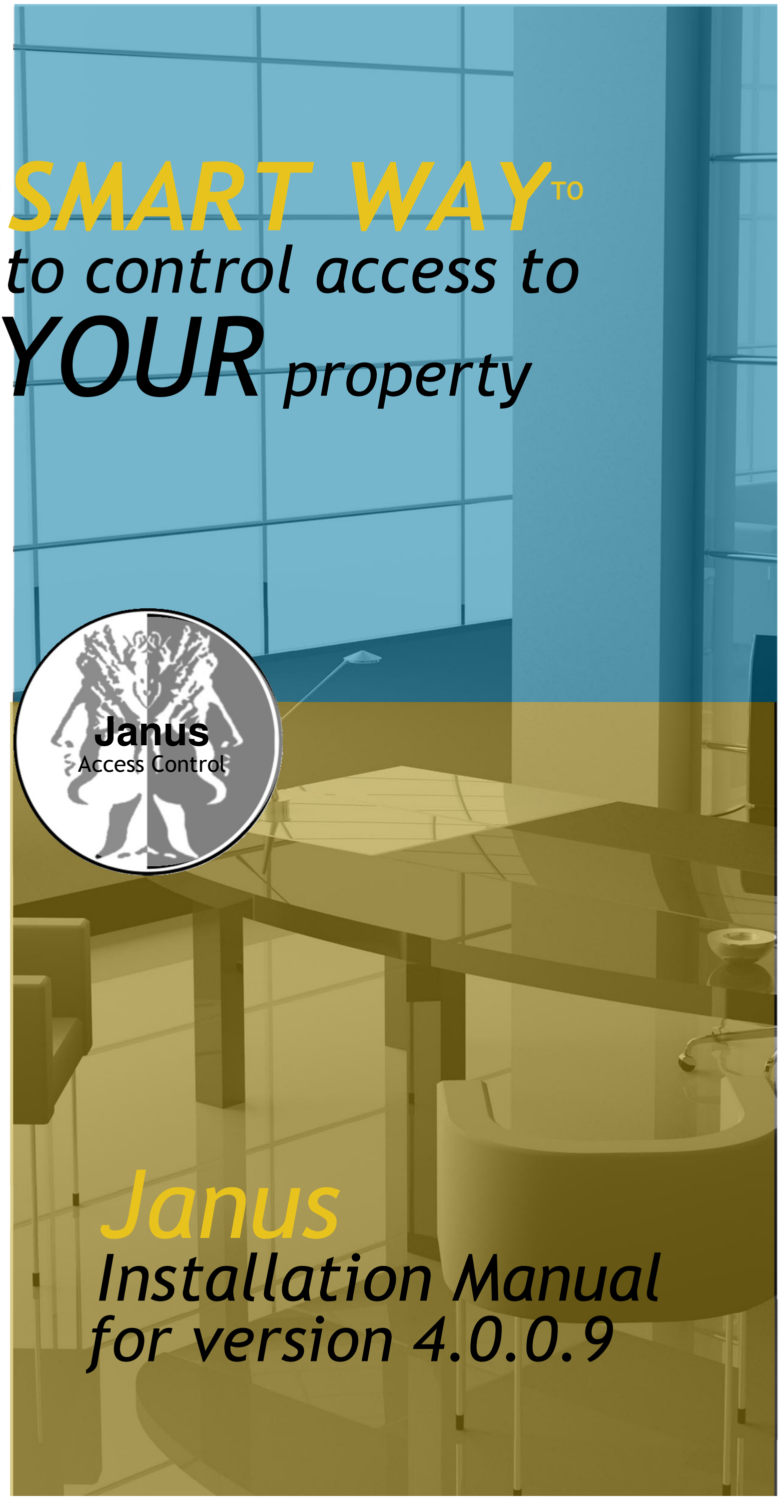


THE + SMART WAY TO

to control access to

YOUR property

Janus

Access Control

# Janus

## Installation Manual for version 4.0.0.9

# Janus Installation Manual

## Overview

This is the installation manual for the Janus 4 system. The user manual is a separate document.

## Versions

Available version are listed in the Janus brochure or the Janus user manual. Please ensure you purchased the desired version before installation.

## System Requirements

See the Janus brochure or the Janus user manual for system requirements. Ensure the required networking, computing and scanner equipment are ready before starting to install.

## Versioning

Document: v 4.0.0.9 dated 5 Nov 2014.

## Known issues

Some ADO interfaces were changed in Windows 7 SP1 to be associated with new instance identifiers. This means Windows XP, Windows Server 2007 and other operating systems before Windows 7 SP1 can cause the software installation to fail, and the Janus software may also not run on these operating systems. See http://support.microsoft.com/kb/2517589 and http://support.microsoft.com/kb/2640696.

## Requirements

Before installing, ensure you have the following:

- Computer on which Janus is to be installed, with Winfows 7 SP1 or Windows 8 installed.
- Wifi access point and its installation software.
- eSkan devices, USB cable supplied with the device. Scanner driver software.
- [Janus Standard/Professional] Microsoft SQL Server Express 2012 (or the full licensed version).
- The Janus software and its activation key.

## Janus Client Software: installation guide

Installation comprises the sequence of steps below. Depending on your hardware and software requirements, some of these steps can be skipped, as indicated on the following pages.

## Installing required third-party hardware and software

### Install and configure the wifi router on your network

A wifi router is required if you purchased eSkan 250 scanners for wireless download.

1. Plug in the wifi router on the network, and follow the instructions provided with your device to configure it as a wifi access point. See the annexures to this document for setup instructions for certain wifi products.

Annexure 3: Network setup and configuration of Ubiquity Picostation M2

2. Configure the computer where Janus is to be installed with a static IP address. This is set in Control Panel, Network Options.

For a stand-alone PC (Janus Lite or Standard installations), you can typically set the PC to:

IP address of PC: 192.168.1.100, Subnet Mask: 255,255,255,0     [i.e. a static IP address]

Default Gateway: left blank if only a single PC connected to wifi

Preferred DNS Server: Left blank if only a single PC connected to wifi.

> This manual describes install based on a static IP.
>
> If you have a DNS server on a larger network, consult the advice of your network administrator to configure the DNS server. The PC/server where the scans are delivered as well as each scanner however still require fixed IP addresses.

### Install the Excellent ID eSkan driver software

1. The ExcellentID installation manual is included with the scanners and/or with the Janus installation software. Follow that manual to setup the driver software for the scanners and to open the Windows firewall as required. Note that with Windows 8 additional procedures are required to restart Windows in a special mode for the USB setup – make sure to read the provided additional instructions.

2. Make sure the Windows firewall was configured as per the ExcellentID installation manual. See the section “Windows firewall setup” in the ExcellentID manual. It boils down to access for the eSkan.Service program on the local PC, or open access to TCP/IP port 7509 on a networked firewall.

3. After successfully installing, open the Decoder Software in administrator mode and set the following:

* Check the mark “Decoder runs on this PC”.

* Make sure the Directory type is set to “Single directory”.

* Change the Root Directory to “c:\scannerdata”

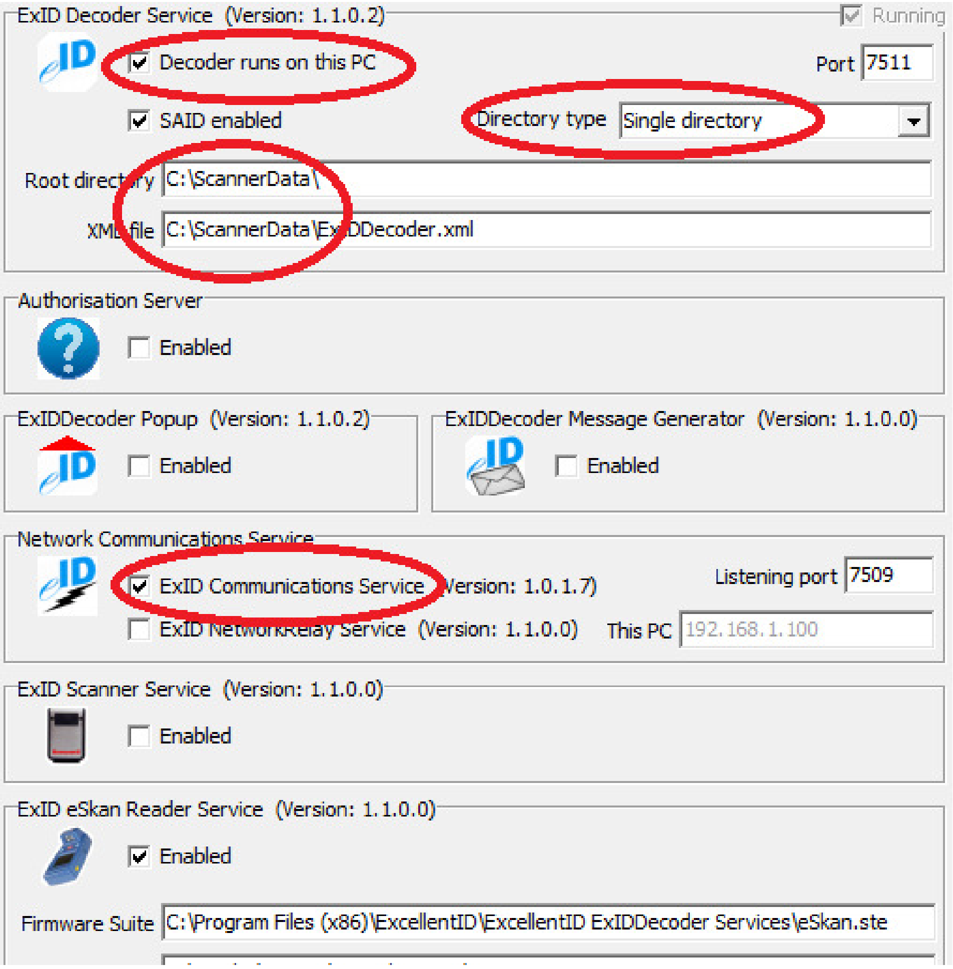
* Change the “XML File” path to “c:\scannerdata\ExIDDecoder.xml”

* Set the “User Directory” path to “c:\scannerdata\Firmware\”

* Make sure the ExID Communications Service is checked.

* Enable the ExID eSkan Reader service.

The Authorisation Service and NetworkRelay service should be left disabled.



ExID Decoder Service (Version: 1.1.0.2) ☑ Running

☑ Decoder runs on this PC Port 7511

☑ SAID enabled Directory type Single directory

Root directory C:\ScannerData\

XML file C:\ScannerData\ExIDDecoder.xml

Authorisation Server

☐ Enabled

ExIDDecoder Popup (Version: 1.1.0.2)

☐ Enabled

ExIDDecoder Message Generator (Version: 1.1.0.0)

☐ Enabled

Network Communications Service

☑ ExID Communications Service (Version: 1.0.1.7) Listening port 7509

☐ ExID NetworkRelay Service (Version: 1.1.0.0) This PC 192.168.1.100

ExID Scanner Service (Version: 1.1.0.0)

☐ Enabled

ExID eSkan Reader Service (Version: 1.1.0.0)

☑ Enabled

Firmware Suite C:\Program Files (x86)\ExcellentID\ExcellentID ExIDDecoder Services\eSkan.ste

3. Plug in the scanner on USB, and do a few barcode scans or license scans. Check that after each scan a couple of files are added in c:\scannerdata. Do not bother at this stage if the sequence in which the scanners ask for driver or vehicle scans are not suited to your situation. The test at this stage is to ensure USB based communication between the scanner and the computer is fine. Possible issues at this stage may be related to USB driver issues, or more likely that the above-mentioned path was not set.

4. Configure the scanner for wifi access as per the ExcellentID manual. Disconnect the scanner from the USB cable, and test that any scanned files now transmit via wifi and end up in c:\scannerdata. The test at this stage is to ensure the wifi communication between the scanner and the computer is fine. The final scanner setup described in the main section in this document "Programming the scanner". Then the scanners will also be programmed and configured for use with Janus. Possible issues at this stage:

   - the above-mentioned path was not set.

   - wifi is switched off or is improperly configured.

   - the scanner was not properly configured for wifi. Follow the ExcellentID troubleshooting instructions. In the bottom middle of the scanner screen shows a dot, that changes to a colon (:) when the wifi access point is detected. It shows a three-pointed antenna icon when it connected, and if there are any scans to be transmitted, the scanner icon should turn to a lightning bolt, and the files should transmit.

- If the colon and/or antenna icon does not show, the scanner is probably not yet properly configured for wifi access. See the section “Configure the eSkan” in the ExcellentID installation manual. It may also be that the scanner fails to authenticate access to the wifi access point. In this case inspect the scanner wifi configuration and re-do it. Check the wifi access point is connected and switched on.

- If the lightning icon does not show, but the antenna icon shows, look for issues related to the Windows firewall blocking access to ExcellentID (See Annexure 1 as well as the section “Windows firewall setup” in the ExcellentID installation manual). In the ExcellentID Decoder Setup program, make sure the ExID Communications Service is checked, as illustrated in Paragraph 2 above.

5. Delete all test scan files from c:\scannerdata directory as they are still formatted incompatibly with Janus. The section in the install manual “Programming the scanner” describes configuring it for Janus.

## Install the database software

Users of Janus Lite can skip database installation instructions and proceed to installing the Janus software.

Instructions below are for installing SQL Server Express 2012 for Janus Standard or Janus Professional. Large clients who have a paid full licensed Microsoft SQL Server, should consult with their database administrator about possibly using that instead of SQL Express.

1. Run the installer for SQL Server Express 2012 (or the full SQL Server, if you prefer).

   You do not need to check SQL Server Replication and LocalDB in the Features box.

   Make sure you enable Mixed mode authentication.

   Annexure 2 gives a step-by-step outline of the SQL Server Express installation with specific notes to be aware of for Janus.

2. After installing SQL Server, start the SQL Server Configuration Manager and enable Named Pipes and TCP/IP. This is described in Annexure 2 of this document, and in Microsoft's own documentation.

3. For Janus Professional, you may need to set SQL Server for allowing networked connections on SQL Server. Microsoft suggests two options, one with the SQL Browser enabled, and one with the browser disabled, depending on your security preferences. The browser version is shown in Annexure 2.

4. Make a note of the 'sa' user's password you used during install, as you will need this for Janus install.

## Install the Janus software

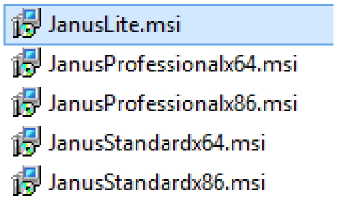
1. Run the Janus software installer.

Separate installers are provided for:

* Janus Lite

* Janus Standard

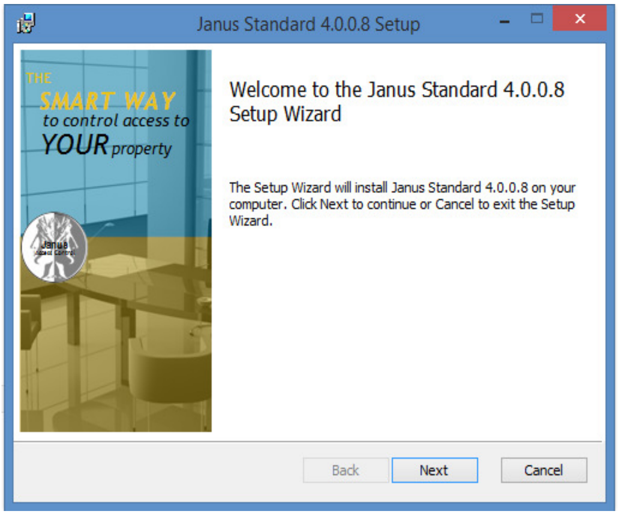
* Janus Professional.



JanusLite.msi
JanusProfessionalx64.msi
JanusProfessionalx86.msi
JanusStandardx64.msi
JanusStandardx86.msi

Janus Lite installs as 32-bit only. For Janus Standard and Janus Professional, the 64 bit installers should be used for fest performance. The 32-bit installers for Standard and Professional are provided as backup only as most Windows 7 and Windows 8 machines now are fully 64 bit compatible.

Activate the desired installation software for your product.

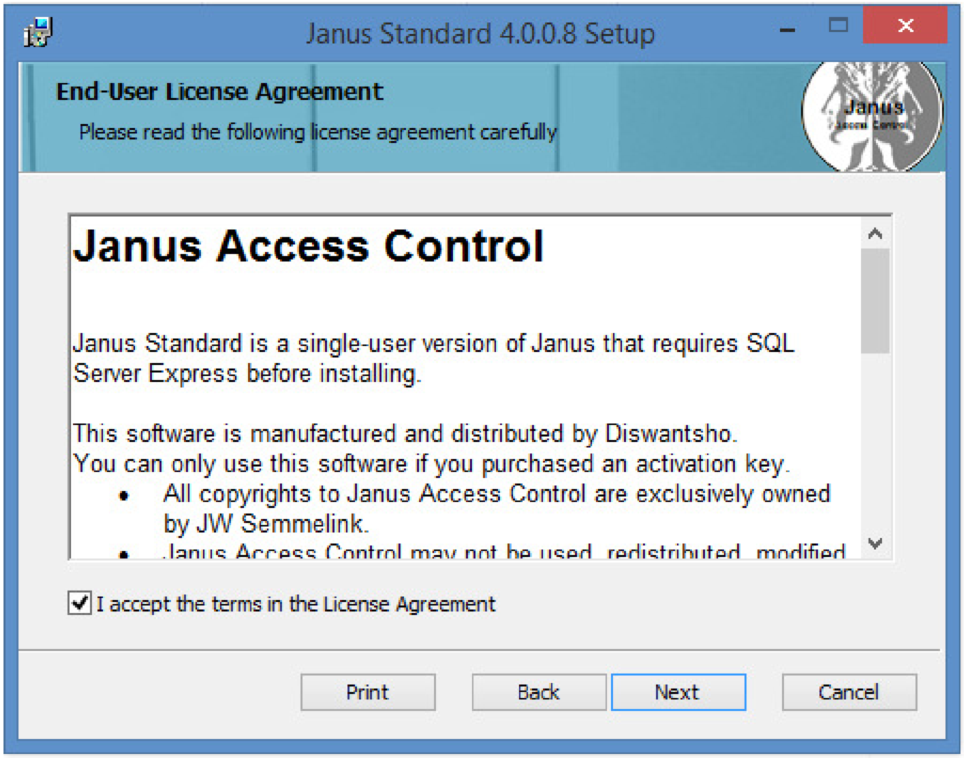


Janus Standard 4.0.0.8 Setup

Welcome to the Janus Standard 4.0.0.8 Setup Wizard

The Setup Wizard will install Janus Standard 4.0.0.8 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

2. Check the box to accept the license agreement.



Janus Standard 4.0.0.8 Setup

**End-User License Agreement**

Please read the following license agreement carefully

Janus Access Control

Janus Standard is a single-user version of Janus that requires SQL Server Express before installing.

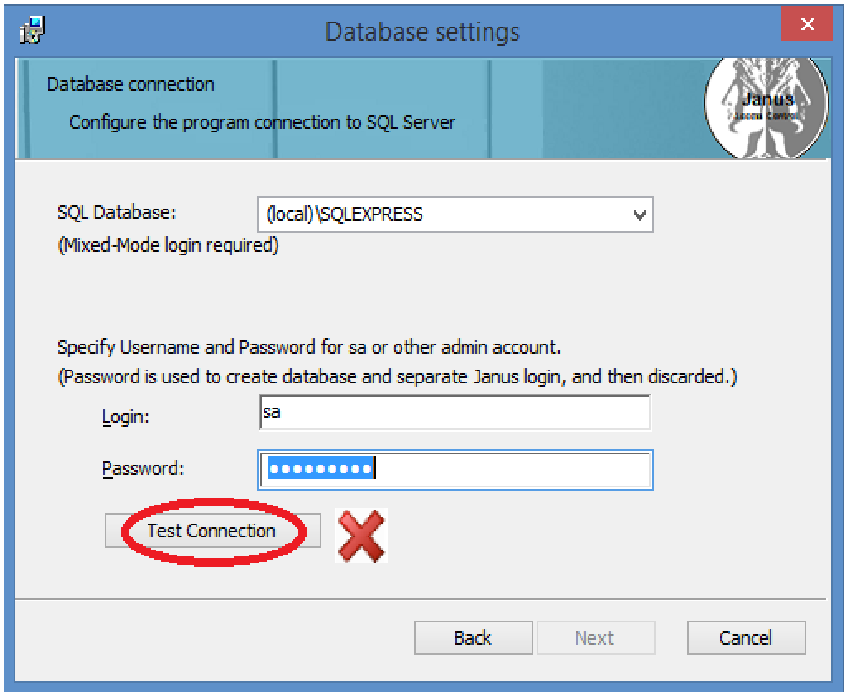
This software is manufactured and distributed by Diswantsho.
You can only use this software if you purchased an activation key.

