

Installation and Configuration Guide

netMatrix Xsite Time&Attendance



Time&Attendance

All rights reserved by XPECTRA Remote Management 2019
The total or partial reproduction of this Guide is prohibited, by any
means, without the written consent of XPECTRA Remote
Management

Installation and Configuration Guide

netMatrix Xsite Time&Attendance

Reviews of the Guide

When contacting the Technical Support personnel of **XPECTRA Remote Management** in reference to this Guide, be sure to include the following information:

TITLE OF THE GUIDE: Installation and Configuration Guide netMATRIX Xsite Time&Attendance.

Edition	Date	Description of changes	Software Versions
1 st Edition	31/05/2019	New edition. It corresponds to version 7 in Spanish.	netMATRIX 6.1.2.0 incluye Xsite 1.0.0.0

Content

Chapter 1. Introduction	6
Objective of the Guide _____	7
Solution general architecture _____	7
Who must read this Guide? _____	8
Assistance	8
Conventions used in this Guide	8
Topics in each Chapter	8
Selections of buttons and menus	8
Content of the Package _____	9
Service and Applications Server Requirements _____	9
Database Server Requirements _____	9
 Chapter 2. - Preparation of the Services and Applications Server	 10
Minimum Hardware and Software Requirements of the Services and Applications Server _____	11
Power Feed _____	11
2.1 Server installation and configuration process _____	12
2.1.1 Installation and activation of the IIS service	12
2.1.2 XsiteBack configuration	15
2.1.3 XsiteFront Configuration	21
2.1.4 Procedure to be followed in case of type files JSON are non-visible	23
2.1.5 Process of configuring the routing towards the IIS server in case of not using the biometric device	24
 Chapter 3. - Preparation of Database Server	 26
Minimum requirements of Hardware and Software of the server's database.	27
Procedure to restore the local netMATRIX database. _____	27
 Chapter 4.-netMATRIX Desktop-Work station type 1	 35
Minimum Hardware and Software Requirements Work station type 1 _____	36

NetMATRIX desktop installation process	36
Select the _____	36
Chapter 5. Configuration of the ODBC of netMATRIX	40
Step by Step Configuration _____	41
General Description	41
Preliminary conditions	41
ODBC Configuration of netMATRIX _____	41
Chapter 6.- Configuring the netMATRIX Platform	55
Setting up the branch in netMATRIX _____	60
Configuring schedules in netMATRIX _____	64
Staff configuration in netMATRIX _____	66
User configuration in netMATRIX _____	71
Equipment configuration in netMATRIX. _____	72
Chapter 7.- Services in the Type 2 and Type 3 Work Stations (use mode with biometric device)	75
Minimum Hardware and Software Requirements for Type 2 work station ____	76
Minimum Hardware and Software Requirements for Type 3 work station ____	76
Process of installation of the services in work stations Type 2 and Type 3 (Installation Attended) _____	77
Process of installation of the services in work stations type 2 and 3 (Unattended Installation) _____	82

Chapter 1. Introduction

Objective of the Guide

This Guide describes the procedures carried out for the installation and configuration of the **Xsite Time & Attendance** solution, specifically designed to manage employee assistance to the workplace in an organization. Installation and configuration changes according to the modality of use of **Xsite Time & Attendance** solution: with Biometric or Non-biometric.

Solution general architecture

Figure 1 shows the general architecture of the solution with all the possible elements involved. The element associated with the locality (in the left part of Figure 1) is required only in the modality with a biometric device

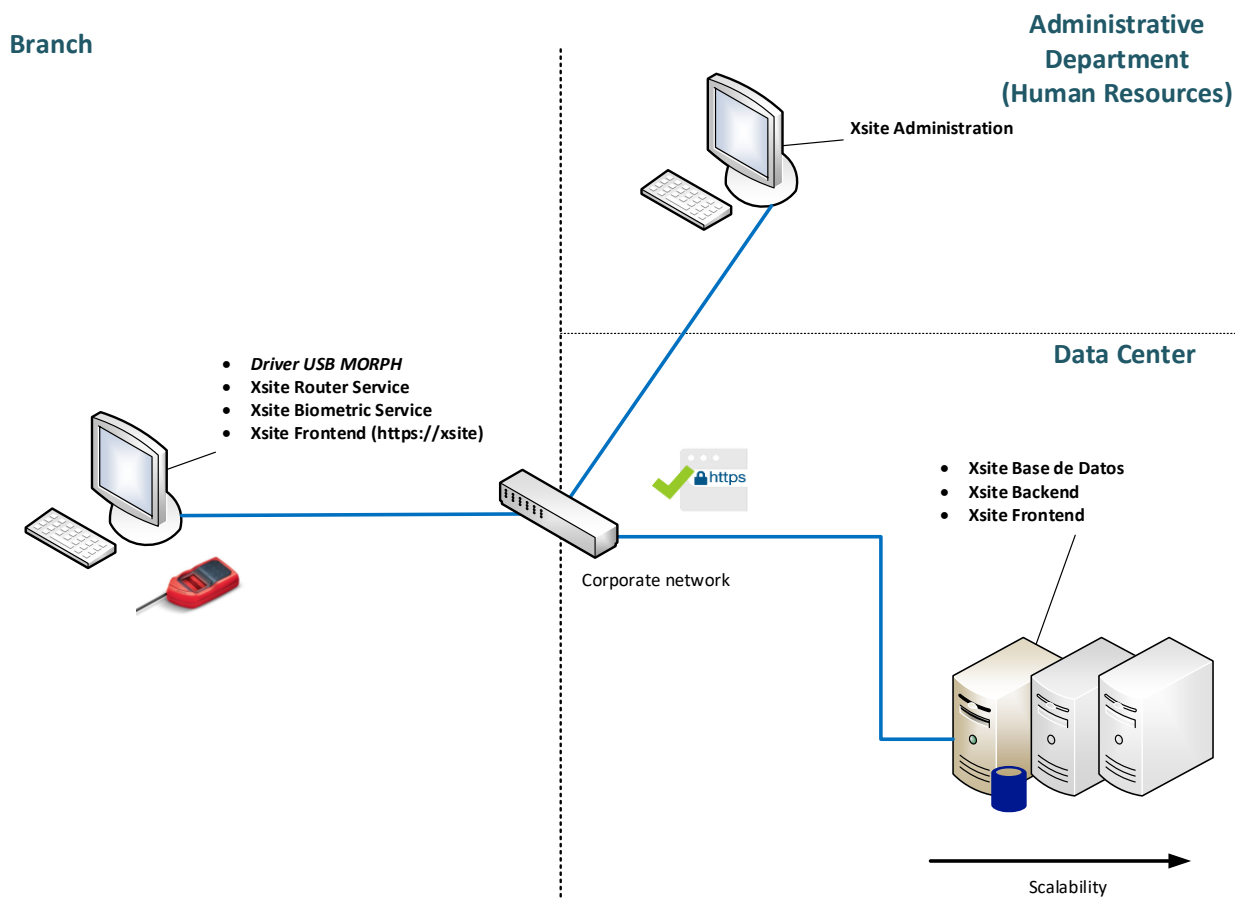


Figure 1. - Solution general architecture

Who must read this Guide?

If you have basic knowledge of Microsoft Windows and are comfortable with systems and database configuration processes, in this Guide you will find the additional information that you need to understand the installation process of **Xsite Time&Attendance**. "Step by step" procedures have been included for the use of each one of the functionalities of the system guaranteeing the user a better understanding. ***If you aren't familiar with Microsoft Windows environment, please review your Windows documentation.***

Assistance

If you need more information, refer to the online help or contact our technical support representative via the e-mail: soporte.tecnico@xpectra.com, who immediately will assist you. Our technical Support Group will be pleased to work with you to resolve any questions or problems.

You can also get more information about our products on the website: www.xpectra.com.

Conventions used in this Guide



ALERT: Every time you see a yellow triangle with an exclamation mark, it will indicate that there is a notice of attention or alert. The information marked with this icon could prevent the loss of data, serious handling errors, etc. The paragraph will always start with the word **ALERT** in **bold** capitals

NOTE: When you find a shaded gray frame, this will have additional useful information for the user of the Guide. The paragraph will start with the Word **NOTE** in **bold** capitals.



This icon will indicate an idea or special *tip* related with the subject matter.

Topics in each Chapter

When starting each Chapter the most important issues will be exhibited. The objective is to present information to the user in an organized manner. Selections of buttons and menus

Selections of buttons and menus

When it is required to use any menu or button in the application, the instruction will be written in **bold**. The menu selections will be separated by a *slash* (/) and made up of the names of the items that you must select. They will also be written in **bold**.

For example: ***c:/programData/Xpectra/Netmatrix6/XSITE/Enrutamiento/***

Content of the Package

- 1.** netMATRIX database
2. netMATRIX desktop
3. Xsite-Servicios Setup
4. Folders with Backend and Frontend XSite files for IIS
5. Folder Herramientas Xsite
6. Folder Herramientas

Service and Applications Server Requirements

- 1.** IIS installed and activated.
- 2.** Core Windows Server Hosting installed.
- 3.** Microsoft URL Rewrite Module for IIS installed.

Database Server Requirements

- 1.** Microsoft SQL Server 2012 Enterprise Edition **installed**

Type 2 Workstation Requirements

- 1.** Fingerprint Drivers installed. Only necessary for the modality with biometric device.

Chapter 2. - Preparation of the Services and Applications Server

Minimum Hardware and Software Requirements of the Services and Applications Server

Requirement	Description
Operating System	Windows Server 2012 Enterprise
Processors	Intel Xeon Processor E5-4650 v3
Memory RAM	16 GB RAM
Hard Drive	50 GB DD
Servidor Web	IIS 8.0
XSite	Backend and Frontend XSite
Others	Communications Server netMATRIX 6.1.1.0



ALERT: The installation of the application makes changes in the configuration of the system, such as the registration of some components and/or DLL files, therefore, this installation is required to be carried out under an administrator account that has all the rights of users required to perform this task, otherwise, the installation may generate errors and some software elements may not work correctly..



Power Feed

It is strongly recommended that an Uninterruptible Power Supply is used (UPS) in the computer where the application operates, since the same not only protects the equipment of possible alterations of voltage coming from the main electric network, but also provides complete isolation between the computer and the AC network. In addition, it guarantees a battery backup that allows the correct closing of the applications that may be running.

2.1 Server installation and configuration process



Alert: The following components are found in the installation package: **Core Windows Server Hosting, Microsoft URL Rewrite Module for IIS**, in the following path: Paquete de Instalación/ Herramientas / Herramientas Xsite. It is essential to have these components previously installed to successfully perform the configurations below.

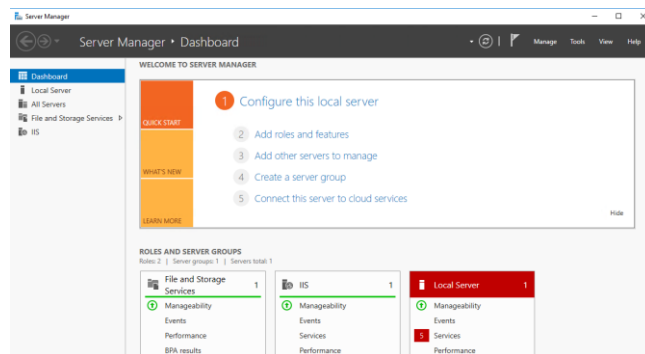
<input type="checkbox"/> Name	Date modified	Type	Size
 rewrite_amd64	11/10/2016 5:01 PM	Windows Installer ...	6,128 KB
 DotNetCore.1.0.0.RC2-WindowsHosting	11/10/2016 5:00 PM	Application	41,225 KB

2.1.1 Installation and activation of the IIS service

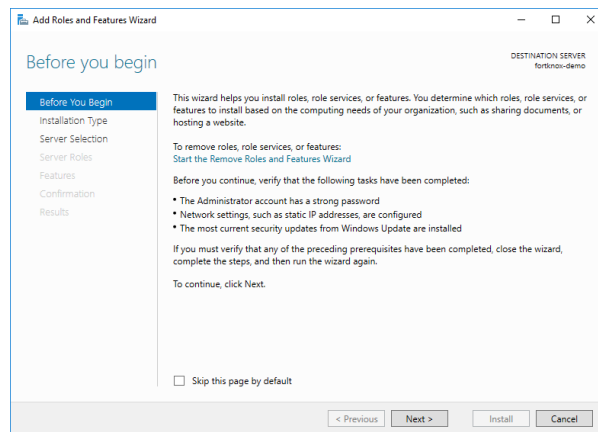
Verify that **Internet Information Services (IIS)** is installed and enabled on the server

Perform the following steps for verification:

Step 1: **Start the Server Manager.**

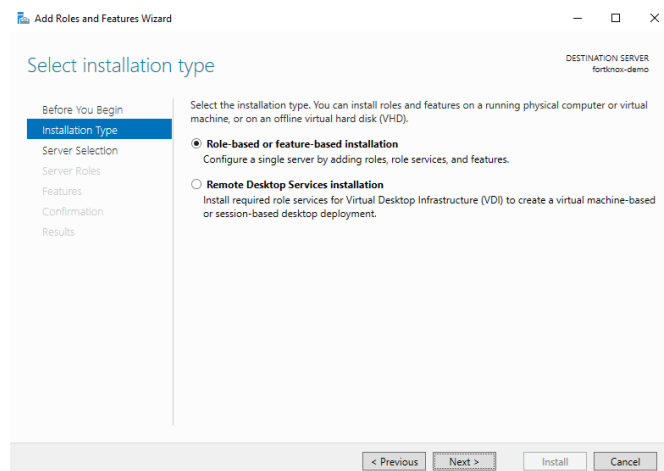


Step 2: **Enter Server Manager.** Click on **"Add roles and features"**.
Click **"Next"**.



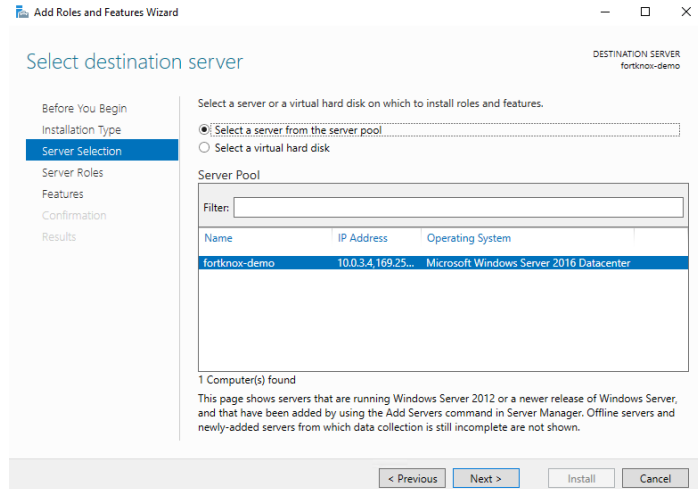
Step 3: Choose the type of installation.

Select **"Role-based or feature-based installation"**. Click **'Next'**.



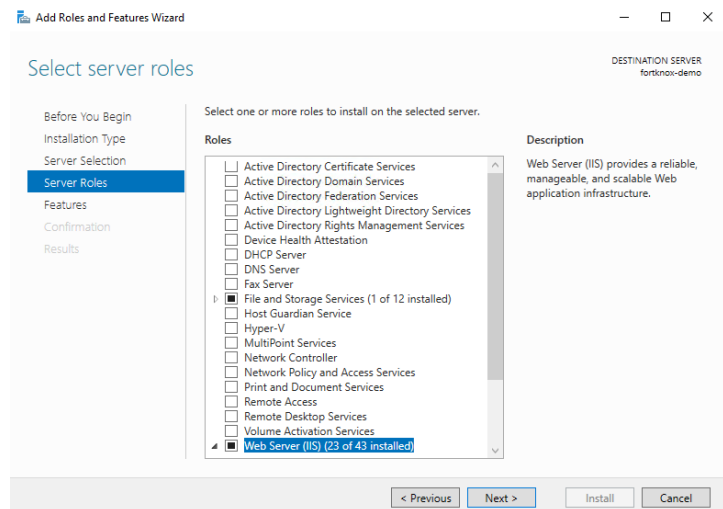
Step 4: Select the appropriate server.

Select the appropriate server. By default, you must select the local server. Click **'Next'**.



Step 5: Verify that IIS this enabled.

