select TWP.
Password: password of the device, useful for the supervision.
Duplicate x: Number of the device in the list. If the number is 6674 and you specified 2 then 6674 and 6675 will be created.

- *From nothing*: you can create an Intercom group without number. In this case, the user extensions must have the supervision keys of other device which status must be visible.



Name Intercom

Device(s)

2. **Giving permissions to users for Intercom group created:** Only users who will have the same Intercom group can see each other or see the status of devices supervised by configured Intercom group devices (see chapter 7.4.4)

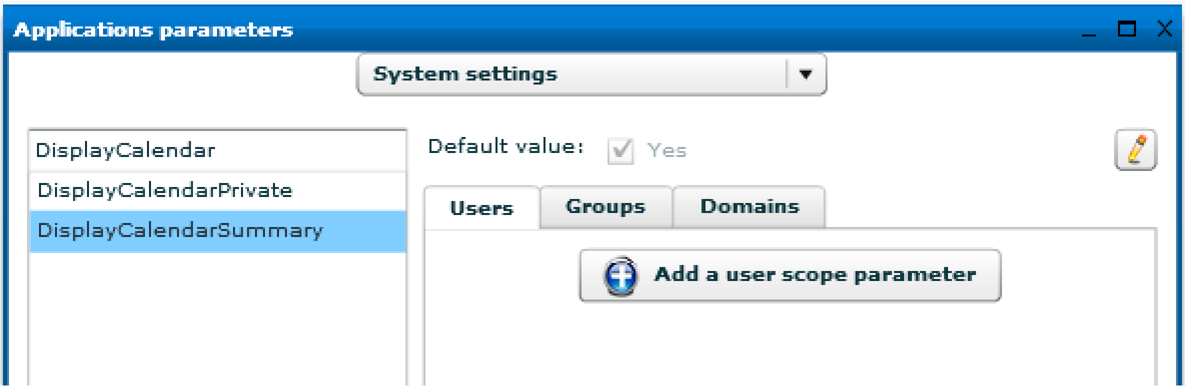
Attention: On AASTRA PBX, check that the devices that are supposed to be supervised are this time in the same PBX intercom group.

9.1.3. Calendar presence - collaboration

See chapter 8.5.3, 8.6.2, 8.7.4 depending on the type of mail server you have.

After configuring the connectors to mail servers and the necessary authorizations, all authorized users have the ability to view the calendar events: the status and details by hovering the contact picture.

It is possible, however, to limit the feature for a user, group or domain. Go to *Applications / Applications parameters* then *System settings* and search "*DisplayCalendar*". There is 2 settings:

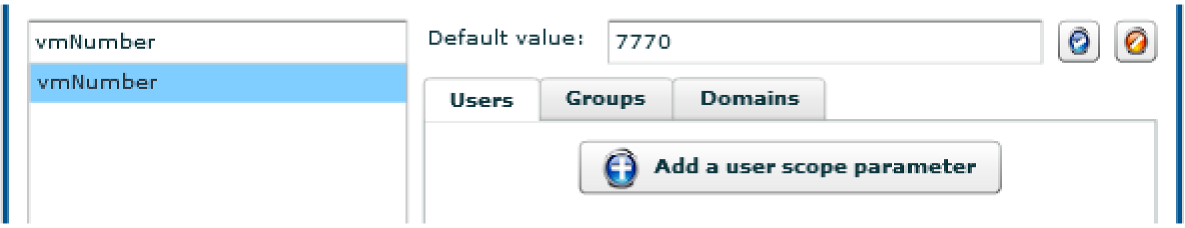


- *DisplayCalendarSummary*: Yes or No the calendar event details of a contact is visible for users (Busy state, on the contact card – other state will be visible by hovering the contact image)
- *DisplayCalendarPrivate*: Yes or No the PRIVATE calendar event information (state and details) is visible for other users. A normal calendar event is visible for the same users.

9.1.4. Voicemail number

With the Caller application, a user can directly call to voice mail by clicking on the button provided for this purpose in the sidebar button.

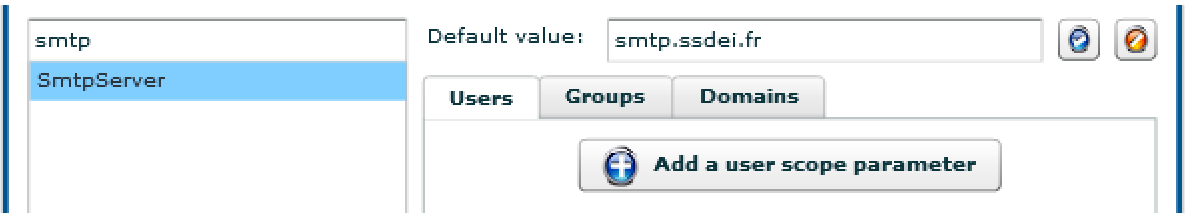
To change this value, go to the *Applications / Applications parameters* menu, choose TWP *Caller* then search "*vmNumber*". Fill in the voicemail number as the default value. It is also possible to give a different number for a user, a group or a domain.



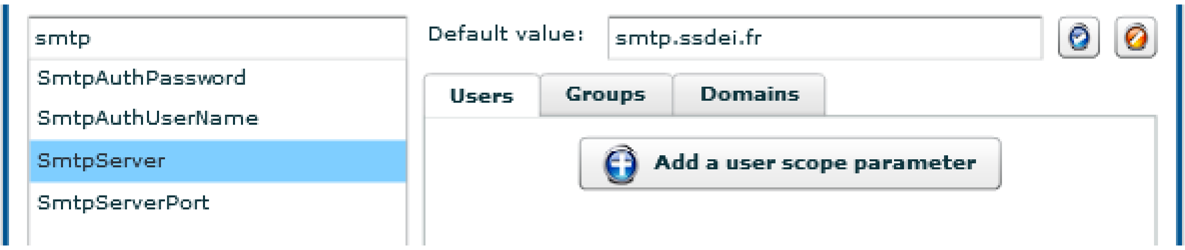
9.1.5. E-mail alerts – SMTP configuration

With the Caller application, a user may receive an email alert informing him of a missed call. For this feature, you must configure the SMTP setting.

In the *Applications* / *Applications parameters* menu, choose TWP *Server* then search “smtp”. Fill in the SMTP server address as the default value. It is also possible to give a different address for a user, a group or a domain.


smtp
SmtpServer
Default value: smtp.ssdei.fr

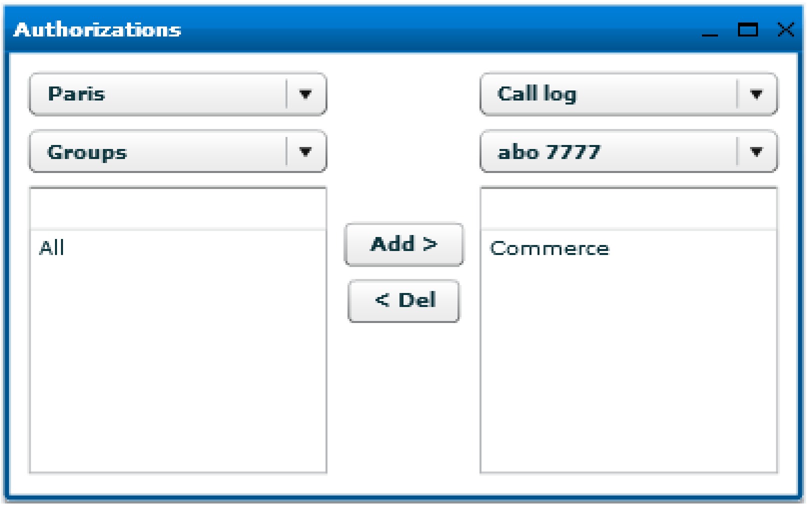
Advanced (Expert mode)
If you need to enter the port and an account for the SMTP connection then check the *(Mode Expert)* case you will modify the value of the parameters “*SmtpAuthUserName*” for the user name, “*SmtpAuthPassword*” for the password and “*SmtpServerPort*” for the connection port.


smtp
SmtpAuthPassword
SmtpAuthUserName
SmtpServer
SmtpServerPort
Default value: smtp.ssdei.fr

9.1.6. Call logs of other users

With the Caller application, a user can access to call logs of a contact via the event log. To be able to visualize these call logs authorization must be given (see chapter 7.4.6).

All users in group Commerce of the domain Paris have the rights the call logs of the user « abo *7777* ».



Data of call logs of users are kept only for a limited number of days (see chapter 10.2.1.).

9.1.7. Boss Secretary feature

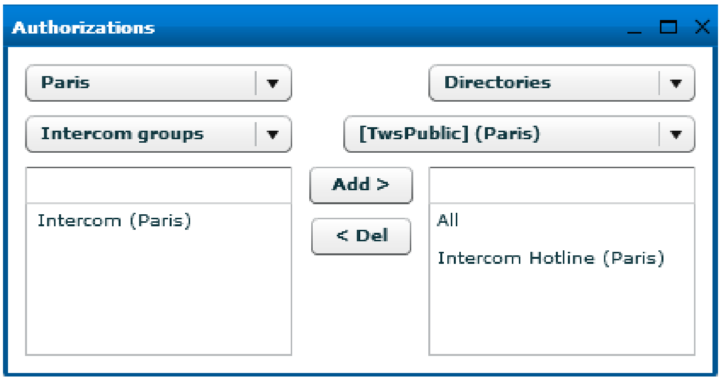
With the Caller application, specific information of one or more users (the bosses) can be seen by other users (secretaries):

- The details (the first and last name if present in directories or the phone number) of the call that is on one of the bosses devices to intercept the call if needed.
- The active forward rule that one of the bosses implemented

Allow a user to view the details of a call of another user (from their contact card):

NB: For A5000 PBX whose devices are supervised in VTIXML, call informations are displayed only when the phone rings. For other supervised in CSTA, the information is displayed when the call has been picked up.

1. Configure an intercom group (see chapter 9.1.2.) and allow users (bosses and secretaries) to the same group.
2. Give the intercom group permissions to contact directories. It is thanks to these authorizations as the contact's name will appear if the number is found in directories in question.

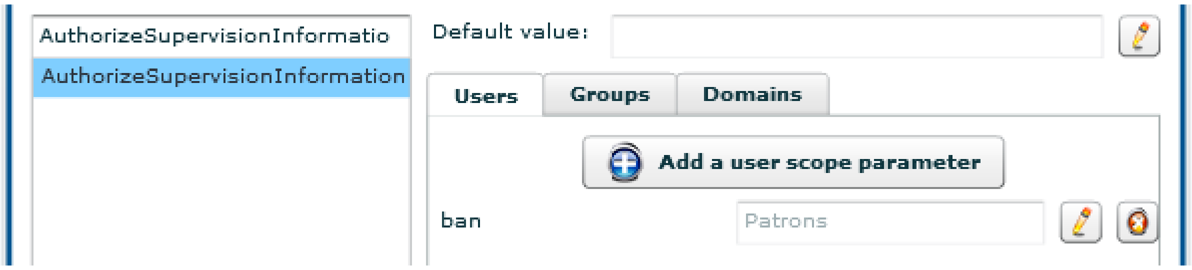


Intercom (Paris)

All

Intercom Hotline (Paris)

3. Create a new group in the *Users / Groups* menu.
4. Add users (bosses) whose incoming call information will be visible by going to the *Users / Groups-Users* menu.
5. In the *Applications / Applications parameters* menu, select TWP *Caller* and configure the setting "*AuthorizeSupervisionInformation*" like below:



AuthorizeSupervisionInformatio

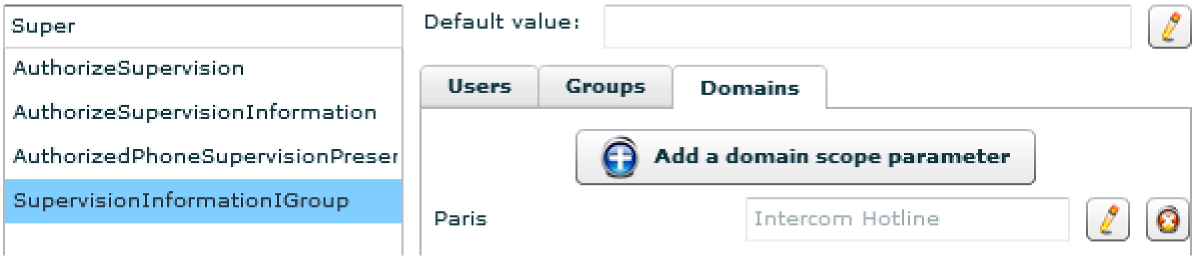
AuthorizeSupervisionInformation

ban Patrons

On the *Users* or *Groups* tab, select the user or group of users who will see the information after clicking the *Add* button ... Then fill the value with the name of the user group you created earlier and then validate.

Here for example, the user "ban" will see the incoming call information of the users' group "Patrons".

6. If one or more users of the group "Patrons" belong to several Intercom groups, it is best to set the Intercom group to be selected for the resolution of the name issue.
   In the *Applications / Applications parameters* menu, select TWP *Caller*, do not forget to check the "Expert mode" (chap. 10.2) and configure the setting "*SupervisionInformationIGroup*" like below, only on the domain or as the default value:



Super

AuthorizeSupervision

AuthorizeSupervisionInformation

AuthorizedPhoneSupervisionPreser

SupervisionInformationIGroup

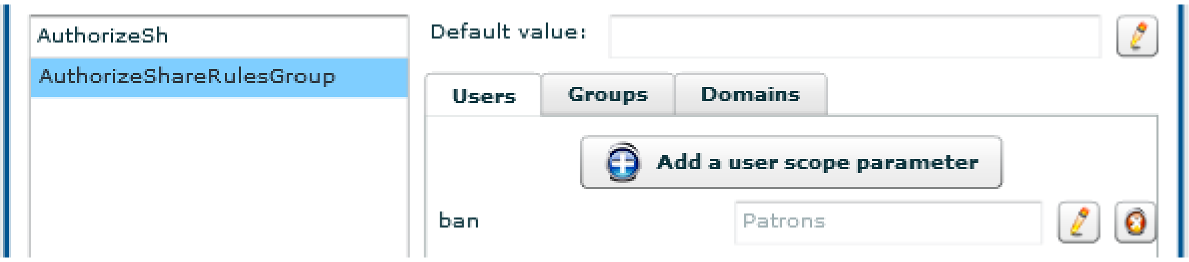
Paris Intercom Hotline

Here, only the permissions of directories of the Intercom group with "Intercom Hotline" as name will be considered for the resolution of the name issue in the display of call informations for users in domain "Paris".

Attention: Restart the TWS4$TWS_EventServices service after any modifications of these settings.