- All copyrights to Janus Access Control are exclusively owned by JW Semmelink.
- Janus Access Control may not be used, redistributed, modified

☑ I accept the terms in the License Agreement

3. Janus Standard and Janus Professional require access to the local SQL Server instance.

Choose from the drop down list the instance to which access is required. Provide the login details and click to test the connection.



Database settings

Database connection

Configure the program connection to SQL Server

SQL Database: (local)\SQLEXPRESS

(Mixed-Mode login required)

Specify Username and Password for sa or other admin account.

(Password is used to create database and separate Janus login, and then discarded.)

Login: sa

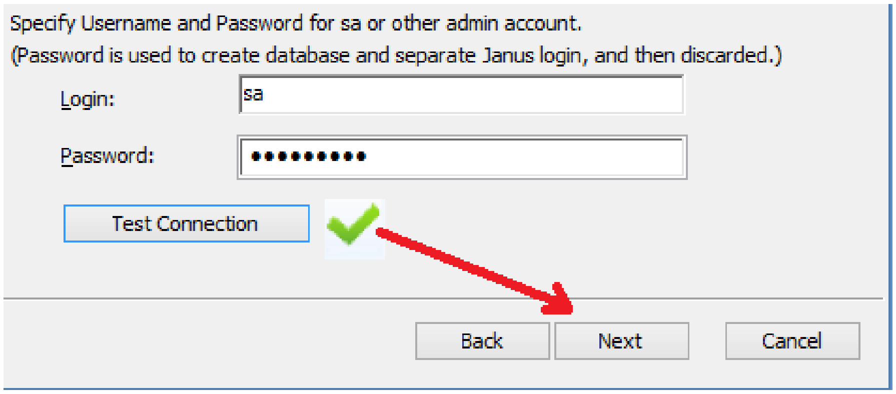
Password: ●●●●●●●●●

If the connection succeeds, the red cross will be replaced with a green check and the "NEXT" button will enable for you to proceed.

For Janus Professional client software you should specify the server's instance name where the Janus database is located. If you connect to SQL Server Express, the typical SQL instance name is "<my computer's name>\SQLEXPRESS", e.g. "SHAKESPEARE\SQLEXPRESS" if your machine name is "SHAKESPEARE". Remote clients must specify the server's name to connect to.

| Full SQL Server<br>Default Instance | Full SQL Server Named Instance OR<br>SQL Server EXPRESS | Comments |
|---|---|---|
| SHAKESPEARE | SHAKESPEARE\SQLEXPRESS<br>SHAKESPEARE\SQL2K8R2 | Works for connections either on local machine, or from a remote machine. (Recommended for Janus Standard and Janus Professional) |
| (LOCAL) | (LOCAL)\SQLEXPRESS<br>(LOCAL)\MYNAMEDINSTANCE | local only, Suitable for Janus Standard. |
| . | .\SQLEXPRESS<br>.\MYNAMEDINSTANCE | local only |
| LOCALHOST | LOCALHOST\SQLEXPRESS<br>LOCALHOST\MYNAMEDINSTANCE | local only |

The installer requires administrator authorisation for creating the Janus database, and to create a new login for Janus 4. Thereafter Janus will login using the new Janus user. The 'sa' user credentials are not stored by the installer or used in any way after installation.



Specify Username and Password for sa or other admin account.
(Password is used to create database and separate Janus login, and then discarded.)

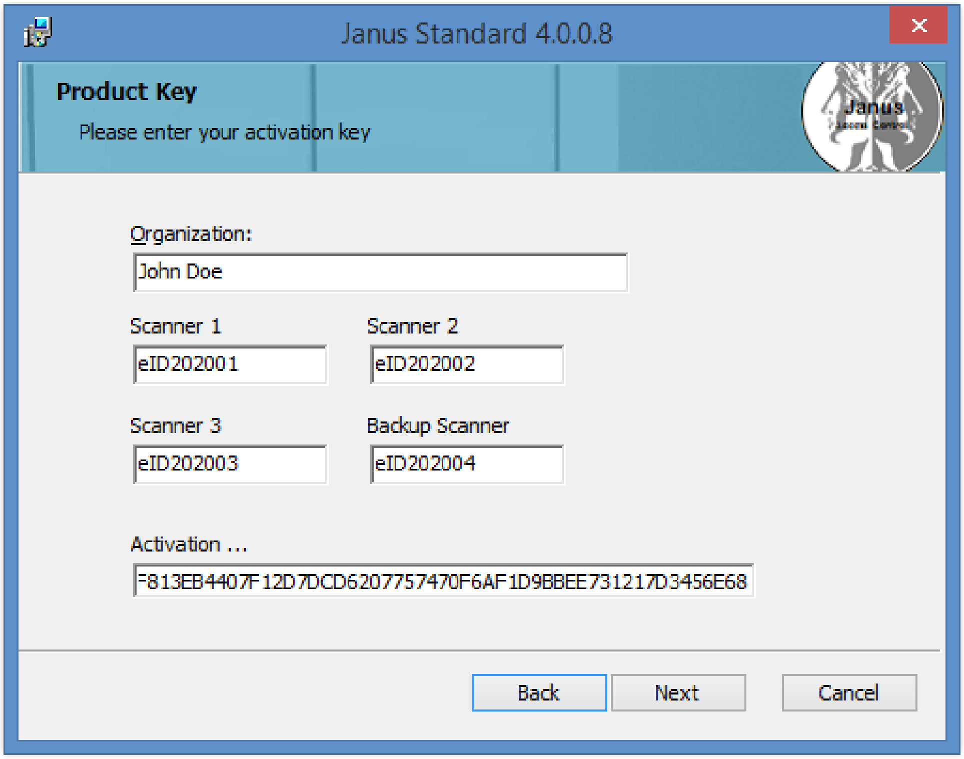
Login: sa

Password: ●●●●●●●●●●

Once the connection passes testing, the NEXT button enables and you can proceed.

The installer was not tested creating a database on a remote server. If you wish to do that, manually create an empty database “Janus4” on the remote server. Then finish installing on the local machine (creating a local database). Afterwards edit the connection string in the Janus config file to connect to the remote machine. If the connection succeeds, Janus will start and the local database can safely be dropped.

4. Enter the name in which your license was issued, the list of scanners to be used in the software and the software activation key.



Janus Standard 4.0.0.8

Product Key

Please enter your activation key

Organization: John Doe

Scanner 1: eID202001

Scanner 2: eID202002

Scanner 3: eID202003

Backup Scanner: eID202004

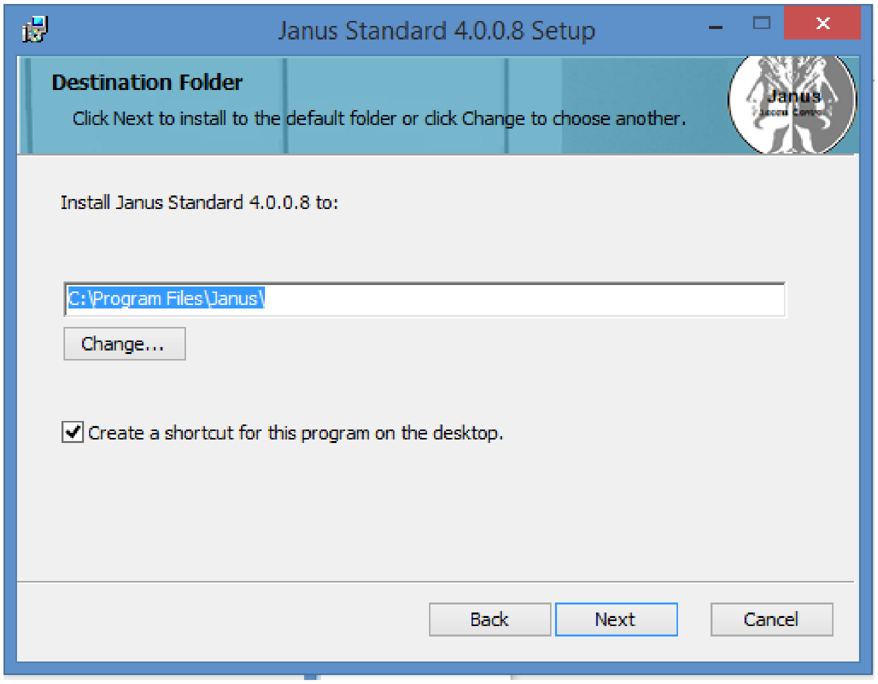
Activation ...: F813EB4407F12D7DCD6207757470F6AF1D9BBEE731217D3456E68

Please obtain a valid license before installing, because the installer software checks the license before allowing the install to continue.

If the details are not filled in automatically from the accompanied license file, then open the license with Notepad and copy and paste into the installer. Any spelling differences (or upper/lower case) in the organisation name or the scanners can invalidate the activation key.

5. You can usually accept the default path where Janus will be installed. Janus Standard and Janus Professional are usually installed as 64-bit applications and install in c:\Program Files.

Janus Lite is a 32-bit application and installs in the 32-bit folder c:\Program Files (x86).



Destination Folder

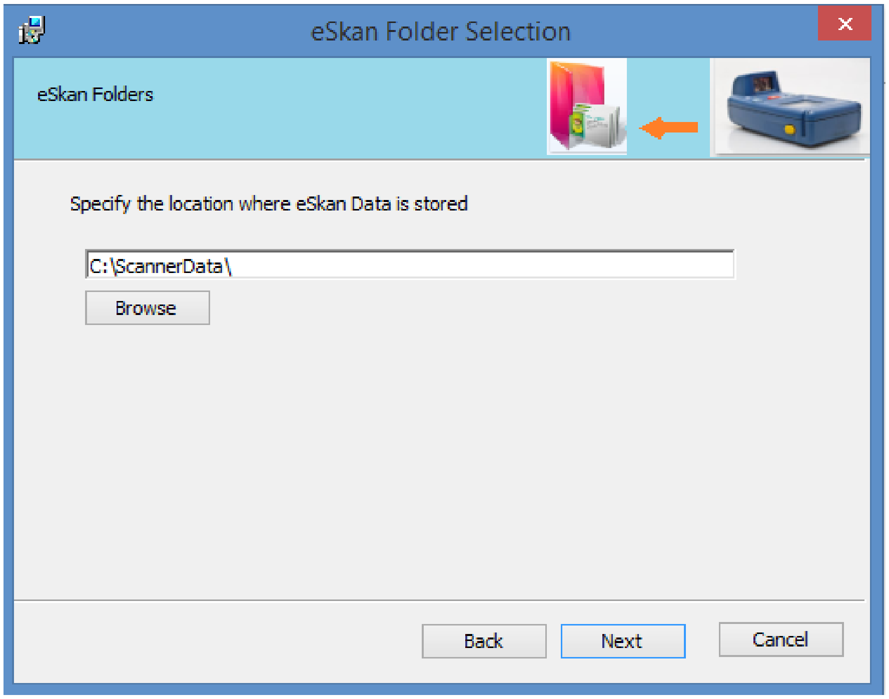
Click Next to install to the default folder or click Change to choose another.

Install Janus Standard 4.0.0.8 to:

C:\Program Files\Janus\

☑ Create a shortcut for this program on the desktop.

6. You can usually accept the default path where this software gets the scanner files. You will recognise this is the same path that was set up in the ExIDDecoder tool. The path must be the same both in ExID and in Janus. By default the path is c:\scannerdata.

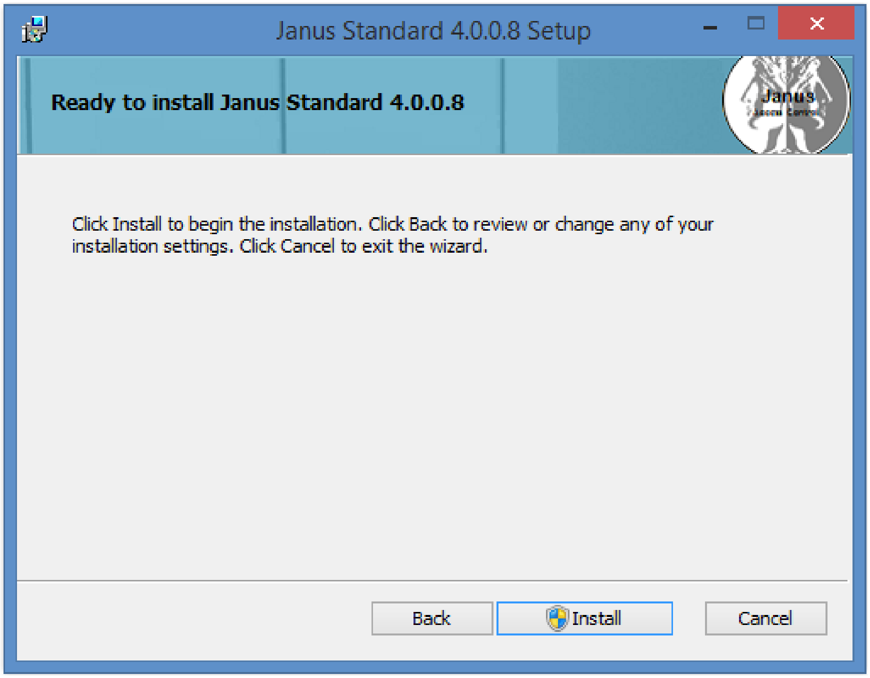


eSkan Folders

Specify the location where eSkan Data is stored

C:\ScannerData\

7. Now you have a last chance to go back and review settings, or to click Next and proceed with the installation.



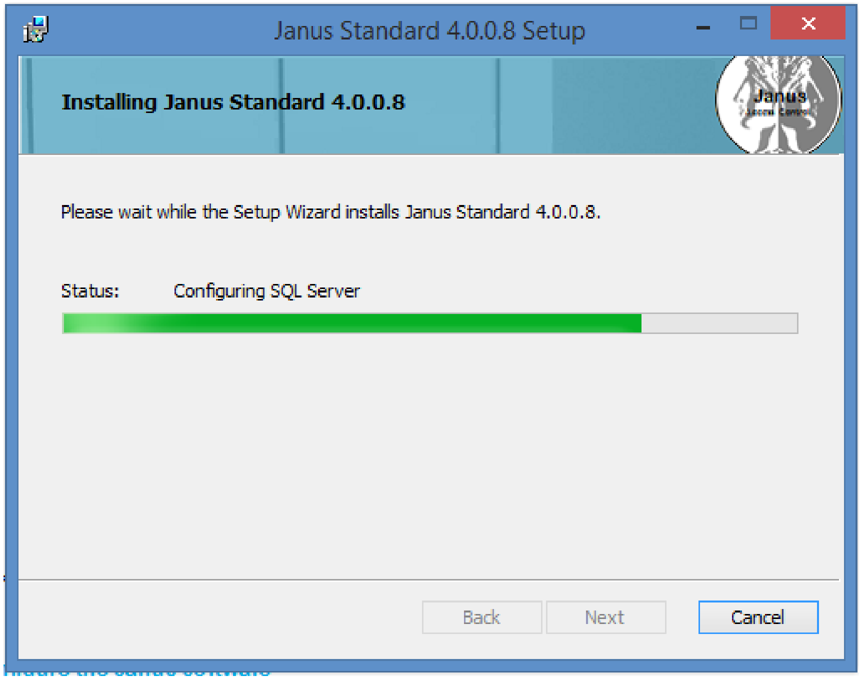
Janus Standard 4.0.0.8 Setup

**Ready to install Janus Standard 4.0.0.8**

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

8. Click “Install” to proceed with the installation.

As illustrated below, the Janus standard and the Janus professional also login to SQL Server during install to create a database and user login credentials for the Janus user. If a failure occurs at this moment, it is usually due to SQL Server not authorizing the user that was provided.



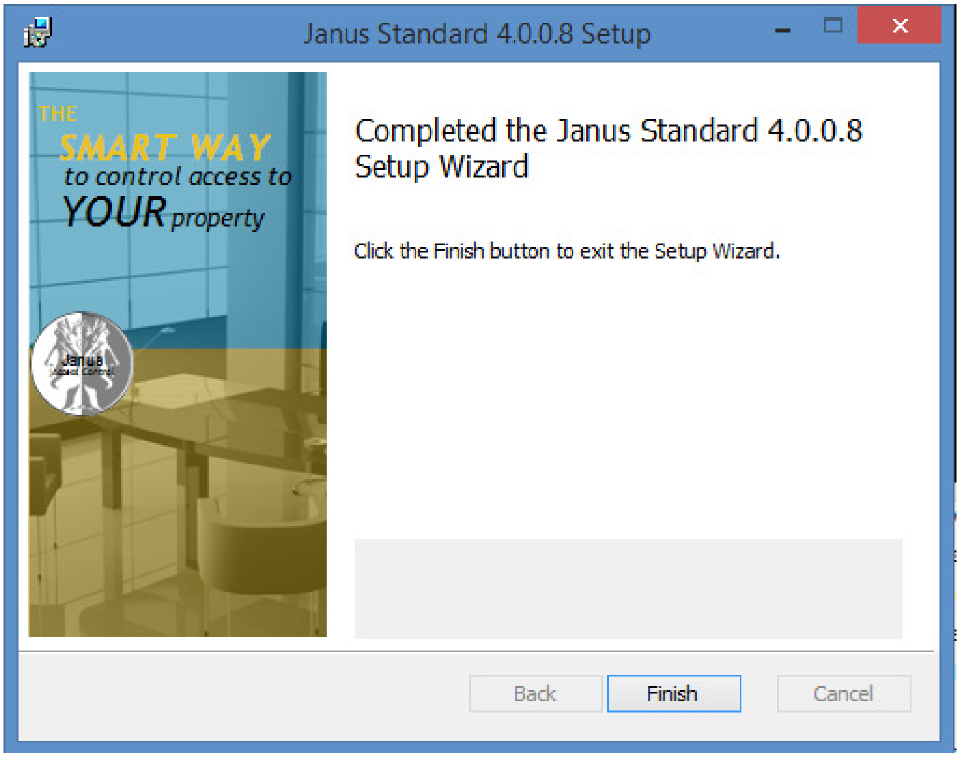
Janus Standard 4.0.0.8 Setup

**Installing Janus Standard 4.0.0.8**

Please wait while the Setup Wizard installs Janus Standard 4.0.0.8.

Status: Configuring SQL Server

9. Once the installation is complete, you can click “Finish” to close the installer.



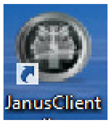
Completed the Janus Standard 4.0.0.8 Setup Wizard

Click the Finish button to exit the Setup Wizard.

After installing the Janus software, it is necessary to configure the system according to your preferences, Thereafter, some of those preferences will be applied to configuring the scanner for your particular needs. Below, configuring the system is firstly described, and thereafter the scanner configuration.

## Configure the Janus software

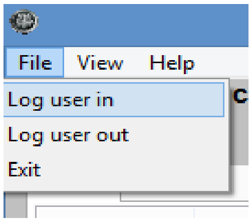
1. Run the Janus client. An icon is available on the Windows desktop to start Janus.



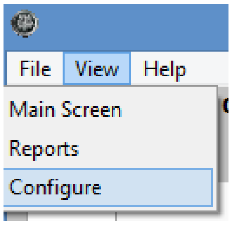
On first start, the Janus software will create the tables in the database.

2. **Configure Janus.**

You must be logged in as admin user to be able to configure Janus. Use the userid and password that were provided to you with your user license.

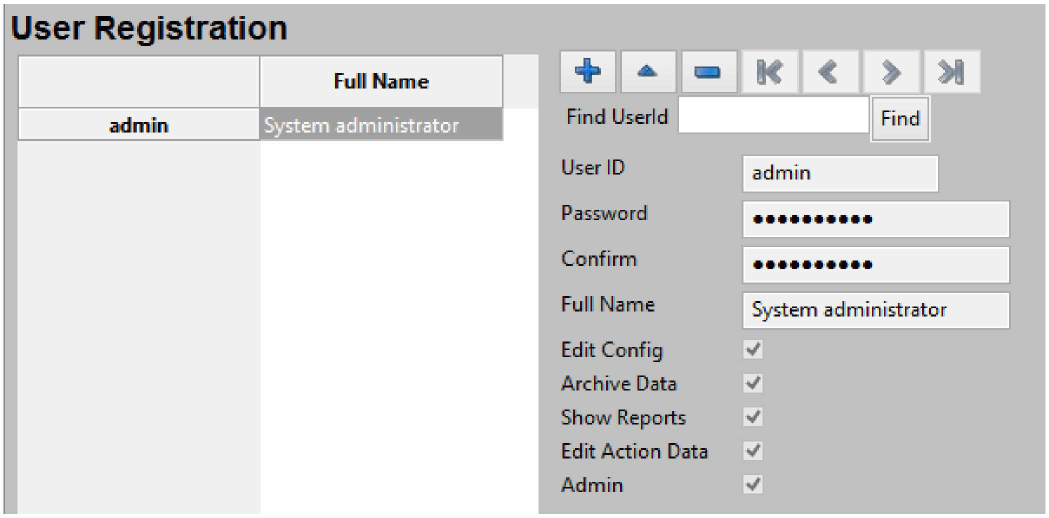


Open the Configure screen



## Capture users who may log in and provide restrictions on their use of the system.

(Janus Config screen, Users option)



User Registration

| | Full Name |
|---|---|
| admin | System administrator |

User ID: admin

Password: ●●●●●●●●●●

Confirm: ●●●●●●●●●●

Full Name: System administrator

Edit Config ✓

Archive Data ✓

Show Reports ✓

Edit Action Data ✓

Admin ✓

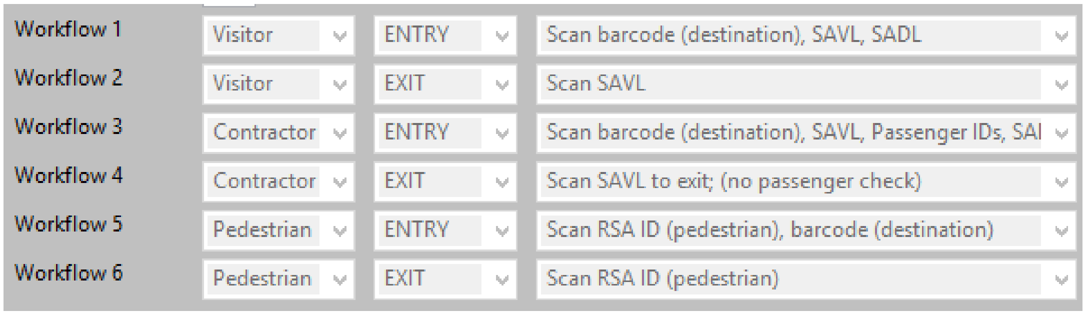
Make sure that the administrator password is reserved only for one person in charge. Give each guard (or all the guards as a group) their own user and password to the system.