Verify that the option WEB server (IIS), is checked, it indicates that the IIS is **installed and active**. Otherwise you must tick the option and press "**Next**" so that the necessary components are installed.



NOTE: Once verified that the **IIS** is active, must perform the configuration of the sites in **IIS Manager**

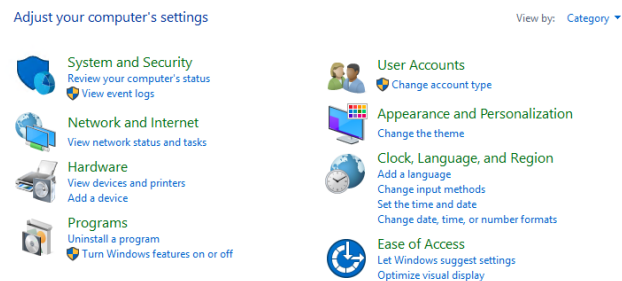
2.1.2 XsiteBack configuration

You must create the web site Xsiteback in the Internet Information Services (IIS) as part of the process of configuration of the applicative Xsite.

NOTE: In this chapter you will use the files provided in the installation package folder /Xsite Attendance/xsiteback which should be copied to **C:\\inetpub\\wwwroot**

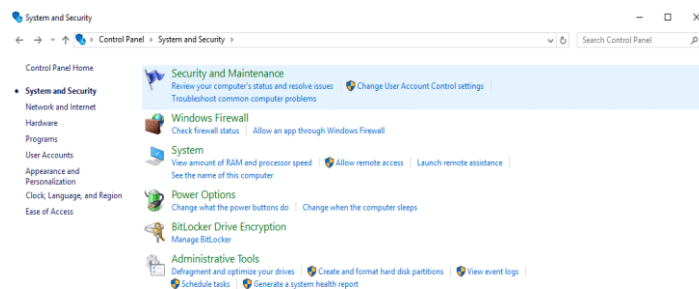
Step 1: Log in to Control Panel.

Go to control panel and select the option "**System and Security**".



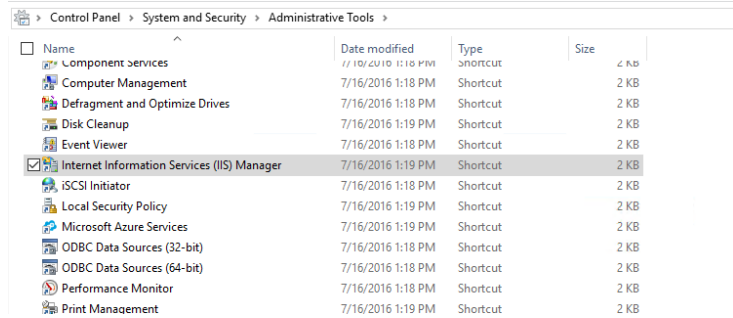
Step 2: Log on to system and security.

In the system and security section, locate the **Administrative Tools** option, and then click.



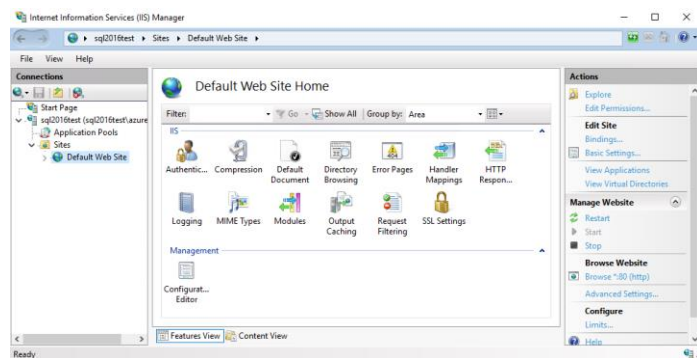
Step 3: Access to the Internet Information Services (IIS) Manager.

Select **Internet Information Services (IIS)** Manager



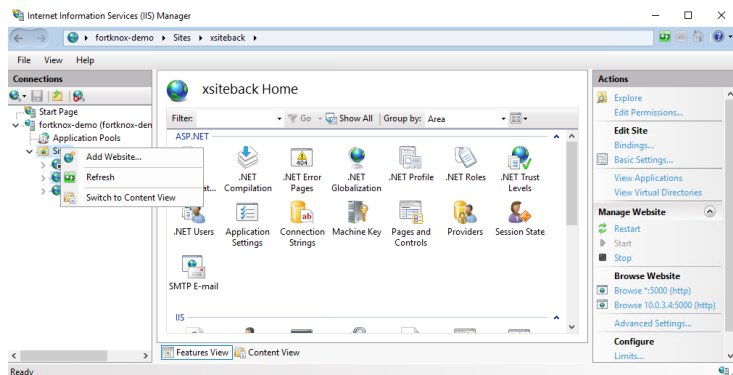
Step 4: Stop the site Default Web Site.

Once inside IIS Manager, select **Default web site** and press the **"Stop"** button.



Step 5: Log in to add web site.

Locate the folder **Sites** and with the right button of the mouse, deployment context menu and select the option **"Add website"**.

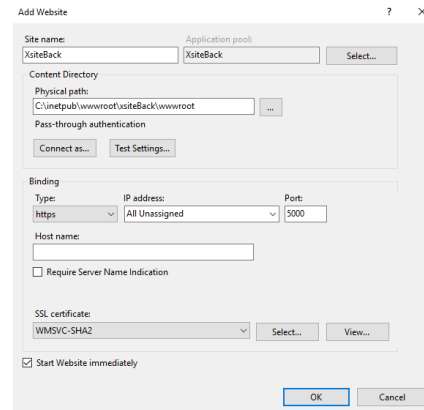


Step 6: Set the name to Xsiteback.

In the expanded form:

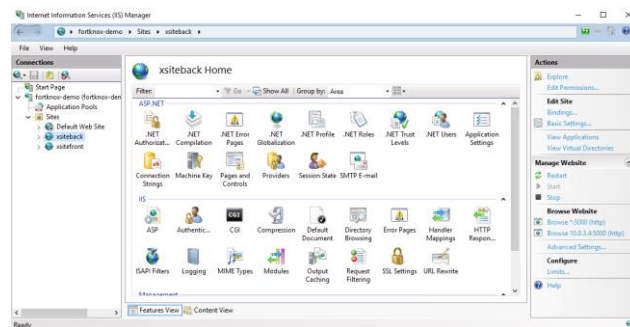
- Set the Name of the site, in this case it is **Xsiteback**,
- Place the path where the application files were previously copied in the physical path:

- **C:\inetpub\wwwroot\XsiteBack\wwwroot,**
- Select the type of link **https,**
- Set to port **5000** and
- Select the SSL certificate to use for the app.
- Select **"OK"**



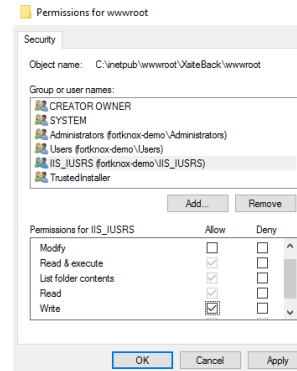
Step 7: **Edit the permissions of the added website.**

Edit the permissions of the added **website**, follows: choose the site with the name **XsiteBack** and click on the **"Edit permissions"** option.



Step 8: **Assign write permissions.**

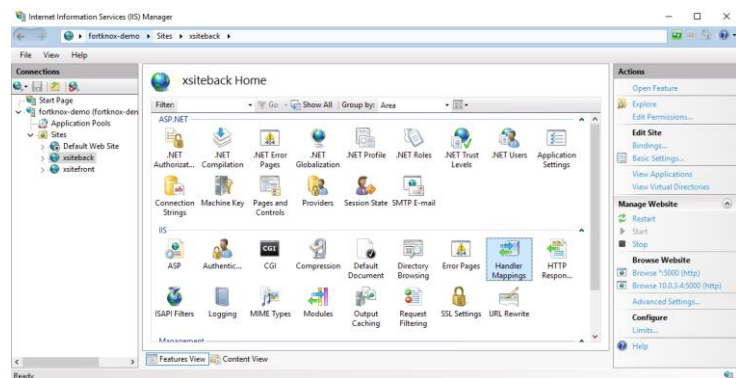
Select **IIS_IUSRS** and assign write permissions. Select **"OK"**



NOTE: This step is important because it allows the IIS_IUSRS user has permissions on the directory from XsiteBack, this permissions are required to allow the creation of attachments, at the site, and the activation of the downloading application functionality.

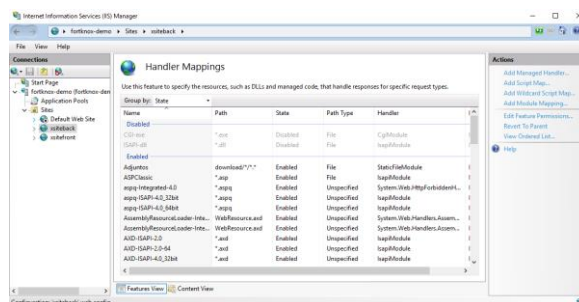
Step 9: Create the path Mapping of module.

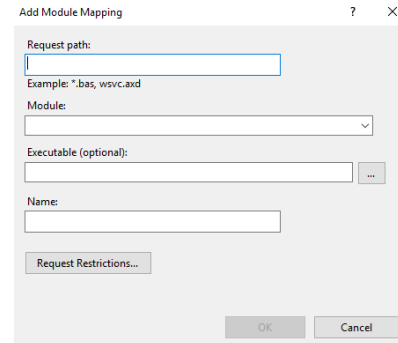
Select the site **Xsiteback** and the **"Handler Mappings"** option.



Step 10: Add the module's allocation.

Once inside of **"Handler Mappings"**, select the option **"Add Module Mapping"**.





Add Module Mapping

Request path:

 Example: *.bas, wsvc.axd

Module:

Executable (optional):
 ...

Name:

Request Restrictions...

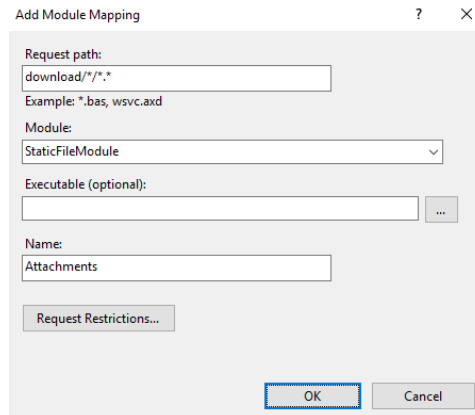
OK Cancel

Step 11: **Set configuration of module's allocation.**

Fill out the form with the following information:

- Request path: **download/*/*.***
- Module: **StaticFileModule**
- Name: **Adjuntos**

Press '**Ok**' to continue.



Add Module Mapping

Request path:

 Example: *.bas, wsvc.axd

Module:

Executable (optional):
 ...

Name:

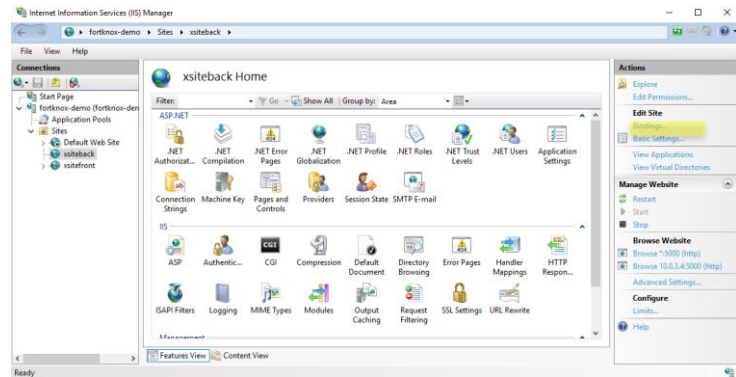
Request Restrictions...

OK Cancel

NOTE: Steps 9, 10 and 11 sets the path where are downloaded the attached files generated by the application. If this route is not enabled, it will not be possible to download the reports requested by the user of the application.

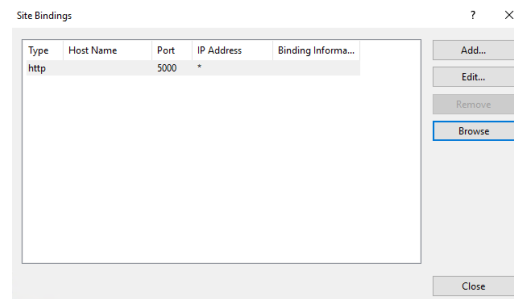
Step 12: **Link the Site Bindings Back.**

Select the created site **Xsiteback**, then choose "**Bindings**".



Step 13: Add the link of the site.

Press "**Add**", in the form **Site Bindings**.

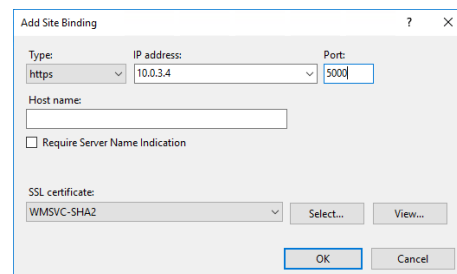


Step 14: Configure the Site link.

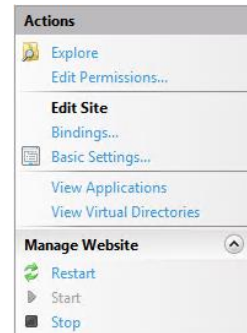
In the form **Add Site Binding**:

- Set "**https**" link type,
- Set the ip address "**server ip**",
- Set to port **5000**, and
- Choose the SSL certificate to be used.

Press '**OK**' to continue.



After assigning the IP address of bonding, you must stop the site, click on the option "**Stop**" and then click in the option "**Start**" to start the site on the new IP.



2.1.3 XsiteFront Configuration

As part of the adapting process of the Xsite application, the Xsitefront website must be created in the **Internet Information Services (IIS)**

NOTE: In this chapter will be used the files supplied in the package, folder, installation/Xsite Attendance/xsitefront, which should be copied to **C:\\inetpub\\wwwroot\\client**

Step 1: Create the site FrontEnd in IIS.

Locate the folder sites, with the right button of the mouse to display the shortcut menu, select the option **"Add Website"**.

In the expanded form set the **Site name**, in this case it is **XsiteFront**, place the path where the application files were previously copied in the physical path:

C:\\inetpub\\wwwroot\\client,

Select the type of link **https**, set to port **80** and choose the SSL certificate to use for the app.

Add Website

Site name: Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

Type: IP address: Port:

Host name:

☐ Require Server Name Indication

SSL certificate:

☒ Start Website immediately

Step 2: Link and assign the Site Bindings Front.

Locate the created site **Xsiteback** and select the **"Enlaces"** option (see step 12 and 13 of section 2.1.2).

Step 3: Assign the IP address.

In the pop-up window:

- Set the link **Type** to **"https"**,
- Enter server Ip address in **IP Address**,
- Enter the port **443** value and
- Select the SSL certificate.
- Then, stop the site, press **"Stop"** and then **"Start"** to start the site with the new configuration, in the right bar of Options of IIS Manager.

Binding

Type: IP address: Port:

Host name:

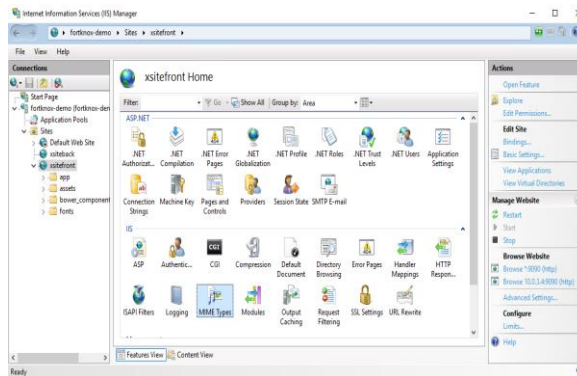
☐ Require Server Name Indication

SSL certificate:

☒ Start Website immediately

Step 4: Configure the allowed file types on the site.

Click on the website **Xsitemfront**, to deploy Main Page, select "**MIME Types**" and double click on it. Validate if the .json extension may be seen in the list.



MIME Types

Use this feature to manage the list of file name extensions and associated content types that are served as static files by the Web server.