Allow a user to see the first active forward rule of another user (by hovering the contact photo):

1. Create a new group in the *Users / Groups* menu
2. Add users (bosses) whose first active forward rule will be visible by going to the *Users / Groups-Users* menu
3. In the *Applications / Applications parameters* menu, select TWP *Caller* and configure the setting "*AuthorizeShareRulesGroup"* like below:



AuthorizeSh

AuthorizeShareRulesGroup

Default value:

ban: Patrons

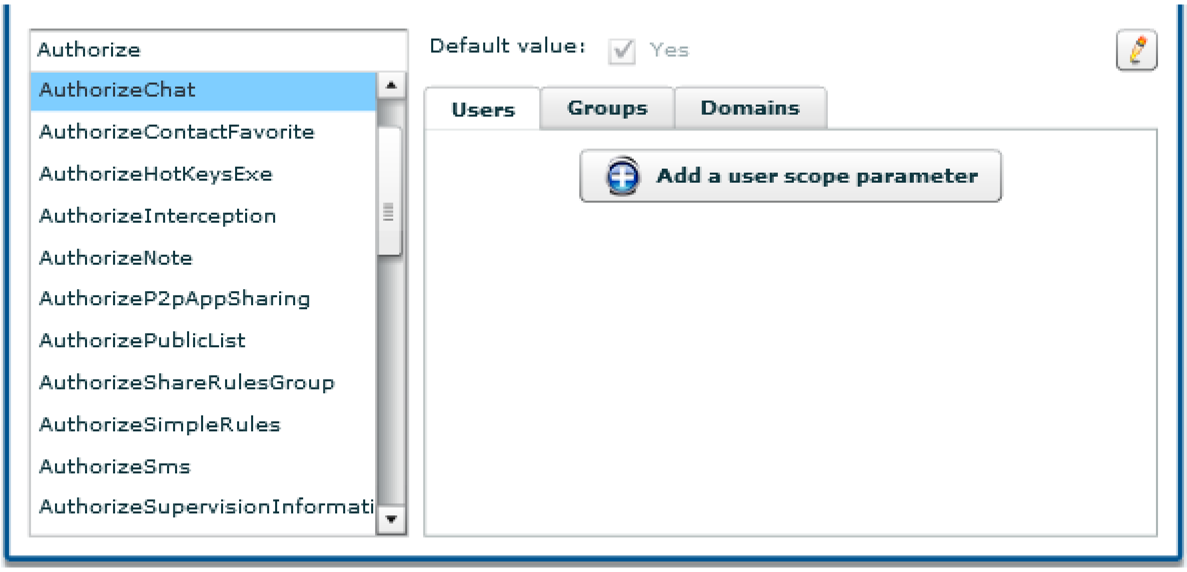
On the *Users* or *Groups* tab, select the user or group of users who will see the information after clicking the *Add* button ... Then fill the value with the name of the user group you created earlier and then validate.

Here for example, the user "ban" will see the first active forward rule of the users' group "Patrons".

9.1.8. All features to enable or disable

With the Caller application, it is possible to make visible or invisible features for a limited number of users or even all users.

In the *Applications / Applications parameters* menu, select TWP *Caller* and search "Authorize" and all the settings that enable or disable Caller features appear.



Authorize

AuthorizeChat
AuthorizeContactFavorite
AuthorizeHotKeysExe
AuthorizeInterception
AuthorizeNote
AuthorizeP2pAppSharing
AuthorizePublicList
AuthorizeShareRulesGroup
AuthorizeSimpleRules
AuthorizeSms
AuthorizeSupervisionInformati

Default value: ☑ Yes

- *AuthorizeChat*: Yes or No the user, the users of a group or the users of a domain have the rights to chat (text) together. The button to display the chat window will appear or not in the contact card.

- *AuthorizeContactFavorite*: Yes or No the user, the users of a group or the users of a domain have the rights to create their private contacts. The button to create new contact will appear or not in the contacts manager.

- *AuthorizeHotKeys*: Yes or No the user, the users of a group or the users of a domain have the rights to use the keyboard shortcuts "Ctrl+F1 / +F2 / … / +F11" to make a call of the contact number chosen in the Caller application contact list.

- *AuthorizeHotKeysExe*: Yes or No the user have the rights to use the keyboard shortcut "*Ctrl+F12*" to make a call of a highlighted number. The user can modify this setting from the preferences of the Caller.

  Note: This setting does not prevent users from applying other keyboard shortcuts ("Ctrl+F1", "Ctrl+F2", …) to contacts via the contact card.

- *AuthorizeInterception*: Yes or No the user, the users of a group or the users of a domain have the rights to intercept calls arriving at the contacts devices.

- *AuhtorizeNote*: Yes or No the user, the users of a group or the users of a domain have the rights to post a public note. The text fields in the event log window to post a note will appear or not.

- *AuthorizeP2pAppSharing*: Yes or No the user, the users of a group or the users of a domain have the rights to initiate an application sharing from their PC. The button to do it in the chat window will appear or not.

- *AuthorizePublicList*: Yes or No the user, the users of a group or the users of a domain have the rights to change a list from private to public to be accessible by other users. The button to make a list public will appear or not in the list manager windows in the contacts manager.

- *AuthorizeShareRulesGroup*: see chapter 9.1.7

- *AuthorizeSimpleRules*: Yes or No the user, the users of a group or the users of a domain have the rights to create, modify or delete the forwarding rules (simple or advanced). All button to manage forwarding rules will appear or not.

- *AuthorizeSms*: Yes or No the user, the users of a group or the users of a domain have the rights to send SMS to a mobile number of a contact. The button to send a SMS will appear or not in the contact card.

- *AuthorizeSupervisionInformation*: see chapter 9.1.7

- *AuhtorizedCurrentDevice*: Yes or No the user, the users of a group or the users of a domain have the rights to send SMS to create a new current device. The button to create it will appear or not in the profile tab.

Settings to be modified from the version 4.1.SP2b in Expert Mode

- *AuthorizedAdvancedSearch*: Yes or No the user, the users of a group or the users of a domain have the rights to do an advanced search from the Caller application. The advanced search can be activated from the Caller application by clicking the magnifying glass icon in the search box.

- *AuthorizedCalendarPresences*: Yes or No the user, the users of a group or the users of a domain have the rights to view calendar events of contact in the contact lists.

- *AuthorizedCreateProfil*: Yes or No the user, the users of a group or the users of a domain have the rights to create a new profile from the corresponding menu in Caller application preferences.

- *AuthorizedCustomMessagePresences*: Yes or No the user, the users of a group or the users of a domain have the rights to create and use messages for custom presence.

- *AuthorizedEmailNotification*: Yes or No the user, the users of a group or the users of a domain have the rights to configure email notifications when there is missed calls or voicemails left.

- *AuthorizedExternalChat*: Yes or No the user, the users of a group or the users of a domain have the rights to chat with external parties if an external collaboration account is configured.

- *AuthorizedMultiChat*: Yes or No the user, the users of a group or the users of a domain have the rights to chat during a conference session.

- *AuthorizedSaveChat*: Yes or No the user, the users of a group or the users of a domain have the rights to configure instant messages backup mechanism. If it is No, the messages will never be saved.

- *AuthorizedPhoneSupervisionPresences*: Yes or No the user, the users of a group or the users of a domain have the rights to view phone supervision events of contacts in the Caller application contact lists.

- *DisplaySimpleRules*: Yes or No the user, the users of a group or the users of a domain have the rights to view, in the preferences menu Profiles, the forward rules created or enabled from the telephone.

- *AuthorizedForwardOriginAll, AuthorizedForwardOriginExternal, AuthorizedForwardOriginInternal, AuthorizedForwardPresenceAsbsent, AuthorizedForwardPresenceBusy, AuthorizedForwardPresenceCalendar, AuthorizedForwardPresenceOffline, AuthorizedForwardPresenceOnline, AuthorizedForwardTypeBusy, AuthorizedForwardTypeImmediate, AuthorizedForwardTypeNoAnswer* :

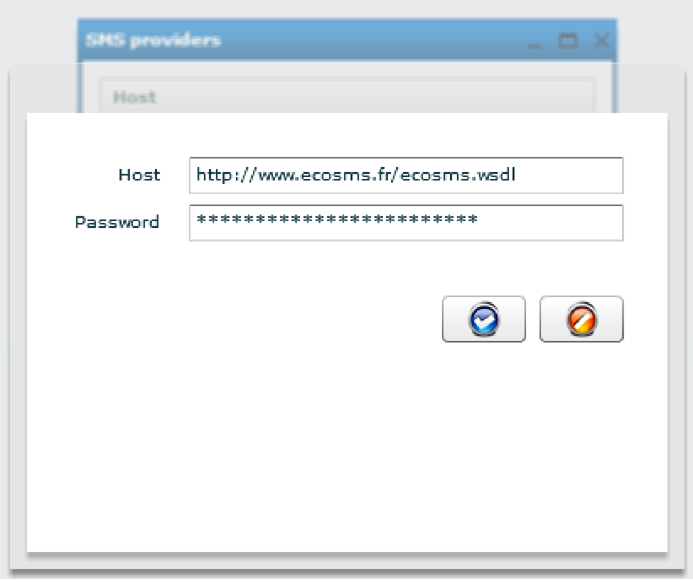
  Yes or No the user, the users of a group or the users of a domain have the rights to create forward rules with specific parameters: the origin of the call, the type of presence or type of forward to achieve.

9.1.9. SMS feature

With the Caller application, it is possible to send sms to the mobile phone of your contact.
TWP works with a unique SMS provider called J2S Telecom.

How to contact J2S Telecom
J2S TELECOM - Espace Performance - bâtiment C1/C2 – 35760 Saint Grégoire
+33 (0) 2.99.23.60.81 - contact@j2stelecom.com

How to configure a SMS provider
In the *Telephony / SMS Providers* menu, click the add button and complete the fields as follows:



Host: http://www.ecosms.fr/ecosms.wsdl
Password: ************************

- *Host*: fill with the web service URL of J2S. In general it is : http://www.ecosms.fr/ecosms.wsdl
- *Password*: it is the key identifier given by J2S.

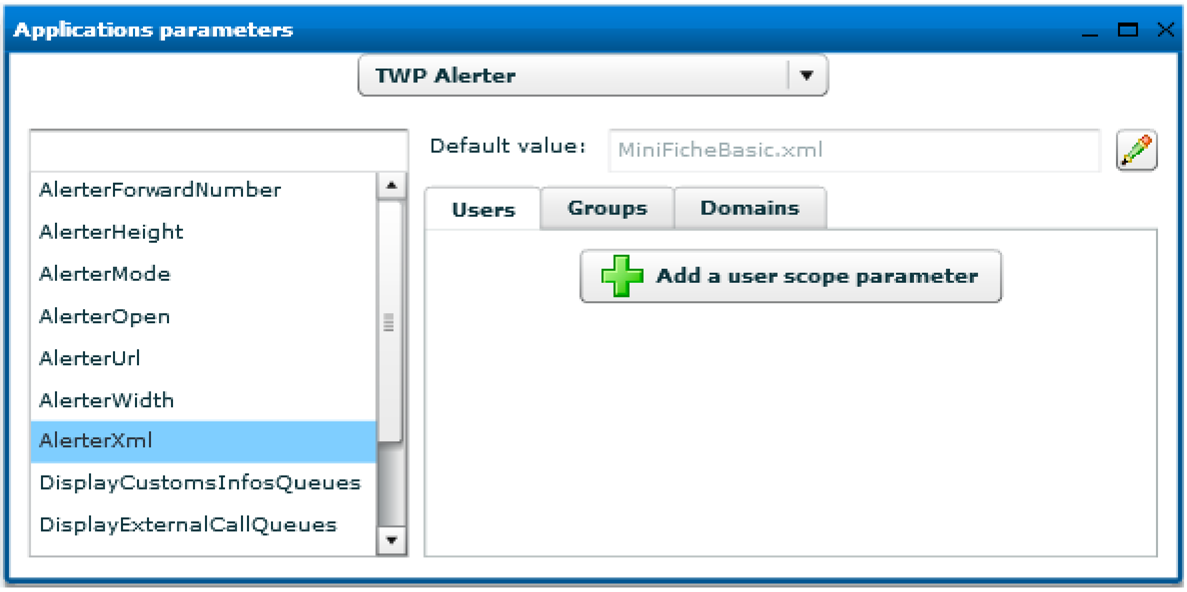
9.2. Alerter configuration

The Alert application is a tool to provide an advanced and customizable window card of a contact on calls. It also includes the feature of shared call queues.
To have these features the user must have the rights to the Alert application, which consume a license Alerter.

9.2.1. Customization and settings

Select the *Applications* / *Applications parameters* menu.

Select TWP *Alerter* application.



Each parameter has a default value defined during installation. It can be changed. It is possible to set the value of a parameter by user, group or domain. In this case, this value will override the default.

Setting '*AlerterWidth*': This parameter defines the width of the Alerter window in pixels.
Setting '*AlerterHeight*': This parameter defines the height of the Alerter window in pixels.
Setting '*AlerterMode*': This parameter configures the Alerter mode to display to users. Two possible values:

- « XML »
  - Displays the phone action buttons (Reply, divert)
  - Displays the caller information (customizable)

- « URL »
  - Displays the phone action buttons (Reply, divert)
  - Displays an HTML page selected by the administrator.

Setting '*AlerterXml*': This parameter is used when '*AlerterMode*' parameter value is "*XML*". It contains the name of the XML file used to customize the display of contact information.

This file is located in "\TWS4\TWS_Web\TWS_Config\TWS_Alerter\".

The root tag of the XML file is:

<alerter></alerter>

This tag « alerter » can accept one attribute:

- `vip="true"` or `vip="false"`: VIP mode is activated if value is true. If the contact is recognized as a "VIP", the background color of Alerter will be the selected color in Caller preferences.

The root tag contain three types of tags:

<**text**>Text to display</**text**>: To display text.

<**image**>http://urldelimage.com/image.jpg</**image**>: To display an image.

<**button**>Text of the button</**button**>: To allow a user action.

Each of these tags accepts the following attributes:

x="10" y="5": For the placement in pixels of the element in the Alerter window (the origin is the upper left corner)

directory="exchange": To limit the display element with the specific directory in which the caller is present or not. It is possible to specify multiple directories separated by commas. If "none" is specified, the item will only be displayed if the caller is not present in any directory.

The <button> tag accepts the following attributes:

exe="c:\Windows\notepad.exe [-PhoneNumber-]": Launch an executable when clicked by the user. Here opens a notepad with the phone number of the caller as file name.

url="http://www.google.fr/search?q=[-DisplayName-]": Opens a URL in the default browser when user click. Here opens a Google search with the full name of the caller.

In the XML file, each field is delimited by “[-” and “-]” and is replaced by the information of the caller or the callee.

The available fields are:

- [-Lastname-] : replaced by the last name of the caller
- [-Firstname-] : replaced by the first name of the caller
- [-DisplayName-] : replaced by the full name of the caller
- [-CompanyName-]: replaced by the company name of the caller
- [-Picture-] : replaced by the photo url of the caller
- [-AssistantPhone-] : replaced by the assistant phone number of the caller
- [-StandardPhone-] : replaced by the standard phone number of the caller
- [-WorkPhone-] : replaced by the office phone number of the caller
- [-MobilePhone-] : replaced by the mobile number of the caller
- [-HomePhone-] : replaced by the home phone number of the caller
- [-Email1-] : replaced by the email 1 of the caller
- [-Email2-] : replaced by the email 2 of the caller
- [-Url-] : replaced by the web site of the caller
- [-PhoneNumber-] : replaced by the current phone number of the caller
- [-ServerName-] : replaced by the TWP server name
- [-PersonGuid-] : replaced by the internal identifier of the caller

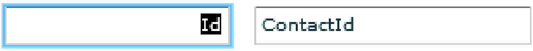
- [-Contact2DisplayName-] : replaced by the full name of the one who divert the call
- [-Contact2PhoneNumber-] : replaced by the phone number of the one who divert the call

For additional private fields, the default contact information will replace the following:

- [-Custom0-] to [-Custom9-]: replaced by the 0 to 9 private fields of the caller configured at the directory

The use of the field's names [-Custom0-] to [-Custom9] is not recommended in the Alerter application. The setting of fields of a directory allows you to name them as desired. It is preferable to mention these names in the XML file surrounded by '[-' and '-]'.

