Deltek

Deltek People Planner 4.4

Technical Installation Guide

November 25, 2022

This edition published November 2022.

Contents

Introduction

This guide describes how to install the People Planner software and complete the basic configuration, such as connecting to a Maconomy system.

This guide is intended for use by Deltek Technical Consultants After installation, Deltek Business Consultants who perform customization and various integrations, should refer to the *People Planner Administration Guide* and the *People Planner Integrations Guide.*

The installation steps are first presented as a detailed walkthrough. This is also summarized as a shorter checklist in Appendix A.

At key points during the installation process, you should stop and verify the current "health" of the installation. Verification steps are either *simple verifications* or *advanced verifications*. An advanced verification is a verification that requires some additional actions and is usually within the responsibility of Business Consultants; for the most part, this is the importing of users from Maconomy into People Planner. For brevity, simple verifications are called "verifications" throughout this guide.

It is assumed that you are proficient in installing and configuring on the Maconomy side—that is, that you know how to use MConfig and the Maconomy Workspace Client.

Note: In People Planner 4.0, the following installers are now organized into a single Web Applications installer.

- MyPlan
- People Planner Web Components
- People Planner API web service
- The new People Planner RESTful web service (RestApi)
- People Planner Security Service

The People Planner Outlook Web Service is not included in this, and it still has its own installer.

Attention: Before updating to 4.3, you must uninstall previous People Planner Web Components (including MyPlan and API).

This document does not cover how to setup the People Planner in the Maconomy web client. For that, refer to the *Deltek Maconomy System Admin Guide*. To set it up on the People Planner side only require that you install the People Planner RESTful web service (RestApi)

Prerequisites for Installing the People Planner Software

This section lists the prerequisites for installing the People Planner software.

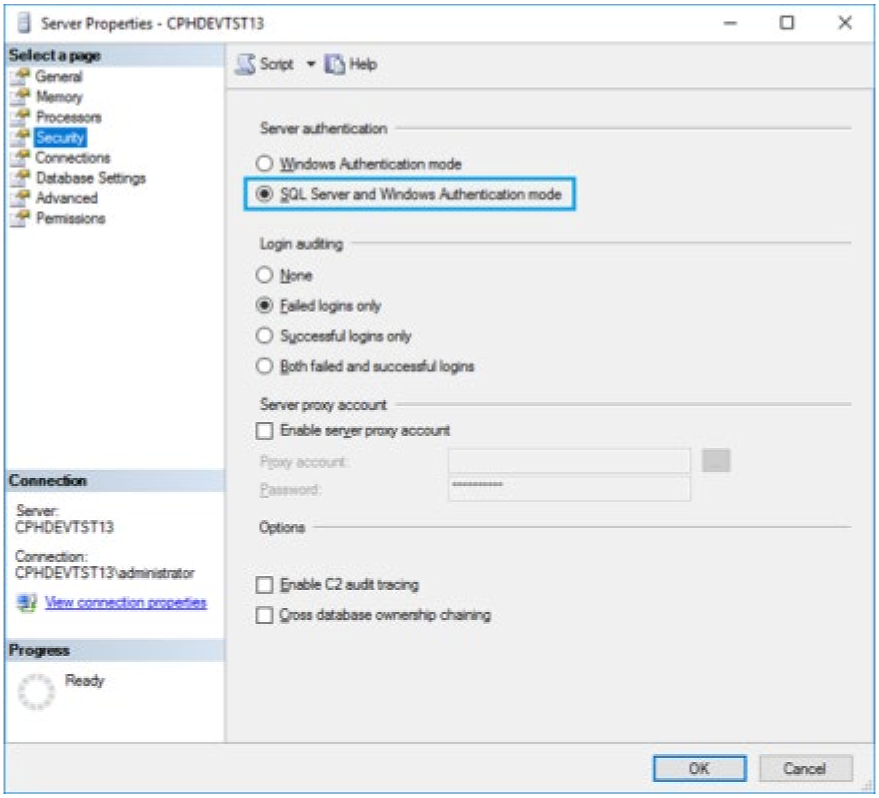
For information about supported versions of the software, see the People Planner section of the Compatibility Matrix:

- Internal Link: https://home.deltek.com/sites/products/Documents/DeltekProductSupportCompatibilityMatrix.pdf
- External Link – Deltek Customer Care Connect: Deltek Product Support Compatibility Matrix

Prerequisites for Installing the People Planner Database

A SQL Server must have been installed to host the People Planner database. SQL Server 2012 and newer is supported.

The installation must support **SQL Server and Windows Authentication**.



This guide assumes that you have created a Named Instance when you installed the SQL Server, but this is not a requirement; that is, you can use the Default Instance if you prefer.

You must also have SQL Server Management Studio installed.

Collation

Deltek recommends that you configure the People Planner database to be **case-insensitive**.

This is not an absolute requirement; however, if you configure the database to be case-sensitive, it has adverse consequences for:

- The sorting order on columns in People Planner
- Filtering on columns in People Planner
- Any SQL scripts that you create, such as those to use with import mappings

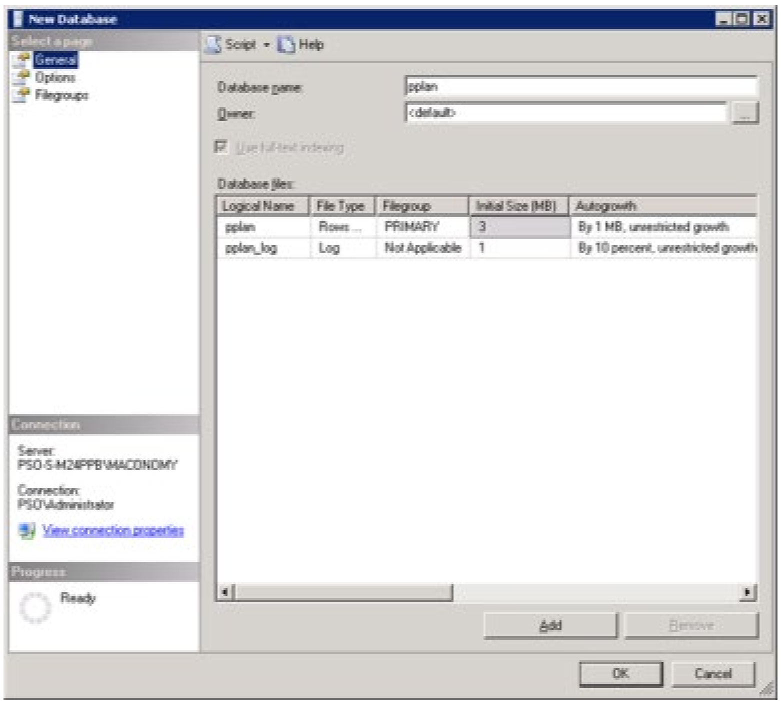
For example: Using a case-sensitive database, columns are sorted first in the order a-z, and then A-Z.

You can configure SQL Server to be either case-sensitive or case-insensitive. This is part of the **collation** of the SQL Server. Any database that you create on the SQL Server inherits the collation of the SQL Server. Any tables that you create in the database inherit the collation of the database. Unfortunately, while you can later change the collation of, say, the database, this does not change the collation of the individual tables. It is therefore best to ensure that you have the correct collation of the database before adding tables to it.

If your SQL Server is configured to be case-sensitive—for example, because it also hosts a Maconomy database—you can still create a case-insensitive database for People Planner.

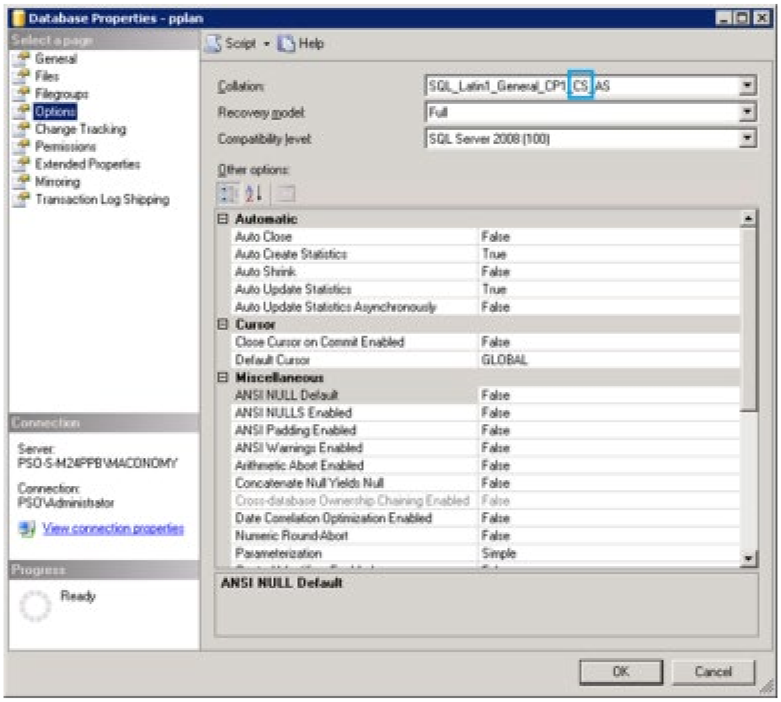
To create a case-insensitive People Planner database, when the SQL Server is case-sensitive:

1. Open the SQL Server Management Studio.
2. In the Object Explorer, right-click the **Databases** node. This opens a shortcut menu.
3. Choose **New Database…** from the shortcut menu. This opens the New Database dialog.
4. Click the **General** page.
5. Enter the **Database name**.



6. Click **OK**.
7. Refresh the Object Explorer to see the new database.
8. Right-click the database and choose **Properties**.

9. Click the **Options** page.



10. Inspect the **Collation** field. In the drop-down list of its possible values, part of the name of each variant includes either CS (for case-sensitive) or CI (for case-insensitive).
11. Select the case-insensitive variant of the current collation from the drop-down list of variants.
12. Click **OK**.

When you have done this, you have a case-insensitive and empty database. When you create the People Planner database using the People Planner Admin Tool, you should—instead of creating another database—select this empty database and perform a database update.

Prerequisites for Installing the People Planner Windows Software

People Planner requires a Windows operating system. On the server side, Windows Server 2012 and newer is supported. On the client side, Windows 7 and newer is supported, except for Windows 8, which is desupported.

The People Planner Windows software requires .NET Framework 4.7.2 or newer.

Prerequisites for Installing the People Planner Web Software

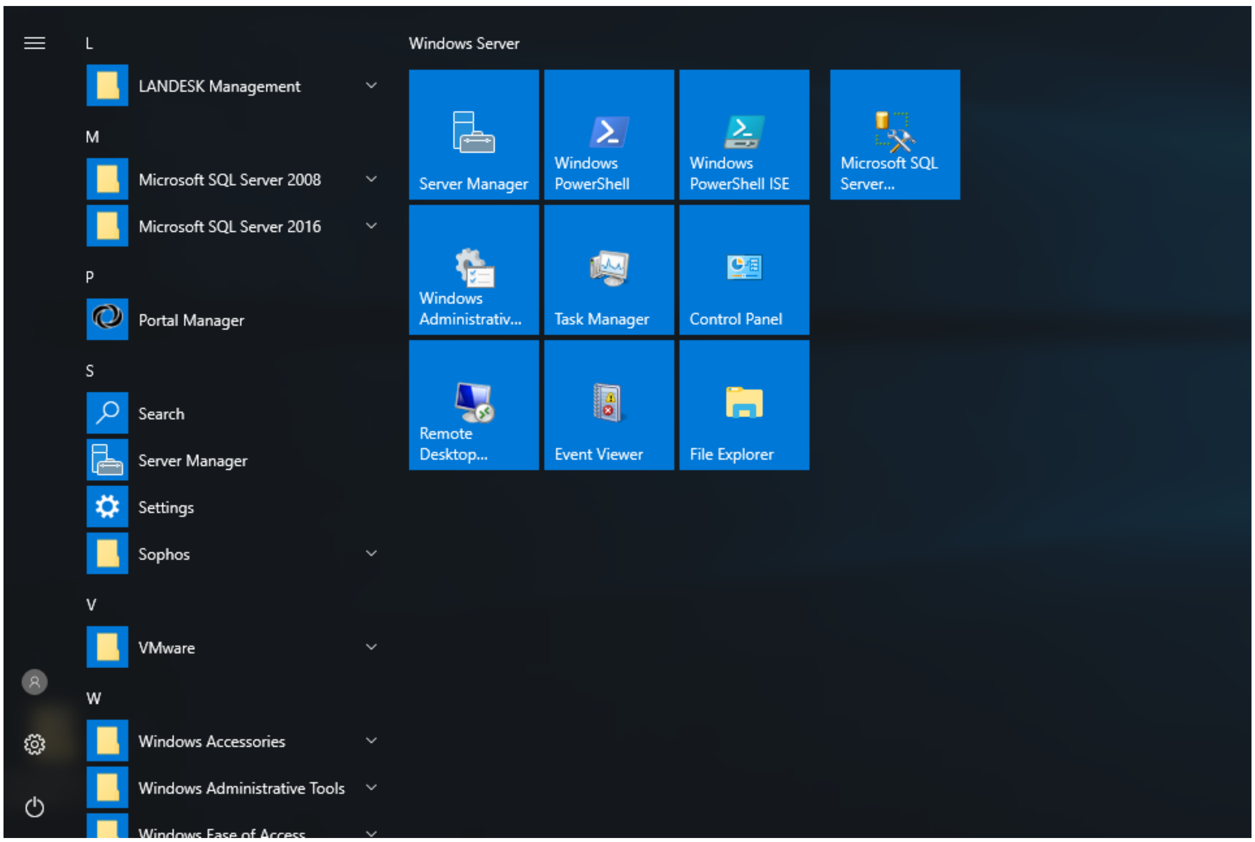
The People Planner Web software requires .NET Framework 4.7.2 or newer, and .NET Core 3.1.10 or newer.

The People Planner Web applications require a Microsoft IIS Webserver to run. IIS 10 and newer is supported.

Installing Internet Information Services (IIS)

Note: As of People Planner 3.8, the requirements for the configuration of the IIS have been simplified, compared to previous versions. As an example, you are no longer required to enable the IIS Metabase Compatibility during the installation. This was a requirement in People Planner 3.7.1 or older versions.

The IIS Webserver comes bundled with Windows, but it is not enabled by default. To enable and configure the IIS, you use the Server Manager application. In Windows Server 2016, the Server Manager are located directly via the Windows Start screen.



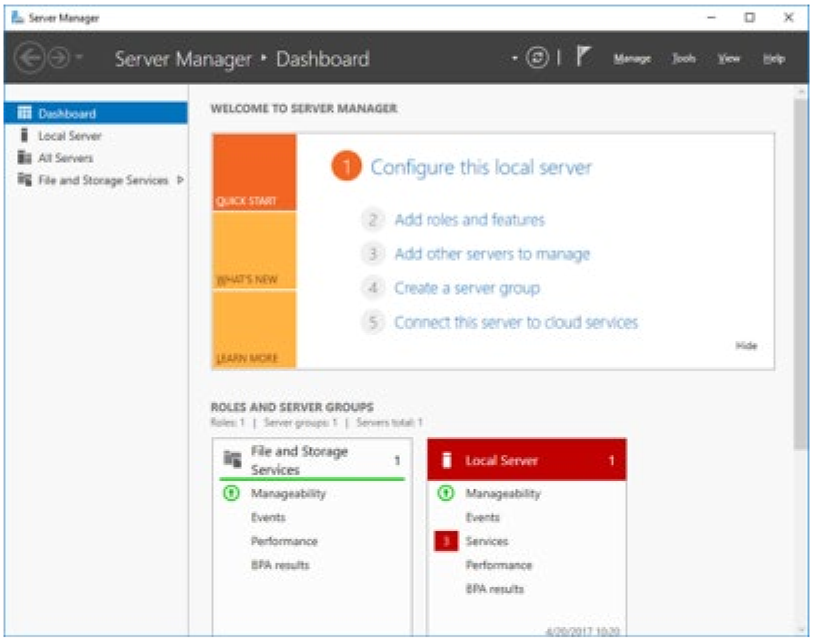
Tip: An alternative way to start the Server Manager is to open the **Control Panel**, go to **Programs and Features**, and then click **Turn Windows Features on or off**.

Prerequisites for Installing MyPlan and the Web Components

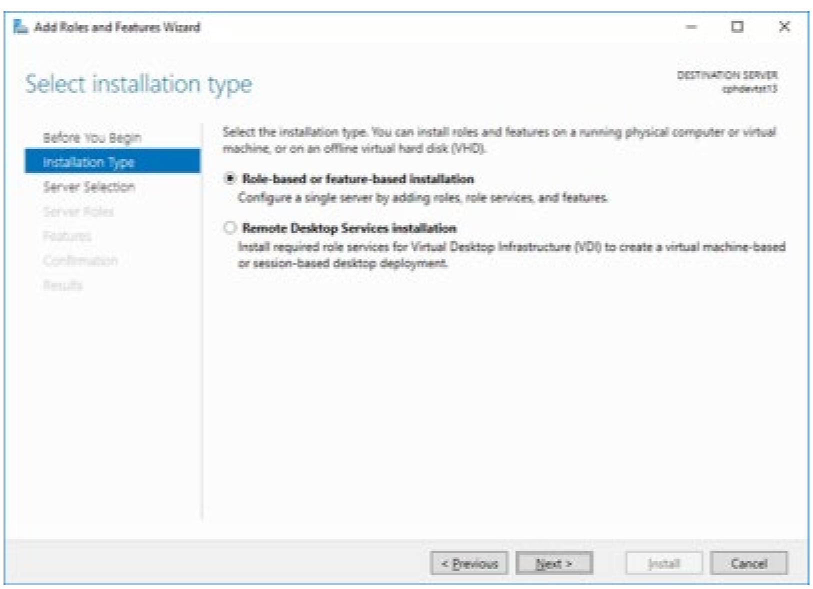
This section describes how to configure the IIS to fulfill the requirements for installing MyPlan and the People Planner Web Components.

To enable the IIS Web server and configure it with the prerequisites for installing the MyPlan and the People Planner Web Components:

1. Start the **Server Manager** application.

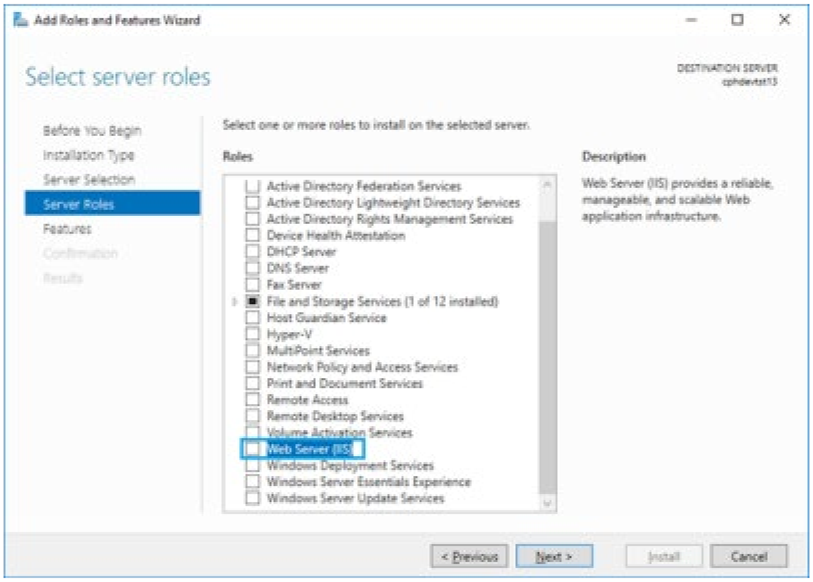


2. Start the **Add Roles and Features Wizard**.
3. Under **Installation Type**, select **Role-based or feature-based installation** and click **Next**.



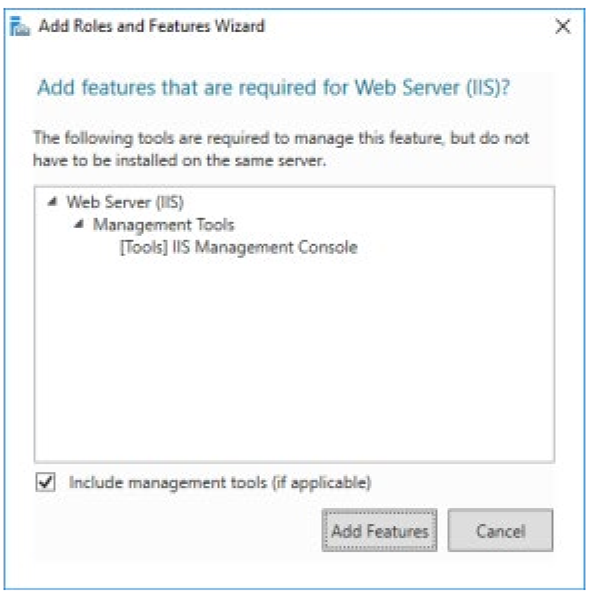
4. Under **Server Selection**, select the destination server and click **Next**.

5. Under **Server Roles**, select **Web Server (IIS)**.



This opens the Add Roles and Features Wizard to tell you about additional features that will be included.

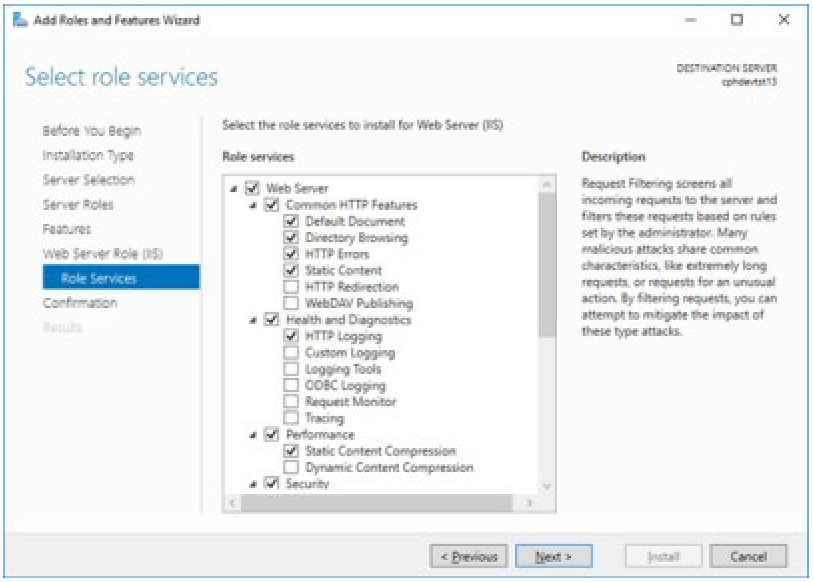
6. Click **Add Features**.



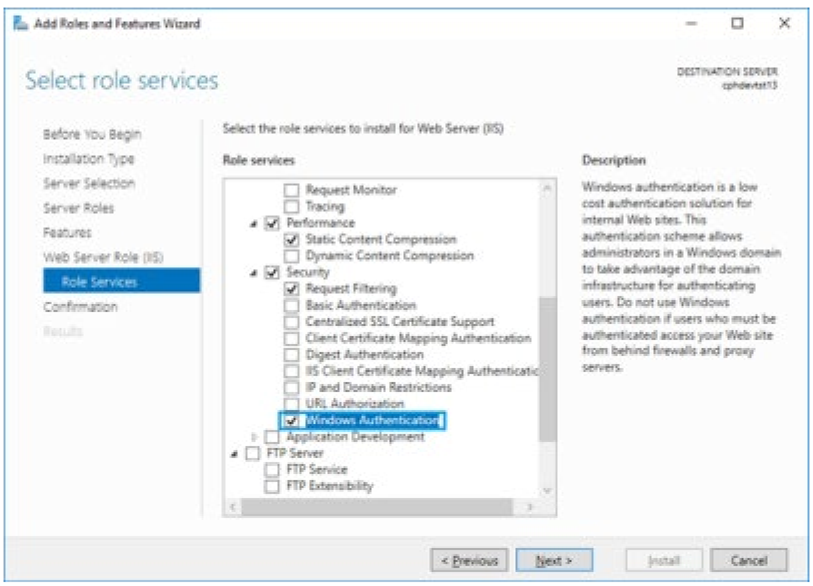
This closes the wizard, and returns you to Server Roles.

7. Click **Next**.
8. Under **Features**, click **Next**.

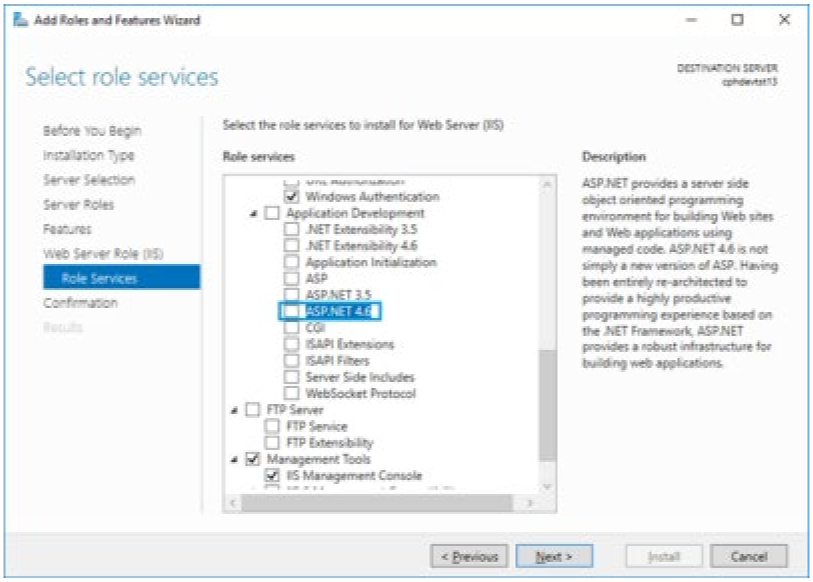
9. Under **Web Server Roles (IIS)**, click **Next** or select **Role Services**.



10. Under **Role Services**, select **Web Server » Security » Windows Authentication**.

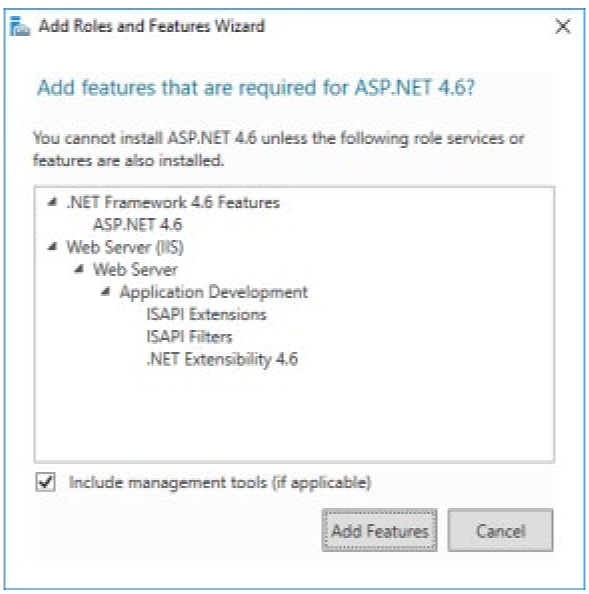


11. Select **Web Server » Application Development » ASP.NET 4.7**.



This opens the Add Roles and Features Wizard to tell you about additional features that will be included.

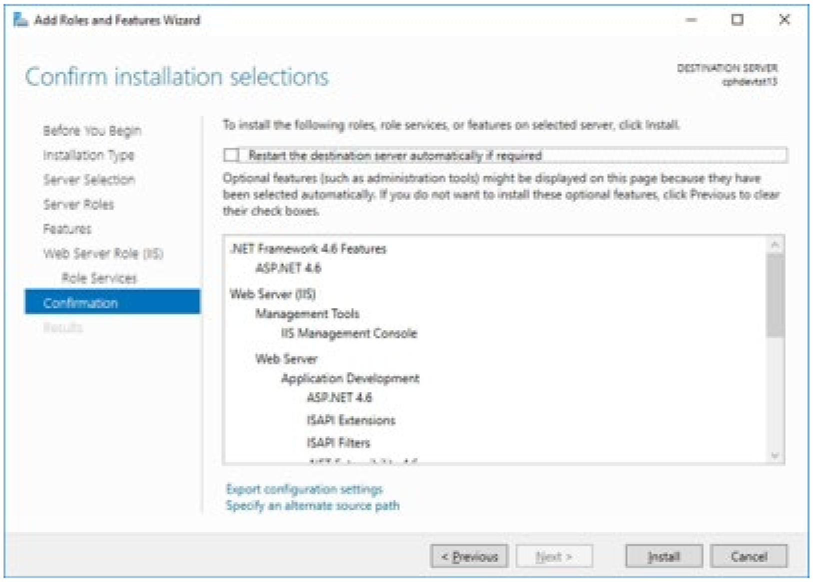
12. Click **Add Features**.



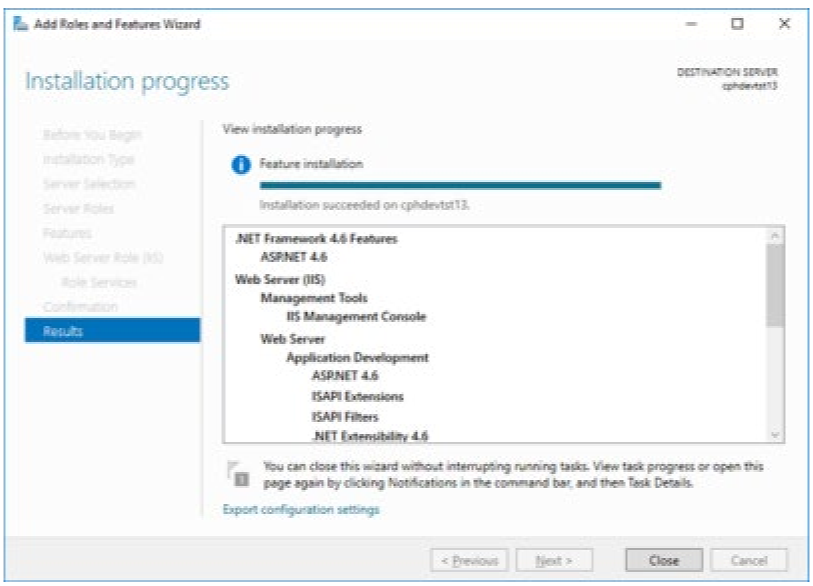
This closes the wizard and returns you to Role Services.

13. Click **Next**.

14. Under **Confirmation**, click **Install**.

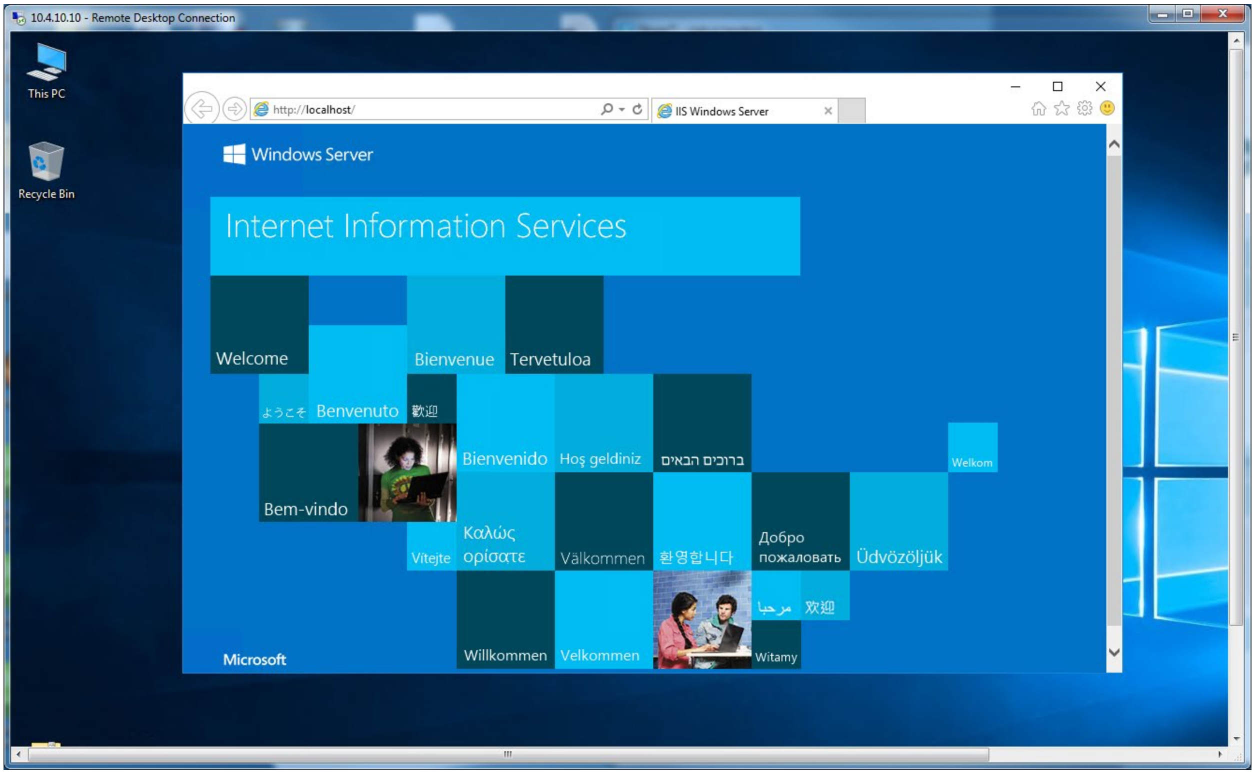


15. When the installation has completed, click **Close**.



16. Close the **Server Manager**.

You can verify that the IIS Web server has been installed correctly by opening a Web browser and navigating to http://localhost. This should display the Internet Information Services start page.



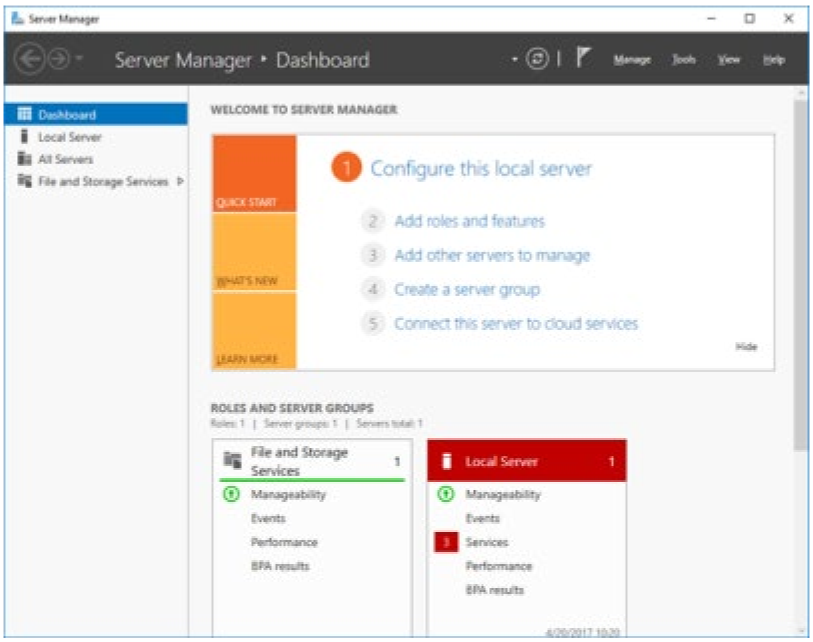
Prerequisites for Installing the People Planner Web Services

Before continuing with this section, you must first have fulfilled the prerequisites of installing MyPlan and the people Planner Web Components. See Prerequisites for Installing MyPlan and the Web Components for information about this.

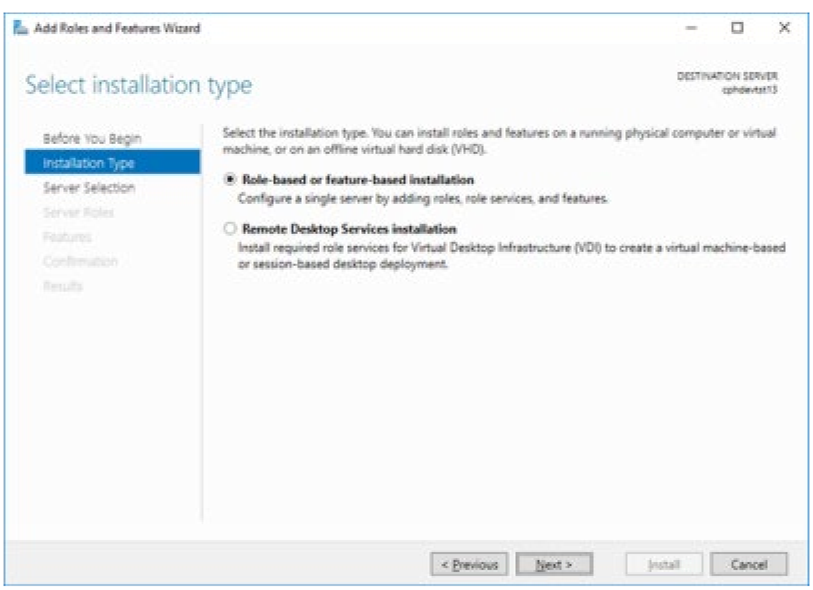
This section describe how to configure the **IIS** to fulfill the additional requirements for installing the People Planner Web services.

To configure the IIS with the prerequisites for installing the People Planner Web services:

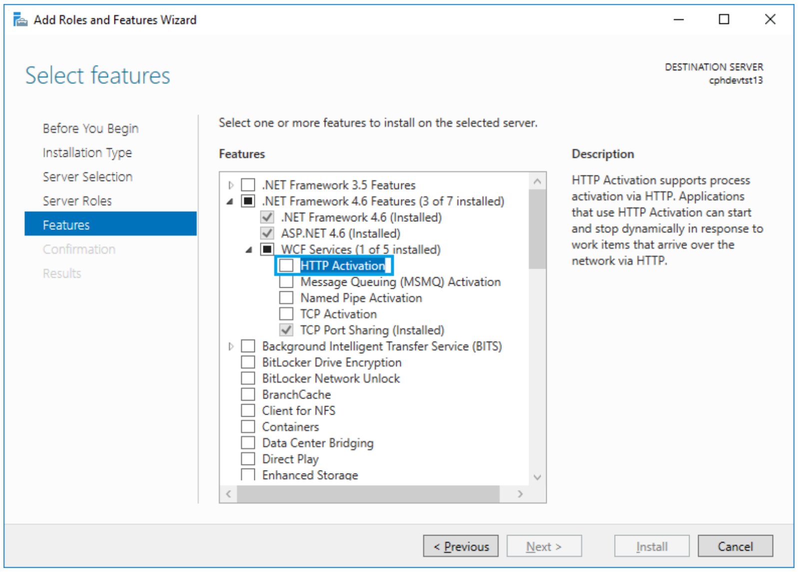
1. Start the **Server Manager** application.



2. Start the **Add Roles and Features Wizard**.
3. Under **Installation Type**, select **Role-based or feature-based installation** and click **Next**.

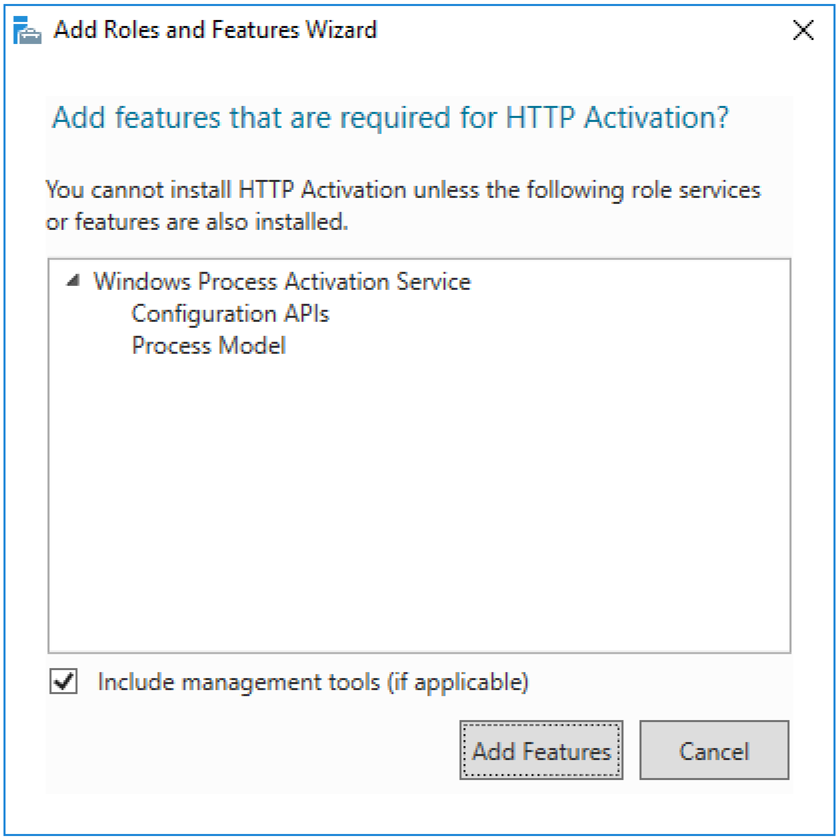


4. Under **Server Selection**, select the destination server and click **Next**.
5. Click **Features**.
6. Select **.NET Framework 4.7 Features » WCF Services » HTTP Activation**.



This opens the **Add Roles and Features Wizard** dialog to inform you of additional features that will be included.

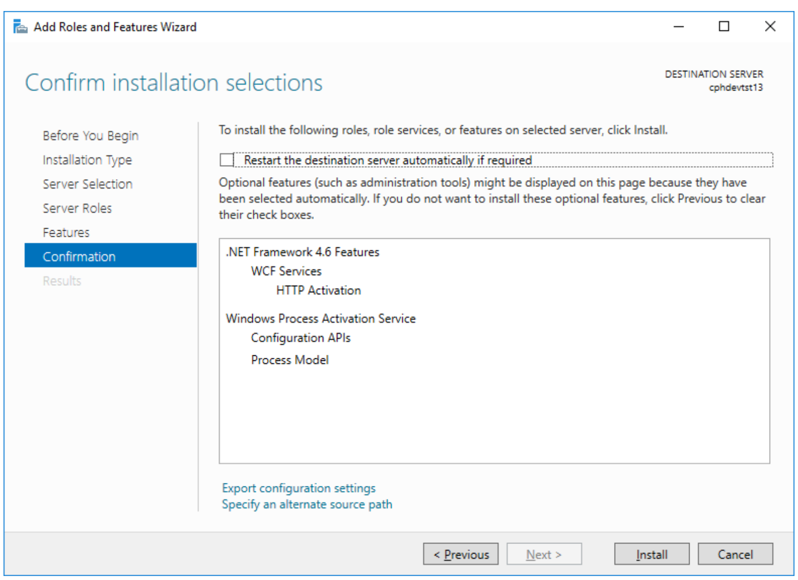
7. Click **Add Features**.



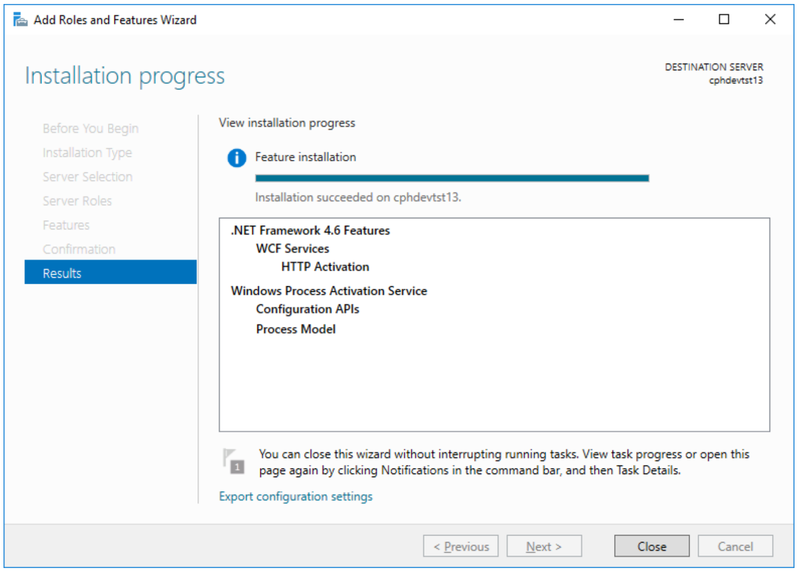
This closes the dialog, and you return to **Features**.

8. Click **Next**.

9. Under **Confirmation**, click **Install**.



10. When the installation has completed, click **Close**.

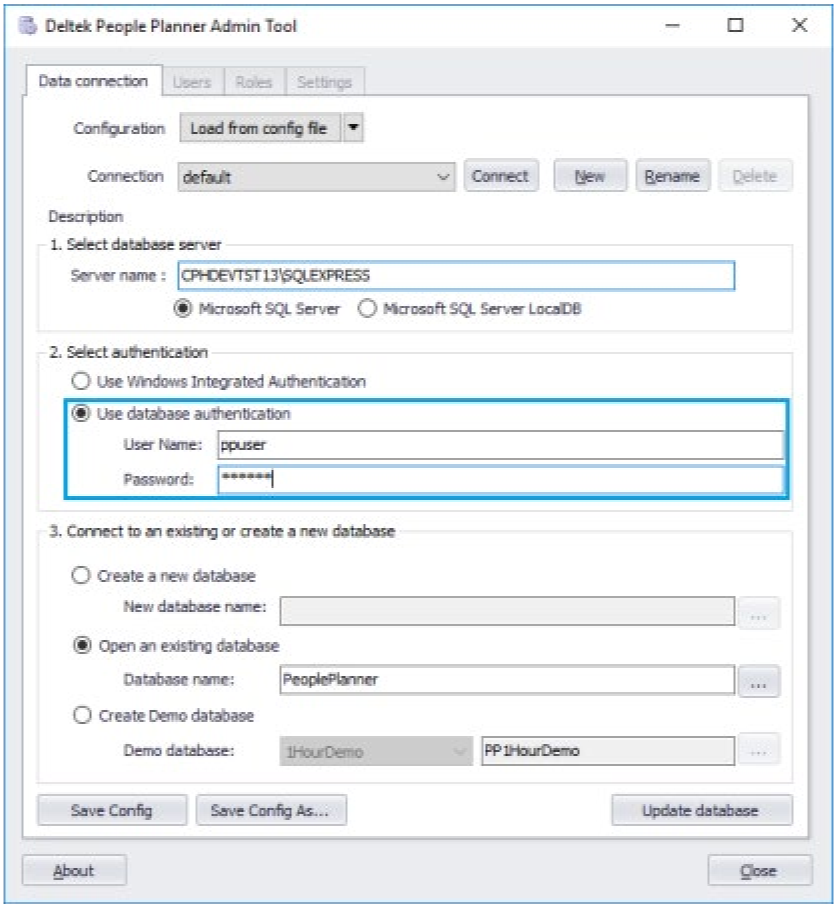


11. Close the **Server Manager**.

Restrictions on the DataConnection.xml File

The DataConnection.xml file contains the details on how to connect to the People Planner database; each of the People Planner applications needs its own copy of this file. Create a People Planner Database describes how to configure this file.

When used by the People Planner Web applications, the DataConnection.xml file must be configured for using Database Authentication.



Installation and Basic Setup of the People Planner Core Software

Any People Planner installation starts with the following steps:

1. Install the People Planner Admin Tool.
2. Install the People Planner Web Applications, including the People Planner Security Service.
3. Use the Admin Tool to:
    a. Create a new People Planner database.
    b. Do the basic setup of the People Planner system.
    c. Create the DataConnectin.xml file.
4. Install and configure the People Planner Windows Application.
5. Use the People Planner Windows Application to verify that the People Planner installation works.

Note: In this section, the installation of the People Planner Windows Application is on the server. The installation of a People Planner Windows Application on each client computer can be done in the same manner, but it is recommended that instead you use a Group Policy to push the Deltek People Planner.msi file to the client computers. Procedures for doing this are not provided in this guide.

Install the People Planner Admin Tool

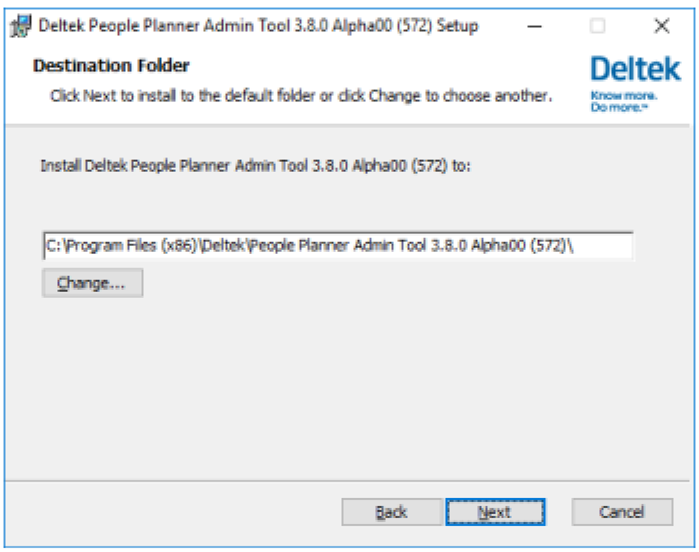
The People Planner Admin Tool is used for the basic setup and customization. Any installation of the People Planner software therefore starts with the installation of the Admin Tool.

To install the Admin Tool:

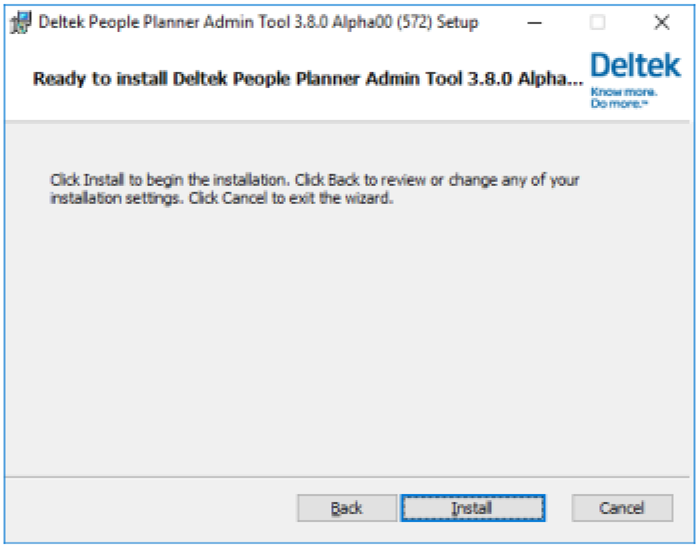
1. Extract the zip file that contains the People Planner installers.
2. Double-click the **Deltek People Planner Admin Tool msi file** and click **Yes** when you are prompted to allow the installer to make changes on your computer.

The Admin Tool Setup Wizard then starts.

3. Click **Next** to continue.

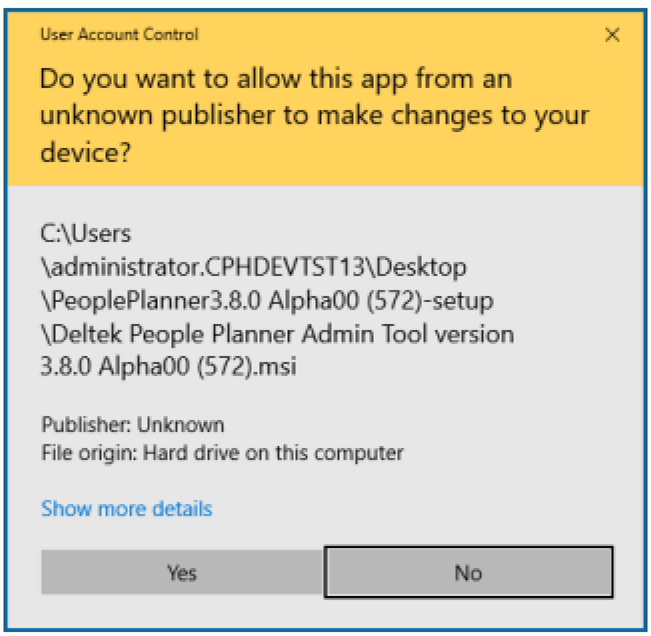


4. Click **Next** to continue.



5. Click **Install** to begin the installation.

Note: At this point the User Account Control dialog box might prompt you for confirmation. Click **Yes** to accept.



6. Click **Finish** to close the Setup Wizard.

Tip: See also Side-by-Side Installations.

Install the People Planner Web Applications

Installing the **People Planner Security Service** is required if you want to be able log in to the People Planner Windows Application.

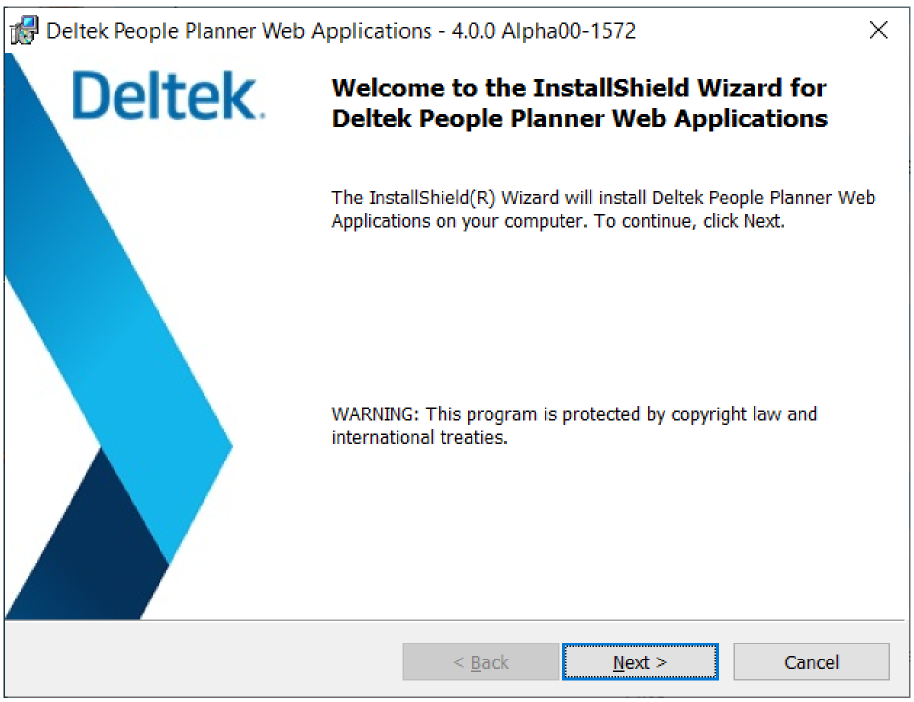
From People Planner 4.0 and on, the Security Service is included in the collective installer for the **People Planner Web Applications**.

> **Prerequisite:** You must install the ASP.NET Core Runtime 6.0 Hosting Bundle before you install the Web Applications. You can download this from the Microsoft .NET Download homepage (https://dotnet.microsoft.com/download).

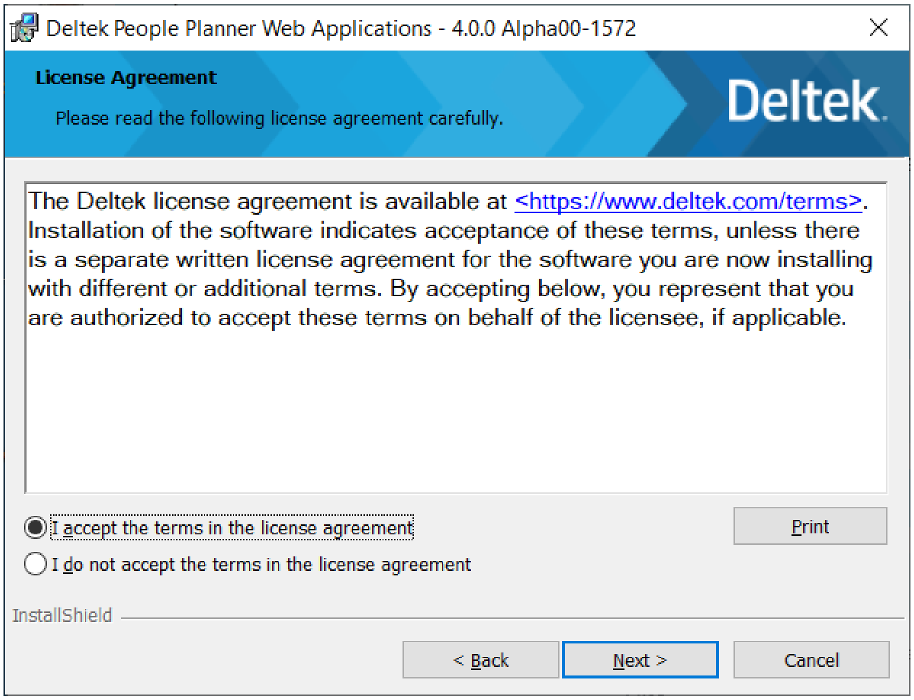
To install the People Planner Web Applications:

1. Extract the zip with the People Planner installers.
2. Double-click the **Deltek People Web Applications exe-file** and click **Yes** if you are prompted to allow the installer to make changes on your computer.