You can also opt to give the guards no rights, so they cannot log in to special functions, and only the main screen will be accessible to them.

## Create a scanner config file (Janus Config screen, Scanners Option)

Depending on your needs, the scanners can be configured in several ways. The screen allows you to configure the scanners for up to 6 workflows. The guards will be able to select different workflows using the red scroll button on the scanner. For each workflow, the scanner will go through a sequence of steps to scan or otherwise obtain required input.

Initially to get everyone used to the system, you may wish to program scanners for “Visitors” only, and later as the guards, visitors and residents get better acquainted to the new process, you can re-program the scanners for more elaborate processes.



| | | | |
|---|---|---|---|
| Workflow 1 | Visitor | ENTRY | Scan barcode (destination), SAVL, SADL |
| Workflow 2 | Visitor | EXIT | Scan SAVL |
| Workflow 3 | Contractor | ENTRY | Scan barcode (destination), SAVL, Passenger IDs, SAI |
| Workflow 4 | Contractor | EXIT | Scan SAVL to exit; (no passenger check) |
| Workflow 5 | Pedestrian | ENTRY | Scan RSA ID (pedestrian), barcode (destination) |
| Workflow 6 | Pedestrian | EXIT | Scan RSA ID (pedestrian) |

You can set the “Workflow” to  Visitor, Contractor, Pedestrian, or Resident.  You can also change the names of these “Workflows” to your needs, e.g. “personnel” instead of “residents” (if you run a business) or “guests” for “visitors” (e.g. if you set this up for a hotel).

- Visitor – processes related to visitors or guests arriving with vehicles.
- Contractor – similar to visitor, except that you can optionally configure the scanners to scan RSA ID barcodes for all passengers on entry (requires also scanning them on exit).
- Pedestrians – RSA ID/personnel card is scanned instead of vehicle disk or driver license.
- Residents – Process that saves time by scanning barcode (e.g. from a personnel card) on entry and exit instead of vehicle license and driver license. Also no destination is captured as these persons should be well known.

For every visitor, contractor or pedestrian workflow, you must set an ENTRY and an EXIT scan sequence.

The last items in each row select the process to follow for scanning; i.e. the sequence of steps that the scanner will prompt the guard to follow. Select the option that corresponds to your requirements.

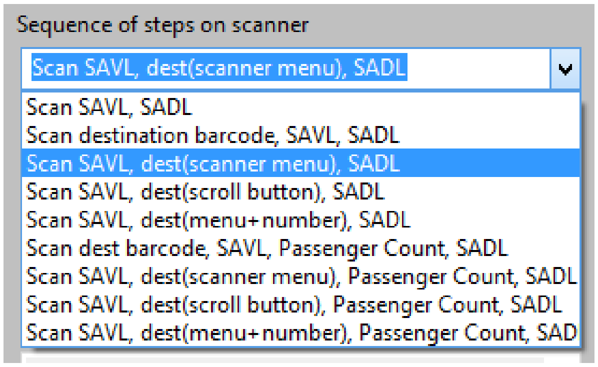
* SAVL: Scanner will ask guard to scan a vehicle license disk.

* SADL: Scanner will ask guard to scan driver license

* Destination can be captured in one of the following ways:

- scan barcode – print and laminate barcodes for each place. Guard then scans the barcode.

- scanner menu – You load up to 15 place names to show on a menu in the scanner. (see bottom of screen).



Sequence of steps on scanner

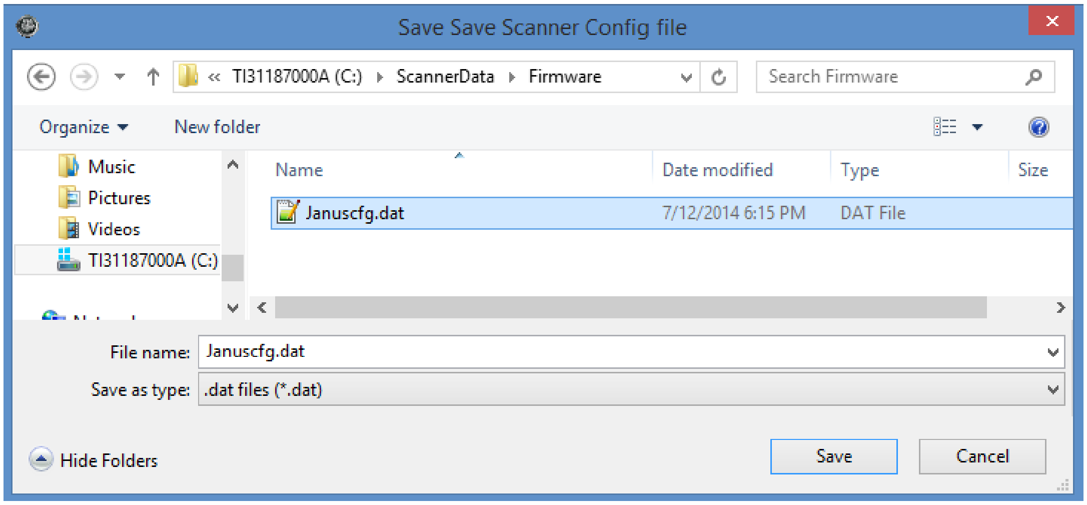
Scan SAVL, dest(scanner menu), SADL

Scan SAVL, SADL
Scan destination barcode, SAVL, SADL
Scan SAVL, dest(scanner menu), SADL
Scan SAVL, dest(scroll button), SADL
Scan SAVL, dest(menu+number), SADL
Scan dest barcode, SAVL, Passenger Count, SADL
Scan SAVL, dest(scanner menu), Passenger Count, SADL
Scan SAVL, dest(scroll button), Passenger Count, SADL
Scan SAVL, dest(menu+number), Passenger Count, SAD

- scroll button – guard enters erf number by scrolling digits with the scanner keys.

- menu + number – use the 15 spaces at the bottom of the screen to define a scanner menu for up to 15 street names. Guard selects street, then toggles house number with the scanner keys.

Once you finished setting up the scanner, click the button to create a scanner config file. Save and replace file c:\scannerdata\firmware\<scanner no>\scannerconfig.dat, where <scanner no> in the path is a directory with the same name as the scanner serial number. Each scanner gets its own config file. This button is disabled while you are still editing the data. Click the button with the check mark to commit changes, then create the config file.



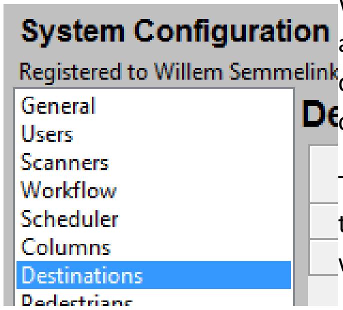
| Name | Date modified | Type | Size |
|---|---|---|---|
| Januscfg.dat | 7/12/2014 6:15 PM | DAT File | |

File name: Januscfg.dat

Save as type: .dat files (*.dat)

This configuration file must be loaded on the specific scanner for which it was prepared in Janus. See the next main section in this document "Programming the scanner" for this part.

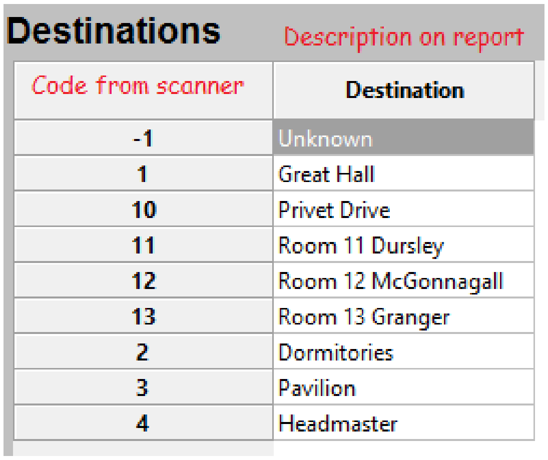
### *Options for capturing the destination (where visitors are going) on the scanner*:



When you select the scanner workflow sequence (see above), you will be able to select one of several options how the scanner records the destination where the visitor is going. These destinations also have to be captured in the Janus system.

The scanner sends a number to the system, and you use this screen to pair that number with the description of the destination. This description is what will appear on reports and on the Janus main screen.

In the destinations screen, match each code that can be sent from the scanner to the description you wish to be shown on reports or on the Janus screen when such a destination was provided:

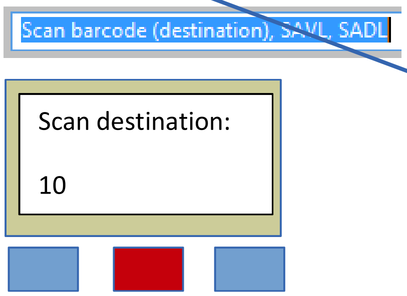


| Code from scanner | Destination |
|---|---|
| -1 | Unknown |
| 1 | Great Hall |
| 10 | Privet Drive |
| 11 | Room 11 Dursley |
| 12 | Room 12 McGonnagall |
| 13 | Room 13 Granger |
| 2 | Dormitories |
| 3 | Pavilion |
| 4 | Headmaster |

Use the Destinations screen to pair the code sent from a scanner to the description in the destinations screen as follows:

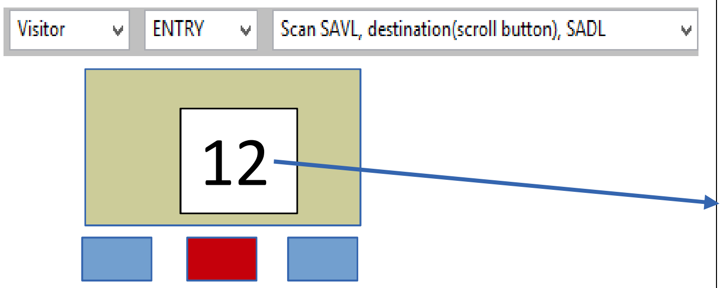
**** If you configure the scanner to get destinations from barcodes***:

Configure workflow sequences that indicate the scanner will scan destinations from a barcode. On the Janus software disk is a Microsoft Word document containing several barcodes. You can print the document, and laminate the pages for scanning barcodes. For each destination, you must also create an entry in the Janus Destinations Screen (see further below), using the same code as the barcode you selected for the destination/address.

| **Prepare a document with barcodes for the guards to scan.** | **Configure scanner** | **Configure the destination in Janus** |
|---|---|---|
| <br> 010<br>Privet Drive 4<br>Write or type the address description under each barcode so the guard can identify the code to scan. | Janus Config:<br>**Scanners screen**<br>Select sequences for Barcode destinations<br><br>Scan barcode (destination), SAVL, SADL<br>Scan destination:<br>10 | Janus Config:<br>**Destinations screen**<br>Make sure you use the ***same*** number as the barcode so Janus can match the barcode with the address description<br>Code 10="Privet Drive 4" |

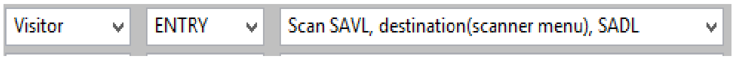
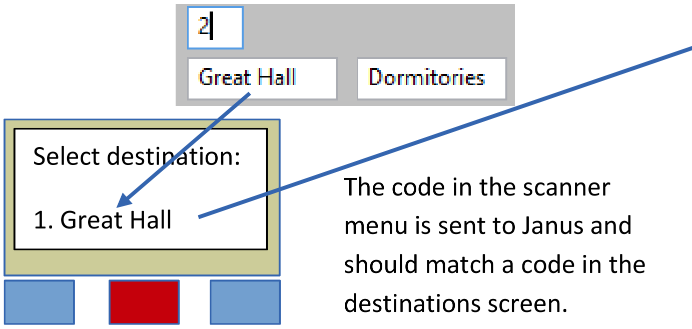
**** If you configure the scanner to get destination by scrolling red button on scanner***:

The scanner operator pushes the scanner's red button to scroll from 0...9 with the red scroll key on the scanner, and a blue key to move to the next digit (numbers up to 999 can be captured). This saves time as the guard does not need to fiddle with pages of barcodes. This also works well if the destinations are school room numbers, building numbers or stand/erf numbers.

| **Configure scanner** | **Configure the destination in Janus** |
|---|---|
| Janus Config: **Scanners screen**<br>Select sequences for entering destinations via scanner scroll key.<br><br>Visitor \| ENTRY \| Scan SAVL, destination(scroll button), SADL<br>12 | Janus Config: **Destinations screen**<br>Make sure you use the ***same*** number as the number to enter so Janus can match the number with the address description<br>Code 11="Room 11 - Dursley"<br>Code 12="Room 12 - McGonagall"<br>Code 13="Room 13 - Granger" |

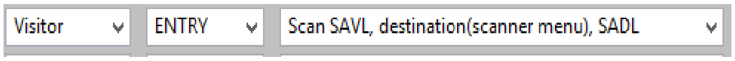
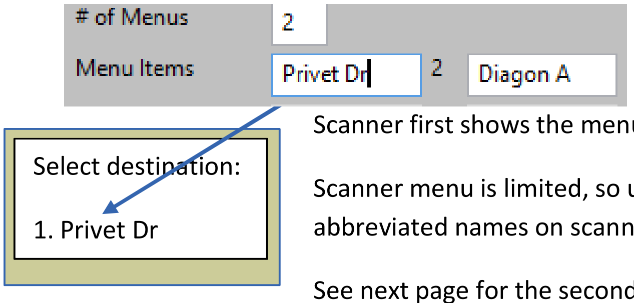
**** Enter destination by menu on scanner***:

The scanner can display a menu of up to 15 destinations, which you can configure with names such as Admin, Workshop, Store Room, Shop, … etc. When the operator chooses an item, the scanner sends a destination code ranging from 1...15 back to the server. In the Destination Screen, create items with codes 1,...15 to match the menu items.

| **Configure scanner** | **Configure the destination in Janus** |
|---|---|
| Janus Config: **Scanners screen**<br>Select sequences for Menu destinations<br><br>Visitor ENTRY Scan SAVL, destination(scanner menu), SADL<br>Capture text to show in the menu:<br><br>2<br>Great Hall Dormitories<br> <br> <br>The code in the scanner menu is sent to Janus and should match a code in the destinations screen. | Janus Config: **Destinations screen**<br>Make sure you use the ***same*** number as the menu item so Janus can match the scanner's number with the address description<br>Code 1="Great Hall"<br>Code 2="Dormitories"<br>Code 3="Pavilion"<br>Code 4="Headmaster"<br>...etc... |

**** Enter destination by menu and number on scanner***:

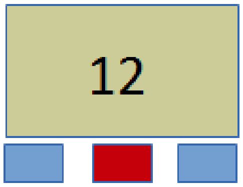
The scanner can display display a menu of up to 15 destinations, which can be used for street names or building names. Once the guard selected that from the menu, the scanner then asks for a street number (or use for a room number in the building) to be captured.

| **Configure scanner** | **Configure the destination in Janus** |
|---|---|
| Janus Config: **Scanners screen**<br>Select sequences for Menu destinations<br><br>Visitor ENTRY Scan SAVL, destination(scanner menu), SADL<br>Capture text to show in the menu:<br><br># of Menus 2<br>Menu Items Privet Dr 2 Diagon A<br> <br> <br>Scanner first shows the menu.<br>Scanner menu is limited, so use abbreviated names on scanner<br>See next page for the second | Janus Config: **Destinations screen**<br>[see next page] |

**Scanner sequence (continued)**

**Scanner multiplies menu item with 10000.**

Then it asks for street number and adds it to the menu selection



Menu 2 “Diagon Alley” becomes 2 x 10000 = 20 000.

Add 12, and scanner sends number 20012 to represent the address “Diagon Alley 12”

Janus Config: **Destinations screen**

Make sure you use the ***same*** number as the number sent from scanner so Janus can match the number with the address description

Code 10001=”Privet Drive 1”

Code 10002=”Privet Drive 2”

Code 10003=”Privet Drive 3”

Code 10004=”Privet Drive 4”

…

Code 20001=”Diagon Alley 1”

Code 20002=”Diagon Alley 2”

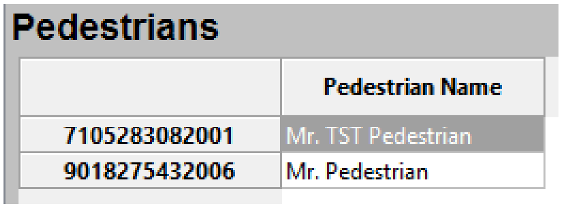
Code 20003=”Diagon Alley 3”

Code 20004=”Diagon Alley 4”

…

Code 20012=”Diagon Alley 12”

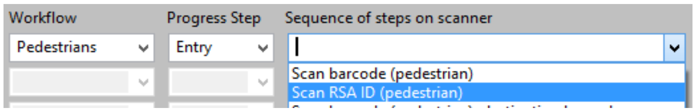
## Capture names of allowed pedestrians.



**Pedestrians**

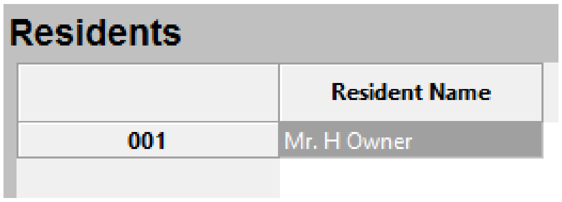
| | Pedestrian Name |
|---|---|
| 7105283082001 | Mr. TST Pedestrian |
| 9018275432006 | Mr. Pedestrian |

The Pedestrians configuration screen is used to configure regular pedestrians who are allowed, e.g. domestic workers, gardeners and other people who enter the estate by foot.

| Configure scanner | Configure pedestrians in Janus |
|---|---|
| Janus Config: **Scanners screen**<br>Select whether the pedestrian is scanned by RSA ID number, or whether these persons have a personnel card which is scanned.<br><br>Workflow: Pedestrians<br>Progress Step: Entry<br>Sequence of steps on scanner:<br>Scan barcode (pedestrian)<br>Scan RSA ID (pedestrian) | Janus Config: **Pedestrians screen**<br>Make sure you use the ***same*** RSA ID or barcode as will be scanned.<br>7105283082001=”Mr TST Pedestrian”<br>9018275432006=”Mr. Pedestrian” |

Janus will flag alerts if a pedestrian is scanned who is not in the list – treat as attempted security breach.

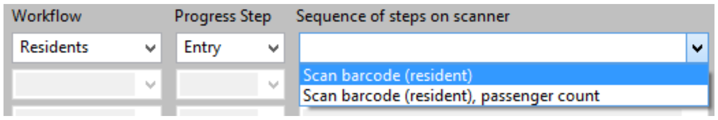
## Capture names of allowed residents or personnel.



Residents

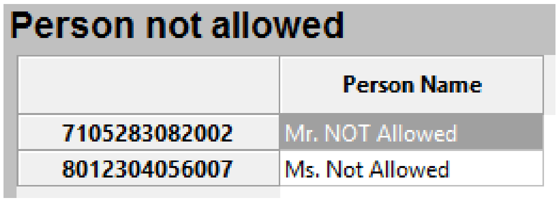
| | Resident Name |
|---|---|
| 001 | Mr. H Owner |

The Residents configuration screen is used to configure residents who are allowed, e.g. home owners, rental residents, etc. If you configure Janus for a business, you can rename "Residents" in the "Workflow" tab to "Personnel". Then use this for access control on personnel.

| Configure scanner | Configure residents or personnel in Janus |
|---|---|
| Janus Config: **Scanners screen**<br>Select a workflow for scanning residents. The assumption is that a resident card (or personnel card) is scanned. The SAVL and SADL scans are not performed when they enter.<br><br>Workflow: Residents<br>Progress Step: Entry<br>Sequence of steps on scanner:<br>Scan barcode (resident)<br>Scan barcode (resident), passenger count | Janus Config: **Residents screen**<br>Make sure you use the ***barcode*** ID as will be scanned for the resident.<br>001="Mr H Owner" |

Janus will flag alerts if a resident is scanned who is not in the list – treat as attempted security breach.