Example: Here the information to fill in the Alerter application is [-id-].



Id

ContactId

The available fields of the callee are:

- [-MyFirstname-] : replaced by the first name of the callee
- [-MyLastname-] : replaced by the last name of the callee
- [-MyUsername-] : replaced by the user name of the callee
- [-MyCompany-]: replaced by the company name of the callee
- [-MyDevice-] : replaced by the device number of the callee
- [-MyGsmPhone-] : replaced by the mobile number of the callee
- [-MyEmail-] : replaced by the e-mail of the callee
- [-MyExternalKey-] : replaced by the id of the callee
- [-MyCustom0-] : replaced by the private field 0 of the callee
- [-MyCustom1-] : replaced by the private field 1 of the callee

Setting *'AlerterUrl'*: This parameter is used when *'AlerterMode'* parameter value is "URL". It contains the web site address to display in the Alerter window. The web site address can be configured with all the settings above.

For example: `http://www.google.fr/search?q=[-DisplayName-]`

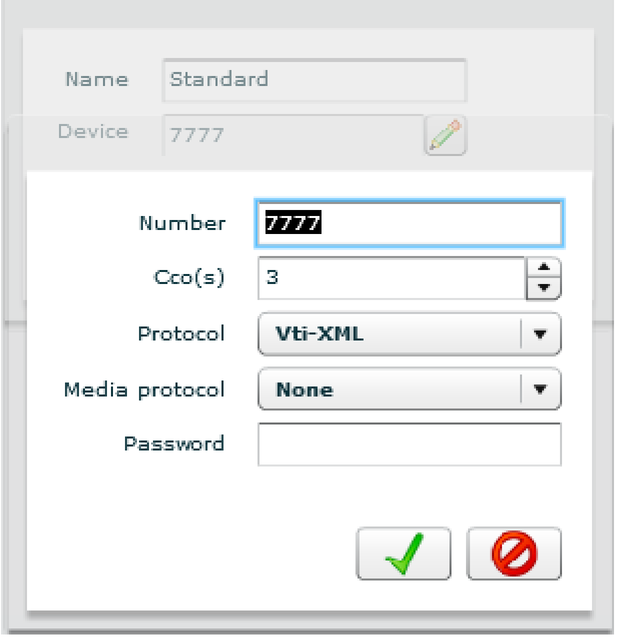
9.2.2. Call queues configuration

To properly configure a queue, follow the procedure below:

3. **Create a call queue :**

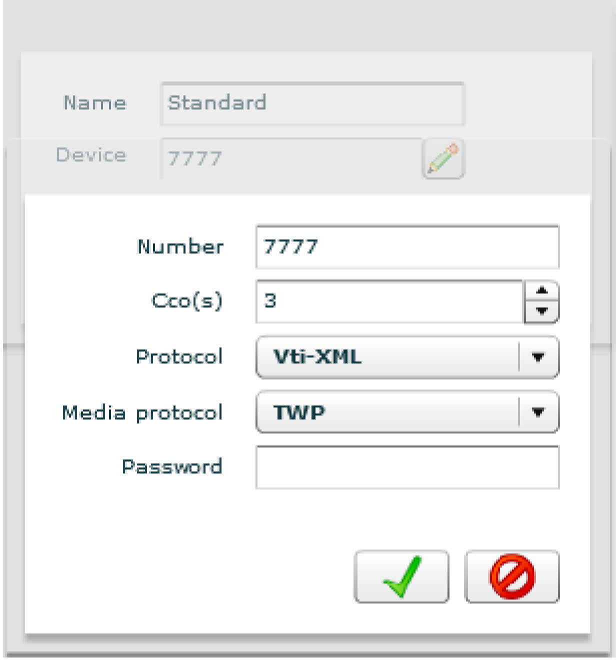
   There are several ways to create a call queue.
   In the *Telephony / Phone queues* menu, click on the "+" button to add a new call queue. Give name and number and click the edit button. Fill in the information as follows:

- *From an existing physical extension*: you already have a physical extension (device) that can be supervised by TWP, then its number can be specified to create a call queue.


Name: Standard
Device: 7777
Number: 7777
Cco(s): 3
Protocol: Vti-XML
Media protocol: None
Password:

Number: device number.
Cco(s): Number of lines available. **Value not used** because the device already has physical lines.
Protocol: choose the protocol of the device supervision.
Media protocol: In the case of an existing physical extension, select ***None***.
Password: device password if existing, useful for application monitoring.

- *From a virtual device*: create a virtual device in your PBX linked no physical extension (e.g. VTIXML/IP device on A5000). Fill the number in the configuration of the call queues.


Name: Standard
Device: 7777
Number: 7777
Cco(s): 3
Protocol: Vti-XML
Media protocol: TWP
Password:

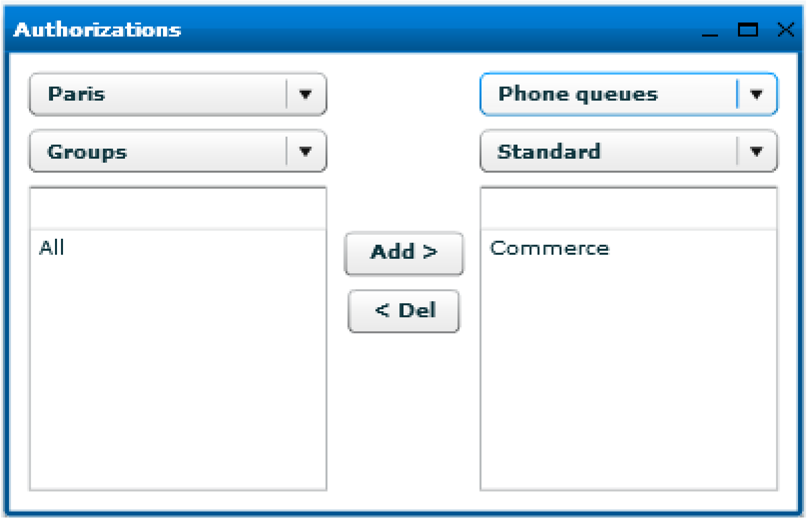
Number: device number.
Cco(s): Number of lines available. Please fill in enough to have a number of simultaneous calls therefore.

Protocol: choose the protocol of the device monitoring.
Media protocol: In the case of a virtual device, select *TWP*.
Password: device password if existing, useful for application monitoring.

4. **Give viewing permissions to users:**

Select the *Users / Authorizations* menu, select at the top right *Phone queues* then below the call queue to view. Add the rights to users or users groups (see chapter 7.4.5).

In the example, all users in the group Commerce in the domain Paris have the rights to see the "Standard" call queue.



Paris
Groups
All

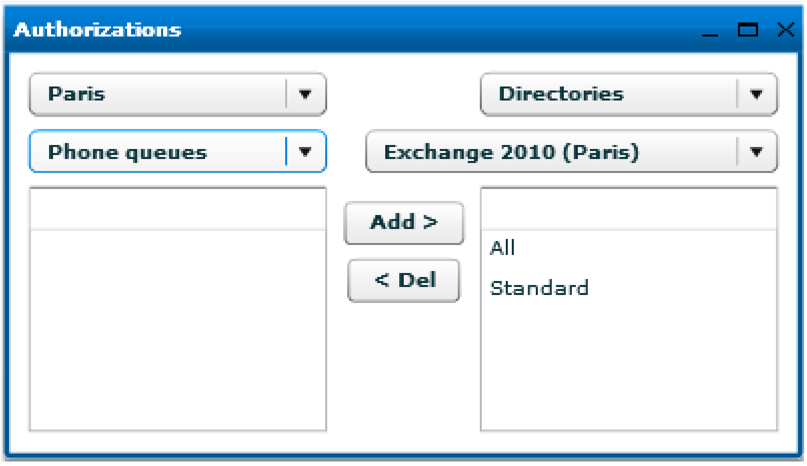
Phone queues
Standard
Commerce

5. **Directories rights :**

To display the contacts and companies names who call, the corresponding call queue may be allowed to access to TWP directories.
And the callers' information present in the corresponding directories will be automatically displayed.

Select the *Users / Authorizations* menu, select at the top right *Directories* then below the directory to authorize. In the list at the bottom left, select *Phone queues* and add the rights to the call queue.

In the example, the group “All” and the call queue “Standard” have the rights to the directory Exchange.



Information: Note that, as the Alert window, the phone queue window can also display information of private fields of directories but this is directly to activate in each user Caller preferences in menu Alerts.

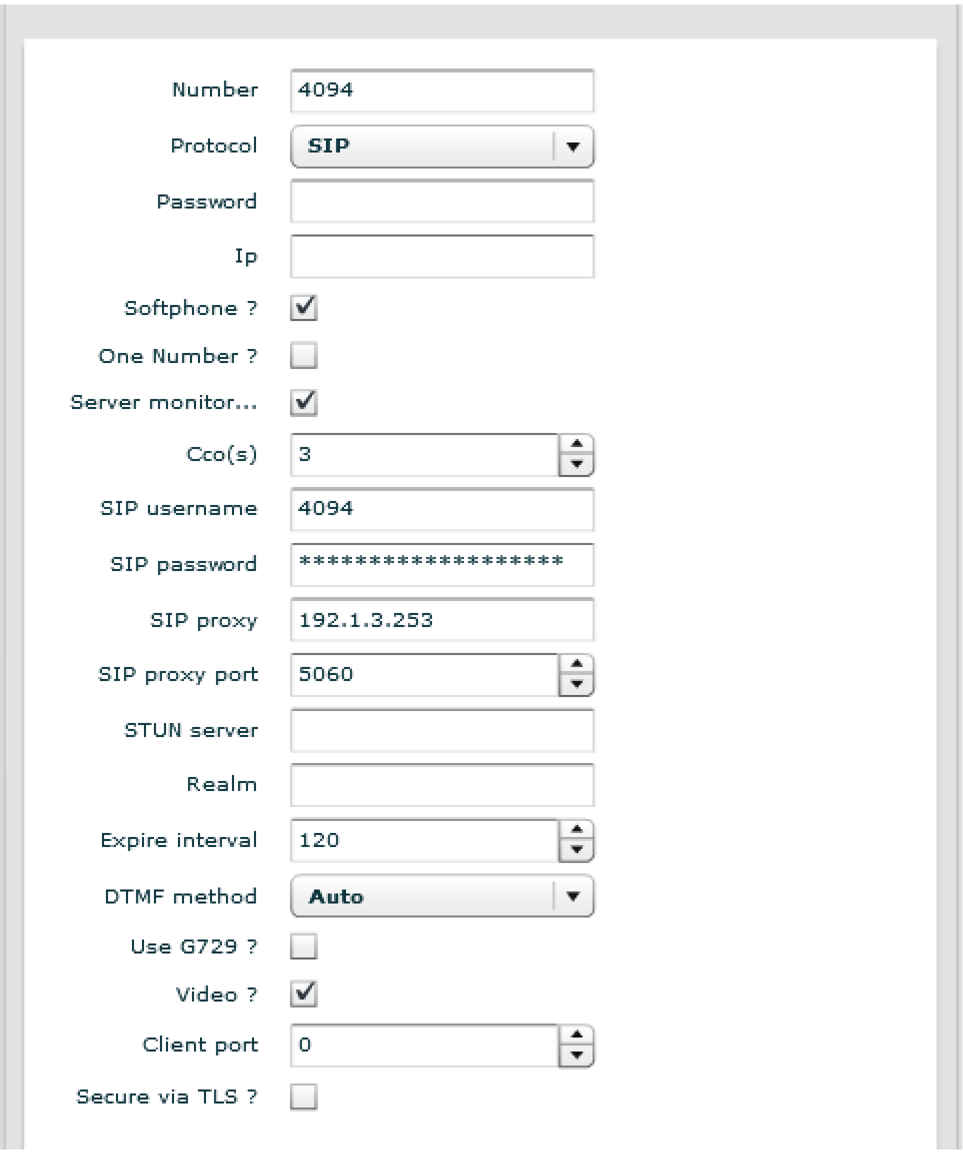
9.3. Soft phone configuration

To define the device of a user in Soft phone you must go through the menu User Management to create or modify the user as explained in chapter 3.3.4.

1. *Configuration*

To create a soft phone device, go to the *Users* / *Users* menu and create or edit a user.

Fill the device number: 4094 for example, and click on the edit button. The window below will open after choosing “SIP” as protocol.



Number	4094
Protocol	SIP ▾
Password	
Ip	
Softphone ?	☑
One Number ?	□
Server monitor...	☑
Cco(s)	3
SIP username	4094
SIP password	******************
SIP proxy	192.1.3.253
SIP proxy port	5060
STUN server	
Realm	
Expire interval	120
DTMF method	Auto ▾
Use G729 ?	□
Video ?	☑
Client port	0
Secure via TLS ?	□

Set the values as shown in the screenshot above:

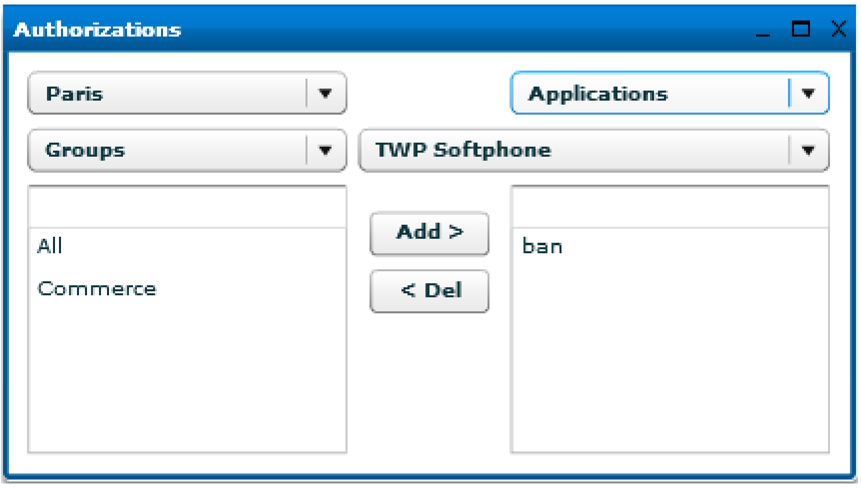
- **Number:** Soft phone device number
- **Protocol:** SIP
- **Password:** Password of the device
- **IP:** only used for the Recorder IP application
- **One Number:** checked, the soft phone is an associated device
- **Cco(s):** the number of Ccos assigned to Soft phone
- **SIP username:** SIP Id
- **SIP Password:** the password (MD5) of the SIP device if it exists.
- **SIP proxy:** IP address of the SIP proxy (in general, PBX IP address)
- **SIP proxy port:** SIP proxy port.
- **STUN Server:** reserved
- **Realm:** reserved.
- **DTMF method**: RTP to be in RFC2833 mode or SIPINFO
- **G729**: checked to allow G729.
- **Video:** checked to allow video calls.
- **TLS:** checked to use an encrypted connection.

Remark: the PBX must be configured accordingly.

2. *Authorizations*

The Soft Phone feature consumes a license. You have to give permissions to the user with a Soft Phone feature configured.

To give these permissions, go to the menu *Users / Authorizations* and give rights as below. In this example, the user “ban” can execute its Caller in Soft phone mode.