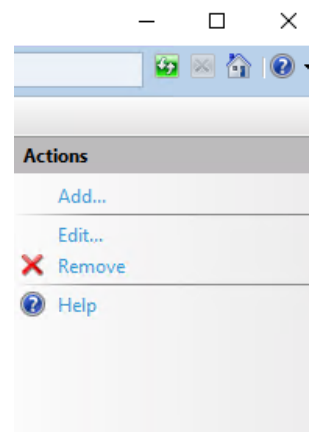
Extension	MIME Type	Entry Type
.jpeg	image/jpeg	Inherited
.jpg	image/jpeg	Inherited
.js	application/javascript	Inherited
.jsonld	application/ld+json	Inherited
.jsx	text/jsxscript	Inherited
.latex	application/x-latex	Inherited
.less	text/css	Inherited
.lit	application/x-ms...	Inherited
.lpk	application/octet...	Inherited
.lsf	video/x-la-asf	Inherited
.lsx	video/x-la-asf	Inherited
.lzh	application/octet...	Inherited
.m13	application/x-ms...	Inherited
.m14	application/x-ms...	Inherited
.m1v	video/mpeg	Inherited
.m2ts	video/vnd.dlna.m...	Inherited
.m3u	audio/x-mpegurl	Inherited
.m4a	audio/mp4	Inherited

NOTE: If the types JSON non-visible should be the procedure described below.

2.1.4 Procedure to be followed in case of type files JSON are non-visible

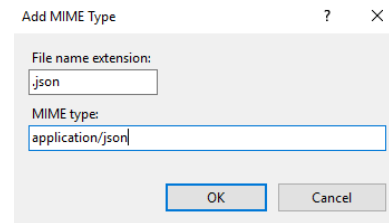
Step 1: Add MIME type.

From the main page of the site, in the right pane, click the "**Add**" tab.

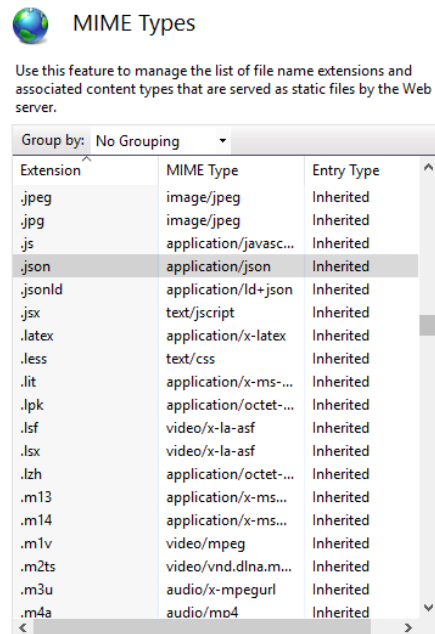


Step 2: Name the file.

Enter in **File name extension:** **.json** and Enter en **MIME type:** **application/json**, Then press "**Ok**".

**Step 3: Verify the file.**

After adding the MIME type, verify that appears in the list the **.json** extension and restart the IIS.



NOTE: From this configuration, the site will have the ability to interpret documents with extension JSON

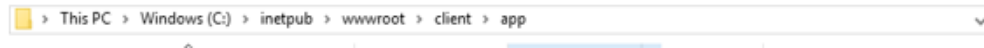
2.1.5 Process of configuring the routing towards the IIS server in case of not using the biometric device

NOTE: This procedure only applies to the case of not using the biometric device.

Step 1: Access the client folder.

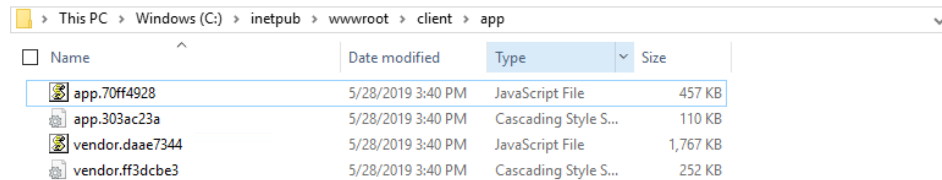
Enter the following path:

C:\inetpub\wwwroot\client\app



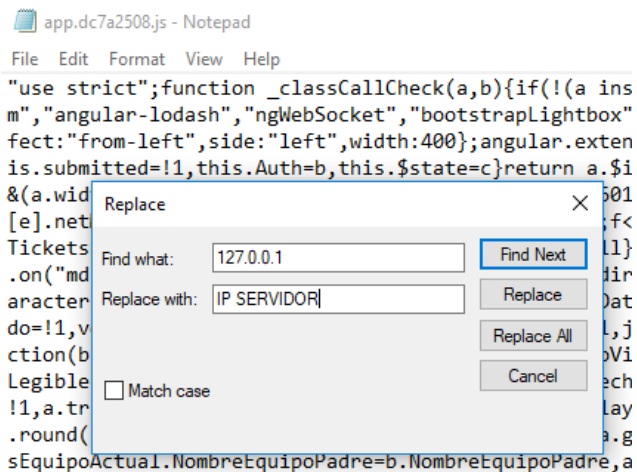
Step 2: **Locate and select the file.**
 .Json.

Locate the folder, select the JS file with name **app.abcd123** (this file can change name keeping the letters app)



Step 3: **Edit the file and replace IP server.**

Open file **app.abcd123** with Notepad and replace the **IP 127.0.0.1** for the ip of the server.



Step 4: **Save the file.**

Once replaced the ip address, save the file, press the **"Replace"** option

Chapter 3. - Preparation of Database Server

Minimum requirements of Hardware and Software of the server's database.

Requirement	Description
Operating System	Windows Server 2012 Enterprise
Processors	Intel Xeon Processor E5-4650 v3
Memory RAM	16 GB RAM
Hard Drive	250 GB DD
Software Additional	SQL Server 2012 Enterprise Edition
Database	netMATRIX

Procedure to restore the local netMATRIX database.

This section explains how to restore the netMATRIX database and associate the corresponding login.

NOTE: The configuration shown below responds to default values to configure the netMATRIX database. If required, these values can be customized.

Step 1: **Open the
SQL Server
2012
Administrator.**

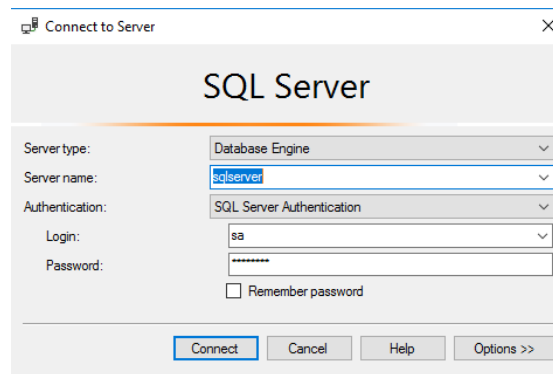
Select the **Star/SQL Server Management Studio** menu to open the Database administration application.



Step 2: **Select the
server to
restore the
database.**

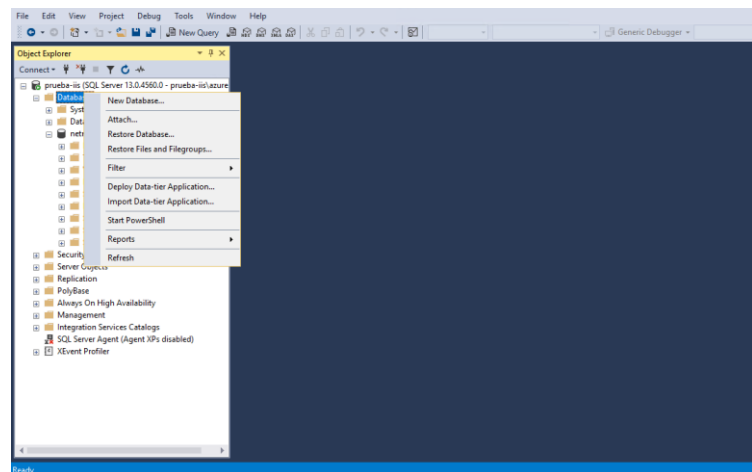
In the window that appears, select or write values in each field as indicated below:

- In the "**Server Name**" field, type the name of the Database Server where the local netMATRIX database is installed.
- In the "**Authentication**" field, select the option "**SQL Server Authentication**".
- Enter the **Login** and **Password** that has been provided by the database administrator of your organization.
- Finally click on the "**Connect**" Button.

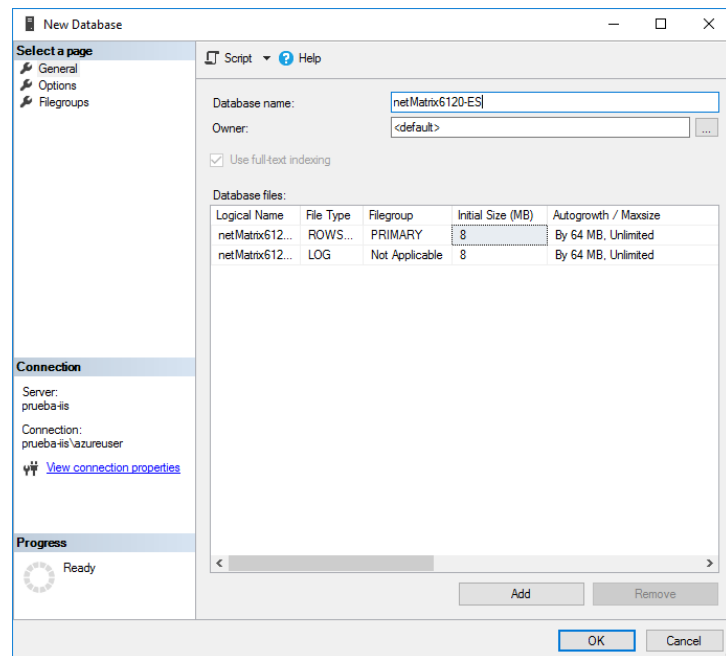


Step 3: Create the netMATRIX Database.

Click on the right button of the mouse on the **"Database"** folder of the menu that is displayed, select the option **"New database"**, as shown in the following figure:



In the window that appears, indicate the name of the database to be created and then press the **"Ok"** button. You can also modify the paths of the Data files and the Transaction Log files.

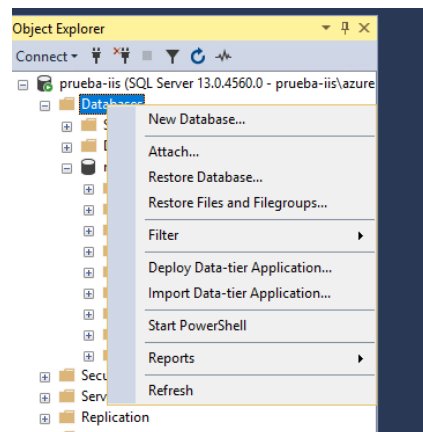


NOTE: It is recommended that the name of the database be netMATRIX.

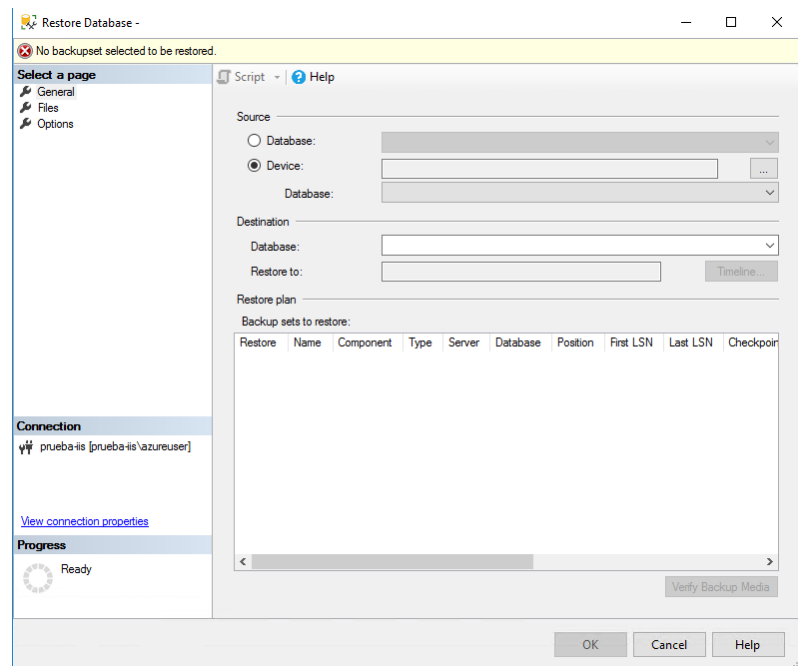
Step 4: Restore the netMATRIX Database.

To complete the installation of the database, you must mount the structure and default data of the Database; is done from the ".bak" file of the database to be restored.

For this task, right click on the database, a menu of options will be displayed, select the option "**Restore Database**".

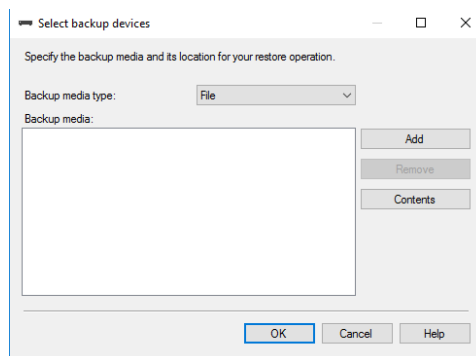


On the **General** page, select "**Device**" option and locate the database file.

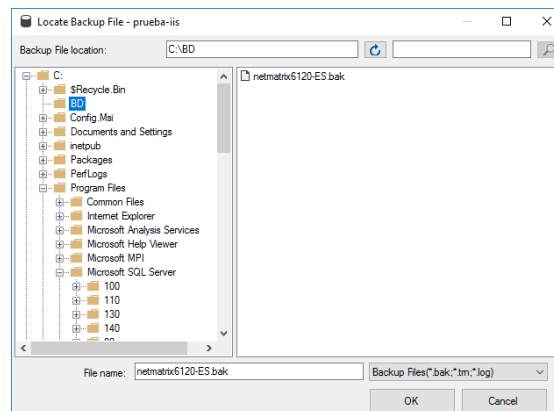


NOTE: The file to be restored is located on the installation package that XPECTRA will provide. You must know the directory where it is located.

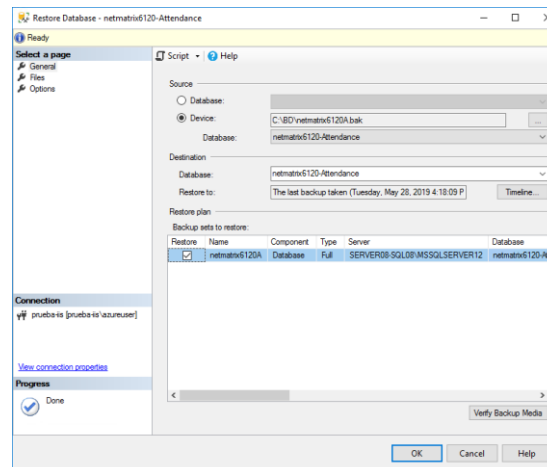
Several windows will appear for the selection of the file to be restored. In the first window that is displayed "**Select backup devices**", click on the "**Add**" button.



In the next window "**Locate Backup File**" look for the restoration file, select it and press the "**OK**" button in the next windows.

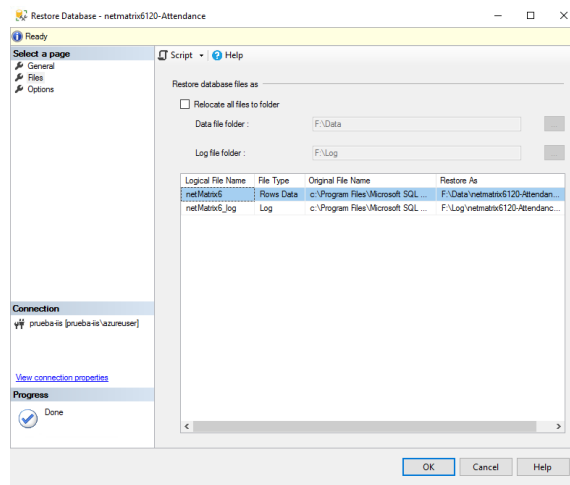


In the "**Backup Sets to restore**" area, check the corresponding database to be restored.