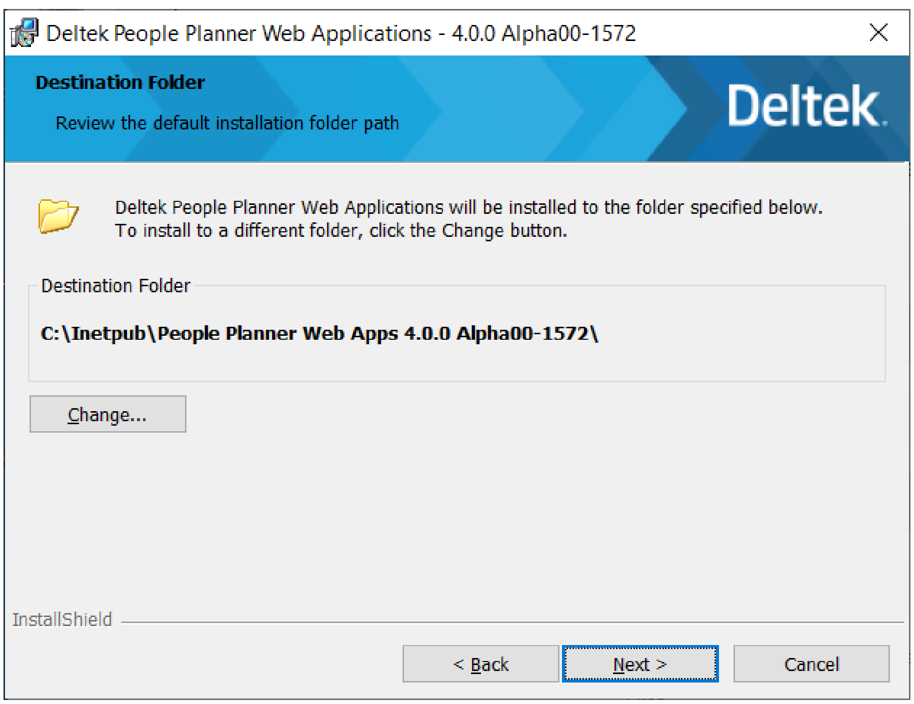
   The Setup Wizard starts.

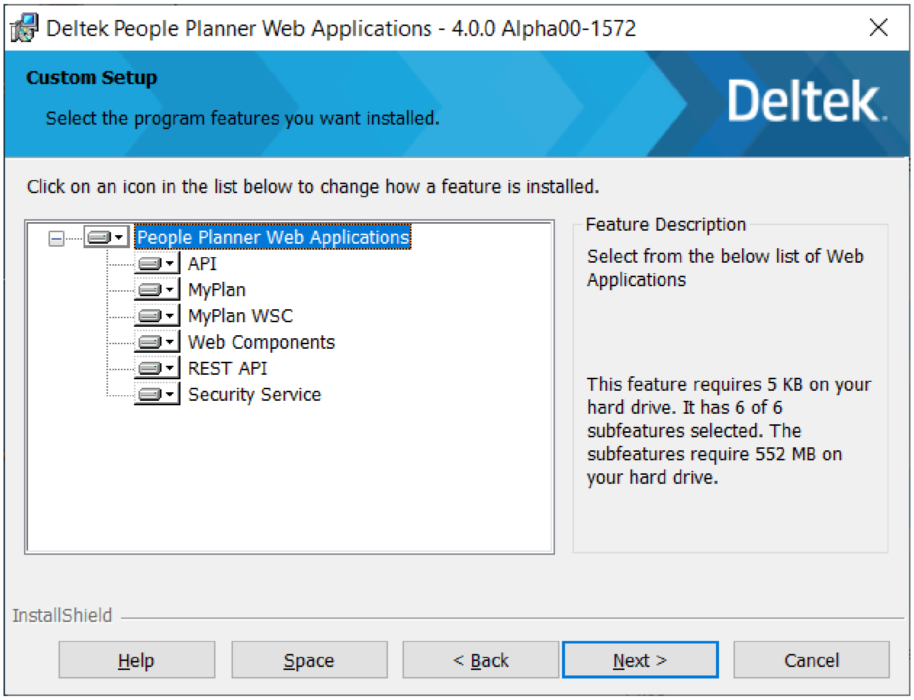
3. Click **Next** to continue.



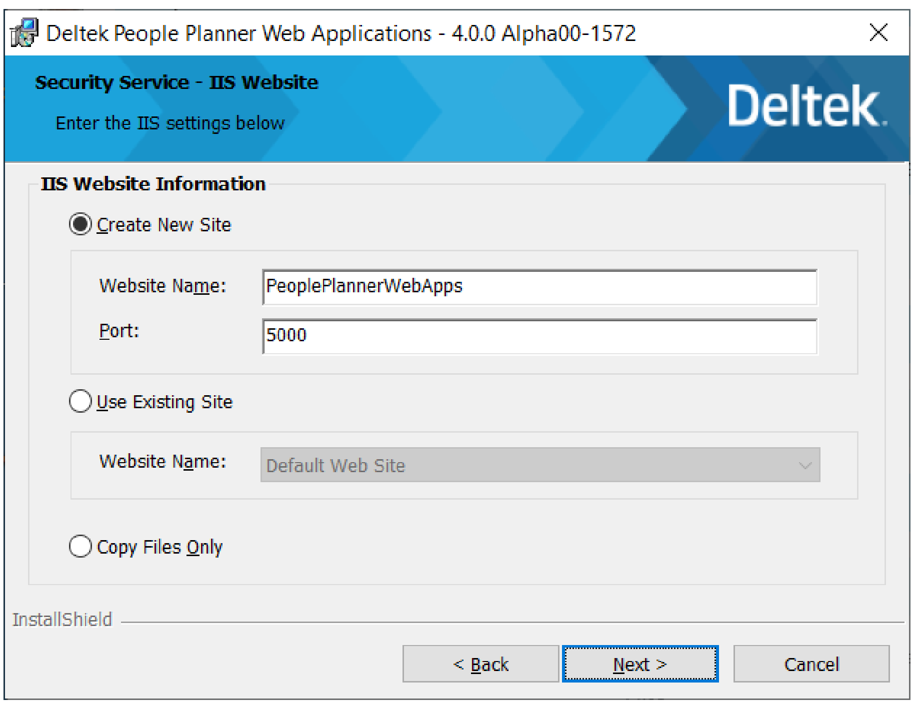
4. Accept the license, and then click **Next** to continue.



5. Click **Next** to continue.



6. Click **Next** to continue.



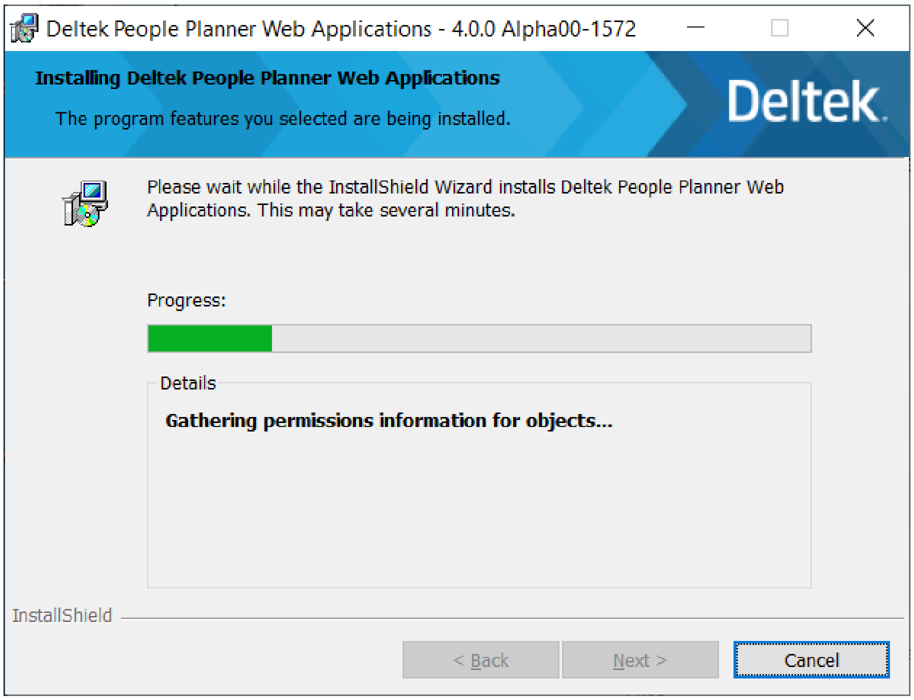
7. Select the Web site where you want to install the People Planner Web Applications.

   You can choose between creating a new web site or chose to install them under an existing web site.

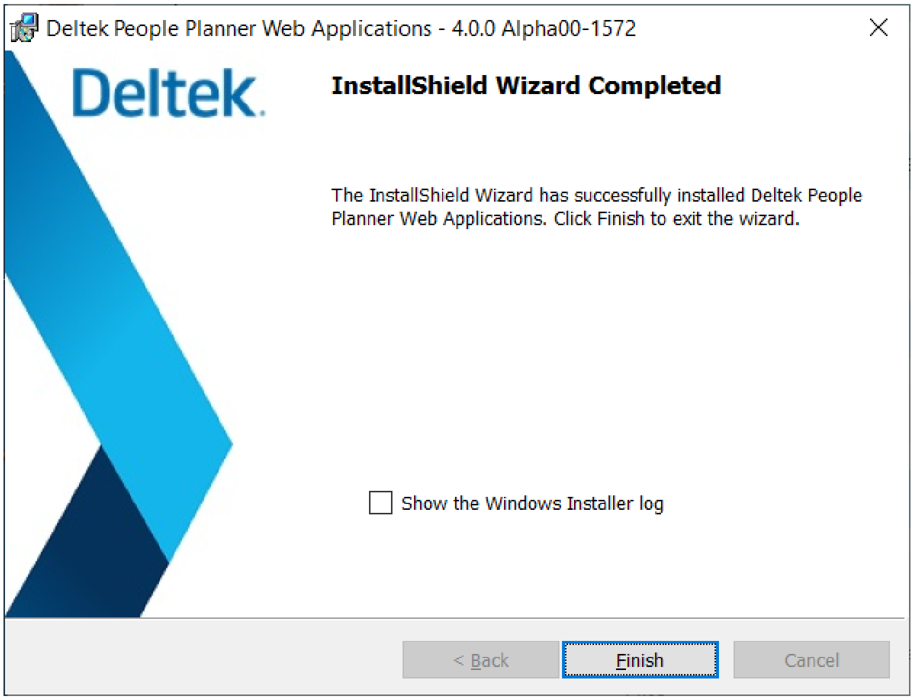
Note: The web site should be set up for using SSL and for Windows Authentication.

When the People Planner Windows Application connects to the Security Service, it must be over SSL; otherwise, there is no added security. See the appendix Configure the People Planner Windows Application to Use the Security Service for additional details about setting up the connection between the People Planner Windows Application and the Security Service.

8. Click **Next** to continue.



9. Click **Install** to begin the installation.



10. Click **Finish** to close the Setup Wizard.

Next, the People Planner Web Applications needs to have access to the DataConnection.xml file to connect to the People Planner database. See Create a People Planner Database for information about how to create and where to place the DataConnection.xml file.

At this stage of the People Planner installation, we are mainly interested in the People Planner Security Service as this is required by the setup of the People Planner Windows Application. For further information about the setup of the remaining People Planner Web Applications, please see section Setup of the People Planner Web Applications.

Create a People Planner Database

When the People Planner Admin Tool has been installed, you can use it to create an empty People Planner database.

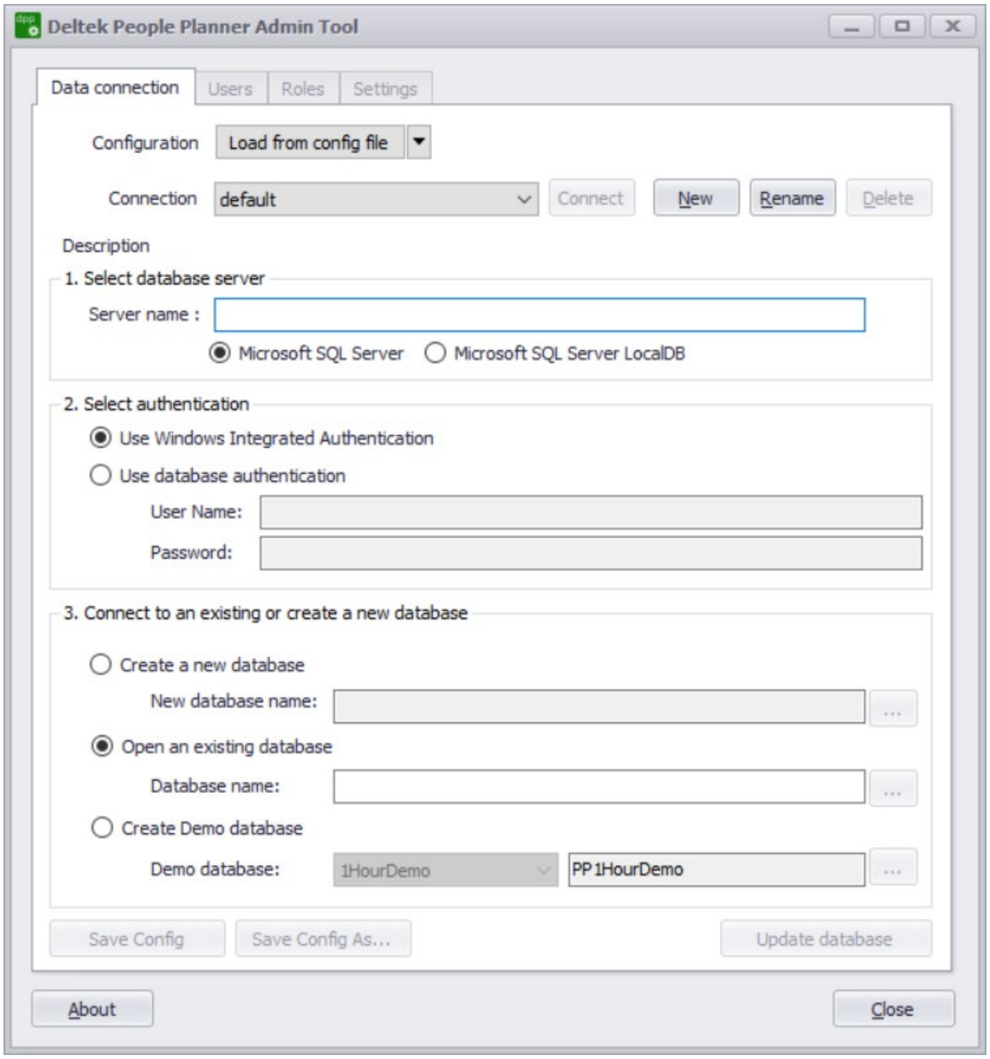
The following is an overview of the steps:

1. Use the People Planner Admin Tool to create a People Planner database.
2. Use the SSMS to create a login and assign it to the database.
3. Use the People Planner Admin Tool to configure the DataConnection.xml file.
4. Use the People Planner Admin Tool to perform some basic configuration tasks.

Create a People Planner Database

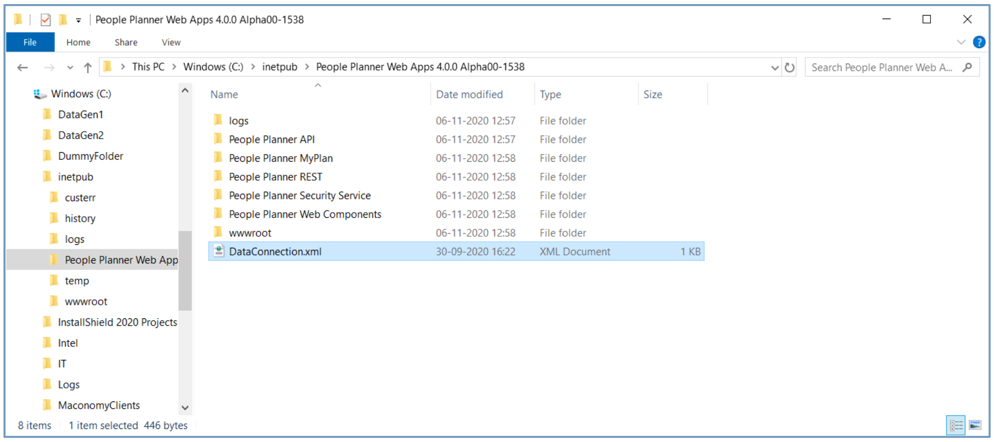
To create a People Planner database:

1. Run the **People Planner Admin Tool**.



2. Click the **Load From Config File** button. This opens an Open File dialog box.

3. Use the Open File dialog box to locate and load the existing **DataConnection.xml** file under the People Planner Web Apps directory under the inetpub directory.

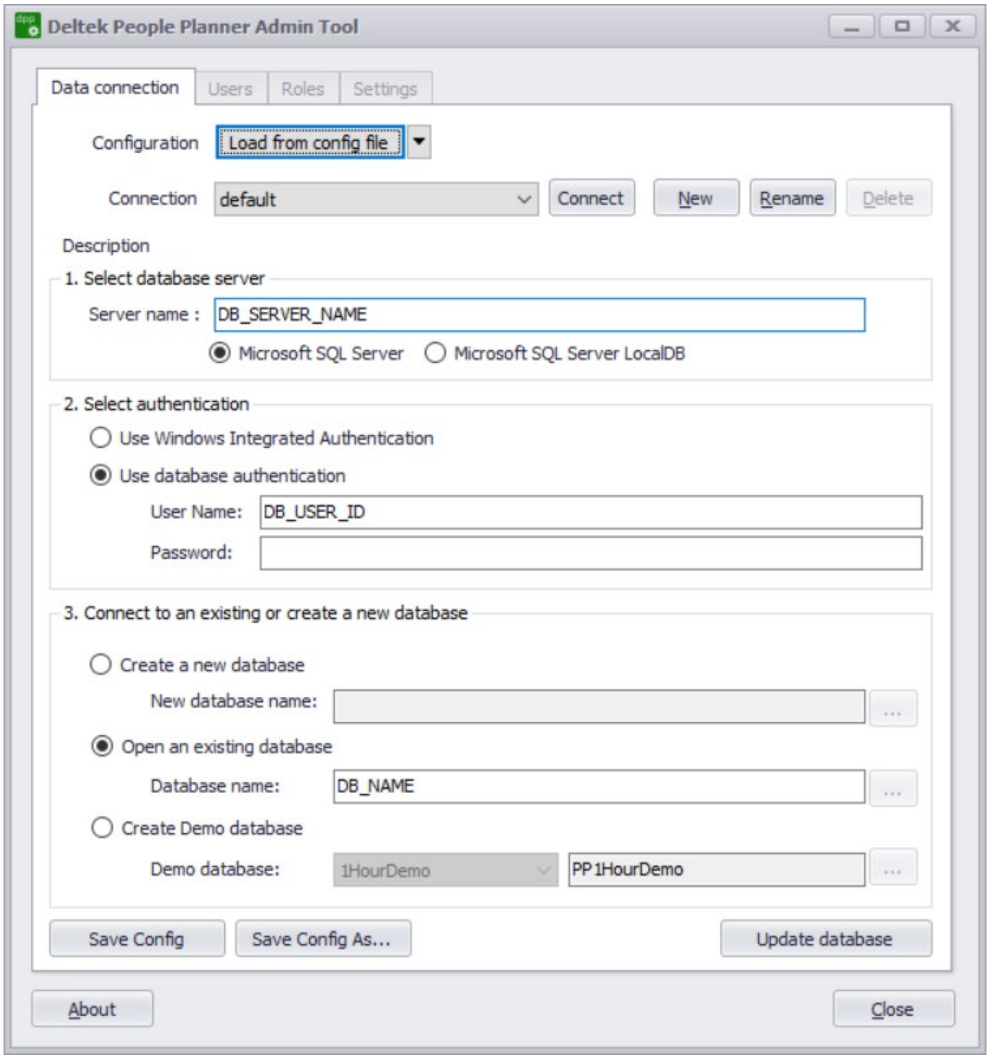


The path looks something like the following:

`C:\inetpub\People Planner Web Apps 3.8.6 Alpha00 (383)\DataConnection.xml`

> **Note:** Before People Planner 3.8.6, the DataConnection.xml file was located in the People Planner installation directory.

If this is the first time that People Planner has been installed on this computer, this file only contains the dummy settings.



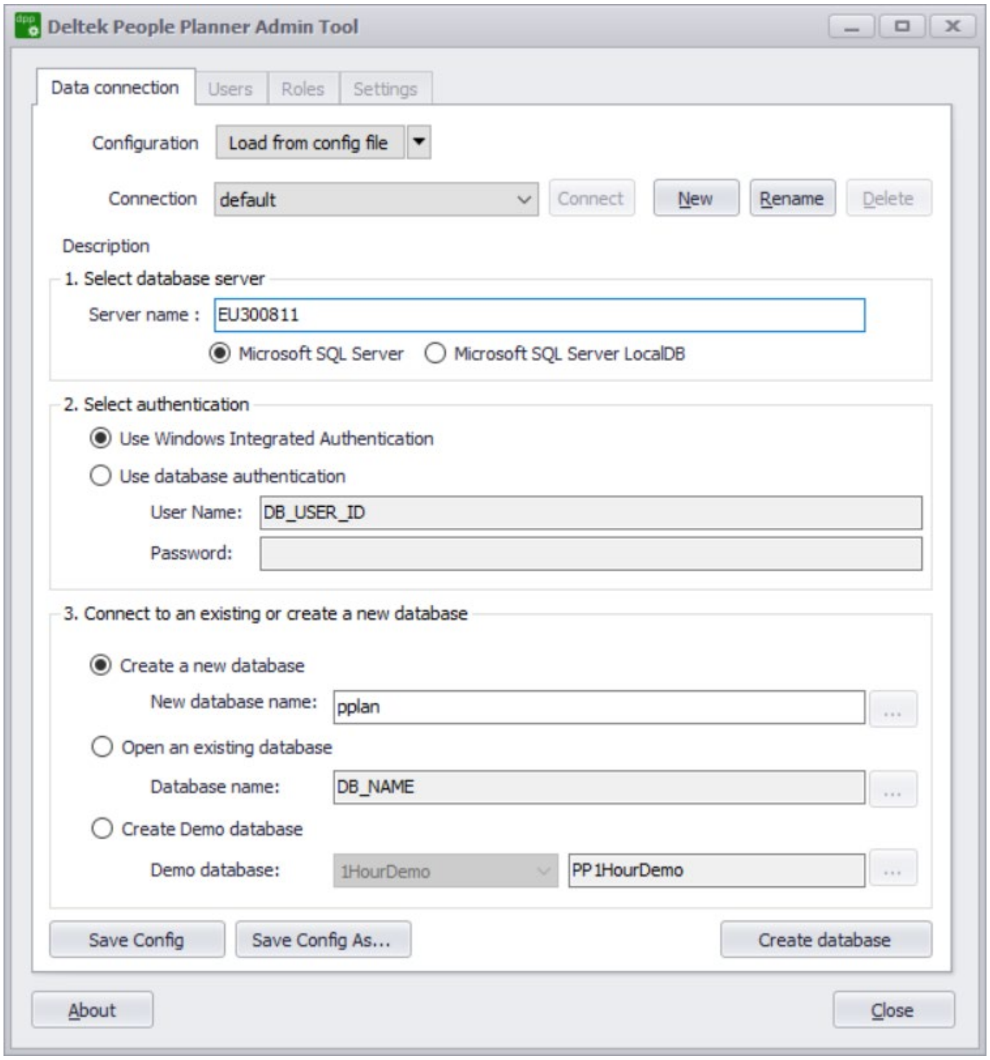
4. Enter the SQL Server and instance in the **Server name** field.

> **Tip:** The **Microsoft SQL Server** radio button is selected by default; this is normally the correct setting.
>
> You typically select the Microsoft SQL Server LocalDB radio button only in a few cases, such as setting up a small demo system.

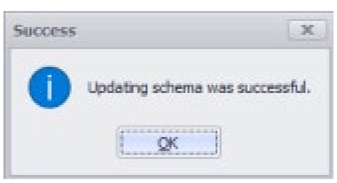
5. Under **Select authentication**, do **one** of the following to specify an account that has privileges to create a database on the SQL Server:
   - Use **Windows Integrated Authentication**.
   - Use the **sa** user.

> **Note:** Before the People Planner database has been completed, change to a user that has only enough privileges to read and write to the database. See Configure the DataConnection.xml File to Use the ppuser Login.

6. Select **Create a new database** and enter a name for the database, such as **pplan**.



7. Click the **Create database** button. The database is created.



8. Click the **Save Config** button to save the modified DataConnection.xml file.

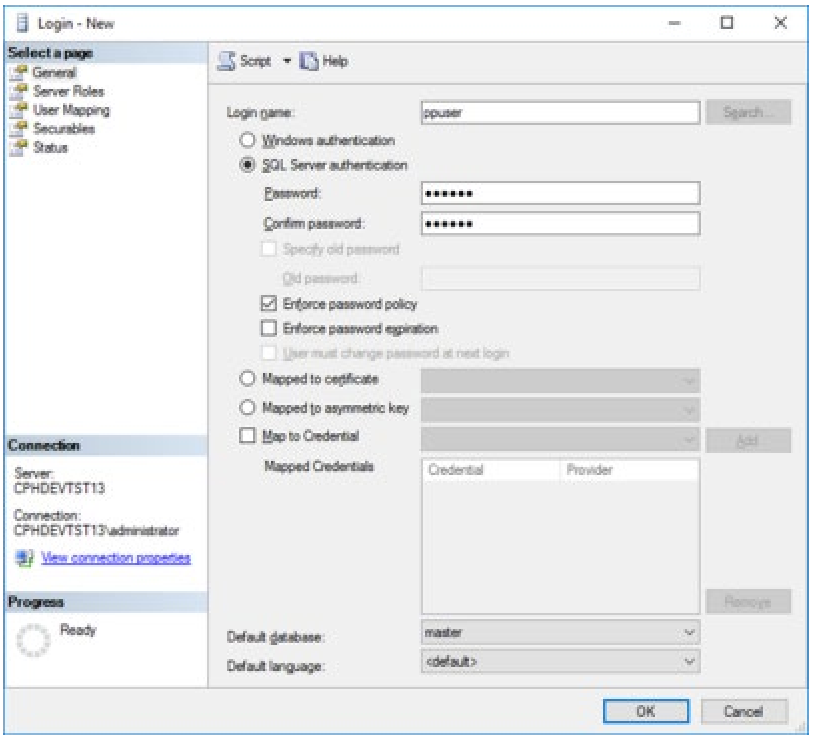
Tip: See also Side-by-Side Installations.

Create a Database Login

To create a database login:

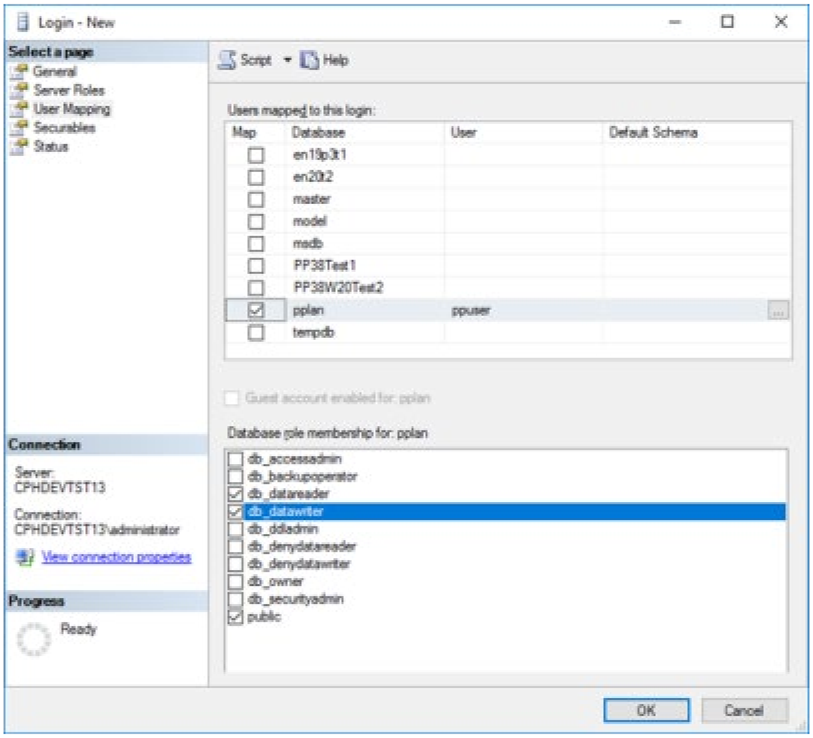
1. Run the **SQL Server Management Studio** application.

2. Navigate to **Security » Logins**.
3. Right-click and then click **New Login…**
4. Under **Select a page**, click **General**.
5. Enter a name for the login, such as **ppuser**.
6. Select **SQL Server authentication**.
7. Enter a password in the **Password** field and confirm it in the **Confirm password** field.
8. Deselect the **Enforce password expiration** check box to set the password policy to never expire.



9. Under **Select a page**, click **User Mapping**.
10. Select the **People Planner database**, for example pplan in the following figure.

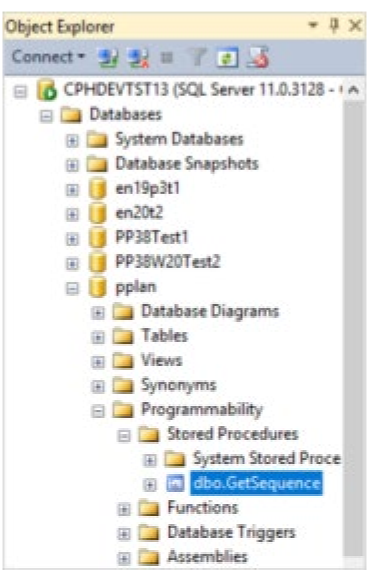
11. Select the database roles **db_datareader**, **db_datawriter**, and **public**.



12. Click **Ok**.

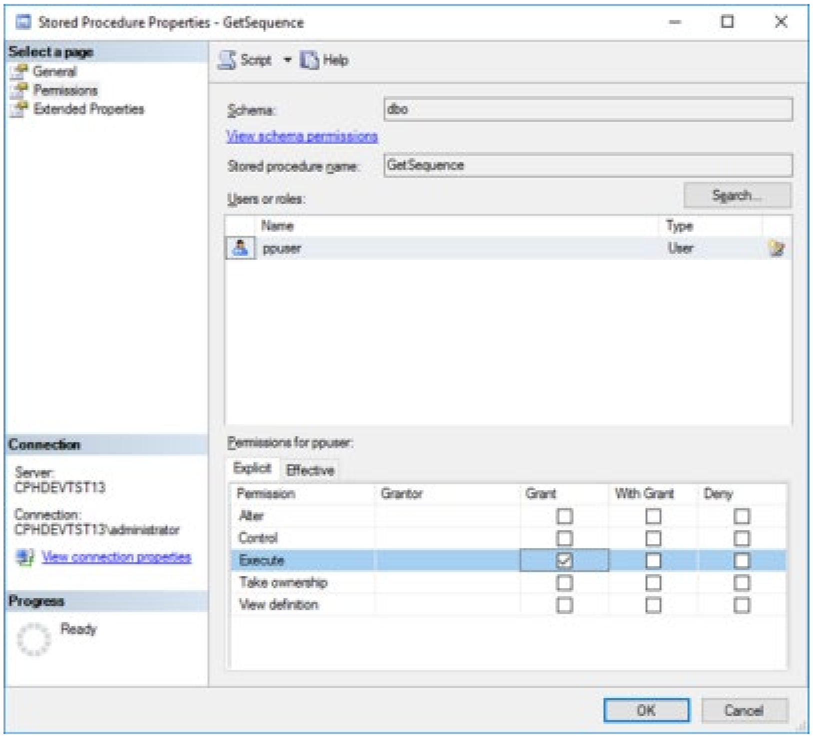
To give the database login execute privileges to the GetSequence stored procedure:

1. Under **Databases**, select the **People Planner database**.
2. Navigate to **Programmability » Stored Procedures**.
3. Select the **GetSequence** stored procedure.



4. Right-click and then click **Properties**.

5. Under **Select a page**, click **Permissions**.
6. Use **Search** to find the ppuser login.
7. Under **Permissions for ppuser**, on the **Explicit** tab, select the **Grant** check box for the **Execute** permission.



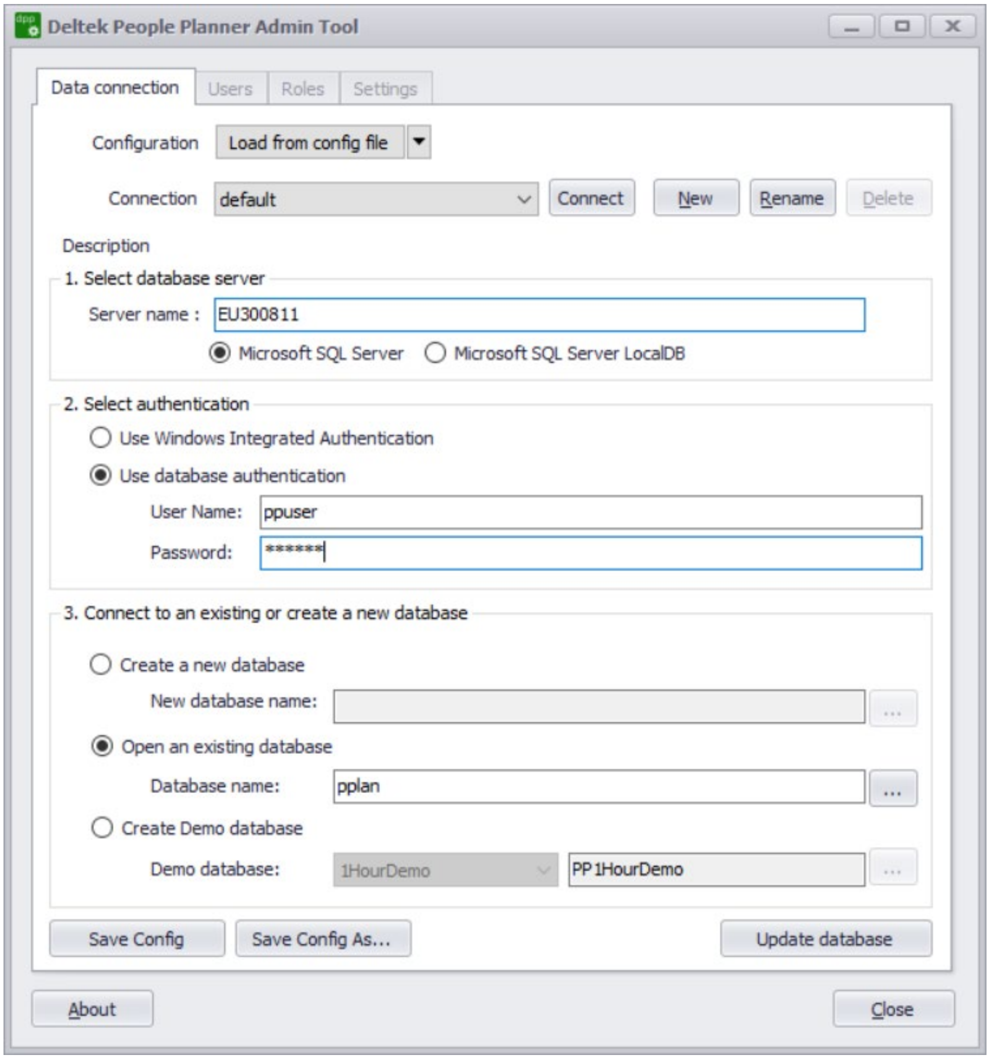
8. Click **OK**.

Configure the DataConnection.xml File to Use the ppuser Login

To configure the DataConnection.xml file to use the ppuser login:

1. Run the **People Planner Admin Tool**.
2. Load the **DataConnection.xml file**.
3. Under **Select authentication**, select **Use database authentication**.

4. Enter the user name and password that you created for the ppuser database-login in the **User Name** and **Password** fields, respectively.



5. Click the **Save Config** button to save the modified DataConnection.xml file.

After you have configured the DataConnection.xml file, you must restart the People Planner Security Service so that it rereads the changed settings.

Verification

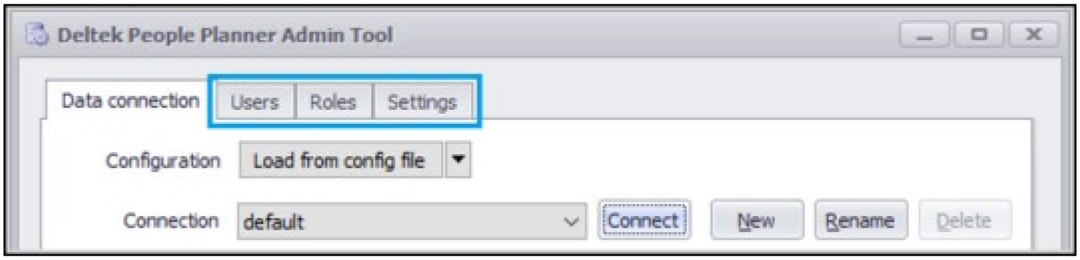
To verify that the People Planner database has been created correctly and that the People Planner software will be able to connect to it:

1. Close the **People Planner Admin Tool**.
2. Restart the **Admin Tool**, and load the **DataConection.xml file**.
3. Verify that the database settings are all correct.

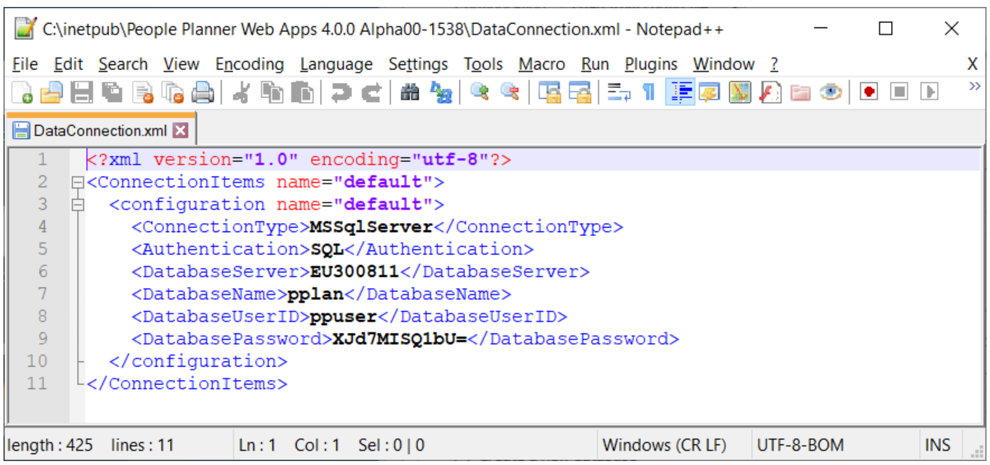
> **Note:** For security reasons, the password field is blanked out.

4. Enter the password for the ppuser login.
5. Click the **Connect** button.

   The **Users**, **Roles**, and **Settings** tabs should become enabled, as shown in the following figure.



Note: When this part of the setup is finished, the DataConnection.xml file should look like the following figure.




```xml
<?xml version="1.0" encoding="utf-8"?>
<ConnectionItems name="default">
  <configuration name="default">
    <ConnectionType>MSSqlServer</ConnectionType>
    <Authentication>SQL</Authentication>
    <DatabaseServer>EU300811</DatabaseServer>
    <DatabaseName>pplan</DatabaseName>
    <DatabaseUserID>ppuser</DatabaseUserID>
    <DatabasePassword>XJd7MISQ1bU=</DatabasePassword>
  </configuration>
</ConnectionItems>
```

Basic Configurations

When you have created a new People Planner database, you can use the People Planner Admin Tool to add the basic settings to it.

The basic configurations consist of:

- Adding yourself as a People Planner Admin user.
- Configuring the path to the People Planner license file.
- Configuring the URLs to the Maconomy integration.
- Configuring settings to the People Planner Silent Sign-In.

The last two items are related to the integration with a Maconomy system, and are described in Installation and Basic Setup of the Maconomy Web Services and in Set Up People Planner Silent Sign-In, respectively.

Add Yourself as an Admin User to the People Planner Database

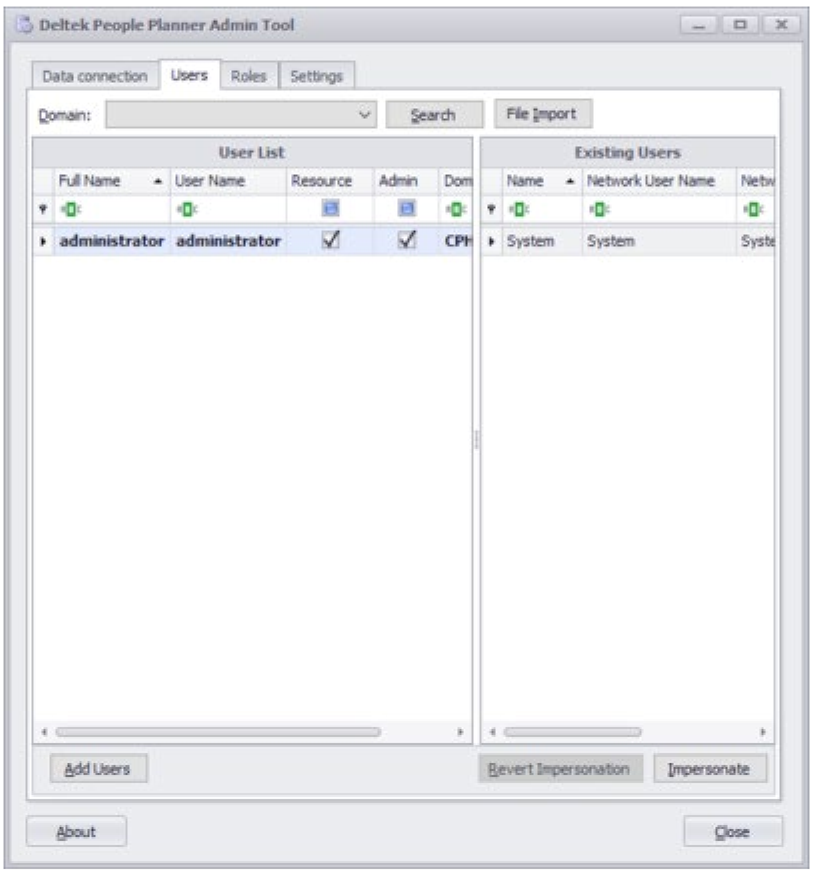
Before you can log in to the People Planner system, you must be added to the People Planner database as a People Planner Admin user.

To add yourself as an Admin user:

1. Run the **People Planner Admin Tool**.
2. Load the **DataConnection.xml file**.
3. Enter the password for the ppuser.

> **Warning:** Alternatively, you can switch to Windows Integrated Authentication for this. However, you then must be careful not to save this change to the DataConnection.xml file.

4. Click **Connect** to connect to the People Planner database.
5. Click the **User**s tab.



6. Click **Add Users** to add yourself as a resource and as a People Planner Admin user.

It is not important that you be added as a resource. However, only users that are also a resource can start the People Planner MyPlan Web application. Thus, if you do not add yourself as a resource, you will not be able to later verify that you have installed MyPlan correctly.

Note: If you have not added yourself as a user, you will get the following error message when you try to start the People Planner Windows Application.

Set Up the People Planner License File

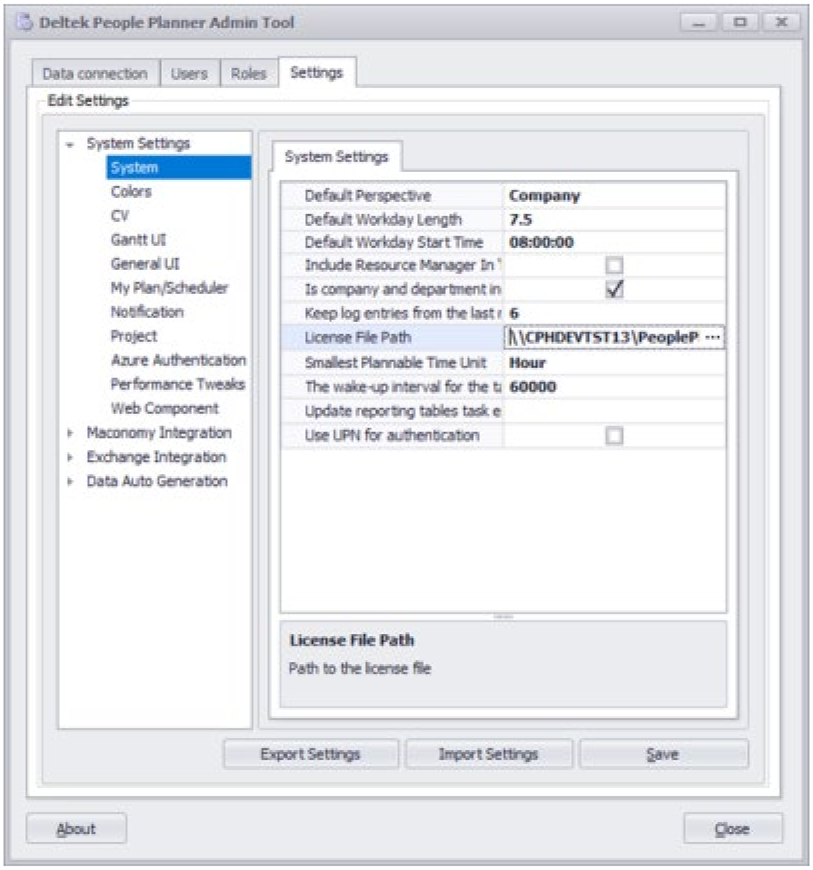
Before anything else, you must decide where to place the People Planner license file, **PeoplePlannerLicense.lic**. Each installation of the People Planner Windows Application must have access to the license file. You have the following options:

- Bundle a copy of the license file with each installation of the People Planner Windows Application.
- Place a single instance of the license file on a network share and point each People Planner Windows Application to that instance.

To set up the license file using a single copy on a network share and pointing each People Planner Windows Application to that copy:

1. Create a folder on the file share, for example, C:\PeoplePlanner.
2. Copy the **PeoplePlannerLicense.lic** file to the C:\PeoplePlanner folder.
3. Create a share of the C:\PeoplePlanner, for example \\CPHDEVTST13\PeoplePlanner.
4. Run the **People Planner Admin Tool**.
5. Load the **DataConnection.xml file**, enter the password for the ppuser, and connect to the People Planner database.

6. Click the **Settings** tab.



7. Under **System Settings**, edit the **License File Path** to point at the location of the license file, for example:

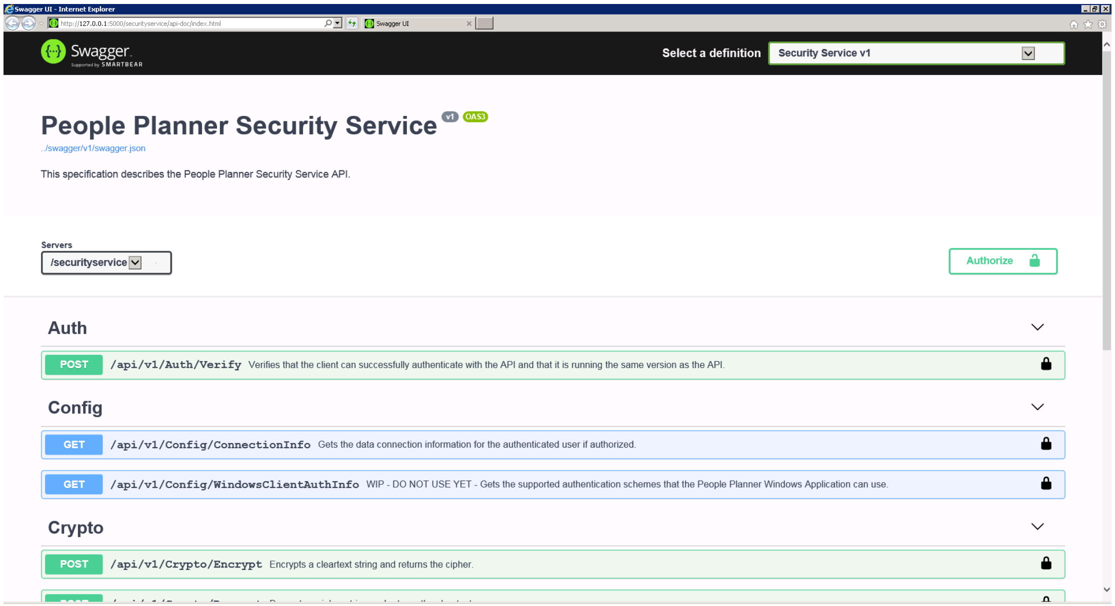
   `\\CPHDEVTST13\PeoplePlanner\PeoplePlannerLicense.lic`

8. Click **Save** to save the changed setting to the People Planner database.

Verification

When the database has been created, and the settings have been saved in the DataConnection.xml file, you should be able to call the People Planner Security Service successfully.

To test this, you can enter the URL to the Swagger documentation page of the Security Service into a browser:



The URL, should look like this:
http://<host>:<port>/SecurityService/api-doc/index.html

Note: Under certain circumstances, if the People Planner Security Service fails with an authentication-error, it may be due to a conflict with Maconomy. See the appendix, section Possible Conflict with Maconomy for details.

Install the People Planner Windows Application

Installing the People Planner Windows Application on the server is not strictly necessary. However, it is convenient because you can use it to verify that you can start the People Planner software.

You can also use it to do the initial imports form Maconomy, when this integration has been set up.

Note: Before People Planner Release 3.8.6, installing the People Planner Windows Application also provided you with a dummy DataConnection.xml file that you could modify, using the Admin Tool. That was an additional reason for installing the People Planner Windows Application. However, beginning with 3.8.6, the DataConnection.xml file has been relocated to the People Planner Web Apps under inetpub.

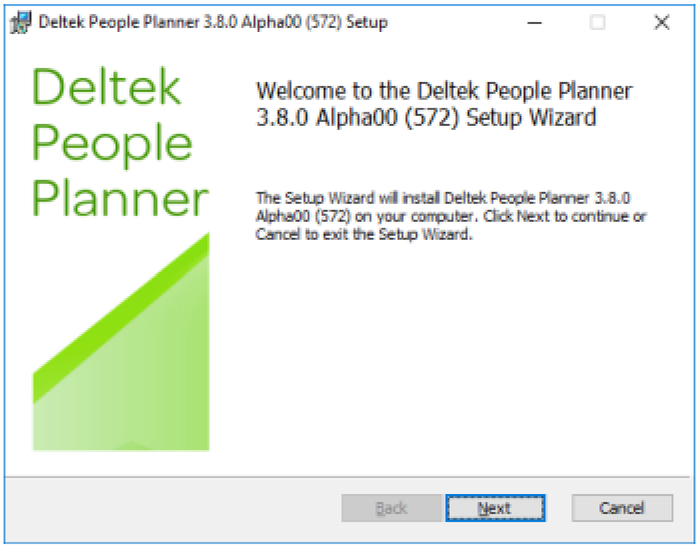
Tip: You sometimes hear the “People Planner Windows Application” referred to as the “People Planner Client,” the “People Planner Rich Client,” or even as the “People Planner Citrix Client.” However, these are misnomers because People Planner is not a Client/Server application.

To install the People Planner Windows Application:

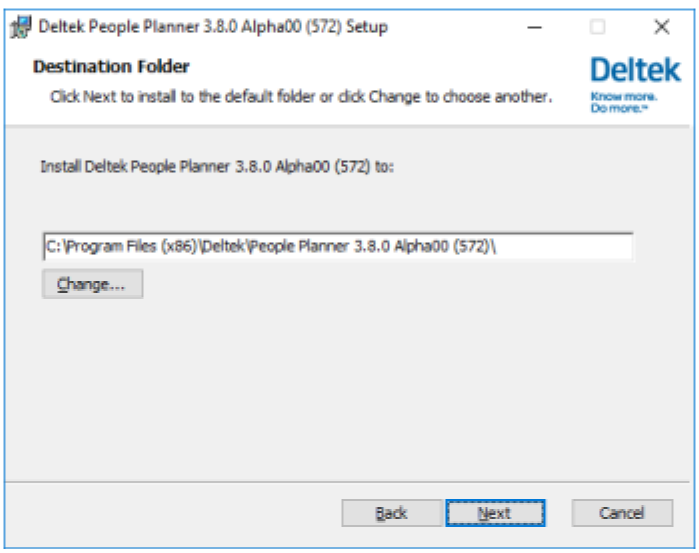
1. Extract the zip file that contains the People Planner installers.

2. Double-click the **InstallPeoplePlanner.vbs** file and click **Yes** at the prompt to allow the installer to make changes on your computer.

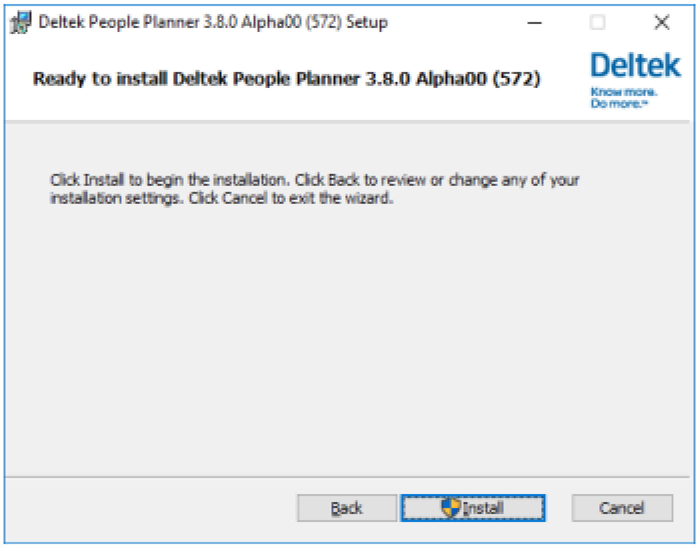
   The People Planner Setup Wizard starts.



3. Click **Next** to continue with the installation.

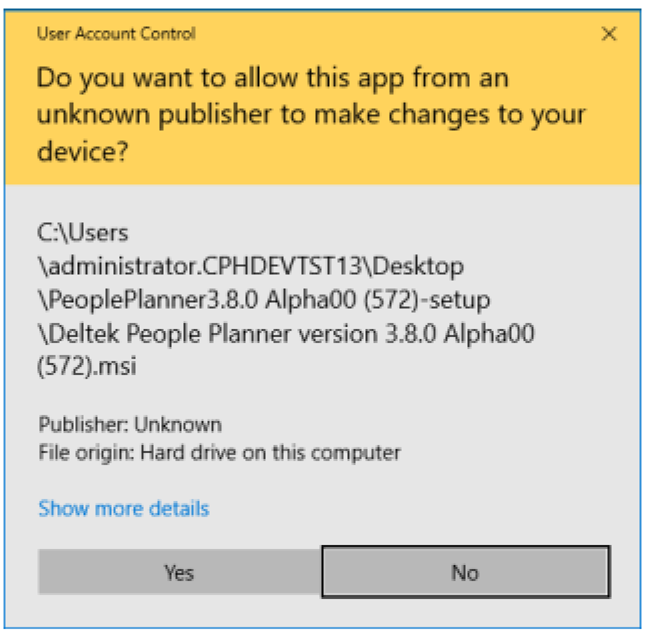


4. Click **Next** to continue with the installation.



5. Click **Install** to begin the installation.

Note: At this point the User Account Control dialog box might prompt you for confirmation. Click **Yes** to accept.



6. Click **Finish** to close the Setup Wizard.

Tip: See also Side-by-Side Installations.

Configure the People Planner Windows Application to Use the Security Service

You must set up the People Planner Windows Application for using the People Planner Security Service.

In the installation directory of the People Planner Windows Application, edit the PeoplePlanner.exe.config file. Look for the section where the URL for the Security Service is configured:

```
<PeoplePlannerSecurityService hideUrls="true" hideTestButton="true">
   <Services>
      <Service name="Default"
      url="https://INSERT_SECURITY_SERVICE_URL_HERE/SecurityService" />
   </Services>
</PeoplePlannerSecurityService>
```

Replace this with the actual URL, which could look something like this:

```
<PeoplePlannerSecurityService hideUrls="true" hideTestButton="true">
   <Services>
      <Service name="Default" url="http://10.4.9.17:5000/SecurityService" />
   </Services>
</PeoplePlannerSecurityService>
```

> **Note:** The People Planner Security Service should be configured for SSL, and only respond on HTTPS-urls.
>
> The People Planner Windows Application, from the end user’s Windows computer, should be able to call the Security Service over HTTPS.
>
> It should be able to authenticate with the IIS, using either Windows Authentication (Kerberos/NTLM) or using Microsoft AzureAD.
>
> The infrastructure must allow for the above: firewalls, proxies, cloud setup, and so on.
>
> See Appendix C: Securing the People Planner Security Service for additional information on how to setup this.

Verification

If you have entered the settings correctly, you should now be able to start the People Planner Windows Application.

It does not look terribly interesting at this point, but that is ok.