## Capturing persons not allowed in the estate

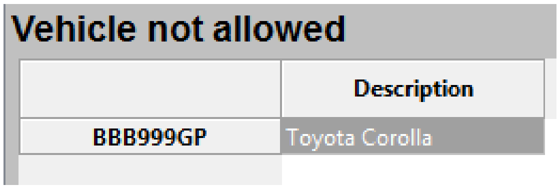


Person not allowed

| | Person Name |
|---|---|
| 7105283082002 | Mr. NOT Allowed |
| 8012304056007 | Ms. Not Allowed |

Capture the RSA ID number of persons who are not allowed in the estate. When this ID is scanned in a RSA Driver License or RSA ID Book, Janus will flag alerts. Treat as an attempted security breach.

## Capturing vehicles not allowed in the estate



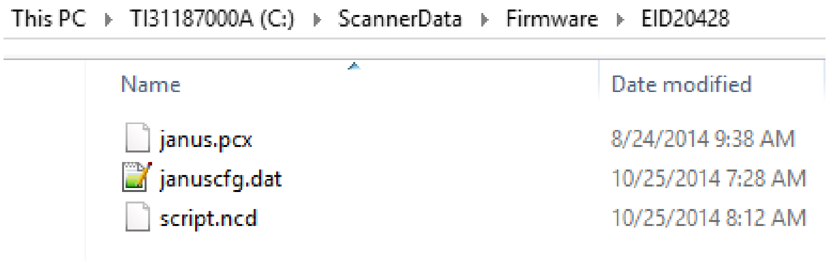
Vehicle not allowed

| | Description |
|---|---|
| BBB999GP | Toyota Corolla |

Capture the registration no of vehicles not allowed in the estate. When this registration number is scanned in a SAVL scan, Janus will flag alerts. Treat as an attempted security breach.

## Programming the scanner

1. Ensure the scanner config file you created, is located in c:\scannerdata\firmware\<scanner ID\>. You should see the following three files in Windows Explorer:



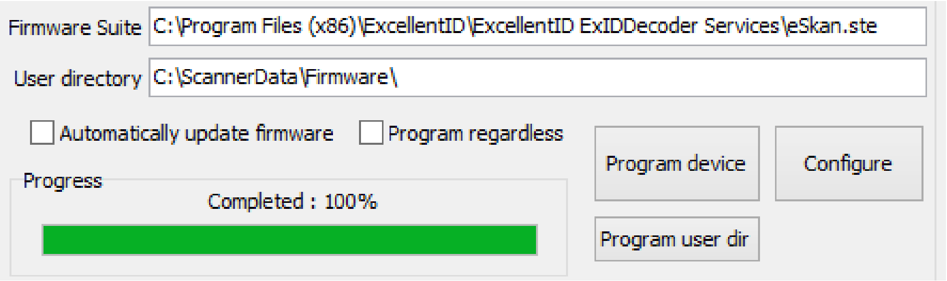
This PC ▸ TI31187000A (C:) ▸ ScannerData ▸ Firmware ▸ EID20428

| Name | Date modified |
|---|---|
| janus.pcx | 8/24/2014 9:38 AM |
| januscfg.dat | 10/25/2014 7:28 AM |
| script.ncd | 10/25/2014 8:12 AM |

There should exist separate subfolders for each scanner. You can configure them differently (e.g. one starting up with “Entry” and one starting up with “Exit”, or scanners dedicated to either visitors with vehicles vs pedestrians). In each scanner folder should exist Janus.pcx and script.ncd. Use Janus Scanners config screen to create a JanusCfg.dat for each folder.

2. Start the ExID Decoder Setup. It should have an icon on the desktop. For more information, see the ExID software documentation.

3. Plug in the scanner. The ExID Decoder Setup will display the screen below. Note the option to automatically update the firmware should be unchecked.



Firmware Suite: C:\Program Files (x86)\ExcellentID\ExcellentID ExIDDecoder Services\eSkan.ste

User directory: C:\ScannerData\Firmware\

□ Automatically update firmware □ Program regardless

Progress

Completed : 100%

* Double-click the “User Directory” edit box. Select the path (see paragraph 1 above) for the specific scanner that is now connected.

* Click “Program user dir” : this will load your Janus config settings on the scanner. It will also program the scanner for access control with the Janus system.

* Click the Configure Button.

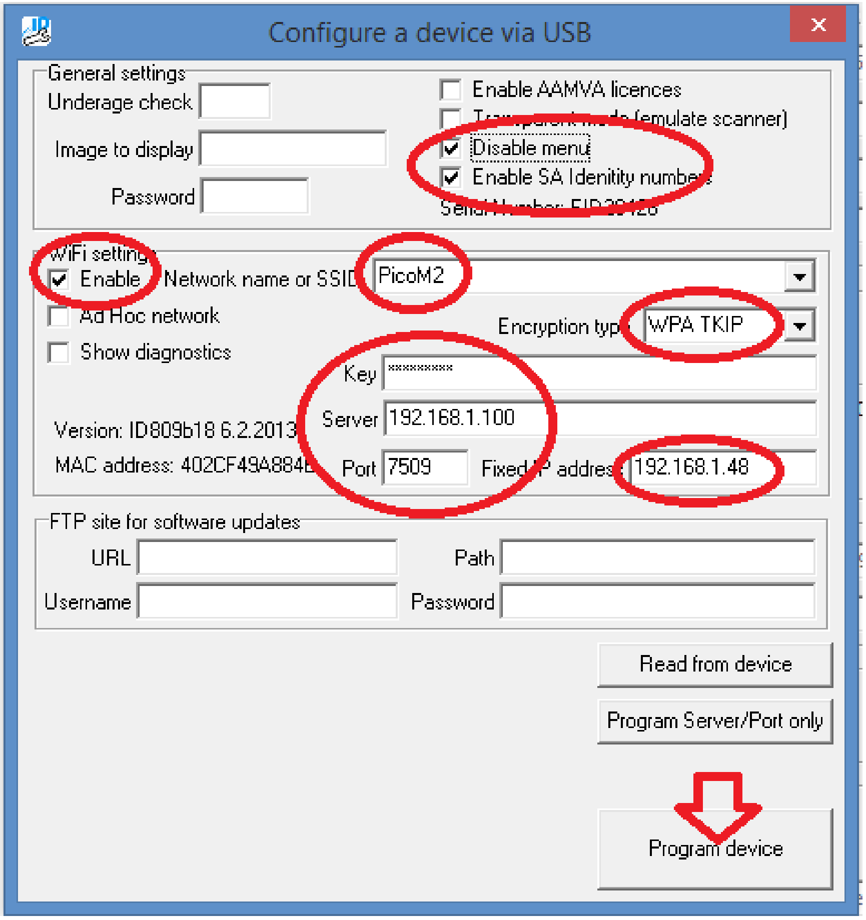
The Excellent ID installation manual describes how to configure a scanner, and the instructions there should be followed. The notes below just outline the specific settings required for operation with Janus.

- Disable menu. You can enable while testing and installing the system, but disable it before deploying the scanner for use.

- Enable SA Identity numbers, as these are used as backup when driver license is not presented. RSA ID are also used for pedestrian scans.

- Enable Wifi settings.

- SSID is the wifi SSID that you provided when you set up your wifi access point. It should appear in the drop-down box when your network is correctly set up and the wifi is on.
- Encryption type should match what you configured for security in your wifi setup.
- Key is the password you typed when you configured your wifi access point security.
- Server is the IP address of the computer where the Excellent ID software is installed.
- Port is always set at 7509.
- Fixed IP address is an IP address that we provide for the scanner. We usually follow a convention to use the same network IP as the server (in this illustration 192,168,1,xxx) where xxx is then the last two digits of the scanner ID. So if your scanner ID is eID20521, we set its IP address to 192.168.1.21, assuming that the scanner ID's you purchased, do not overlap in their last digits. So each scanner gets its own unique fixed IP address on the network.



Configure a device via USB

General settings

Underage check

Image to display

Password

□ Enable AAMVA licences

□ Transparent mode (emulate scanner)

☑ Disable menu

☑ Enable SA Idenitity numbers

Serial Number: EID20126

WiFi settings

☑ Enable

Network name or SSID: PicoM2

□ Ad Hoc network

□ Show diagnostics

Encryption type: WPA TKIP

Key: *********

Server: 192.168.1.100

Port: 7509

Fixed IP address: 192.168.1.48

Version: ID809b18 6.2.2013

MAC address: 402CF49A884E

FTP site for software updates

URL

Path

Username

Password

4. Start the Janus software.

5. Do a few test scans and check that the scans are processed.

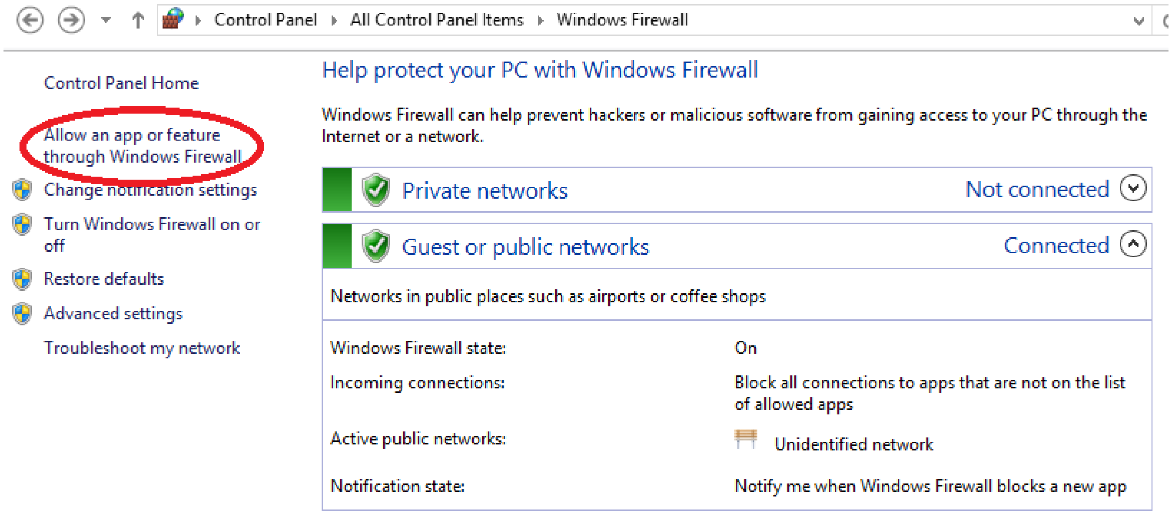
--------------------o0o--------------------

# Annexure 1. Checking the Windows firewall

The ExcellentID software requires rules on the Windows firewall to ensure that messages from scanners are not blocked by the firewall. The ExcellentID manual describes the setup of the firewall in detail. These instructions are intended for Janus troubleshooting and do in no way replace the ExcellentID manual.

## Firewall setup for excellent ID Service

The Windows Firewall is activated by the Windows Control Panel, and at the bottom, select “Windows Firewall”.


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

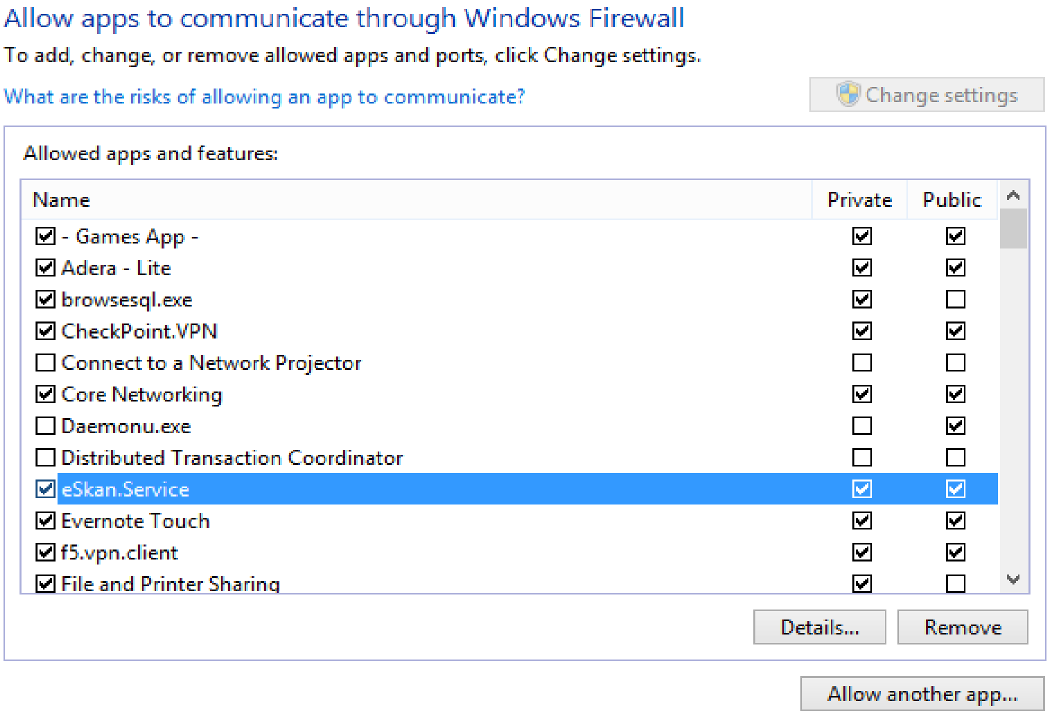
Guest or public networks — Connected

Networks in public places such as airports or coffee shops

| | |
|---|---|
| Windows Firewall state: | On |
| Incoming connections: | Block all connections to apps that are not on the list of allowed apps |
| Active public networks: | Unidentified network |
| Notification state: | Notify me when Windows Firewall blocks a new app |

After a successful installation as per the ExcellentID manual, you can verify the firewall is configured correctly by the following steps: Select “Allow an app or feature through Windows Firewall”.

The “eSkan.Service” should display with tick marks both on Private and Public, as shown below.



Allow apps to communicate through Windows Firewall

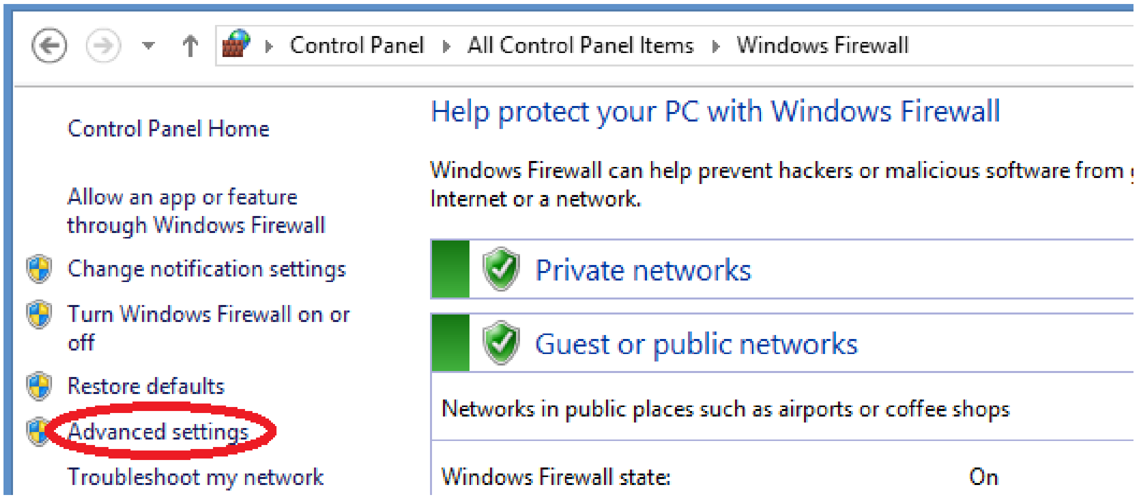
To add, change, or remove allowed apps and ports, click Change settings.

Allowed apps and features:

| Name | Private | Public |
|---|---|---|
| ☑ - Games App - | ☑ | ☑ |
| ☑ Adera - Lite | ☑ | ☑ |
| ☑ browsesql.exe | ☑ | □ |
| ☑ CheckPoint.VPN | ☑ | ☑ |
| □ Connect to a Network Projector | □ | □ |
| ☑ Core Networking | ☑ | ☑ |
| □ Daemonu.exe | □ | ☑ |
| □ Distributed Transaction Coordinator | □ | □ |
| ☑ eSkan.Service | ☑ | ☑ |
| ☑ Evernote Touch | ☑ | ☑ |
| ☑ f5.vpn.client | ☑ | ☑ |
| ☑ File and Printer Sharing | ☑ | □ |

If this does not appear, install by clicking on “Allow another app” and choosing the eSkan.Service program as described in the ExcellentID installation manual.

You can also inspect the inbound rules list in the firewall. When the Windows firewall starts, select “Advanced settings”.


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from
Internet or a network.

Private networks

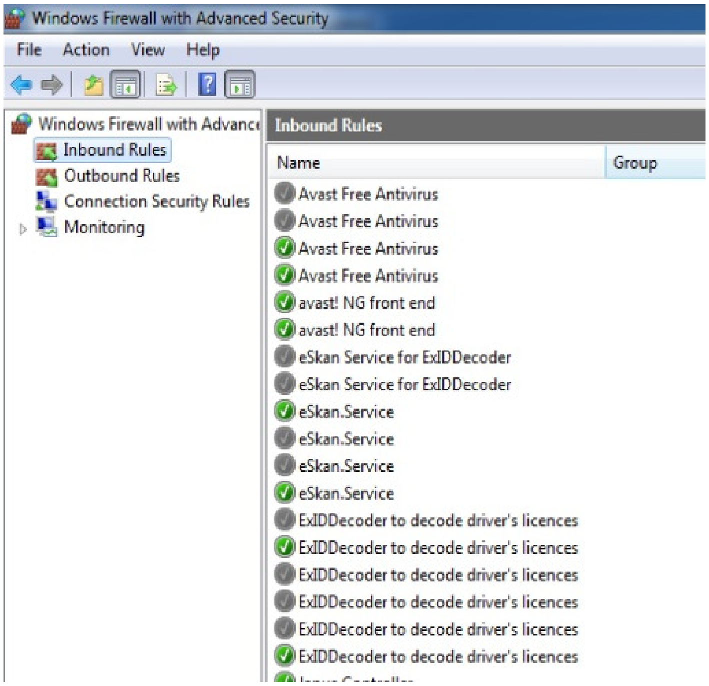
Guest or public networks

Networks in public places such as airports or coffee shops

Windows Firewall state: On

Several duplicate entries for eSkan Service and the eSkan decoder (as shown on the right) can be cause for disabled wifi communication.

They can be safely deleted and replaced either by installing as described above, or with the port entry described below.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

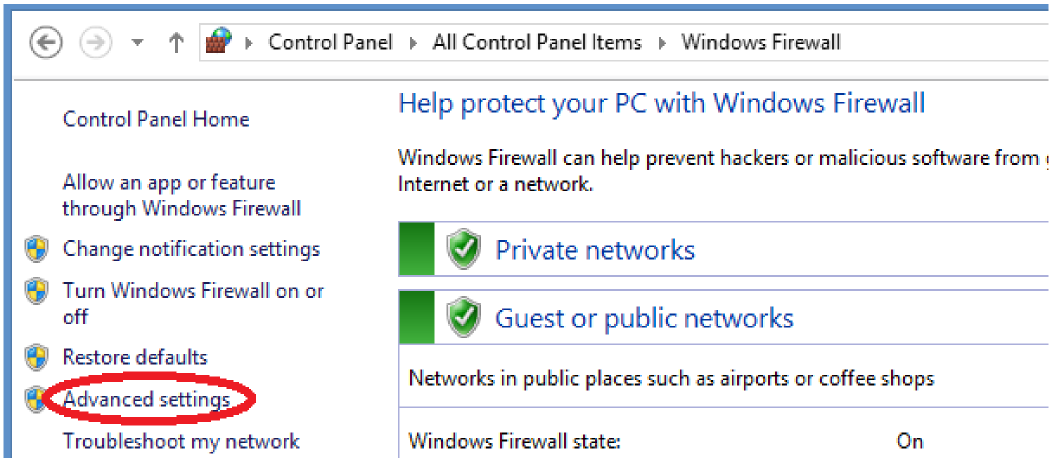
Inbound Rules

| Name | Group |
|---|---|
| Avast Free Antivirus | |
| Avast Free Antivirus | |
| ✓ Avast Free Antivirus | |
| ✓ Avast Free Antivirus | |
| ✓ avast! NG front end | |
| ✓ avast! NG front end | |
| eSkan Service for ExIDDecoder | |
| eSkan Service for ExIDDecoder | |
| ✓ eSkan.Service | |
| eSkan.Service | |
| eSkan.Service | |
| ✓ eSkan.Service | |
| ExIDDecoder to decode driver's licences | |
| ✓ ExIDDecoder to decode driver's licences | |
| ExIDDecoder to decode driver's licences | |
| ExIDDecoder to decode driver's licences | |
| ExIDDecoder to decode driver's licences | |
| ✓ ExIDDecoder to decode driver's licences | |

## Firewall exclusion based on Port number only:

Start the Windows Control Panel, and select Firewall.