Authorizations

Paris

Applications

Groups

TWP Softphone

All

Commerce

ban

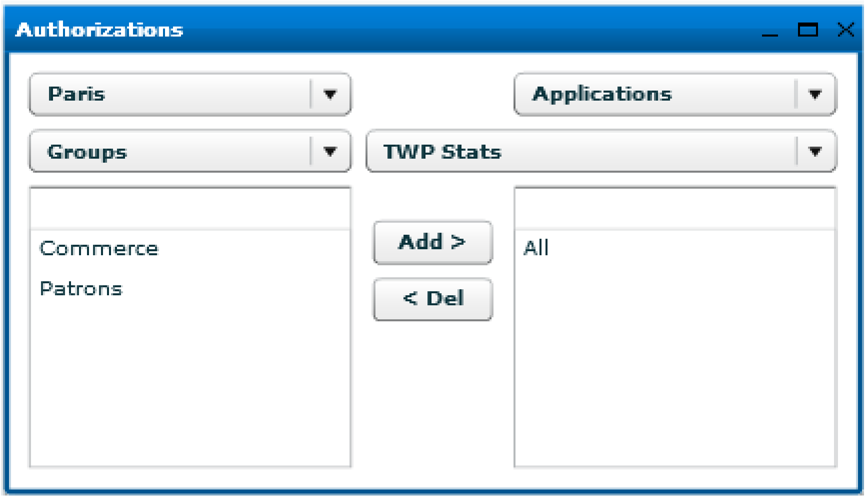
9.4. Statistics configuration

Through the application of statistics, a user can view by various different graphics its call data or other users' data.

The Stats data of users are stored only for a certain number of days (see 10.2.2.).

9.4.1. TWP Stats

To dispose of this application and allow a user to view their own statistics, you only have to give the permissions to the application TWP *Stats*, in the administration *Users / Authorizations* menu. This consumes 1 Stats license per user.



Authorizations

Paris

Applications

Groups

TWP Stats

Commerce

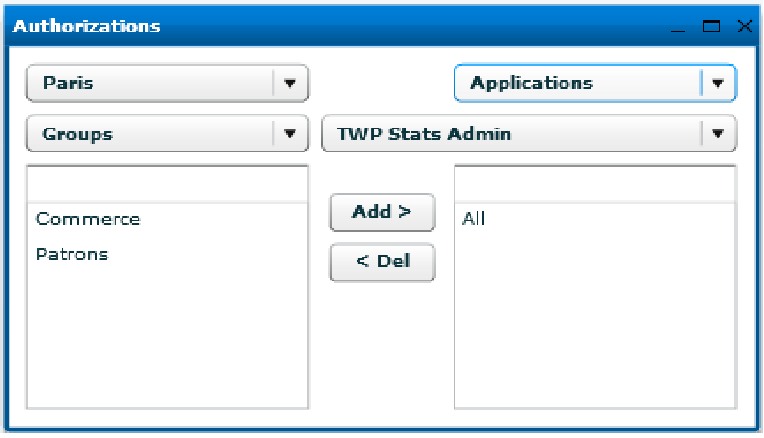
Patrons

All

9.4.2. TWP Stats Admin

1. *Application Authorizations*

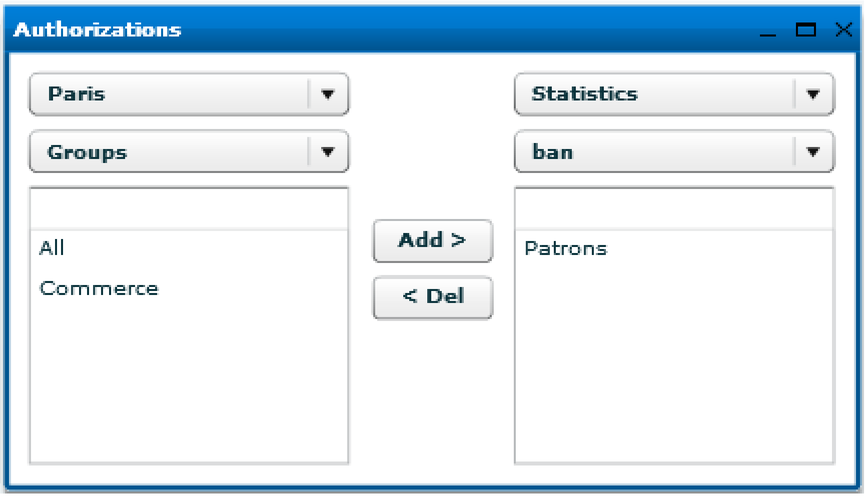
To dispose of this application and allow a user to view their own statistics, you only have to give the permissions to the application TWP *Stats Admin*, in the administration *Users / Authorizations* menu. This consumes 1 Stats Admin license per user.



2. *Users Statistics Data Authorizations*

So that the user has access to statistics data of other users, permissions should be given to this user. In the administration *Users / Authorizations* menu, choose *Statistics* in the top right of the window. Unlike permissions on other objects, those for the statistics data are done conversely (see chapter 7.4).

Indeed, the example below shows that user "ban" have access to the statistics of users of the group 'Patrons'.

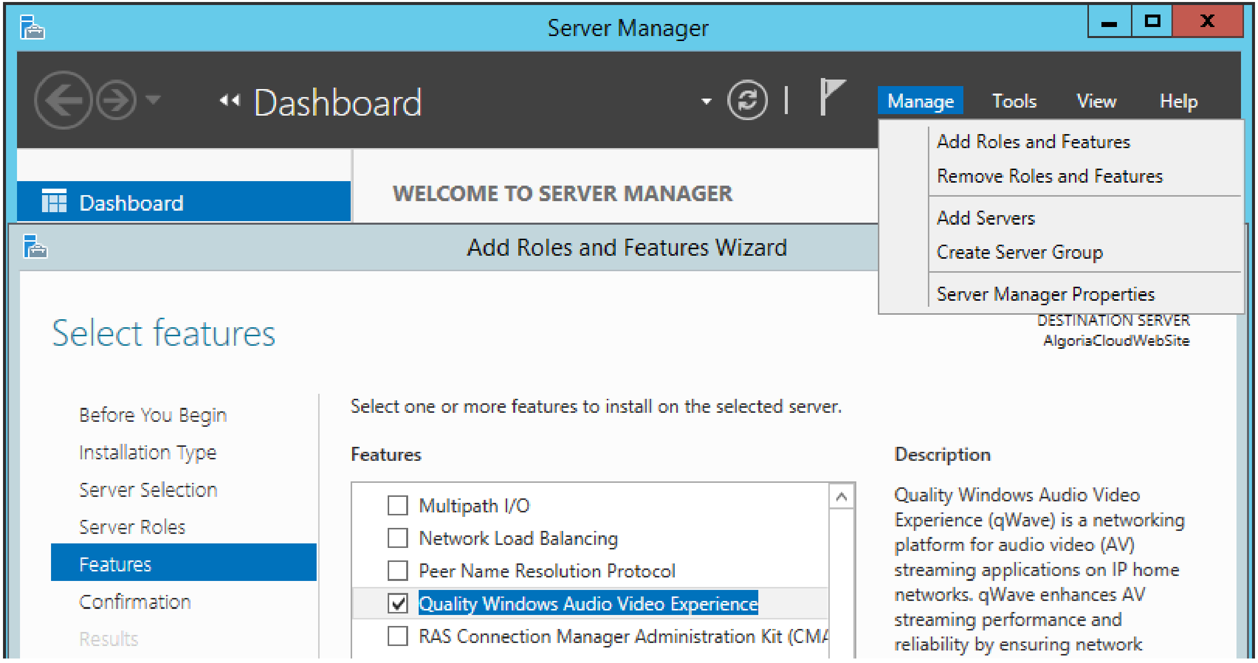


9.5. Configuration of resources for Rules, Mail, VideoShare applications

Virtual device resources allow the user to configure an announcement in a forwarding rule which will be read before the call forwarding for the Rules application.
Virtual device resources allow a user to conference.

Prerequisites:

- Install Quality Windows Audio Video Experience on the Windows system from the Server Manager / Manage / Add Roles and Features. Example on a Windows Server 2012 below. **Attention**: Without this feature, the TWS4$TWS_ConferenceServices does not start.



Select features

DESTINATION SERVER
AlgoriaCloudWebSite

Select one or more features to install on the selected server.

Features

- ☐ Multipath I/O
- ☐ Network Load Balancing
- ☐ Peer Name Resolution Protocol
- ☑ Quality Windows Audio Video Experience
- ☐ RAS Connection Manager Administration Kit (CMA

Description

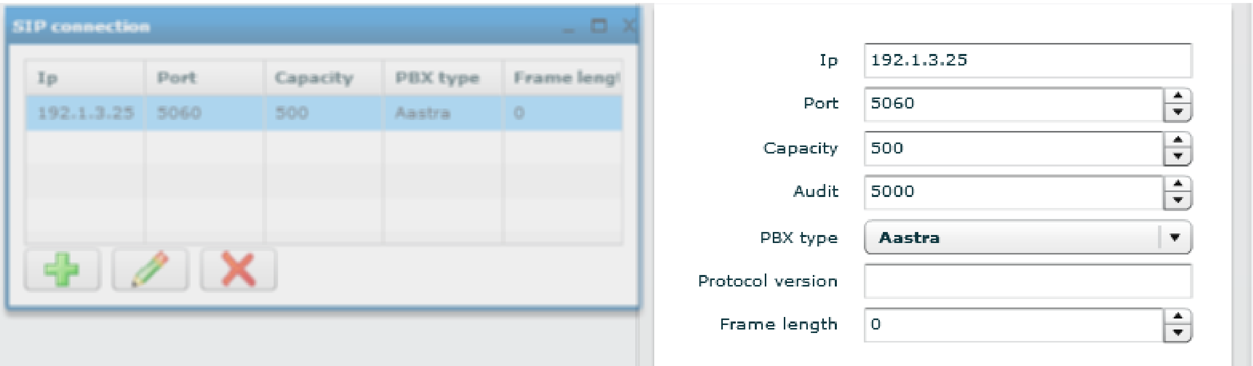
Quality Windows Audio Video Experience (qWave) is a networking platform for audio video (AV) streaming applications on IP home networks. qWave enhances AV streaming performance and reliability by ensuring network

- The telephone exchange (PABX) should allow the supervision of SIP virtual device via a SIP connection.

9.5.1 SIP connection

Before configuring the resources to use in different applications, you must create the necessary SIP registration to the PBX connection.

In administration, *Connections* / *SIP connection* menu, click the "+" button to add a new SIP connection.



SIP connection

Ip	Port	Capacity	PBX type	Frame lengt
192.1.3.25	5060	500	Aastra	0

Ip	192.1.3.25
Port	5060
Capacity	500
Audit	5000
PBX type	Aastra
Protocol version	
Frame length	0

In the new window that opens enter the most basic information as follows:

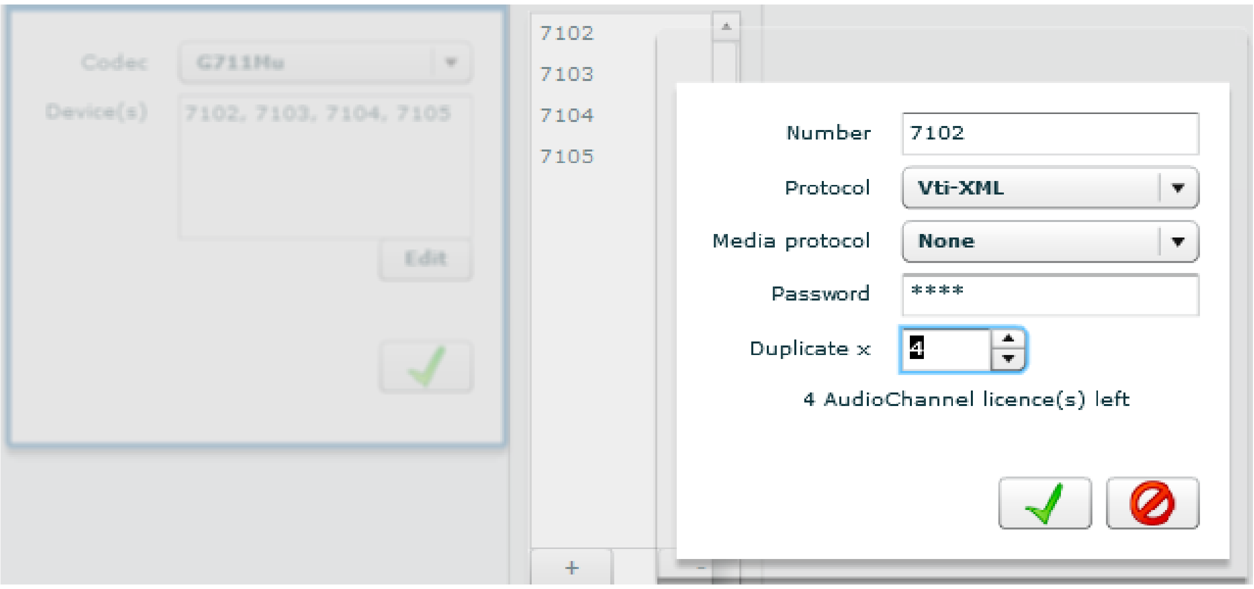
- **Ip**: IP address PBX that supports SIP registration
- **Port**: PBX port for the SIP registration
- **PBX type**: choose the PBX type

Leave the values of other default information. Then validate. A new SIP connection is created.

Note: One SIP connection is required and will be used. To configure a second SIP connection, it is essential to do so in a new domain.

9.5.2 Configuration of virtual device resources

To configure these resources, go to the administration, *Applications* menu then select the relevant application: TWP *Rules*, TWP *VideoShare*… Then click on the *Edit* button, then in the new window on the “+” button.



Codec: G711Mu

Device(s): 7102, 7103, 7104, 7105

7102
7103
7104
7105

Number: 7102

Protocol: Vti-XML

Media protocol: None

Password: ****

Duplicate x: 4

4 AudioChannel licence(s) left

In the new window that opens enter the most basic information as follows:

- **Number**: first resource number of the list of resources to create

- **Protocol**: *SIP* only

- **Media protocol**: *None* only

- **Password**: Password for the SIP registration of all virtual device resources to create. *0000* per default.

- **Duplicate x**: Number of the devices in the list to create.

Validate and close the windows.
The resources are created. **It is necessary to restart the $TWS4TWS_MediaServices service so that they register to the PBX.**

9.6. Configuration of the Rules application

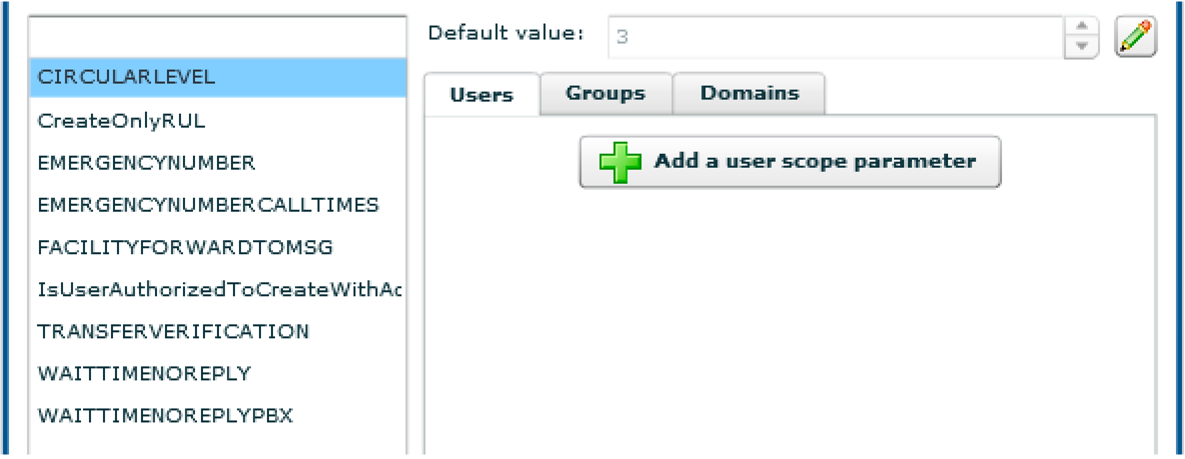
Without the Rules application, a user can already divert his calls by configuring simple forwarding rules that will apply a forward in the PBX while they will be activated. Thanks to the Rules application, users can now make this forward from an advanced (extremely customizable) rule that are based on a number of features to configure.