Side-by-Side Installations

If you are installing the People Planner Admin Tool or the People Planner Windows Application on a system where an older version of the software is already installed, you will be offered the following options:

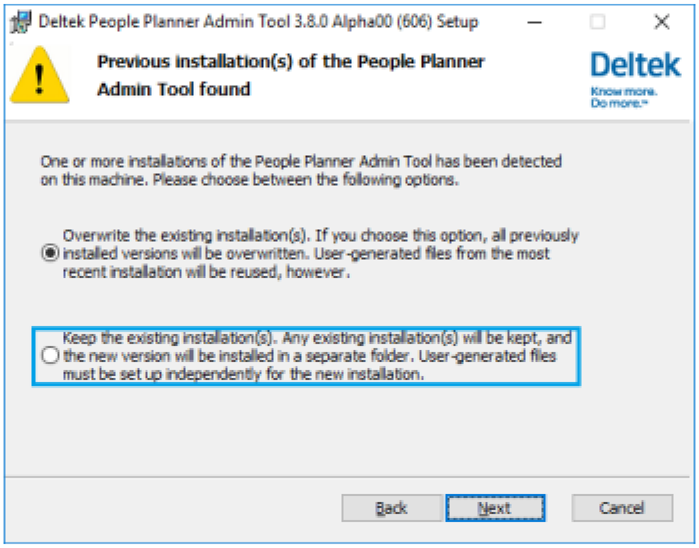
- To update the old version with the new — This removes the old installation.
- To do a side-by-side installation — This keeps the old installation.

Side-by-side installations can be useful if you want to keep the old version while trying out the new version. Such an installation is usually combined with a separate People Planner database for each version.

Of the People Planner software, only the People Planner Admin Tool, the People Planner Windows Application, and the People Planner Service support side-by-side installations out-of-the-box. You can do side-by-side installations of the other People Planner software. However, this is a manual process and it is not covered in this guide.

Side-by-Side Installation of the People Planner Admin Tool

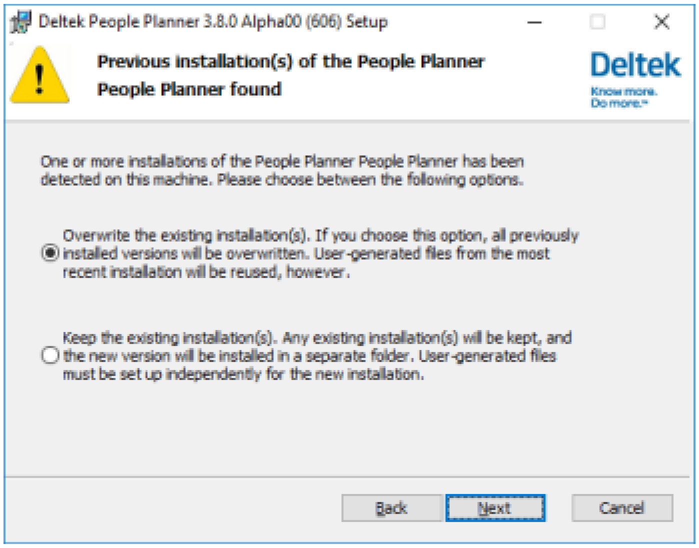
If an older version of the People Planner Admin Tool already exists, the Setup Wizard gives you the option to **Overwrite** or to **Keep the existing** installation. Keeping the existing installation amounts to doing a side-by-side installation. The installation process is otherwise identical.



Warning: When you have multiple installations of the People Planner Admin Tool, and you want to use one of these to update one of the People Planner databases, you should be careful that you are updating the correct database. Unless you have a backup, you cannot reverse an update. The People Planner software has a built-in version check, and you cannot use a version of People Planner with a database that has been updated to a newer version of People Planner.

Side-by-Side Installation of the People Planner Windows Application

If an older version of the People Planner Windows Application already exists, the Setup Wizard gives you the option to **Overwrite** or to **Keep the existing installation**. Keeping the existing installation amounts to doing a side-by-side installation. The installation process is otherwise identical.



Each installation of the People Planner Windows Application needs its own individual version of the DataConnection.xml file. To create these files, you need a side-by-side installation of the People Planner Admin Tool as well.

> **Note:** Versions of the People Planner Windows Application prior to People Planner Release 3.8.6 require a copy of the DataConnection.xml file to exist in the Settings subfolder under the application's installation folder.
>
> Versions of the People Planner Windows Application beginning with People Planner Release 3.8.6 require an installation of the corresponding People Planner Security Service. These versions do **not** have a DataConnection.xml file in the Settings subfolder.

In addition, each installation requires its own version of the People Planner database; two different versions of the People Planner software cannot use the same People Planner database. You can create the databases using the Admin Tool as described in Create a People Planner Database.

Side-by-Side Installation of the People Planner Service

The installation and configuration of the People Planner Service are described in Installation and Basic Setup of the People Planner Service.

If an older version of the People Planner Service already exists, the Setup Wizard gives you the option to **Overwrite** or to **Keep the existing installation**. Keeping the existing installation amounts to doing a side-by-side installation. The installation process is otherwise identical.

Each installation of the People Planner Service needs its own individual version of the DataConnection.xml file, and they need to connect to two different versions of the People Planner database. The DataConnection file is created as described in Side-by-Side Installation of the People Planner Windows Application and is then copied to each of the installation folders of the People Planner Services.

Side-by-Side Databases – Different People Planner Versions

With side-by-side installations of at least two different versions of the People Planner Admin Tool, you can create a People Planner database for each of the systems. Indeed, this is a requirement because you cannot use the same People Planner database from two different versions of People Planner; a version-check prevents this.

The process for creating a People Planner database is described in Create a People Planner Database; there is nothing new to add to that information.

Side-by-Side Databases – Same People Planner Version

A different kind of side-by-side database scenario is when you only have one version of the People Planner software, but you want to be able to connect to different databases, for example, to a test database and to the production database.

To do this, you must install a People Planner Security Service for each database to which you want to provide access. See Configure the People Planner Windows Application to Use the Security Service for information about how to configure the Windows Application to use multiple Security Services.

Installation and Basic Setup of the People Planner Service

The People Planner Service is a Windows Service used for running import and export jobs that must be executed on a scheduled basis. It is also a required install if the People Planner system is intended to be integrated with an external system, such a Maconomy installation.

Create a Service Account

The People Planner Service is a Windows service, and therefore it needs an account to run.

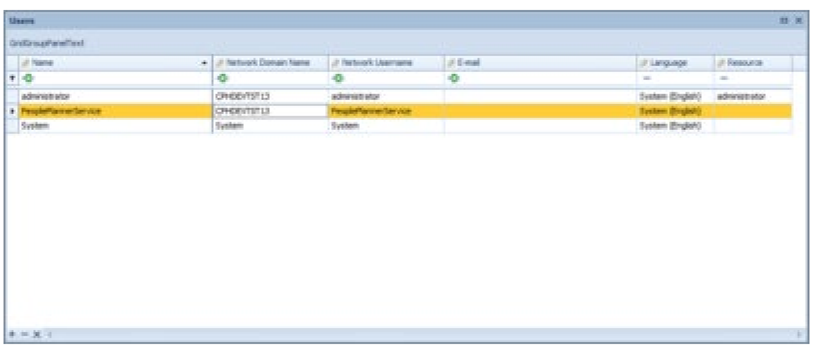
You can use the same account as you are using as People Planner Admin user, or you can create an account specifically for this purpose:

1. Create a user on the system, for example, named PeoplePlannerService.
    a. Enter a password.
    b. Deselect the **Enforce password expiration** check box to set the password policy to never expire.

Add the Account as a People Planner User

Next, you must add this account as a user in People Planner:

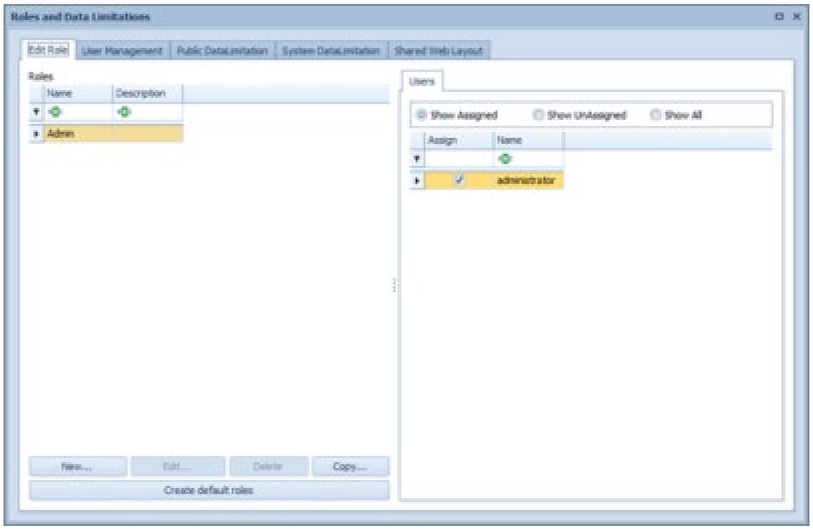
1. Run the **People Planner Windows Application** as the Admin user.
2. Navigate to **Views » Security » Users**.
3. To add a new user, click the **+** button in the lower-left corner of the **Users** view.
4. Enter **PeoplePlannerService** in the **Name** field.
5. Enter the domain name, for example the computer name, in the **Network Domain Name** field.
6. Enter **PeoplePlannerService** in the **Network User Name** field.



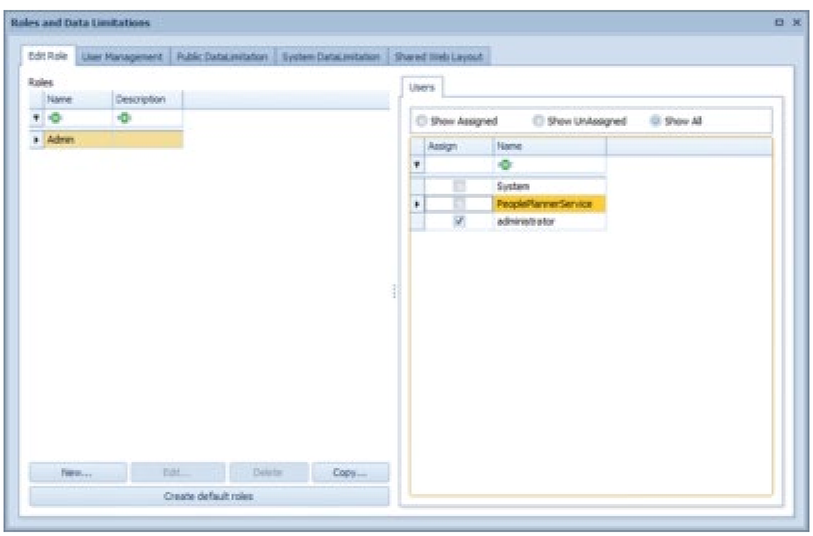
Make the Account into a People Planner Admin User

The People Planner Service requires that the user is also a people Planner Admin user:

1. Run the **People Planner Windows Application** as the Admin user.
2. Navigate to **Views » Security » Roles and Data Limitations**. Alternatively, you can navigate under the top navigation bar » Home » Roles and Data Limitations.



3. Click the **Edit Role** tab.
4. Click the **Admin** role.
5. Select either the **Show UnAssigned** or **Show All** radio button to see the users that are not assigned to the Admin role.



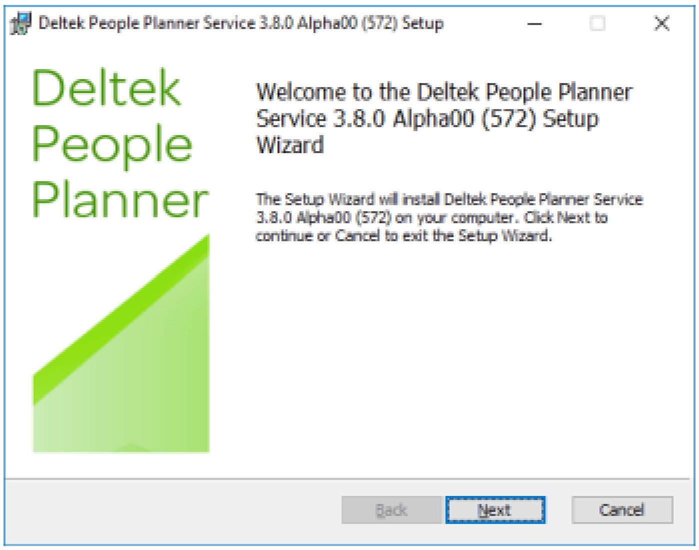
6. Select the **Assign** check box for the **PeoplePlannerService** user.

Note: Future versions of the People Planner Service might relax the requirement that the user must be a People Planner Admin user.

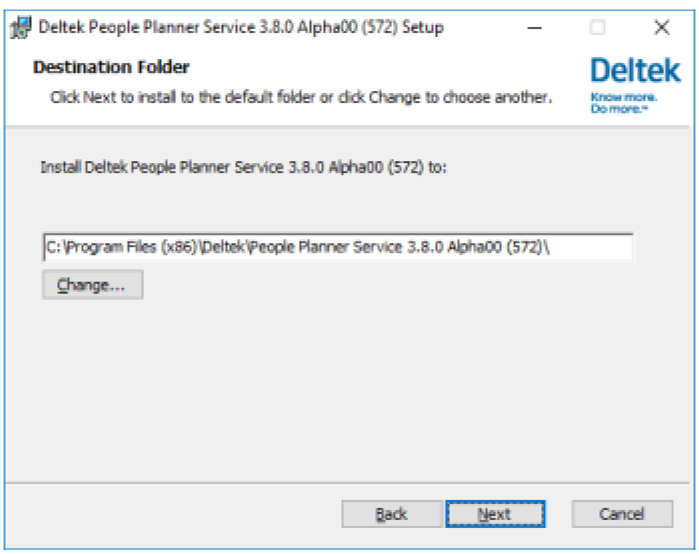
Install and Configure the People Planner Service

To install the People Planner Service software:

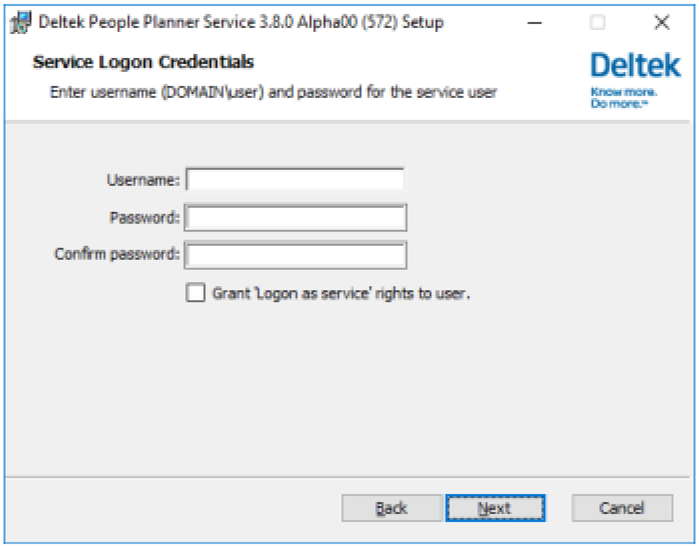
1. Extract the zip file that contains the People Planner installers.
2. Double-click the **InstallPeoplePlannerService.vbs** file and click **Yes** at the prompt to allow the installer to make changes on your computer. The Deltek People Planner Service Setup Wizard then starts.



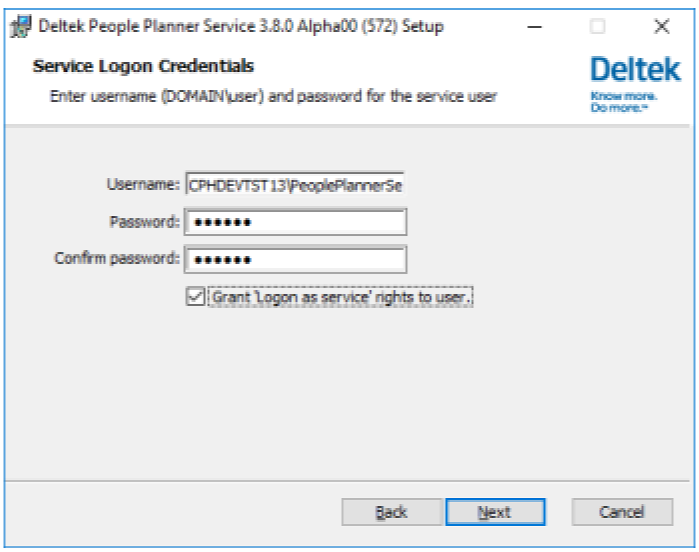
3. Click **Next** to continue.



4. Click **Next** to continue.

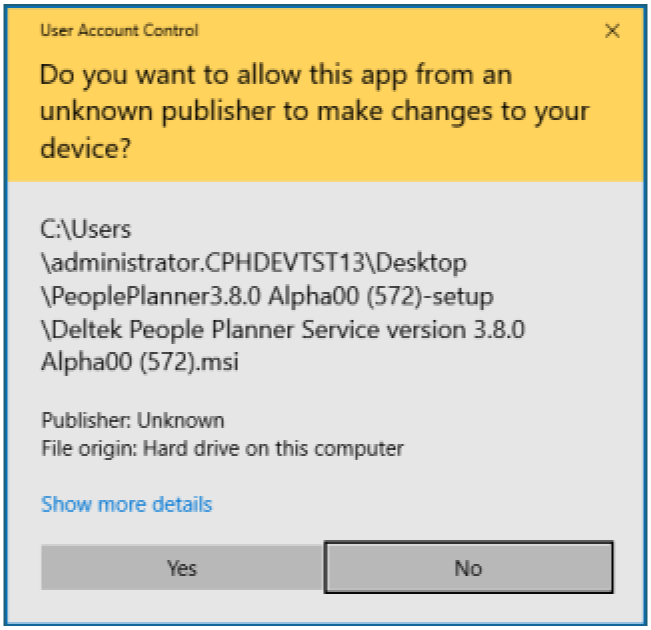


5. In the **Service Logon Credentials** dialog box, enter the user name and password for the PeoplePlannerService user in the **Username** and **Password** fields, respectively, and confirm the password.



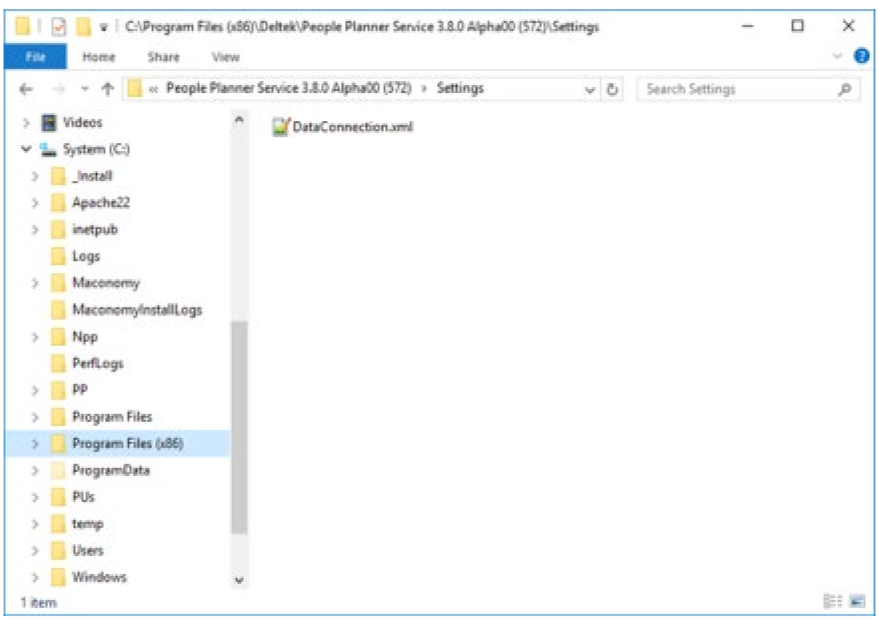
6. Select the **Grant 'Logon as service' rights to user** check box.
7. Click **Next** to continue.

> **Note:** At this point the User Account Control dialog box might prompt you for confirmation. Click **Yes** to accept.



8. Click **Finish** to close the Setup Wizard.

When you have installed the People Planner Service, you must copy the **DataConection.xml file**—which is located in the installation folder of the People Planner Security Service under the inetpub folder—to the **Settings** subfolder under the location where you installed the People Planner Service, overwriting the existing DataConnection.xml file.



Tip: See also Side-by-Side Installations.

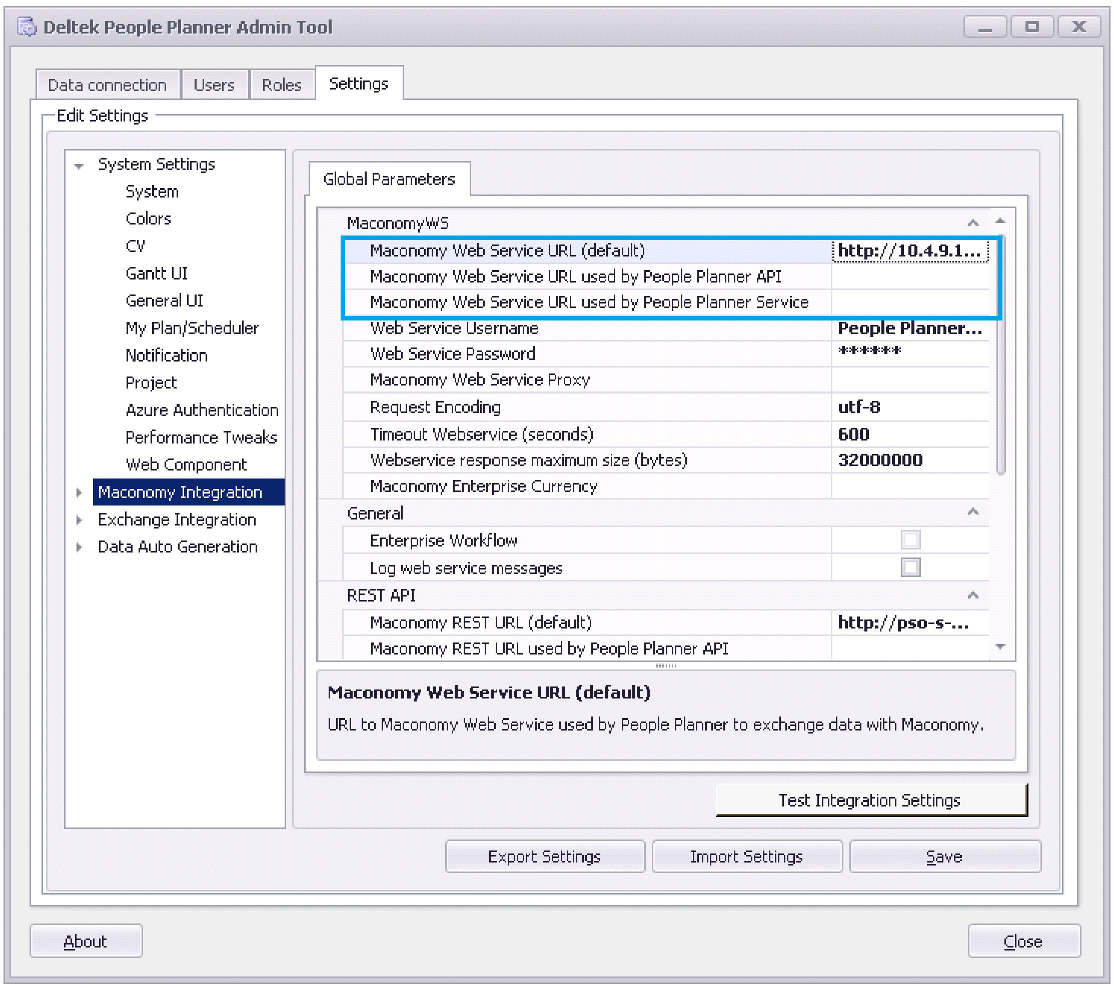
Alternative Maconomy Web Service URLs

The People Planner Service needs to know the URLs to call the MaconomyWS web service and optionally to call the Maconomy RESTful web service as well.

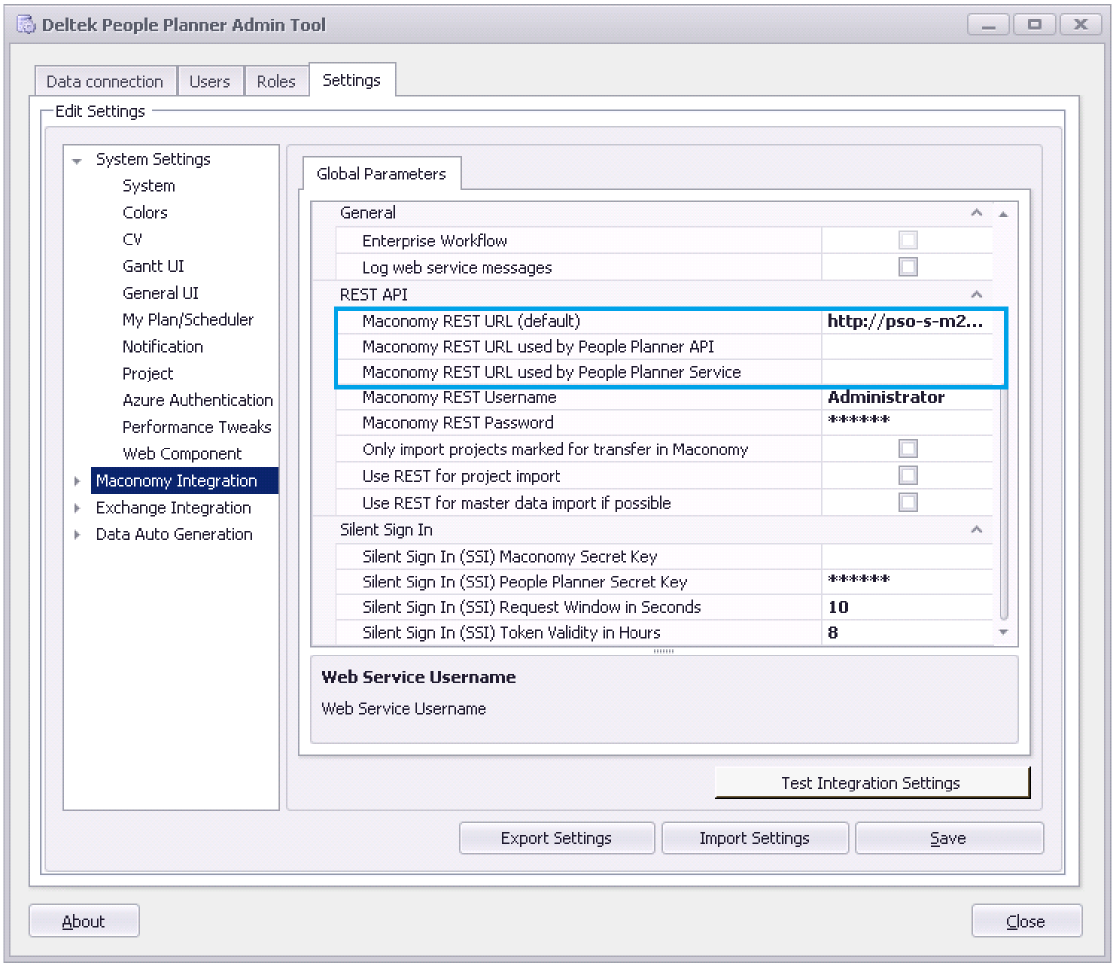
You can define a default URL to be used, or you can enter an alternative URL. This can be useful in situations where the People Planner Service has been installed in a different machine than the People Planner Windows Application and needs to call the MaconomyWS web service in a different way.

You do this setup from the People Planner Admin Tool, at System Settings » Maconomy Integration » Global Parameters. There are two subsections, one for MaconomyWS and one for REST API.

If you only entered a value for the default MaconomyWS URL, the People Planner Service uses this setting. However, if you entered a value for the **Maconomy Web Service URL used by People Planner Service** setting, the People Planner Service uses that value, instead.



Similarly, for the Maconomy RESTful web service:



If you only entered a value for the default **Maconomy REST URL**, the People Planner Service uses that. However, if you entered a value for the **Maconomy REST URL used by People Planner Service**, it uses that value, instead.

Installation and Basic Setup of the Maconomy Web Services

The integration between People Planner and a Maconomy system requires installations and configurations on both the Maconomy side and the People Planner side.

This section describes the setup on the Maconomy side. Install the Maconomy RESTful Web Service describes the setup on the People Planner side. Finally, Configuration in People Planner describes how to set up the People Planner Silent Sign-In functionality. These are parts A, B, and C of the checklists at the beginning of this guide.

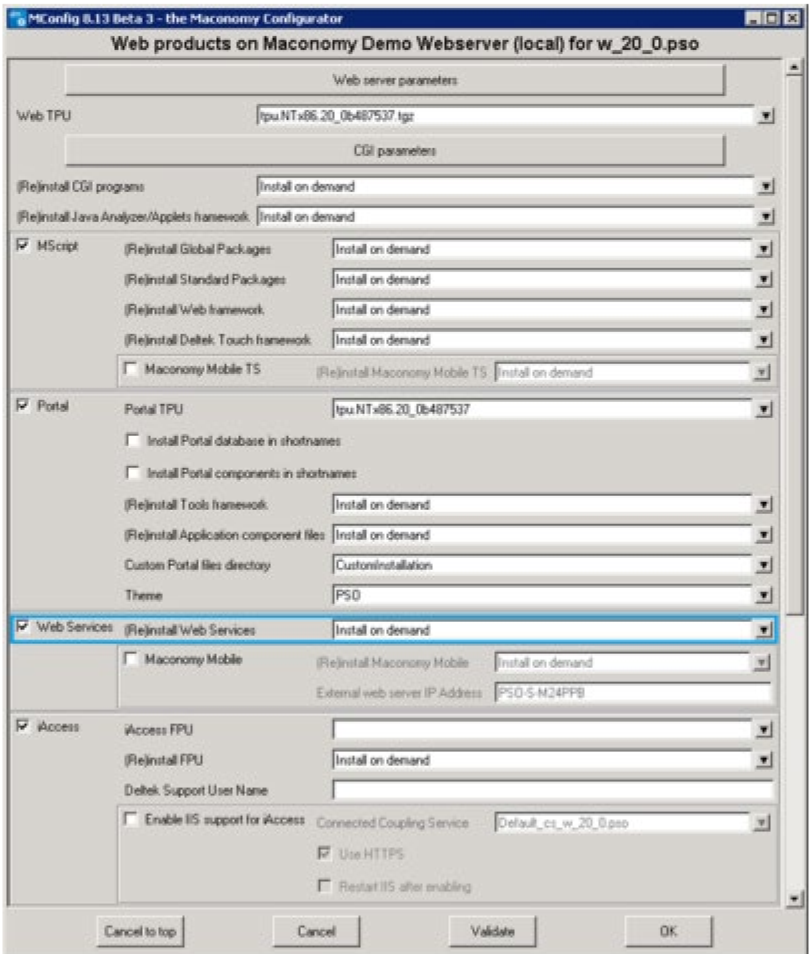
Install the MaconomyWS Web Service

Installing the MaconomyWS Web service is mandatory. In contrast, installing the Maconomy RESTful Web service is in principle optional, but since this means reduced functionality, it is not a very likely scenario.

To install the MaconomyWS Web service:

1. Run the Maconomy **MConfig** application.
2. Navigate to the **Web Products** page.
3. Select the **Web Services** check box.

4. Choose either **Install on Demand** or to **Install Unconditionally** for the **(Re)install Web Services** field.

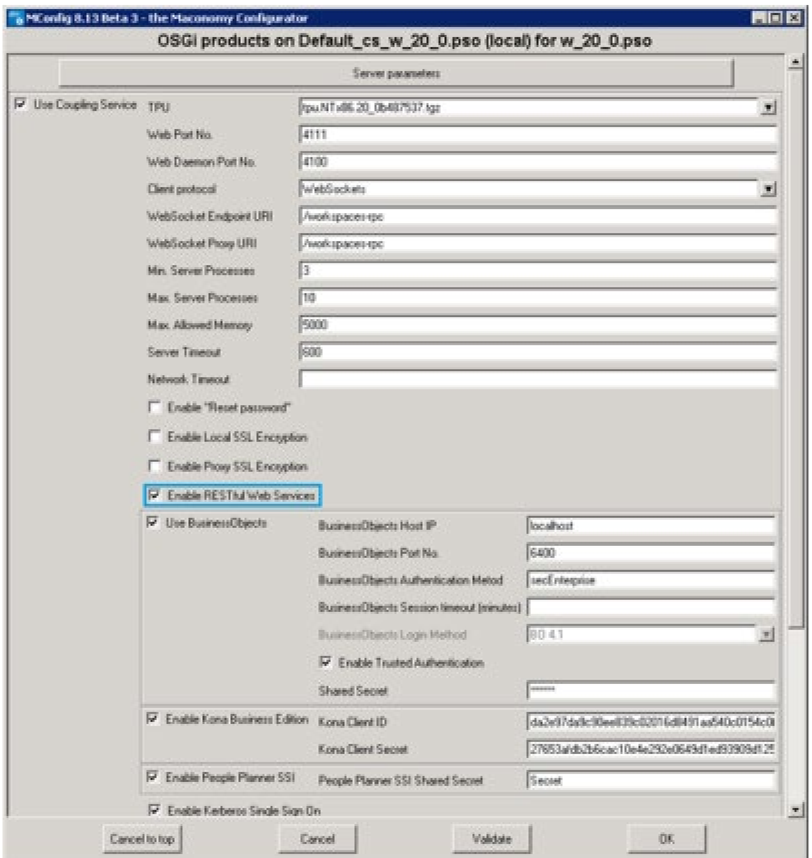


Install the Maconomy RESTful Web Service

Important: People Planner currently only supports v1 of the Maconomy RESTful Web Service.

To install the Maconomy RESTful Web service:

1. Navigate to the **OSGi Products** page.
2. Select the **Enable RESTful Web Services** check box.

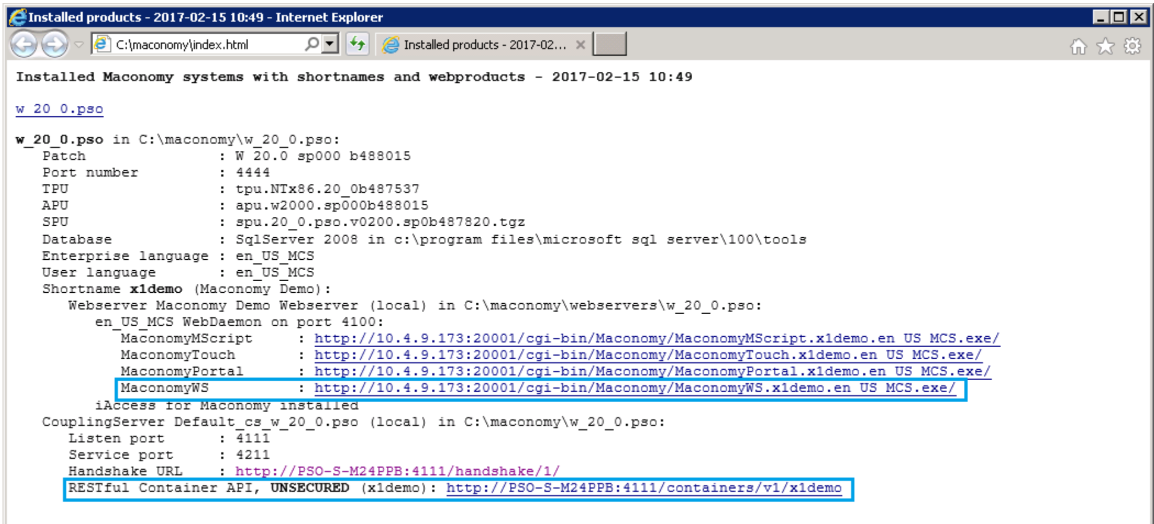


3. Click the **Finish** button to complete the installation.

Configuration in People Planner

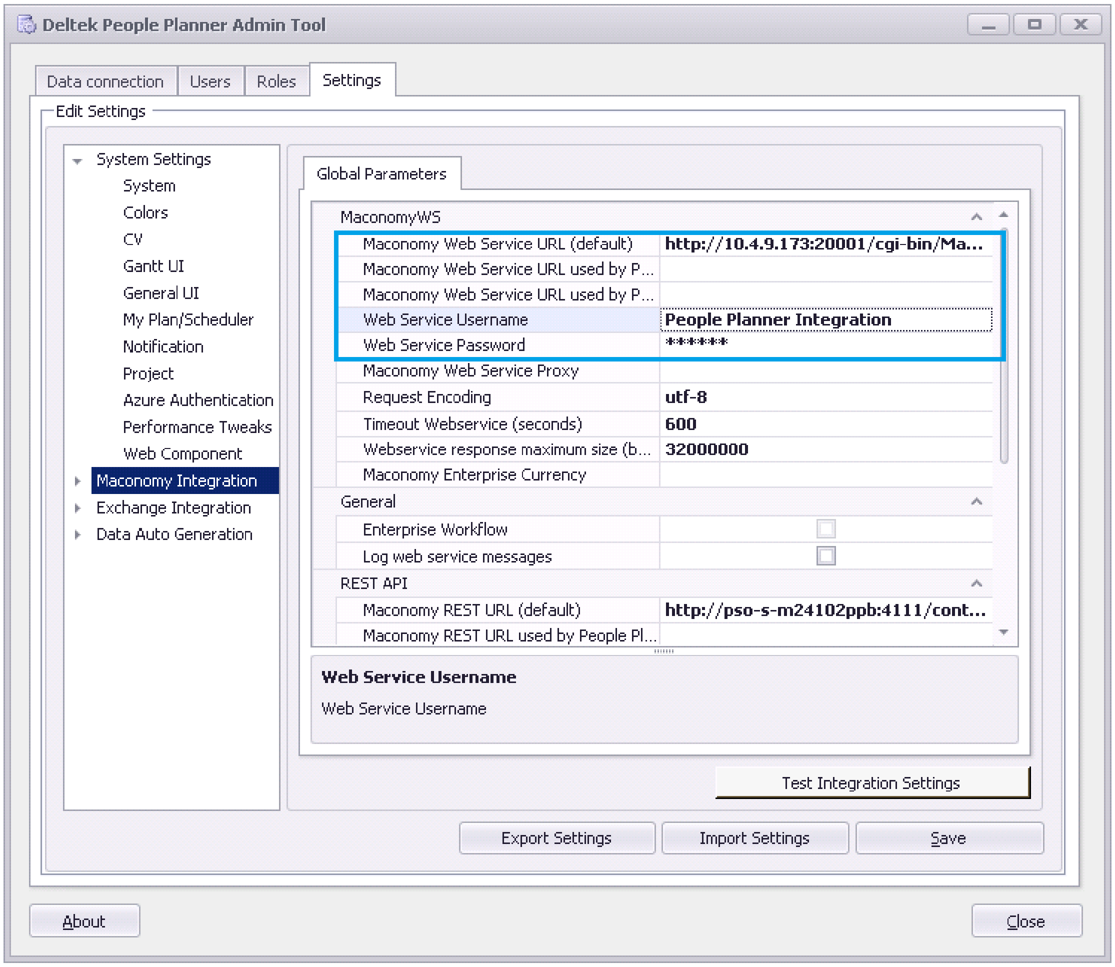
Next, you must configure People Planner with the URLs of the Maconomy Web services:

1. Open the **Maconomy index.html file**, for example, `C:\Maconomy\index.html`.



2. Run the **People Planner Admin Tool**.
3. Click the **Settings** tab.
4. Navigate to **Maconomy Integration » General**.

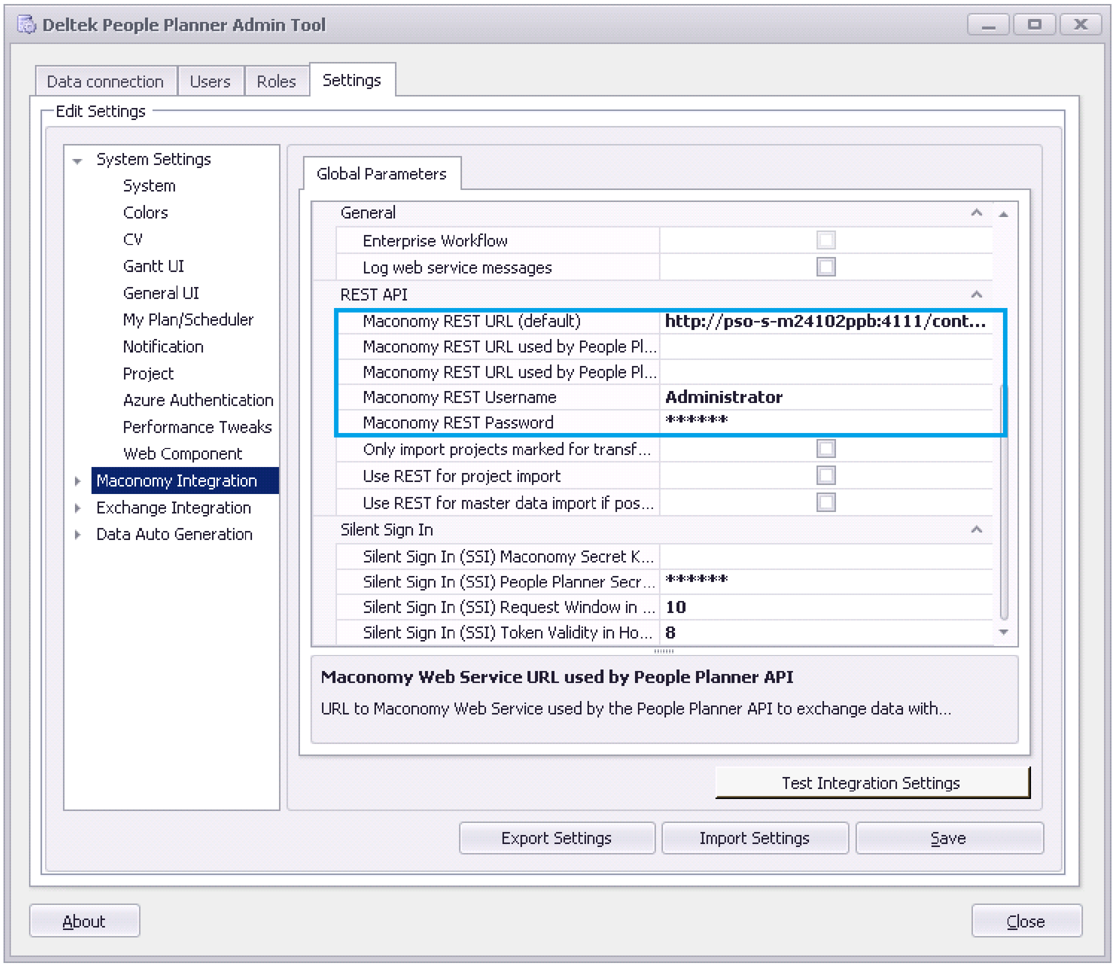
5. Copy the **MaconomyWS** URL from the Maconomy index file into the **Maconomy Web Service URL** field.



Note: You can supply alternative MaconomyWS URLs to be used by the People Planner API and the People Planner Service, respectively.

6. Enter the user credentials in the **Web Service Username** and the **Web Service Password** fields, respectively.

7. Copy the **RESTful Container API** URL from the Maconomy index file into the **Maconomy REST URL** field.

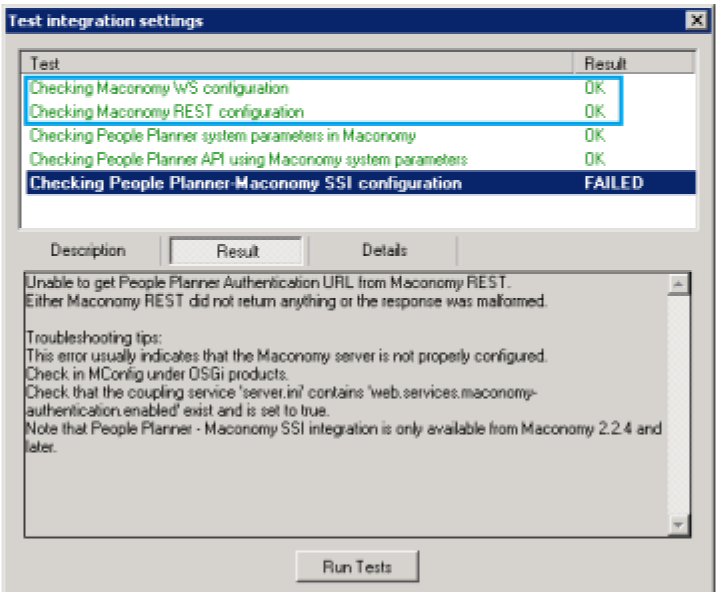


Note: You can supply alternative Maconomy RESTful URLs to be used by the People Planner API and the People Planner Service, respectively.

8. Enter the user credentials in the **Maconomy REST Username** and the **Maconomy REST Password** fields, respectively.
9. Click **Save** to save the changed settings to the People Planner database.

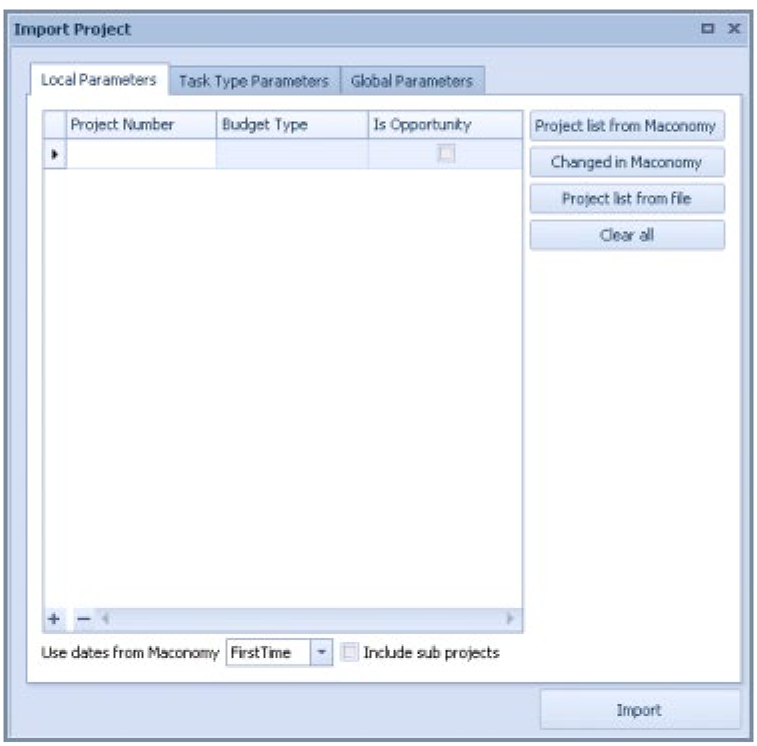
Verification

You can verify that People Planner can call the Maconomy Web services by clicking the **Test Integration Settings** button.

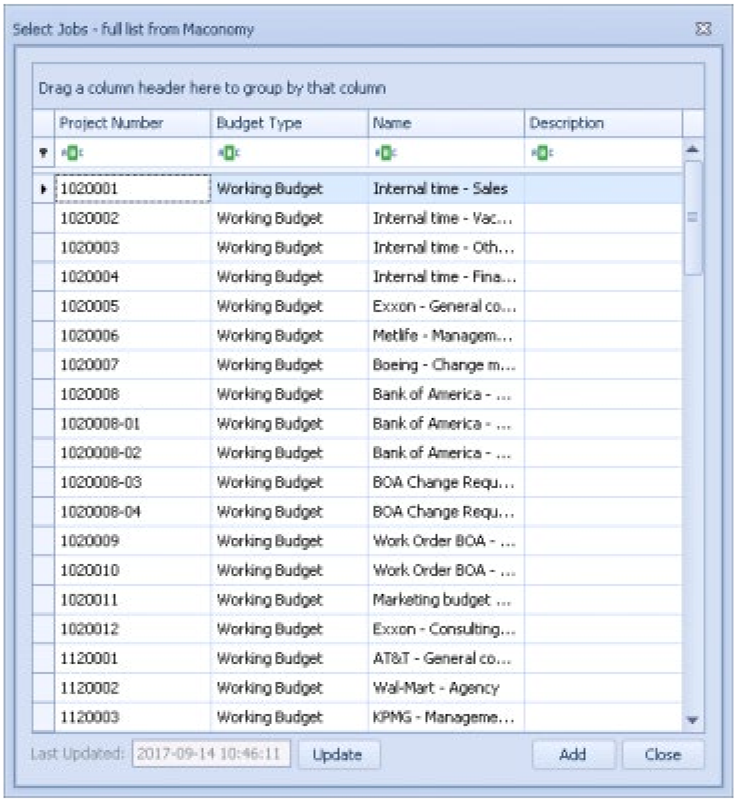


As an additional verification you can check that People Planner can retrieve the list of jobs from Maconomy:

1. Run the **People Planner Windows Application** as a People Planner **Admin user**.
2. Navigate to **Views » Tasks » Import Project**.



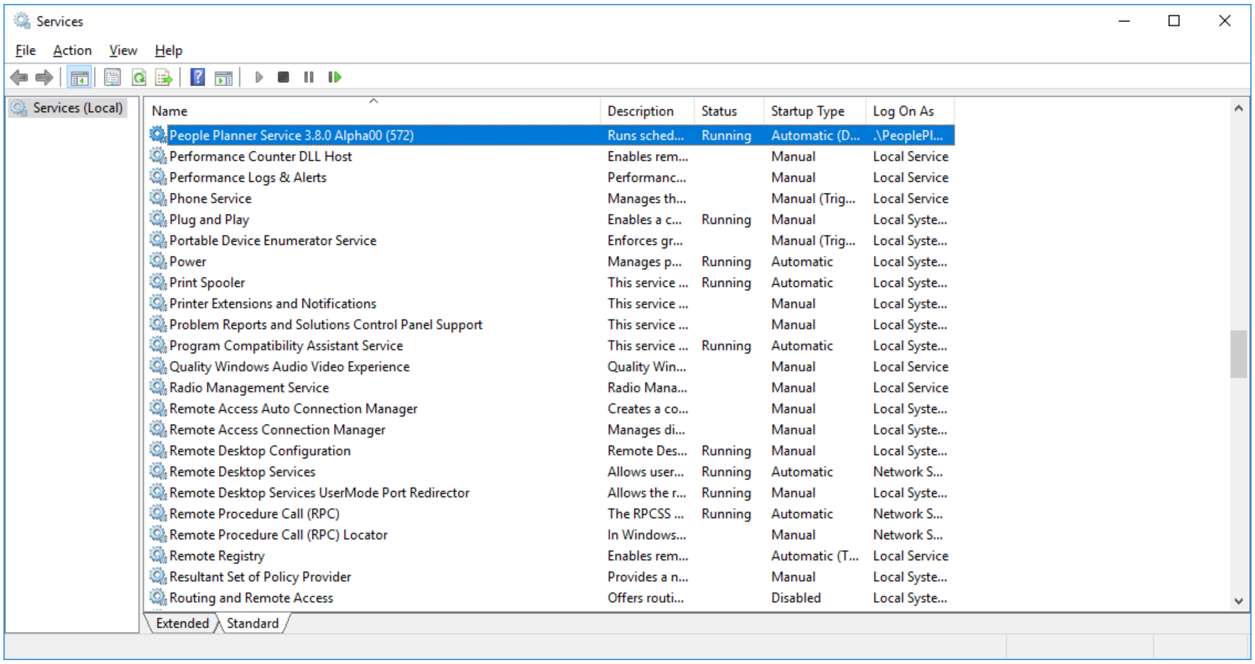
3. Click **Project list from Maconomy**.
4. Verify that you get a list of the current jobs in Maconomy.



5. Click **Close**.
6. Click the **x** button in the upper-right corner of the Import Project view to close it.

Start the People Planner Service

As the final step, open Windows Services and start the People Planner Service.

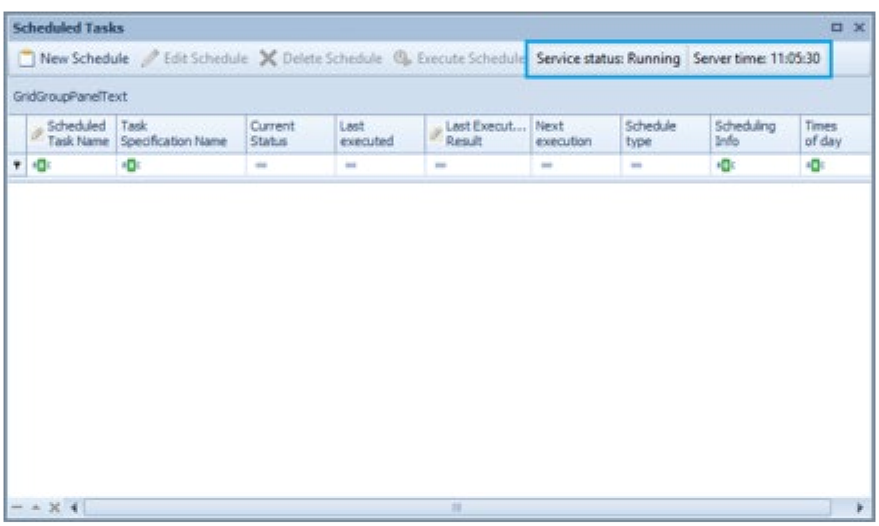


Verification

To verify that the People Planner Service is set up correctly:

1. Run the **People Planner Windows Application**.
2. Navigate to **Views » Tasks » Scheduled Tasks**.

The **Service status** should be **Running**, and the **Server time** should be continuously updated.



Setup of the People Planner Web Applications

The People Planner Web applications are:

- MyPlan Web page
- People Planner API Web Service
- People Planner RESTful Web Service (RestApi)
- People Planner Security Service
- People Planner Web Components

The installation and configuration of the People Planner Security Service is described in People Planner Security Service.

You can use these applications singly, for example:

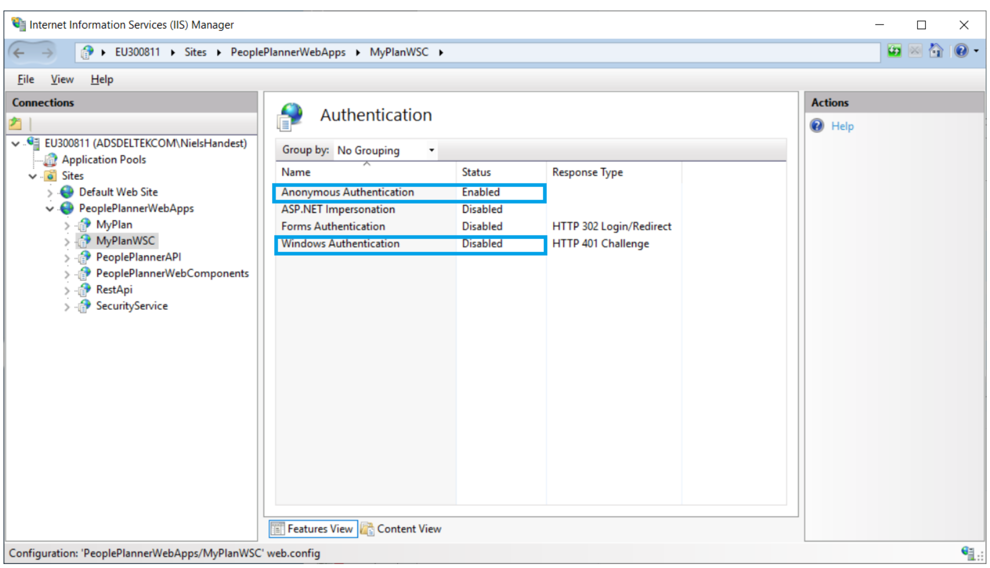
- Install MyPlan alone and use it directly from a browser.
- Install the People Planner API alone and use it from the Maconomy Workspace Client by clicking the Send Job to People Planner button.

However, this is not a very common setup, and this section therefore treats them as a packaged installation.

Before you continue, you must first make sure that you have installed the IIS Web server and configured it with the prerequisites.

Set Up Anonymous Authentication

Some of the People Planner Web applications require Windows Authentication, while most require Anonymous Authentication.



Which applications require which types of authentication is specified in the description of each Web application later in this section; however, the following table provides a summary.