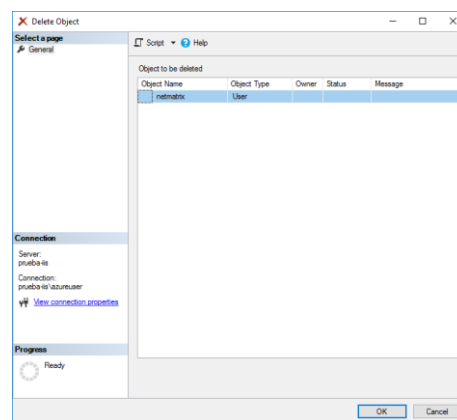
Select the "**Files**" page and indicate the path of the data and log files of the database. You can keep the default route or modify it if necessary.

Press the "**OK**" button to start the process.



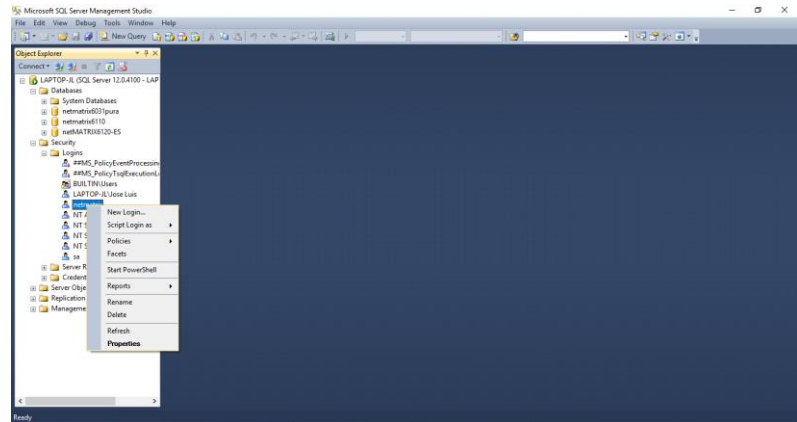
At the end of the process, a message will be displayed indicating that the restoration of the database has been successful. Press the "**Ok**" button to continue.

In the tree, look for the database created and go to "**Security > Users > netMATRIX**", click with the right mouse button on this folder, select from the menu displayed the "**Delete**" option and press "**Ok**".



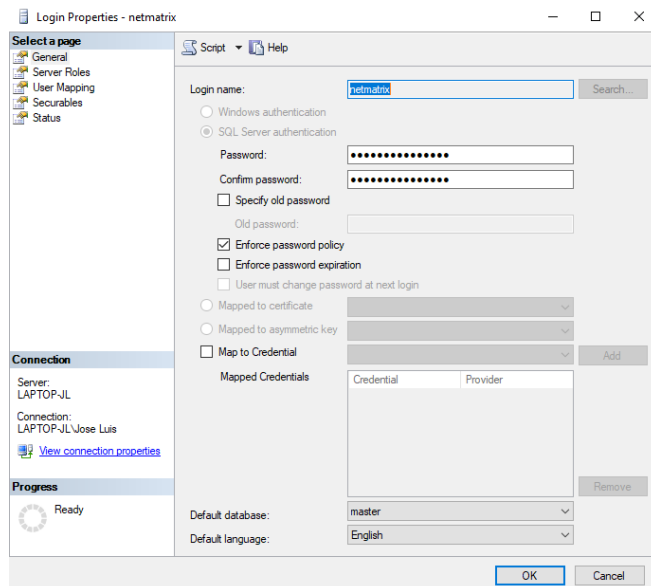
Step 5: Create database user.

- Locate the "**Security > Login > netMATRIX**" folder in the right pane of the "**SQL Server Management Studio**" window.
- Click with the right mouse button on this folder and select from the menu that the "**Properties**" option is displayed.



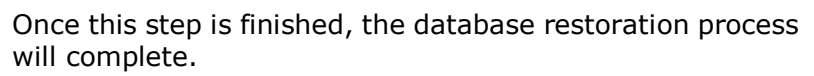
In the window that is presented, configure the user data to be created, as indicated below:

- In the "**Login name**" field enter "netMATRIX" or the user name assigned by the database administrator.
- Select the option "**Authentication of SQL Server**" and enter in the fields "**Password**" and "**Confirm Password**" the word systems or the key given to the user created by your organization.



Locate the **User Mapping** page, select the restored database, and assign the permissions "public", "**db_datawriter**" and "**db_datareader**".

Then press the "**OK**" button.



Chapter 4.-netMATRIX Desktop-Work station type 1

Minimum Hardware and Software Requirements Work station type 1

Type 1 workstations, include the software required by the solution to implement the netMATRIX 6 desktop, from which the functions of platform: configuration, database administration and request for reports, will be carried out nationwide.

For each workstation of this type, it is required:

Requirement	Description
Operational System	Support of the Operating System Windows 8.1 Pro or higher, 64 bits
Processors	Intel Core i7, of at least the following features: <ul style="list-style-type: none"> • Processor base frequency: 3.6 GHz • Core amount: 4 • Cache: 4MB
Memory RAM	8 GB DDR3, 1600MHz
Hard Drive	50 GB SATA
netMATRIX	Desktop netMATRIX version 6.1.1.0 or higher
Navegator Web	Chrome 52 o superior, Firefox 48 o superior, Microsoft EDGE en su última versión.

NetMATRIX desktop installation process

Description of the netMATRIX desktop

The **netMATRIX** desktop is a software that contains the necessary applications to exploit the functionalities of the **netMATRIX platform**, according to the applications that have been included in the license acquired by the client.

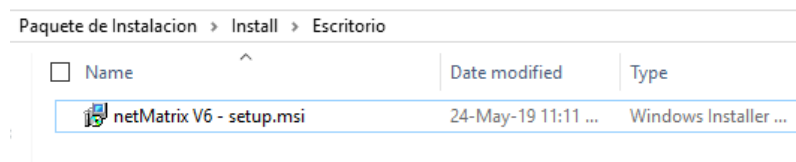
Installing the netMATRIX desktop

To install the desktop of **netMATRIX** perform the steps that are described below:

Step 1: Select the option netMATRIX.

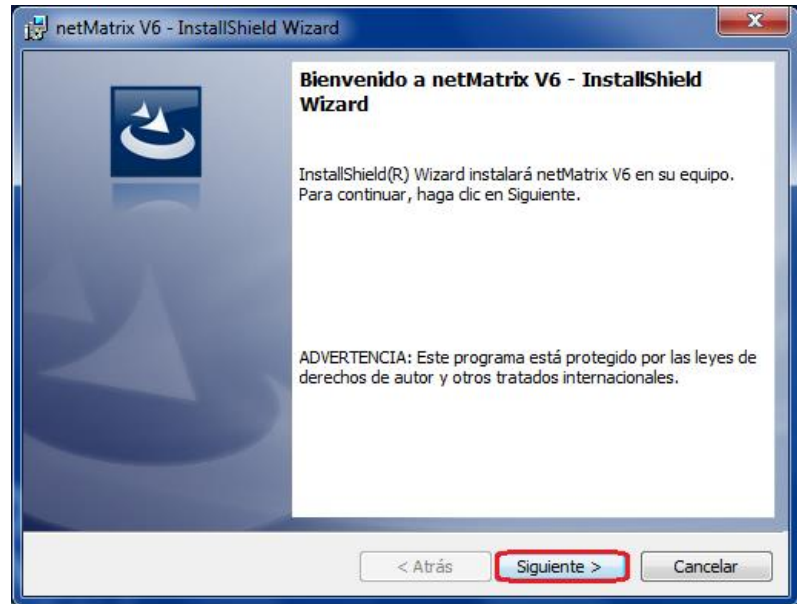
Locate in the installation package provided by your XPECTRA provider, the file **netMatrix V6 - setup.msi** in the following path: **Paquete de Instalación/Install/Escritorio/**

Double-click on the **netMATRIX V6 - setup.msi** icon

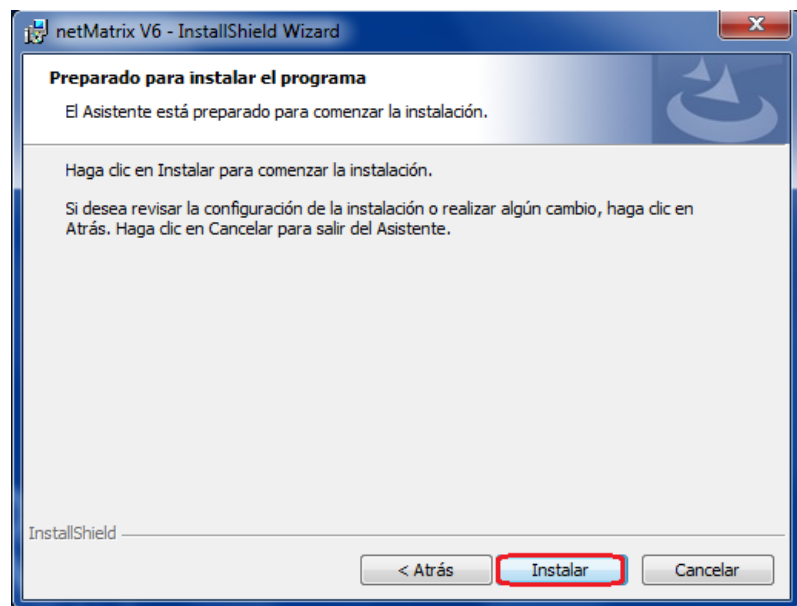


Step 2: **Start the
installation
of
netMATRIX.**

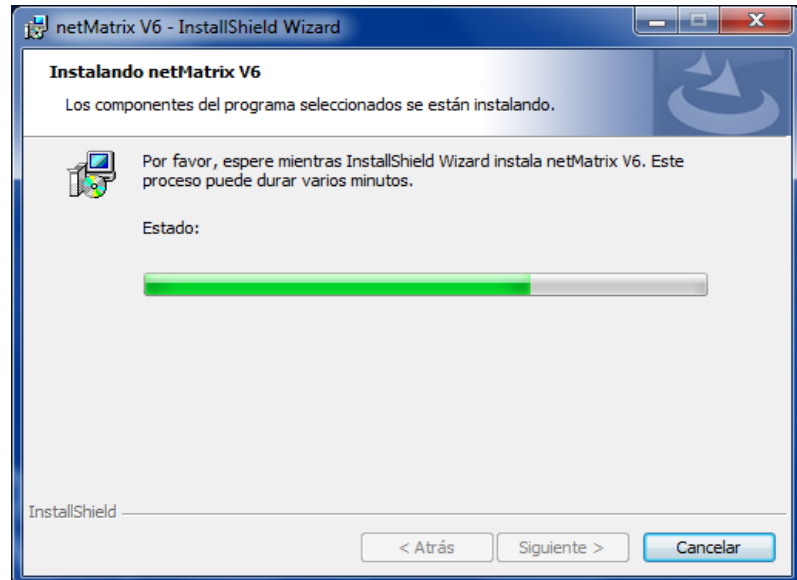
In the installation window click the button "***Siguiente***".



In the following window, click on the button ***Instalar*** and the installation of the **netMATRIX** desktop will start immediately.

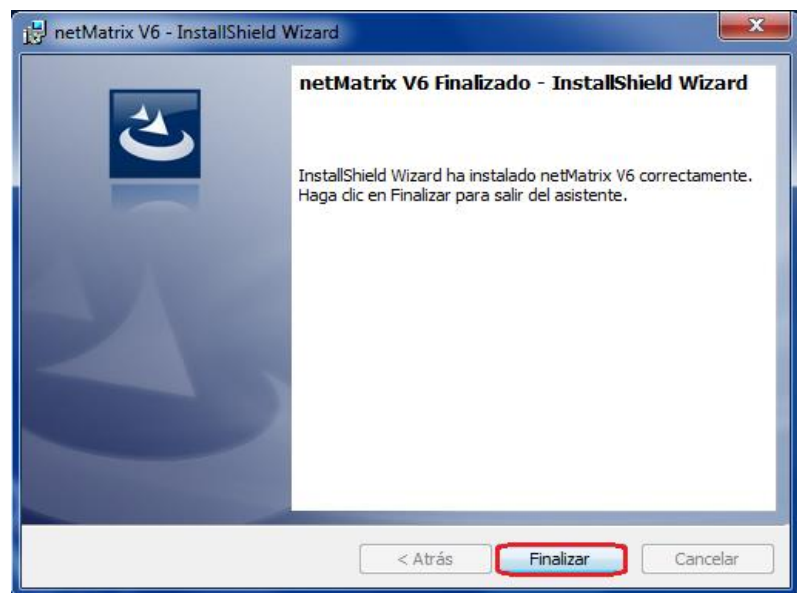


The installation process may take several minutes; you may observe its advance while the process runs.



Step 3: **Close the
installation
window.**

Once the process is completed, close the installation window by clicking on the button "**Finalizar**".



And then it will automatically create a shortcut icon for the application on your desktop.

**Step 4: Configure
 the
 connection
 to the local
 database of
netMATRIX
 .**

To perform the connection of the netMATRIX desktop to the database of the netMATRIX Platform it is necessary to configure a chain of connection.

By default, when installing any application of **netMATRIX**, this is automatically created in the directory ***Inicio/Todos los programas/netMatrix***, of the application "netMATRIX 6 BD Setup", which allows you to perform this configuration.

NOTE: For details on how to make this configuration please consult Chapter 5 of this Guide: "**Configuration of the ODBC of netMATRIX**".

**Step 5: Verify the
 installation
 of the
 desktop
 of
netMATRIX.**

Once you configure the chain of connection, you may access the **netMATRIX** desktop and verify that it opens correctly. For this, click in the Windows menu ***Inicio/Todos los programas/netMATRIX/netMatrix 6***.

To access you only need to enter your username and password assigned by the administrator of the Platform **netMATRIX** of your organization.

Chapter 5. Configuration of the ODBC of netMATRIX

Step by Step Configuration

General Description

This section of the Manual describes how to establish communication between the **netMATRIX** platform, the local primary database of the Platform and an alternate database (Example: Contingency database, in case of existing) through a connection chain. To perform this configuration use the application "**ConexiónBaseDatos.exe**" provided by XPECTRA. This application is available in **Paquete de Instalación / Herramientas / DBConnSetup / ConexionBaseDatos.exe**

Preliminary conditions

When configuring the **netMATRIX** connection chains, contact the database administrator of your organization and validate that the connection data of the primary and alternate database (if any) provided by XPECTRA are correct, for this see the following information, which is required to create the connection chains of **netMATRIX**:

- Name of the netMATRIX primary local database.
- Name of the database server where the netMATRIX primary local database is hosted.
- User name and login key to the primary database

If there is an alternate server hosting the netMATRIX database that is a mirror or replica of the database that is in production, see the following information:

- Name of the alternate local database of netMATRIX.
- Name of the database server where the alternate local database of netMATRIX is hosted.
- User name and login key to the alternate database

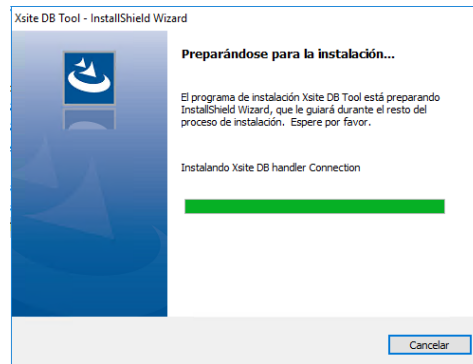


ALERT: All the equipment where the **netMATRIX** desktop is installed must have a connection to the primary and alternate database (if any) of the Platform.