9.6.1 Configuration of virtual device resources

See chapter *9.5*.

9.6.2 Configuration of Rules settings

A number of parameters manage features of advanced rules. To access these settings, go to the administration, *Applications / Applications parameters*. Select TWP *Rules*.



- **CIRCULARLEVEL**: *Number* of following forward to forbid before the call returns to first device which get it. If the system encounters this conflict, no forward is executed.
  0 = no verification
  1 = A can't forward to A
  2 = B can't forward to B and can't forward to A which forwards to B…

- **CreateOnlyRUL**: *Yes or No* users will only have advanced rules. No more forward will be apply in the PBX.

- **EMERGENCYNUMBER**: *number* of emergency to call if the contacts to who users forward their calls don't answer (in the case the setting *TRANSFERVERIFICATION* = *Yes* (True)).

- **EMERGENCYNUMBERCALLTIMES**: *Number* of times the emergency number will be called if there is nobody answering.

- **IsUserAuthorizedToCreateWithAdminRules**: *Yes or No* the user may create his forward rules when the administrator will impose him others.

- **TRANSFERVERIFICATION**: *Yes or No* the system will verify that the calls forwarded by users will be well answered by the correspondent. If a rule contains a false number as a forward number, the system will detect and will divert to the emergency number if configured.

- **WAITTIMENOREPLY**: Duration in *seconds* to wait for an advanced rule before it forwards by no answer.

- **WAITTIMENOREPLYPBX**: Duration in *seconds* to wait for a PBX/simple rule before it forwards by no answer. This value must be copied from the PBX.

9.7. Configuration of VideoShare application

9.7.1 Configuration virtual device resources

See chapter *9.5*.

9.7.2 Configuration of settings linked to the Audio – Video conferencing and application sharing

A number of parameters manage some configurations related to Audio – Video conferencing and Application Sharing. To access these settings, go to the administration, *Applications / Applications parameters* menu.

Select TWP *MediaServer*.

- **AppSharingRouterIP**: IP address of the server where the TWS4$TWS_AppSharingRouterServices service is running for Application Sharing. **It is important to change this value to the IP address of the server TWP.**

- **AppSharingRouterPort**: Port of the server where the TWS4$TWS_AppSharingRouterServices service is running. Per default, the value is 8202.

(Expert Mode)

- **MediaServerSIP_IP**: The IP address of the server where the TWS4$TWS_ConferenceServices service is running. **It is important to change this value if it is a remote server**.

- **MediaServerSIP_Port**: Port of the server where the TWS4$TWS_ConferenceServices service is running for Audio – Video conferencing. Per default, the value is 8201.

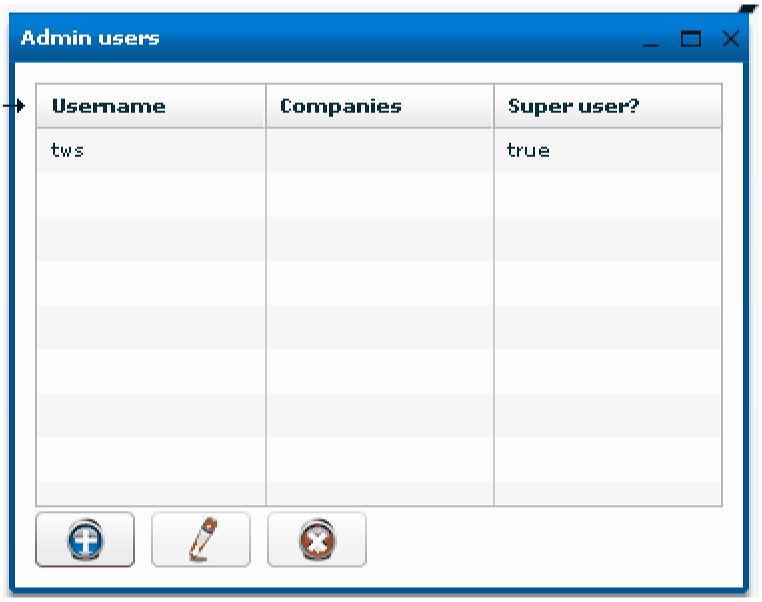
10. Maintenance

10.1. Manage administrator profiles

The administrators typically are responsible for managing specific user rights.

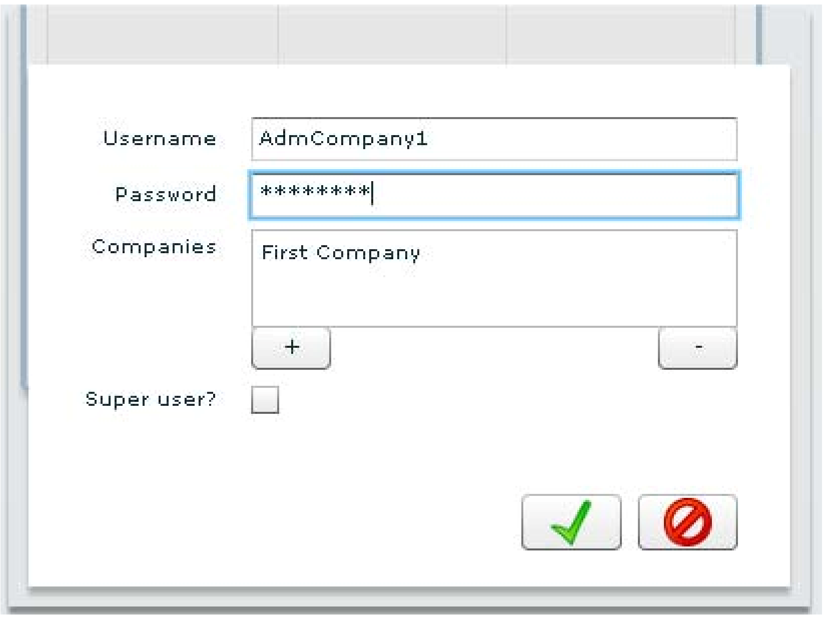
If you want to limit access to the administration interface to a single company, you need to create a new administrator account.

Select the *Global* / *Admin us*ers menu.



Username	Companies	Super user?
tws		true

Then click on “+”.



Username: AdmCompany1

Password: ********

Companies: First Company

Enter the administrator name and password, and then add the list of authorized companies for this administrator by clicking the "+" button.

The Super User option allows the user to access all relevant companies.

10.2. System settings and Expert mode

System settings

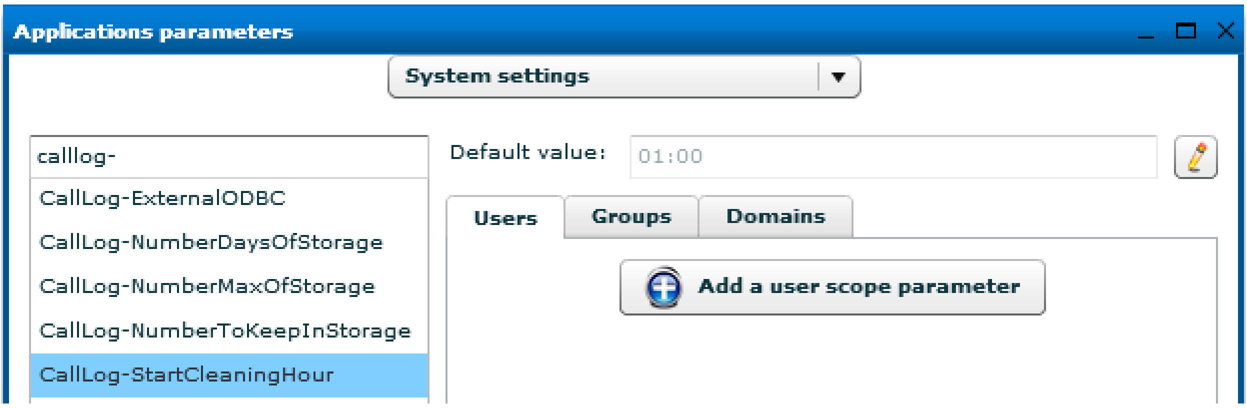
All standard system settings of TWP server are present in the *Applications / Applications parameters* menu then choose *System settings*. Do not change any of these settings unless described in this document or if the support asks you to.

Expert Mode

Whatever setting type, if it is system or application, there are parameters that are only visible in Expert mode. You can enable it in the administration by passing the mouse to the right of "*Log out*" button. The checkbox will appear and this time click and new parameters appear.

10.2.1. Deleting automatically data: call logs

In the *Applications / Applications parameters* menu, choose *System settings*, search "*CallLog-*" and settings will appear:


Applications parameters

System settings

calllog-

CallLog-ExternalODBC

CallLog-NumberDaysOfStorage

CallLog-NumberMaxOfStorage

CallLog-NumberToKeepInStorage

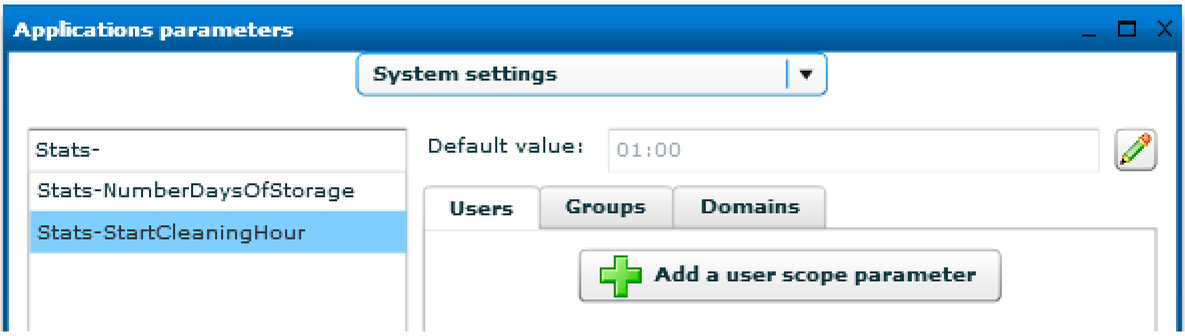
CallLog-StartCleaningHour

Default value: 01:00

- *CallLog-StartCleaningHour*: in HH:MM format (hour and minute), change only the default value to the time of the day when call logs cleaning will be started.
- *CallLog-NumberMaxOfStorage*: Number of lines per type of call (Incoming, Outgoing, Missed) to retain after a day. Default value is 30.
- *CallLog-NumberDaysOfStorage*: Regardless of the previous setting, it means the number of days to keep calls in the logs. Default value is 30.
- *CallLog-NumberDaysOfStorage*: Regardless of the previous settings, it means the minimum number of calls to keep in the log of a user. Default value is 30.

10.2.2. Deleting automatically data: Statistics

In the *Applications / Applications parameters* menu, choose *System settings*, search “*Stats-*” and 2 setting appear:



System settings

Stats-

Stats-NumberDaysOfStorage

Stats-StartCleaningHour

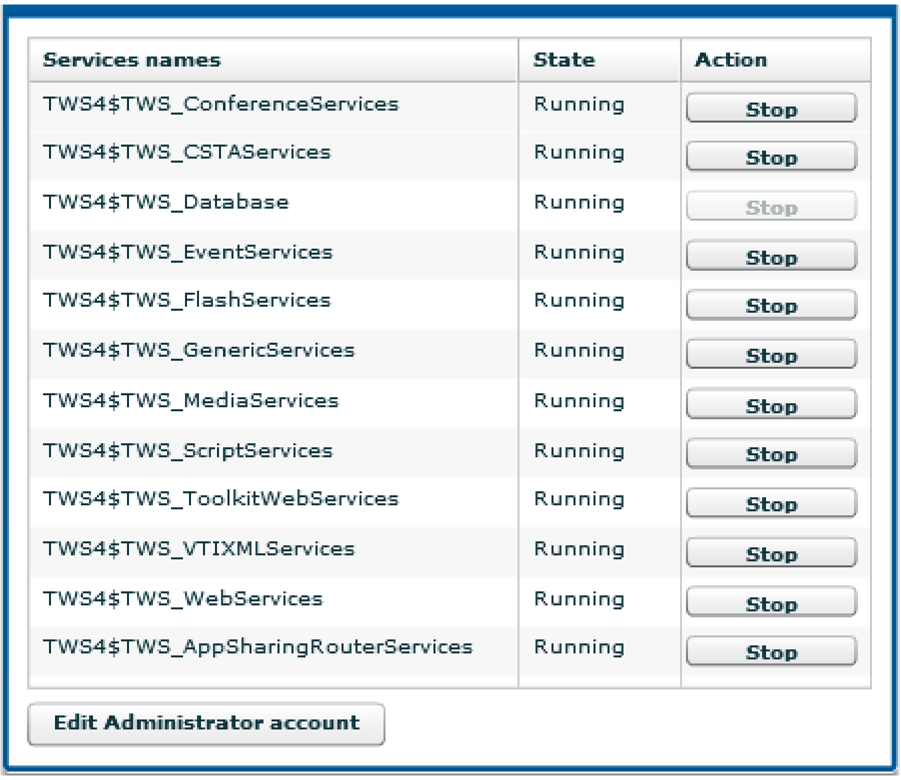
Default value: 01:00

- *Stats-StartCleaningHour*: in HH:MM format (hour and minute), change only the default value to the time of the day when the cleaning of statistics data will be started.
- *Stats-NumberDaysOfStorage*: This parameter specifies the number of days for which statistical data are maintained.

10.3. Services

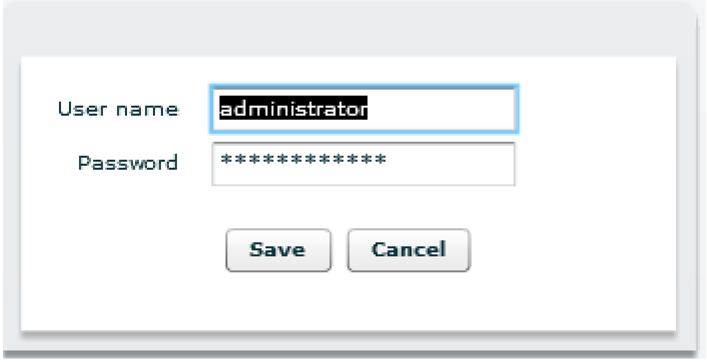
Open the drop-down *Tools* menu and click the TWP Services menu.

This menu allows you to monitor the status of TWP server services.



Services names	State	Action
TWS4$TWS_ConferenceServices	Running	Stop
TWS4$TWS_CSTAServices	Running	Stop
TWS4$TWS_Database	Running	Stop
TWS4$TWS_EventServices	Running	Stop
TWS4$TWS_FlashServices	Running	Stop
TWS4$TWS_GenericServices	Running	Stop
TWS4$TWS_MediaServices	Running	Stop
TWS4$TWS_ScriptServices	Running	Stop
TWS4$TWS_ToolkitWebServices	Running	Stop
TWS4$TWS_VTIXMLServices	Running	Stop
TWS4$TWS_WebServices	Running	Stop
TWS4$TWS_AppSharingRouterServices	Running	Stop

Click on "*Edit Administrator account*": you must enter the information of the local administrator of the machine to start and stop Windows services from this screen.