People Planner Web Application	IIS Authentication Scheme
MyPlan	Windows Authentication
MyPlanWSC	Anonymous Authentication
People Planner API	Anonymous Authentication
People Planner Outlook Web Service	Windows Authentication
People Planner RestApi	Anonymous Authentication
People Planner Security Service	Anonymous- and Windows Authentication
People Planner Web Components	Anonymous Authentication

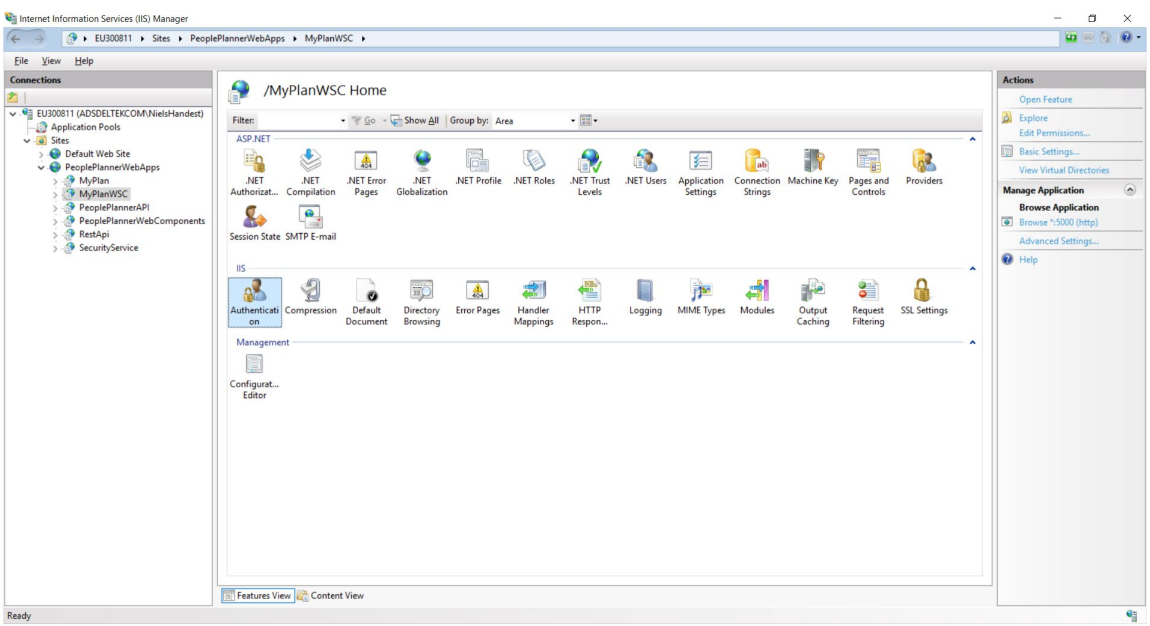
When you configure a Web application for Anonymous Authentication, the IIS requires that you specify a Windows account to use with the Web application. You can specify this, either directly on the People Planner Web site, or individually on each of the Web applications. The latter is useful if you want to configure the Web services to use different accounts.

The People Planner Web Applications installer, will setup the Web Applications to use the IUSR account with Anonymous Authentication. You can change this manually, if desired.

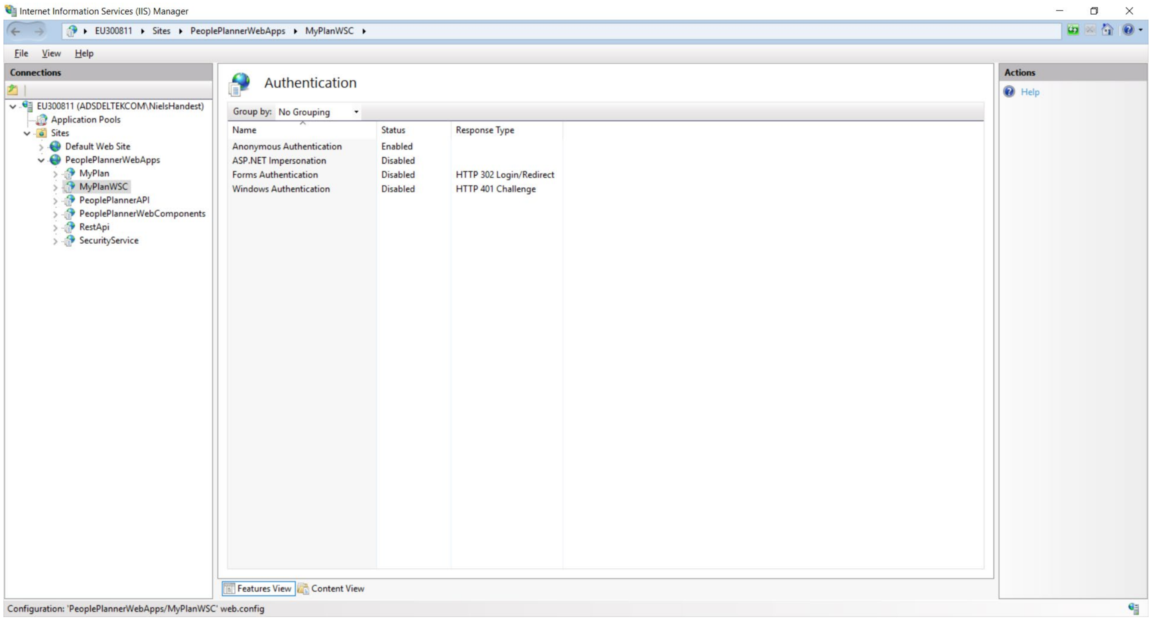
In this guide, it is assumed that you have created a **PeoplePlannerIIS** account, and that you have configured the password for this account to never expire. In addition, you should add that account to the lists of users in the People Planner database; instructions for doing that are provided in Add the Account as a People Planner User and Make the Account into a People Planner Admin User.

For example, to configure MyPlanWSC for Anonymous Authentication and to use the PeoplePlannerIIS account:

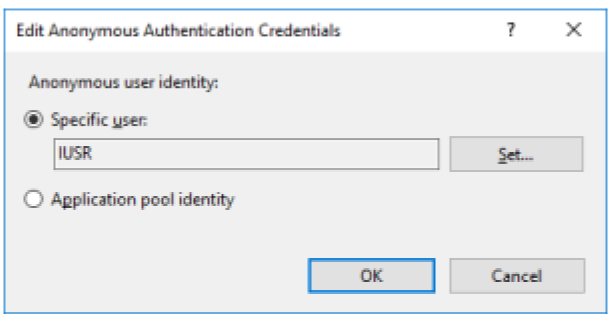
1. Run the Internet **Information Services (IIS) Manager**.
2. Navigate to the **MyPlanWSC** Web application.



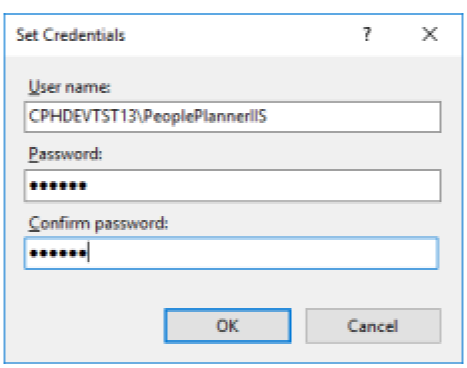
3. Click the **Authentication** icon.



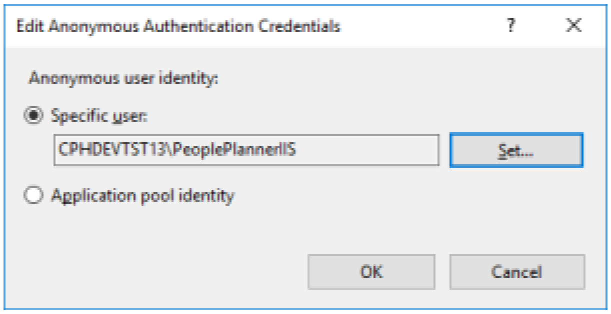
4. Right-click on **Anonymous Authentication** and click **Edit…**



5. Click **Set**.
6. Enter the credentials of the user you want to use:
   - It must be a valid Windows account.
   - It must be a People Planner Admin user.
   - For example, you can set the user to the user that you are using for installation of the People Planner software, such as <domain/machine-name>\PeoplePlannerIIS.



7. Click **OK**.



8. Click **OK**.

MyPlan Web Application

People Planner MyPlan either can run directly from a browser or embedded in the Maconomy Workspace client.

> **Note:** From People Planner 4.0, a version of MyPlan is also implemented in the Maocnomy web client, but this is not covered here. Please see under People Planner RESTful Web Service (RestApi).

Configure MyPlanWSC for Anonymous Authentication

One reason for the two MyPlan-installations—MyPlan and MyPlanWSC—is to be able to apply different themes to MyPlan, depending on the context in which it is used.

Another reason is that you can set each one up for a different authentication scheme in the IIS.

- MyPlan requires Windows Authentication.
- MyPlanWSC requires Anonymous Authentication. The authentication is then handled by the People Planner Silent Sign-In functionality.

During the installation, you set each of them up for the correct type of authentication. However, MyPlanWSC requires that you choose an account as described in Setup for Anonymous Authentication.

Configure MyPlan for Alternative Types of Authentication

People Planner MyPlan is typically set up for using Windows Authentication. This works provided the users are on the same domain as the web server where MyPlan is installed.

However, if the users are on a different domain, it is possible to configure MyPlan for alternative types of authentication, including:

- Azure Authentication
- OAuth 2 and OpenId Connect (OIDC)

Attention: Azure Authentication is deprecated in People Planner 4.3. This will be removed altogether in People Planner 4.4.

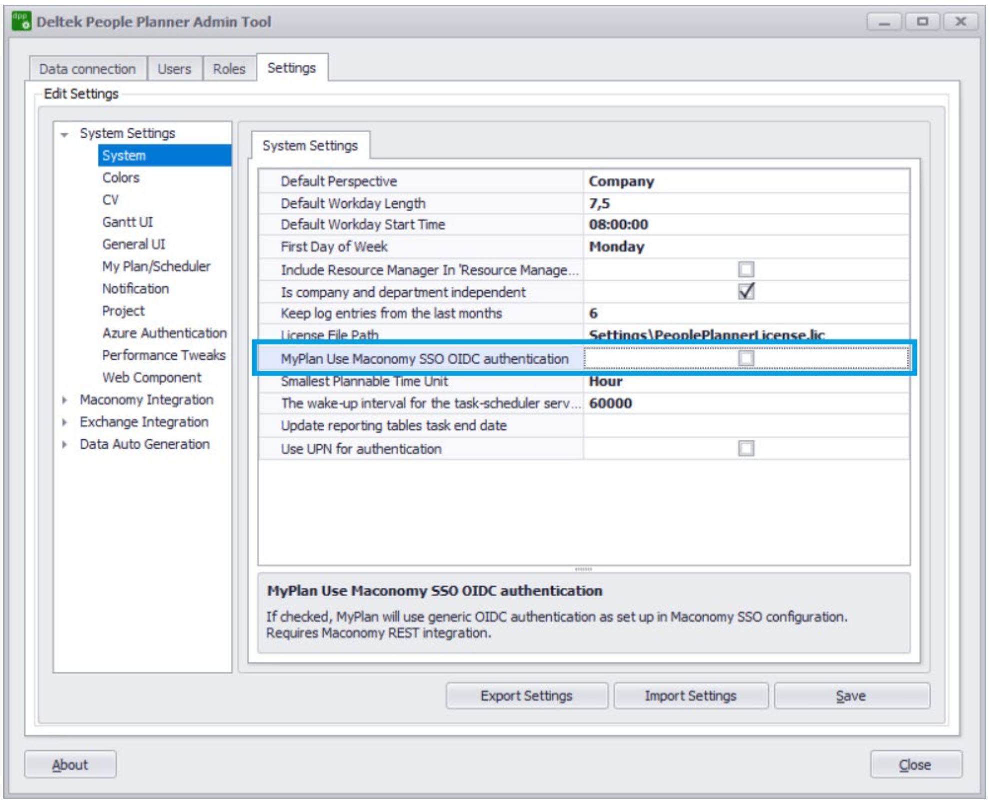
Azure Setup

Set up of Azure Authentication is described in details in the *Deltek People Planner Admin Guide*.

OIDC Setup

People Planner is built on top of the OIDC setup in Maconomy. For it to work, you need to do two steps in People Planner, using the People Planer Admin Tool:

1. In the People Planner Admin Tool, configure People Planner to use the Maconomy RESTful web service.
2. Also in the Admin Tool, select the **MyPlan Use Maconomy SSO OIDC authentication** check box.



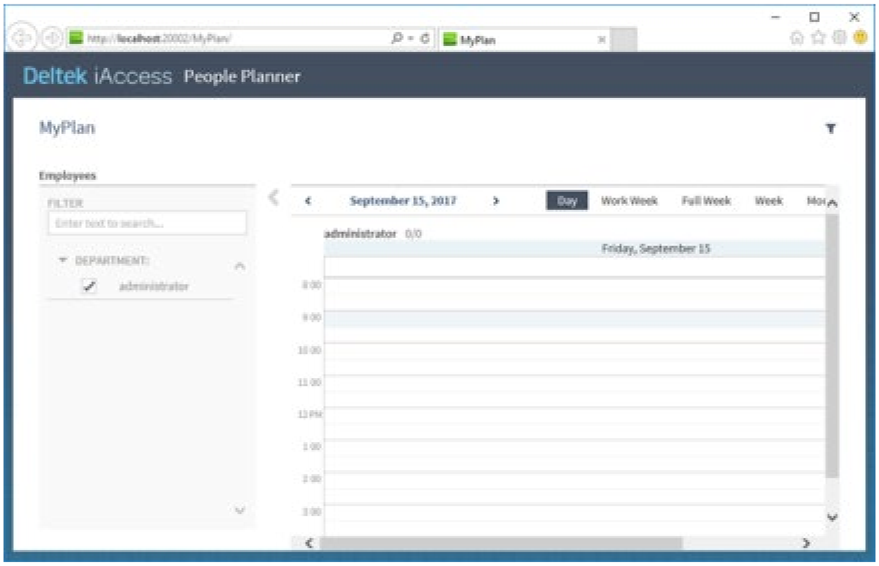
3. With the OIDC provider, configure the MyPlan URL as a valid callback URL.

For further information about how to setup OIDC in Maconomy, see the *Deltek Maconomy System Admin Guide*, under setup of Single Sign-On.

Note: OIDC is supported from People Planner 3.9.2 CU2.

Verification

You can check that MyPlan has been installed and configured correctly by opening a Web browser and navigating to `http://localhost:<port>/MyPlan`.



> **Note:** When you added yourself as a People Planner Admin user in the People Planner database, you had the option to create yourself as a resource, as well. If you declined to do that, MyPlan shows the following message, instead:
>
> `The current user is not associated with a Resource in People Planner. Please assign a resource to Administrator.`
>
> For strictly verification purposes, this is fine, because it, too, confirms that MyPlan is working.

People Planner API Web Service

The People Planner API Web Service is used when Maconomy needs to call People Planner, for example, because a user clicked the Send Job to People Planner button in the Maconomy Workspace Client.

Configure for Anonymous Authentication

The People Planner API must be set up for Anonymous Authentication. The steps for doing this are provided in Setup for Anonymous Authentication.

Later, you must configure the selected account on the Maconomy side as well. See Settings for the People Planner API Web Service.

> **Note:** The selected user must be a valid Windows account. Before Release 3.8, People Planner required that the account also be a People Planner Admin user. However, this requirement is relaxed as of Release 3.8. If you have not added the user to the People Planner database, it is automatically created the first time that the People Planner API Web Service is called. The user is not a People Planner Admin user in this case.

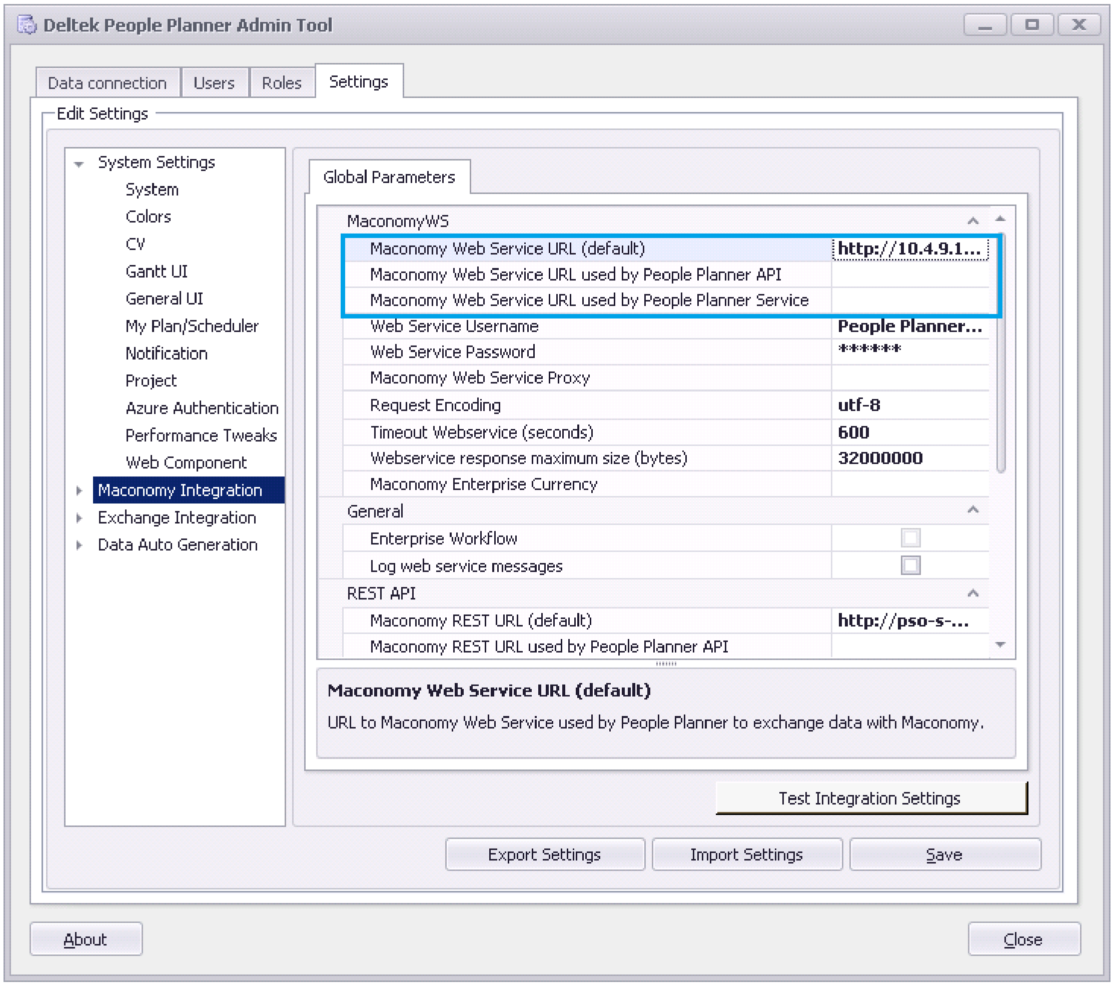
Alternative Maconomy Web Service URLs

The People Planner API need to know the URLs to call the MaconomyWS web service and optionally to call the Maconomy RESTful web service as well.

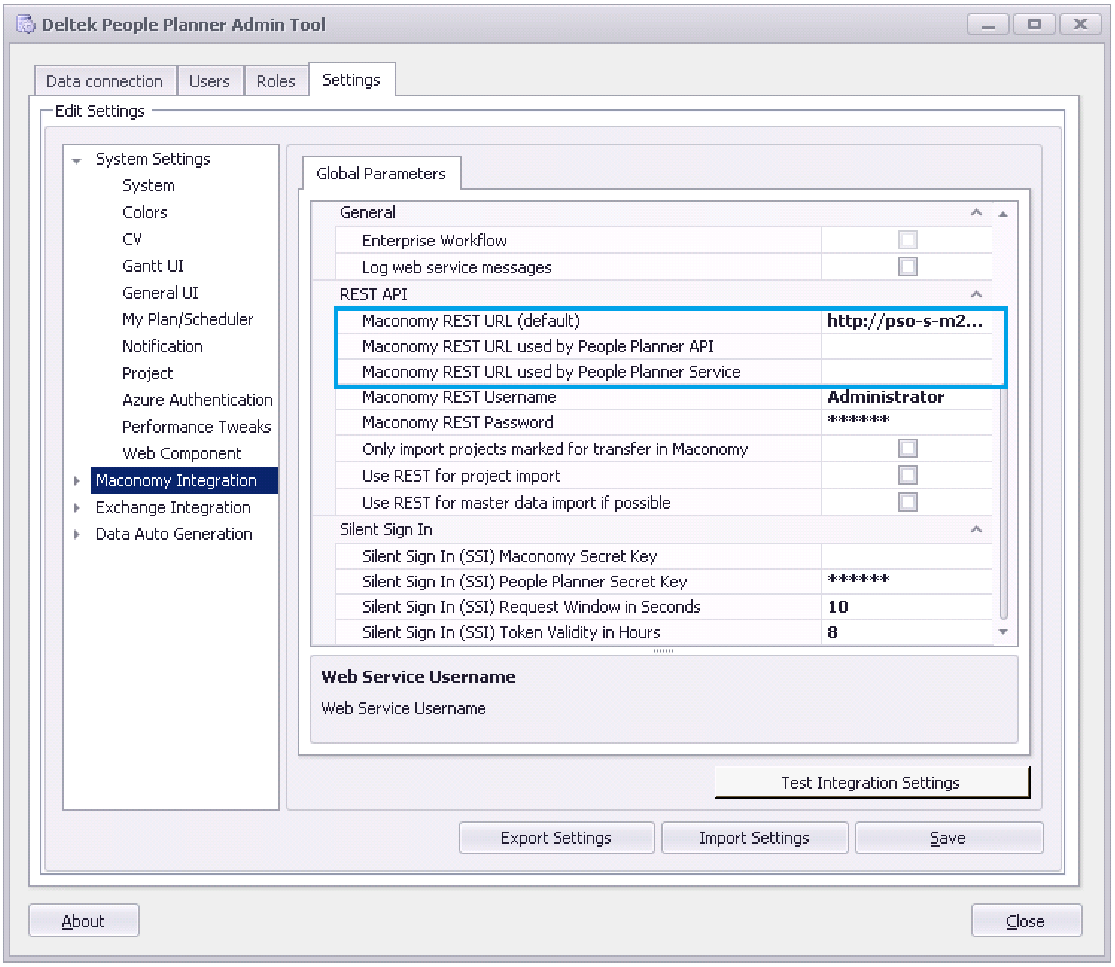
You can define a default URL to be used, or you can fill in an alternative URL. This can be useful in situations where the People Planner API has been installed in a different machine than the People Planner Windows Application and need to call the MaconomyWS web service in a different way.

The setup is done from the People Planner Admin Tool, in the section: System Settings > Maconomy Integration > Global Parameters. It has two subsections, one for MaconomyWS and one for REST API.

If only the default MaconomyWS URL has been filled in, the People Planner API will use this setting. However, if the **Maconomy Web Service URL used by People Planner API** setting has also been filled in, the People Planner API will instead use this.



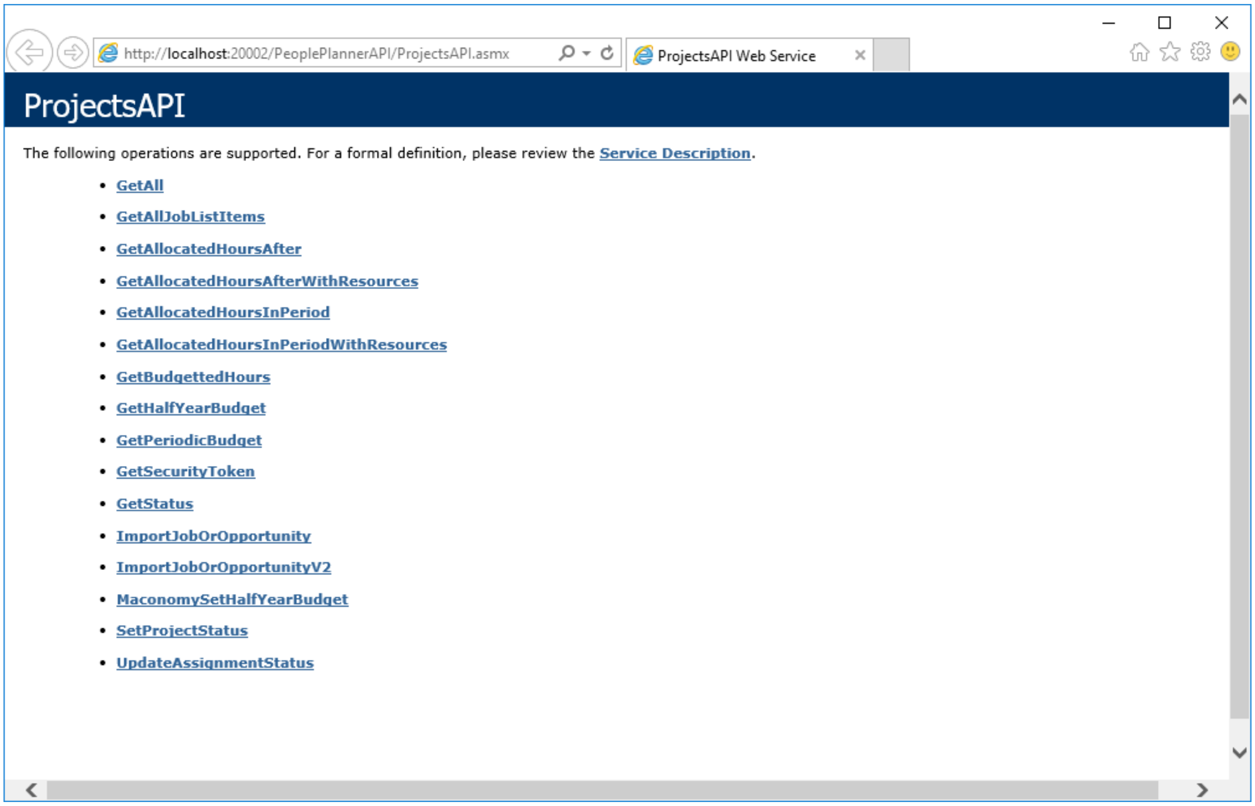
Similarly, for the Maconomy RESTful web service:



If only the default **Maconomy REST URL** has been filled in, the People Planner API will use that. However, if the **Maconomy REST URL used by People Planner API** has been filled in, it will use this instead.

Verification

You can check that the People Planner API has been installed and configured correctly by opening a Web browser and navigating to `http://localhost:<port>/PeoplePlannerAPI/ProjectsAPI.asmx`



Advanced Verification

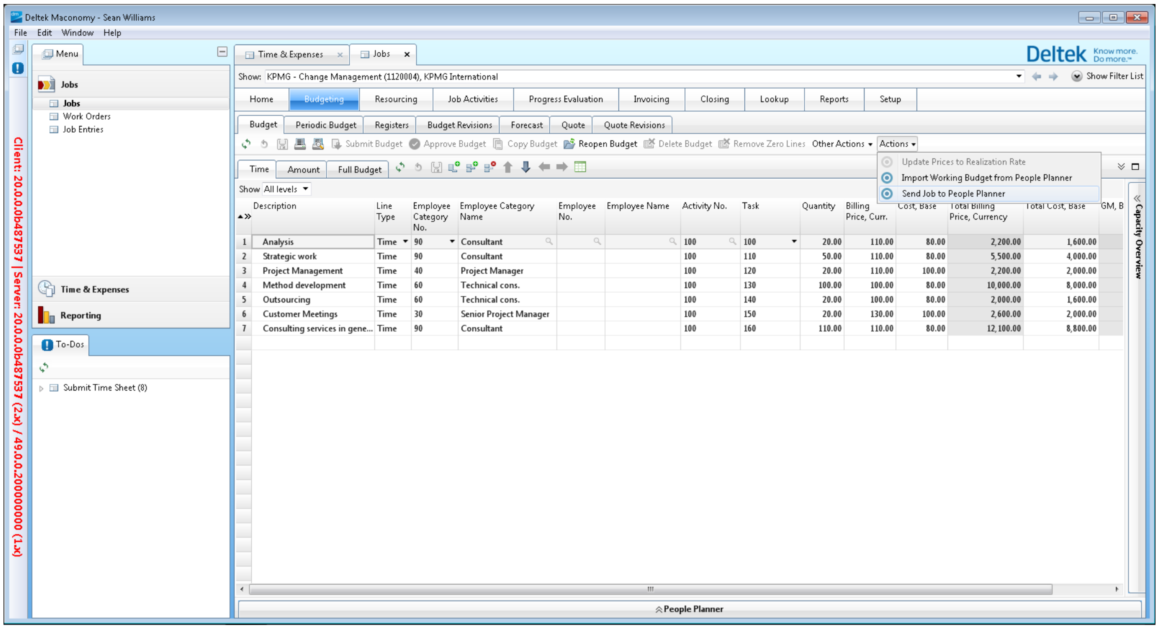
The previous verification does not actually call the People Planner API. It is, therefore, not an absolute guarantee that there are no errors.

Note: The following verification process requires that you have already installed and configured the Maconomy Web services.

To verify that it is possible to call the People Planner API Web service:

1. Run the **Maconomy Workspace Client** as a normal user.

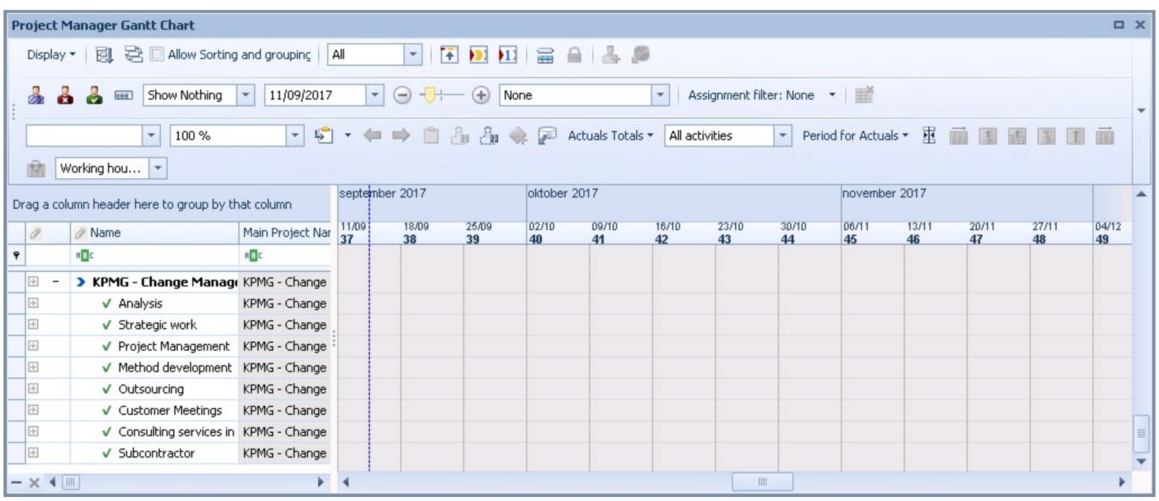
2. Navigate to the **Jobs » Jobs** workspace.



3. Click **Send Job to People Planner**.

   If this does not result in an error, the export was successful. You can, however, also verify this by finding the project in People Planner, as follows.

4. Run the **People Planner Windows Application** as a People Planner Admin user.
5. Navigate to **Views » Projects » Project Manager Gantt Chart**.



Note: You can select the project and press the Delete key to delete the project from People Planner.

People Planner RESTful Web Service (RestApi)

The People Planner RESTful Web Service is new with People Planner 4.0. It is required for use of the People Planner integration in the Maconomy web client.

This document does not describe how to configure the People Planner integration in the Maconomy web client. For this, please refer to the *Deltek Maconomy System Admin Guide*.

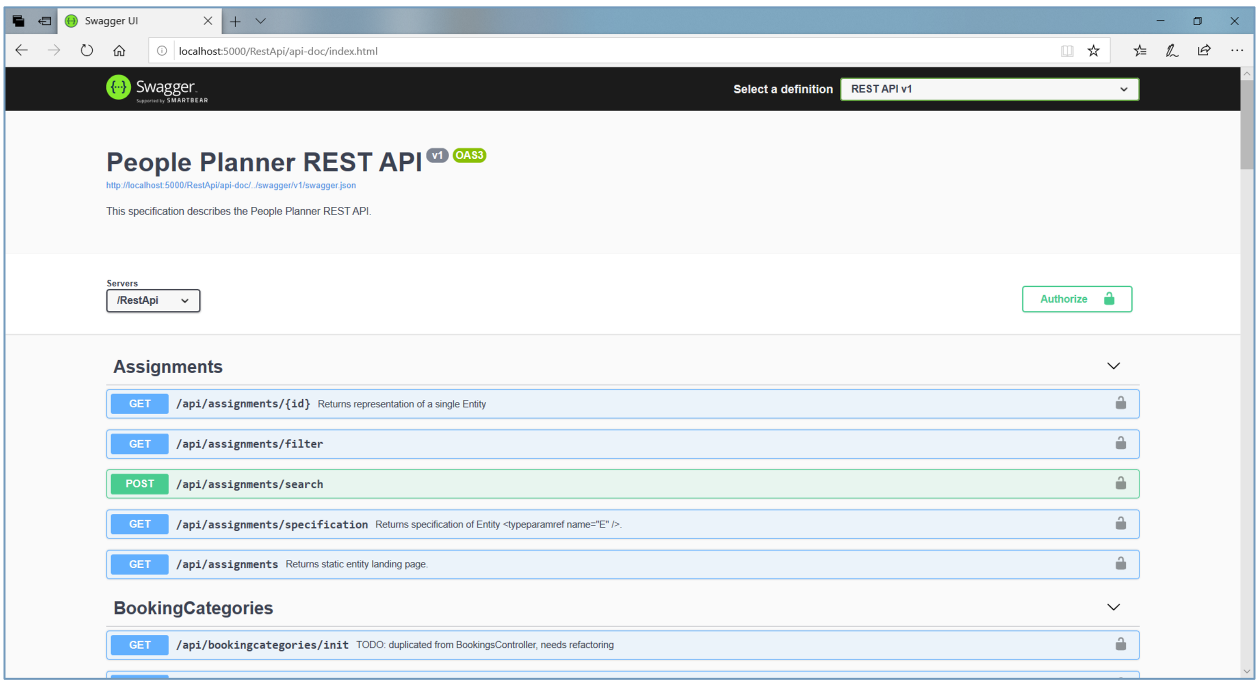
> **Note:** The RestApi is not released as a general purpose API for People Planner. In People Planner 4.0, it only supports the integration to the Maconomy web client.

Configure for Anonymous Authentication

The RestApi must be set up for Anonymous Authentication. The steps for doing this are provided in Setup for Anonymous Authentication.

Verification

Verify the installation of the People Planner RESTful Web Service (RestApi) by opening its Swagger-documentation in a browser on the server.



The URL for the Swagger documentation is in the following format:

http://<host>:<port>/RestApi/api-doc/index.html

where

port is the port in which you installed the RestApi.

> **Note:** If you have not yet configured for SSL, the scheme is http, not https.

If the Swagger documentation displays successfully, you can assume that the RestApi is correctly installed.

People Planner Security Service

Before you can run the People Planner Windows Application and use it for initial imports from the Maconomy system, you must verify that the People Planner Security Web Service works correctly.

If the Security Service is running, it is very likely that the rest of the People Planner Web Applications are also running.

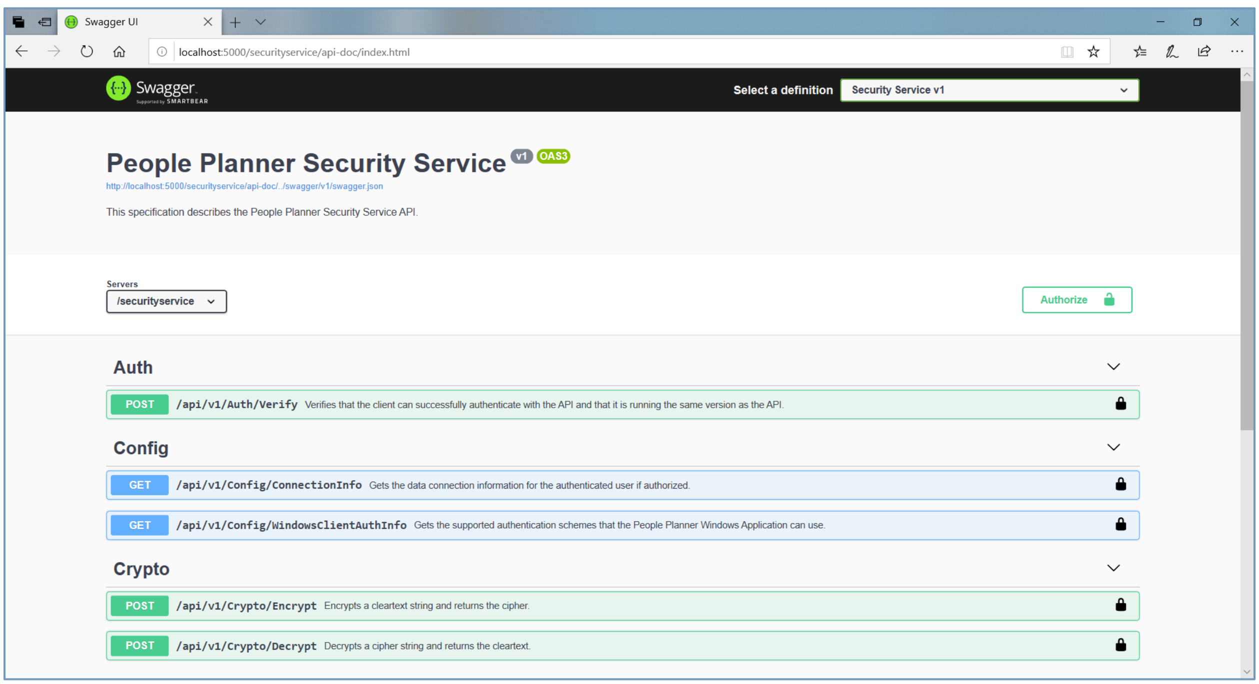
For details of setup and troubleshooting with the People Planner Security Service, see Appendix C: Securing the People Planner Security Service.

Configure for Anonymous and Windows Authentication

The People Planner Security Service must be set up for both Anonymous Authentication and for Windows Authentication. The steps for setting up the Anonymous Authentication this are provided in Setup for Anonymous Authentication.

Verification

Verify the installation of the People Planner RESTful Web Service (RestApi) by opening its Swagger-documentation in a browser on the server.



The URL for the Swagger documentation is in the following format:

http://<host>:<port>/RestApi/api-doc/index.html

where

port is the port in which you installed the RestApi

Note: If you have not yet configured for SSL, the scheme is http, not https.

If the Swagger documentation displays successfully, you can assume that the RestApi is correctly installed

People Planner Web Components

The People Planner Web Components is a Web page that is designed specifically to be embedded in the Maconomy Workspace Client (WSC).

> **Note:** The Web Components use cookies; this requires that your browser allows cookies. If the browser does not allow cookies, the Web Components will fail.

Configure for Anonymous Authentication

The People Planner Web Components must be set up for Anonymous Authentication. The steps for doing this are described in Setup for Anonymous Authentication.

Although you could use a different account for each, it is recommended that you use the same account for MyPlan and the People Planner Web Components.

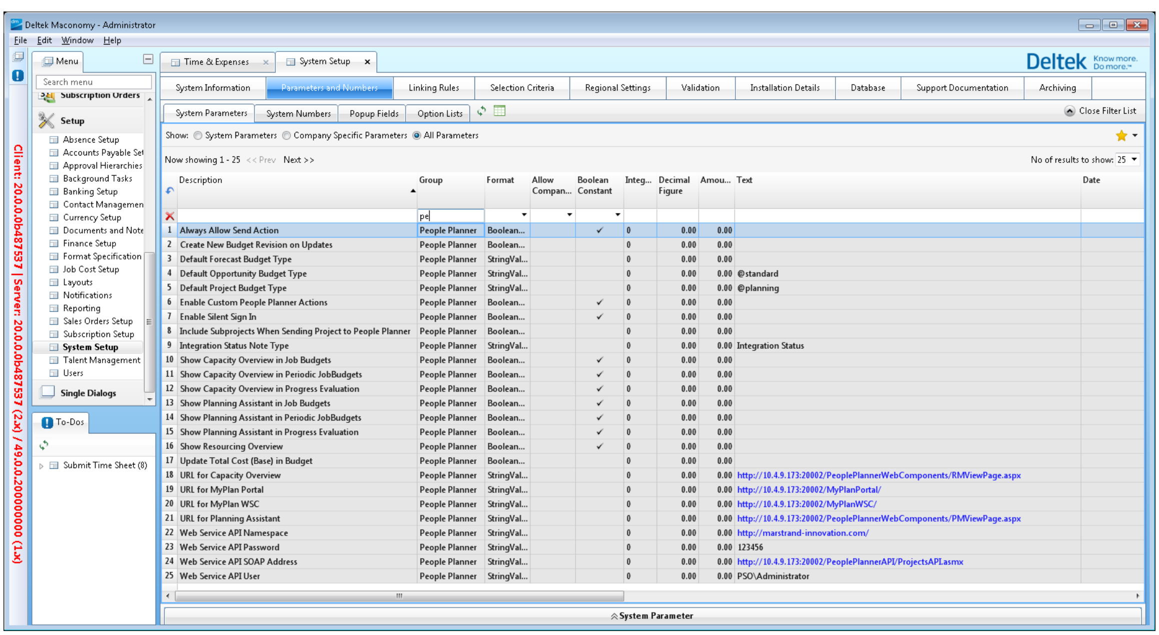
Verification

At this point in the installation, you cannot easily verify that the People Planner Web Components have been installed and configured correctly. This requires that you have also set up the People Planner Silent Sign-In functionality and imported the users from Maconomy.

Configuration in Maconomy

Before Maconomy can use the People Planner Web Components, it must be configured:

1. Run the **Maconomy Workspace Client** as a Maconomy Admin user.
2. Navigate to **Setup » System Setup » Parameters and Numbers » System Parameters**.
3. Filter on the **Groups** columns to see only the system parameters that relate to People Planner.



Settings for the People Planner API Web Service

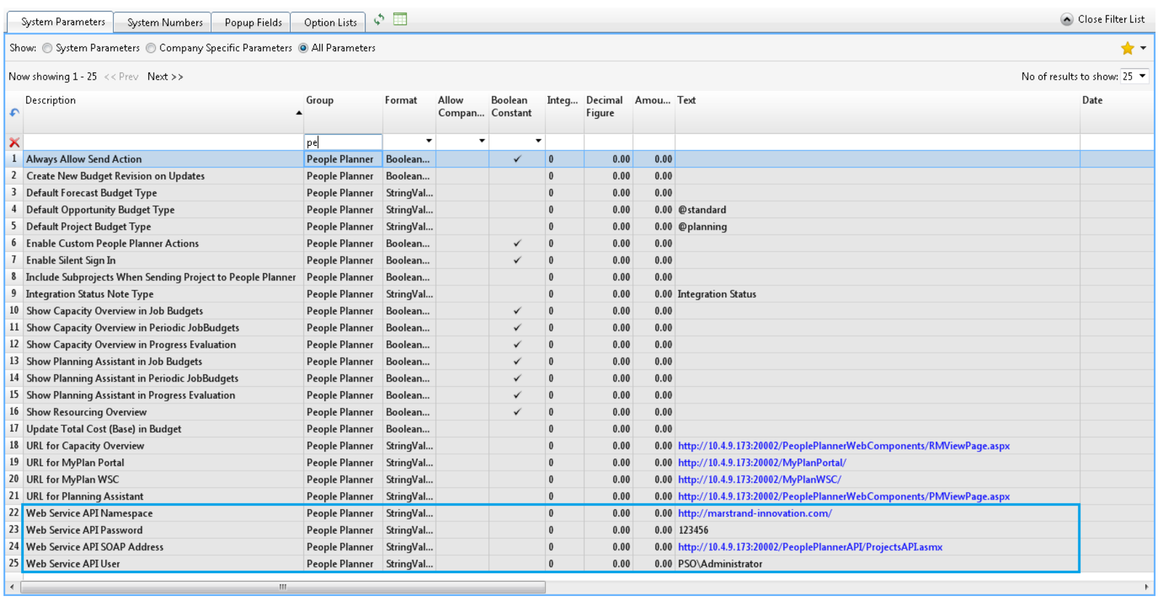
Maconomy uses the People Planner API Web Service when a user clicks one of the People Planner buttons in the clients—for example, if a user clicks the **Send Job to People Planner** button. The Web Service is also used as a central component in the People Planner Silent Sign-In functionality.

> **Warning:** Beginning with People Planner 3.9 the API Web Service Namespace was changed. You must **set this value in Maconomy to**:
>
> http://peopleplanner.deltek.com/api/
>
> If you do not make this change in Maconomy, the People Planner / Maconomy integration will not work.
>
> This is also the default for Maconomy 2.5 and newer.

To set the values for the People Planner API Web Service settings:

1. Set the **Web Service API SOAP Address** to the URL of the People Planner API Web Service: `http://<host>:<port>/PeoplePlannerAPI/ProjectsAPI.asmx`
2. Set the **Web Service API User** and **Web Service API Password** to the credentials for the People Planner API Web service.

> **Note:** The User and the Password must be those of the account that you used when configuring Anonymous Authentication for the People Planner API. See Configure for Anonymous Authentication.



	Description	Group	Format	Allow Compan...	Boolean Constant	Integ...	Decimal Figure	Amou...	Text	Date
		pe								
1	Always Allow Send Action	People Planner	Boolean...		✓	0	0.00	0.00		
2	Create New Budget Revision on Updates	People Planner	Boolean...			0	0.00	0.00		
3	Default Forecast Budget Type	People Planner	StringVal...			0	0.00	0.00		
4	Default Opportunity Budget Type	People Planner	StringVal...			0	0.00	0.00	@standard	
5	Default Project Budget Type	People Planner	StringVal...			0	0.00	0.00	@planning	
6	Enable Custom People Planner Actions	People Planner	Boolean...		✓	0	0.00	0.00		
7	Enable Silent Sign In	People Planner	Boolean...		✓	0	0.00	0.00		
8	Include Subprojects When Sending Project to People Planner	People Planner	Boolean...			0	0.00	0.00		
9	Integration Status Note Type	People Planner	StringVal...			0	0.00	0.00	Integration Status	
10	Show Capacity Overview in Job Budgets	People Planner	Boolean...		✓	0	0.00	0.00		
11	Show Capacity Overview in Periodic JobBudgets	People Planner	Boolean...		✓	0	0.00	0.00		
12	Show Capacity Overview in Progress Evaluation	People Planner	Boolean...		✓	0	0.00	0.00		
13	Show Planning Assistant in Job Budgets	People Planner	Boolean...		✓	0	0.00	0.00		
14	Show Planning Assistant in Periodic JobBudgets	People Planner	Boolean...		✓	0	0.00	0.00		
15	Show Planning Assistant in Progress Evaluation	People Planner	Boolean...		✓	0	0.00	0.00		
16	Show Resourcing Overview	People Planner	Boolean...		✓	0	0.00	0.00		
17	Update Total Cost (Base) in Budget	People Planner	Boolean...			0	0.00	0.00		
18	URL for Capacity Overview	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerWebComponents/RMViewPage.aspx	
19	URL for MyPlan Portal	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/MyPlanPortal/	
20	URL for MyPlan WSC	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/MyPlanWSC/	
21	URL for Planning Assistant	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerWebComponents/PMViewPage.aspx	
22	Web Service API Namespace	People Planner	StringVal...			0	0.00	0.00	http://marstrand-innovation.com/	
23	Web Service API Password	People Planner	StringVal...			0	0.00	0.00	123456	
24	Web Service API SOAP Address	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerAPI/ProjectsAPI.asmx	
25	Web Service API User	People Planner	StringVal...			0	0.00	0.00	PSO\Administrator	

Settings for the MyPlan Web Application

The MyPlan Web page can be embedded in the Maconomy Workspace Client (WSC), Maconomy web client, and in the Maconomy Portal.

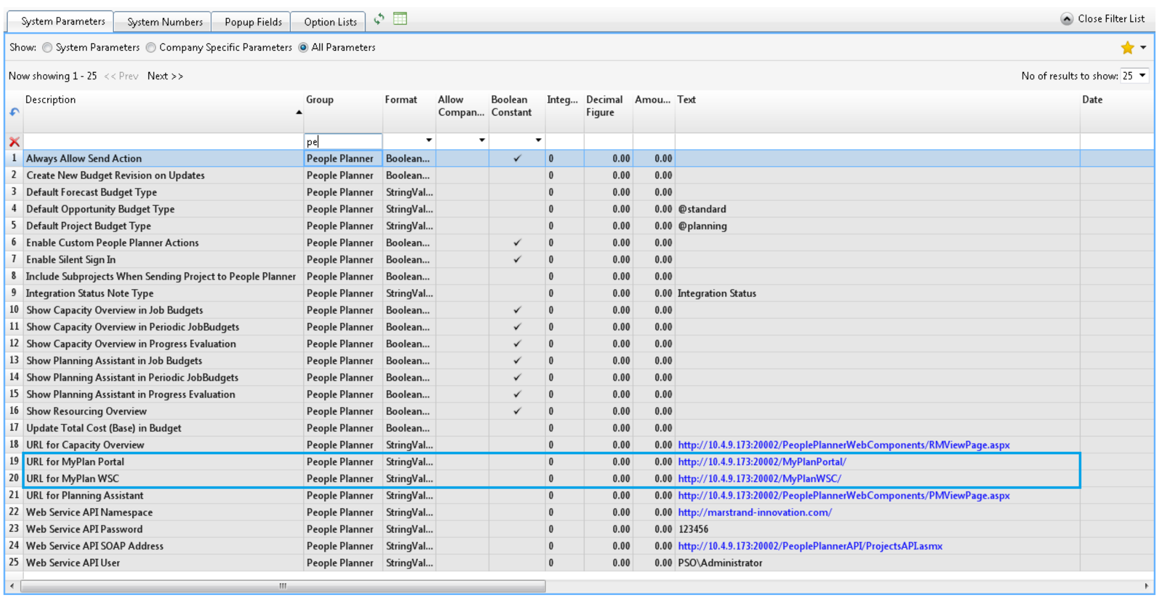
> **Attention:** MyPlan in the Maconomy Portal is deprecated in People Planner 4.3. This will be removed altogether in People Planner 4.4.
>
> Currently, the Maconomy Portal is available only when using Maconomy 2.5.x and older versions.

To embed the MyPlan Web application in the WSC:

- Set the **URL for MyPlan WSC** to the URL of the MyPlanWSC Web page:
  `http://<host>:<port>/MyPlanWSC`

To embed the MyPlan Web application in the Maconomy Portal:

- Set the **URL for MyPlan Portal** to the URL of the MyPlan Web page:
  `http://<host>:<port>/MyPlan`



System Parameters | System Numbers | Popup Fields | Option Lists | Close Filter List

Show: System Parameters | Company Specific Parameters | All Parameters

Now showing 1 - 25 << Prev Next >> | No of results to show: 25

	Description	Group	Format	Allow Compan...	Boolean Constant	Integ...	Decimal Figure	Amou...	Text	Date
		pe								
1	Always Allow Send Action	People Planner	Boolean...		✓	0	0.00	0.00		
2	Create New Budget Revision on Updates	People Planner	Boolean...			0	0.00	0.00		
3	Default Forecast Budget Type	People Planner	StringVal...			0	0.00	0.00		
4	Default Opportunity Budget Type	People Planner	StringVal...			0	0.00	0.00	@standard	
5	Default Project Budget Type	People Planner	StringVal...			0	0.00	0.00	@planning	
6	Enable Custom People Planner Actions	People Planner	Boolean...		✓	0	0.00	0.00		
7	Enable Silent Sign In	People Planner	Boolean...		✓	0	0.00	0.00		
8	Include Subprojects When Sending Project to People Planner	People Planner	Boolean...			0	0.00	0.00		
9	Integration Status Note Type	People Planner	StringVal...			0	0.00	0.00	Integration Status	
10	Show Capacity Overview in Job Budgets	People Planner	Boolean...		✓	0	0.00	0.00		
11	Show Capacity Overview in Periodic JobBudgets	People Planner	Boolean...		✓	0	0.00	0.00		
12	Show Capacity Overview in Progress Evaluation	People Planner	Boolean...		✓	0	0.00	0.00		
13	Show Planning Assistant in Job Budgets	People Planner	Boolean...		✓	0	0.00	0.00		
14	Show Planning Assistant in Periodic JobBudgets	People Planner	Boolean...		✓	0	0.00	0.00		
15	Show Planning Assistant in Progress Evaluation	People Planner	Boolean...		✓	0	0.00	0.00		
16	Show Resourcing Overview	People Planner	Boolean...		✓	0	0.00	0.00		
17	Update Total Cost (Base) in Budget	People Planner	Boolean...			0	0.00	0.00		
18	URL for Capacity Overview	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerWebComponents/RMViewPage.aspx	
19	URL for MyPlan Portal	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/MyPlanPortal/	
20	URL for MyPlan WSC	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/MyPlanWSC/	
21	URL for Planning Assistant	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerWebComponents/PMViewPage.aspx	
22	Web Service API Namespace	People Planner	StringVal...			0	0.00	0.00	http://marstrand-innovation.com/	
23	Web Service API Password	People Planner	StringVal...			0	0.00	0.00	123456	
24	Web Service API SOAP Address	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerAPI/ProjectsAPI.asmx	
25	Web Service API User	People Planner	StringVal...			0	0.00	0.00	PSO\Administrator	

Settings for the People Planner Web Components

The People Planner Web Components Web page is designed to be embedded in the Maconomy Workspace Client (WSC).

The configuration in Maconomy consists of two parts:

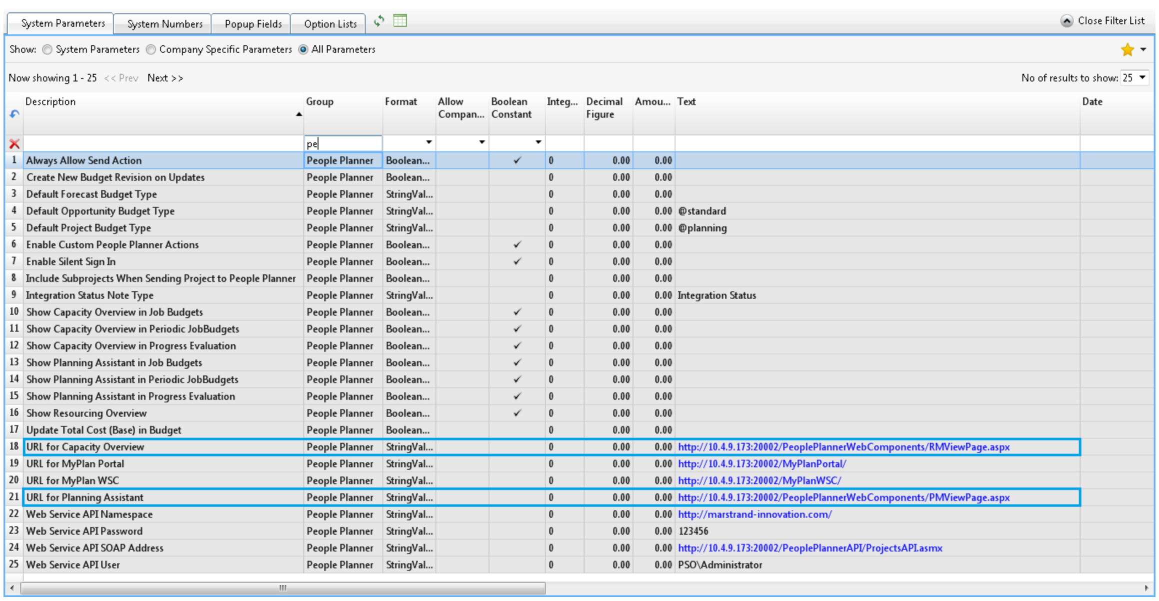
- Configure the URLs
- Tweak the location where the Web Component is embedded in the WSC

To set up the URLs:

1. Set the **URL for Capacity Overview** to the URL for RMViewPage.aspx. This URL follows the general form: `http://<host>:<port>/PeoplePlannerWebComponents/RMViewPage.aspx`

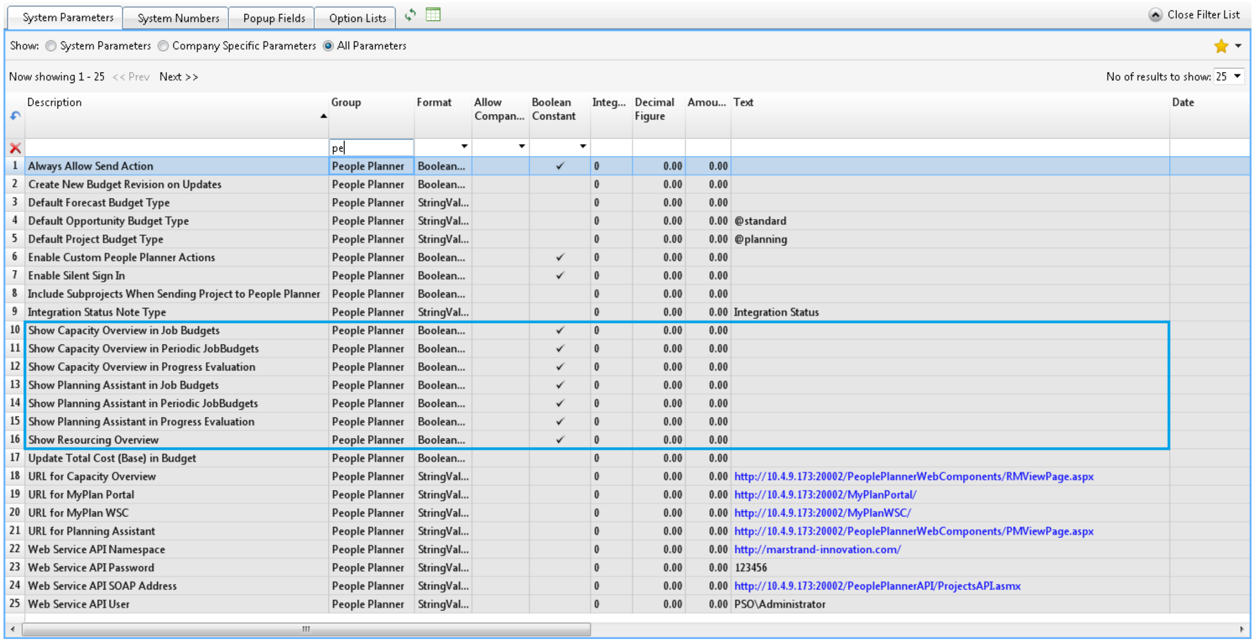
> **Note:** The URL for Capacity Overview is available in Maconomy 2.4 LA or newer. You can safely ignore it if this setting does not exist.