Click “Advanced settings” in the Firewall.


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from Internet or a network.

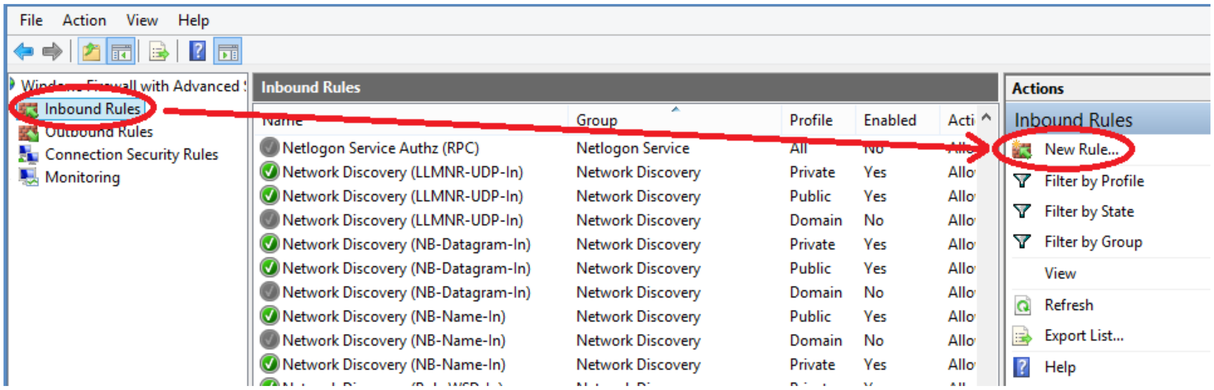
Private networks

Guest or public networks

Networks in public places such as airports or coffee shops

Windows Firewall state: On

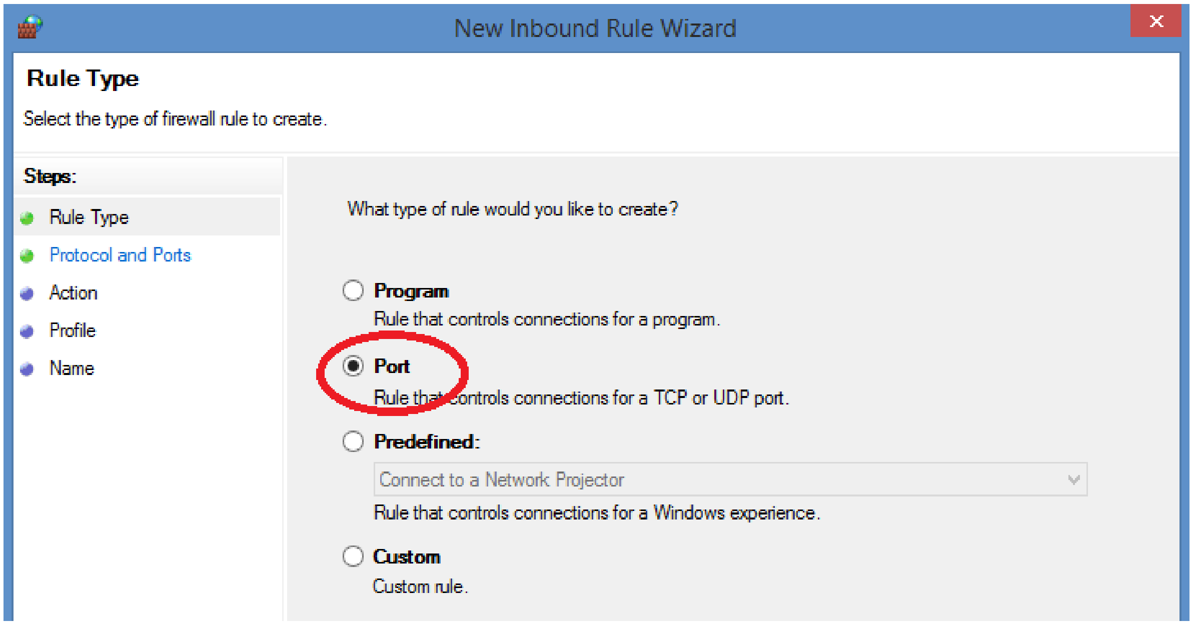
Click Inbound Rules, then select “New Rule”



Inbound Rules

| Name | Group | Profile | Enabled | Acti |
|---|---|---|---|---|
| Netlogon Service Authz (RPC) | Netlogon Service | All | No | Allo |
| Network Discovery (LLMNR-UDP-In) | Network Discovery | Private | Yes | Allo |
| Network Discovery (LLMNR-UDP-In) | Network Discovery | Public | Yes | Allo |
| Network Discovery (LLMNR-UDP-In) | Network Discovery | Domain | No | Allo |
| Network Discovery (NB-Datagram-In) | Network Discovery | Private | Yes | Allo |
| Network Discovery (NB-Datagram-In) | Network Discovery | Public | Yes | Allo |
| Network Discovery (NB-Datagram-In) | Network Discovery | Domain | No | Allo |
| Network Discovery (NB-Name-In) | Network Discovery | Public | Yes | Allo |
| Network Discovery (NB-Name-In) | Network Discovery | Domain | No | Allo |
| Network Discovery (NB-Name-In) | Network Discovery | Private | Yes | Allo |

Select to create a rule based on a TCP/IP port.



**Rule Type**

Select the type of firewall rule to create.

What type of rule would you like to create?

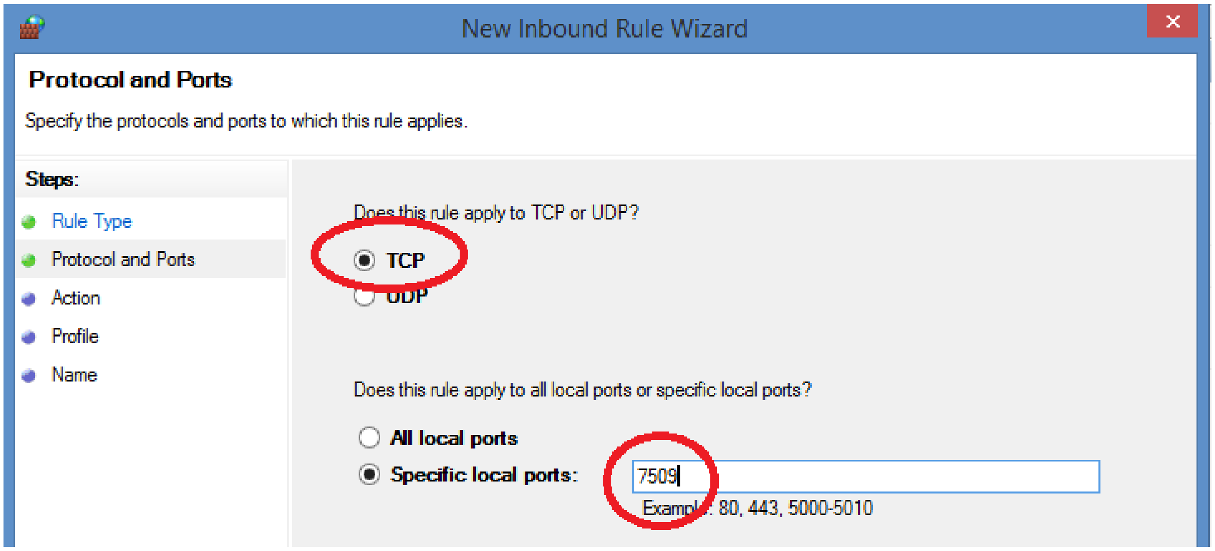
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
Connect to a Network Projector
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Provide the port for the ExID Communications Service. Confirm it shows in the ExID Decoder Service sreen.



New Inbound Rule Wizard

**Protocol and Ports**

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

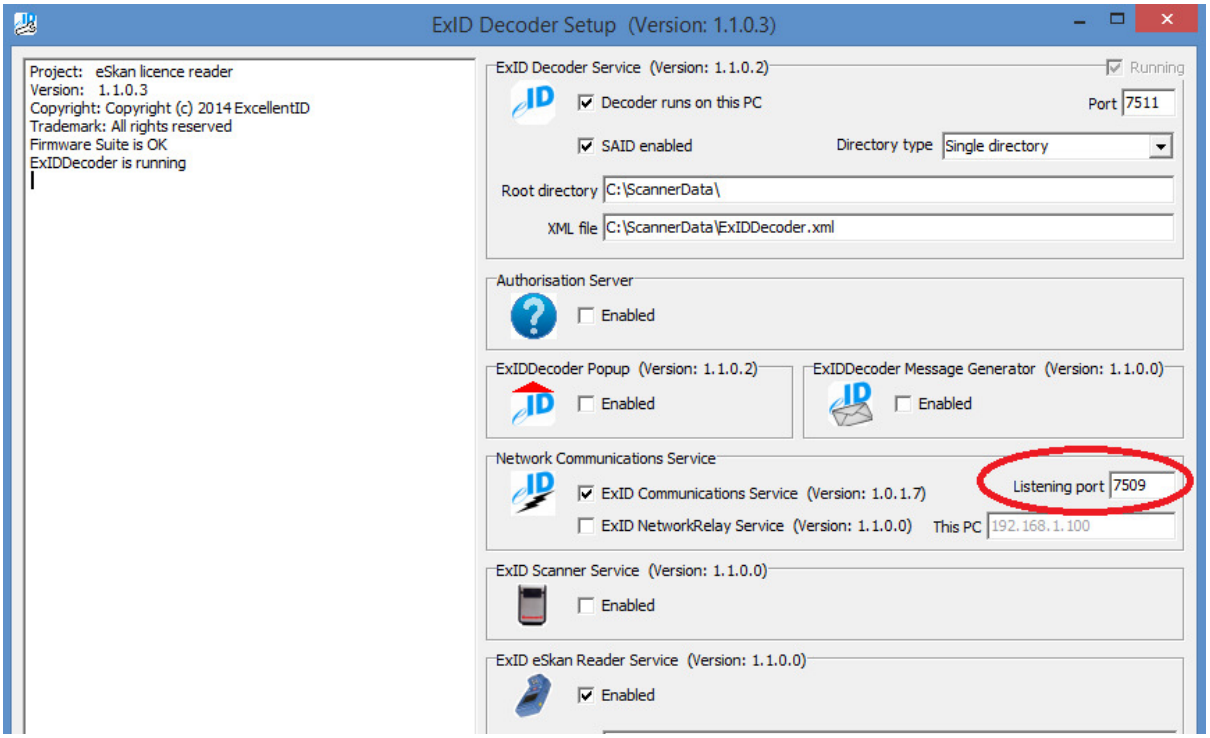
● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 7509

Example: 80, 443, 5000-5010

Start the ExIDDecoder Service and confirm the communication service is configured with port number 7509.



ExID Decoder Setup (Version: 1.1.0.3)

```
Project:   eSkan licence reader
Version:   1.1.0.3
Copyright: Copyright (c) 2014 ExcellentID
Trademark: All rights reserved
Firmware Suite is OK
ExIDDecoder is running
```

ExID Decoder Service (Version: 1.1.0.2) ☑ Running
☑ Decoder runs on this PC Port 7511
☑ SAID enabled Directory type Single directory
Root directory C:\ScannerData\
XML file C:\ScannerData\ExIDDecoder.xml

Authorisation Server
☐ Enabled

ExIDDecoder Popup (Version: 1.1.0.2)
☐ Enabled

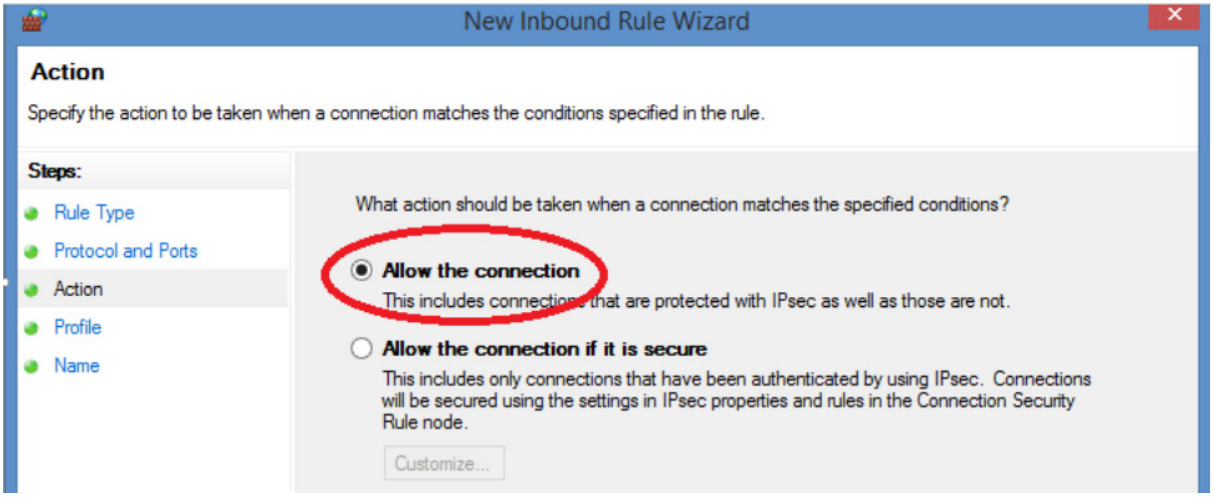
ExIDDecoder Message Generator (Version: 1.1.0.0)
☐ Enabled

Network Communications Service
☑ ExID Communications Service (Version: 1.0.1.7) Listening port 7509
☐ ExID NetworkRelay Service (Version: 1.1.0.0) This PC 192.168.1.100

ExID Scanner Service (Version: 1.1.0.0)
☐ Enabled

ExID eSkan Reader Service (Version: 1.1.0.0)
☑ Enabled

Back in the firewall wizard, choose the option to allow this connection:



**Action**

Specify the action to be taken when a connection matches the conditions specified in the rule.

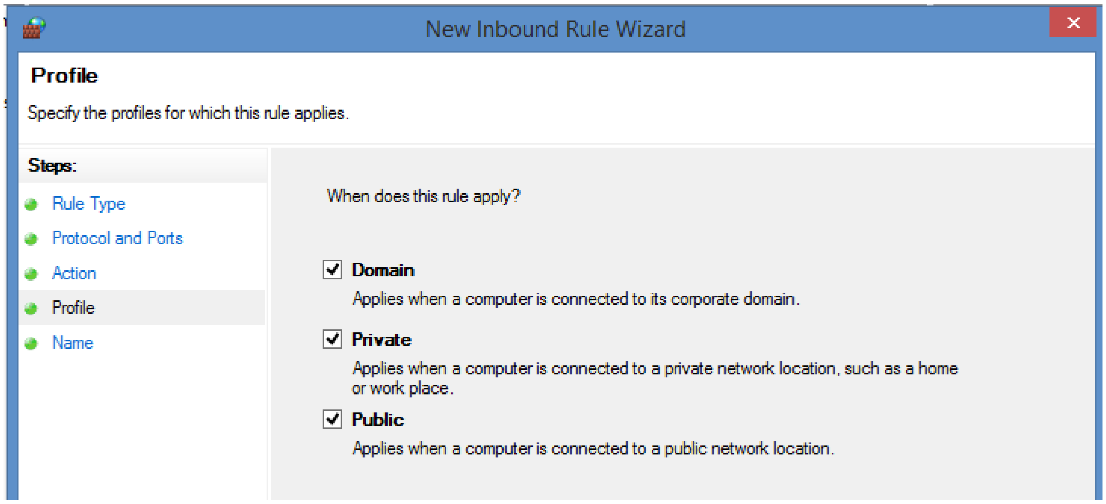
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Then set the firewall to open this port on private, public and domain networks:



**Profile**

Specify the profiles for which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

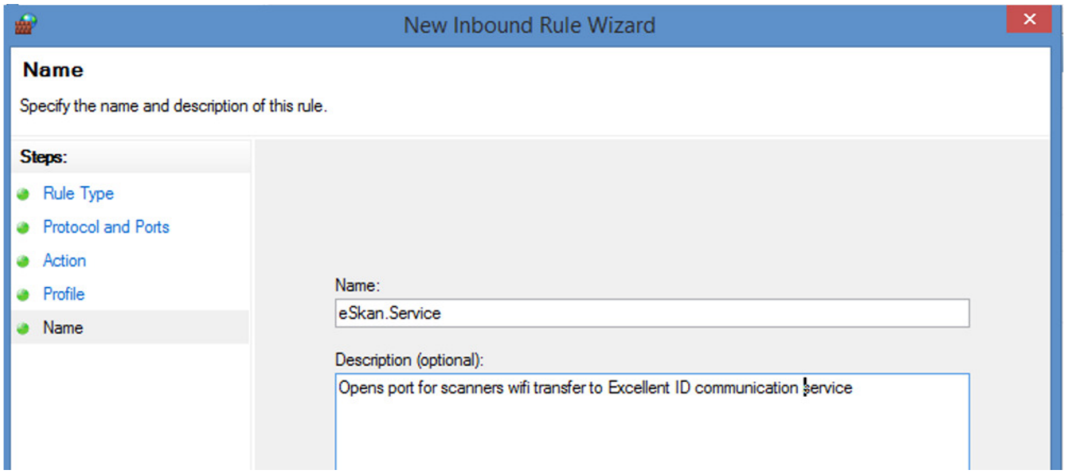
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

Lastly, provide a name for this rule (text that will appear in the firewall list of rules). It is optional to provide a description to remind the network administrator why the port was opened.



**Name**

Specify the name and description of this rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

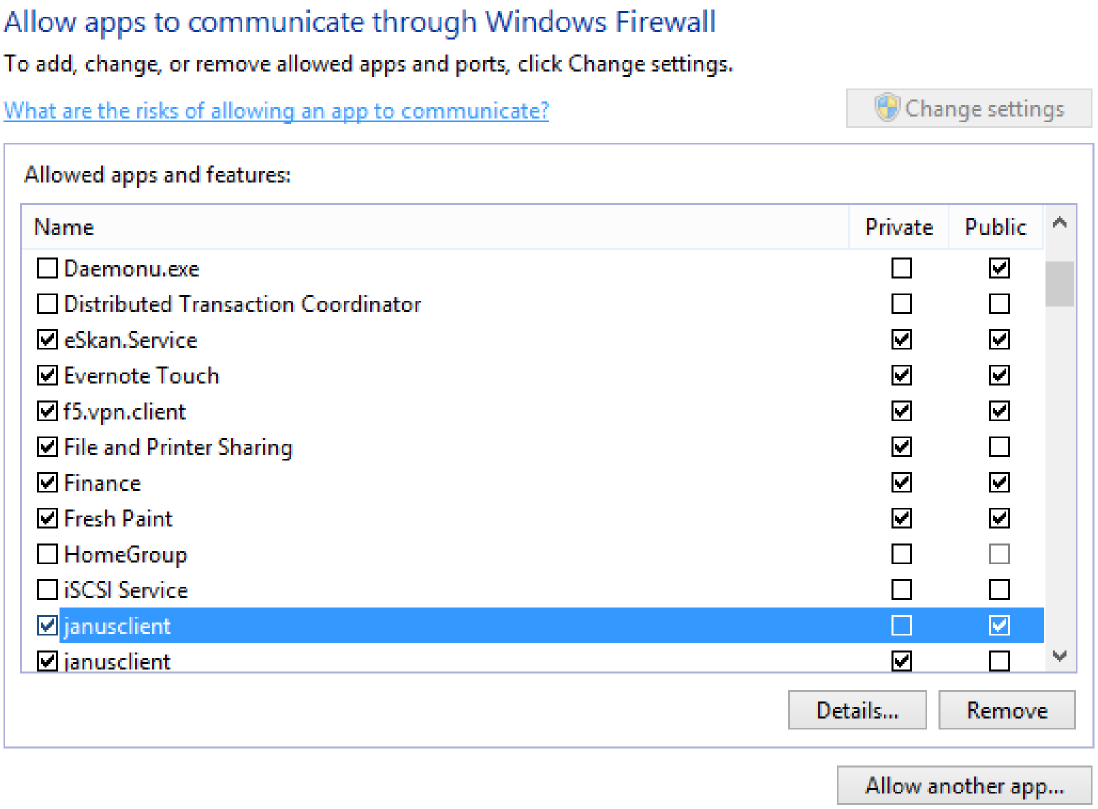
Name: eSkan.Service

Description (optional): Opens port for scanners wifi transfer to Excellent ID communication service

## Firewall setup for Janus

When Janus is started the first time, Windows will ask the user if the firewall may allow Janus. The user should allow this. Windows then automatically creates an entry for Janus on the local firewall.