User name: administrator

Password: ************

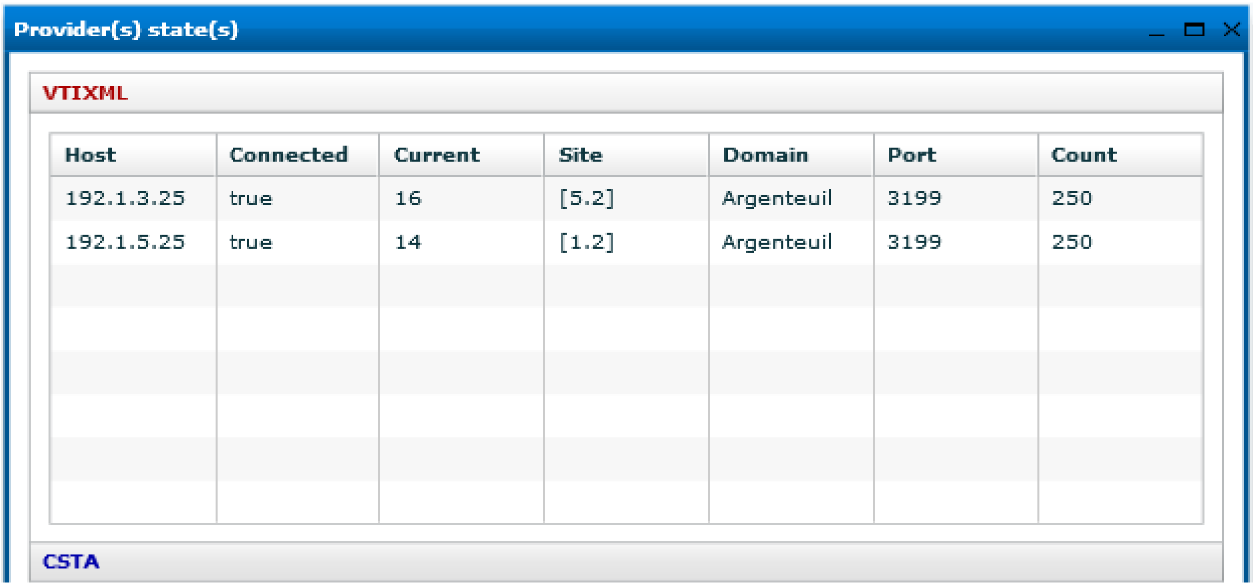
Click on "*Save*".

- Start TWS4$TWS_Database service if not started
- Start TWS4$TWS_GenericServices, the other services will be automatically started

10.4. Connections states

Tools menu and *Provider(s) state(s)* menu, in this menu you will monitor the PBX connections state.

The example below shows the VTIXML connection status:



Provider(s) state(s)

VTIXML

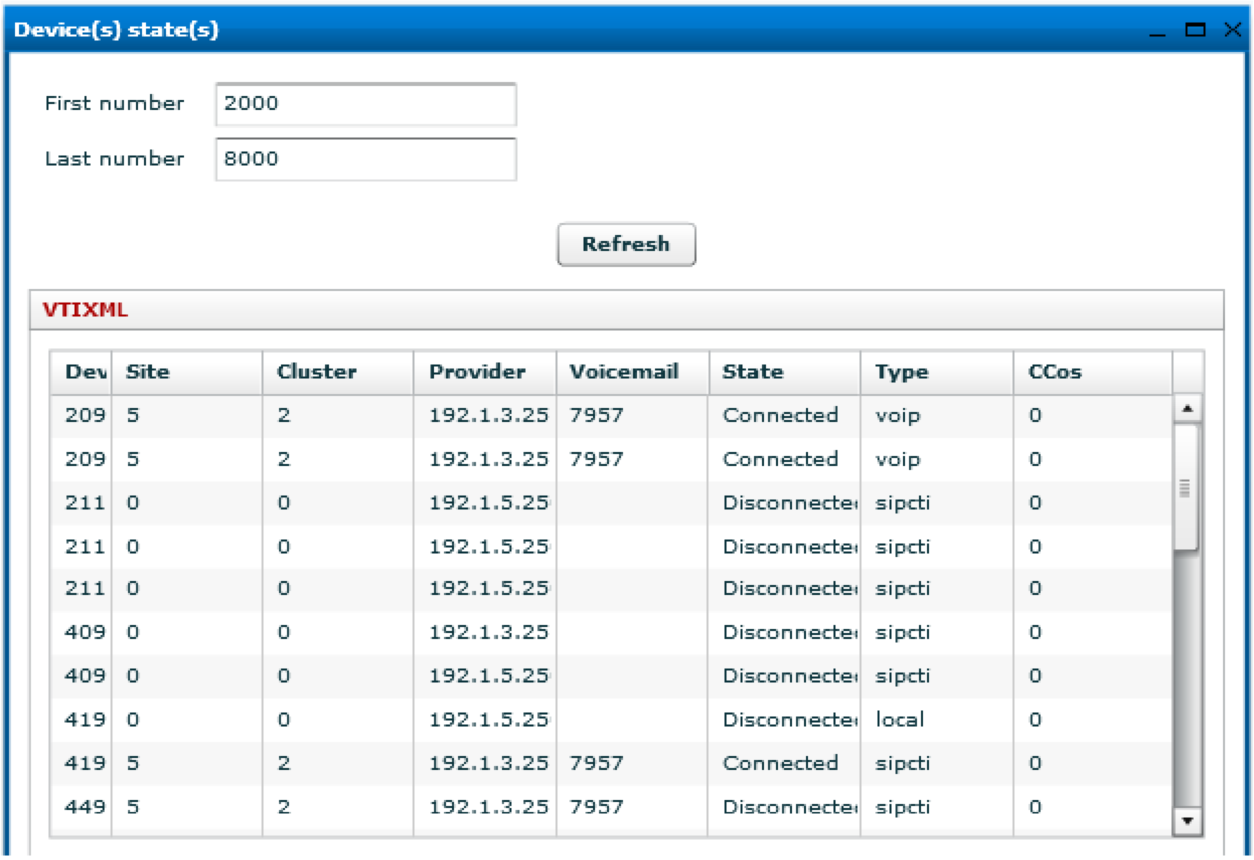
Host	Connected	Current	Site	Domain	Port	Count
192.1.3.25	true	16	[5.2]	Argenteuil	3199	250
192.1.5.25	true	14	[1.2]	Argenteuil	3199	250

CSTA

- *Host*: PBX IP address
- *Connected*: true if the link is connected
- *Current*: number of positions supervised by this link
- *Site*: Site.cluster defined for the link (only for the VTIXML connector)
- *Domain*: Domain name assigned to the link
- *Port*: TCP port used by the connector
- *Count*: maximum number of devices supervised by this link

10.5. Devices states

Tools menu and *Device(s) state(s)* menu. Fill the first and the last number of the devices that you want to monitor and click on Refresh:



First number: 2000

Last number: 8000

VTIXML

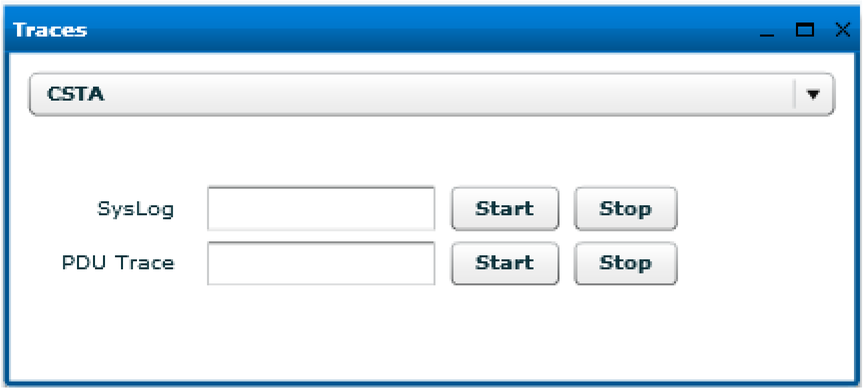
Dev	Site	Cluster	Provider	Voicemail	State	Type	CCos
209	5	2	192.1.3.25	7957	Connected	voip	0
209	5	2	192.1.3.25	7957	Connected	voip	0
211	0	0	192.1.5.25		Disconnecte	sipcti	0
211	0	0	192.1.5.25		Disconnecte	sipcti	0
211	0	0	192.1.5.25		Disconnecte	sipcti	0
409	0	0	192.1.3.25		Disconnecte	sipcti	0
409	0	0	192.1.5.25		Disconnecte	sipcti	0
419	0	0	192.1.5.25		Disconnecte	local	0
419	5	2	192.1.3.25	7957	Connected	sipcti	0
449	5	2	192.1.3.25	7957	Disconnecte	sipcti	0

- *Devices*: number of the subscriber
- *Site*: Site where the subscriber is logged (only VTIXML)
- *Cluster*: Cluster where the subscriber is logged (only VTIXML)
- *Provider*: Id of the provider connection
- *Voicemail*: Voicemail number linked to the subscriber
- *State*: Connected / Disconnected
- *Type*: CTI / VOIP / SIPCTI, device monitoring type.
- *CCos*: number of CCos, device lines (only for Soft phone).

10.6. Traces

Tools menu and *Traces*.

You can log TWP services remotely by using Syslog software or by triggering the PDU.
This option is only used under the approval of technical support.



Pdu trace:

Don’t "start Pdu trace" without the approval of technical support.
Select the protocol you want to log.

Start: start the Pdu trace for the device number defined in the field. Enter '*' character to log all.

Stop: stop the Pdu trace

The directory containing the logs is in:

- CSTA: C:\Program Files\TWS4\TWS_Services\TWS_CSTAServices\Trace
- VTI-XML: C:\Program Files\TWS4\TWS_Services\TWS_VTIXMLServices\Trace

Syslog:

Enter the IP address specified by the technical support. It is IP address of PC which executes Syslog software:

Start: Start syslog

Stop: Stop syslog
The logs will be sent to the syslog server as defined.

10.7. Save the configuration

Make a backup of the database

- Go to the directory « \TWS4\TWS_Web\TWS_Data\DatabaseBackup »
- Run « backup.bat »
- The backup is in the "data" folder and is named with the day name

Make a full backup of the configuration

- Save files:
  - \TWS4\TWS_Web\TWS_Config
  - \TWS4\TWS_Web\TWS_Data

Do a restore of the database

- Go to the directory « \TWS4\TWS_Web\TWS_Data\DatabaseBackup »
- Run « restore.bat »
- A list of available backups is displayed. Enter the name of the backup to restore
- The TWP database is restored

Create a scheduled task to backup the database

- Go to the directory « \TWS4\TWS_Web\TWS_Data\DatabaseBackup »
- Run « backup_create_windows_task.bat »
- The task is created, it executes the "backup.bat" script daily at 2am
- The Scheduled Tasks Manager opens, it is possible to change the "TWS_DATABASE_BACKUP" task to refine its configuration. [optional]

Automatically copy the backups to another computer

- Edit "backup.bat" file with notepad.
- Complete line "set COPYPATH =" with the path where to copy the backup

(Example: set COPYPATH=\\10.0.0.1\share\Backup\TWP)

- Save Changes

10.8. Troubleshooting

10.8.1. Standard problems

Below are some malfunction examples, with the possible sources of the problems and their solutions.

Type of problem	Error message or symptoms	Test	Details or actions
The application does not start	Certain users cannot connect	The user parameters are badly defined (check in the TWP administration)	The following fields are compulsory: - Login - Authorizations (server and applications) - Init or set number - Monitoring type
	Licenses	The licenses (applications or server) are not taken into account.	Consult chapter to enter or check the licenses via the TWP administration.
	PABX	The connection to the PBX does not work	Check the concordance between the IP address entered in the TWP administration and the PBX address
	Services	The TWP services have not started	Check their state (Started/Stopped) via administration. Start them if necessary
	Certain users cannot connect	The user login has not been saved on the server or the server domain	If the domains are different between the user and the TWP server, add the user (same login, same password) in the local server accounts.
	CSTA	If CSTA mode: check the number of CSTA licenses in the PBX	The number of licenses must correspond to the number of licenses used in CSTA mode.
	CSTA	If CSTA mode: check the configuration of the CSTA port (3211: cf. doc)	The CSTA port is not always configured by default in the PBX.
	"Access denied"	The user does not have access rights to the http server	Check the user's rights on the TWP server
Failure retrieving the directory	The waiting period is long (Manual mode)	This is normal if there are a lot of files	The import may take time if there are a lot of files Do not interrupt the process

	The Exchange directory import fails (1)	The Login/Password are wrong	In the User/Password fields you must enter a login with *Exchange Domain Server* rights on the intended Exchange server.
	The Exchange directory import fails (2)	The connection address is wrong	Test the connection url in Internet Explorer (this should open an Outlook Web Access page)
	The LDAP import does not work	The Login/password have been entered wrongly or the LDAP keys are wrong	Mind the cases (upper/lower) on the group and domain names

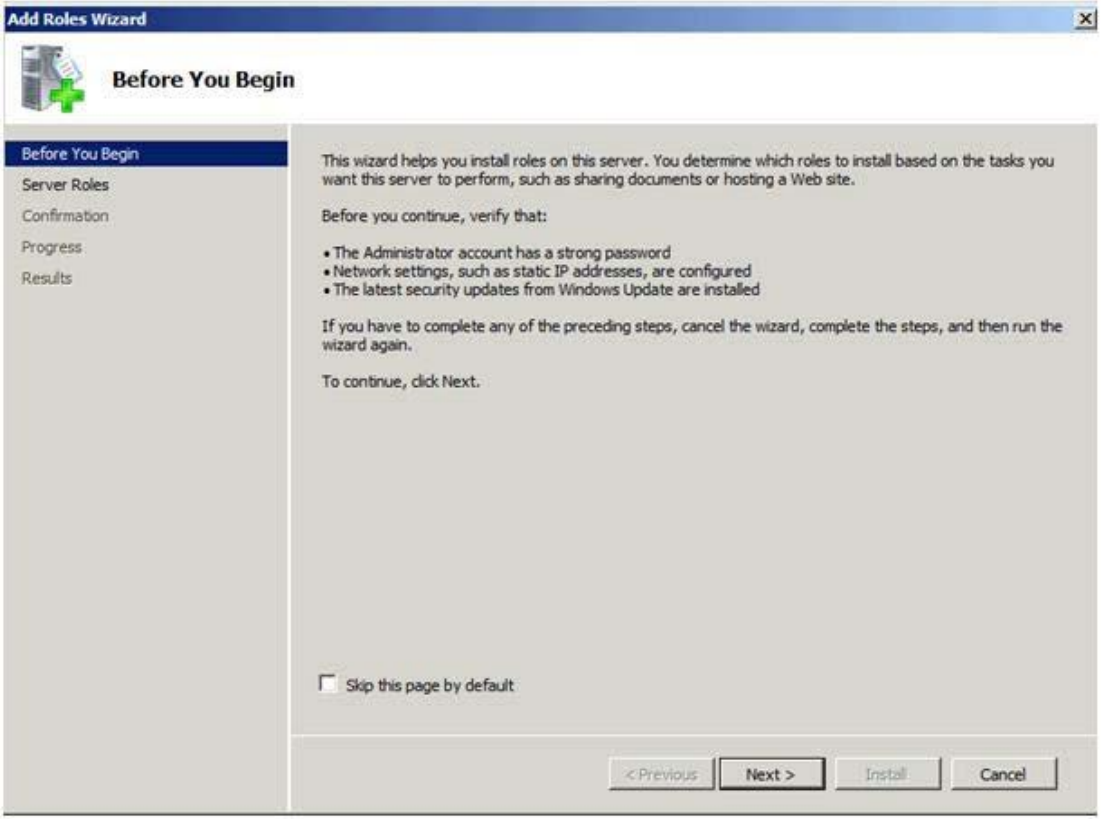
11. Annexes

11.1. Windows 2008 – 2012 x64 Setup

11.1.1 Installing IIS

At the Server Manager, select the menu to add new roles (*right click on Roles* menu > *Add roles* for W2008 - *Manage* > *Add roles and features* for W2012).