2. Set the **URL for Planning Assistant** to the URL for PMViewPage.aspx. This URL follows the general form: `http://<host>:<port>/PeoplePlannerWebComponents/PMViewPage.aspx`



	Description	Group	Format	Allow Compan...	Boolean Constant	Integ...	Decimal Figure	Amou...	Text	Date
1	Always Allow Send Action	People Planner	Boolean...		✓	0	0.00	0.00		
2	Create New Budget Revision on Updates	People Planner	Boolean...			0	0.00	0.00		
3	Default Forecast Budget Type	People Planner	StringVal...			0	0.00	0.00		
4	Default Opportunity Budget Type	People Planner	StringVal...			0	0.00	0.00	@standard	
5	Default Project Budget Type	People Planner	StringVal...			0	0.00	0.00	@planning	
6	Enable Custom People Planner Actions	People Planner	Boolean...		✓	0	0.00	0.00		
7	Enable Silent Sign In	People Planner	Boolean...		✓	0	0.00	0.00		
8	Include Subprojects When Sending Project to People Planner	People Planner	Boolean...			0	0.00	0.00		
9	Integration Status Note Type	People Planner	StringVal...			0	0.00	0.00	Integration Status	
10	Show Capacity Overview in Job Budgets	People Planner	Boolean...		✓	0	0.00	0.00		
11	Show Capacity Overview in Periodic JobBudgets	People Planner	Boolean...		✓	0	0.00	0.00		
12	Show Capacity Overview in Progress Evaluation	People Planner	Boolean...		✓	0	0.00	0.00		
13	Show Planning Assistant in Job Budgets	People Planner	Boolean...		✓	0	0.00	0.00		
14	Show Planning Assistant in Periodic JobBudgets	People Planner	Boolean...		✓	0	0.00	0.00		
15	Show Planning Assistant in Progress Evaluation	People Planner	Boolean...		✓	0	0.00	0.00		
16	Show Resourcing Overview	People Planner	Boolean...		✓	0	0.00	0.00		
17	Update Total Cost (Base) in Budget	People Planner	Boolean...			0	0.00	0.00		
18	URL for Capacity Overview	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerWebComponents/RMViewPage.aspx	
19	URL for MyPlan Portal	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/MyPlanPortal/	
20	URL for MyPlan WSC	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/MyPlanWSC/	
21	URL for Planning Assistant	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerWebComponents/PMViewPage.aspx	
22	Web Service API Namespace	People Planner	StringVal...			0	0.00	0.00	http://marstrand-innovation.com/	
23	Web Service API Password	People Planner	StringVal...			0	0.00	0.00	123456	
24	Web Service API SOAP Address	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerAPI/ProjectsAPI.asmx	
25	Web Service API User	People Planner	StringVal...			0	0.00	0.00	PSO\Administrator	

Configuring where the People Planner Web Components are embedded is controlled by the various **Show…** settings.



System Parameters | System Numbers | Popup Fields | Option Lists | Close Filter List

Show: System Parameters Company Specific Parameters All Parameters

Now showing 1 - 25 << Prev Next >> | No of results to show: 25

	Description	Group	Format	Allow Compan...	Boolean Constant	Integ...	Decimal Figure	Amou...	Text	Date
		pe								
1	Always Allow Send Action	People Planner	Boolean...		✓	0	0.00	0.00		
2	Create New Budget Revision on Updates	People Planner	Boolean...			0	0.00	0.00		
3	Default Forecast Budget Type	People Planner	StringVal...			0	0.00	0.00		
4	Default Opportunity Budget Type	People Planner	StringVal...			0	0.00	0.00	@standard	
5	Default Project Budget Type	People Planner	StringVal...			0	0.00	0.00	@planning	
6	Enable Custom People Planner Actions	People Planner	Boolean...		✓	0	0.00	0.00		
7	Enable Silent Sign In	People Planner	Boolean...		✓	0	0.00	0.00		
8	Include Subprojects When Sending Project to People Planner	People Planner	Boolean...			0	0.00	0.00		
9	Integration Status Note Type	People Planner	StringVal...			0	0.00	0.00	Integration Status	
10	Show Capacity Overview in Job Budgets	People Planner	Boolean...		✓	0	0.00	0.00		
11	Show Capacity Overview in Periodic JobBudgets	People Planner	Boolean...		✓	0	0.00	0.00		
12	Show Capacity Overview in Progress Evaluation	People Planner	Boolean...		✓	0	0.00	0.00		
13	Show Planning Assistant in Job Budgets	People Planner	Boolean...		✓	0	0.00	0.00		
14	Show Planning Assistant in Periodic JobBudgets	People Planner	Boolean...		✓	0	0.00	0.00		
15	Show Planning Assistant in Progress Evaluation	People Planner	Boolean...		✓	0	0.00	0.00		
16	Show Resourcing Overview	People Planner	Boolean...		✓	0	0.00	0.00		
17	Update Total Cost (Base) in Budget	People Planner	Boolean...			0	0.00	0.00		
18	URL for Capacity Overview	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerWebComponents/RMViewPage.aspx	
19	URL for MyPlan Portal	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/MyPlanPortal/	
20	URL for MyPlan WSC	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/MyPlanWSC/	
21	URL for Planning Assistant	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerWebComponents/PMViewPage.aspx	
22	Web Service API Namespace	People Planner	StringVal...			0	0.00	0.00	http://marstrand-innovation.com/	
23	Web Service API Password	People Planner	StringVal...			0	0.00	0.00	123456	
24	Web Service API SOAP Address	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerAPI/ProjectsAPI.asmx	
25	Web Service API User	People Planner	StringVal...			0	0.00	0.00	PSO\Administrator	

Tip: This part of the setup is usually left to the Business Consultants. You should just make sure to select (check-mark) all of the appropriate items.

Set Up People Planner Silent Sign-In

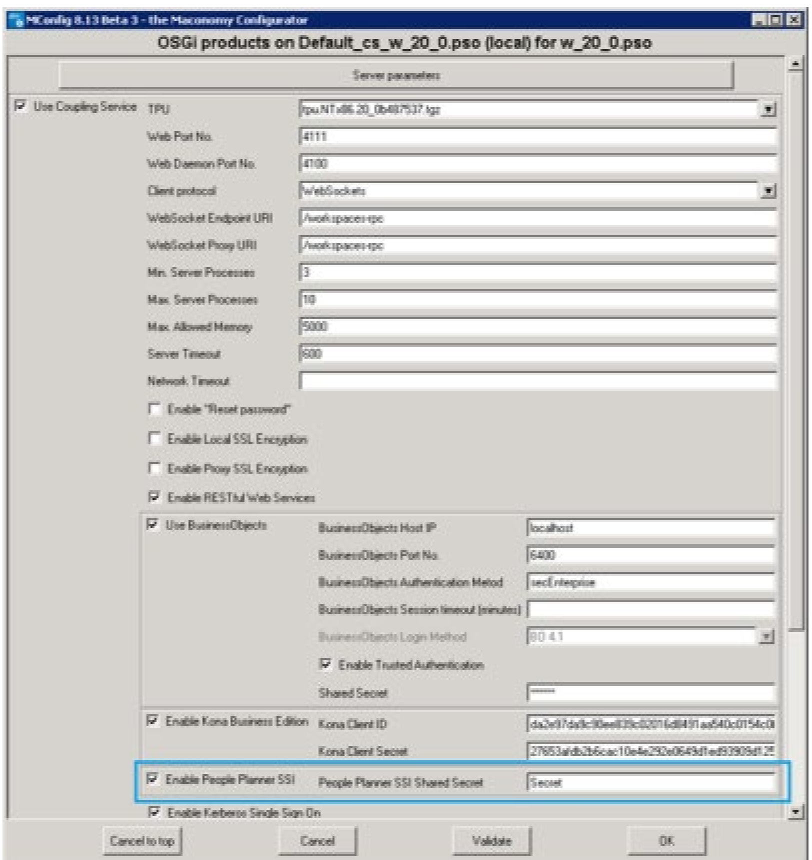
The People Planner Silent Sign-In (SSI) functionality is used by Maconomy to authenticate a user to People Planner when the user navigates to where either MyPlan or the Web Components are embedded in the Maconomy Workspace Client.

Setting this up requires work on both sides of the integration—on the People Planner side and on the Maconomy side.

Configuration in Maconomy MConfig

First, you must enable People Planner SSI in Maconomy:

1. Run the Maconomy **MConfig** application.
2. Navigate to the **OSGi products** page.
3. Select the **Enable People Planner SSI** check box.
4. Enter a unique value of your choosing in the **People Planner SSI Shared Secret** field.

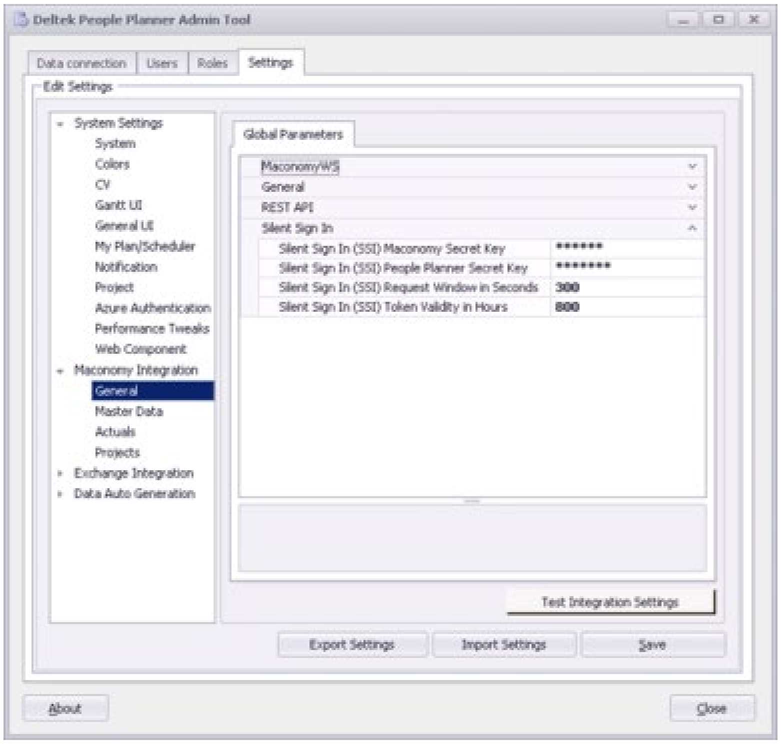


5. Complete the installation.

Configuration in the People Planner Admin Tool

You must also configure the SSI on the People Planner side:

1. Run the **People Planner Admin Tool**.
2. Click the **Settings** tab.
3. Navigate to **Maconomy Integration » General**.



4. Enter a value for the **Silent Sign In (SSI) Maconomy Secret Key**.

   This value must be the same value that you chose in MConfig, where it was called the *People Planner SSI Shared Secret*.

5. Enter the **Silent Sign In (SSI) People Planner Secret Key**.

   Note: For security, you should set the value of **People Planner Secret Key** to something different from the value of **Maconomy Secret Key**.

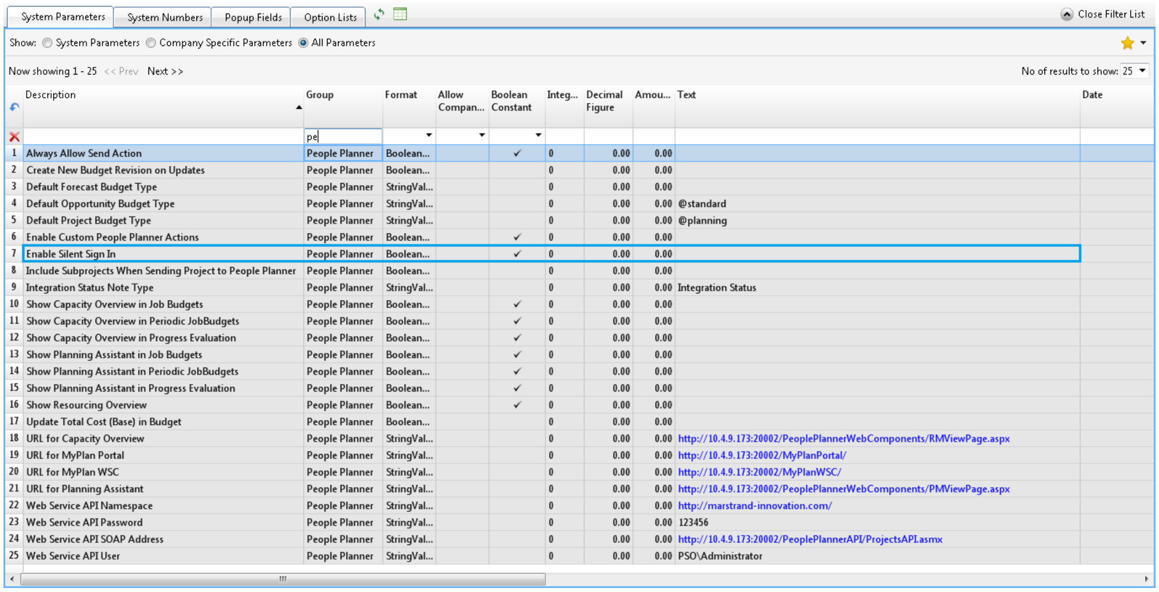
6. Click **Save** to save the changed setting in the People Planner database.

Configuration in the Maconomy Workspace Client

Now you must only provide the final setting in Maconomy:

1. Run the **Maconomy Workspace Client (WSC)** as a Maconomy Admin user.
2. Navigate to **Setup » System Setup » Parameters and Numbers » System Parameters**.
3. Filter on the **Groups** columns to see only the system parameters that relate to People Planner.

4. Select the **Enable Silent Sign In** check box.



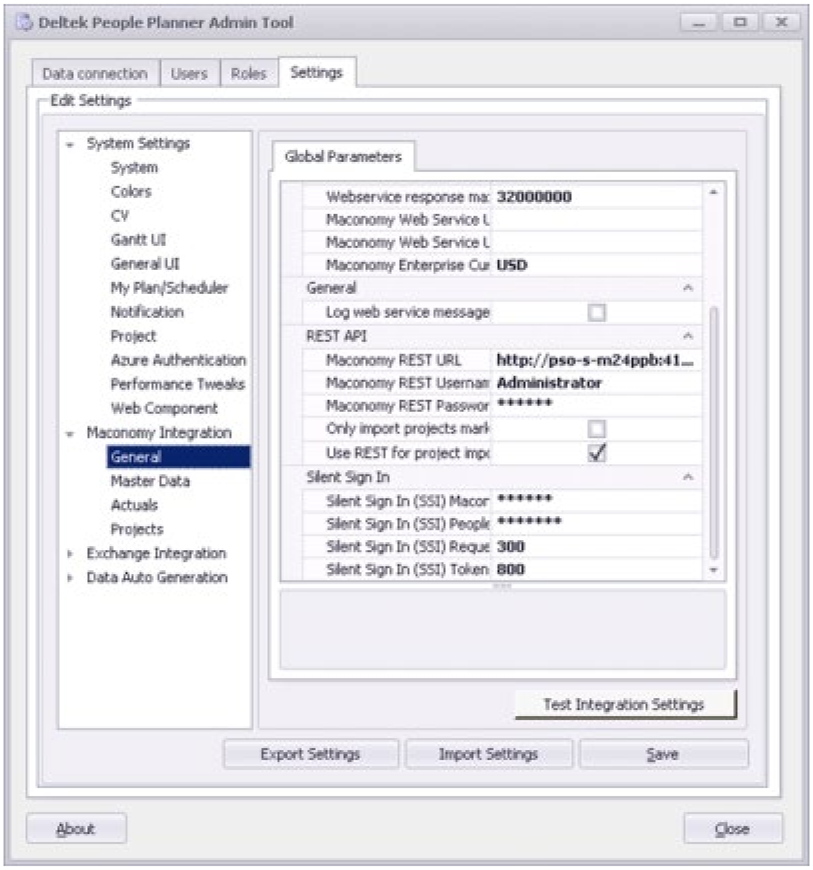
	Description	Group	Format	Allow Compan...	Boolean Constant	Integ...	Decimal Figure	Amou...	Text	Date
1	Always Allow Send Action	People Planner	Boolean...		✓	0	0.00	0.00		
2	Create New Budget Revision on Updates	People Planner	Boolean...			0	0.00	0.00		
3	Default Forecast Budget Type	People Planner	StringVal...			0	0.00	0.00		
4	Default Opportunity Budget Type	People Planner	StringVal...			0	0.00	0.00	@standard	
5	Default Project Budget Type	People Planner	StringVal...			0	0.00	0.00	@planning	
6	Enable Custom People Planner Actions	People Planner	Boolean...		✓	0	0.00	0.00		
7	Enable Silent Sign In	People Planner	Boolean...		✓	0	0.00	0.00		
8	Include Subprojects When Sending Project to People Planner	People Planner	Boolean...			0	0.00	0.00		
9	Integration Status Note Type	People Planner	StringVal...			0	0.00	0.00	Integration Status	
10	Show Capacity Overview in Job Budgets	People Planner	Boolean...		✓	0	0.00	0.00		
11	Show Capacity Overview in Periodic JobBudgets	People Planner	Boolean...		✓	0	0.00	0.00		
12	Show Capacity Overview in Progress Evaluation	People Planner	Boolean...		✓	0	0.00	0.00		
13	Show Planning Assistant in Job Budgets	People Planner	Boolean...		✓	0	0.00	0.00		
14	Show Planning Assistant in Periodic JobBudgets	People Planner	Boolean...		✓	0	0.00	0.00		
15	Show Planning Assistant in Progress Evaluation	People Planner	Boolean...		✓	0	0.00	0.00		
16	Show Resourcing Overview	People Planner	Boolean...		✓	0	0.00	0.00		
17	Update Total Cost (Base) in Budget	People Planner	Boolean...			0	0.00	0.00		
18	URL for Capacity Overview	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerWebComponents/RMViewPage.aspx	
19	URL for MyPlan Portal	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/MyPlanPortal/	
20	URL for MyPlan WSC	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/MyPlanWSC/	
21	URL for Planning Assistant	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerWebComponents/PMViewPage.aspx	
22	Web Service API Namespace	People Planner	StringVal...			0	0.00	0.00	http://marstrand-innovation.com/	
23	Web Service API Password	People Planner	StringVal...			0	0.00	0.00	123456	
24	Web Service API SOAP Address	People Planner	StringVal...			0	0.00	0.00	http://10.4.9.173:20002/PeoplePlannerAPI/ProjectsAPI.asmx	
25	Web Service API User	People Planner	StringVal...			0	0.00	0.00	PSO\Administrator	

Verification

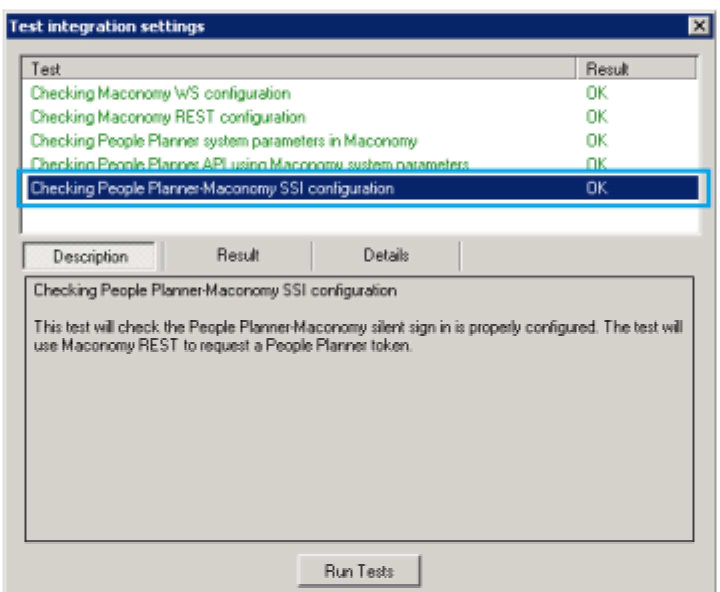
To verify that the SSI settings have been set up and configured correctly, you can use the Test Integration Settings button in the People Planner Admin Tool:

1. Run the **People Planner Admin Tool**.
2. Load the **DataConnection.xml file** and connect to the People Planner database.
3. Click the **Settings** tab.

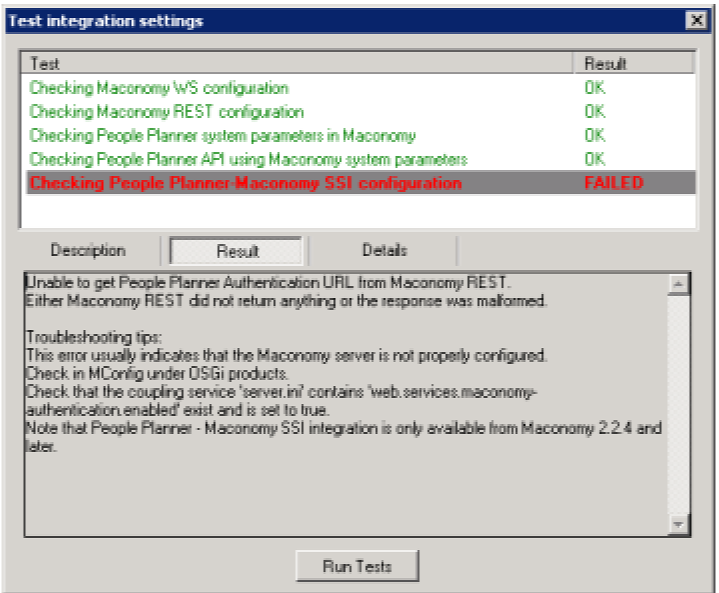
4. Navigate to **Maconomy Integration » General**.



5. Click the **Test Integration Settings** button.



If the People Planner SSI has been configured correctly, it reports the status as OK. If it fails, you can click **Results** to get information about what might be wrong.



Advanced Verification

As a further verification that the People Planner SSI has been configured correctly, you can try to access MyPlan from inside the Maconomy Workspace Client (WSC):

1. Run the **Maconomy WSC** as a normal user.
2. Navigate to the location where MyPlan is embedded, for example, **Time & Expenses » Time » MyPlan**.
3. Wait for MyPlan to load.
4. Inspect the People Planner API Web Service log file, which is located at C:\inetpub\People Planner Web Apps 3.8.5 Alpha00 (343)\Logs\Api.log

> **Note:** Before People Planner 3.8.5, the logs for each of the People Planner Web applications were located in a subdirectory of each installation folder. Beginning with People Planner 3.8.5 all of the logs are located in the Logs folder under the People Planner Web Apps folder.

If IIS has been installed, and it works correctly, the log file should contain a line like:

```
[2017-09-18 09:25:52] Api Information [4088]: GetSecurityToken called.
encryptedMessage=cmenJnWEQcVxjw6QJnTU4xh6lLYQMMsownIGdBFqkzWIzt40pbeZtDaRfMuf1YPvVc+Yr
5Qu1mq23gV/Q3TC4WET3fAo5xSI5mAg0JIBMIHx6SI/dRBZkabTTBla5wnP
```

You can perform a similar check using the People Planner Web Components instead of MyPlan. However, this requires a few more steps and does not provide any additional information.

Note: Before you can access MyPlan as described, People Planner must have performed a master data import of at least the users from Maconomy. A Business Consultant usually sets that up; thus, it is not described in this guide. See the *Deltek People Planner Integrations Guide* for more information about master data imports.

Installation and Basic Setup of Integration with Exchange and Outlook

This section describes how to install the integration between People Planner and Exchange/Outlook.

This integration consists of two parts:

- A synchronization between People Planner and Exchange/Outlook.
- A lookup from Outlook to People Planner when creating Assignments in Outlook.

Synchronization between People Planner and Exchange/Outlook

The synchronization between People Planner and Outlook is always via the Exchange server.

Bookings are created in either the People Planner applications or in Outlook. The bookings are then synchronized first with the Exchange server and from there with the other system.

The synchronization between Exchange and Outlook occurs entirely between Exchange and Outlook, and does not depend on any People Planner software or settings.

People Planner synchronizes with Exchange by calling the EWS Exchange Web service. A scheduled task is set up to call this Web service from People Planner.

Setup on the Exchange Server

The People Planner Exchange integration uses a Windows Domain user to connect to the Exchange Server. This user must have access to create/edit/read appointments in the mailboxes for the Exchange users. The user that is used for the People Planner Exchange integration is not required to have a mailbox.

For the maintenance of the access to the users' mailboxes in the People Planner Exchange integration, Deltek recommends that you create a Windows Domain Group and make all users members of that group. When a resource is enabled for the Exchange Synchronization in People Planner, the same user should be added to the Windows Domain Group and removed when the Exchange Synchronization is disabled.

To configure for Exchange 2010 or newer:

1. Create a Windows Domain user, such as PPexchange.
2. Create a Windows Domain group, such as PeoplePlannerExchangeUsers.
3. Make users/mailbox users members of PeoplePlannerExchangeUsers.

> **Note:** You only need to do this for the specific group of users that should be synchronized with Exchange, for example, the users that have Synchronize this Resource with Exchange enabled in the Resources view in the People Planner Windows Application.

4. On the Exchange Server, create a **Management Scope** and then do a **Role Assignment** that allows the PPexchange account to impersonate the members of the PeoplePlannerExchangeUsers group. You do this by running the following commands on the Exchange Server in the Exchange Management Shell:

    a. `$PPuser = "PPexchange"`

    b. `$PPgroup = "CN=PeoplePlannerExchangeUsers,CN=Users,DC=<theServer>,DC=com"`

    c. `New-ManagementScope -name:PeoplePlannerExchange -RecipientRestrictionFilter:"MemberOfGroup -eq '$PPgroup'"`

    d. `New-ManagementRoleAssignment -Name:PeoplePlannerExchangeRole -Role:ApplicationImpersonation -User:$PPuser -CustomRecipientWriteScope:PeoplePlannerExchange`

The value that is used for the **$PPgroup** must be the **Active Directory Distinguished Name** (ADDN) of the PeoplePlannerExchangeUsers security group. To get this, use the following **dsquery** command:

```
dsquery group "People*"
```

If the New-ManagementScope and New-ManagementRoleAssignment commands have been run with incorrect values, you can clean up and remove the incorrect ones, using the following commands:

```
Remove-ManagementRoleAssignment -Identity PeoplePlannerExchangeRole

Remove-ManagementScope -Identity PeoplePlannerExchange
```

Setup in Office 365

People Planner supports Office 365 as long as the bundled Exchange server is a supported version. The steps are the same as those that are described in Setup on the Exchange Server, with one possible exception.

In the Microsoft data centers, certain objects are consolidated to save space. When you attempt to use Windows PowerShell to modify one of these objects for the first time, you might encounter the following error message:

```
"This operation is not allowed for the organization with disabled customizations. To
enable this operation, you need to execute Enable-OrganizationCustomization task
first."
```

This is likely to happen when you run the New-ManagementRoleAssignment-command. In this case, you must run the following additional command:

```
Enable-OrganizationCustomization
```

You only need to run this once; on subsequent runs, it results in the following error message:

```
"This operation is not available in the current service offer."
```

Setup in People Planner

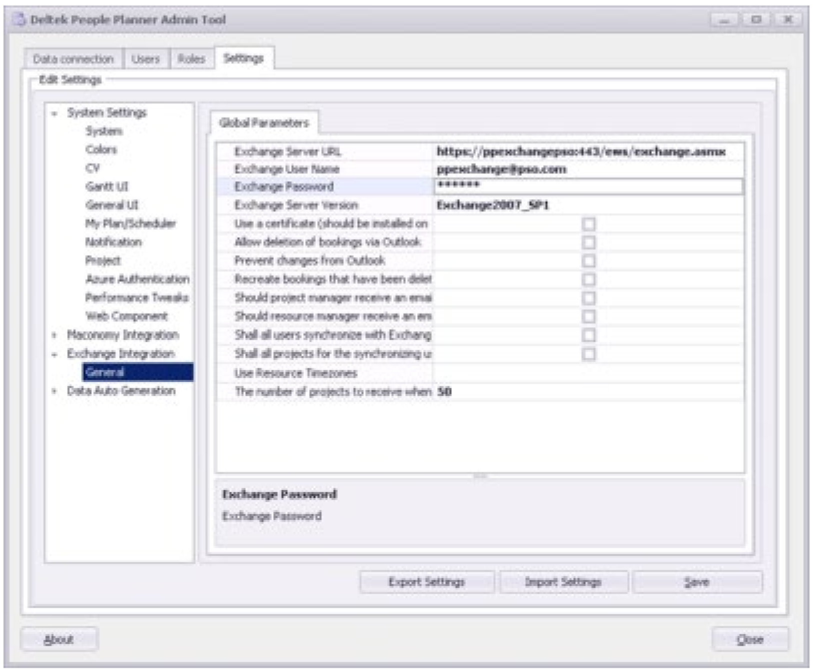
No special People Planner software must be installed for the synchronization; this only requires that the People Planner Service be installed, but that is a general requirement for running any scheduled task.

People Planner must know how to call the EWS Exchange Web service:

1. Run the **People Planner Admin Tool**.
2. Load the **DataConnection.xml file** and connect to the People Planner database.
3. Click the **Settings** tab.
4. Navigate to **Exchange Integration » General**.
5. Enter the following in the **Exchange Server URL** field:

   `https://<exchange-ip>:443/ews/exchange.asmx`

6. Enter the credentials of the user that you defined in the Exchange system in the **Exchange User Name** and the **Exchange Password** fields, respectively.



7. Click **Save** to save the changed settings to the People Planner database.

Lookup from Outlook into People Planner

When creating People Planner bookings from Outlook, a user must do a lookup in the People Planner database to find the projects or tasks to book on. Two pieces of People Planner software are involved in this:

- People Planner Outlook AddIn – installed in Outlook.
- People Planner Outlook Web Service – installed with the other People Planner Web services

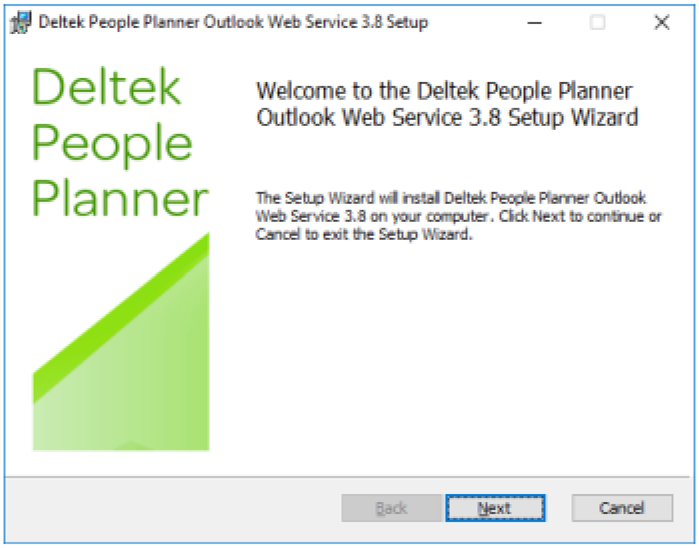
Install and Configure the People Planner Outlook Web Service

The installer for the People Planner Outlook Web service is not included in the installer for the People Planner Web Applications, and instead it has its own installer.

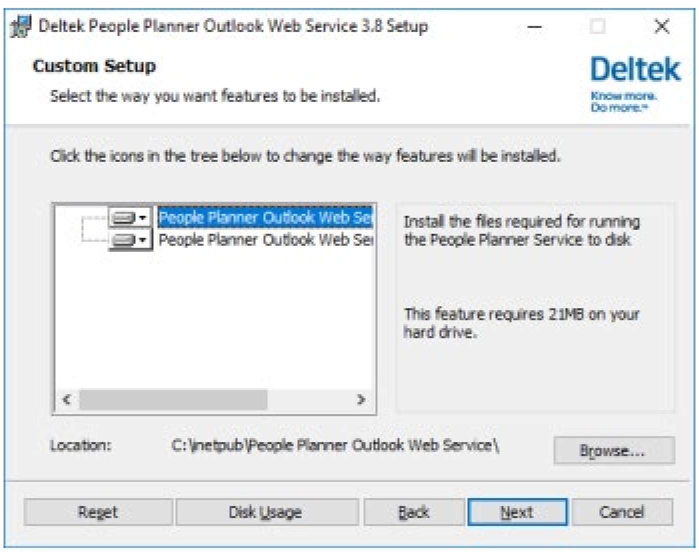
To install the People Planner Outlook Web service:

1. Extract the zip file that contains the People Planner installers.

2. Double-click the **InstallOutlookWebService.vbs file** and click **Yes** at the prompt to allow the installer to make changes on your computer. The Setup Wizard for People Planner Outlook Web service then starts.

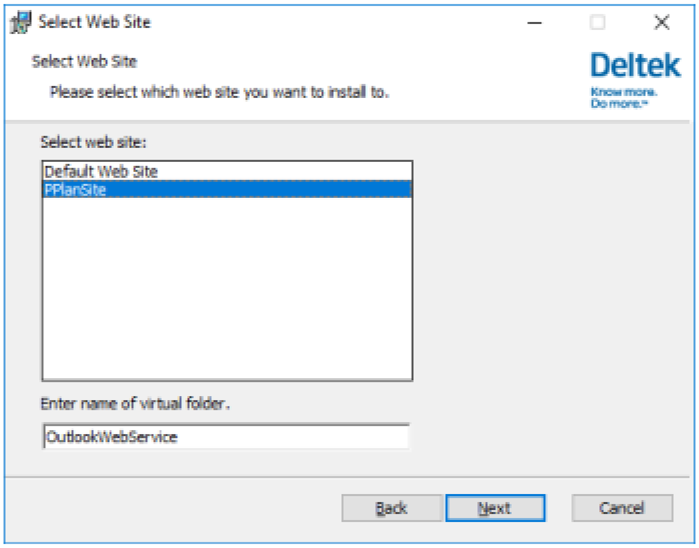


3. Click **Next** to continue.



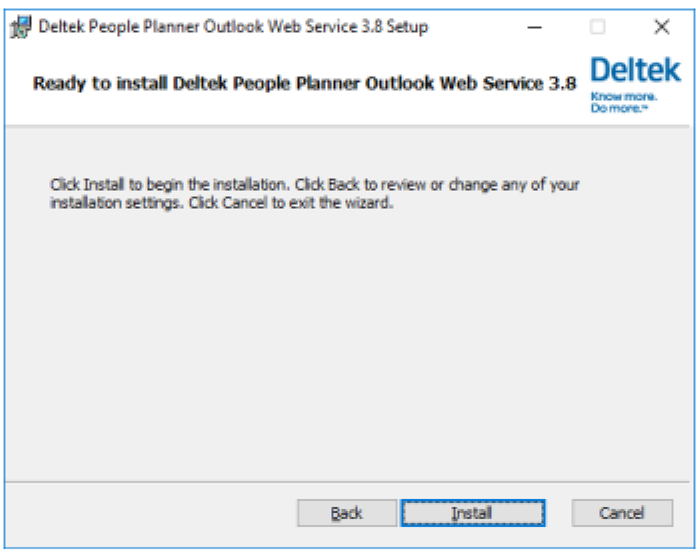
4. Click **Next** to continue.

5. Select the Web site where you want to install the People Planner Outlook Web service.



Note: If you have not used the IIS Manager to create a Web site, only the Default Web Site appears in the list of Web sites.

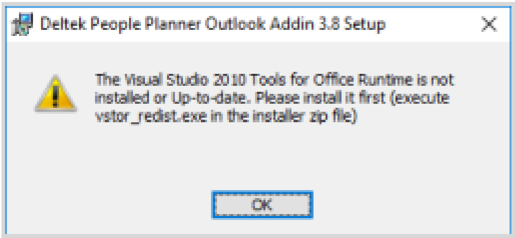
6. Click **Next** to continue.



7. Click **Install** to begin the installation.
8. Click **Finish** to close the Setup Wizard.

Install and Configure the People Planner Outlook AddIn

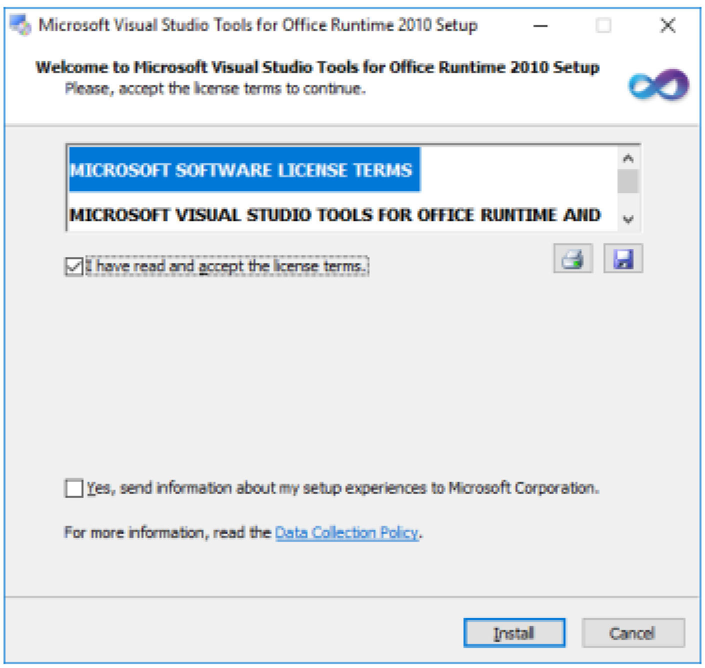
Before you can install the People Planner Outlook AddIn, you must make sure that the Visual Studio Tools for Office Runtime (VSTO) are installed. If they are not, an error message is displayed when you attempt to install the AddIn:



The zip package that contains the People Planner installers also contains an installer for VSTO.

To install the VSTO:

1. Extract the zip file that contains the People Planner installers.
2. Click **vstor_redist.exe**.

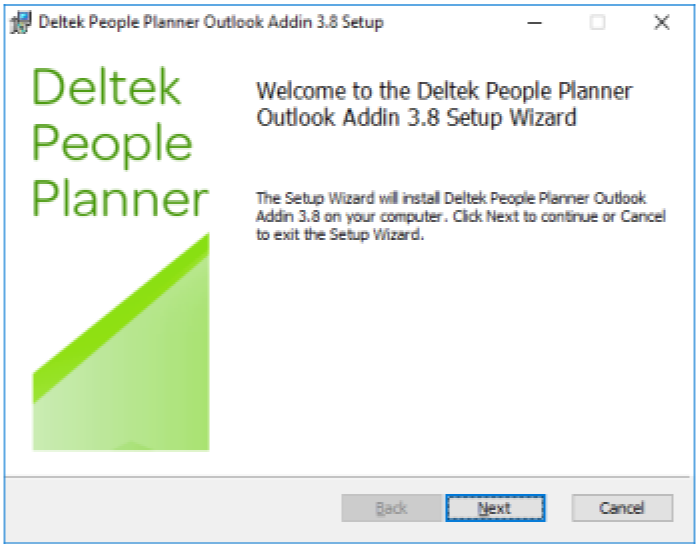


3. Select the **I have read and accept the license terms** check box.
4. Click **Install**.
5. Click **Finish** to close the installer.

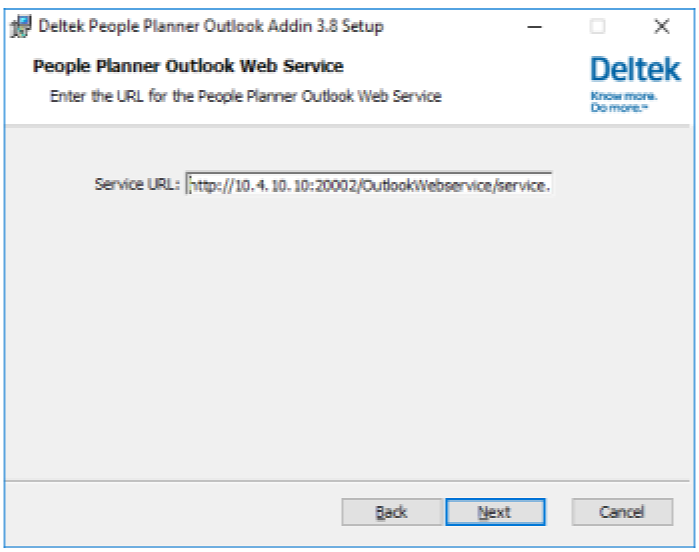
To install the People Planner Outlook AddIn:

1. Extract the zip file that contains the People Planner installers.

2. Double-click the **People Planner Outlook AddIn msi file** and click **Yes** at the prompt to allow the installer to make changes on your computer. The Setup Wizard for the People Planner Outlook AddIn starts.



3. Click **Next**.



4. Enter the **Service URL** to where the People Planner Outlook Web service is installed. The form of this URL is

   http://<host>:<port>/PeoplePlannerOutlookWebService/service.svc

5. Click **Next**.
6. Click **Install**.
7. Click **Finish** to close the Setup Wizard.

Appendix A: Installation Checklists

This section provides you with a set of checklists for the most effective way to complete the installation of the People Planner software.

These checklists should provide enough information, but additional detail about the individual items are provided in the rest of this guide.

Warning: Beginning with People Planner Release 3.8.6, there are changes to how users log in to the People Planner Windows Application. Consequently, the DataConnection.xml file has been moved to a new location. You must also install the People Planner Security Service, which is a new web service as of Release 3.8.6.

Install the People Planner Core Software

Before you can install any other People Planner software, you must have established the core People Planner system.

1. Check prerequisites:
    a. Windows Applications.
        - NET 4.7.2
        - SQL Server
    b. Web Applications
        - APS NET 4.7
        - .NET Core 3.1.10
        - SQL Server
2. Install the People Planner Admin Tool application.
3. Install the People Planner Security Service.
4. Create a People Planner database:
    a. Run the People Planner Admin Tool:
        i. Click the **Data Connection** tab.
        ii. Load the **DataConnection.xml** file, which is located in the People Planner Web Apps folder under inetpub.
        iii. Correct the **Server Name**—for example, PSO-S-M24PPB\MACONOMY
        iv. Select your initial **Database Authentication**. It must have rights to create a database:
            - For example, using **Windows Authentication** or using the sa user
        v. Enter a name for the People Planner database.
        vi. Click **Create Database**.
        vii. Click **Save Config** to save the updated DataConnection.xml file.

5. Set up the database privileges:
    a. Run **SQL Server Management Studio**:
        i. Create a login—for example, named *ppuser*.
            1. Select **SQL Server Authentication**.
            2. Enter a password.
            3. Deselect the **Enforce password expiration** check box to set the password policy to never expire.
            4. Under **User Mapping**, select the People Planner database.
            5. Select the database role memberships: **db_datareader**, **db_datawriter**, and **public**.
        ii. Under **Databases**, select the **People Planner database**.
            1. Navigate to **Programmability » Stored Procedures** and select the **GetSequence** stored procedure.
            2. Right-click and select **Properties**.
            3. Under **Permissions**, add the **ppuser** and **Grant Execute** permissions.
6. Correct the DataConnection.xml file to use the ppuser login:
    a. Run the **People Planner Admin Tool**:
        i. Load the **DataConnection.xml** file.
        ii. Change the **Authentication** to **Database Authentication**.
        iii. Enter the user name and password for the ppuser login in the **User Name** and **Password** fields, respectively.
        iv. Click the **Save Config** button.
    b. Verification: Check that you can connect to the People Planner database:
        i. Close and then restart the **People Planner Admin Tool**.
        ii. Load the **DataConnection.xml** file.
        iii. Verify that **Authentication** is set to use the ppuser login.
        iv. Click the **Connect** button and verify that you can connect to the People Planner database.
7. Basic configuration:
    a. Add yourself as a People Planner Admin user.
        i. Run the **People Planner Admin Tool** and connect to the **People Planner database**.
        ii. Click the **Users** tab.
        iii. Use the **Add Users** button to add yourself as Admin.
    b. Set up the license file:
        i. Copy the People Planner license file, **PeoplePlannerLicense.lic**, to a suitable location, such as a file share where it can be accessed from other computers, for example:

           ```
           \\PeoplePlanner\peoplePlannerLicense.lic
           ```

ii. Run the **People Planner Admin Tool** and connect to the **People Planner database**.

iii. Click the **Settings** tab then select **System** and enter the following in the **License File Path**:

```
\\PeoplePlanner\PeoplePlannerLicense.lic
```

c. Verification: Check that you can call the People Planner Security Service test URL from a browser.

8. Install the People Planner Windows Application.

    a. Configure the People Planner Windows Application to use the People Planner Security Service.

    b. Verification: Check that you can start the People Planner Windows Application.

Install the People Planner Windows Service

The People Planner Service is required for running scheduled tasks from People Planner, such as importing data form Maconomy.

1. Check prerequisites.
    - .NET 4.7.2
2. Create a Windows account on the server where the People Planner Windows Service is running, for example, an account named PeoplePlannerService.

    a. Enter a password.

    b. Deselect the **Enforce password expiration** check box to set the password policy to never expire.

3. Run the People Planner Windows Application:

    a. Navigate to **Views » Security » Users**.

    b. Click the **+** button in the lower-left corner of the Users view and add the user **PeoplePlannerService**:

    i. Enter **PeoplePlannerService** in the **Name** field.

    ii. Enter the computer’s hostname in the **Network Domain Name** field.

    iii. Enter **PeoplePlannerService** in the **Network Username** field.

    c. Navigate to **Views » Security » Roles and Data Limitations**.

    d. Click the **Roles** tab, select the **Admin** role, and assign the **PeoplePlannerService** user to the Admin role.

    > **Tip:** If you install the People Planner Service on the same server where the People Planner Admin Tool is installed, you can use the Admin Tool to add the PeoplePlannerService user to the People Planner database, rather than performing the preceding manual steps to add that user.

4. Install the People Planner Service.

    a. When asked for **Service Login Credentials**, use the credentials of the **PeoplePlannerService user**.

   b. Select the **Grant Logon as Service** check box.

5. Create the **DataConnection.xml** file. You can do this by copying the DataConnecction.xml file, which is located under the People Planner Web Apps subfolder under the inetpub folder, to the **Settings** folder under the People Planner Service installation directory, replacing the existing file.
6. Under **Windows Services**, start the **People Planner Service**.
7. Verification: Run the People Planner Windows Application:
   a. Navigate to **Views » Tasks » Scheduled Tasks**.
   b. Check that the server time is being updated.

Integration with a Maconomy System

The setup of the integration between People Planner and Maconomy is organized into three parts:

- Part A: Installing and configuring the Maconomy Web services.
- Part B: Installing and configuring the People Planner Web applications.
- Part C: Setting up People Planner Silent Sign-In (SSI).

Part A: Install the Maconomy Web Services

Any integration with a Maconomy system always requires that you install the **MaconomyWS** Web service. The **Maconomy RESTful** Web service is optional; however, you must install it if you want to take advantage of the extra functionality that it enables.

1. Install the Maconomy Web services:
    a. Run the Maconomy **MConfig** tool:
        i. Install the MaconomyWS Web service:
            1. Navigate to **Web Products**.
            2. Select the **Web Services** check box.
            3. Select either **Install on Demand** or **Install Unconditionally** for **(Re)install Web Services**.
        ii. **If required**: Install the Maconomy RESTful Web service:
            1. Navigate to **OSGi Products**.
            2. Select the **Enable RESTful Web Services** check box.
            3. If you are planning to use SSI:
                a. Select the **Enable People Planner SSI** check box.
                b. Choose a **People Planner SSI Shared Secret**.
2. Configure the Web service URLs in People Planner:
    a. Open the Maconomy index file in a browser, for example, C:\Maconomy\index.html
    b. Run the **People Planner Admin Tool**:
        i. Click the **Settings** tab.
            1. Navigate to **Maconomy Integration » General**.
            2. Copy the **MaconomyWS URL** from the Maconomy index.html file to the **Maconomy Web Service URL** field.
                a. Enter **Administrator** in the **Web Service Username** field.
                b. Enter a **Web Service Password**.
            3. If REST is required: Copy the **RESTful Container API URL** from the Maconomy index.html file to the **Maconomy REST URL** field.
                a. Enter **Administrator** in the **Maconomy REST Username** field.
                b. Enter a **Maconomy REST Password**.
                c. If required, select the **Use REST for Project Import** check box according to whether People Planner should use the Maconomy RESTful Web service for importing projects or not.
            4. If you are planning to use SSI:
                a. Edit the **Silent Sign-In (SSI) Maconomy Secret Key** to the value that you chose in MConfig.
                b. Edit the **Silent Sign-In (SSI) People Planner Secret Key** to a different value.

    ii. Verification: Click the **Test Integration Settings** button to verify that People Planner can call the Maconomy Web services.

3. Continue with Part B of the integration.

Part B: Install the People Planner Web Applications

As part of installing the People Planner Core Software, you also install the People Planner Security Service. Since the installer of the Security Service is included in the People Planner Web Applications installer, it is likely that you have already installed these as well, and that they only need any final configuration at this stage.

If you have not installed them, you should run the People Planner web Applications installer again and use that to install the web applications that are still missing.

This checklist assumes that you need to install everything.

1. Check prerequisites:
   - Part A is completed.
   - IIS 10 or newer.
     - Windows Authentication.
     - ASP .NET 4.7
     - .NET Core 3.1.10
2. Create a Windows account on the server, for example one named PeoplePlannerIIS.
   a. Enter a password.
   b. Deselect the **Enforce password expiration** check box to set the password policy to never expire.
3. Run the People Planner Windows Application:
   a. Navigate to **Views » Security » Users**.
   b. Click the **+** button in the lower-left corner of the **Users** view and add the **PeoplePlannerIIS** user:
      i. Enter **PeoplePlannerIIS** in the **Name** field.
      ii. Enter the computer's hostname in the **Network Domain Name** field.
      iii. Enter **PeoplePlannerIIS** in the **Network Username** field.
   c. Navigate to **Views » Security » Roles and Data Limitations**.
   d. Click the **Roles** tab, select the **Admin role**, and assign the **PeoplePlannerIIS** user to the Admin role.

   > **Tip:** If you install the People Planner Web Applications on the same server where the People Planner Admin Tool is installed, you can use the Admin Tool to add the PeoplePlannerIIS user to the People Planner database, rather than performing the preceding manual steps.

4. Create a People Planner site in the IIS. If you have run the People Planner Web Applications installer, it will offer to create the web site for you.

5. The following is required for using the integration of People Planner with the Maconomy WorkSpace Client (WSC):

   If you have not already installed them using the People Planner Web Applications installer to install the Security Service, now install and configure MyPlan, People Planner API, and Web Components:

   a. Install the MyPlan Web Application. This installs two variants: MyPlan and MyPlanWSC.

      Install the People Planner API Web Service.

      Install the People Planner Web Components.

      Install the People Planner RESTful Web Service (RestApi)

      > **Tip:** Select the People Planner site (created in step 4) when asked where to install it.

   b. Edit the Anonymous Authentication for MyPlanWSC, People Planner API Web Service, and Web Components to use the PeoplePlannerIIS user.

      i. Run the **Internet Information Services Manager** application.

      ii. Edit the **Anonymous Authentication** to use the **PeoplePlannerIIS user** for **MyPlanWSC**, **People Planner API Web Service**, and **Web Components**.

6. Configure the People Planner Web applications in Maconomy:

   a. Run the **Maconomy Workspace Client** as administrator.

      i. Navigate to **Setup » System Setup » Parameters and Numbers » System Parameters**. Then filter on the **Group** column to see only the People Planner settings.

      ii. Configure the setting for the People Planner API Web Service:

         1. Enter the following URL of the People Planner API in the **Web Service API SOAP Address** field:

            `http://<host>:<port>/PeoplePlannerAPI/ProjectsAPI.asmx`

         2. Enter the user that you used for Anonymous Authentication for the People Planner API Web Service in the **Web Service API SOAP User** field.

         3. Enter the password that you used for Anonymous Authentication to the People Planner API Web Service in the **Web Service API SOAP Password** field.

            > **Warning:** Beginning with Release 3.9 the API Web Service Namespace was changed. **You must set this value in Maconomy to:**
            >
            > http://peopleplanner.deltek.com/api
            >
            > If you do not make this change in Maconomy, the People Planner / Maconomy integration will not work.
            >
            > This is also the default for Maconomy version 2.5 and newer.

      iii. Configure the settings for the MyPlan Web application:

         1. Enter the following URL of MyPlan in the **URL for MyPlan WSC** field:

http://<host>:<port>/MyPlanWSC/

2. **If required**, enter the following URL for MyPlan in the **URL for MyPlan Portal** field:

   http://<host>:<port>/MyPlan/

> **Attention:** MyPlan in the Maconomy Portal is deprecated in People Planner 4.3. This will be removed altogether in People Planner 4.4.
>
> Currently, the Maconomy Portal is available only when using Maconomy 2.5.x and older versions.

iv. Configure the settings for the People Planner Web Components Web application:

1. Enter the location where the RMViewPage.aspx of the People Planner Web Components is installed for the **URL for Capacity Overview**:

   http://<host>:<port>/PeoplePlannerWebComponents/RMViewPage.aspx

2. Enter the location where the PMViewPage.aspx of the People Planner Web Components is installed for the **URL for Planning Assistant**:

   http://<host>:<port>/PeoplePlannerWebComponents/PMViewPage.aspx

> **Note:** The **URL for Capacity Overview** is only available in Maconomy 2.4 LA or newer. You can safely ignore it on older Maconomy versions. The **URL for Planning Assistant** requires Maconomy 2.3 or newer.

> **Note:** In People Planner 3.7.1 and earlier the **URL for Capacity Overview** was called AssignResourcePage.aspx, and the **URL for Planning Assistant** was called CompactGantChartPage.aspx. Although these pages still exist, you must use RMViewPage and PMViewPage from version 3.8 and forward.

7. Verification for People Planner API: Run the Maconomy Workspace Client as a normal user.
   a. Select a Job and go to the **Budgeting** tab.
   b. Check that you can click the **Send Job to People Planner** button.
8. The following is required for using the integration of People Planner with the Maconomy web client:

   If you have not already installed them using the People Planner Web Applications installer, now install and configure the People Planner RESTful Web Service and Web Components. The Web Components is used both with the Maconomy web client and the WSC:

   a. Install the People Planner RESTful Web Service (RestApi).

   Install the People Planner Web Components.

> **Tip:** Select the People Planner site (created in step 4) when asked where to install it.

   b. Edit the Anonymous Authentication for the RestApi and the Web Components to use the PeoplePlannerIIS user.
      i. Run the Internet Information Services Manager application.
      ii. Edit the Anonymous Authentication to use the PeoplePlannerIIS user for RestApi and the Web Components.
9. Continue with Part C of the integration.

Part C: Set Up the People Planner Silent Sign-In (SSI)

If the integration requires that MyPlan and the People Planner Web Components be embedded in the Maconomy Workspace Client, you must also configure the People Planner SSI functionality.

1. Check prerequisites.
   - Parts A and B are completed.
2. If not already done as part of Part A: Run the Maconomy **MConfig** application:
   a. Navigate to **OSGi products**.
      i. Select the **Enable People Planner SSI** check box.
      ii. Choose a **People Planner SSI Shared Secret**.
3. If not already done as part of Part A: Run the **People Planner Admin Tool**:
   a. Click the **Settings** tab.
      i. Navigate to **Maconomy Integration » General**.
      ii. Edit the **Silent Sign-In (SSI) Maconomy Secret Key** to the value that you chose in MConfig.
      iii. Edit the **Silent Sign-In (SSI) People Planner Secret Key** to a different value.
4. Run the **Maconomy Workspace Client** as Administrator:
   a. Navigate to **Setup » System Setup » Parameters and Numbers » System Parameters**. Then filter on the **Group** column to see only the People Planner settings.
   b. Select the **Enable Silent Sign-In** check box.
5. Verification for MyPlan: Run the **Maconomy Workspace Client**.
   a. Open the **Time & Expansions workspace**.
   b. Navigate to **Time » My Plan**.
      i. Wait for MyPlan to load.