To inspect this setting, activate the Windows Control Panel, and at the bottom, select “Windows Firewall”. Then select “Allow an app or feature through Windows Firewall”. The screen should show Janus in the list.



Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

| Name | Private | Public |
|---|---|---|
| □ Daemonu.exe | □ | ☑ |
| □ Distributed Transaction Coordinator | □ | □ |
| ☑ eSkan.Service | ☑ | ☑ |
| ☑ Evernote Touch | ☑ | ☑ |
| ☑ f5.vpn.client | ☑ | ☑ |
| ☑ File and Printer Sharing | ☑ | □ |
| ☑ Finance | ☑ | ☑ |
| ☑ Fresh Paint | ☑ | ☑ |
| □ HomeGroup | □ | □ |
| □ iSCSI Service | □ | □ |
| ☑ janusclient | □ | ☑ |
| ☑ janusclient | ☑ | □ |

If you have a network-based firewall, and the Janus Professional configuration, you may need to open the port for Janus Controller manually. By default this port is 8004. The port is configurable in the SETTINGS table in the Janus database as CONTROLLERPORT. This port can be changed, but all Janus products on the network then have to be restarted.

You can also manually open this port as described above for the ExID Communications service.

# Annexure 2. SQL Server Express installation instructions

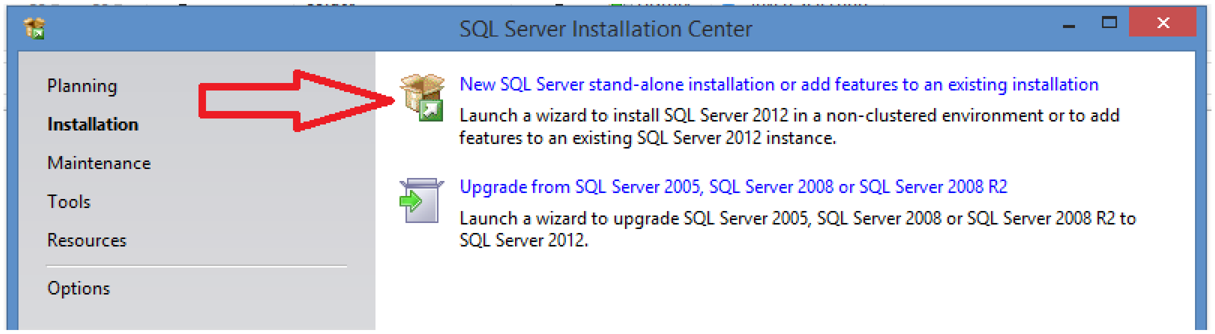
SQL Server Express is a product from Microsoft. The instructions below are provided as a quick guide for installing SQL Express for use with Janus. Please consult Microsoft's manuals and theird online MSDN documentation for a complete reference.

## Installing SQL Express for use with Janus

Start the program SQLEXPRWT_x64_ENU.exe. This is a 64-bit installer, and should be compatible with most machines running Windows 7 or Windows 8. Use of 32-bit installs are therefore no longer necessary.

The installer may take a while to start. Patiently wait for the screen illustrated below to appear.

Choose the option “New SQL stand-alone installation or add features to an existing installation”.



SQL Server Installation Center

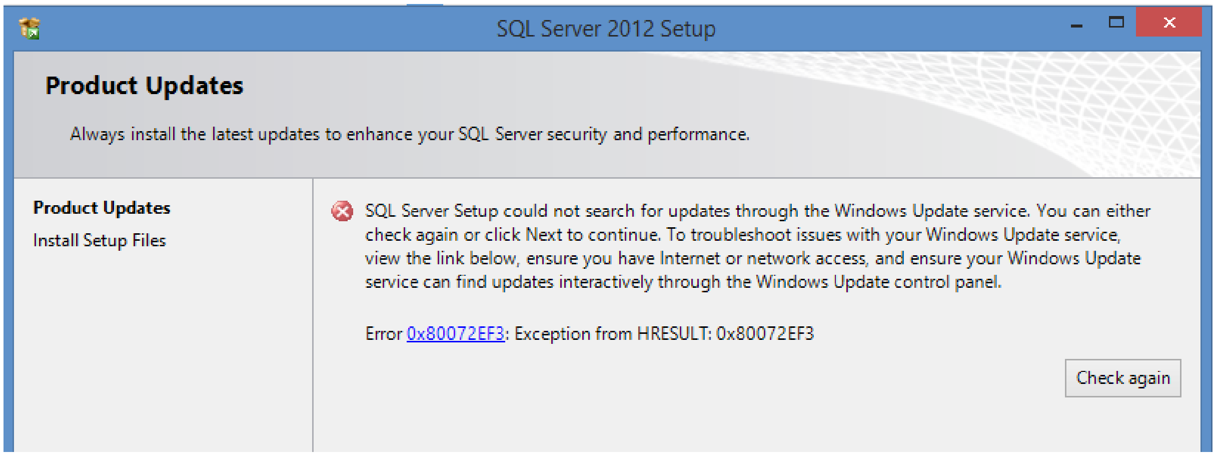
New SQL Server stand-alone installation or add features to an existing installation

Launch a wizard to install SQL Server 2012 in a non-clustered environment or to add features to an existing SQL Server 2012 instance.

Upgrade from SQL Server 2005, SQL Server 2008 or SQL Server 2008 R2

Launch a wizard to upgrade SQL Server 2005, SQL Server 2008 or SQL Server 2008 R2 to SQL Server 2012.

The SQL Server installer will try to upgrade itself via an Internet. In many cases the computers used for Janus are not enabled for Internet access, and the SQL installer will display the warning below.



SQL Server 2012 Setup

Product Updates

Always install the latest updates to enhance your SQL Server security and performance.

SQL Server Setup could not search for updates through the Windows Update service. You can either check again or click Next to continue. To troubleshoot issues with your Windows Update service, view the link below, ensure you have Internet or network access, and ensure your Windows Update service can find updates interactively through the Windows Update control panel.

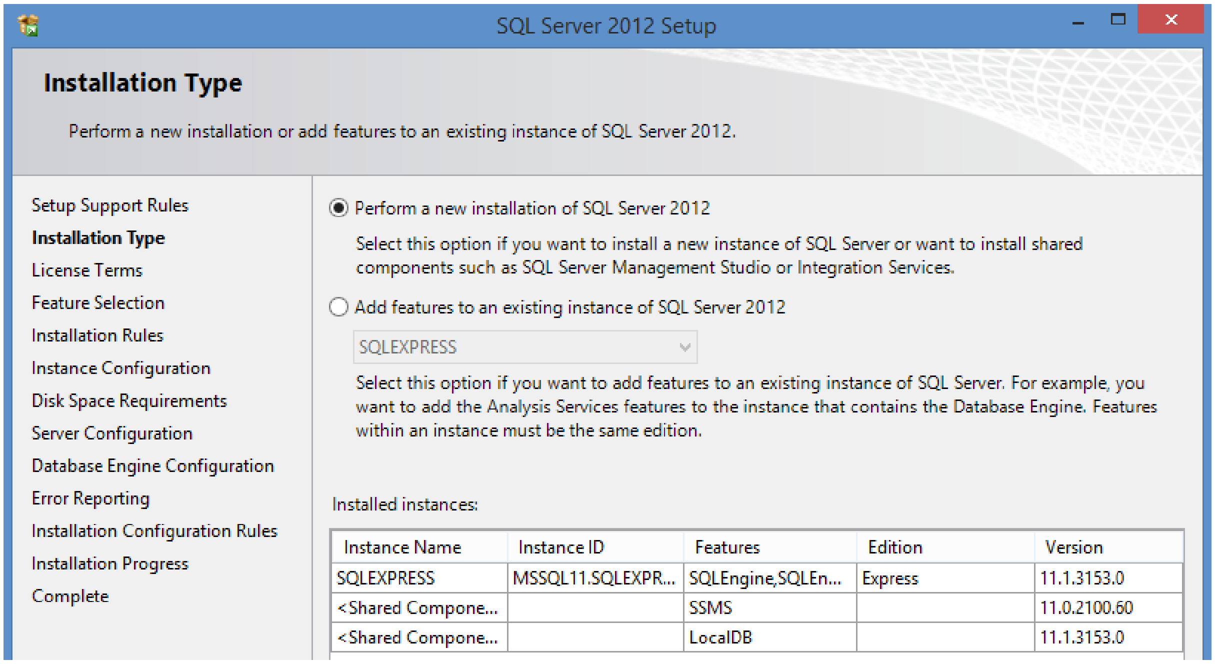
Error 0x80072EF3: Exception from HRESULT: 0x80072EF3

Just ignore this warning and click Next to continue; or establish a temporary Internet link and click “check again”. The upgrade may take a while to complete and is not covered in this guide. Consult Microsoft for more information on such upgrades.

The installer then checks whether an existing SQL Server instance is already present on the computer. If such existing instance is present, you will most likely be able to cancel the install and just use the existing instance. However in cases where such existing instance is very old, compatibility issues, or performance may dictate that you could decide to install an instance dedicated to Janus only.

In this process, the installer may also stop and require that you first install certain other software on which SQL Server Express 2012 is dependent. You will only be able to continue if such dependencies are installed.

Click NEXT to continue.



SQL Server 2012 Setup

**Installation Type**

Perform a new installation or add features to an existing instance of SQL Server 2012.

- Setup Support Rules
- **Installation Type**
- License Terms
- Feature Selection
- Installation Rules
- Instance Configuration
- Disk Space Requirements
- Server Configuration
- Database Engine Configuration
- Error Reporting
- Installation Configuration Rules
- Installation Progress
- Complete

● Perform a new installation of SQL Server 2012

Select this option if you want to install a new instance of SQL Server or want to install shared components such as SQL Server Management Studio or Integration Services.

○ Add features to an existing instance of SQL Server 2012

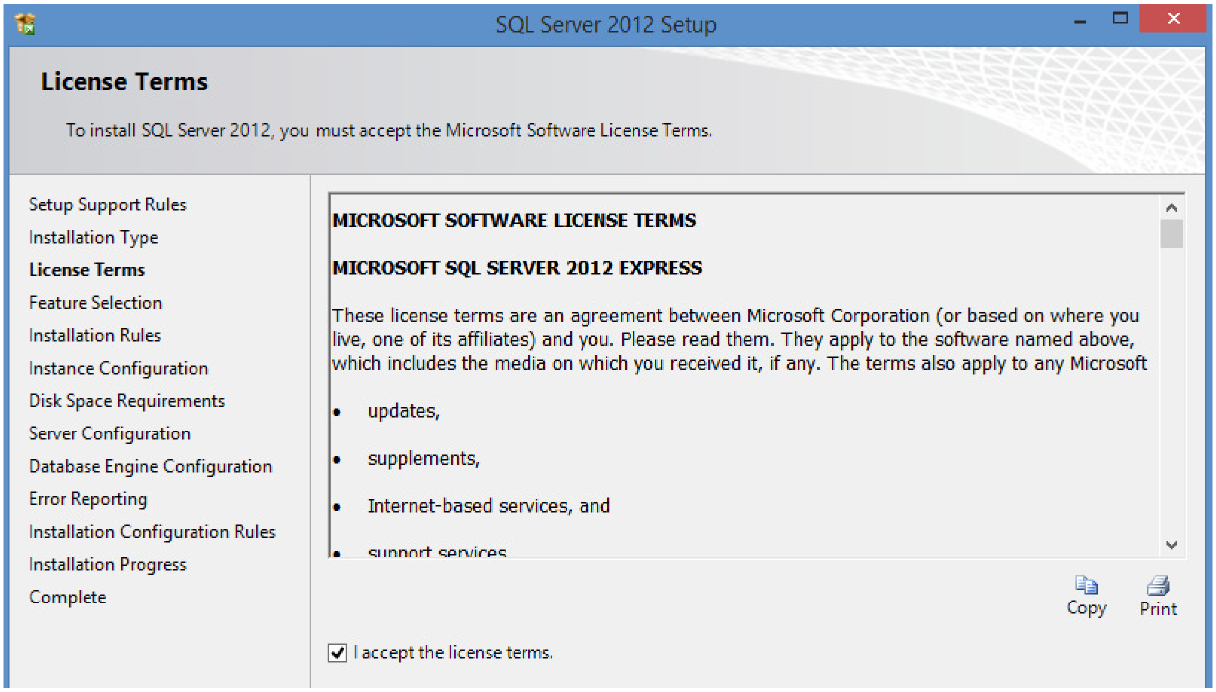
SQLEXPRESS

Select this option if you want to add features to an existing instance of SQL Server. For example, you want to add the Analysis Services features to the instance that contains the Database Engine. Features within an instance must be the same edition.

Installed instances:

| Instance Name | Instance ID | Features | Edition | Version |
|---|---|---|---|---|
| SQLEXPRESS | MSSQL11.SQLEXPR... | SQLEngine,SQLEn... | Express | 11.1.3153.0 |
| <Shared Compone... | | SSMS | | 11.0.2100.60 |
| <Shared Compone... | | LocalDB | | 11.1.3153.0 |

Check the boc to accept the Microsoft license terms for their software, then click NEXT to continue.



SQL Server 2012 Setup

**License Terms**

To install SQL Server 2012, you must accept the Microsoft Software License Terms.

- Setup Support Rules
- Installation Type
- **License Terms**
- Feature Selection
- Installation Rules
- Instance Configuration
- Disk Space Requirements
- Server Configuration
- Database Engine Configuration
- Error Reporting
- Installation Configuration Rules
- Installation Progress
- Complete

**MICROSOFT SOFTWARE LICENSE TERMS**

**MICROSOFT SQL SERVER 2012 EXPRESS**

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

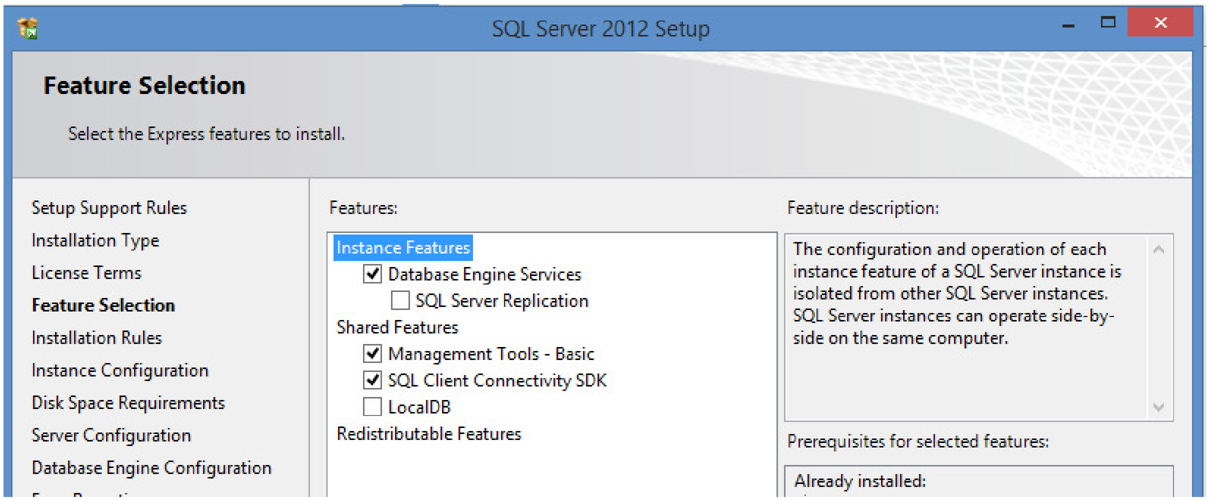
- updates,
- supplements,
- Internet-based services, and
- support services

☑ I accept the license terms.

The Feature Selection screen is displayed next:

Uncheck the SQL Server Replication and the LocalDB boxes. These are not used by Janus.

Check Database Engine Services, Management Tools, and SQL Client Connectivity SDK.



SQL Server 2012 Setup

**Feature Selection**

Select the Express features to install.

Features:

Instance Features
- ☑ Database Engine Services
  - □ SQL Server Replication

Shared Features
- ☑ Management Tools - Basic
- ☑ SQL Client Connectivity SDK
- □ LocalDB

Redistributable Features

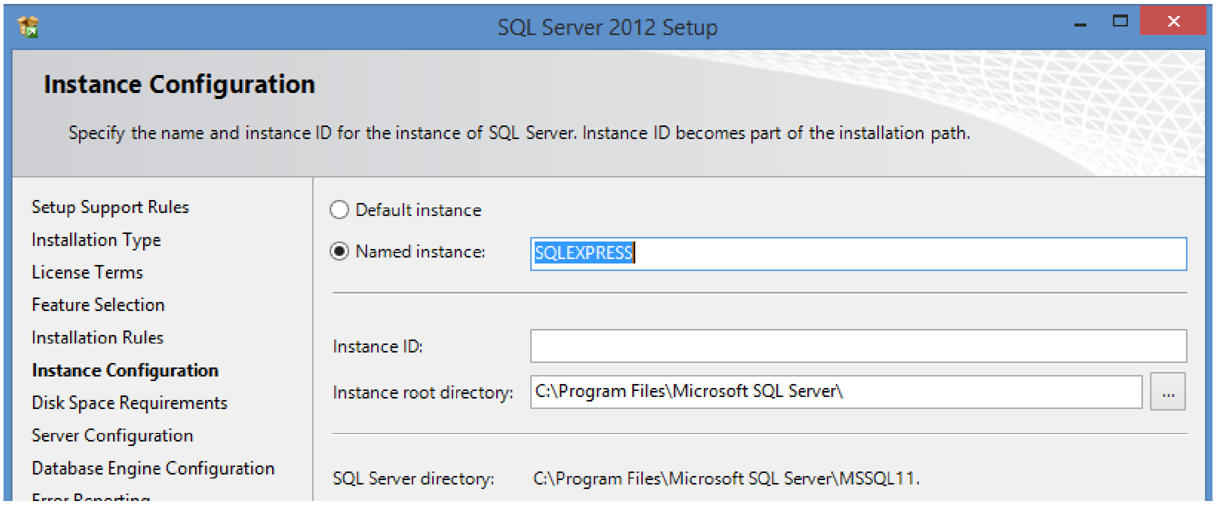
Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on the same computer.

Prerequisites for selected features:

Already installed:

Accept the default instance name that Microsoft provides, usually “SQLEXPRESS”. Select “NEXT”.



SQL Server 2012 Setup

**Instance Configuration**

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

○ Default instance

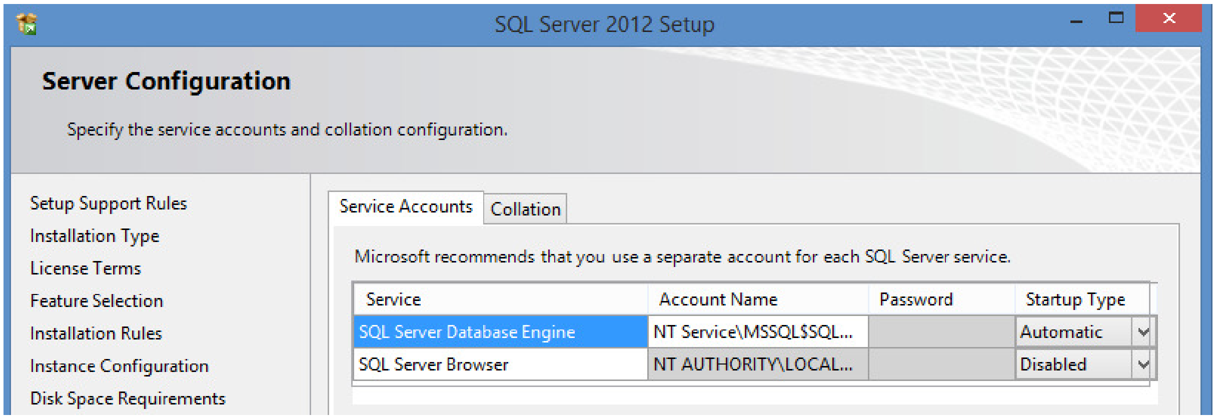
● Named instance: SQLEXPRESS

Instance ID:

Instance root directory: C:\Program Files\Microsoft SQL Server\

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL11.

Accept the default Server Configuration settings, and select “NEXT” to continue.