Add a new role: *IIS*.



Add Roles Wizard

Before You Begin

This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

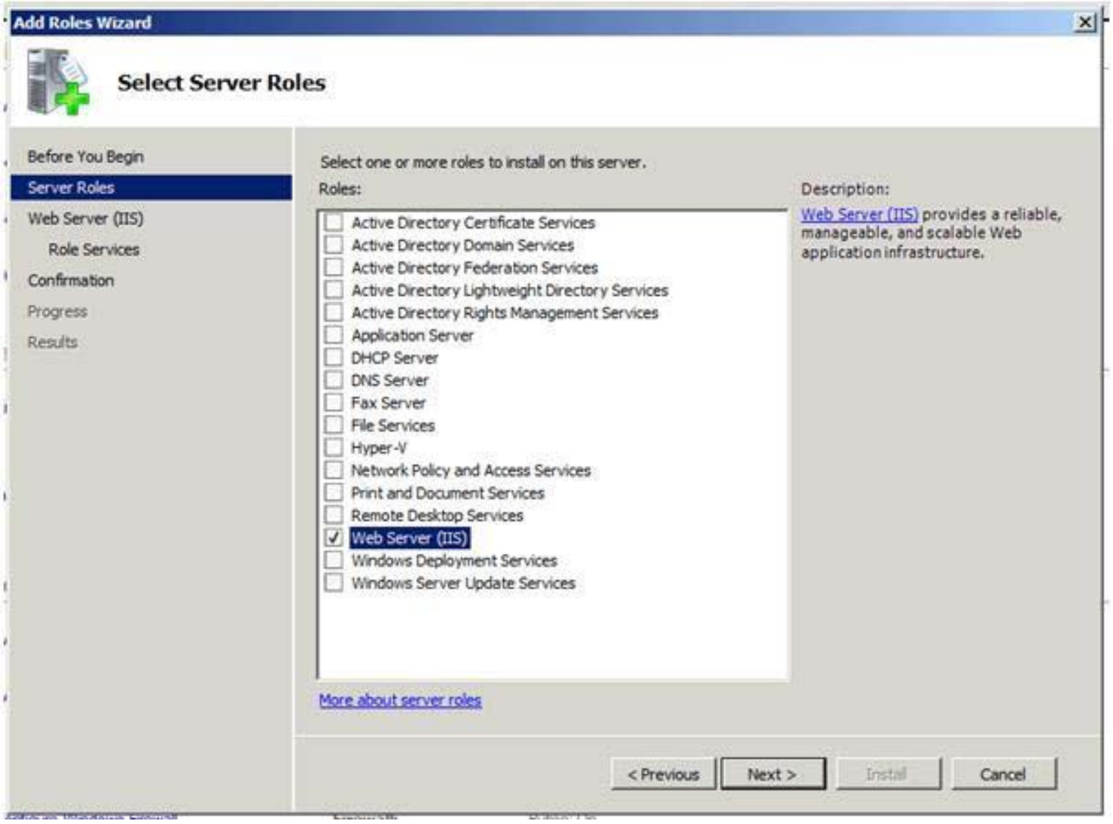
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Click on "Next":



Add Roles Wizard

Select Server Roles

Select one or more roles to install on this server.

Roles:

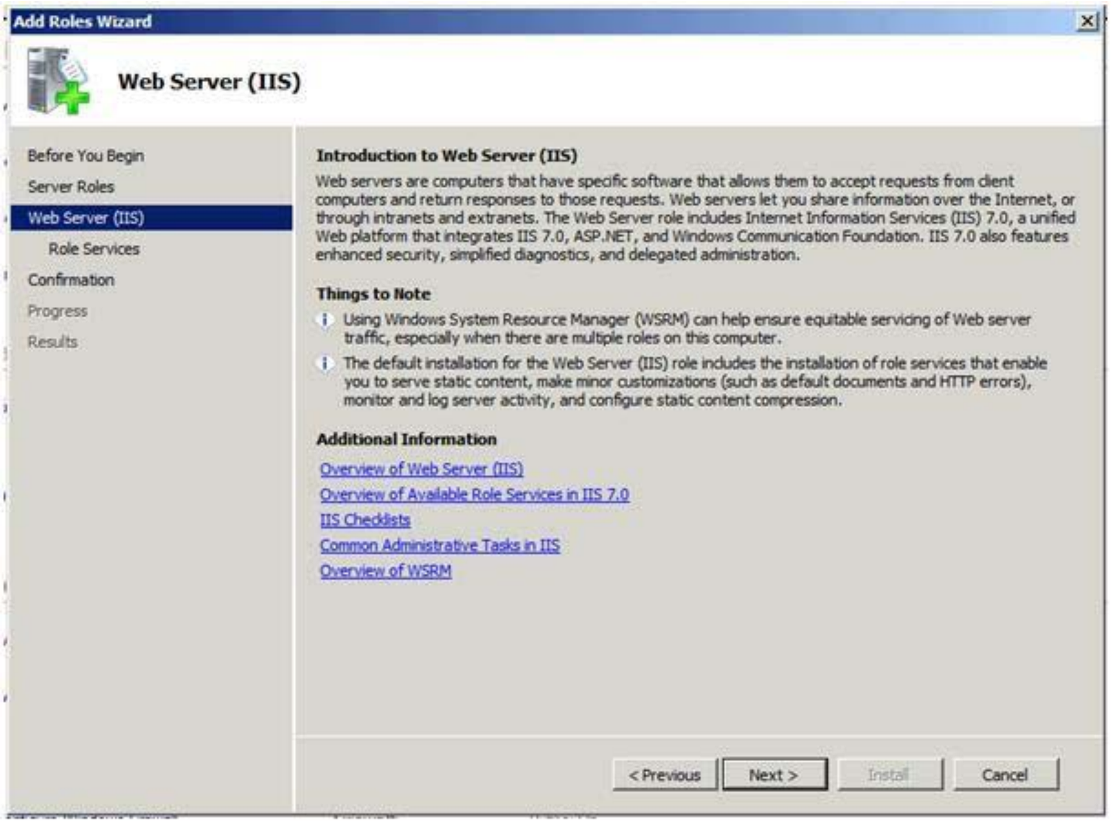
- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Desktop Services
- ☑ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description:

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

More about server roles

Select "Web Server (IIS)". Then click on "Next":



Add Roles Wizard

Web Server (IIS)

Introduction to Web Server (IIS)

Web servers are computers that have specific software that allows them to accept requests from client computers and return responses to those requests. Web servers let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 7.0, a unified Web platform that integrates IIS 7.0, ASP.NET, and Windows Communication Foundation. IIS 7.0 also features enhanced security, simplified diagnostics, and delegated administration.

Things to Note

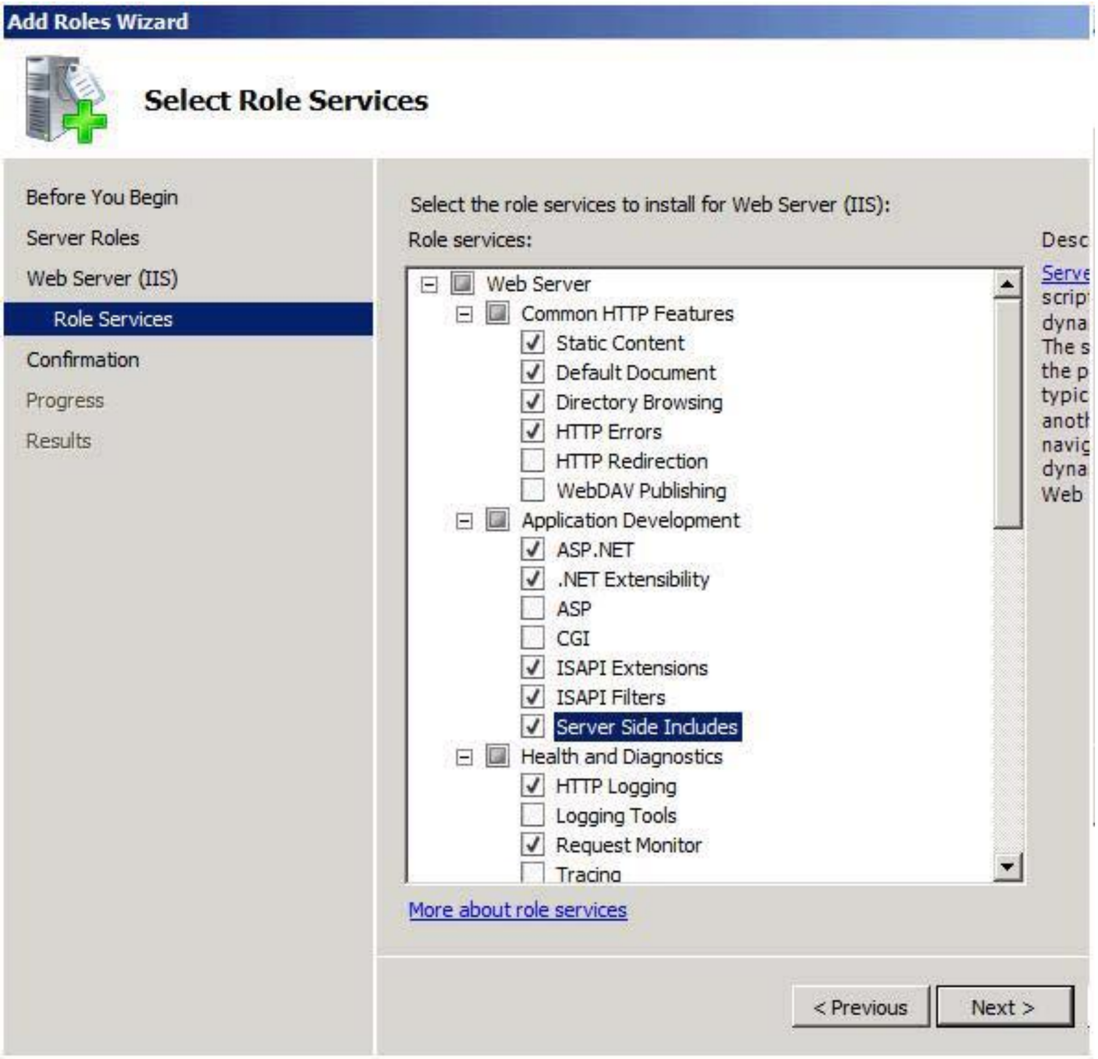
- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

Additional Information

Overview of Web Server (IIS)
Overview of Available Role Services in IIS 7.0
IIS Checklists
Common Administrative Tasks in IIS
Overview of WSRM

Click on "Next". And select the options as below.

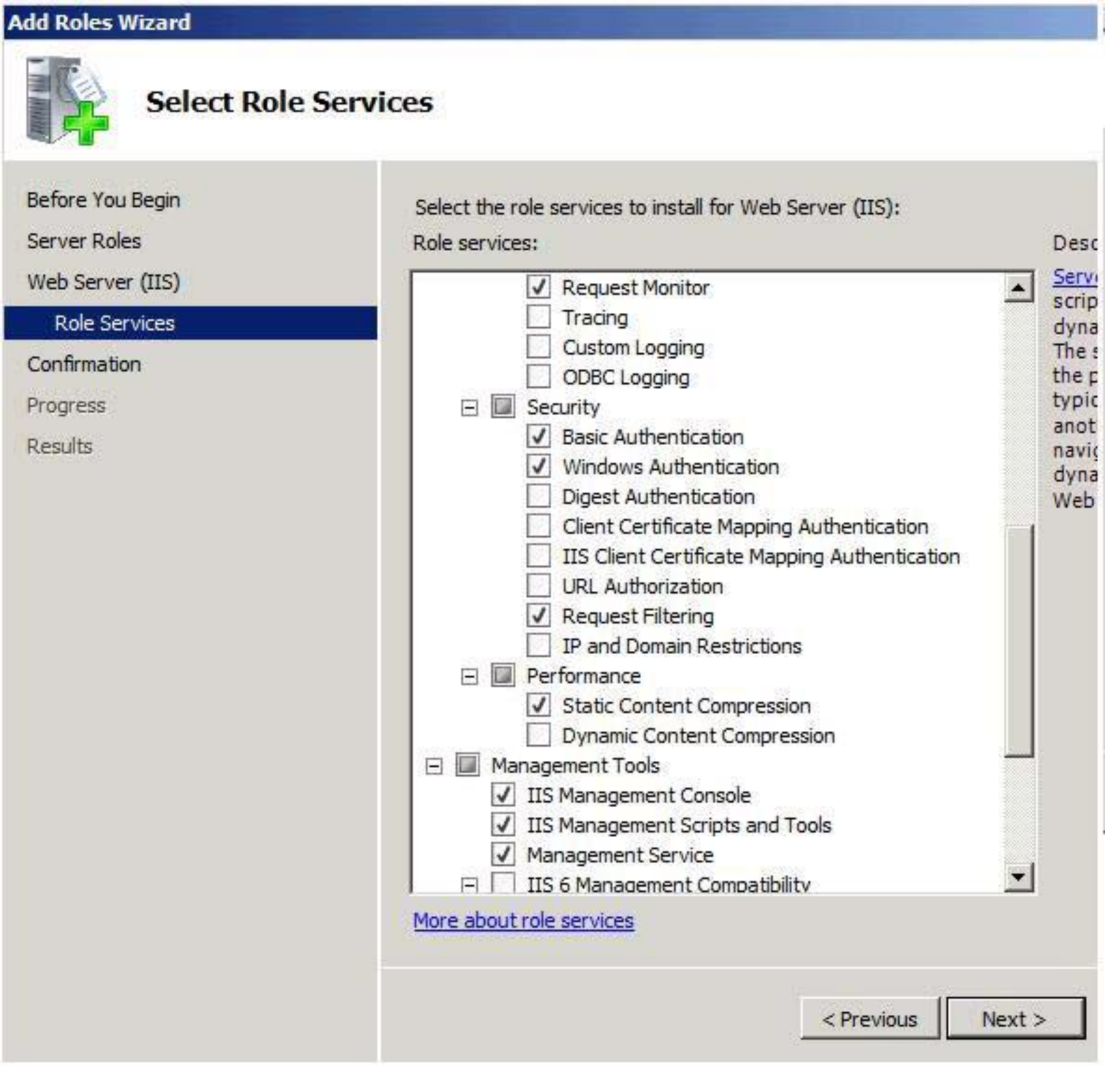
- ***On W2008 & W2012:***



Select the role services to install for Web Server (IIS):

Role services:

- Web Server
  - Common HTTP Features
    - ☑ Static Content
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - □ HTTP Redirection
    - □ WebDAV Publishing
  - Application Development
    - ☑ ASP.NET
    - ☑ .NET Extensibility
    - □ ASP
    - □ CGI
    - ☑ ISAPI Extensions
    - ☑ ISAPI Filters
    - ☑ Server Side Includes
  - Health and Diagnostics
    - ☑ HTTP Logging
    - □ Logging Tools
    - ☑ Request Monitor
    - □ Tracing