      Unless users have been imported into People Planner from Maconomy, MyPlan shows an error message that the user does not exist in People Planner. This is OK; it shows that People Planner is working, even if it is indicating that it does not recognize the user.
6. Verification for People Planner Web Components: Run the **Maconomy Workspace Client**:
   a. Open a job that has been sent to People Planner.
   b. Choose **Budgeting » Time**.
   c. Expand the **People Planner pane**.

i. Wait for the People Planner Web Components (the PMViewPage.aspx) to load.

Unless users have been imported into People Planner from Maconomy, the Web Components show an error message that the user does not exist in People Planner. This is OK; it shows that People Planner is working.

d. Expand the **Capacity Overview** pane.

i. Wait for the People Planner Web Components (the RMViewPage.aspx) to load.

Unless users have been imported into People Planner from Maconomy, the Web Components show an error message that the user does not exist in People Planner. This is OK; it shows that People Planner is working.

Integration with Exchange/Outlook

1. Configure settings on the Exchange server.
   a. Check prerequisites:
      - The **EWS Exchange** Web service must have been installed.

   b. Create a PPuser account to use with the EWS Exchange Web service.
   c. Give the PPuser account rights to create appointments in other mailboxes. You can restrict to only allow it do this for the mailboxes of People Planner users.
2. Run the People Planner Admin Tool:
   a. Click the **Settings** tab.
   b. Navigate to **Exchange Integration » General**.
   c. Enter the URL of the EWS Exchange Web service in the **Exchange Server URL** field:

      `https://<exchange-ip>:443/ews/exchange.asmx`

   d. Enter the credentials for the PPuser account.
3. Install and configure the People Planner Outlook Web service.
   a. Install the People Planner Outlook Web services.
      i. Select the **People Planner site** when asked where to install it.
4. Install the People Planner Outlook AddIn.
   a. Check prerequisites:
      - The Visual Studio Tools for Office (VSTO) must be installed.

   b. Install the People Planner Outlook AddIn.
      i. When asked, enter the URL to the People Planner Outlook Web Service:

         `http://<host>:<port>/PeoplePlannerOutlookWebService/service.svc`

Appendix B: Security

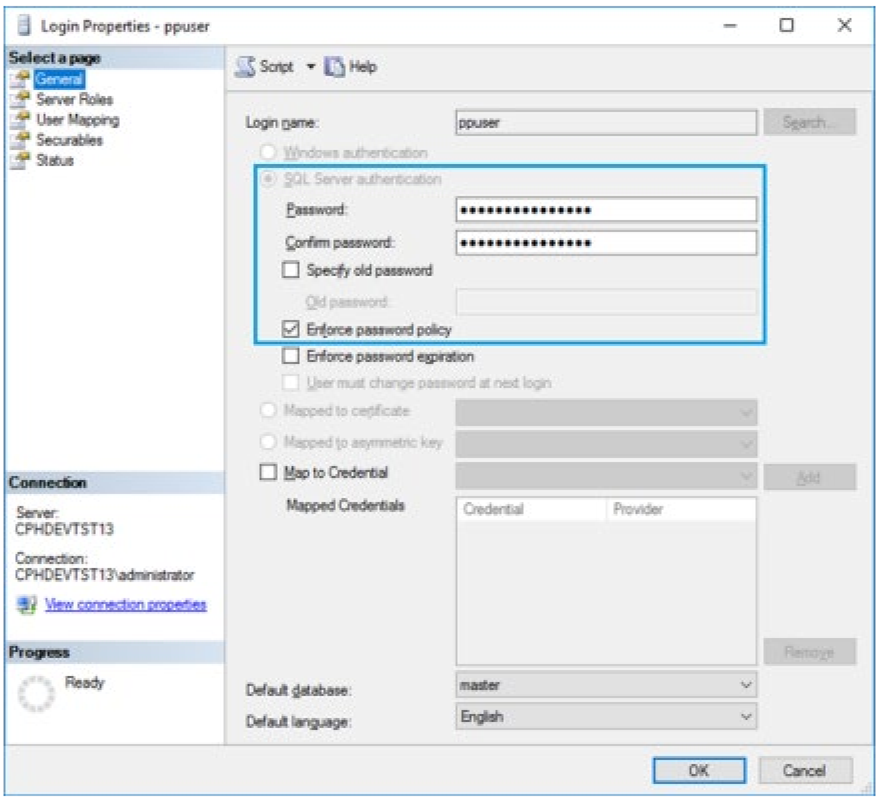
This section describes security measures that you can implement to tighten the overall security of the People Planner installation against hacking attacks.

Microsoft SQL Server

People Planner uses a Microsoft SQL Server to host its database. To minimize the risk of unauthorized access to the data in the database, you should implement the following measures.

Password Policy

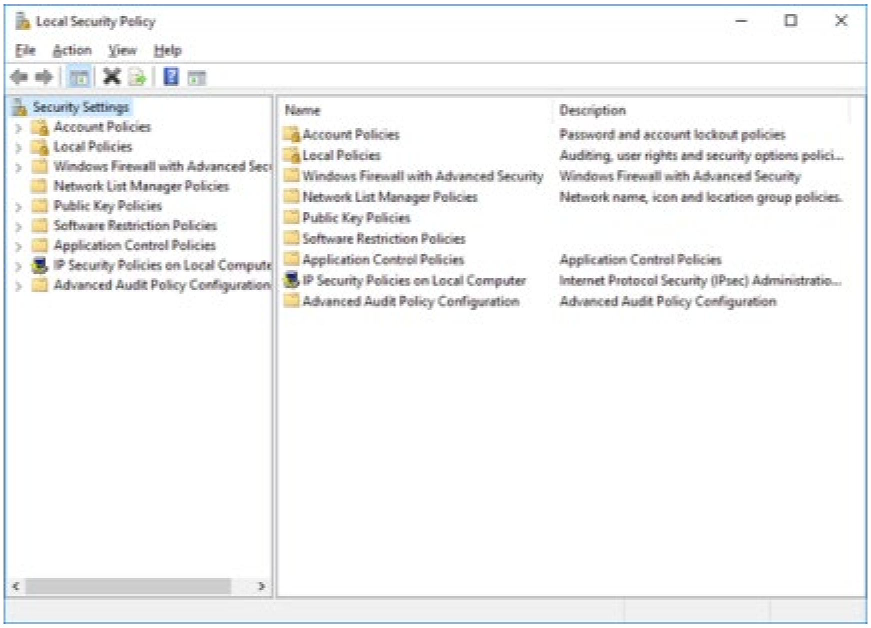
For security reasons, you should configure the Microsoft SQL Server account that People Planner uses to enforce password policy. This forces SQL Server to follow the local Windows password policies.



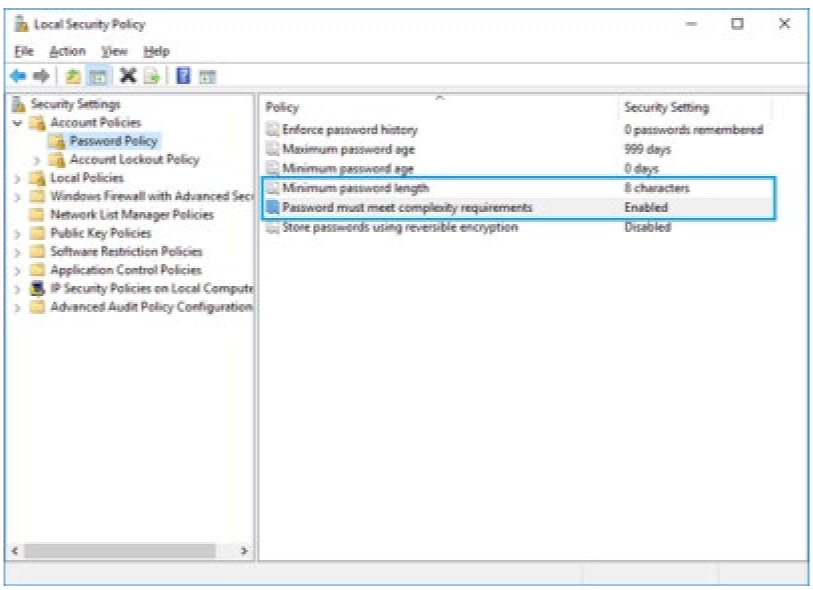
To determine the password polices of the computer:

1. Go to the Windows Start screen and open a CMD prompt.

2. Enter **secpol.msc** in the **Run** dialog box. This opens the **Local Security Policy** window.



3. Navigate to **Security Settings » Account Policies » Password Policy**.



4. Set a minimum password length and complexity enforcement.

Note: If you set a maximum password age in Local Security Policy, this does not have any effect on SQL Server unless you select Enforce Password Expiration.

Authentication

SQL Server supports the following types of authentication:

- Windows Authentication
- SQL Server Authentication

Both the People Planner Windows Application and the People Planner Admin Tool can use Windows Authentication to connect to the People Planner database. However, the People Planner Web applications cannot. Deltek therefore recommends that you generally use SQL Server Authentication to connect to the People Planner database.

Although you can use Windows Authentication under certain circumstances, Deltek does not recommend it. People Planner does not support Windows Security groups. This means that you would be required to add each People Planner user individually as an SQL Server login and give him or her access to the People Planner database. This is not a viable solution for a People Planner installation that has many users, or in a dynamic organization.

Normally, you would only use Windows Authentication for maintenance tasks like updating the People Planner database when an existing People Planner installation is updated to a new version. This type of maintenance requires a login that has special privileges on the SQL Server.

You would use SQL Server Authentication for daily usage of People Planner. This only requires a login that has db_datareader, db_datawriter, and public privileges.

Security Best Practices

For more information about configuring security for the SQL Server, see SQL Server 2012 Security Best Practice - Operational and Administrative Tasks by Bob Beauchemin.

Using Transport Layer Security

The People Planner package includes Web applications that must run under an Internet Information Services (IIS) Web server. To protect against network sniffing or Man-in-the-Middle attacks, you should configure the IIS to run with **Transport Layer Security** (TLS). This requires that you acquire a TLS certificate and install it on the IIS server.

> **Note:** Enabling SSL on the People Planner Web site is not sufficient. You should also specifically disable HTTP.

Currently Maconomy does not support TLS. Thus, you might experience problems when calling the People Planner Web services from the Maconomy end, for example, when sending a project from the Maconomy Workspace Client to People Planner.

Disable Vulnerable SSL Protocols

When enabling SSL, you should take care to disable the older and vulnerable SSL protocols, SSL 1.0, SSL 2.0, SSL 3.0, and TLS 1.0. As of Release 3.8.6, you should only have TLS 1.1 and TLS 1.2 enabled.

Enable HttpOnly with TLS Encryption for MyPlan

HttpOnly is a technique used to protect against the most common types of XSS attacks, including session hijacking. The web.config file for MyPlan contains the following block:

```
<!--Note: in httpCookies, please set requireSSL="true" if SSL certificates are
supported-->
<httpCookies domain="" httpOnlyCookies="true" requireSSL="false"/>
```

You can enable HttpOnly cookies even if there is no TLS certificate installed on the server. However, if TLS is enabled, you can use it to encrypt the HttpOnly cookies and strengthen the security. To do this, you must comment in the specified block.

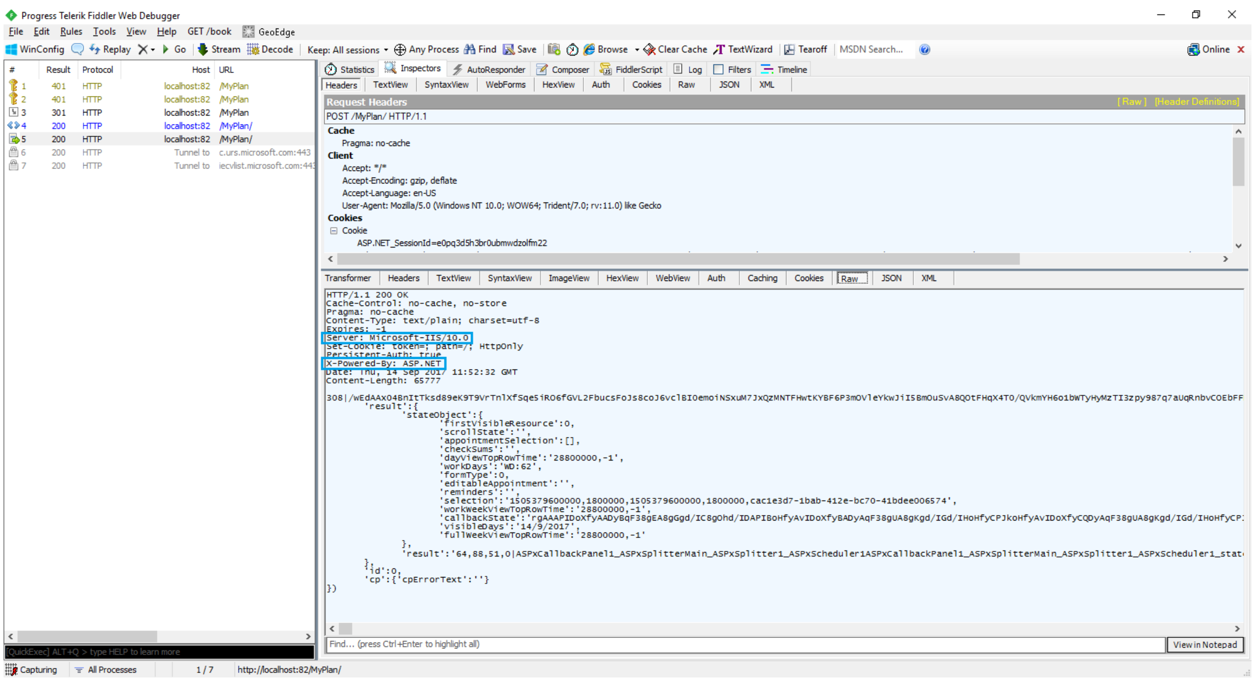
Remove Unnecessary Headers

Although security should not rely solely on this, it is always prudent to secure your system by not revealing any unnecessary details.

The IIS Web server includes a number of HTTP headers when it sends back the contents of the requested page. The browser uses these headers to determine how to render the content and for how long to cache the content. The IIS Web server also sends back identifying information. These identifying headers indicate the Web server version.

While some of the HTTP headers are necessary, the Web server's identifying HTTP headers are not. Providing identifying information can pose a security risk; the less information an attacker has about the system, the better.

The following figure shows an example of the two identifying headers.



Although the preceding figure is based on MyPlan, following procedures also apply to the People Planner Web services and the People Planner Web Components.

The Server Header

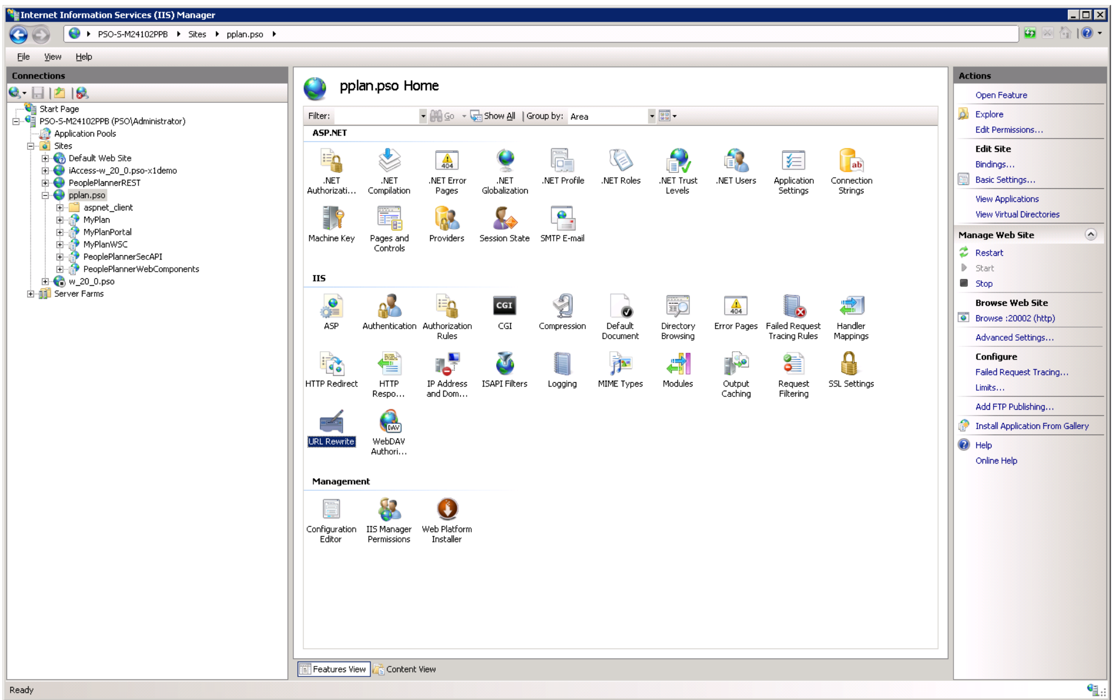
The **Server** header broadcasts that the Web server is an Internet Information Server and provides its version. The browser does not require this information, and there is no need to broadcast it.

> **Note:** If you are using IIS 10 or later, you can skip this section.

> **Prerequisite:** This solution requires that you have installed the URL Rewrite extension on the IIS.

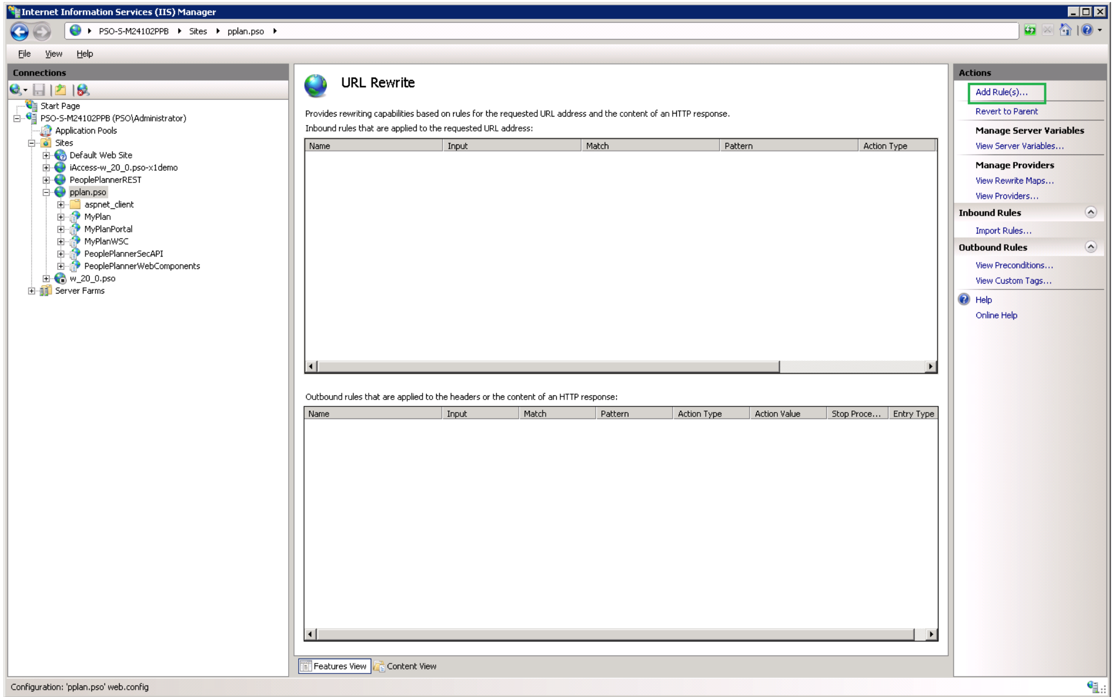
To clear the Server header:

1. Start the **Internet Information Services (IIS) Manager**.
2. Navigate to the **People Planner Web site**.
3. Click the **URL Rewrite** icon in **IIS Grouping**,

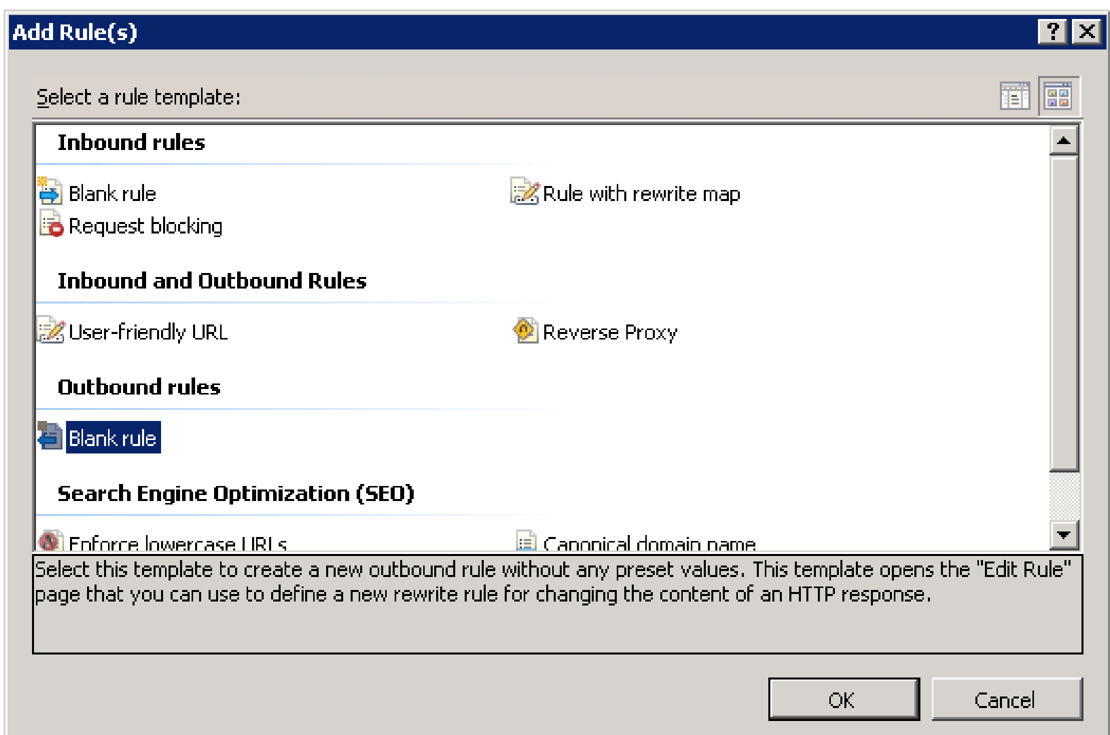


The URL Rewrite window opens.

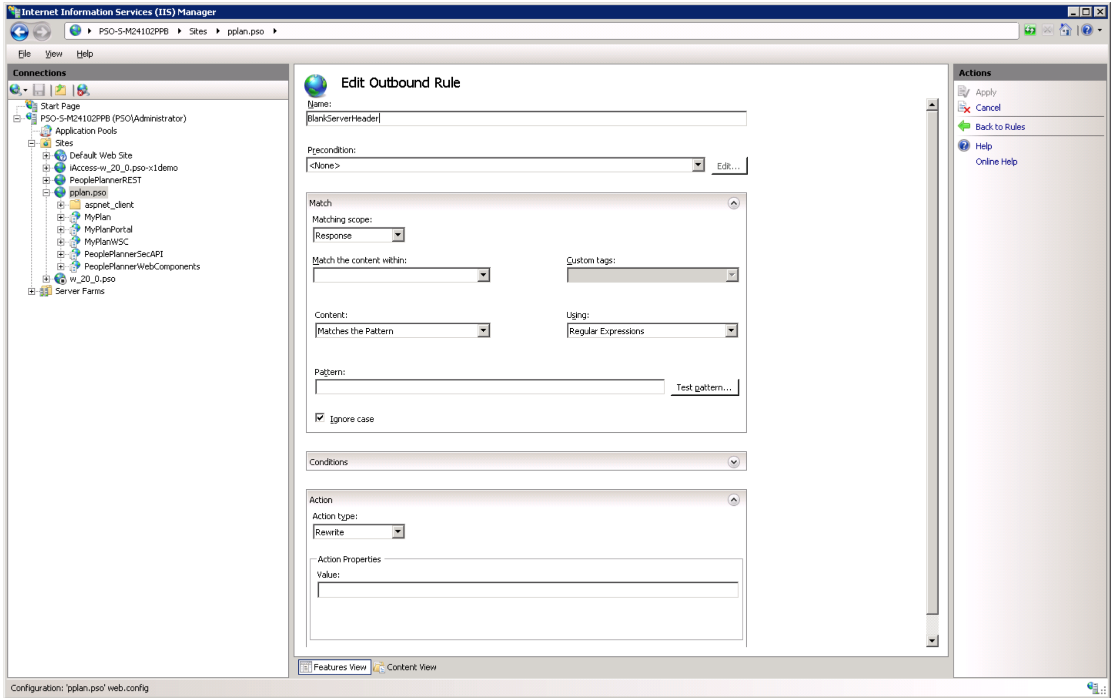
4. Click **Add Rule(s)…** on the right-hand side.



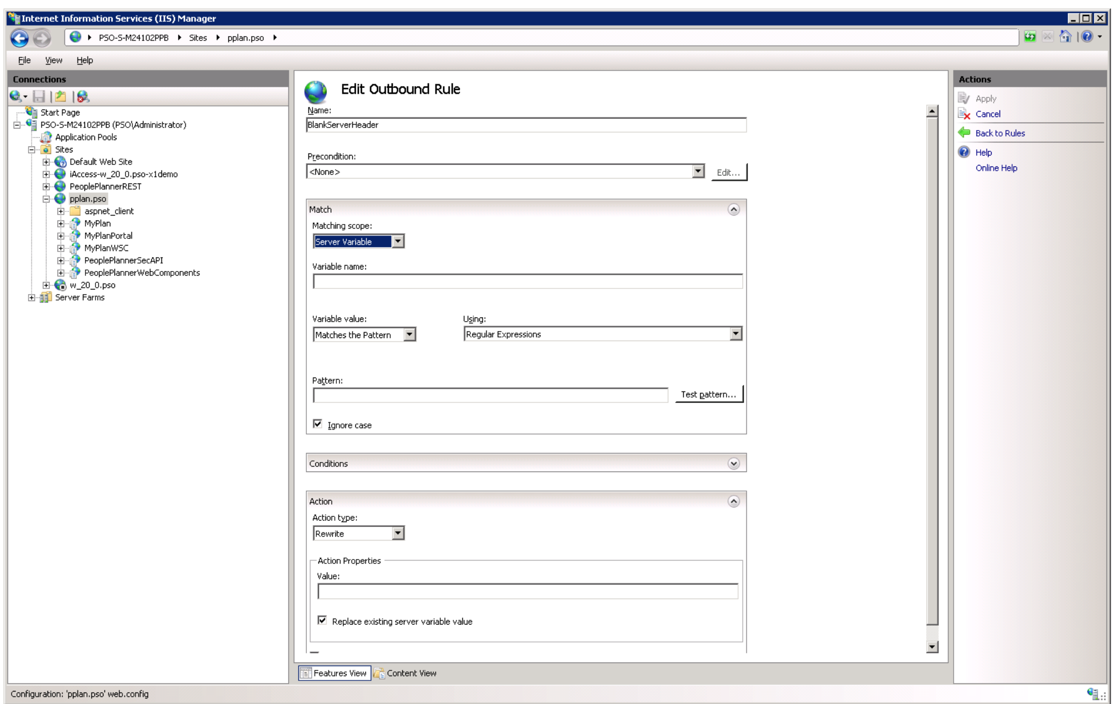
5. In the resulting **Add Rule(s) dialog**, under the **Outbound rules** section, click the **Blank rule** item and click **OK**.



The **Edit Outbound Rule** window opens.

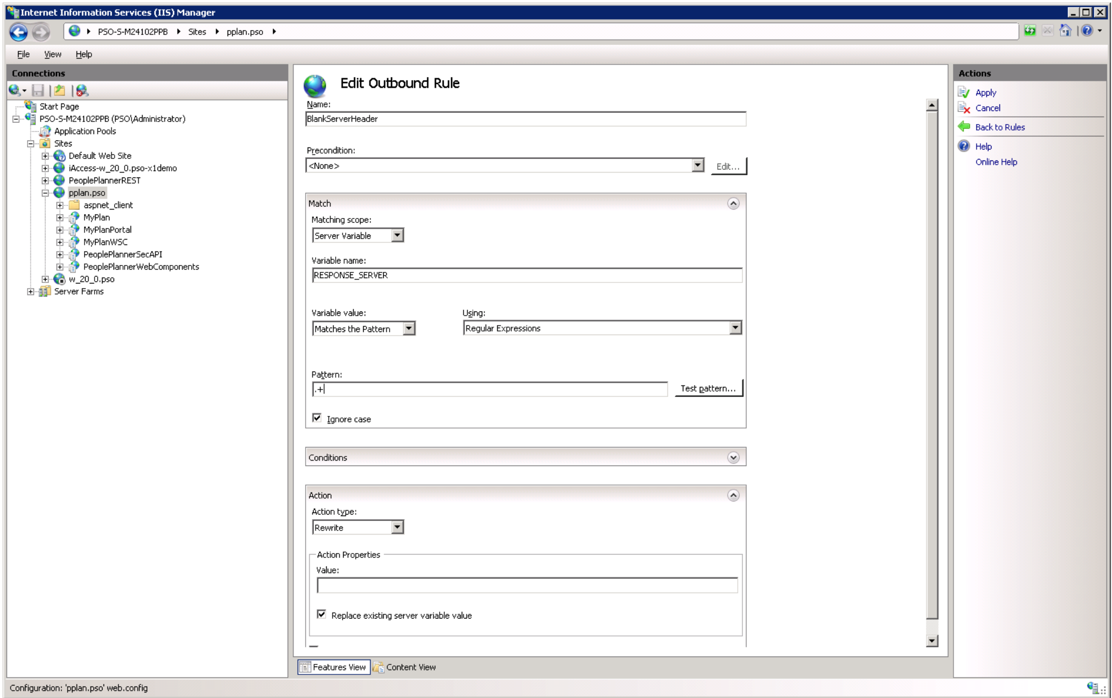


6. Enter a name for the outbound rule in the **Name** field.
7. In the **Match section**, change the **Matching scope** to **Server Variable**.

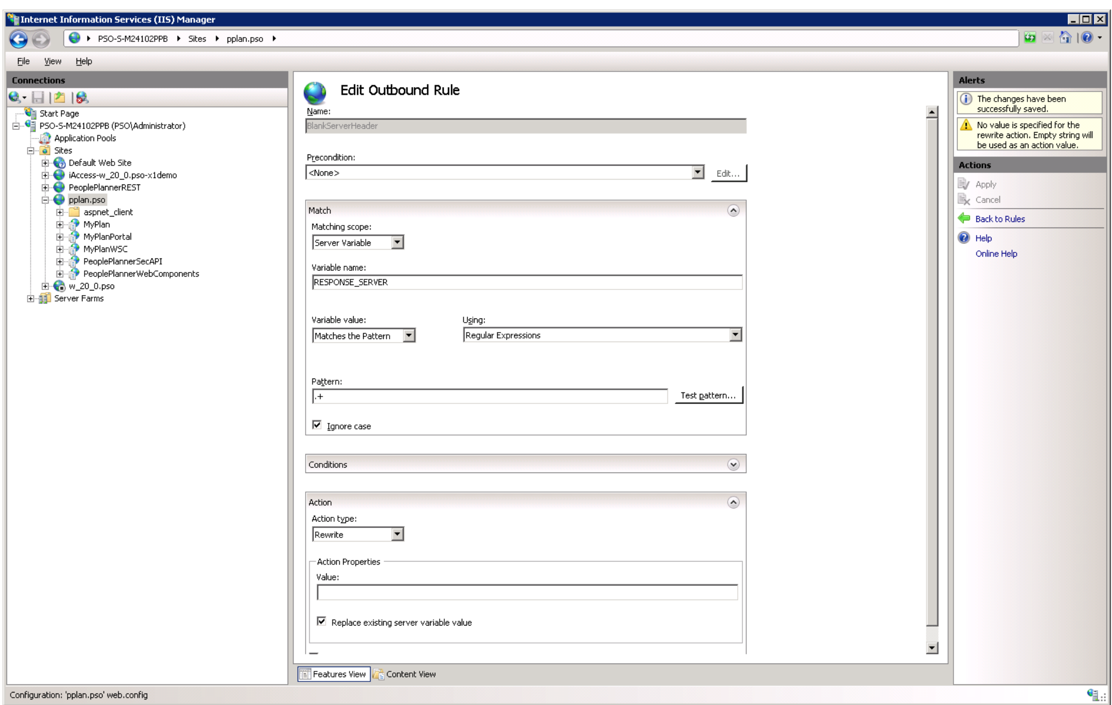


8. In the **Variable name** field, enter **RESPONSE_SERVER**.
9. In the **Variable value** field, select **Matches the Pattern**.
10. In the **Using** field, select **Regular Expressions**.

11. In the **Pattern** field, enter the **.+** pattern (a period followed by a plus character).



12. In the **Action section**, set the **Action type** field to **Rewrite**.
13. Leave the **Value** field blank.
14. Click **Apply** on the right-hand side.

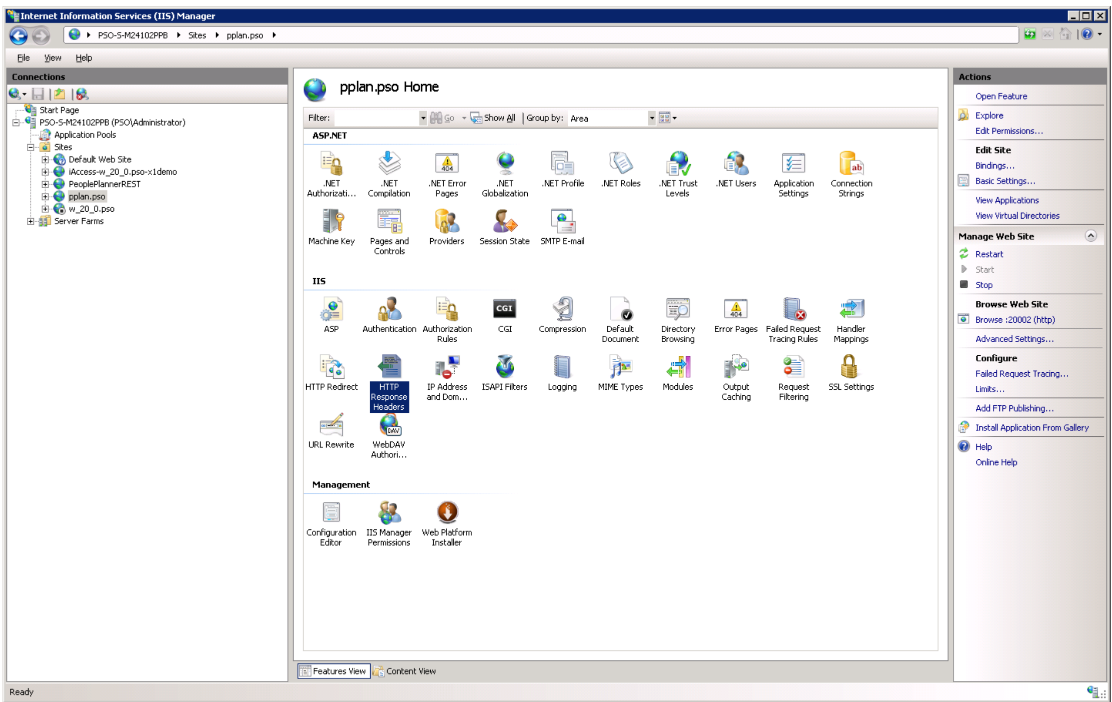


The X-Powered-By Header

The **X-Powered-By** header broadcasts that the application is based on ASP.NET. The browser does not require this information.

To remove the X-Powered-By header:

1. Start the **Internet Information Services (IIS) Manager**.
2. Navigate to the **People Planner Web site**.
3. Click the **HTTP Response Headers** icon in the **IIS grouping**.



4. Select the **X-Powered-By** header and click **Remove**.

Prevent Clickjacking and Dragjacking

By default, all web.config files now include the x-frame-options header with value SAMEORIGIN, which includes a safeguard to prevent them from being framed within another application to avoid clickjacking and dragjacking or confuse end users to perform unwanted actions.

For users running an older IIS, the web.config file for MyPlan and the People Planner Web Components includes this safeguard.

The following section is commented out by default, and you must comment it in yourself, as well as modify it to fit with your system:

```
<!--<add name="X-Frame-Options" value="ALLOW-FROM http://subdomain.domain.com" />-->
```

When updating from an older existing version of People Planner, this section does not necessarily exist, and you must then add it manually by adding the following to your site's web.config file.

```
<system.webServer>

   ...

      <httpProtocol>

         <customHeaders>

            <add name="X-Frame-Options" value="SAMEORIGIN" />

         </customHeaders>

      </httpProtocol>

   ...

</system.webServer>
```

For more information, see https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options

Hiding Error Information

Your system should reveal as little information as possible about itself to normal users.

When installing and configuring the People Planner Web Components in a production environment, you should set the following configuration parameters in the web.config file.

Custom Errors Configuration

Warning: The custom errors configuration should never be set to Off in a production environment.

Use either On or RemoteOnly in a production environment.

```
<customErrors mode="On"></customErrors>
```

For more information see https://msdn.microsoft.com/en-us/library/h0hfz6fc(v=vs.100).aspx

Service Account Privileges

The *Principle of Least Privilege* dictates that Windows services should run under a user account that has the least-set privileges that are required to perform the task. This applies to the People Planner Service as well.

The following process achieves this:

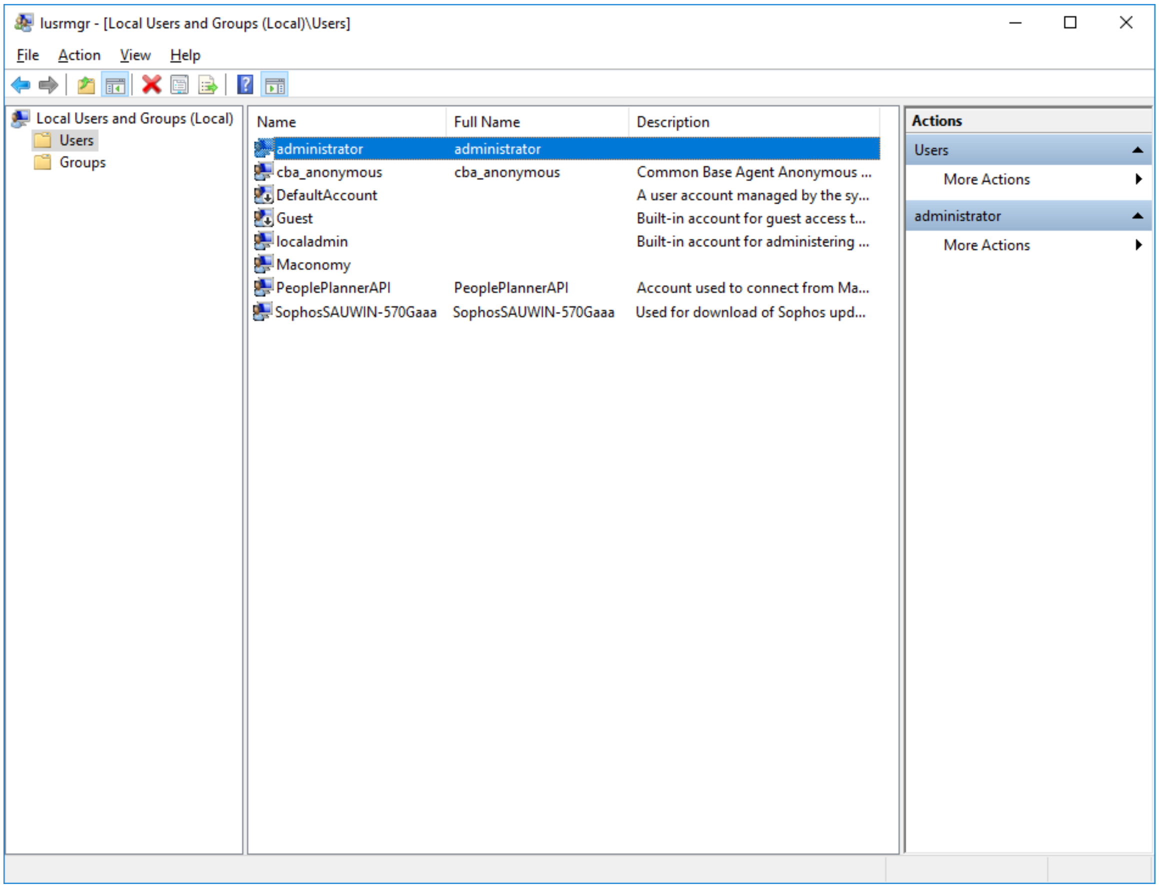
1. Create a local account on the server.
2. Give the account the necessary privileges to the directory where the People Planner Service is installed.
3. Give the account access to the People Planner database.
4. Add the account as a People Planner user.
5. Configure the People Planner service to run under the account.

Create a Local Account

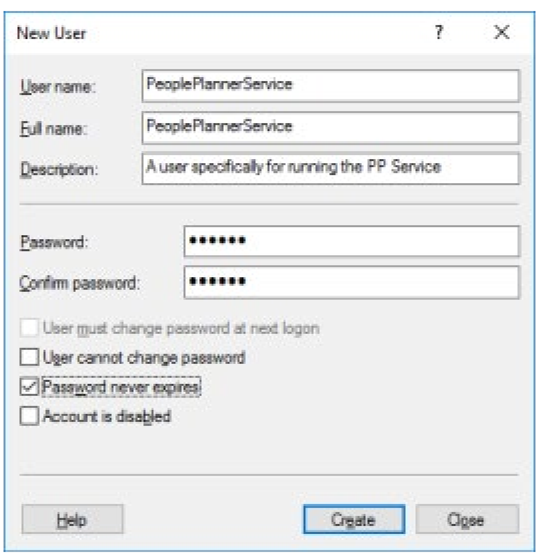
You can create an account either using the Windows Control Panel or by using the **lusrmgr** Microsoft Management Console snap-in.

To create a local account on the server:

1. Go to the Windows **Start** screen.
2. Type **lusrmgr.msc** in the **Run** dialog box to open the **Local Users and Groups** window.



3. Right-click on the **Users** node and select **New User**… to open the New User dialog box.



4. Enter a name for the user in the **User name** field and provide values for the remaining properties.

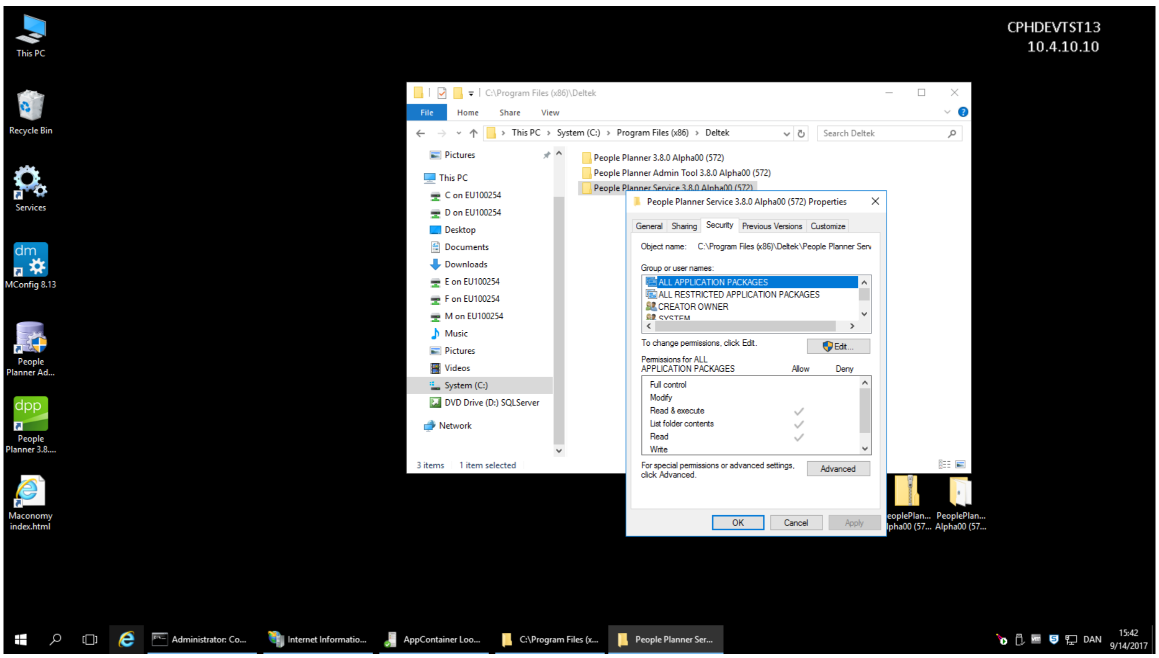
5. Make sure that the password that you enter fulfills the requirements for a strong password.
6. Click **Create**.

Note: By default, the new account is a member of the Users group. You can change this if needed. Right-click on the new account and click Properties and then edit it under the Member Of tab.

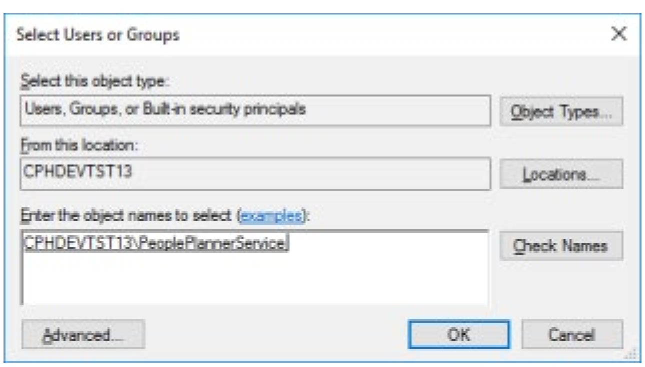
Assign People Planner Service Folder Privileges

To assign privileges to the People Planner Service folder:

1. Right-click on the folder where the People Planner Service is installed and click **Properties**.
2. Click the **Security** tab.



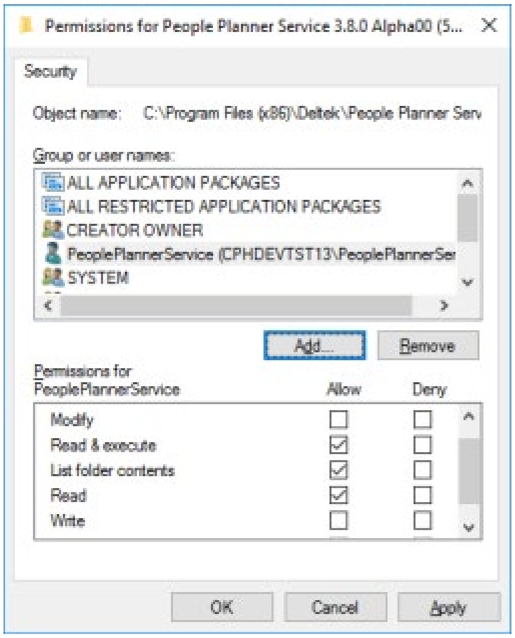
3. Click **Edit…**
4. Click **Add…**
5. Enter the name of the account, and Click **Check Names**.



6. Click **OK**.

7. Enable Read & Execute and Write permissions.

The account must have Read & Execute access to run the service, and it must have Write access to write to the log.



Note: The account also needs Read—and possibly Write—privileges to any other folder that it needs to read from, for example, when a scheduled task is set up to import data from a particular .csv file.

Add the Account as a People Planner User

You must add the account as an Admin user to People Planner. See Make the Account into a People Planner Admin User.

Configure the Service to Run Under the Account

To change the login for the People Planner Service:

1. Click **Start » Administrative Tools and Services**.
2. Right-click the **People Planner Service** and select **Properties**.
3. On the **Log On** tab, select the account and click **Ok**.
4. Right-click on the account and click **Start**.

Backup Procedures

People Planner does not include features for performing backups. You must establish a backup procedure using the tools that the database management system that you are using provides.

Appendix C: Securing the People Planner Security Service

The People Planner Security Service was introduced to lift the security when logging on to the People Planner Windows application.

To realize this security improvement, it is important that you install and configure the Security Service correctly. This section aims to describe how you can do this. It also covers some of the pitfalls you should be aware of, as well as various tips for troubleshooting an installation.

In the examples in this appendix, the Security Service – and the IIS – are installed on “Server01” (with the hostname “SERVER1”) and the Window application is installed on “win10”. The domain controller is the machine “DC1”, and the domain is pptest.com.

The Goal

You need to install the People Planner Security Service and the People Planner Windows application on machines in the same domain.

The Security Service is a web application, and you need to install it on an IIS. This is described in Install the People Planner Security Service.

The Security Service should be protected using SSL on the website, and it should not be possible to reach it using an http-url; only through an https-url.

You need to enable both Anonymous Authentication and Windows Authentication for the website. Furthermore, the website should be configured for using Negotiate and it should be able to use Kerberos instead of NTML.

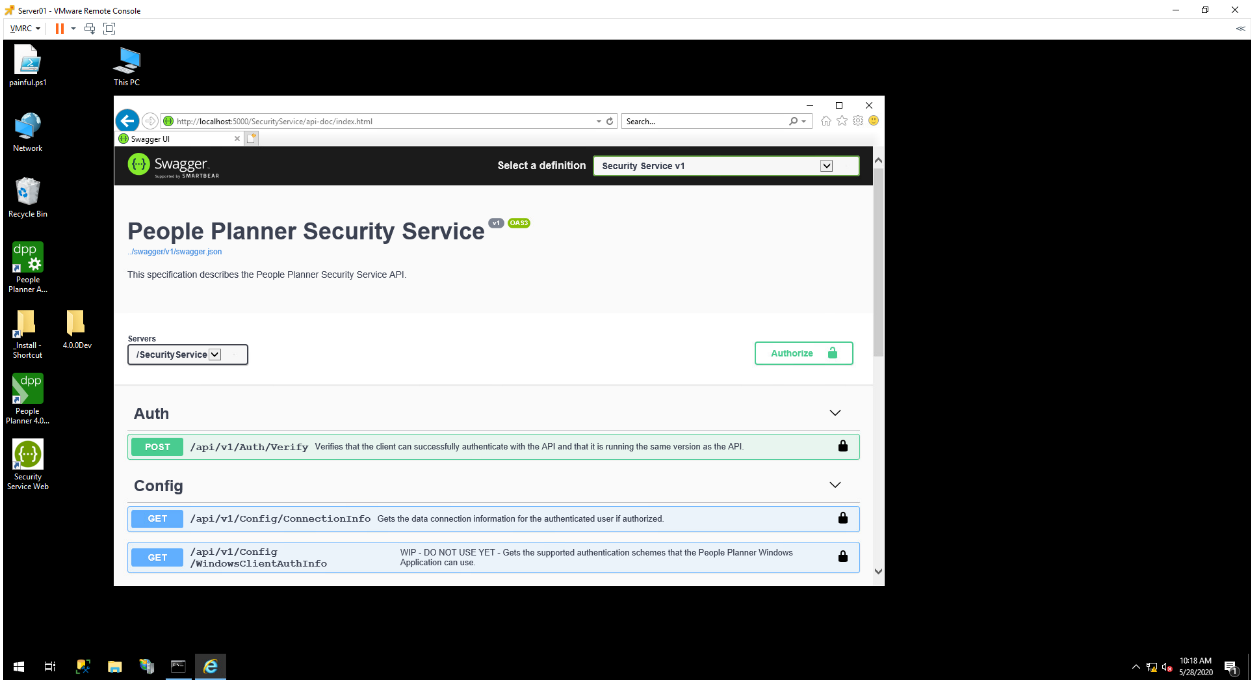
Normally most of this is set up automatically with the installation of the Security Service, and you do not have to worry about it. This section is intended for when something goes wrong.

Basic Verification

After having installed the software, and before setting up the security, it can be useful to first verify that the Windows Security Service works in the basic installation.

Swagger-documentation

One way to verify the installation of the People Planner Security Service – and independent from everything else – is to open its Swagger-documentation in a browser on the server.



The URL for the Swagger-documentation should look like:

http://localhost:5000/SecurityService/api-doc/index.html

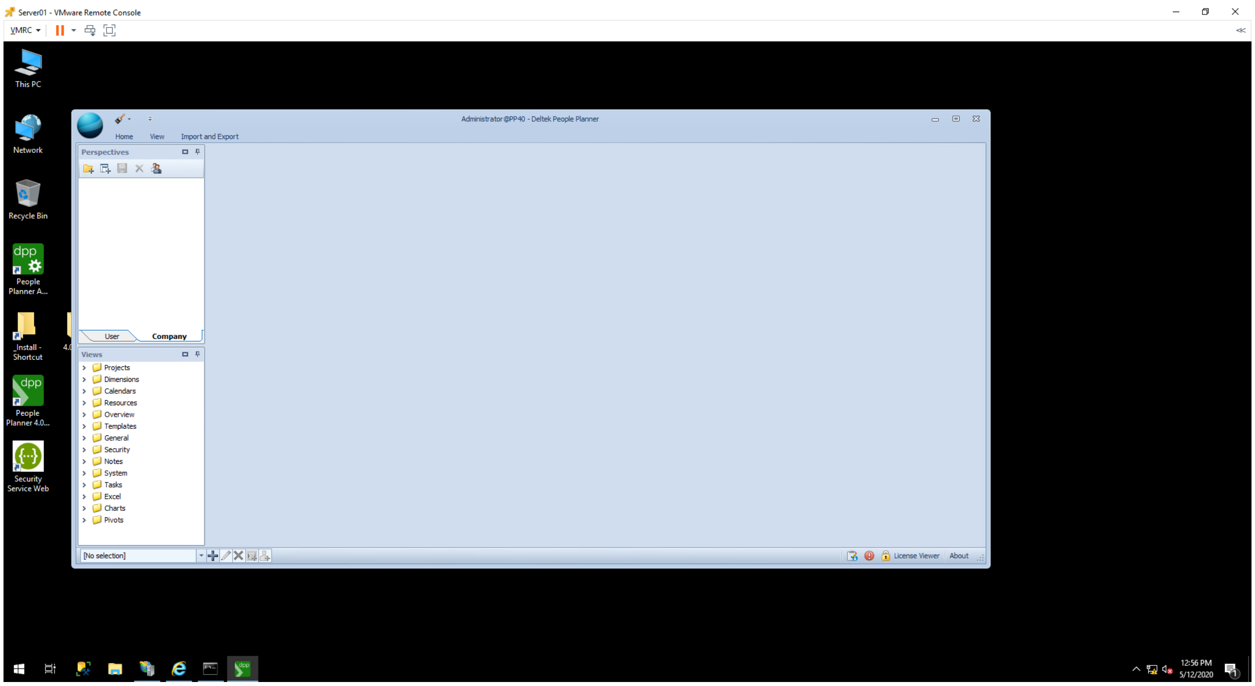
You should use the port that you installed the Security Service under – and since we have not yet configured for SSL – the scheme should be http, not https.

If the Swagger-documentation displays successfully, it can be taken as an indication that the Security Service is correctly installed.

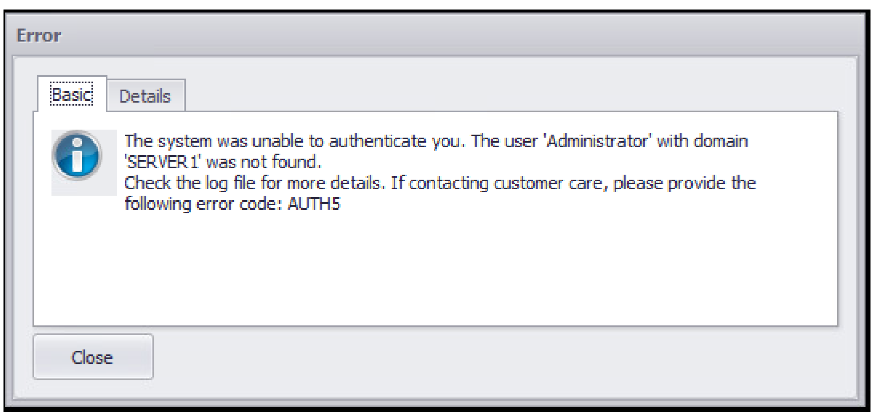
Run a People Planner Windows Application on the Same Machine

The most basic way to verify if the Windows Security Service is working correct is to try to call it from a People Planner Windows application installed on the same machine as the Security Service.

When you start the Windows application, you should either see the Windows application open successfully.



Or, if you have not added the local user to the People Planner database, you will instead receive an error message from People Planner stating that it could not authenticate the user.



Both cases are suitable for our purpose; they prove that there is access through to the Security Service and that it works correctly.

Note: If you want to see the Windows application open, you can use the People Planner Admin Tool to add the user to the People Planner database.