SQL Server 2012 Setup

**Server Configuration**

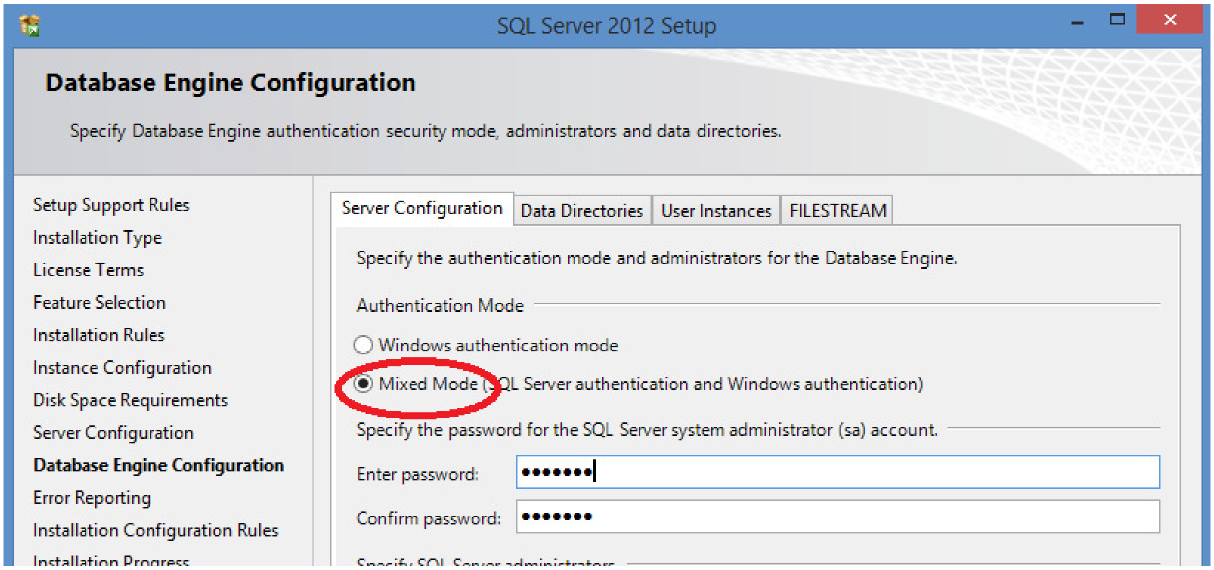
Specify the service accounts and collation configuration.

Microsoft recommends that you use a separate account for each SQL Server service.

| Service | Account Name | Password | Startup Type |
|---|---|---|---|
| SQL Server Database Engine | NT Service\MSSQL$SQL... | | Automatic |
| SQL Server Browser | NT AUTHORITY\LOCAL... | | Disabled |

In the Database Engine configuration screen, make sure that you select “Mixed Mode”.

Provide a password for the “sa” user.



SQL Server 2012 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: •••••••

Confirm password: •••••••

Specify SQL Server administrators

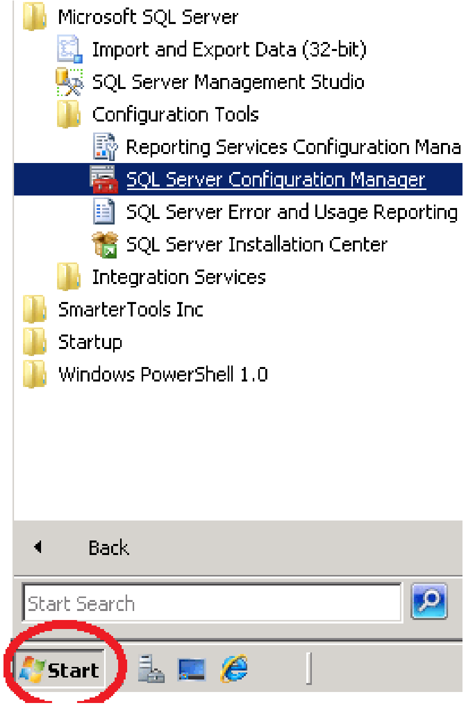
Make a note of the “sa” password that you provide here, as you will have to enter this in the Janus install.

Click “NEXT” to continue.

Hereafter, accept the default settings on all the following screens and let the installation continue.

The install itself may take a while. Do not panic if the progress is standing still for a considerable time, it is busy in the background.

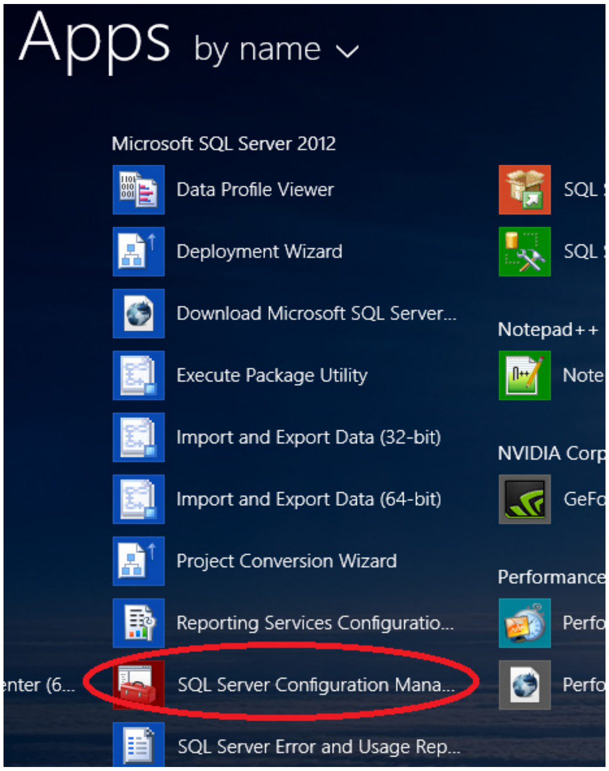
## Configuring SQL Express for use with Janus



Microsoft SQL Server
Import and Export Data (32-bit)
SQL Server Management Studio
Configuration Tools
Reporting Services Configuration Mana
SQL Server Configuration Manager
SQL Server Error and Usage Reporting
SQL Server Installation Center
Integration Services
SmarterTools Inc
Startup
Windows PowerShell 1.0
Back
Start Search
Start

In Windows 7 you will find the SQL Server Configuration Manager in Start, Programs, SQL Server 2012

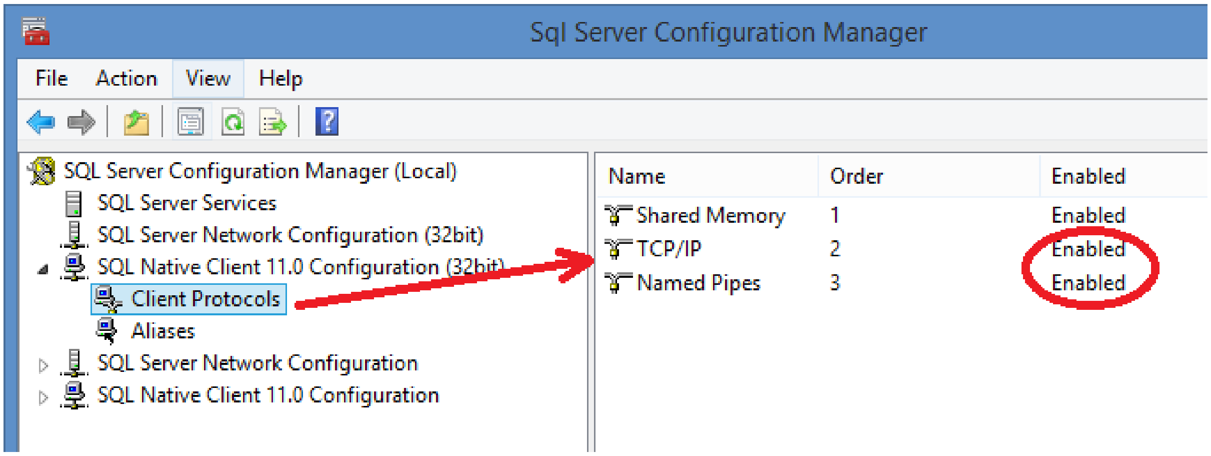
In Windows 8, click Start, and scroll through the tiles for apps till “S” where you will find SQL Server, as illustrated on the right.


Apps by name
Microsoft SQL Server 2012
Data Profile Viewer
Deployment Wizard
Download Microsoft SQL Server...
Execute Package Utility
Import and Export Data (32-bit)
Import and Export Data (64-bit)
Project Conversion Wizard
Reporting Services Configuratio...
SQL Server Configuration Mana...
SQL Server Error and Usage Rep...
enter (6...
SQL
SQL
Notepad++
Note
NVIDIA Corp
GeFo
Performance
Perfo
Perfo

Activate the program:

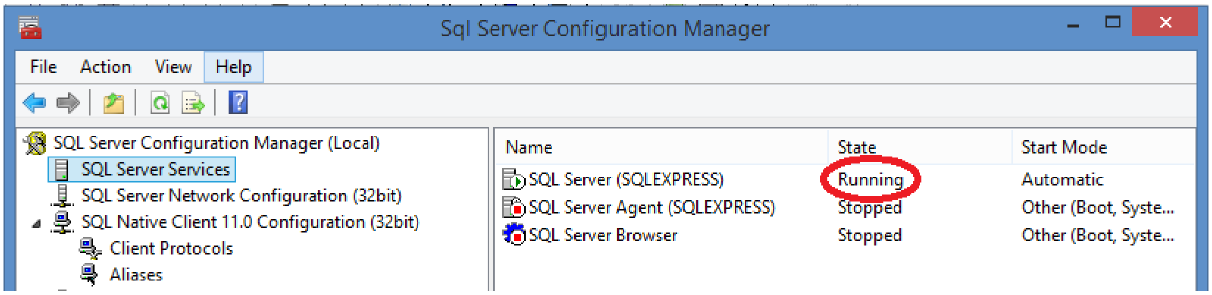
“SQL Server Configuration Manager”

Once the SQL Server Configuration Manager started, enable TCP/IP and Named Pipes.


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 11.0 Configuration (32bit)
Client Protocols
Aliases
SQL Server Network Configuration
SQL Native Client 11.0 Configuration

| Name | Order | Enabled |
|---|---|---|
| Shared Memory | 1 | Enabled |
| TCP/IP | 2 | Enabled |
| Named Pipes | 3 | Enabled |

After enabling TCP/IP and Named Pipes, stop SQL Server, wait a few seconds and start it again so it can apply the changes.


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 11.0 Configuration (32bit)
Client Protocols
Aliases

| Name | State | Start Mode |
|---|---|---|
| SQL Server (SQLEXPRESS) | Running | Automatic |
| SQL Server Agent (SQLEXPRESS) | Stopped | Other (Boot, Syste... |
| SQL Server Browser | Stopped | Other (Boot, Syste... |

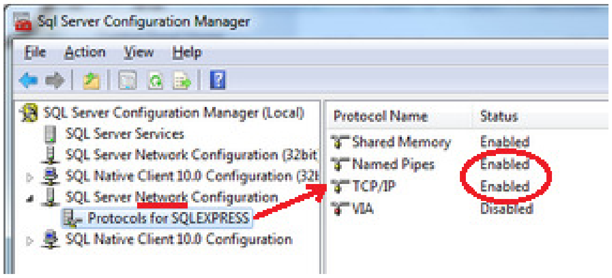
## Allowing remote connections to SQL Server (Janus professional only)

When you install SQL Server Express, the default settings will only allow programs on the same server or PC as the SQL Server instance to connect. With Janus Professional installations, we allow someone on another computer to connect. This requires some changes to SQL Server Express.

We describe here the SQL Server browser method to gain such access. Microsoft also provides alternative means, so you should consult your network administrator or database administrator or the Microsoft documentation for remote access on SQL Server before making any changes.

1. **Enable TCP/IP and Named Pipes on the network**

As described above, only localTCP/IP and named pipes were enabled. Now you will in addition also have to expand the SQL Server Network Configuration and enable TCP/IP and Named pipes there as well.

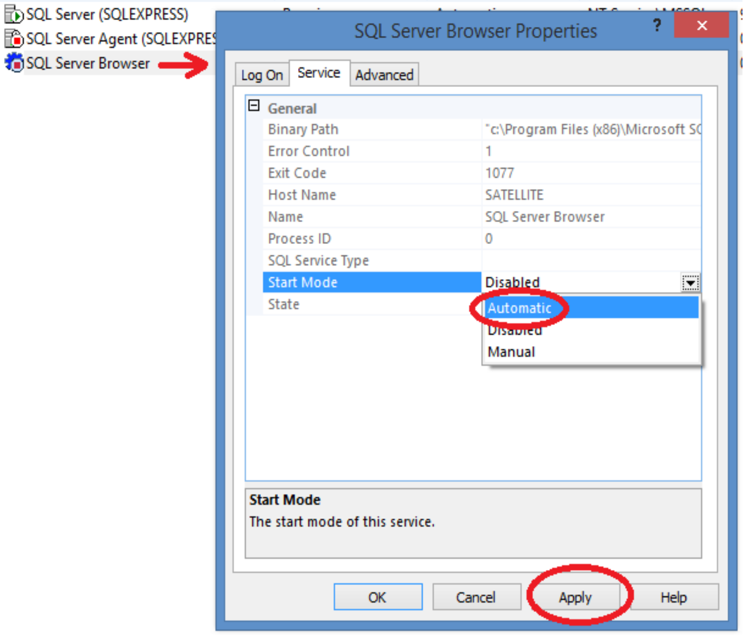


Sql Server Configuration Manager
File Action View Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 10.0 Configuration (32
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration

| Protocol Name | Status |
|---|---|
| Shared Memory | Enabled |
| Named Pipes | Enabled |
| TCP/IP | Enabled |
| VIA | Disabled |

2. **Turn on the SQL Server Browser.**

Using the same SQL Server Configuration Manager that we used to enable TCP/IP, double-click on the SQL Server Browser, as shown in the illustration below.

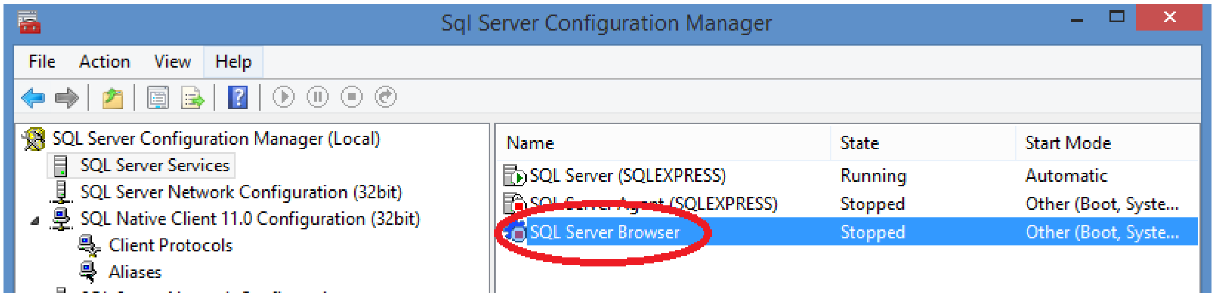


| | |
|---|---|
| Binary Path | "c:\Program Files (x86)\Microsoft SQ |
| Error Control | 1 |
| Exit Code | 1077 |
| Host Name | SATELLITE |
| Name | SQL Server Browser |
| Process ID | 0 |
| SQL Service Type | |
| Start Mode | Disabled |
| State | |

**Start Mode**
The start mode of this service.

In the window that then appears, select the “Service” tab, and then enable the service to start automatically when the machine starts up.

Then right-click on the SQL Server Browser line in the configuration tool, and in the popup menu select “Start”. The display should change from “Stopped” to “Started”.



SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 11.0 Configuration (32bit)
Client Protocols
Aliases

| Name | State | Start Mode |
|---|---|---|
| SQL Server (SQLEXPRESS) | Running | Automatic |
| SQL Server Agent (SQLEXPRESS) | Stopped | Other (Boot, Syste... |
| SQL Server Browser | Stopped | Other (Boot, Syste... |

**3. Allow SQL Server through the Windows Firewall**

* Start the Windows Control Panel, and at the bottom select “Windows Firewall”.

* Click “Allow a program through Windows Firewall”.

* Click “Allow another program”.

* Browse to sqlsrvr.exe [usually in C:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\Binn]. This location will vary, depending on the instance name you used during install, and also depending on the version of SQL Server.

4. **Allow SQL Server Browser through the Windows Firewall**

* Start the Windows Control Panel, and at the bottom select “Windows Firewall”.

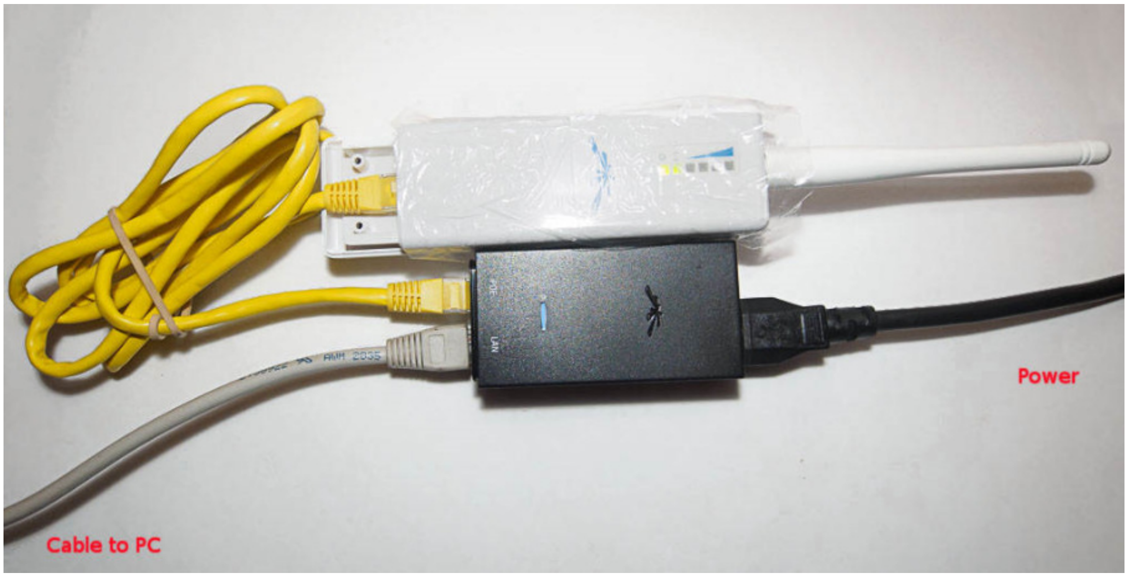
* Click “Allow a program through Windows Firewall”.

* Click “Allow another program”.

* Browse to sqlbrowser.exe [usually in C:\Program Files (x86)\Microsoft SQL Server\90\Shared, also for 64-bit installations].

## Annexure 3. Setup of wifi with the Ubiquity Picostation M2 HP

### Connecting



You will need two Ethernet cables (Cat-5) that are not supplied with the unit.

Connect one to POE socket on the black box, other end into the unit.

Connect other cable to LAN socket on black box, other end goes to PC (or a switch on the network).

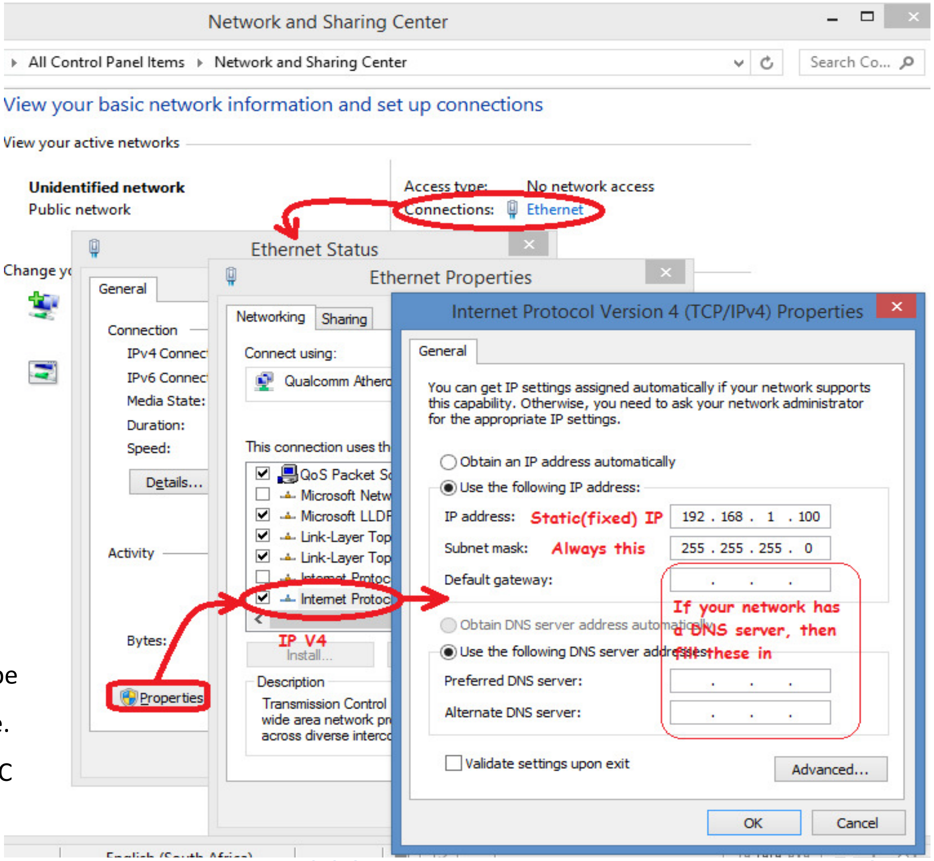
### PC Setup

Select Control Panel,

then network setup.

Give the PC a static IP address, and fill in the Subnet mask. For a single PC and Wifi, leave the gateway and DNS blank

If you have a network with a gateway and a DNS server, then your IT department or your network administrator will be able to give details for those. Then still a fixed IP for the PC is required.