ODBC Configuration of netMATRIX

To configure the **netMATRIX** connection chain perform the Steps described below:

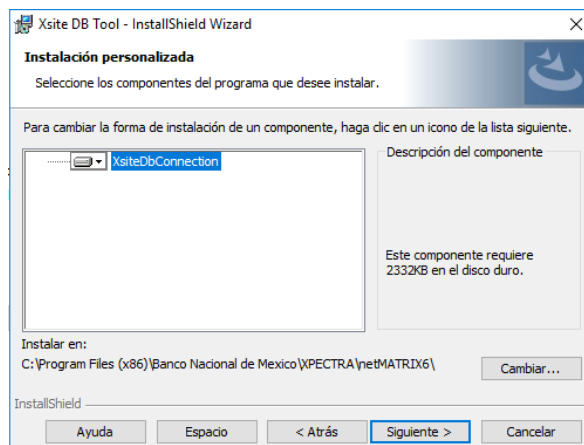
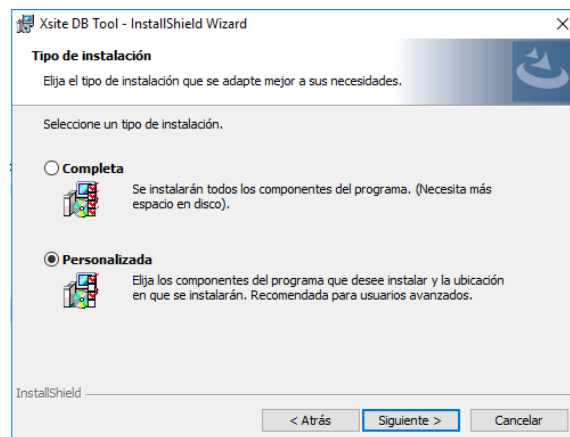
- | | | |
|----------------|---|---|
| Step 1: | Run the database connection application. | In Paquete de Instalación/Herramientas/ Xsite DB Tool / , select and run the Xsite DB Tool Setup.exe application. |
|----------------|---|---|



Step 2: Choose the type of installation.

Select the type of installation you want to perform complete or customized ("**Completa**" o "**Personalizada**"), in the case of choosing "**Completa**" the application will be installed in the following route: **C:\Archivos de Programa\ Banco Nacional de Mexico\ Xpectra\ Netmatrix6**.

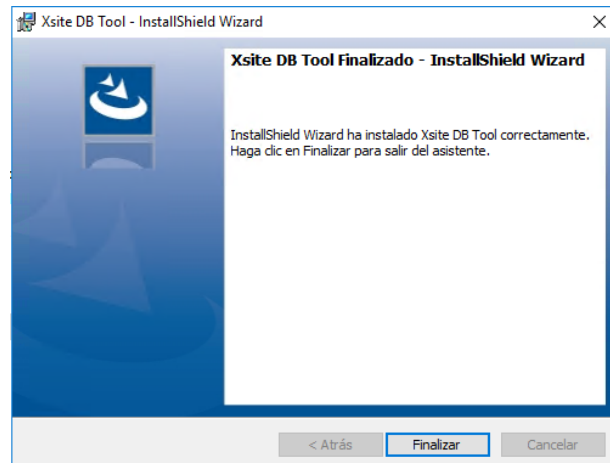
Otherwise, you can choose a different installation route.



Step 3: Completion of the installation.

The wizard will show you a screen indicating that the installation was successful "**InstallShield Wizard ha instalado Xsite DB Tool correctamente**".

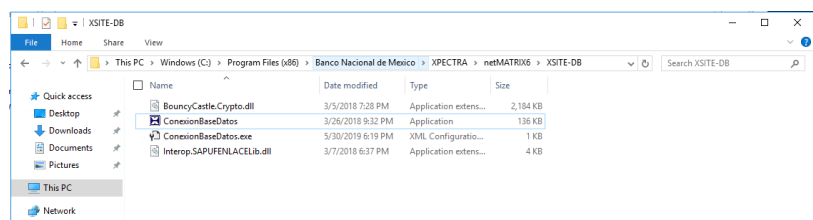
Press "**Finalizar**" to close the wizard.



Step 4: Abra la aplicación de configuración del ODBC.

After the installation of the application, you must locate the **ConexionBaseDatos.exe** icon located in **C:\Archivos de Programa\ Banco Nacional de México\ Xpectra\ Netmatrix6**.

A window appears where you can configure the connection parameters of the netMATRIX platform.





ALERT: For the application work correctly you must run it as administrator.

NOTE: The file "**ConexionBaseDatos.exe**" can be copied and executed from any location

Step 5: Configure the language.

In the **Connection parameters a BD**, in the configuration box, select the **Language** of your choice in the combo box.

Step 6: Configure the parameters of ODBC primary.

In the connection window **Parameters of the BD**, select **Primary** and register the connection parameters as shown below:

- **Server:** Write the IP address or the name of the server of the primary database where the database of the **netMATRIX** platform is installed.
- **Database:** Write the name given to the primary database of the **netMATRIX** platform.
- **User:** Write the name of the user (start of session) of the primary database of platform.
- **Password:** Write the corresponding password of the primary database user.

DB Connection setup

Configuration

Language: English

Connection parameters

Active Primary Secondary Security

Server: 10.0.5.4

Data base: netmatrix6120A

User: azureuser

Password:

✓ Activate

✓ Test Save ✕ Close

Press the button "**Save**" to register the performed configuration.

DB Connection setup

Configuration

Language: English

Connection parameters

Active Primary Secondary Security

Server: 10.0.5.4

Data base: netmatrix6120A

User: azureuser

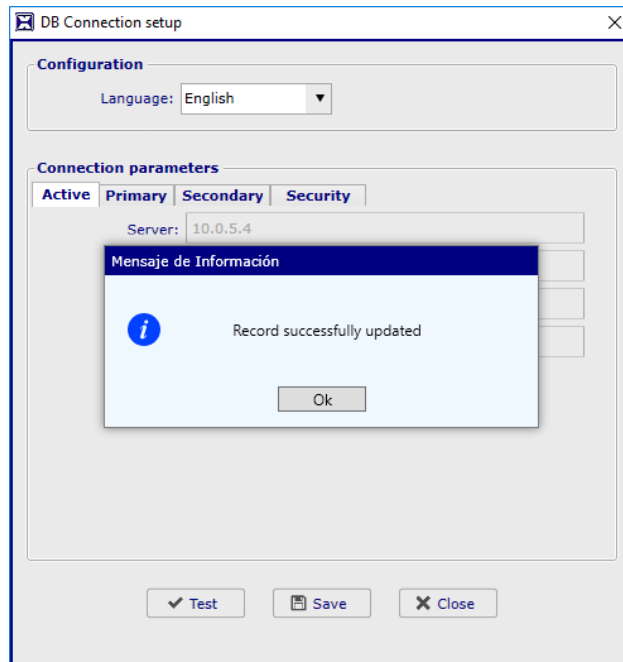
Password:

✓ Activate

✓ Test Save ✕ Close

A message will be shown indicating that the registry has been correctly updated.

Press the button "**Ok**" of this message.



ALERT: If there is an alternate server where the netMATRIX mirror database or the replica is accommodated, continue with Step 3, otherwise go to Step 4.

Step 7: Configure the parameters of alternate ODBC.

In the window **Connection parameters a BD**, select **Secondary** and register the connection parameters as shown below:

- **Server:** Write the IP address or the name of the server of the alternate database where the alternate database of the **netMATRIX** platform is installed.
- **Database:** Write the name given to the alternate database of the **netMATRIX** platform.
- **User:** Write the user name (start of session) of the alternate database of the platform
- **Password:** Write the corresponding password of the alternate database user

DB Connection setup

Configuration

Language: English

Connection parameters

Active Primary Secondary Security

Server: 192.168.1.14

Data base: netMATRIX6120-EN

User: netmatrix

Password:

✓ Activate

✓ Test Save ✕ Close

Press the button “**Save**” to register the performed configuration.

DB Connection setup

Configuration

Language: English

Connection parameters

Active Primary Secondary Security

Server: 192.168.1.14

Data base: netMATRIX6120-EN

User: netmatrix

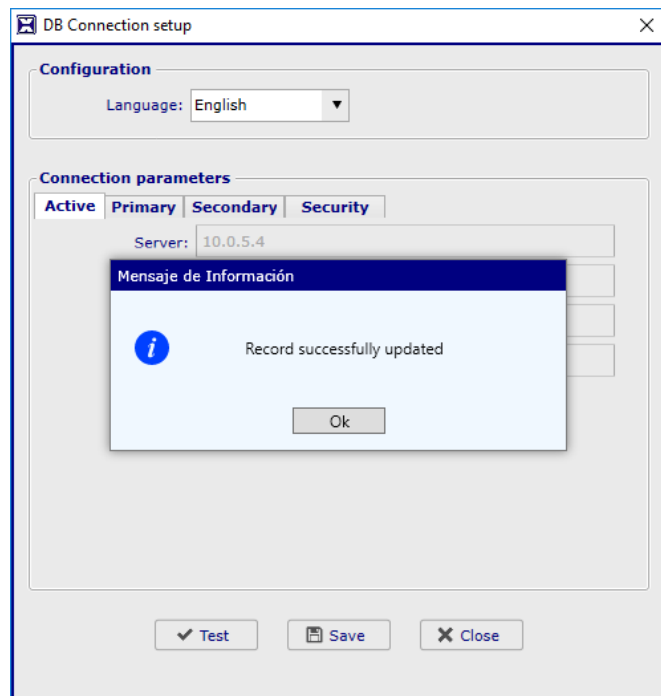
Password:

✓ Activate

✓ Test Save ✕ Close

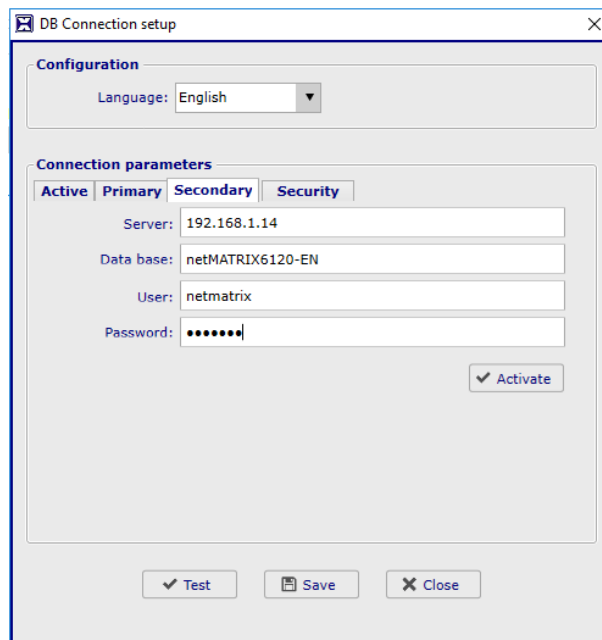
A message will be shown indicating that the registry has been correctly updated.

Press the button “**Ok**” of this message.



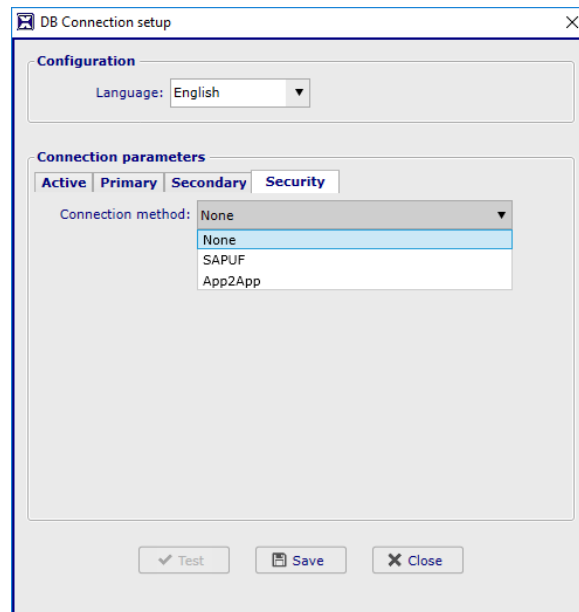
Step 8: **Select the Database server to enable.**

In the database connection parameters window, select the tab of the database that you want to activate, i.e., **Primary** or **Secondary**.

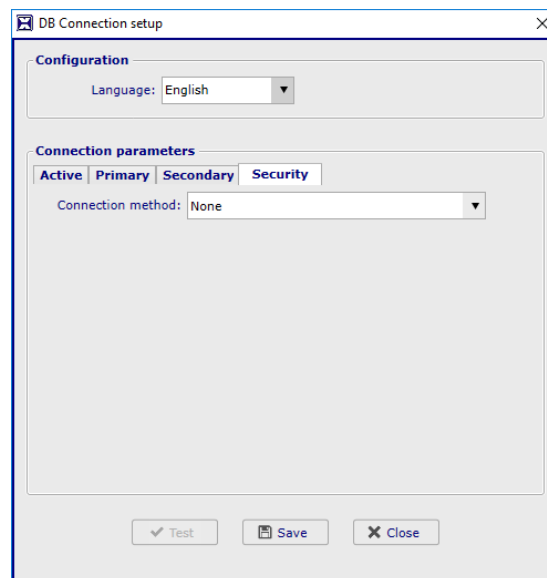


Step 9: **Select the connection method that you want to activate.**

In the database connection parameters window, select tab **Security** and subsequently the connection method that is activated in the combo box, i.e., **None**, **SAPUF**, or **App2App**.



None, indicates that the username and the password entered by the user in the appropriate fields used.



SAPUF, indicates that the connection parameters are used to the appropriate SAPUF server for the connection to the database key.

Once this option is selected, is displayed under the combo the necessary parameters-

The screenshot shows the 'DB Connection setup' dialog box. The 'Configuration' section has 'Language' set to 'English'. The 'Connection parameters' section has tabs for 'Active', 'Primary', 'Secondary', and 'Security'. The 'Connection method' dropdown is set to 'SAPUF'. Below this, the 'SAPUF' section contains five text input fields: 'Target machine:', 'Target user:', 'Application type:', 'Target application:', and 'Start application:'. At the bottom are three buttons: 'Test', 'Save', and 'Close'.

App2App, indicates that the connection parameters will be used to the corresponding App2App server, to get the key connection to the database key.

Once this option is selected, is displayed under the combo the necessary parameters.

The screenshot shows the 'DB Connection setup' dialog box with the 'Connection method' dropdown set to 'App2App'. The 'App2App' section contains six text input fields: 'Web Service URL:', 'Certificate path:', 'Key path:', 'Key password:', 'System name:', and 'Account name:'. The 'Test', 'Save', and 'Close' buttons are at the bottom.

NOTE: netMATRIX must be completed correctly the Security tab to try and save the connection to the database.

Step 10: Activate the selected

Press the "**Activate**" button to record the data saved on the selected tab (**Primary** or **Secondary**) as the data of the current connection.

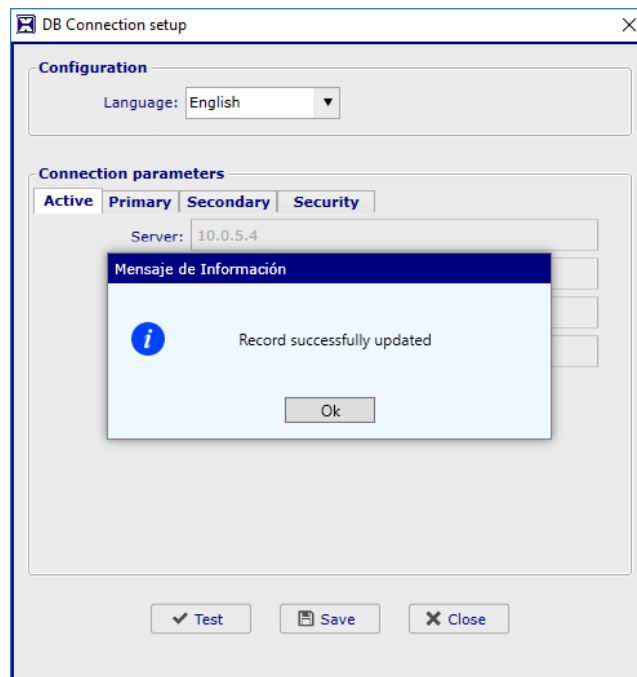
database
server.

The screenshot shows a window titled "DB Connection setup" with a close button (X) in the top right corner. The window is divided into two main sections. The top section, labeled "Configuration", contains a "Language:" dropdown menu set to "English". The bottom section, labeled "Connection parameters", contains four tabs: "Active", "Primary", "Secondary", and "Security". The "Active" tab is selected. Below the tabs are four text input fields: "Server:" with the value "192.168.1.14", "Data base:" with the value "netMATRIX6120-EN", "User:" with the value "netmatrix", and "Password:" with masked characters "••••••". To the right of the password field is an "Activate" button with a checkmark icon. At the bottom of the window are three buttons: "Test" with a checkmark icon, "Save" with a floppy disk icon, and "Close" with an X icon.