Possible Conflict with Maconomy

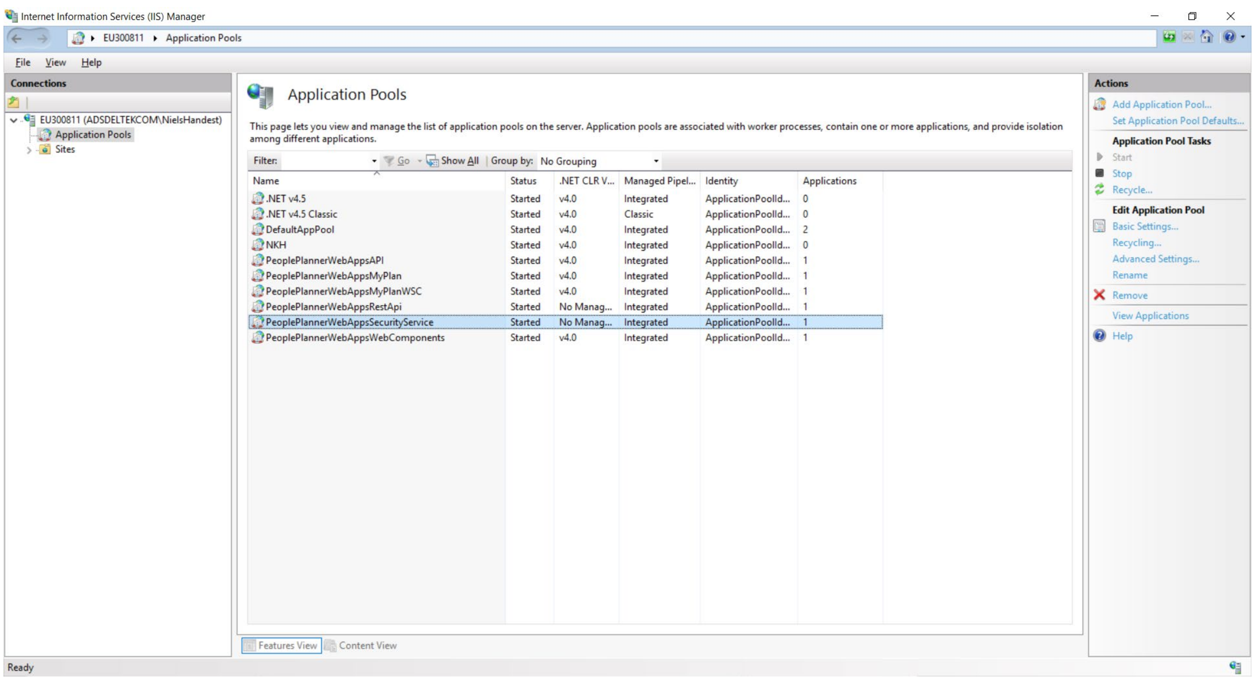
If you are unable to view the Swagger documentation or run a People Planner Windows Application as described above, a possible explanation is that there may be a conflict with Maconomy.

If Maconomy is configured to use SPNEGO and Kerberos, it may be configured so that the account it is running under has taken over the SPN (Server Principal Name) that the Security Service was expecting to use. The SPN is therefore no longer free to the account the Security Service is normally running under.

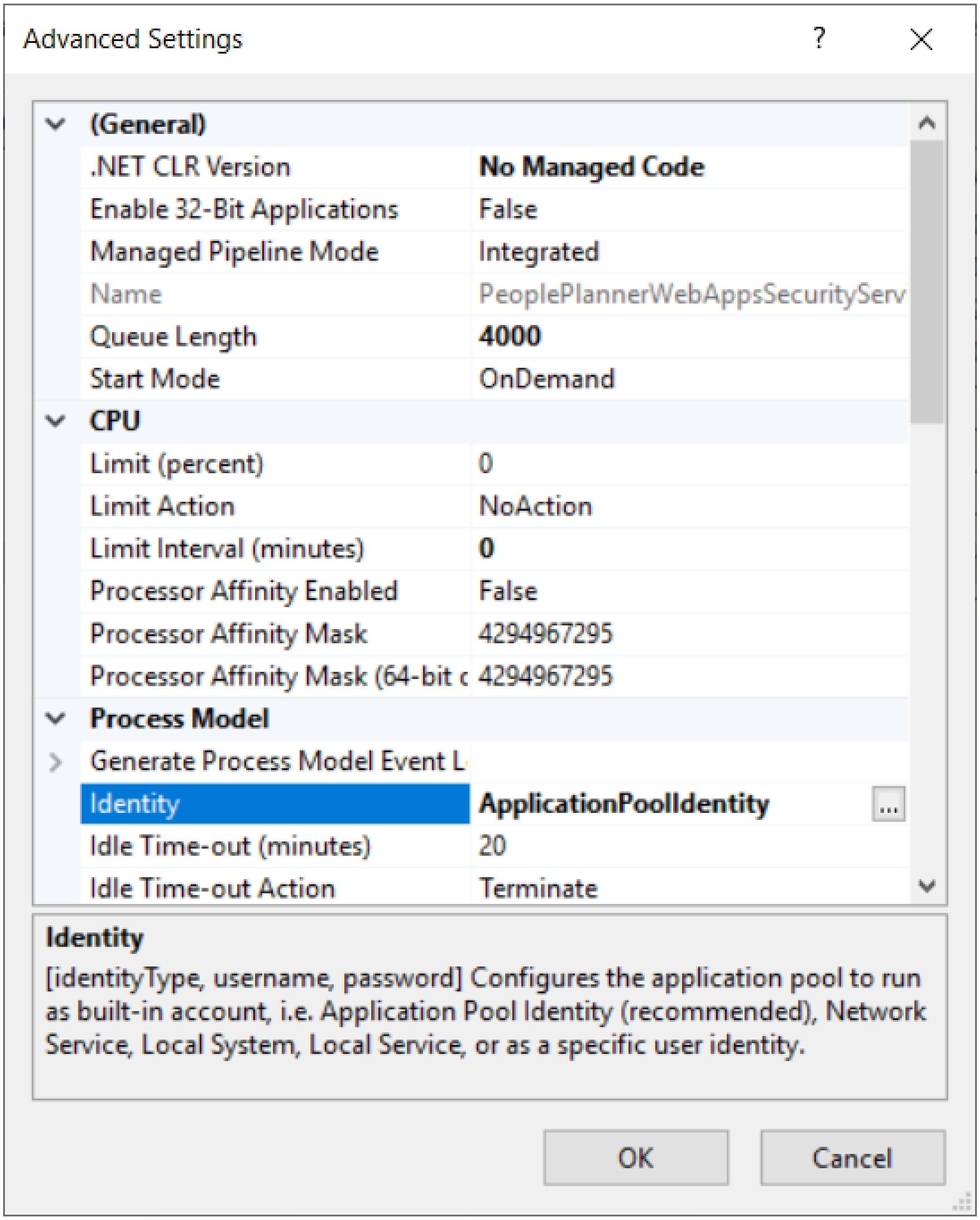
> **Note:** Refer to the *Deltek Maconomy System Admin Guide* for further details on the Maconomy SPNEGO and Kerberos configuration. For more information about SPN, please see section Kerberos Authentication below.

To resolve the conflict with Maconomy:

1. Reconfigure the Application Pool of the People Planner Security Service to use the same account that Maconomy is using.
2. Open the IIS Manager, and select the Application Pool of the Security Service:

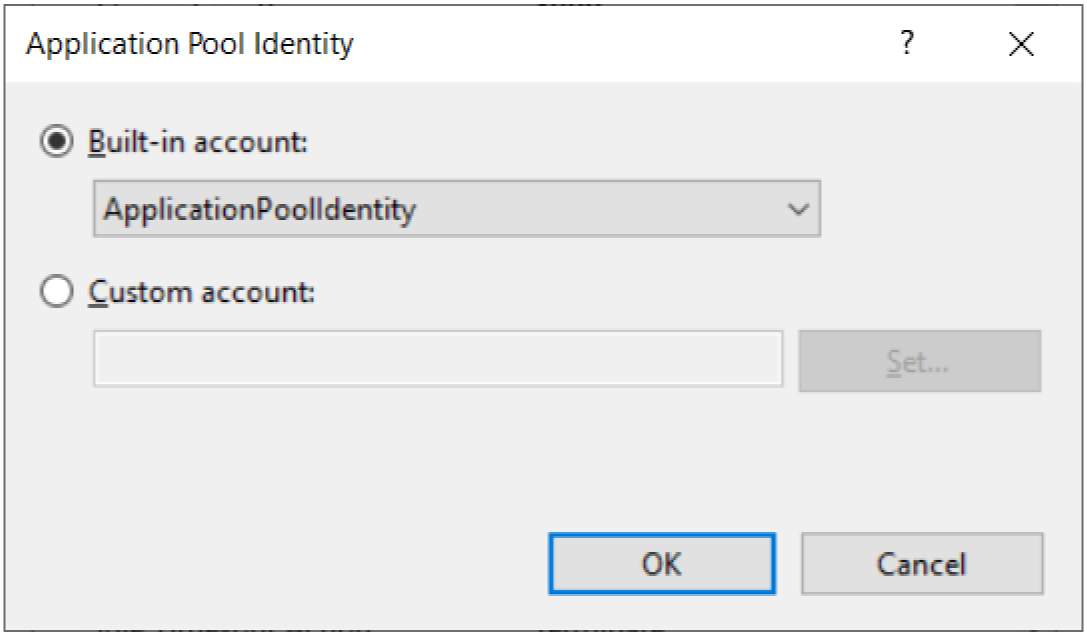


3. Select **Advanced Settings**, and scroll to where the **Identity** is defined:

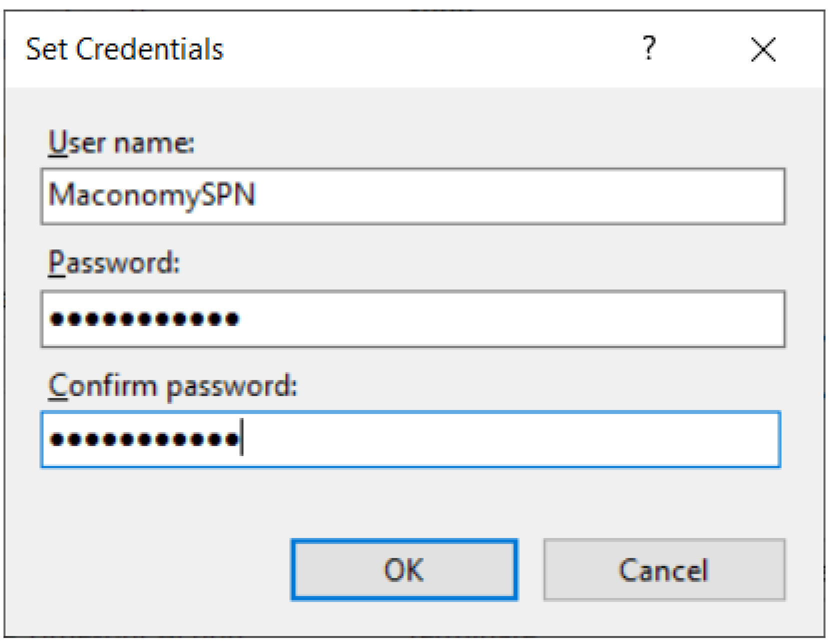


Note: The Identity is the account under which the Application Pool is running.

4. Change the Identity to the account that Maconomy has created. Select the Identity, and click the "…" button to configure the Identity:



5. Select **Custom Account**, and click the **Set**.
6. In the Set Credentials dialog, fill in the credentials of the account Maconomy is using and click **OK**.



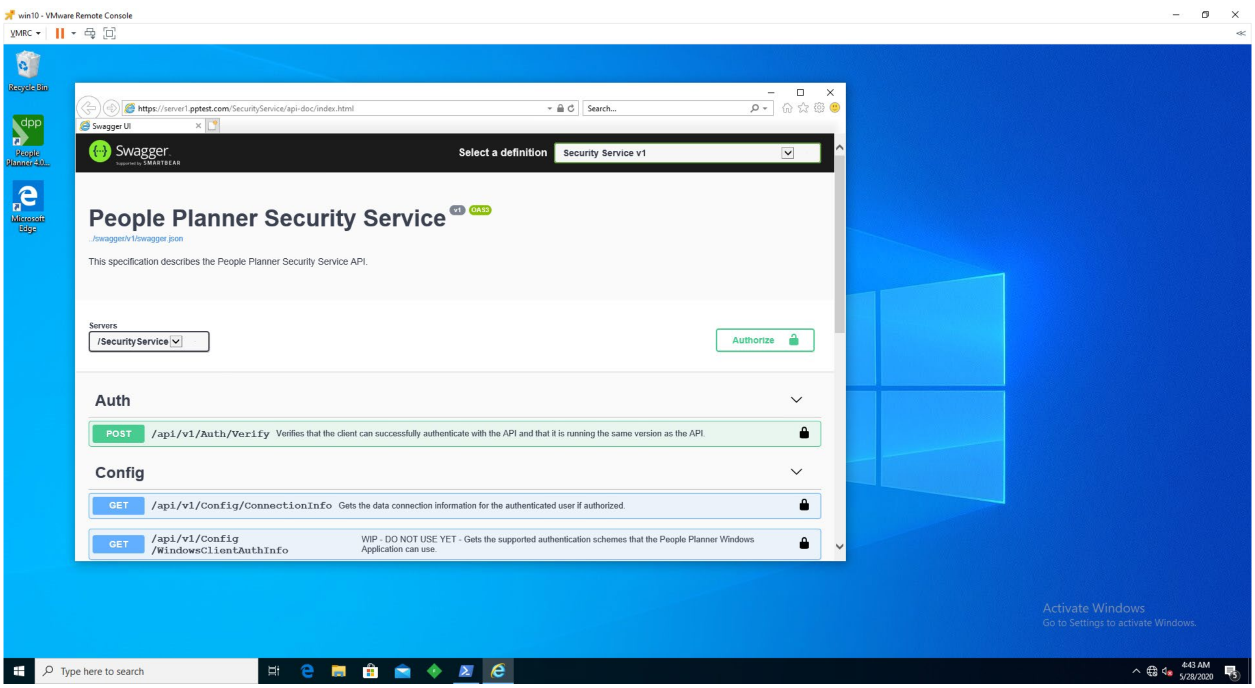
Network Connection

When running the People Planner Windows application on a separate machine from the one with the People Planner Security Service, there has to be a network-connection between the two machines.

To avoid unnecessary complexity to the situation – and since you have still not configured the web site for SSL – you can start by verifying this for http. Later when you have added SSL, you should repeat the verification for https.

Swagger Documentation

If the machine with the People Planner Windows application can reach the server with the People Planner Security Service, it should be possible to open the Swagger-documentation.



The URL for the Swagger-documentation should look like:

http://server1.pptest.com:5000/SecurityService/api-doc/index.html

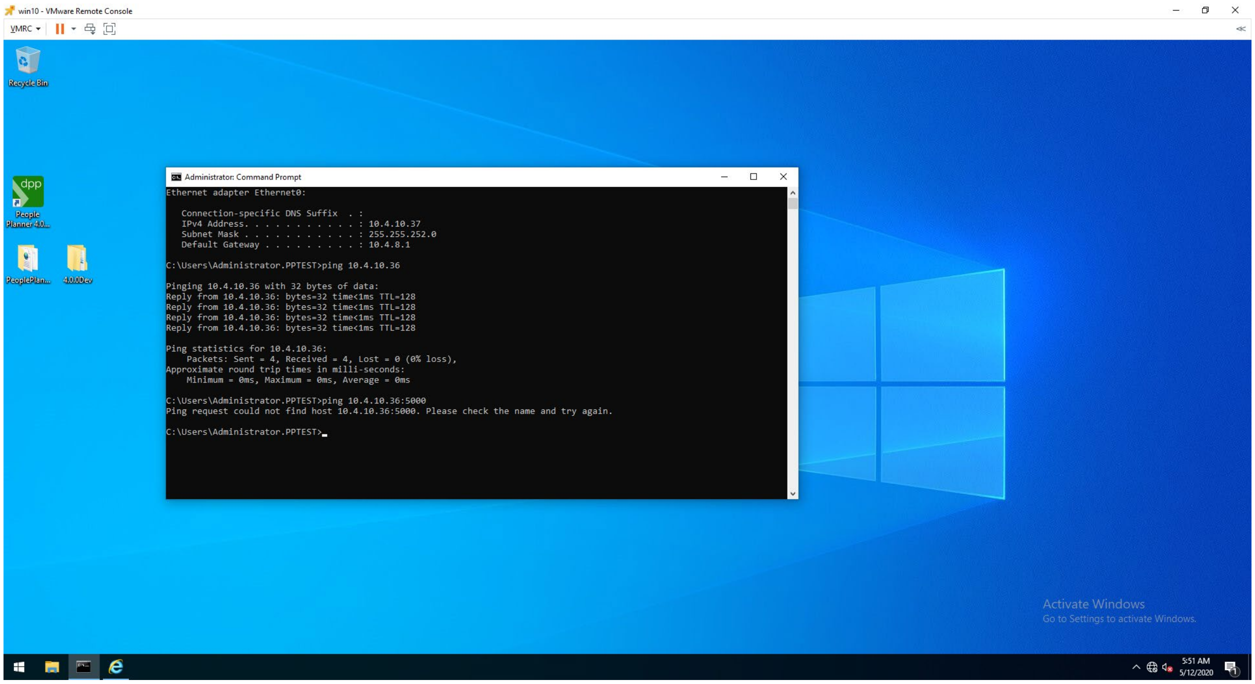
You should here use the port that you installed the Security Service under, and the scheme should be http, not https. Either the server name should be the fully qualified domain name (FQDN) of the server, or alternatively you can use the IP-address.

> **Note:** If the IP works, but the FQDN do not, there is most likely something wrong with the DNS setup of the network.

Check the Network Connection

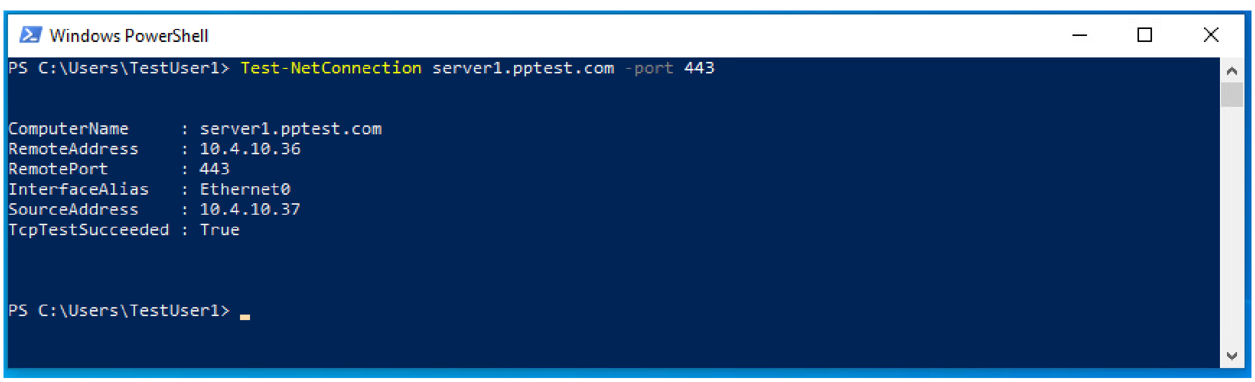
One way to verify that there is a network connection from the machine with the People Planner Windows application to the People Planner Security Service is with the ping-command.

If you cannot access the Swagger documentation as mentioned in the previous section, the following steps can be used to further analyze the issue.



> **Note:** For security reasons, ping – or more specifically, Internet Control Message Protocol (ICMP) echo requests – may have been disabled for the server and so this is not necessarily a sure test.

Another way is to start a Windows PowerShell and run the Test-NetConnection command.



Firewall

If the People Planner Windows application is unable to reach the server with the People Planner Security Service, a possible reason could be that the firewall does not allow it. This section describes how to configure the firewall.

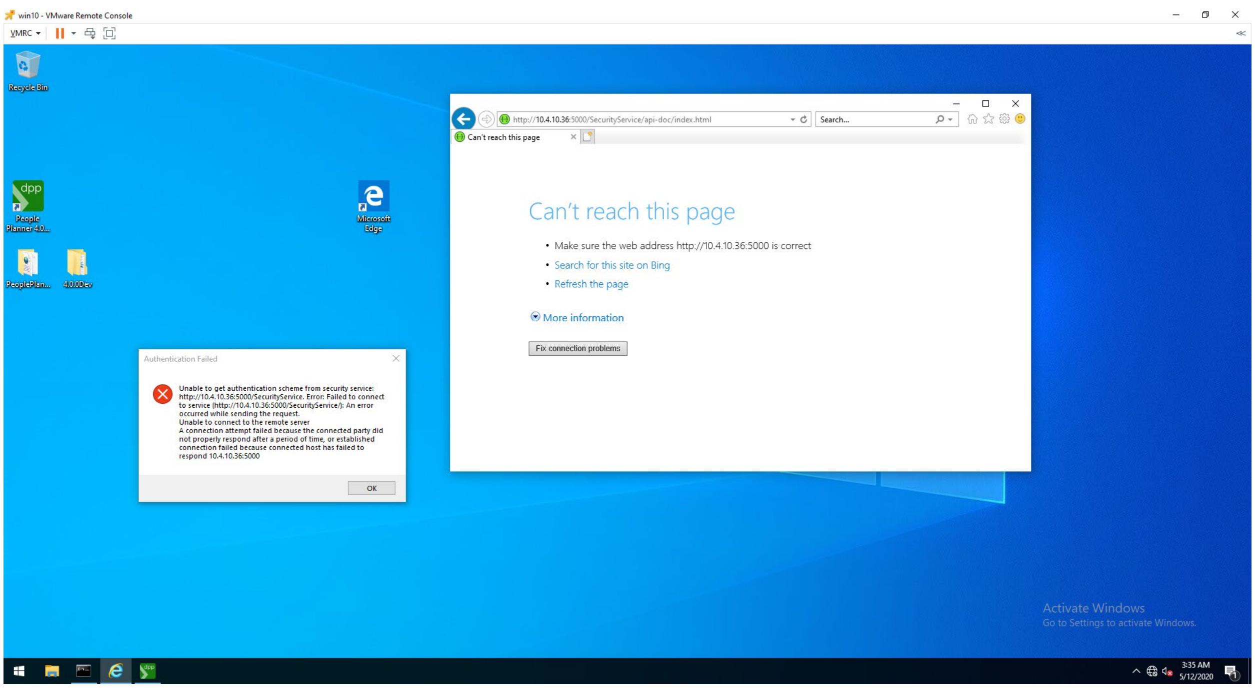
> **Note:** Depending on how the network is organized, there might be more than one firewall between the Windows application and the Security Service. If that is the case, the discussion below apply to each of the firewalls. The text assumes that there is only a single firewall – the one on the machine with the Security Service.

The firewall – on the server with Security Service and the IIS – must be open for the incoming calls from the People Planner Windows application to the Security Service. If it is not open, any calls will be stopped before they even reaches the IIS.

Symptoms of this happening:

1. The Windows application authentication fails with an error: Unable to connect to the remote server.
2. It is not possible to view the Swagger-documentation of the Security Service in a browser.
3. There are no log-entries, status 401 or otherwise, in the IIS-log.

   > **Note:** You might need to flush the IIS cache to be 100% certain that the IIS has written everything from memory to the log-file: netsh http flush logbuffer.



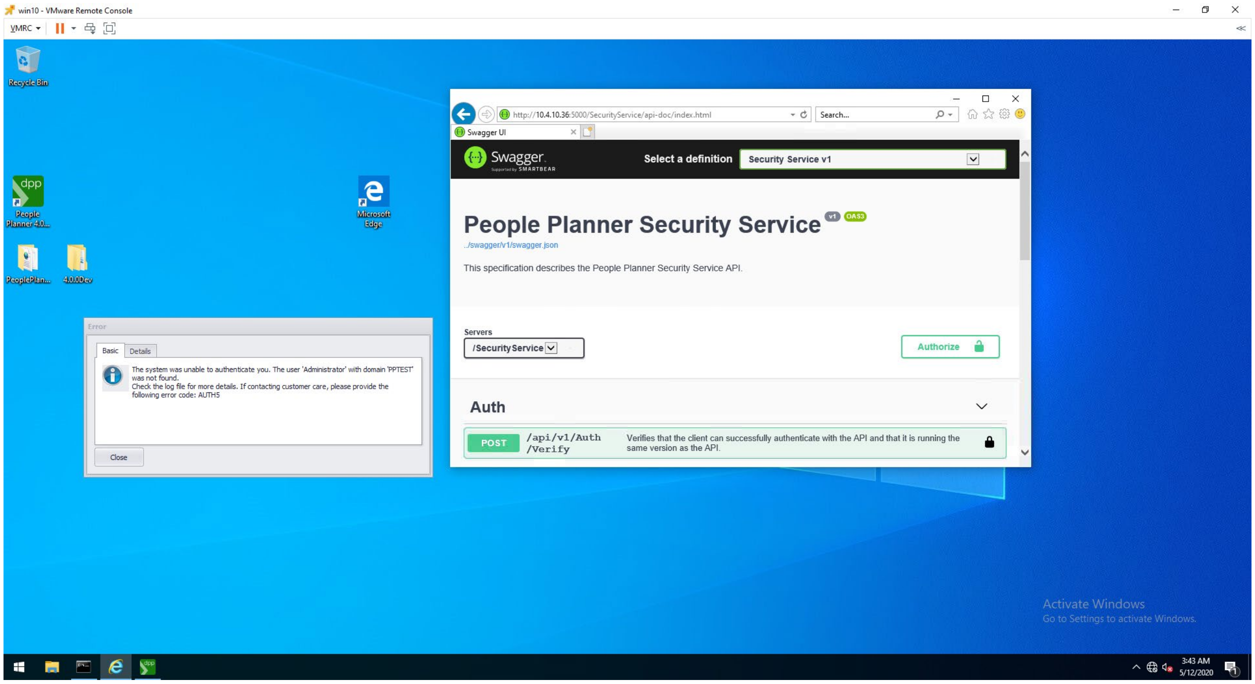
Turn Off the Firewall

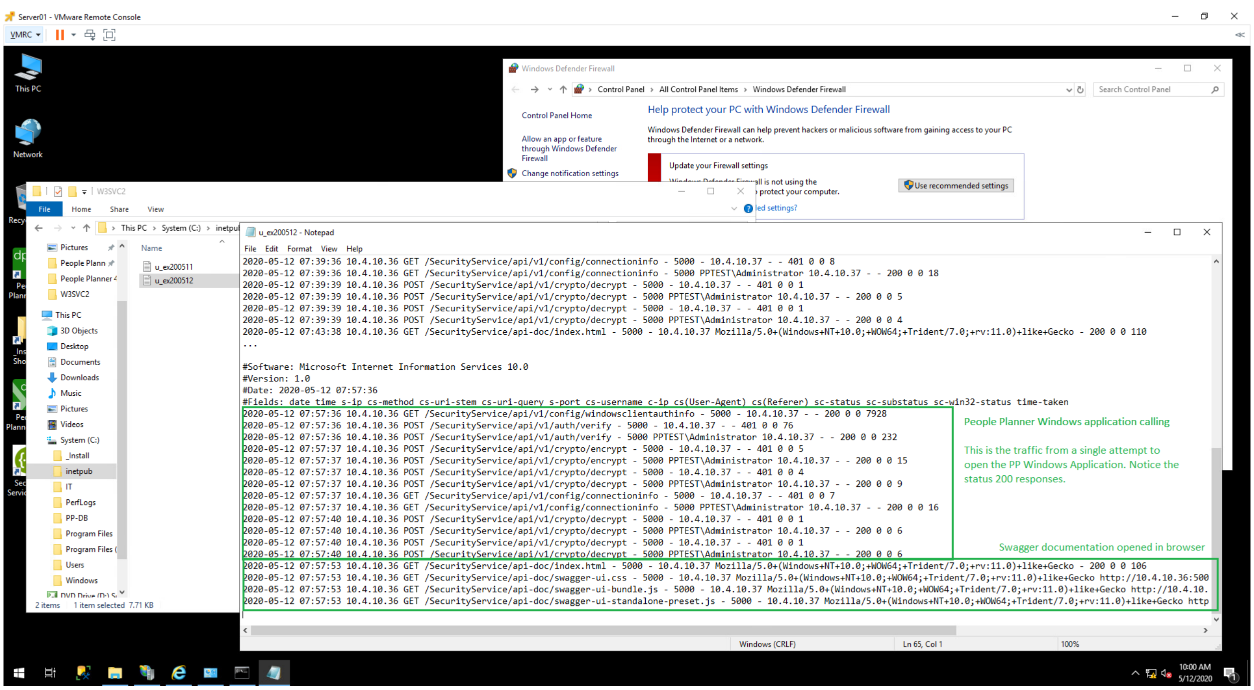
To verify if it is the firewall-settings that are the issue, you can temporarily turn the firewall off.

If you turn the firewall completely off, there should be some kind of connection through:

1. The Windows application might still fail to authenticate the user, but the error should be a People Planner-related error message, and not a network error.
2. The Swagger-documentation should be accessible from a browser,

3. There should be log-entries in the IIS-log, and which documents some level of HTTP-traffic between the Windows application and the IIS.





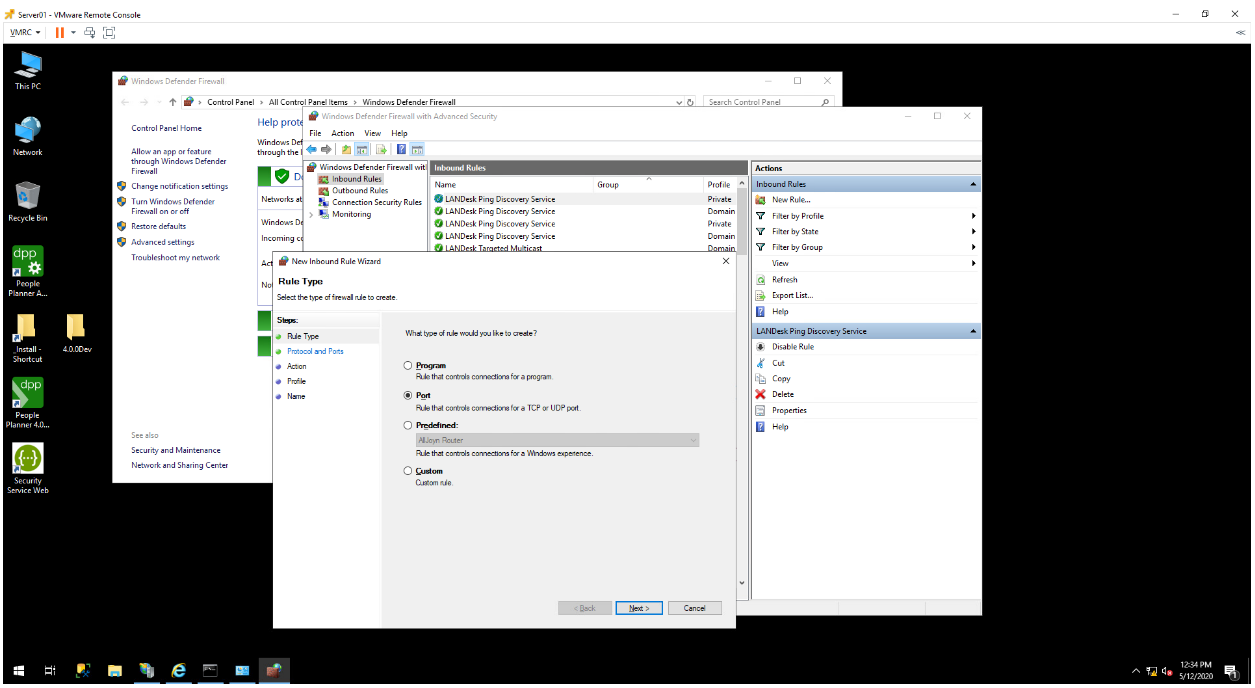
Create an Inbound Rule in the Firewall

Instead of turning the firewall off entirely, you only need to create an Inbound Rule.

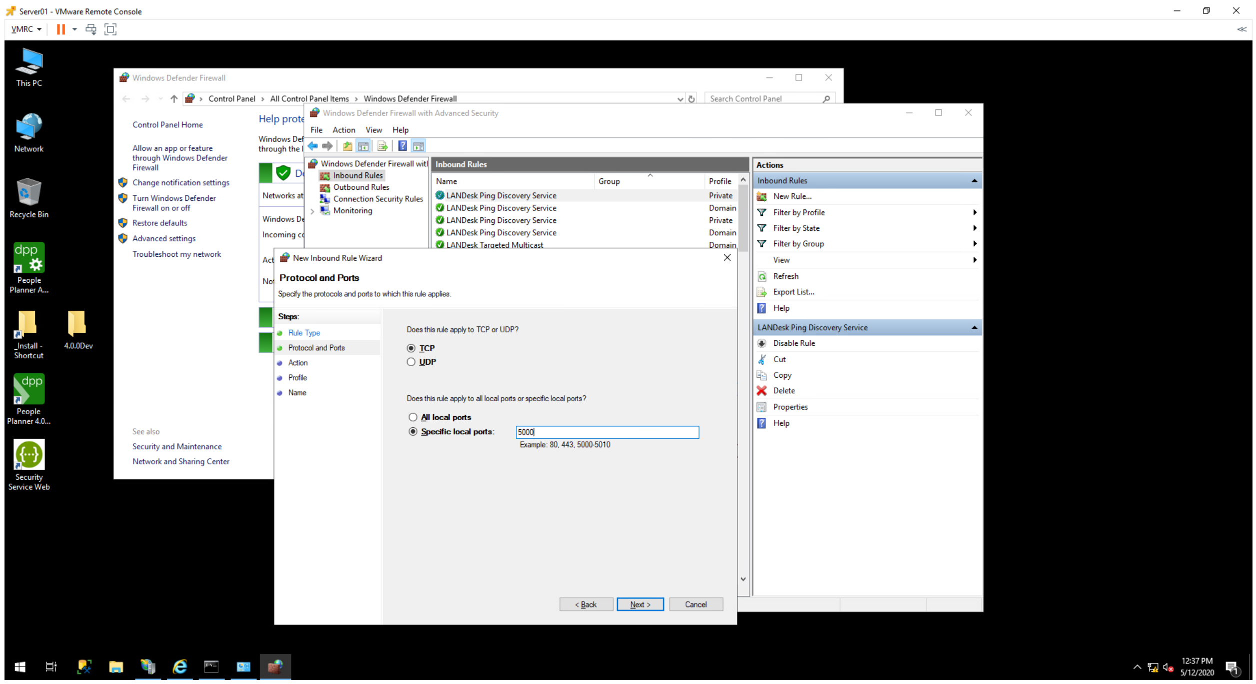
> **Note:** In this documentation, we assume that the firewall is the built-in Windows Defender Firewall. The procedure should be similar for other firewalls.

In this example, we have installed the People Planner Security Service using port 5000, and you need to open for traffic on this port in the firewall.

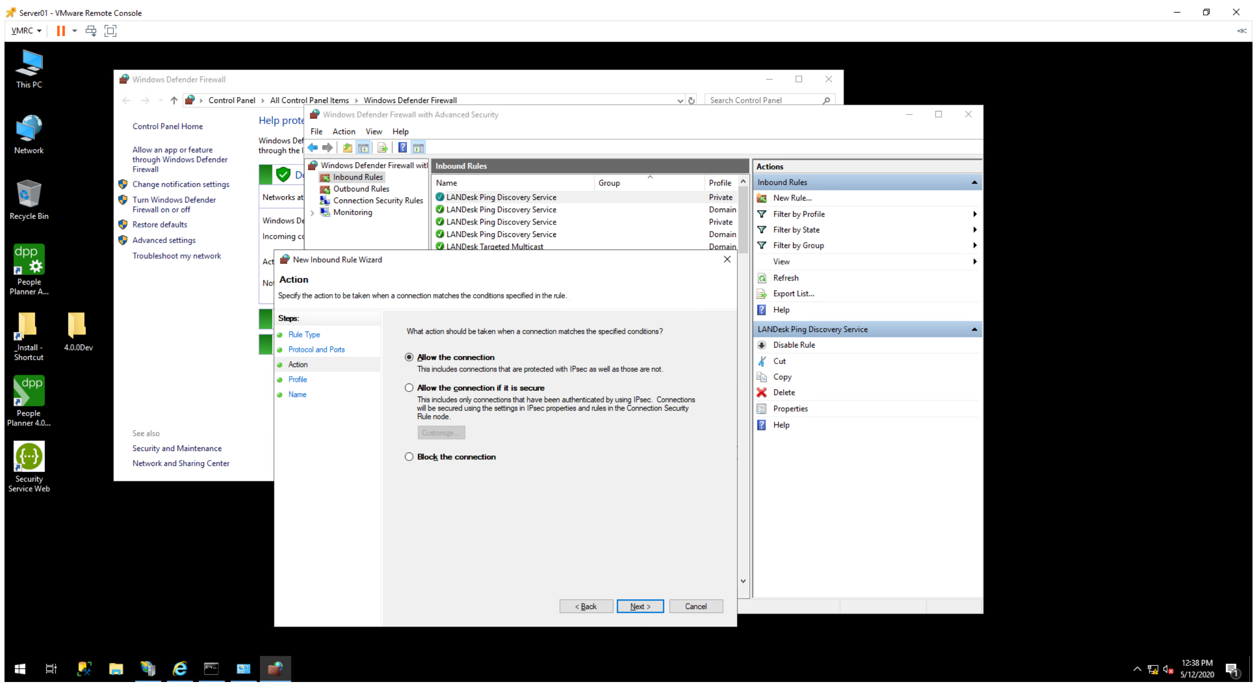
1. Open the Windows Defender Firewall.
2. Select **Advanced Settings**.
3. Select **Inbound Rules**, and then create a **New Rule…**.
4. This opens the New Inbound Rule Wizard. In the wizard, select the radio-button for **Port** and press **Next**.



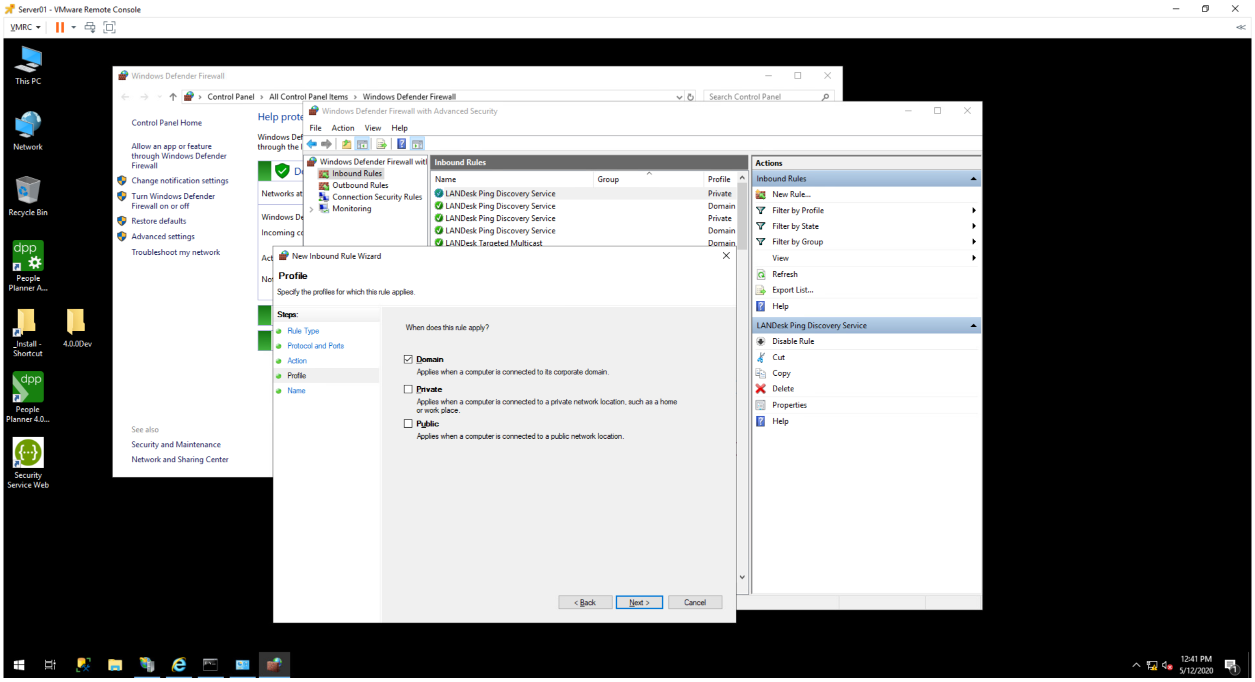
5. Select **TCP** and **Specific local ports**, and set the port to 5000.



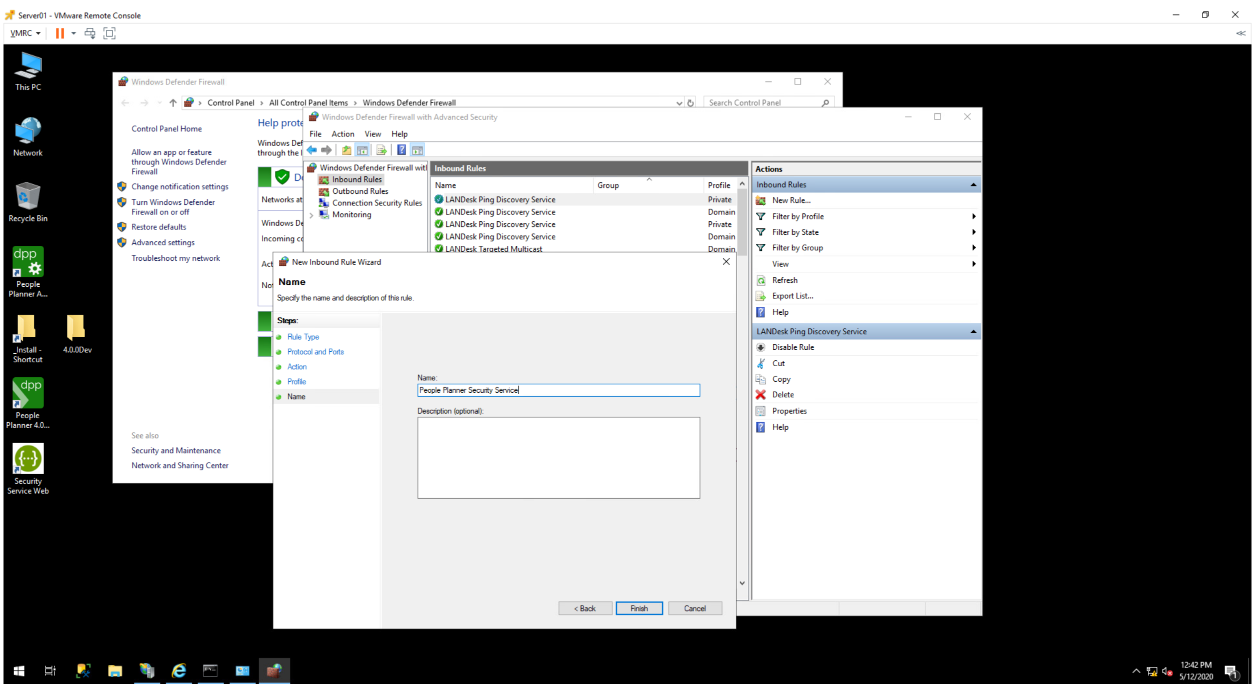
6. Select Allow the connection, and press Next.



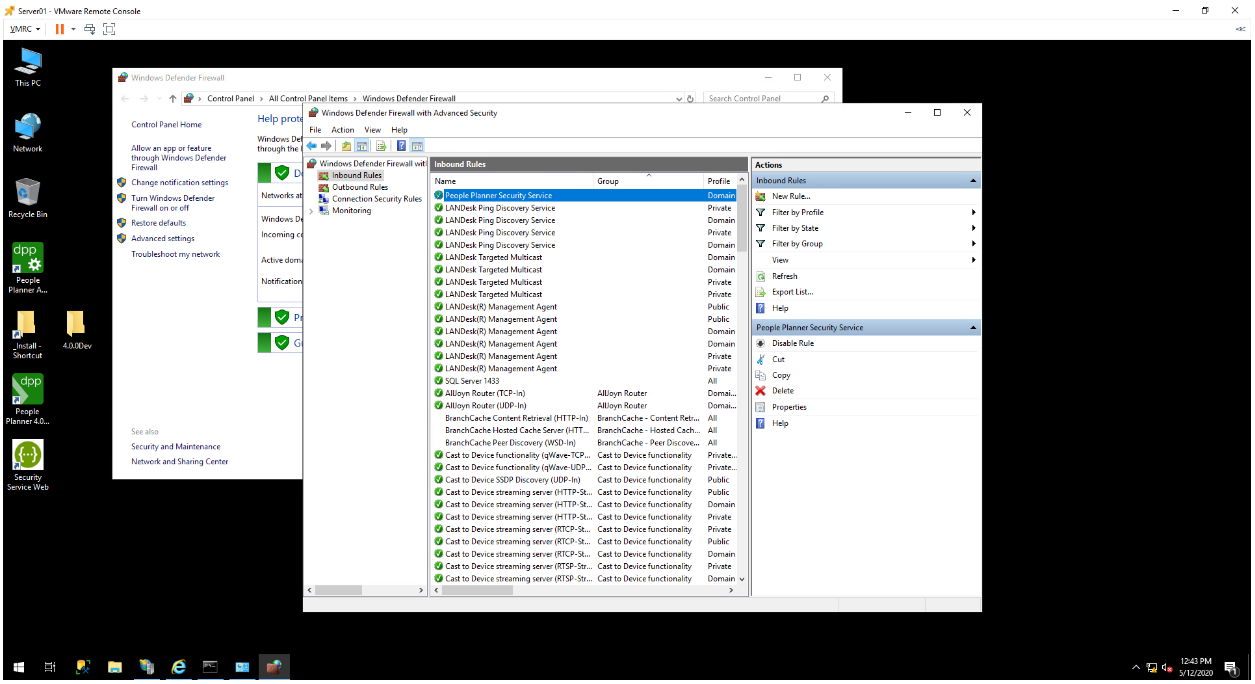
7. Select the rule to apply for **Domain** only, and press **Next**.



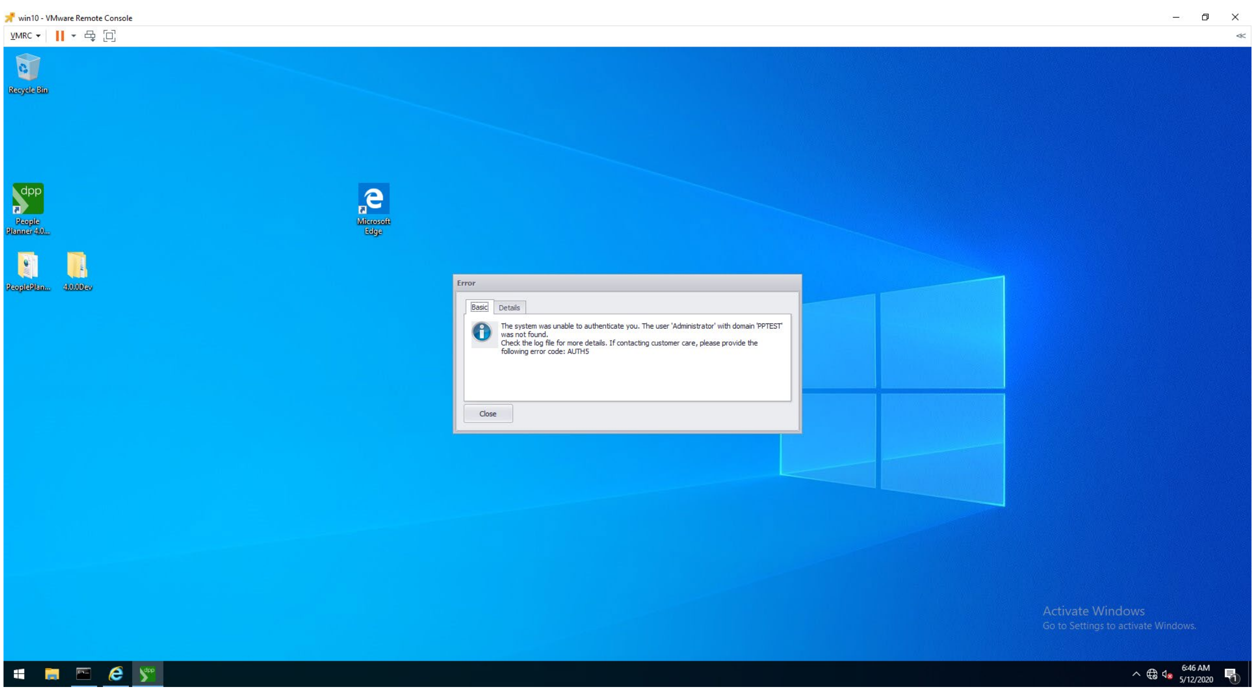
8. Finally, give the inbound rule a descriptive name, and press **Finish** to save the rule.



The rule should be in the list of **Inbound Rules**.



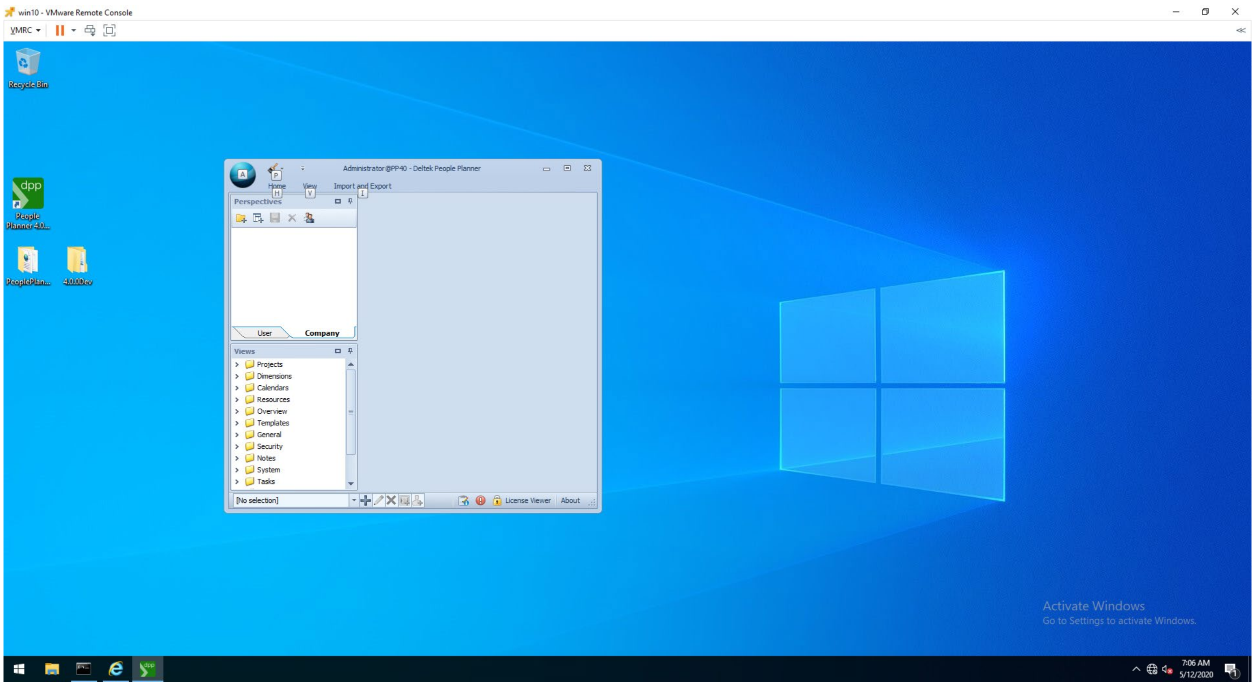
If everything is set up correctly, the People Planner Windows application should behave as when the firewall is disabled.



Add a People Planner User

Unless you have already added the local user – that you are logged in with on the client machine – to the People Planner database, you will get an error message informing you that it could not authenticate the user. That is fine; this is People Planner telling you that it cannot find the user in the database. It proves that there is a connection through to People Planner.

If you want to see the People Planner Windows application open, you can add the login-user to the users in the People Planner database. However, this is not a requirement.



Note: On a new installation, the People Planner window is empty because there is no data in the database at this time. If you are updating from a previous version, data is available in this window.

Set Up the People Planner Security Service for Using SSL

It is important that the People Planner Security Service is configured for using SSL (such as HTTPS) and not respond to HTTP – or else it does not provide any additional security as intended!

Note: You do not necessarily need to disable HTTP-traffic. It is sufficient to not allow it through the firewall.

For SSL to work, you need to install a SSL certificate. On a production system, this should be a certificate signed by a certificate authority (CA).

Note: You should also remember to setup a policy for renewing the SSL certificate before it expires, or the People Planner Windows application will not be able to login.

If you do not have a CA-signed certificate ready, you can go ahead and instead do the setup using a **self-signed certificate**. You can then later swap it with a proper SSL certificate.

A SSL certificate provides security on two fronts:

- It encrypts the network traffic between the client and the server.
- It acts as a guarantee that the client can trust that server is whom it claims to be.

Everyone can create self-signed certificate, and because of this, a self-signed does not add any security to the client that the server are whom the SSL certificate claim it to be.

Create and Install a Self-Signed Certificate

The steps to create and install a self-signed certificate are:

Server:

- Create the certificate.
- Export the certificate to a pfx- and a cer-file.
- Import the pfx- and cer-files into the certificate-store on the server.

Client:

- Copy the cer-file to the client, and install it – telling the client to trust the self-signed certificate.

First, we will cover the server-part of this, and in a later section, we will do the client-part.

To create a self-signed certificate, we can use PowerShell ISE to write a script that does this. The script should be run on the machine where the Security Service is running.

The script:

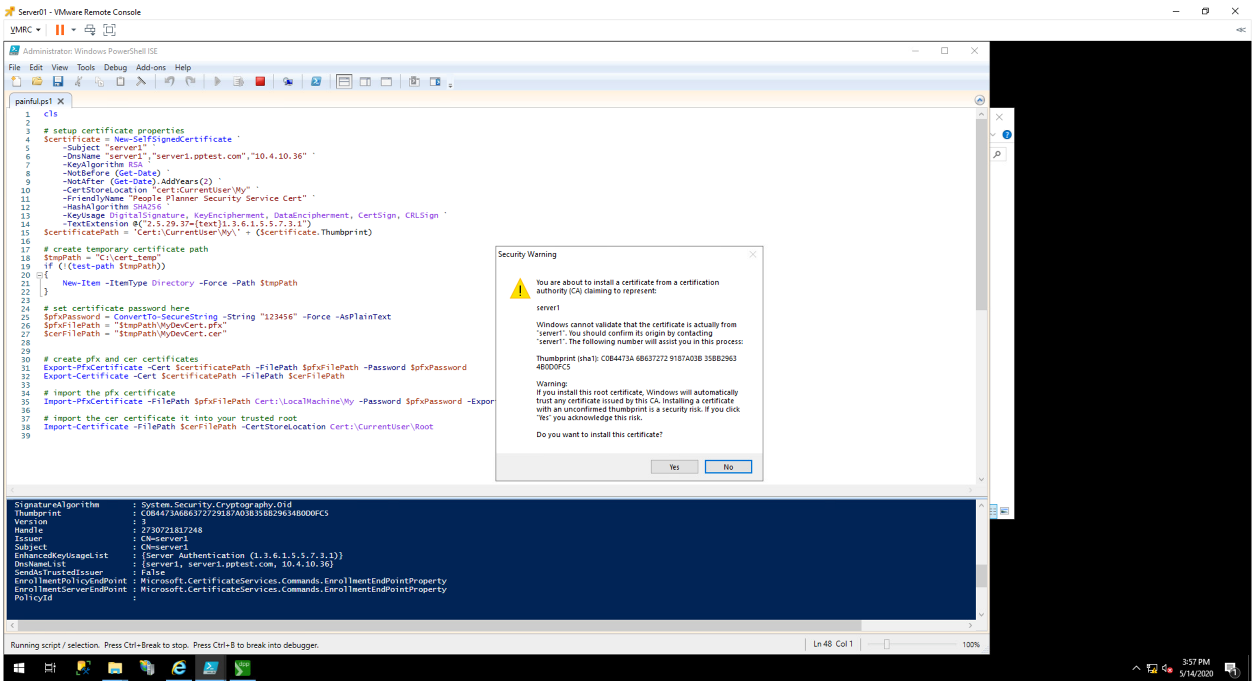
```
# setup certificate properties including the commonName (DNSName) property for Chrome 58+
$certificate = New-SelfSignedCertificate `
    -Subject "server1" `
    -DnsName "server1", "server1.pptest.com","10.4.10.36" `
    -KeyAlgorithm RSA `
    -KeyLength 2048 `
    -NotBefore (Get-Date) `
    -NotAfter (Get-Date).AddYears(2) `
    -CertStoreLocation "cert:CurrentUser\My" `
    -FriendlyName "People Planner Security Service Cert" `
    -HashAlgorithm SHA256 `
    -KeyUsage DigitalSignature, KeyEncipherment, DataEncipherment, CertSign, CRLSign `
    -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.1")
$certificatePath = 'Cert:\CurrentUser\My\' + ($certificate.ThumbPrint)

# create temporary certificate path
$tmpPath = "C:\cert_temp"
if (!(test-path $tmpPath))
{
    New-Item -ItemType Directory -Force -Path $tmpPath
}

# set certificate password here
$pfxPassword = ConvertTo-SecureString -String "123456" -Force -AsPlainText
$pfxFilePath = "$tmpPath\MyDevCert.pfx"
```

```
$cerFilePath = "$tmpPath\MyDevCert.cer"

# create pfx certificate
#Export-PfxCertificate -Cert $certificatePath -FilePath $pfxFilePath -Password $pfxPassword
Export-Certificate -Cert $certificatePath -FilePath $cerFilePath

# import the pfx certificate
#Import-PfxCertificate -FilePath $pfxFilePath Cert:\LocalMachine\My -Password $pfxPassword -
Exportable

# trust the certificate by importing the pfx certificate into your trusted root
Import-Certificate -FilePath $cerFilePath -CertStoreLocation Cert:\CurrentUser\Root  ##THIS NEEDS
TO BE IMPORTED ON CLIENTS WANTING TO TRUST!!

# optionally delete the physical certificates (don't delete the pfx file as you need to copy this
to your app directory)
#Remove-Item $pfxFilePath
#Remove-Item $cerFilePath
```

Key points:

1. To ensure that a certificate cannot be stolen and moved to a different machine than the one it was issued for, a SSL certificate is keyed to a specific machine. Edit the DnsName line to the name(s) of the server.
2. Set the FriendlyName to something descriptive of what the certificate is for.
3. Change the password stored in $pfxPasssword to something more secure.
4. The other lines of the script can be modified, or not, as it suits you.