Network and Sharing Center

All Control Panel Items ▸ Network and Sharing Center

View your basic network information and set up connections

View your active networks

**Unidentified network**
Public network

Access type: No network access
Connections: Ethernet

Ethernet Status

Connection
IPv4 Connec
IPv6 Connec
Media State:
Duration:
Speed:

Activity

Bytes:

Ethernet Properties

Connect using:
Qualcomm Athero

This connection uses th
☑ QoS Packet Sc
☐ Microsoft Netw
☑ Microsoft LLDP
☑ Link-Layer Top
☑ Link-Layer Top
☐ Internet Protoc
☑ Internet Protoc

Description
Transmission Control
wide area network pr
across diverse interco

Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit

Therefore, we set the following IP addresses for the PC:

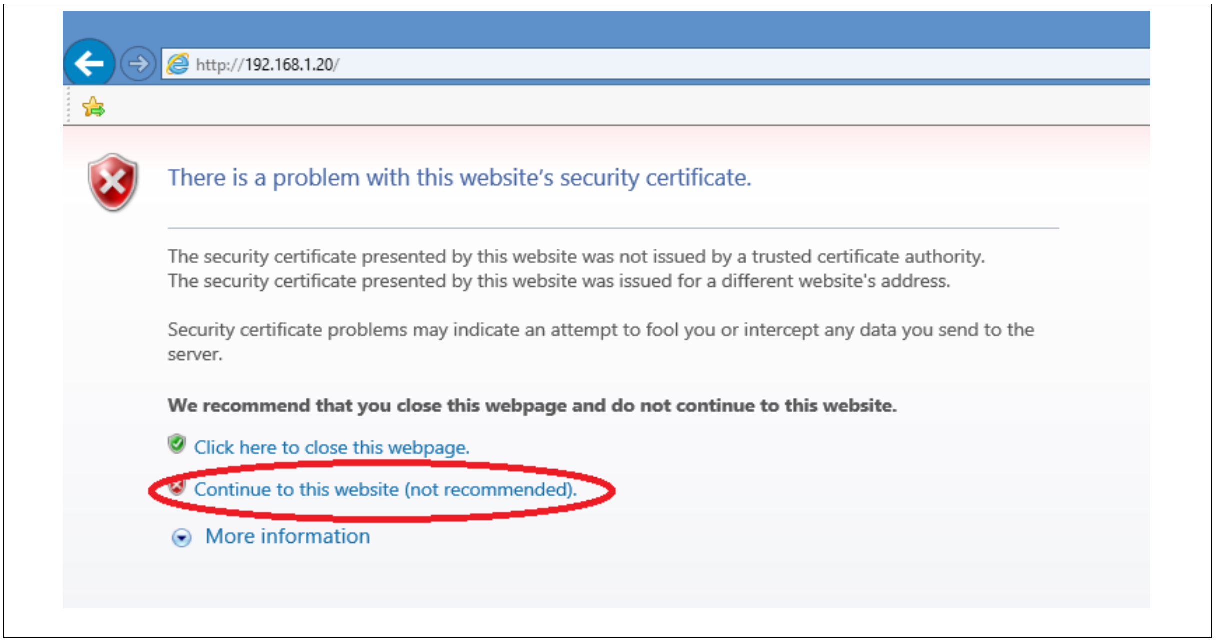
* PC must have a static IP address, use 192.168.1.100

* PC Subnet mask must be 255.255.255.0

## Picostation setup

Start Internet Explorer, point its address to the Picostation, i.e. [http://192.168.1.20](http://192.168.1.20)

If the browser warns about a security certificate, select to continue.



http://192.168.1.20/

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

**We recommend that you close this webpage and do not continue to this website.**

Click here to close this webpage.

Continue to this website (not recommended).

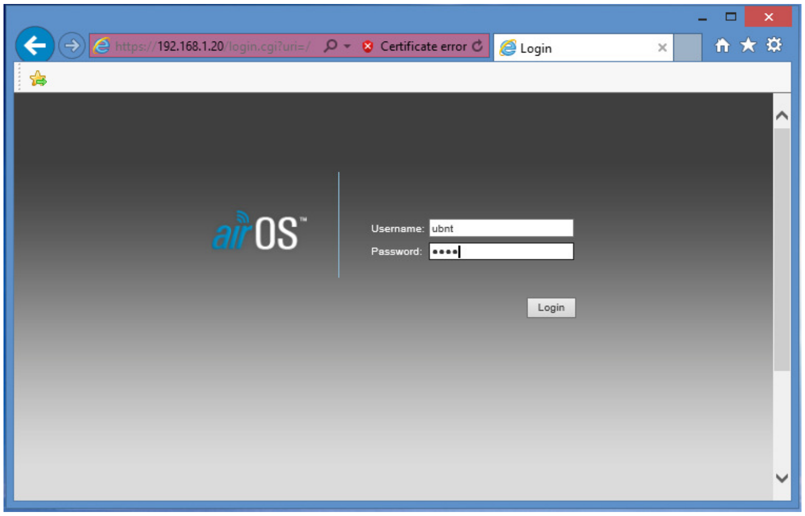
More information

Type the userid and password at the Picostation login window.

Default username: ubnt

Default password: ubnt

The screen may also ask to select your country and to accept terms and conditions.



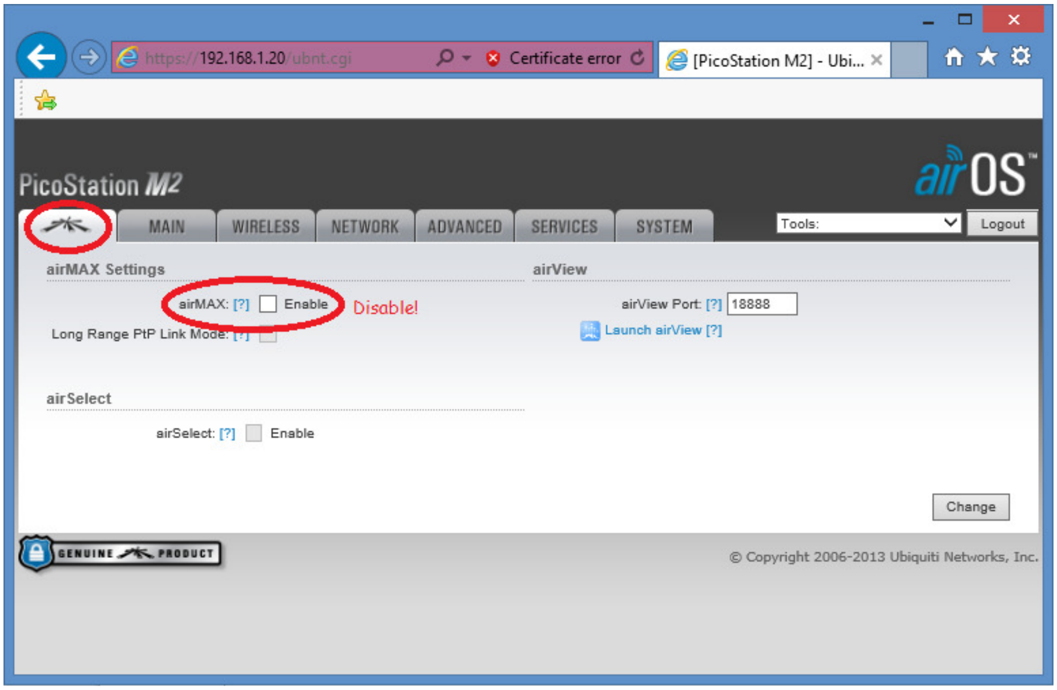
Username: ubnt

Password: ••••

Click login to access the configuration screen.

Select the leftmost tab on the top, left.

The AirMax setting must be disabled.  Click “change” to save settings for this screen.



airMAX Settings

airMAX: [?] □ Enable Disable!

Long Range PtP Link Mode: [?] □

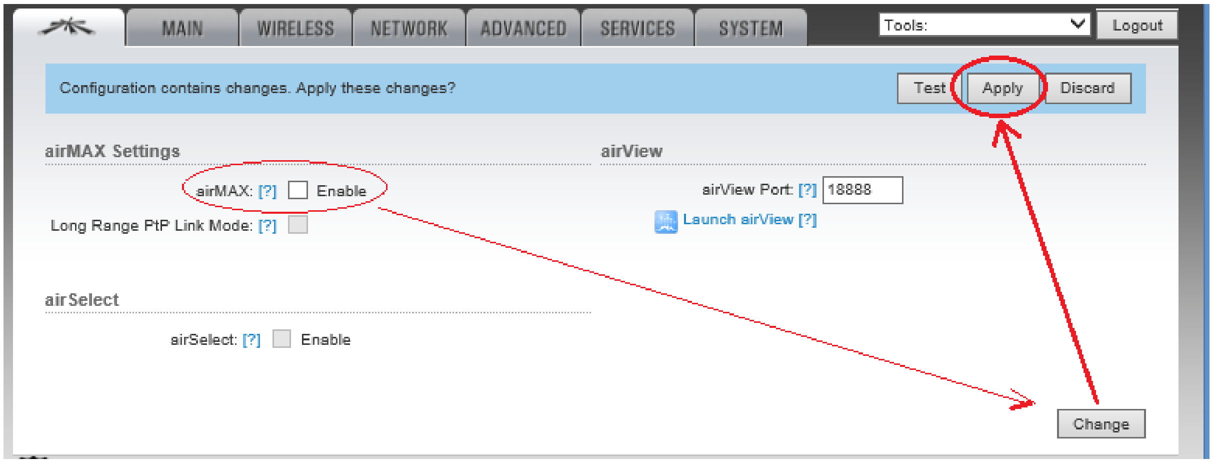
airView

airView Port: [?] 18888

airSelect

airSelect: [?] □ Enable

After clicking “Change”, you will notice a bar on which you must click “Apply”. Make sure you remember to the “apply” button after “change”, else the changes can be lost.



Configuration contains changes. Apply these changes?

airMAX Settings

airMAX: [?] □ Enable

Long Range PtP Link Mode: [?] □

airView

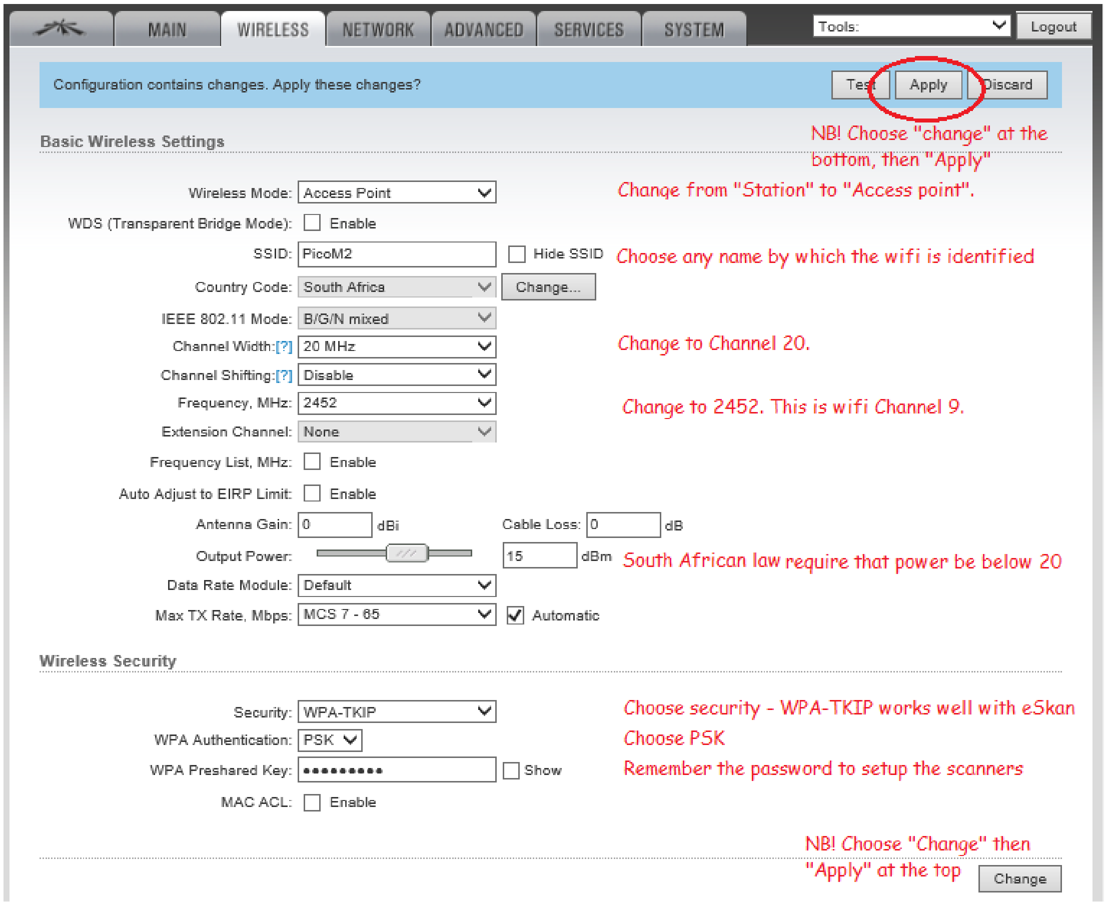
airView Port: [?] 18888

airSelect

airSelect: [?] □ Enable

Go to the “wireless” tab and set the Wifi settings as per the diagram below.

If the drop-down boxes are empty, your web browser's javascript feature is probably off. Temporarily enable javascript in the browser until the Picostation has been set up.  After changing the wifi settings, remember to click both the “change” button at the bottom and “Apply” at the top.



Configuration contains changes. Apply these changes?

NB! Choose "change" at the bottom, then "Apply"

Basic Wireless Settings

Wireless Mode: Access Point

Change from "Station" to "Access point".

WDS (Transparent Bridge Mode): □ Enable

SSID: PicoM2 □ Hide SSID

Choose any name by which the wifi is identified

Country Code: South Africa

IEEE 802.11 Mode: B/G/N mixed

Channel Width:[?] 20 MHz

Change to Channel 20.

Channel Shifting:[?] Disable

Frequency, MHz: 2452

Change to 2452. This is wifi Channel 9.

Extension Channel: None

Frequency List, MHz: □ Enable

Auto Adjust to EIRP Limit: □ Enable

Antenna Gain: 0 dBi Cable Loss: 0 dB

Output Power: 15 dBm

South African law require that power be below 20

Data Rate Module: Default

Max TX Rate, Mbps: MCS 7 - 65 ☑ Automatic

Wireless Security

Security: WPA-TKIP

Choose security - WPA-TKIP works well with eSkan

WPA Authentication: PSK

Choose PSK

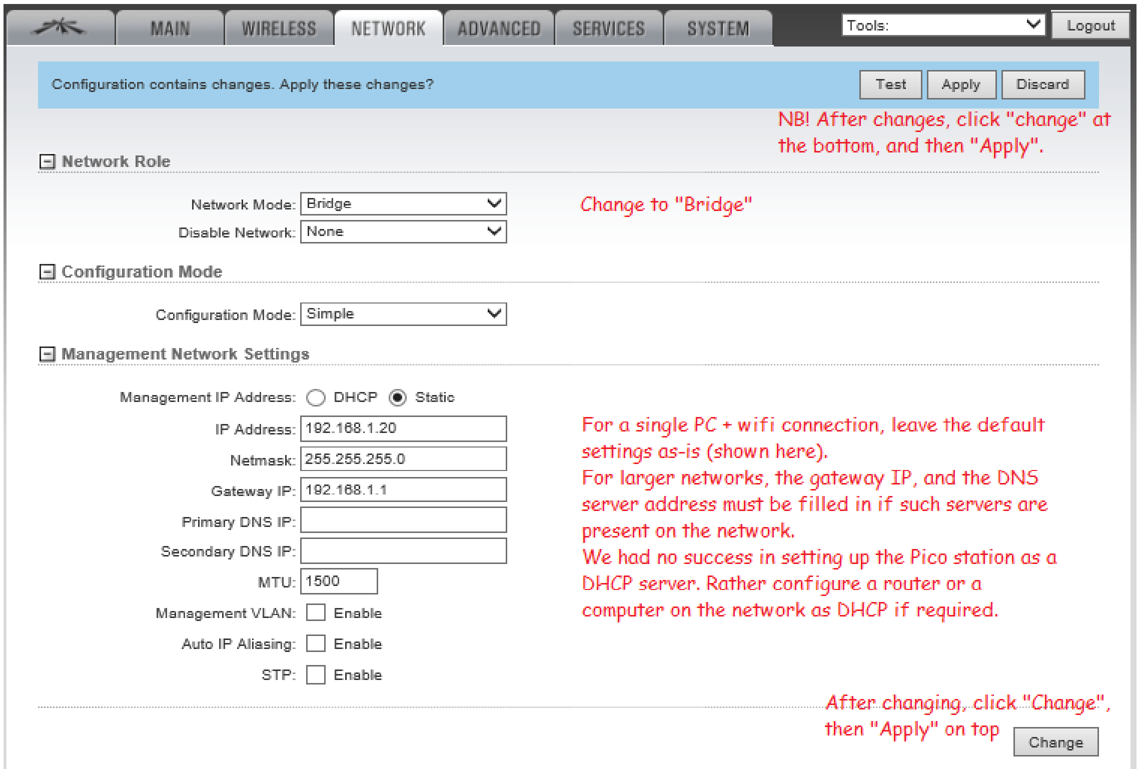
WPA Preshared Key: •••••••••• □ Show

Remember the password to setup the scanners

MAC ACL: □ Enable

NB! Choose "Change" then "Apply" at the top

Thereafter click on the network tab.



Configuration contains changes. Apply these changes?

NB! After changes, click "change" at the bottom, and then "Apply".

Network Role

Network Mode: Bridge

Change to "Bridge"

Disable Network: None

Configuration Mode

Configuration Mode: Simple

Management Network Settings

Management IP Address: ○ DHCP ● Static

IP Address: 192.168.1.20

Netmask: 255.255.255.0

Gateway IP: 192.168.1.1

Primary DNS IP:

Secondary DNS IP:

MTU: 1500

Management VLAN: □ Enable

Auto IP Aliasing: □ Enable

STP: □ Enable

For a single PC + wifi connection, leave the default settings as-is (shown here).
For larger networks, the gateway IP, and the DNS server address must be filled in if such servers are present on the network.
We had no success in setting up the Pico station as a DHCP server. Rather configure a router or a computer on the network as DHCP if required.

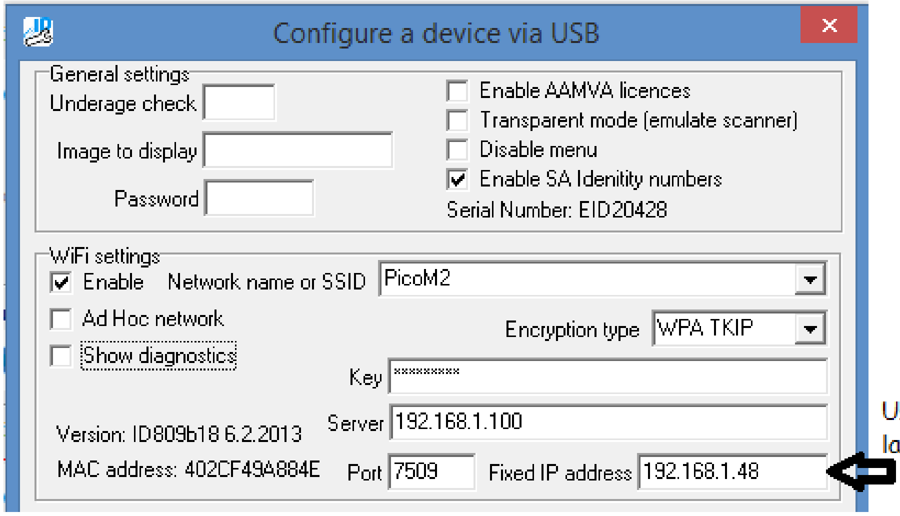
After changing, click "Change", then "Apply" on top

REMEMBER TO CLICK "CHANGE" AT BOTTOM THEN "APPLY" AT TOP OF SCREEN,

Go back to the first screen (leftmost tab) to check again that the "Airmax" setting is indeed off, as we described earlier.

On SYSTEM screen: enable the reset button (in case unit has to be reset), and disable Check for Updates.

Scanners can be programmed as follows (see eID manual for full instructions)



Configure a device via USB

General settings

Underage check

Image to display

Password

☐ Enable AAMVA licences

☐ Transparent mode (emulate scanner)

☐ Disable menu

☑ Enable SA Idenitity numbers

Serial Number: EID20428

WiFi settings

☑ Enable  Network name or SSID: PicoM2

☐ Ad Hoc network

Encryption type: WPA TKIP

☐ Show diagnostics

Key: **********

Version: ID809b18 6.2.2013

Server: 192.168.1.100

MAC address: 402CF49A884E

Port: 7509

Fixed IP address: 192.168.1.48

Use a convention like the last 2 digits of the scanner ID for IP address.

--------------------o0o--------------------