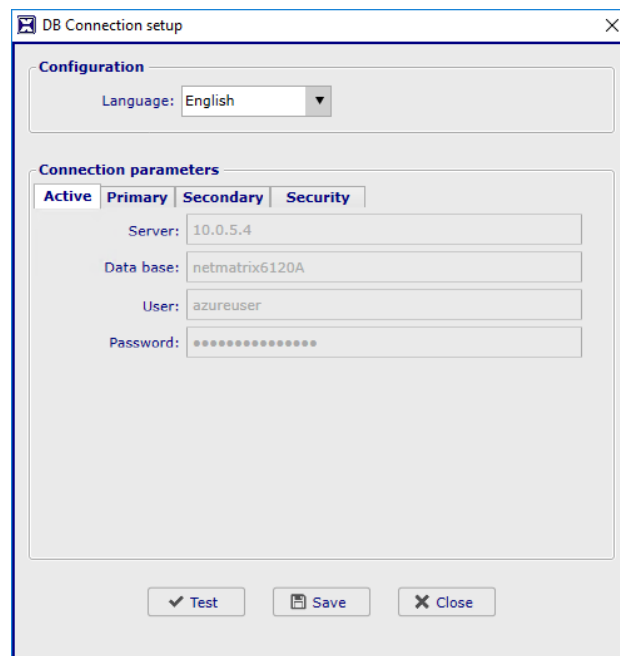
NOTE: netMATRIX connects to the server whose connection parameters are displayed on the **Active** tab of the database connection parameters window.

A message will be shown indicating that the registry has been correctly updated.

Press the button "**Ok**" of this message.



The view of the **Active** tab will change, it will show the new values of the active connection.



Step 11: Test the connection to the database

Press the "**Save**" button to verify if the connection with the database of netMATRIX is successful.

of
netMATRIX.

DB Connection setup

Configuration

Language: English

Connection parameters

Active Primary Secondary Security

Server: 10.0.5.4

Data base: netmatrix6120A

User: azureuser

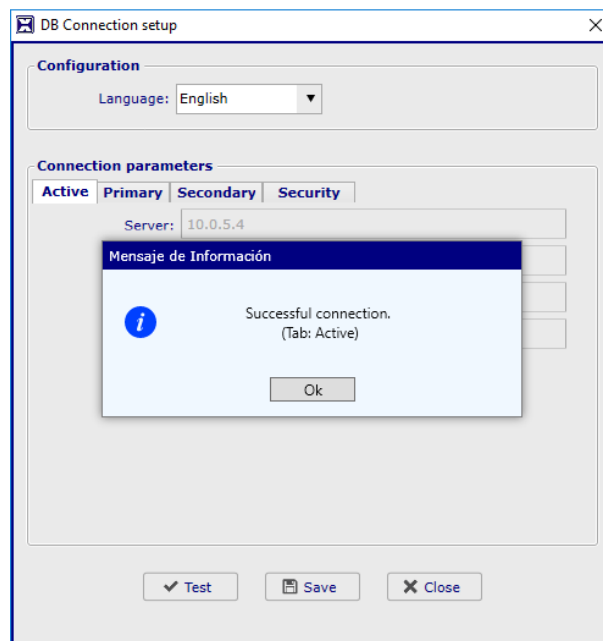
Password:

Test Save Close

A message will be shown indicating that the connection to the database of netMATRIX is successful.

Press the button "**Ok**" in this message.

NOTE: If a successful connection message is not received, you must return to step 2 or 3 (depending on the server database activated, i.e., **Primary** or **Secondary**) and verify the configuration of the ODBC parameters.



Chapter 6.- Configuring the netMATRIX Platform

General Configurations of Xsite Biometric and Xsite control of assistance in netMATRIX

Before configuring the data of the branches, employees, schedules and users, you must make some general configurations that allow you to adjust some values for the Biometric Xsite solution and attendance control.

Perform the following steps:

Step 1: Access the netMATRIX platform.

Enter with the user **banamex** and password **banamex\$1**



Step 2: Access to Gestor de Configuración.

Enter the netMATRIX desktop, locate the option **Gestor de Configuración** and access it.



Step 3: Access to Grupos de configuración.

Within the **Gestor de Configuración**, locate the option "**Grupos de Configuración**" and access it.



Step 4: **Configure
Xsite
Biométrico.**

In the "**Grupos de Configuración**" list, locate the option "**Xsite Biométrico**", select, and with the right mouse click select "**Configuración**".



Step 5: **Select
Parameters of
the Biometric
Xsite.**

In this form you will observe the various parameters to be configured in relation to the **Xsite Biométrico**, each of these parameters can be edited based on the needs.

Id campo	Descripción	Tipo de dato adicional	Valor	Valor binario
LogoClienteBiometricoPNG	Logo para el cuadro de la hora en Xsite	Logo		<Datos Binarios>
LogoClienteLoginPNG	Logo del cliente para el login de Xsite	Logo		<Datos Binarios>
UsaDispositivoBiometrico	Dispositivo Biometrico habilitado	Boolean Genérico	Si	---
XsiteApiPort	Api de enrutamiento	Puerto	5000	---
XsiteIP	IP de enrutamiento	DirecciónIP	127.0.0.1	---
XsiteServerPort	Puerto de enrutamiento	Puerto	80	---

LogoClienteBiometricoPNG: in this field you configure the time table where the location of the personnel in the branch is associated.

LogoClientelloginPNG: in this field the logo that will be displayed by the client in PNG format is configured.

UsaDispositivoBiometrico: this field allows you to configure whether or not the platform will use the biometric device in the Xsite. The default value is **SI**.

XsiteApiport: in this field the port where the Api platform is executed is configured, by default the value will be 5000.

XsiteIP: in this field, the IP address where the Xsite server is located is configured.

XsiteServerPort: in this field the port of the Xsite server is configured, by default the value will be 80.

To edit these values, you must position the mouse on the parameter to be modified, you must locate them on the bar form, and press **the button with the pencil form**.



Step 6: Configure Xsite Control de Asistencia.

In the "**Grupos de Configuración**" list, locate the option "**Xsite Control de asistencia**", select and click with the mouse right bottom and select "**Configuración**".

Id grupo configuración	Descripción
3	Logos
17	Monitor de Dispositivo - Geutebruck
9	Monitor de Dispositivo - Calculo Programado
14	Monitor de Dispositivo - Continuum IO Service
18	Monitor de Dispositivo - IntelBRas
15	Monitor de Dispositivo - Notifier
19	Monitor de Dispositivo - Pelco
20	Monitor de Dispositivo - Samsung
16	Monitor de Dispositivo - SNMP
10	Monitor de Dispositivo - TotalizacionIntervalo
21	Monitor de Dispositivo - UltAdvanced
7	Parámetros SEPROBAN
6	Parámetros Validación Usuarios
23	Pelco - Reusar Render
8	Reporte
1	Rutas
28	Tickets
11	Tipos de Datos Adicionales
31	Xsite Biometrico
26	Xsite Control de asistencia
2	Zona Horaria

Step 7: **Edit**
parameters of
the Xsite
Control
Assistance.

This form shows the various parameters to be configured in relation to the "**Xsite Control de Asistencia**", each of these parameters can be edited based on the needs

Id campo	Descripción	Tipo de dato adicional	Valor
Aviso	Mensaje informativo	String Genérico	Al ingresar su huella, usted está confirmando estar de acuerdo con la hora mostrada por el sistema de
Holgura_Tiempo	Holgura de tiempo para entrada/salida (min)	Entero Genérico	15
Hora_Entrada	Hora de entrada	String Genérico	08:00
Hora_Salida	Hora de salida	String Genérico	17:00
MaximoDiasParaHistoricoGerente	Cantidad maxima de dias para historico (Gerente)	Entero Genérico	90
MaximoDiasParaHistoricoGerentePericardo	Cantidad maxima de dias para historico (Gerente M)	Entero Genérico	90
MaximoDiasParaHistoricoPersonal	Cantidad maxima de dias para historico (Personal)	Entero Genérico	30

NOTE: This field is informative, it defines the message that the employee will see when entering the **Xsite Time & Attendance**.

Holgura_Tiempo: sets the time slack for the entry or exit of personnel, by default is set to 15.

Hora_Entrada: sets the time, by default, in which the employee must make the entry mark, the default value is 08:00.

Hora_Salida: sets the time, by default, in which the employee must make the exit marking, the default value is 17:00.

MaximoDiasParaHistoricoGerente: configures the Maximum number of days for historical (Manager Profile), which by default is 90 days

MaximoDiasParaHistoricoGerenteMercado: configures the Maximum number of days for historical (Profile of Marketing Manager), which by default is 90 days.

MaximoDiasParaHistoricoPersonal: sets the Maximum number of days for history (From the Personnel Profile), which by default is 30 days.

To edit these values, you must position the mouse on the parameter to be modified, you must locate them on the bar form, and press **the button with the pencil form**.



Setting up the branch in netMATRIX

To be able to visualize the location of the personnel in the Xsite, these data must be loaded in the netMATRIX platform.

Once on the netMATRIX platform, you must perform the steps described below:

Step 1: **Access to
Gestor de
Configuración.**

Enter the netMATRIX desktop, locate the option "**Gestor de Configuración**" and access it.



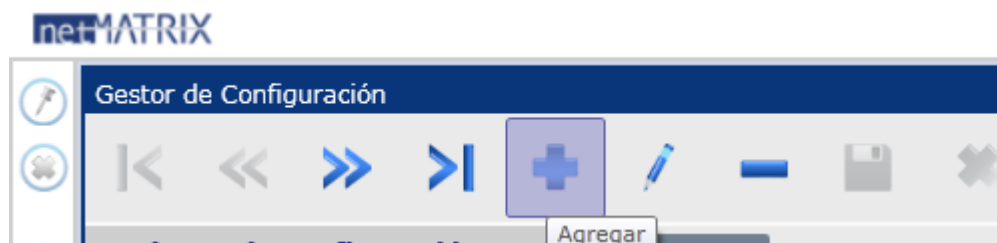
Step 2: **Access to
Ubicaciones.**

In the configuration options, display the menu called **Ubicaciones** and select the "**Ubicaciones**" option.



Step 3: **Add
Locations**

In the top menu, press the *Add* option, identified by the "+" symbol.



Step 4: **Put the
information in
form**

Fill in the **Ubicaciones** form, enter:

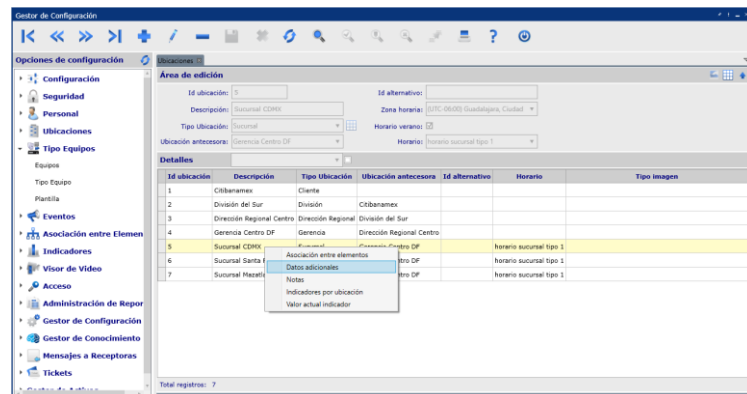
- **ID** of the branch.
- In the **Description** field, enter the name of the branch.
- In **Tipo Ubicación**, select the country, state, city or branch, based on the location we want to configure.
- In **Ubicación antecesora** select the parent location of the one you are configuring, in case of configuring the country, this field would be empty
- **ID alternativo**, usually the same location ID is placed.
- **Zona horaria** and the **Horario** at which the branch works.

In this way, the locations where the staff of each branch will be related will be configured later.

Once all the locations have been created, associations must be made in order to consult the records.

Step 5: **Add additional data.**

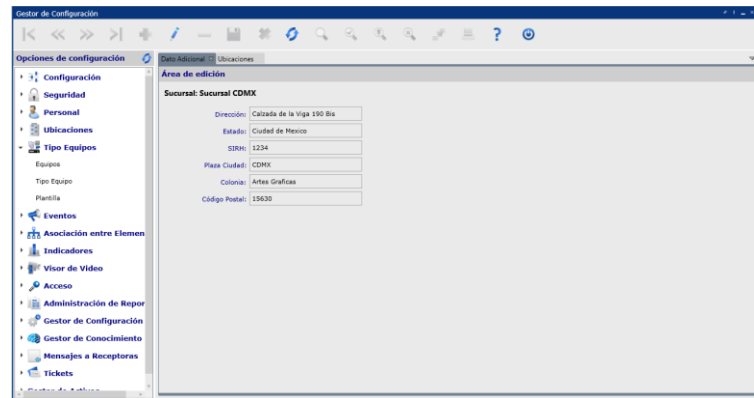
In the list of locations, select the added branch and with the right mouse click, click **Datos Adicionales**.



Step 6: **Edit additional data.**

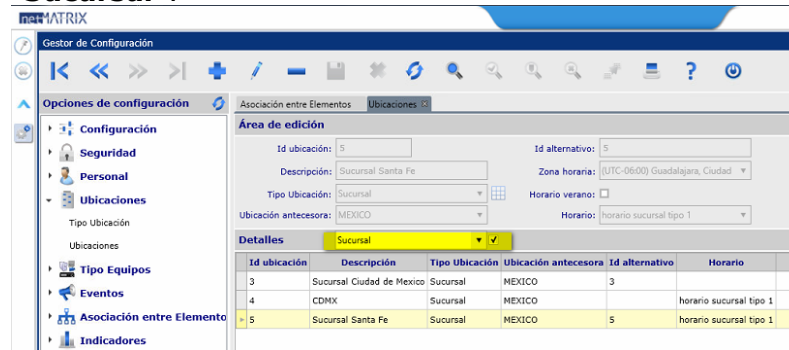
Once the form has opened **Datos adicionales**, you must fill in the information requested there: Address, State, SIRH, Town Square, Colonia, Postal Code (**Dirección, Estado, SIRH, Plaza Ciudad, Colonia, Código Postal**)

NOTE: It is very important to fill the **SIRH** field and not leave it blank.

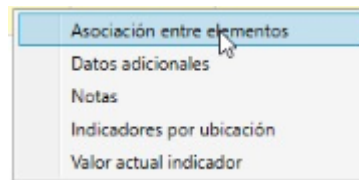


Step 7: **Make associations.**

Locate the list of **Ubicaciones**, and then filter by **"Sucursal"**.

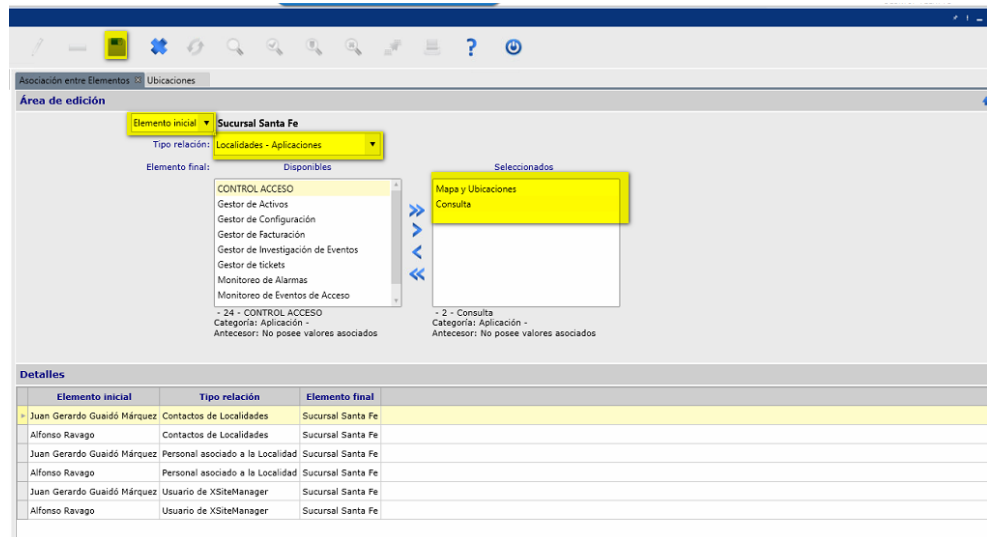


Click on the right button of the mouse and select **"Asociación entre elementos"**.



In the form of association between elements,

- Select **"Elemento inicial"**
- Select the type of relation (**"Tipo de relación"**): **"Localidades – Aplicaciones"**
- Select in the list of available elements (**"Disponible"**) the options **"Mapas y ubicaciones"** and **"Consulta"**, and move them to the **"Seleccionados"** section.
- Then press the **"Guardar"** button.