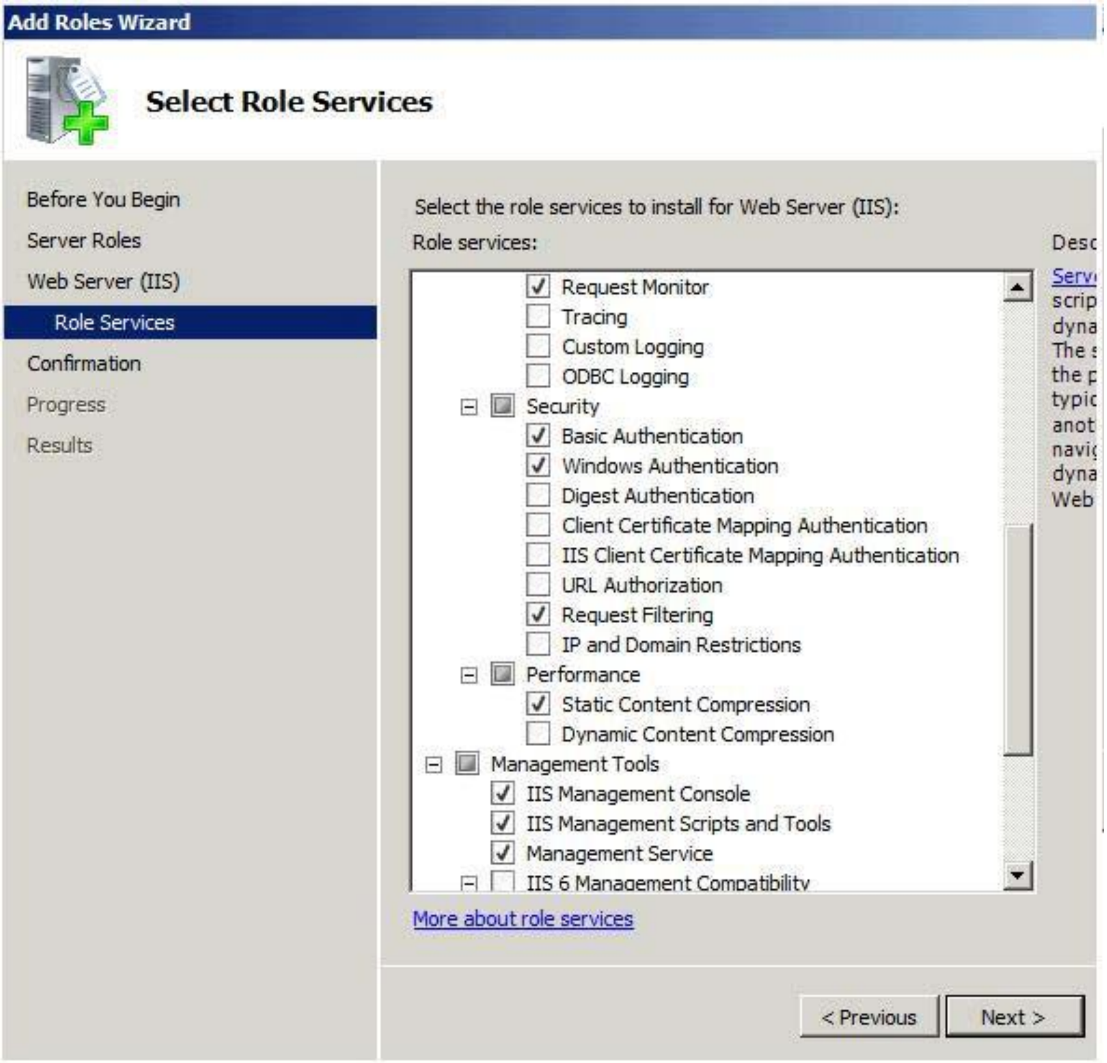


Select Role Services

Select the role services to install for Web Server (IIS):

Role services:

- ☑ Request Monitor
- □ Tracing
- □ Custom Logging
- □ ODBC Logging
- ⊟ ▣ Security
  - ☑ Basic Authentication
  - ☑ Windows Authentication
  - □ Digest Authentication
  - □ Client Certificate Mapping Authentication
  - □ IIS Client Certificate Mapping Authentication
  - □ URL Authorization
  - ☑ Request Filtering
  - □ IP and Domain Restrictions
- ⊟ ▣ Performance
  - ☑ Static Content Compression
  - □ Dynamic Content Compression
- ⊟ ▣ Management Tools
  - ☑ IIS Management Console
  - ☑ IIS Management Scripts and Tools
  - ☑ Management Service
  - ⊟ □ IIS 6 Management Compatibility



Add Roles Wizard

Select Role Services

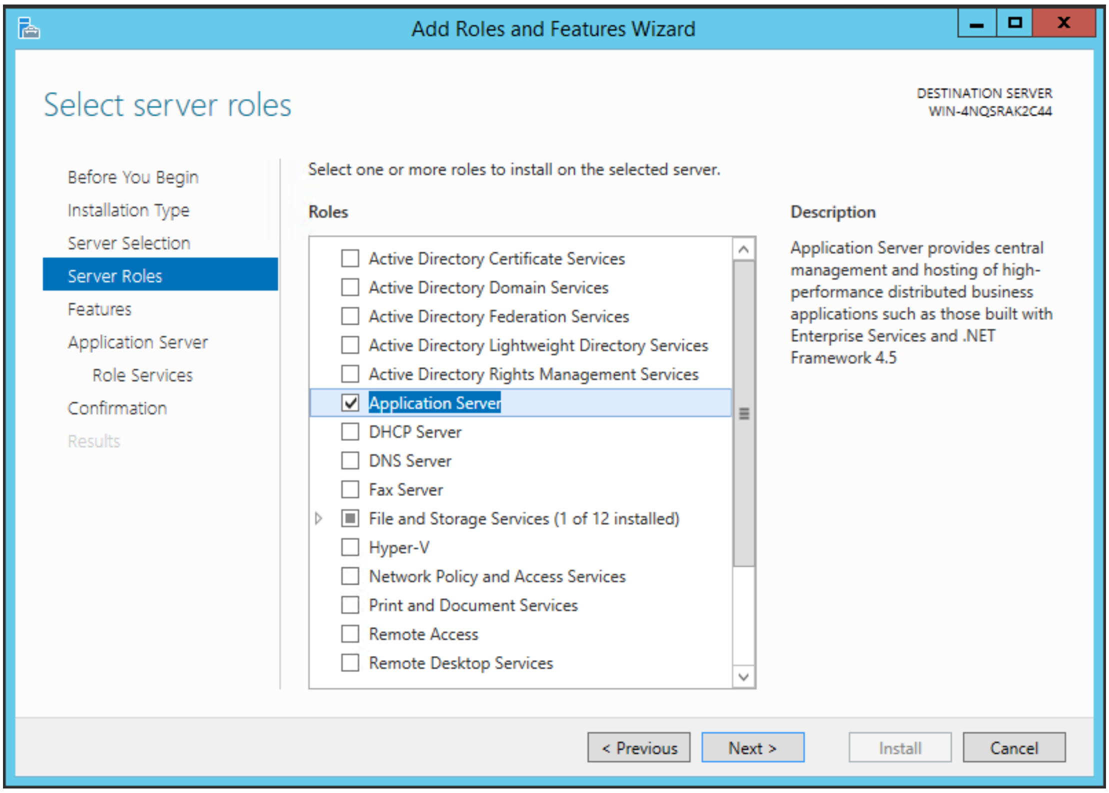
Select the role services to install for Web Server (IIS):

Role services:

- ☑ Request Monitor
- □ Tracing
- □ Custom Logging
- □ ODBC Logging
- ⊟ ▣ Security
  - ☑ Basic Authentication
  - ☑ Windows Authentication
  - □ Digest Authentication
  - □ Client Certificate Mapping Authentication
  - □ IIS Client Certificate Mapping Authentication
  - □ URL Authorization
  - ☑ Request Filtering
  - □ IP and Domain Restrictions
- ⊟ ▣ Performance
  - ☑ Static Content Compression
  - □ Dynamic Content Compression
- ⊟ ▣ Management Tools
  - ☑ IIS Management Console
  - ☑ IIS Management Scripts and Tools
  - ☑ Management Service
  - ⊟ □ IIS 6 Management Compatibility

Desc
Serv
scrip
dyna
The s
the p
typic
anot
navig
dyna
Web

- ***W2012 :*** *In addition, the functionalities “.Net Framework 4.5”, “ASP.NET 3.5” and “ASP.NET 4.5”*



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-4NQSRAK2C44

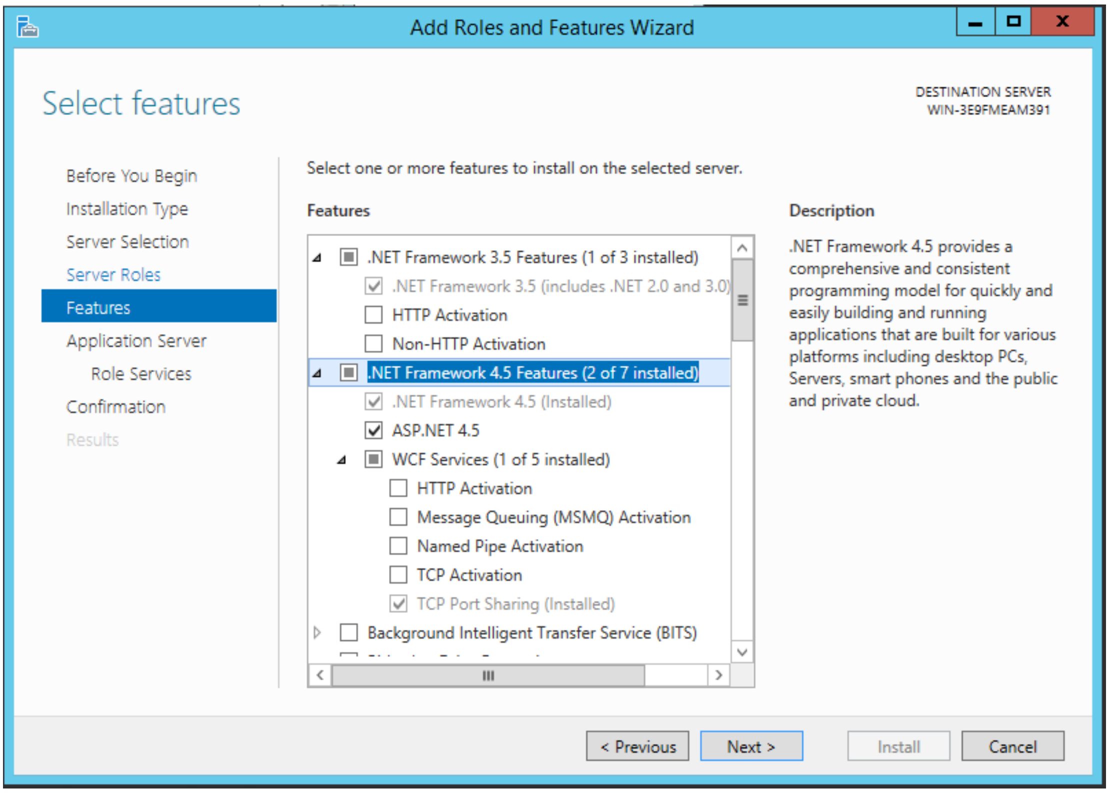
Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- ☑ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▨ File and Storage Services (1 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services

Description

Application Server provides central management and hosting of high-performance distributed business applications such as those built with Enterprise Services and .NET Framework 4.5



Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-3E9FMEAM391

Select one or more features to install on the selected server.

Features

- ▨ .NET Framework 3.5 Features (1 of 3 installed)
  - ☑ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
  - □ HTTP Activation
  - □ Non-HTTP Activation
- ▨ .NET Framework 4.5 Features (2 of 7 installed)
  - ☑ .NET Framework 4.5 (Installed)
  - ☑ ASP.NET 4.5
  - ▨ WCF Services (1 of 5 installed)
    - □ HTTP Activation
    - □ Message Queuing (MSMQ) Activation
    - □ Named Pipe Activation
    - □ TCP Activation
    - ☑ TCP Port Sharing (Installed)
- □ Background Intelligent Transfer Service (BITS)

Description

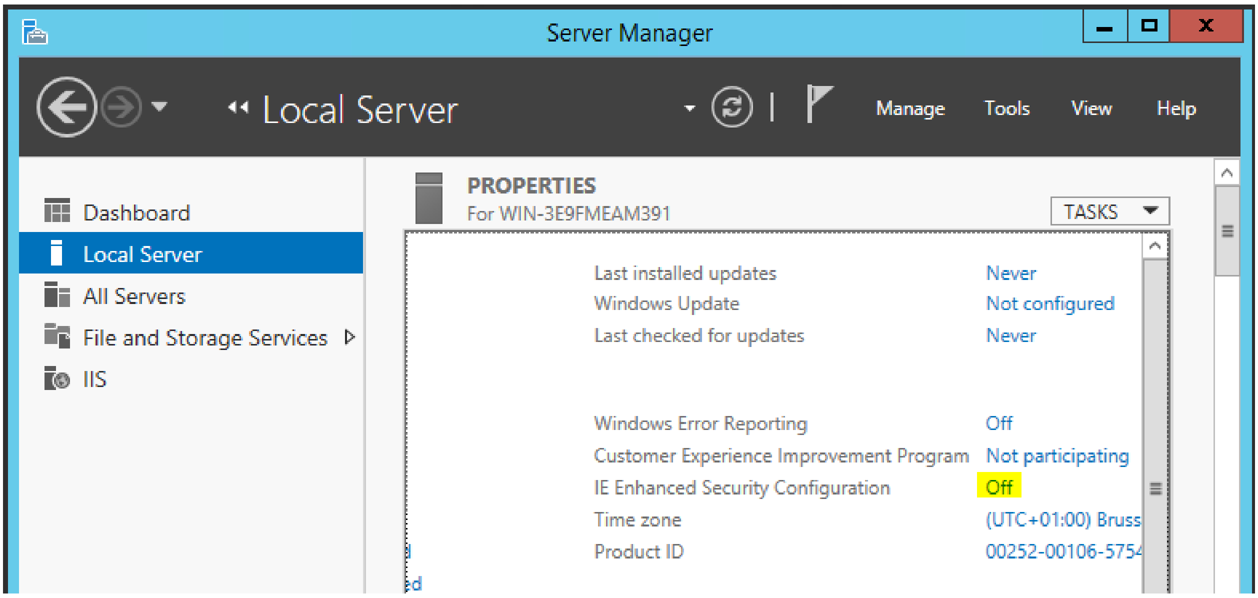
.NET Framework 4.5 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.

After selecting the roles, click on "Next", then Install and after that close the window.
IIS is installed. Restarting the server will be necessary.

11.1.2. Server setting: Internet Explorer Enhanced Security and Firewall

To complete this installation:

- Disable the "Internet Explorer Enhanced Security" via the Server Manager. For example on a server W2012:



Last installed updates: Never
Windows Update: Not configured
Last checked for updates: Never

Windows Error Reporting: Off
Customer Experience Improvement Program: Not participating
IE Enhanced Security Configuration: Off
Time zone: (UTC+01:00) Bruss
Product ID: 00252-00106-5754

- Disable the firewall if possible or manage connections to the server in accordance with the prerequisites.