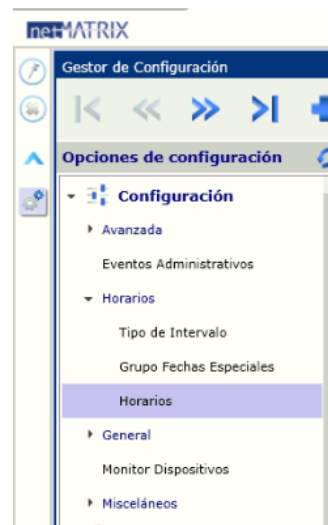
Configuring schedules in netMATRIX

The schedules allow to establish work periods for each staff to be configured, netMATRIX allows to configure the schedules for each client and location.

Next, the steps to carry out this configuration:

Step 1: Access to Schedule.

Enter in netMATRIX **Gestor de Configuración** and in "**Configuración**" option, open the "**Configuración**" menu; press "**Horarios**" sub-menu and select the "**Horarios**" option.



Step 2: Add Schedule.

In the **Horarios** form, press the *Add* option, identified by the "+" symbol at the top of the form.

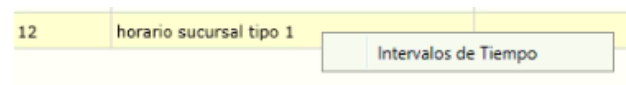


Step 3: Identify the schedule.

In the "**Horarios**" form, place an "**ID**" and in the description ("**Descripción**") write an identifier for the schedule to be created.

Step 4: Identify The new schedule.

In the detail of the configured schedules, identify the new schedule created, position the mouse on it and with the right mouse click, press the option "**Intervalos de tiempo**".



Step 5: Configure the required intervals.

You can create as many time intervals as you wish, based on the workdays of the staff.

Select the start time ("**Hora de inicio**") of the day, the end time ("**Hora de fin**"), and the days of the week, based on the desired configuration.

You can configure the time intervals that are necessary, according to the actual days of the staff.

Detalles							
Id intervalo de tiempo	Hora inicio	Hora fin	Fechas Especiales	Tipo de Intervalo	Lunes	Martes	Miércoles
1	09:00:00	16:30:00		Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	08:30:00	17:30:00		Auxiliar_Alto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	10:00:00	18:00:00		Auxiliar_Bajo	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Staff configuration in netMATRIX

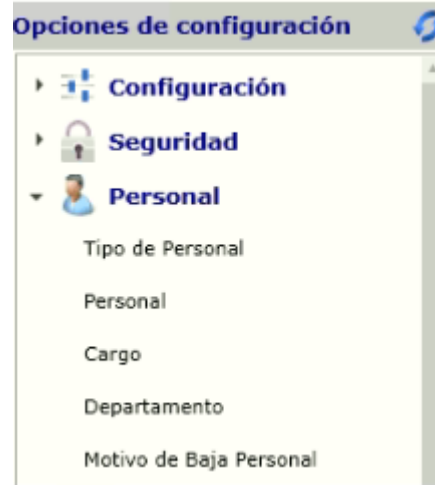
The personnel to be configured will be the personnel that will use the **Xsite** system for attendance control.

This configuration includes branch managers, tellers and other employees.

You must perform the steps described below:

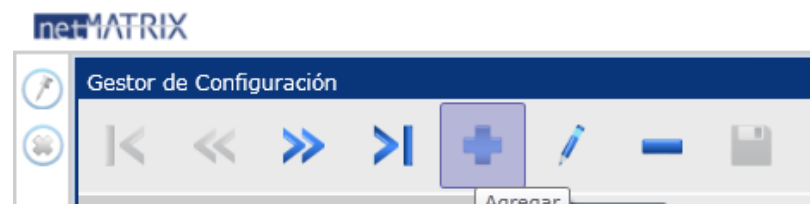
Step 1: Enter the Personal option.

Enter the netMATRIX **Gestor de Configuración** and in the **Configuración** options, display the "**Personal**" menu and then select the "**Personal**" option.



Step 2: Add staff.

Located in the **personnel form**, press the Add option, identified with the "+" symbol located at the top of the form.

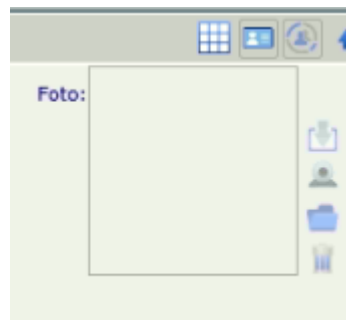


Step 3: Enter personnel information.

In the personal form, select the **Tipo de personal** to add, (in case this list is empty, locate the respective form by clicking on the box on the right hand side of the personal type field and create it on said form).

You must place a personal ID, name, surname, position and department ("**ID**", "**Nombres**", "**Apellidos**", "**Cargo**", "**Departamento**") in which you work (these last two fields can be created in the case that the drop-down lists are empty in the same way that the personal type was created)

You must place the location as a **Tipo elemento antecesor**, which in our case would be a branch, and the **Antecesor** will be the branch where this staff will be associated, that is, the branch where the same works; Finally, fill in the employee's date of birthday ("**Fecha de nacimiento**") and the identification document. In this form you can also upload a **photo** of the employee for better identification in the system. It is important check the **Habilitado** option for staff that appear on the Xsite.



Step 4: Include additional data.

After the staff is created, place the mouse on it, with the right mouse button, press the **Datos adicionales** option.

Step 5: Complete information.

You must fill out each of the requested data in the area **Datos adicional**, in the case that applies, according to the employee.

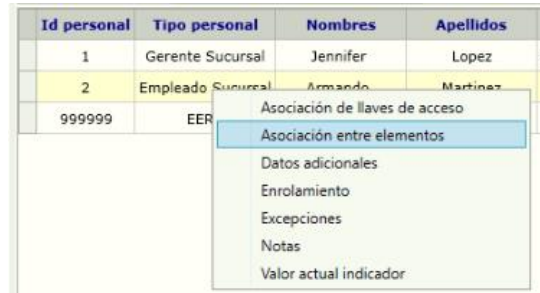
Additional data file of the employee of the branch

Additional data file of the branch manager

NOTE: The **EspersonalTransferi** field by default comes with the value **"SI"** which means that all personnel can be transferred from branch, in the case of a branch manager, this value must be changed to **"NO"**.

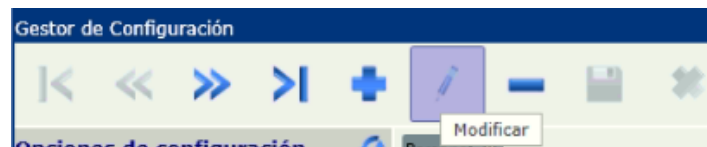
Step 6: Associate staff elements.

Make the association between staff elements, locate in the newly created personnel and with the right mouse button, press "**Asociación entre elementos**".



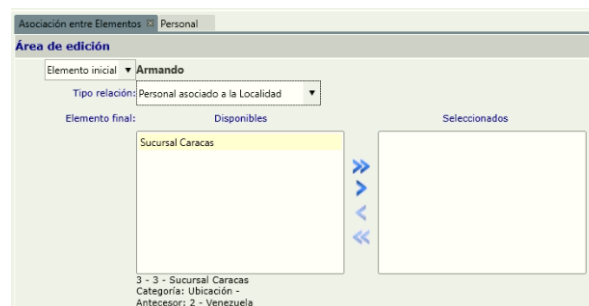
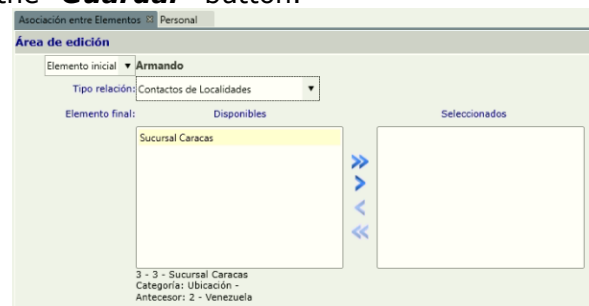
Step 7: Modify personnel association.

In the top menu, mark the pencil which allows you to modify existing associations.



Step 8: Save the staff association.

In the top menu, mark the pencil which allows to modify the existing associations; select "**Elemento Inicial**" and in the type of relationship, select the three that appear, but independently (**Contacto de localidades, Personal asociado a la localidad y Usuario de XsiteManager**), each of them will be in the memory of available, you must pass them to the **seleccionadas** box. Press the "**Guardar**" button.



Asociación entre Elementos: Personal

Área de edición

Elemento inicial: Armando

Tipo relación: Usuario de XSiteManager

Elemento final: Disponibles

Seleccionados

Sucursal Caracas

3 - 3 - Sucursal Caracas
Categoría: Ubicación -
Antecesor: 2 - Venezuela

After saving the changes, you must verify in the details that: in the "**Elemento Inicial**" appears the name of the staff, in "**Tipo relación**" should be the three indicated above, and as a "**Elemento Final**" appears the branch to which the staff was associated.

Detalles			
Elemento inicial	Tipo relación	Elemento final	
Jennifer Lopez	Contactos de Localidades	Sucursal Caracas	
Jennifer Lopez	Personal asociado a la Localidad	Sucursal Caracas	
Jennifer Lopez	Usuario de XSiteManager	Sucursal Caracas	

Step 9: Set the reason for de-registering staff.

In addition, the reasons why the branch staff can be removed should be configured.

Enter to **Personal** menu, then enter the "**Motivo de Baja Personal**" sub-menu.

In this form, you can add the number of reasons for de-registering staff that you want to configure (for example: medical rests, vacations, transfers, etc.).

Opciones de configuración

Configuración

Seguridad

Personal

Tipo de Personal

Personal

Cargo

Departamento

Motivo de Baja Personal

Motivo de Baja Personal

Tipo Dato Adicional

Usuario

Dato Adicional

Personal

Área de edición

Id Motivo: 1

Descripción: Reposo Médico

Detalles

Código	Descripción
1	Reposo Médico
2	Vacaciones

User configuration in netMATRIX

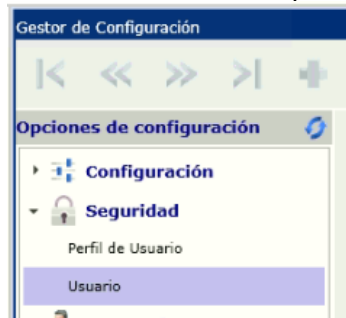
The creation of this user will allow you to access the **Xsite** system later, therefore, the creation of this user will allow you to access the Xsite system later, this step is as important as the creation of the staff.

Two types of users must be created, one with an administrator profile and the other with a user profile.

To perform this configuration you must perform the following steps:

Step 1: Enter the Usuario option.

Enter the **Gestor de Configuración** netMATRIX, in the options of **Configuración**, expand the menu **Seguridad** and then select the option "**Usuario**".



Step 2: Add User.

Located in the user form, press the Add option, identified by the "+" symbol located at the top of the form



Step 3: Enter user information.

In the user form, you must place:

- A user **ID**, which will be used to enter the Xsite.
- **Descripción**, corresponds to the user's name.
- **Perfil** of the user, for the case of the branch managers the profile called "**Xsite Manager**" corresponds to the manager of the Market profile "**Xsite Group Manager**" and for employees use the profile "**Xsite Station**".
- Select the type of personnel ("**Tipo de personal**"), the case may be (**Gerente** or **Empleado**), once the type of personnel has been chosen.
- Enter the personnel associated with that user.
- Place a key and confirm it.
- Check the check as enabled.
- Upload the user's photo.

Press the "**Salvar**" button

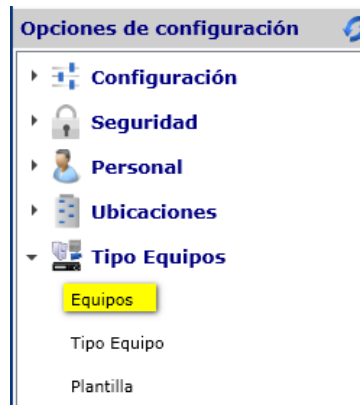
Once this configuration is done in **netMATRIX**, the platform is configured to use the **Xsite** system.

Equipment configuration in netMATRIX.

Add equipment will allow you to establish a connection between the biometric equipment and the netMATRIX system and then the latter recognizes the added device, therefore, the creation of the equipment is important.

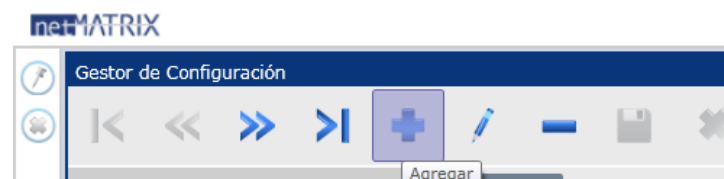
To perform this configuration you must perform the following steps:

- Step 1: Enter the option Tipo Equipos.** Enter to netMATRIX **Gestor de Configuración**, in the **Tipo Equipos** options, open the menu and then select the **"Equipo"** option.



Step 2: Add Equipments.

Once in the equipment ("Equipos") form, press the Add option, identified with the "+" symbol located at the top of the form.



Step 3: Enter equipment information.

In the equipment form ("Equipos"), you must place:

- **Id Equipo**, this identification will be a unique value that will identify the equipment.
- **Descripción**, corresponds to a name that identifies the equipment.
- **Tipo Equipo**, select from a delegable list the type of XSITE Control de Asistencia equipment.
- **Serie**, place the serial number that corresponds to the equipment.
- **Id alternativo**, place an ID for this team, this alternative ID can be the same as the equipment ID or different if you wish.
- **Plantilla**, you must choose the template **Xsite Control de Asistencia**.
- **Tipo de elemento antecesor**, select the type of element (location) which will be assigned to the equipment.
- **Antecesor**, select from the list the predecessor that corresponds to assign the equipment.
- **Habilitado**, check the check to enable the equipment.

Step 4: Save information.

Press the button "**Guardar**".

Área de edición

Id equipo:

130323032

Modelo:

Descripción:

noDevice - Xsite Control de Huella: (*)

Plantilla:

Xsite Control de Asistencia

Tipo Equipo:

XSITE Control de Asistencia

(*)

Tipo elemento antecesor:

Sucursal

Serie:

void

Antecesor:

Sucursal CDMX

Id alternativo:

noDevice

(*)

Habilitado:

☒

Chapter 7.- Services in the Type 2 and Type 3 Work Stations (use mode with biometric device)

Minimum Hardware and Software Requirements for Type 2 work station

Type 2 work stations include the software required by the solution to access the Time Attendance web application (Profile Manager Profile, Profile Employee).

For each workstation of this type, it is required:

Type	Description
Operating System	Support of the Operating System Windows 8.1 Pro or superior, 64 bits
Processors	Intel Core i5, at least the following features: <ul style="list-style-type: none"> • Processor base frequency: 1.8 GHz • Core amount: 4 • Cache: 4MB
RAM	8 GB DDR3, 1600MHz
HDD	50 GB SATA
Web navigator	Chrome 52 or superior, Firefox 48 or higher, Microsoft EDGE in its latest version.
Others	Integration Service with Morpho Fingerprint Reader

Minimum Hardware and Software Requirements for Type 3 work station

Type 3 work stations include the software required by the solution to access the Time Attendance web application (Market Manager Profile).

For each workstation of this type it is required:

Type	Description
Operating System	Support of the Operating System Windows 8.1 Pro or higher, 64 bits
Processors	Intel Core i5, at least the following features: <ul style="list-style-type: none"> Processor base frequency: 1.8 GHz Core amount: 4 • Cache: 4MB
RAM	8 GB DDR3, 1600MHz
HDD	50 GB SATA
Web navigator	Chrome 52 or superior, Firefox 48 or higher, Microsoft EDGE in its latest version.



Power: It is highly recommended that an Energy Backup Unit (UPS) be used in the computer where the application operates, because it not only protects the equipment from possible voltage disturbances from the electrical network, but also provides a complete isolation between the equipment and the AC network. In addition, it guarantees a battery backup that allows the correct closing of the applications that are running.

Process of installation of the services in work stations Type 2 and Type 3 (Installation Attended)

This section of the manual describes the installation process of the software element of the Xsite Time & Attendance solution belonging to the netMATRIX platform, which must be in the work stations where the Xsite Time & Attendance will be operated.

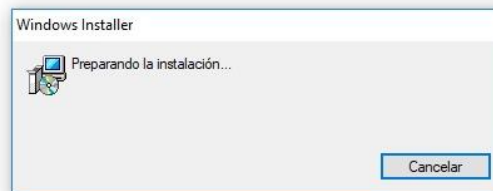
NOTE: this installation process in type 2 and type 3 workstations is only required when using the Xsite Time & Attendance solution in the biometric device mode.

This software element consists of two Windows services, one of them to handle the integration with the fingerprint reader and the other, to handle the routing with the Web server.

Here are the steps that comprise this process:

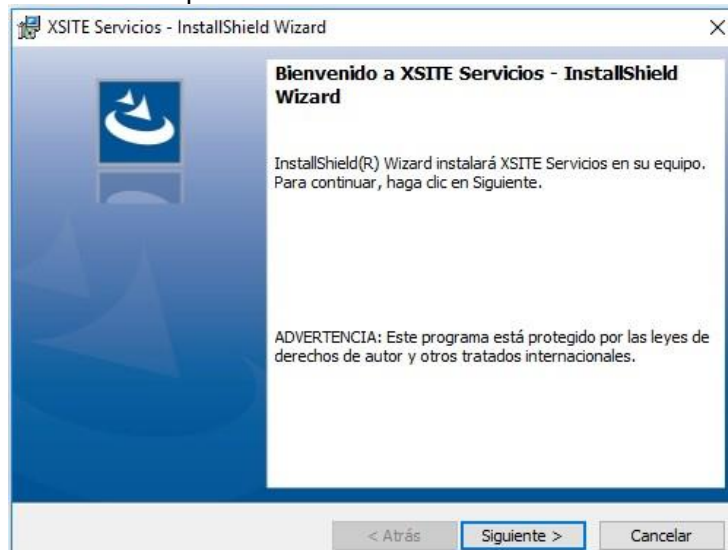
Step 1: Start the installation.

After running netMATRIX - **netMATRIX - Servicios de Xsite Attendance - setup.msi**, the following message is displayed



Step 2: Welcome message from the installation.

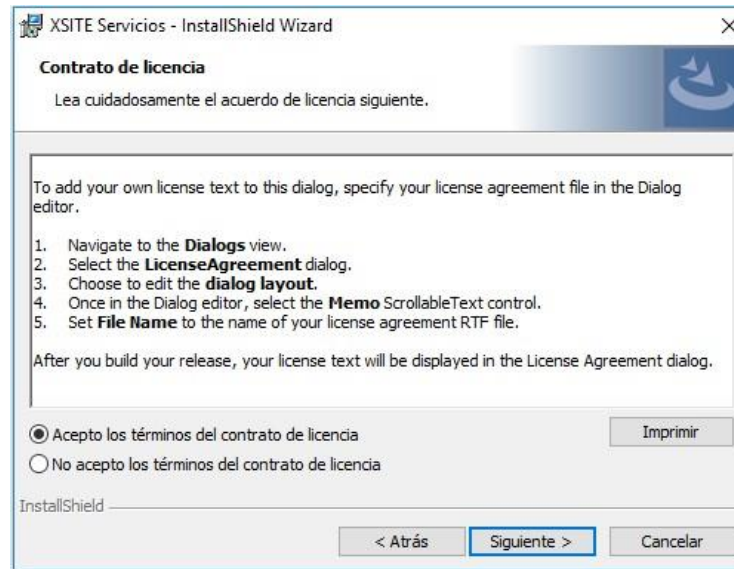
The welcome message appears. Press "**Siguiente**" to continue the process.



Step 3: Receive the License Agreement.

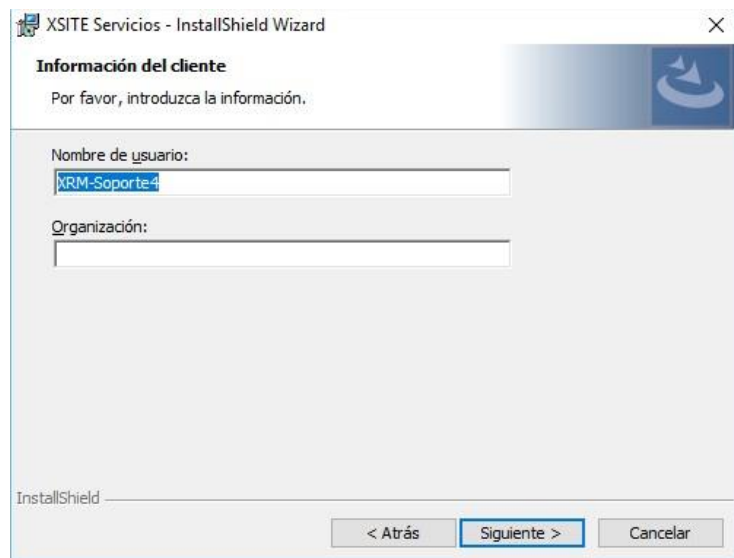
The License Agreement of the terms appears, which you must accept.

To continue the process, press the "**Siguiente**" option.



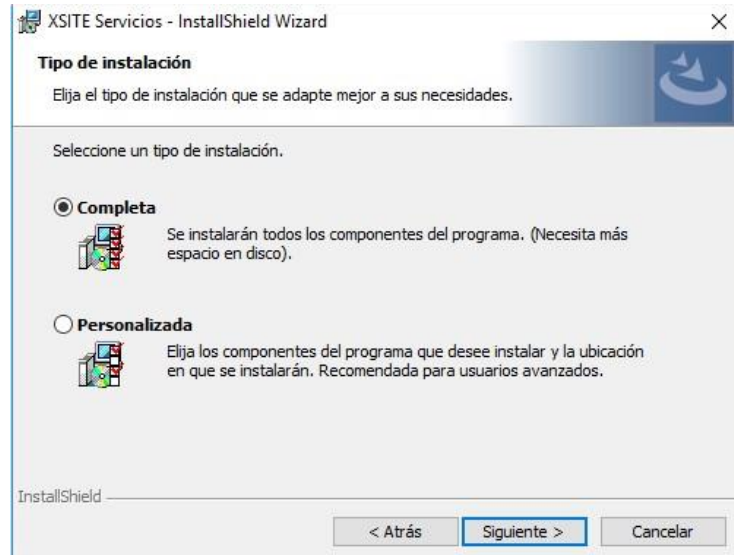
Step 4: Fill in user information.

Fill in the information of the Windows user where you are installing: User name ("**Nombre de usuario**") and Organization ("**Organización**").



Step 5: Select the Type of installation.

You must choose the type of installation, it is recommended to select the option "**Completa**" and then press "**Siguiente**" to continue.



Step 6: **Get start message.**

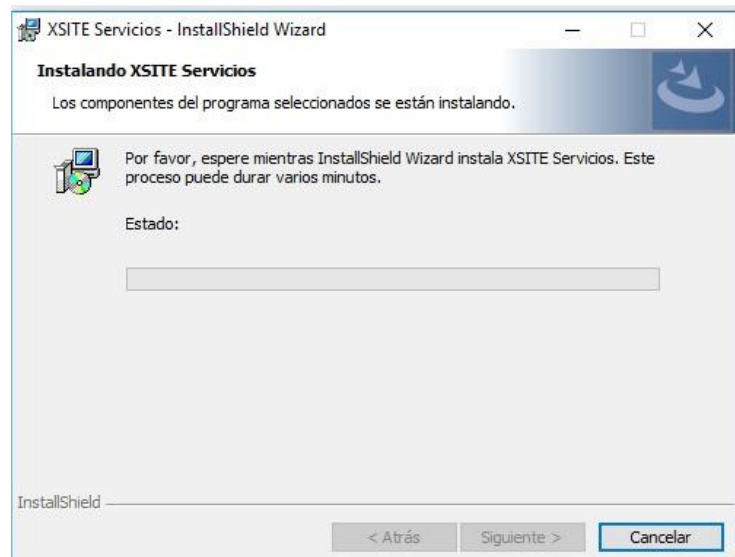
The start message of the installation preparation process is displayed.

Press the "**Instalar**" option.



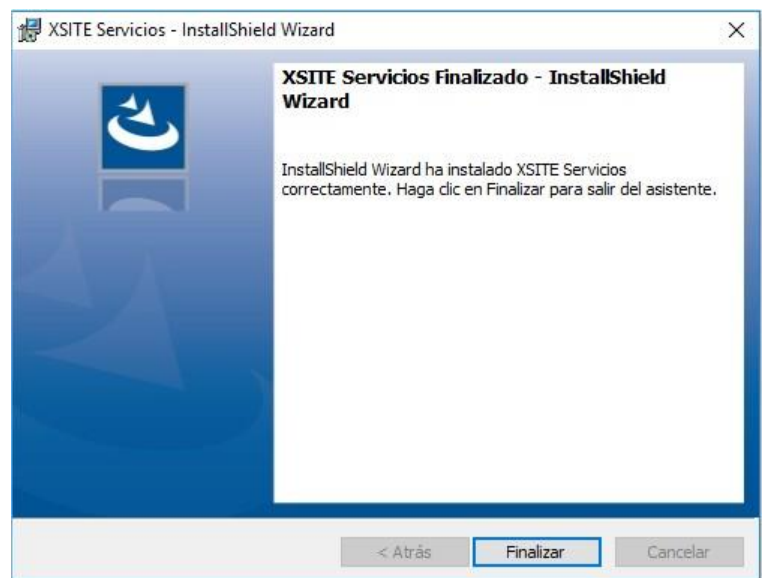
Step 7: **Receive message advance process.**

Visualize the progress of the process of installing the tool on the screen.



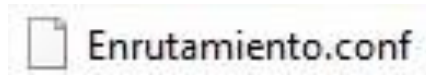
Step 8: **Receive completion message.**

Finally, the message of completion of the indicated process that has been made correctly appears. Press "**Finalizar**" option to close the window.



Step 9: **Configure the Routing File.**

Enter the route corresponding to the configuration of the routing file **C:\Program Files (x86)\Banco Nacional de Mexico\XPECTRA\netMATRIX6\XSITE-SERVICIOS\Enrutamiento\conf\enrutamiento.conf**



Modify the following parameters with a text editor:

- XIP: represents the IP on which the Server serves
- WEB, its default value is: 127.0.0.1
- XPORT: represents the port where the Xsite Frontend is served, its default value is: 80
- XAPIPORT: represents the port where the Xsite Backend is served, its default value is: 5000

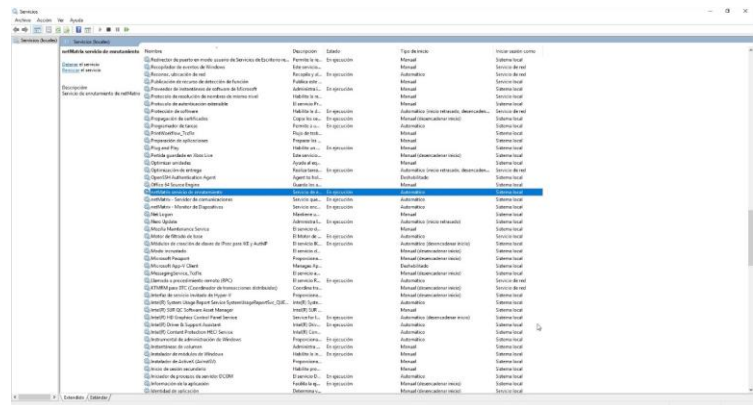
```
Archivo Edición Formato Ver Ayuda
events {} http server { listen 8888; location /xsite{ proxy_pass 'http://[XIP]:[XPORT]/'; }
location /api{ proxy_pass 'http://[XIP]:[XAPIPORT]/'; } location /device{ proxy_pass
'http://127.0.0.1:8080/'; }}
```

Step 10: Verify Windows Service Manager.

For verification of the installation, it is recommended to review the services that are associated with the installation of the tool.

Run the Windows service administrator and verify that the services identified as **netMATRIX servicio de enrutamiento** and **Xsite Biometric** appear.

Additionally, you must make sure that the services have been started and are running correctly.



Step 11: Check the installed services.

Make sure that the services are installed correctly.

Nombre	Descripción	Estado	Tipo de inicio	Iniciar sesión como
netMatrix servicio de enrutamiento	Servicio de e...	En ejecución	Automático	Sistema local
Xsite Biometric	Servicio Bio...	En ejecución	Automático	Sistema local

Process of installation of the services in work stations type 2 and 3 (Unattended Installation)

This section of the manual describes the installation process of the software element of the Xsite Time & Attendance solution belonging to the netMATRIX platform, which must go to the work stations where the Xsite Time & Attendance will be operated.

NOTE: this installation process in type 2 and type 3 workstations is only required when using the Xsite Time & Attendance solution in the biometric device mode

This software element consists of two Windows services, one of them to handle the integration with the fingerprint reader and the other, to handle the routing with the Web server.

Here are the steps that comprise this process.

Step 1: Configure the command line.

To configure the unattended installation command line, the following data must be available:

- Installer route
- XIP in which the IP of the WEB Server serves
- XPORT in which FrontEnd is served
- XAPIPORT in which the Backend is served
- XUSER in which the user with Administrator privileges is served
- XPASS in which the user's password with administrator privileges is served

With this information you should build the following command line:

```
msiexec.exe /i "c:\ netMATRIX - Servicios de Xsite Attendance - setup.msi" /quiet
XIP="192.168.1.13" XPORT="80" XAPIPORT="5000"
XUSER="DOMINIO\USUARIOCONPRIVILEGIOS"
XPASS="PASSWORD"
```

Where "C: \ netMATRIX - Xsite Attendance Services - setup.msi" is the path where the installer is located, **XIP** is the IP of the Web Server, **XPORT** is the port where the Xsite frontend is served and **XAPIPORT** is the port where the Backend is served, the **XUSER** is the User with administrator privileges, **XPASS** is the user's key with administrator privileges.

Step 2: Execute installation command.

From a command console with Administrator permissions, execute the line built in the previous step. For example:

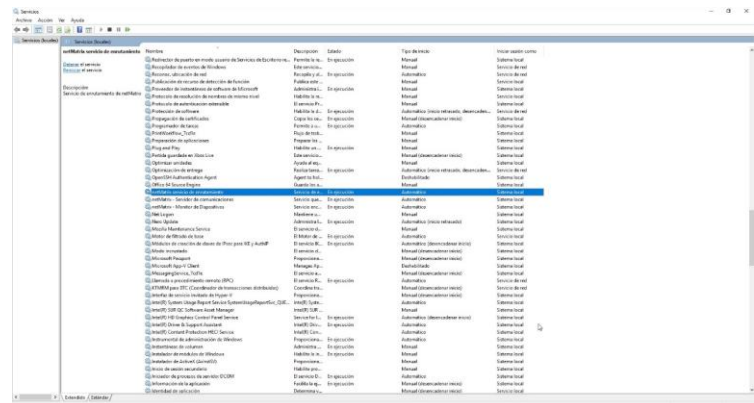
```
msiexec.exe /i "c:\netMATRIX - Servicios de Xsite Attendance - setup.msi" /quiet
XIP="192.168.1.13" XPORT="80" XAPIPORT="5000"
XUSER="DOMINIO\USUARIOCONPRIVILEGIOS"
XPASS="PASSWORD"
```

Step 3: Verify the Windows Service Manager.

For verification of the installation, it is recommended to review the services that are associated with the installation of the tool.

Run the Windows service administrator and verify that the services identified as **netMATRIX servicio de enrutamiento** and **Xsite Biometric** appear.

Additionally, you must make sure that the services have been started and are running correctly.



Step 4: Check the installed services.

Ensure that services were installed correctly.

Nombre	Descripción	Estado	Tipo de inicio	Iniciar sesión como
netMatrix servicio de enrutamiento	Servicio de e...	En ejecución	Automático	Sistema local

Nombre	Descripción	Estado	Tipo de inicio	Iniciar sesión como
Xsite Biometric	Servicio Bio...	En ejecución	Automático	Sistema local



© XPECTRA Remote Management
Salvador Alvarado 8 Interior 507 y 508,
Colonia Hipódromo
Delegación Cuauhtémoc,
México DF, CP 06100
Teléfono (52 55) 65533151 (master)
www.xpectra.com