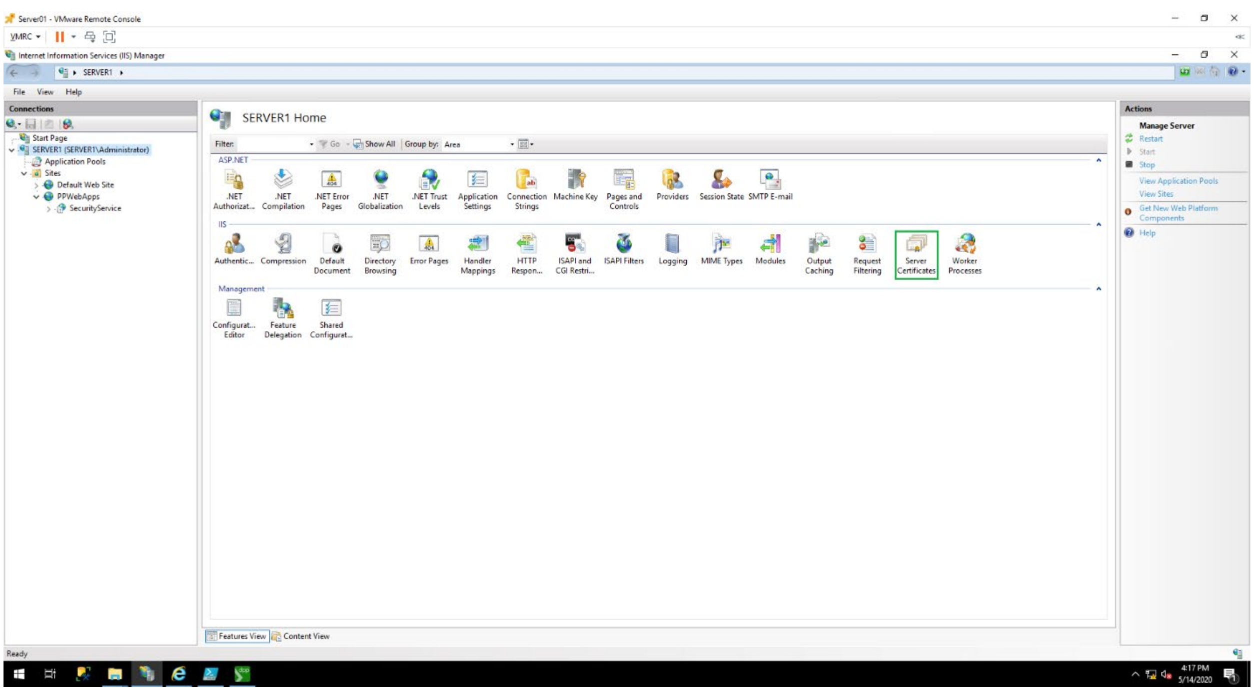
Run the script, and press **Yes** to allow the certificate to be installed.



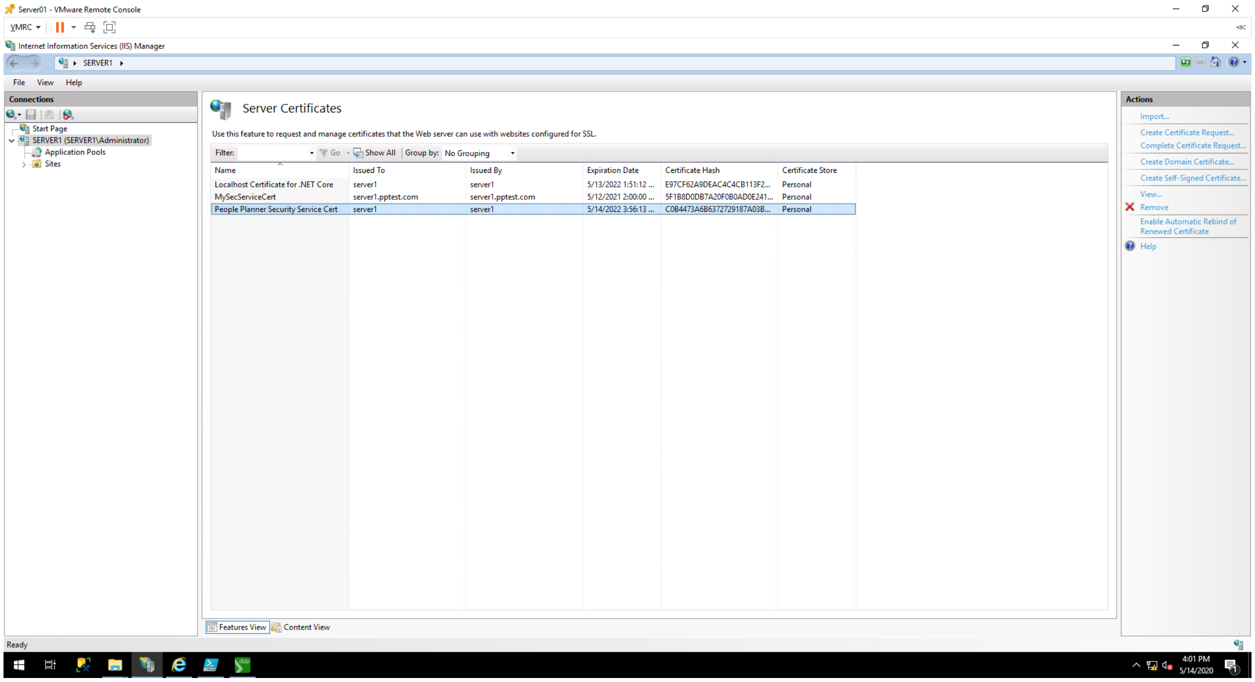
Set Up the Website for SSL

With the SSL certificate in place, you can now setup the People Planner Security Service to bind to SSL.

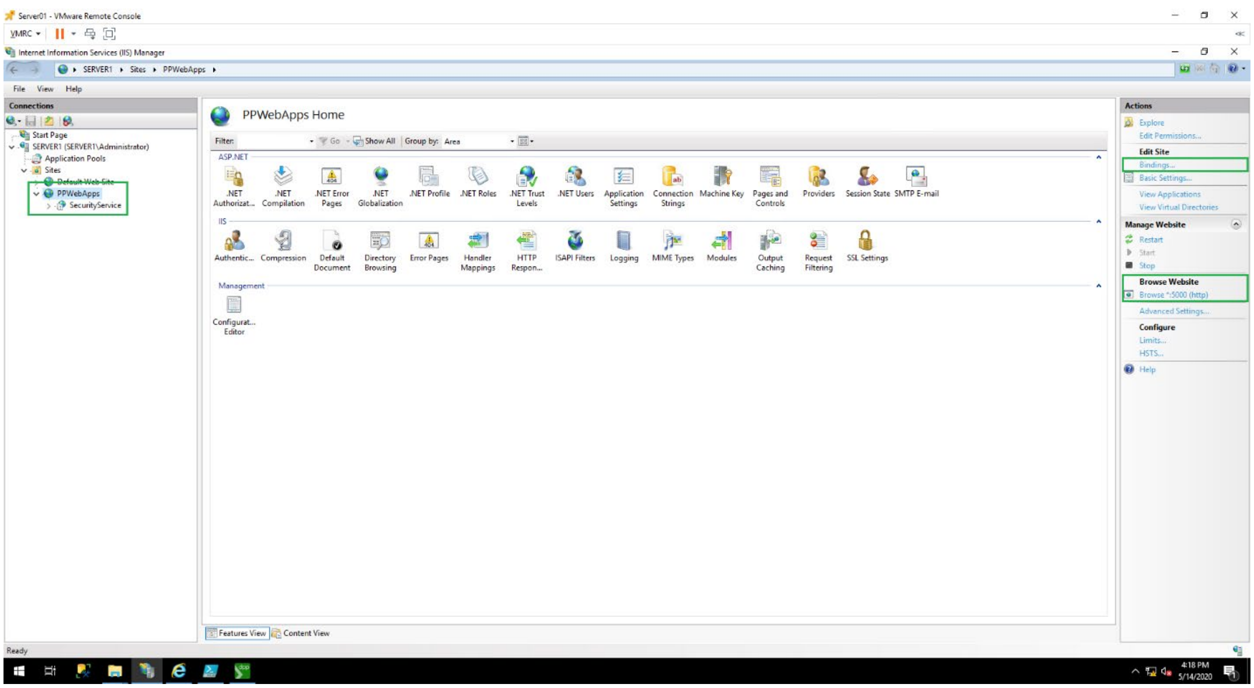
1. Verify that the certificate is available in the IIS. Open the IIS Manager and, select the server-node and then the Server Certificates in the IIS section.



The certificate should be shown in the list of the Server Certificates.

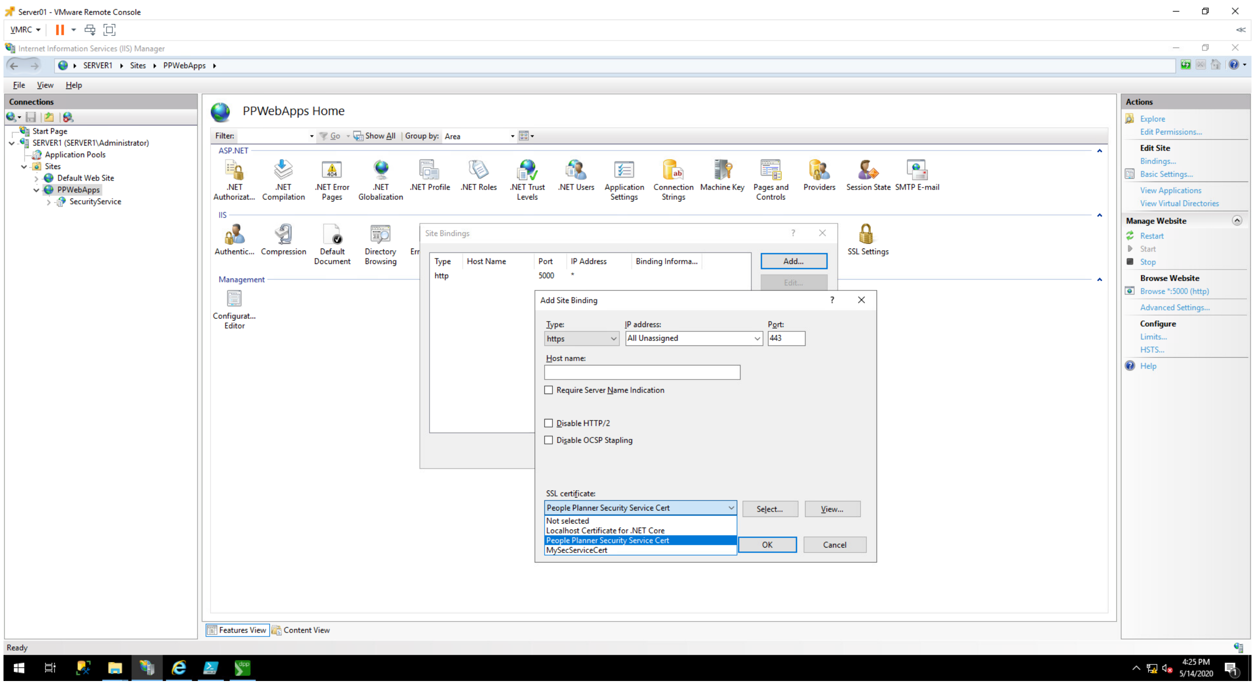


2. Select the web site where the Security Service is installed. Currently, there is a single binding to port 5000 as http.

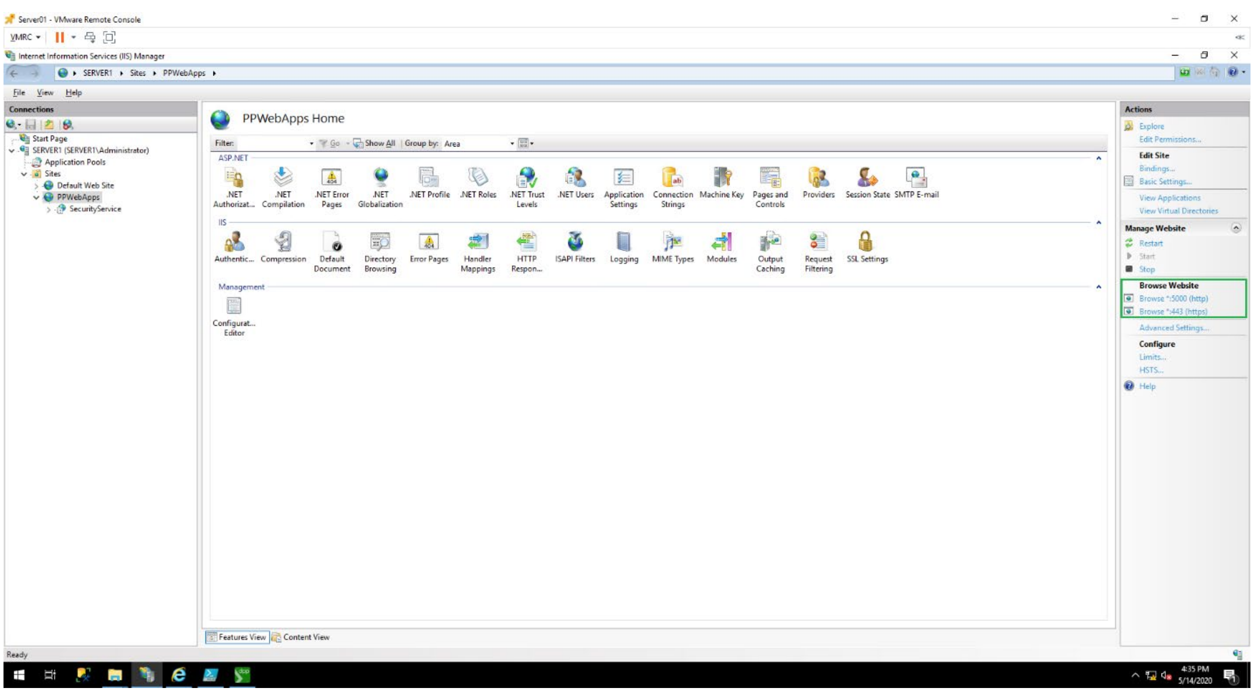


3. To create a second binding to https, such as SSL, press the **Bindings** link. This open the **Site Bindings** wizard. In the wizard, press **Add** to add a new binding.

4. In the **Add Site Binding** window, select “https” and in the SSL certificate dropdown select the self-signed certificate. You can either select a different port for this binding, or you can keep the default port for SSL (port 443).

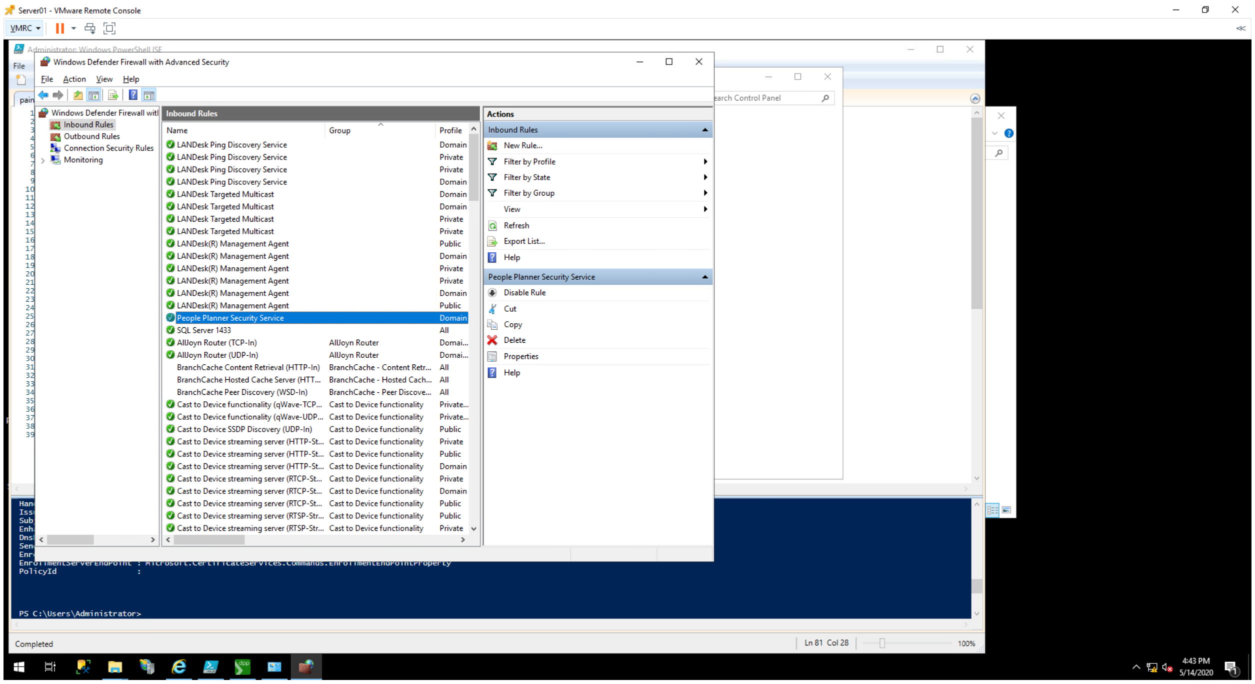


5. Press **Ok** to close the **Add Site Binding** window, and then press **Close**. The https binding should be listed.

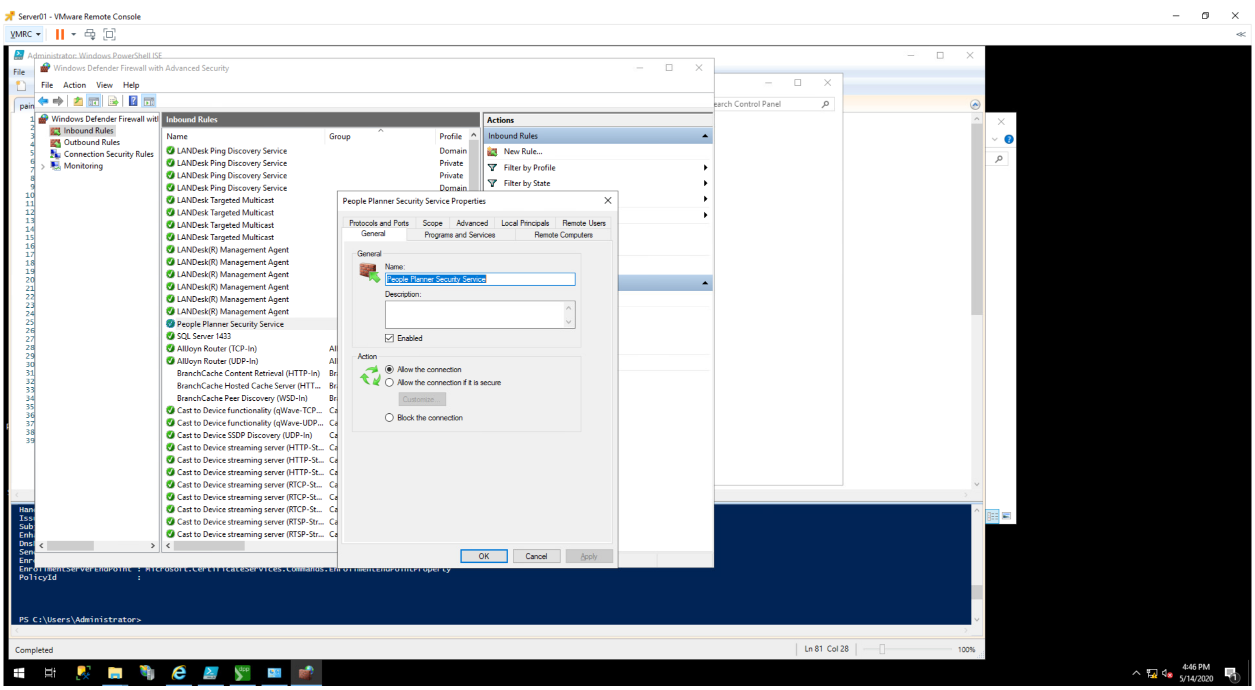


Open the SSL Port in the Firewall

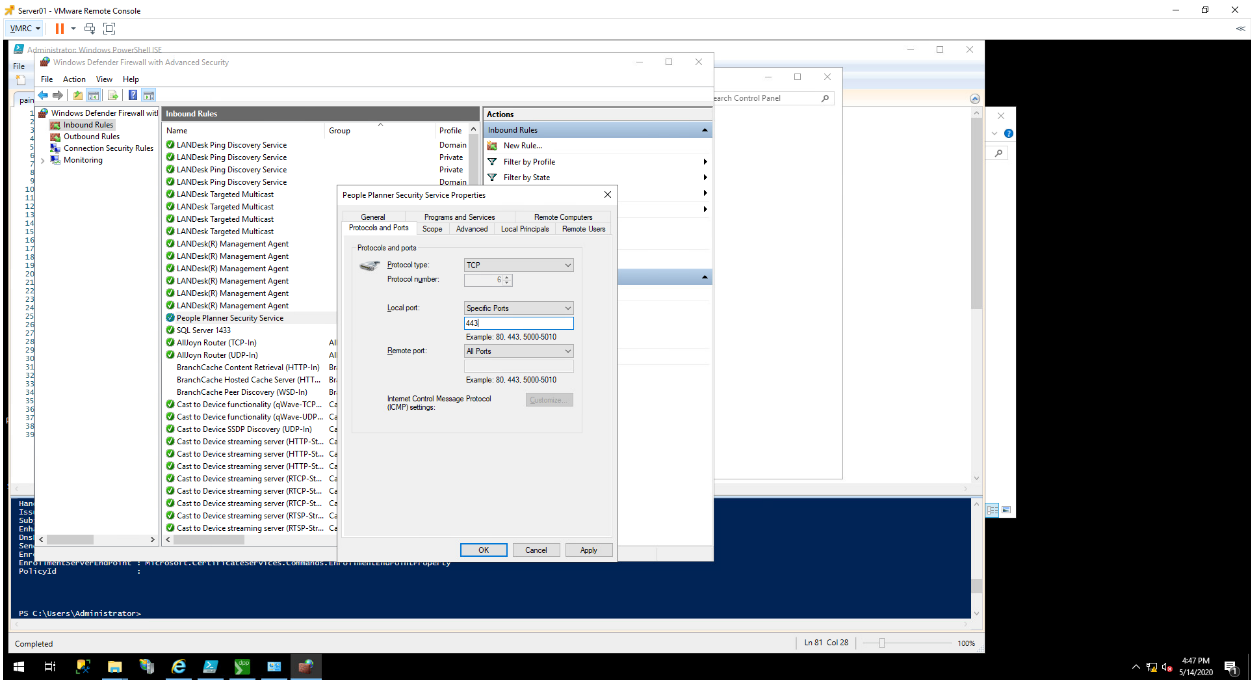
1. Open the Windows Defender Firewall, and edit the inbound rule you created earlier.



2. Right-click on the rule, and select **Properties**.



3. Select the **Protocols and Ports** tab, and edit the **Local port**; Delete the existing port 5000 and enter the SSL port instead.



4. Press **OK** to save the changes to the firewall rule.

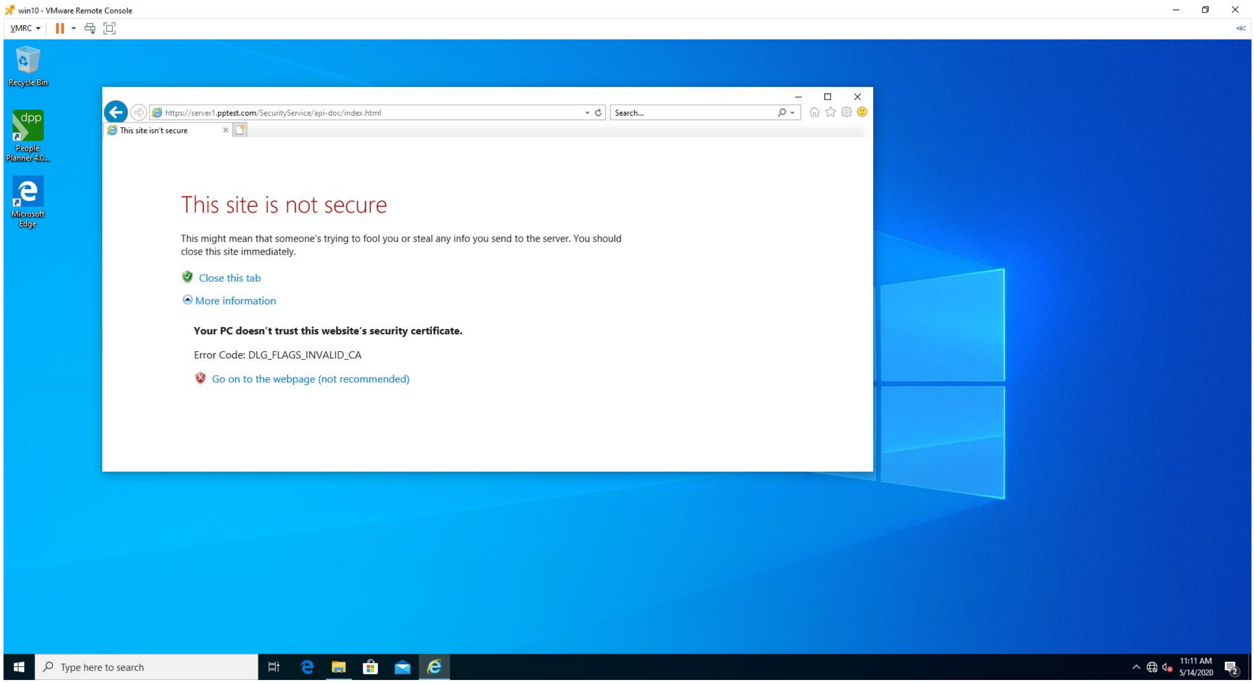
Open the Swagger-documentation from the Client

To verify that the SSL certificate works and the firewall allows the traffic through, you can open the Swagger-documentation in a browser.

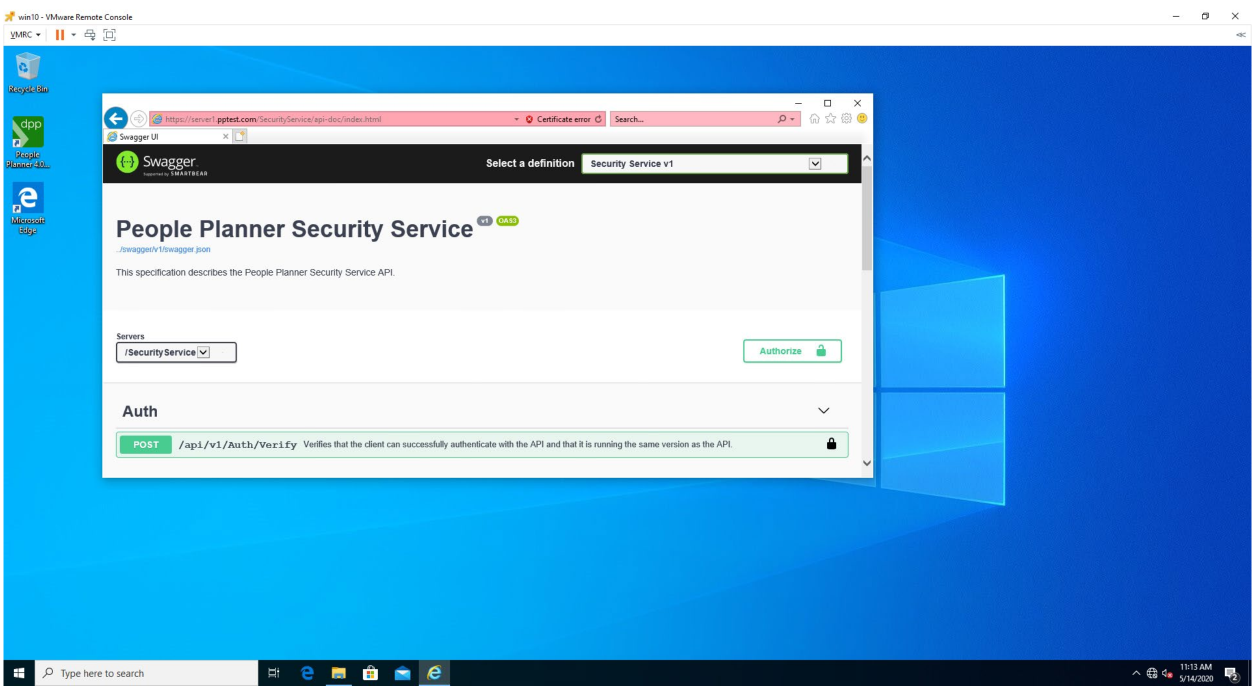
The URL needs to be updated from earlier: the scheme should be changed to “https” and the port should be changed to the port used by the https-binding.

Also, if you used the IP instead of the fully qualified domain name (FQDN), you need to change it to the FQDN. Using the IP address might not work, depending on the configuration.

Since we have not yet told the client that it should trust the certificate, the browser will warn that the site is not secure.

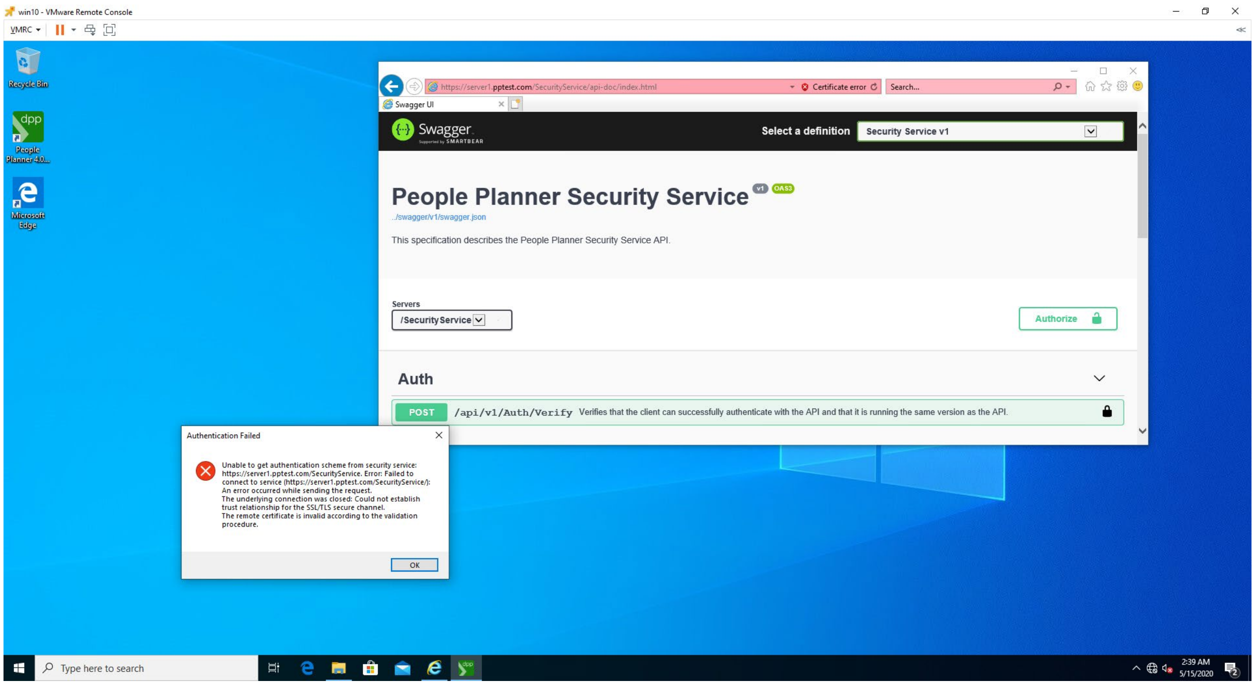


You can force the browser to continue on to the site regardless, and the Swagger-documentation should now be displayed.



Instruct the Client to Trust the Certificate

In the browser, you can force it to accept the certificate. That is not an option for the People Planner Windows application, and it will still fail to authenticate.

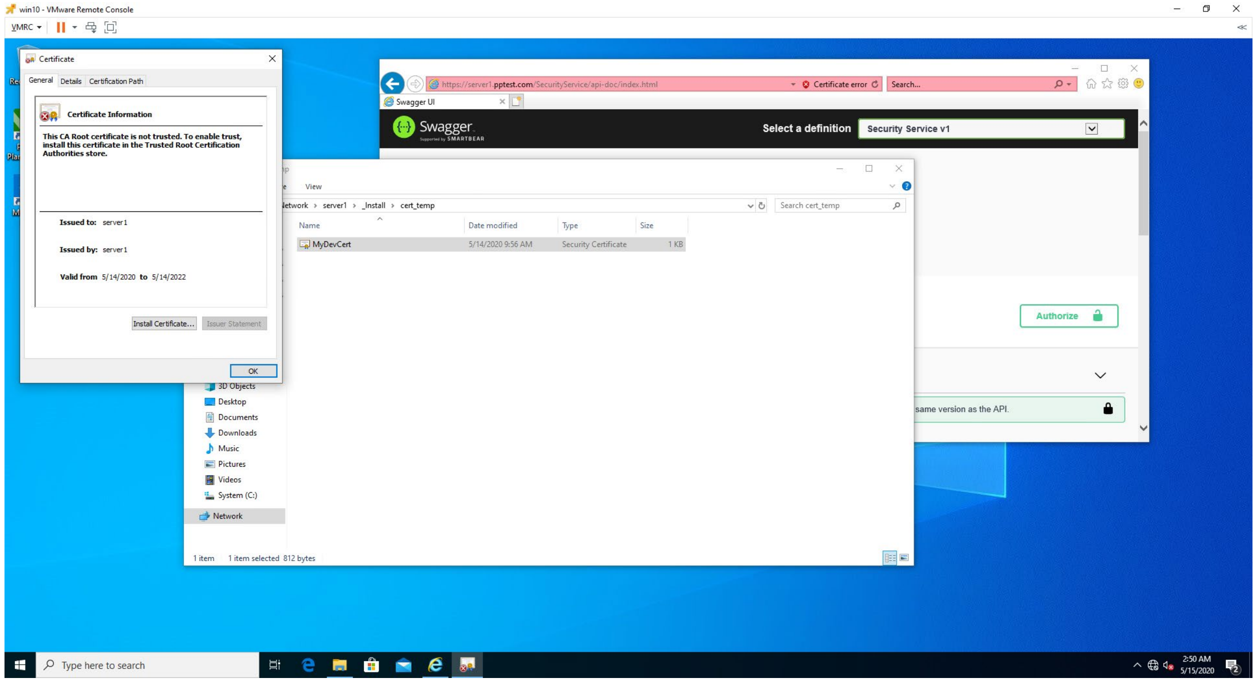


To fix this, you will need to tell the client-machine to trust the certificate.

The script that you used to create the certificate – among other things – created a cer-file in the folder:

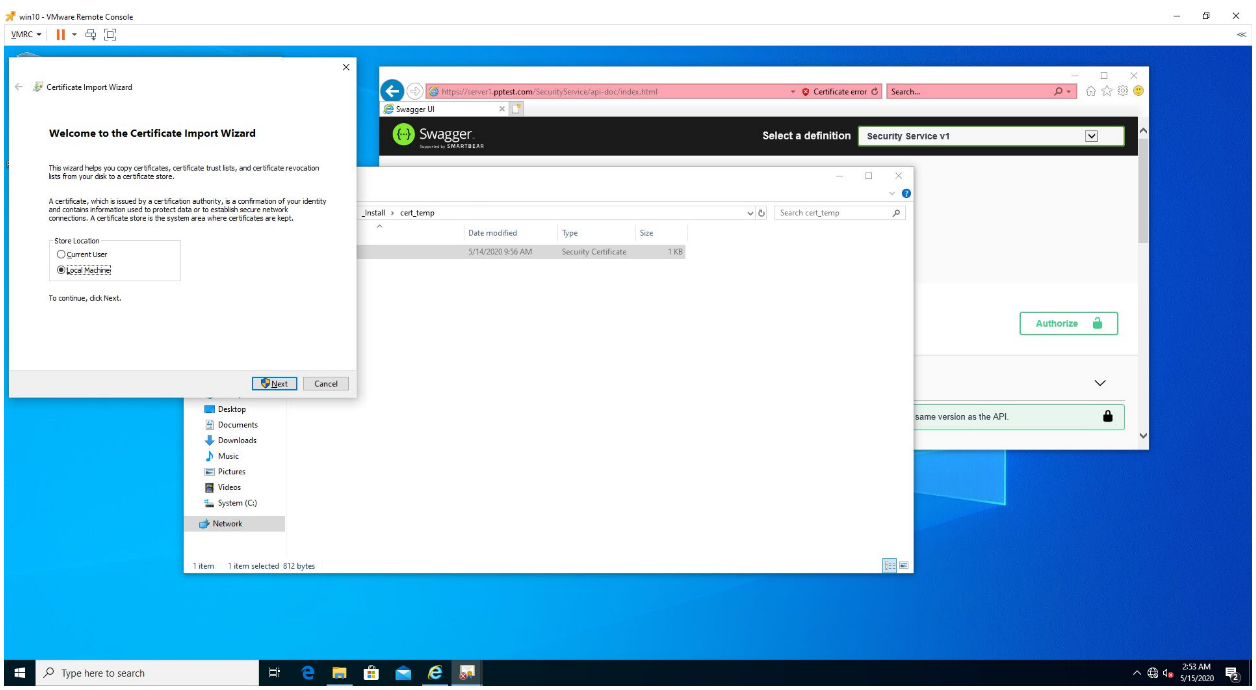
C:\cert_temp.

1. Copy the cer-file to the client machine. Double-click on the file. This opens the Certificate window where you can see the details of the certificate.

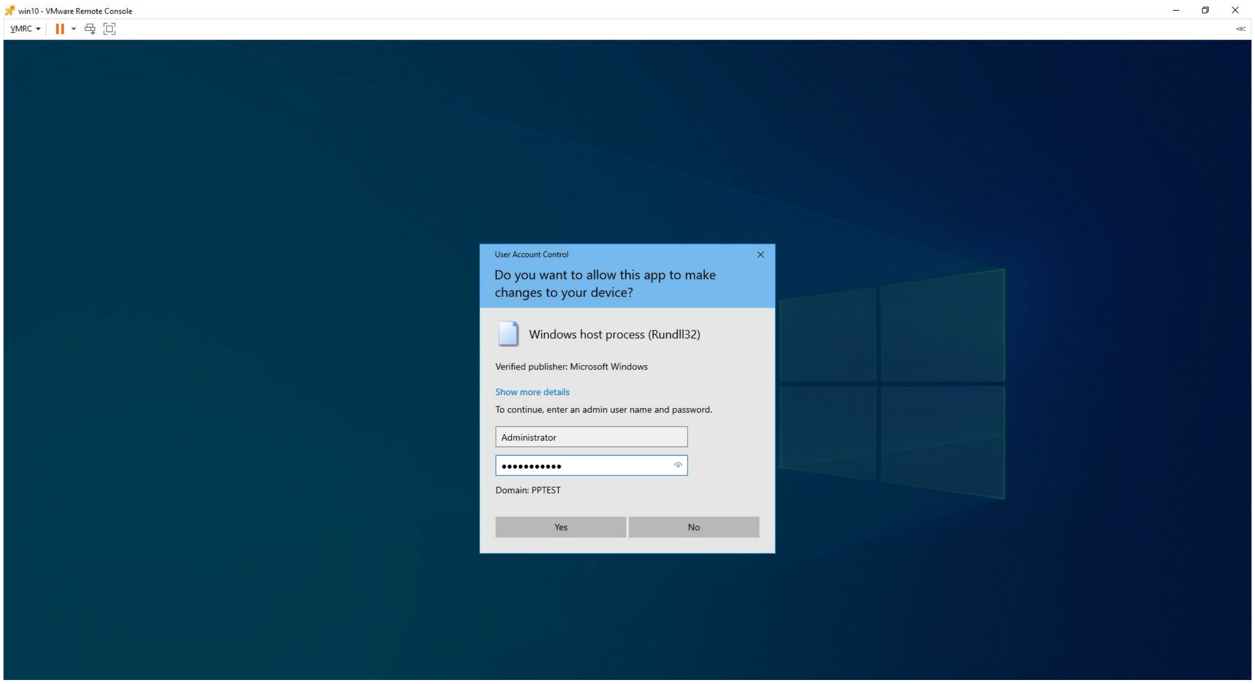


2. When you have ascertained yourself that it is the correct certificate, press the **Install Certificate** button.

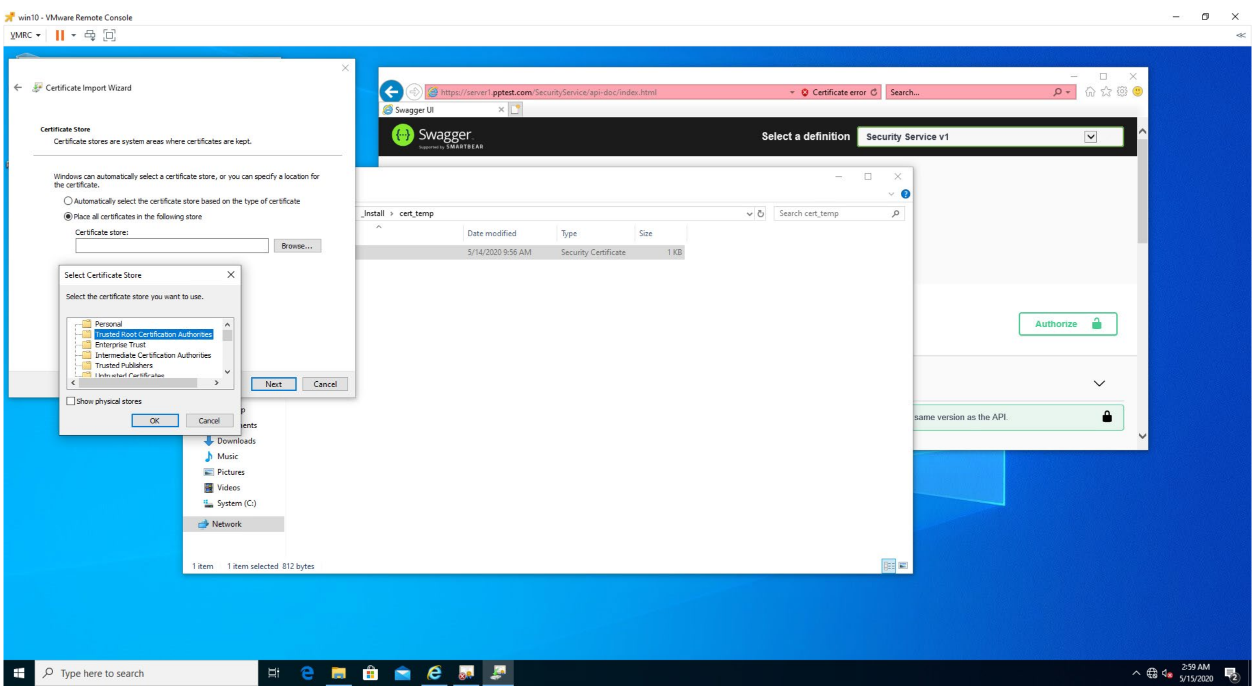
   You are now prompted whether you want to install the certificate. If there is only a single user on the machine, it does not matter. However, if there are multiple users on the machine and the certificate is for all, then you should chose the **Local Machine**.



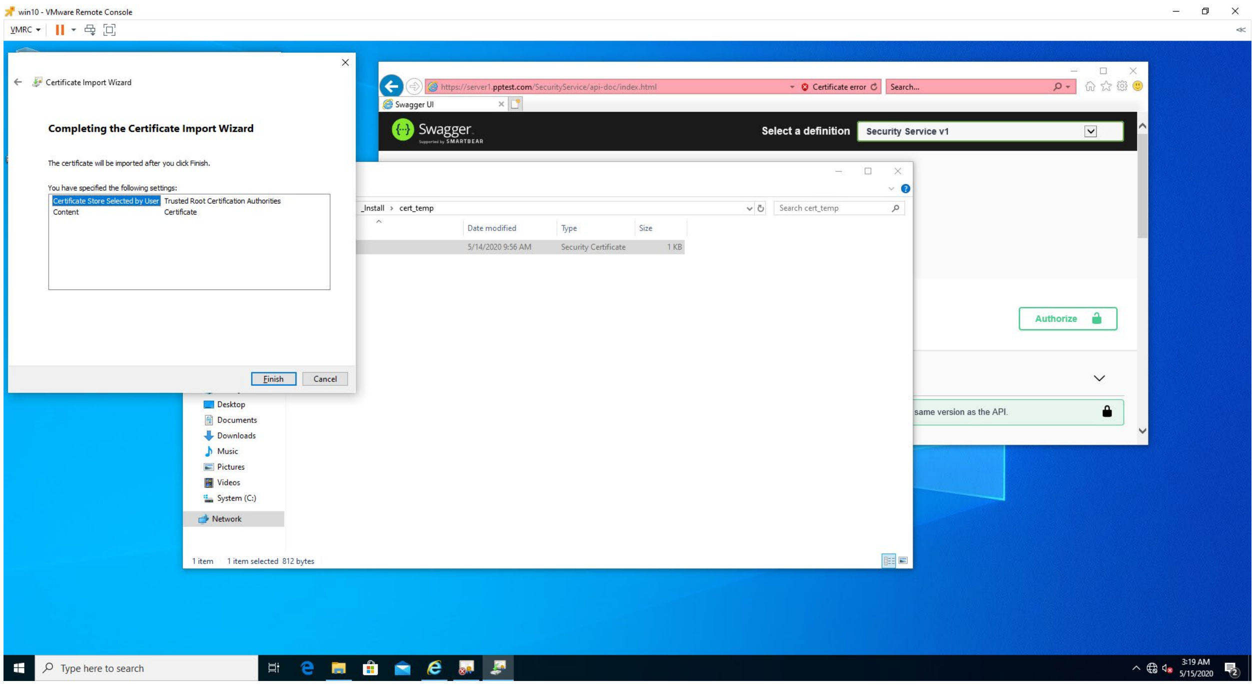
3. Click **Next**. You will now be prompted for the administrator credentials.



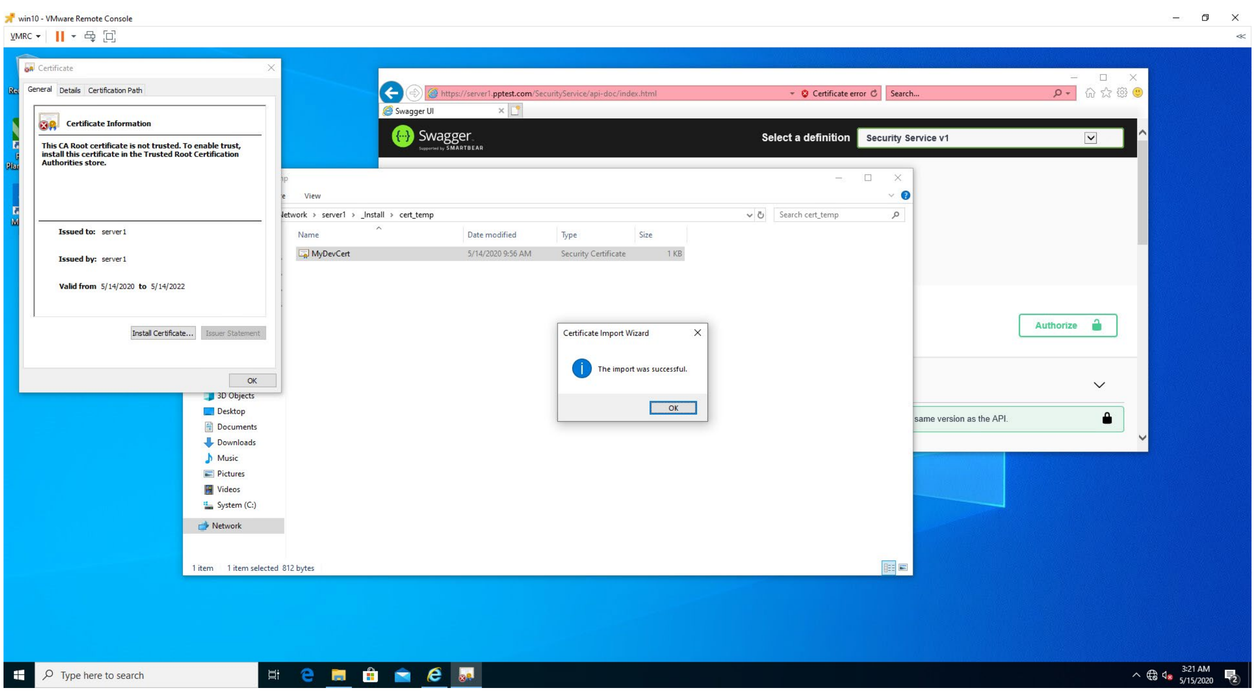
4. Next, select in which certificate-store you want to keep the certificate. Select the **Trusted Root Certification Authorities** store.



5. Click **OK** to accept, and then **Next** to continue.

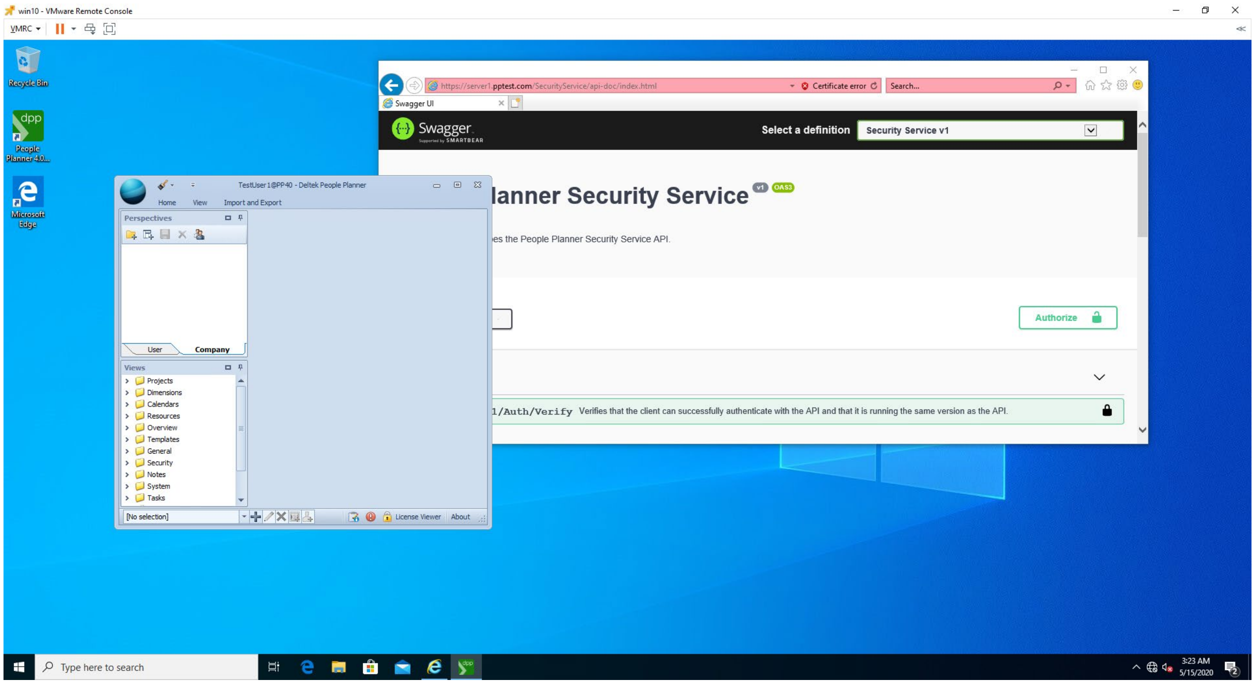


6. Click **Finish**.



7. Finally, click **OK** to the two windows to close them

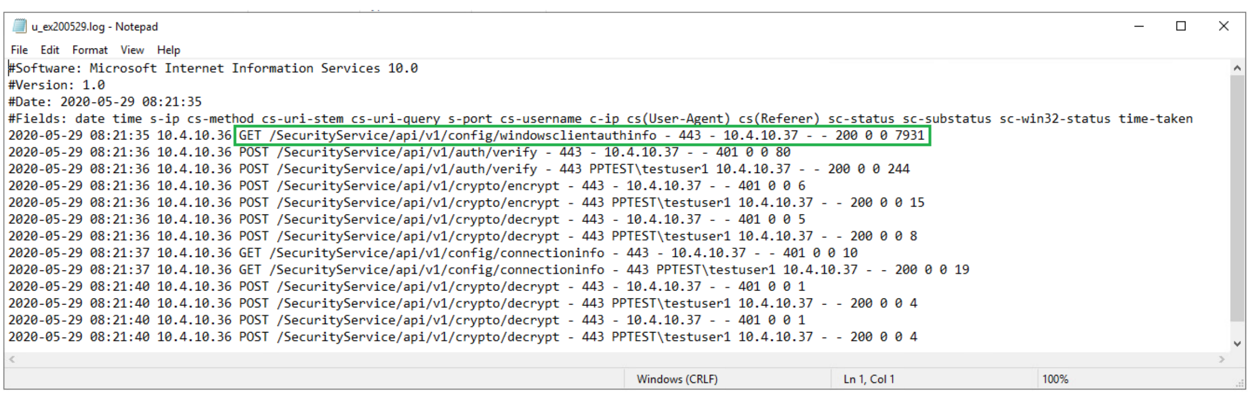
Now, when you open the Windows application, it should authenticate you successfully.



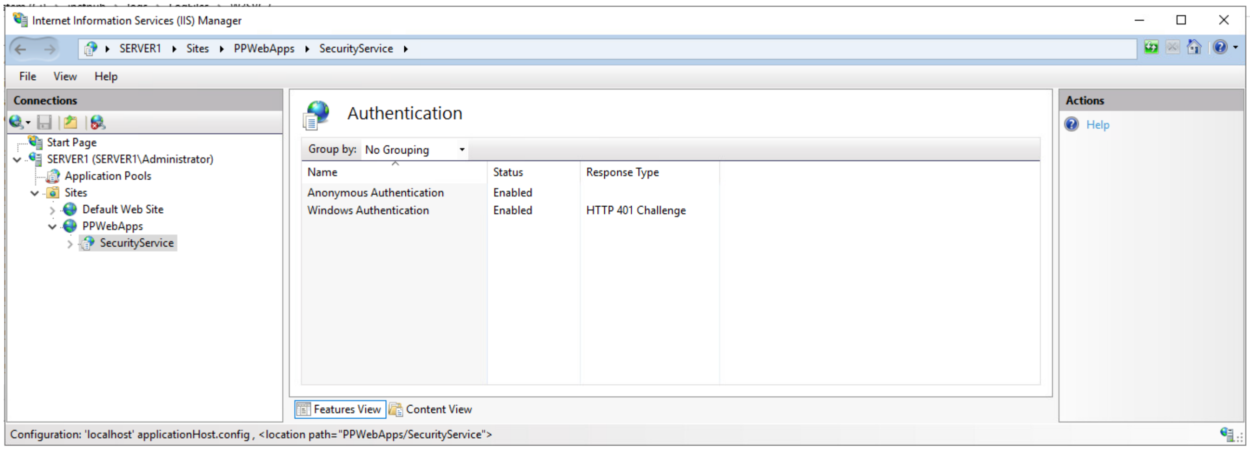
Note: You cannot attempt any of this on the server – it can only be done on the client.

Kerberos Authentication

When the People Planner Windows application connects to the People Planner Security Server, one of the very first things to happen is that it asks how to authenticate the user.



This first call will use Anonymous Authentication, but the calls that follows will use Windows Authentication. It is therefore important that the Security Service have both types of authentication enabled.



Note: Because the subsequent calls uses Windows Authentication, this is the reason why the two machines need to be in the same domain.

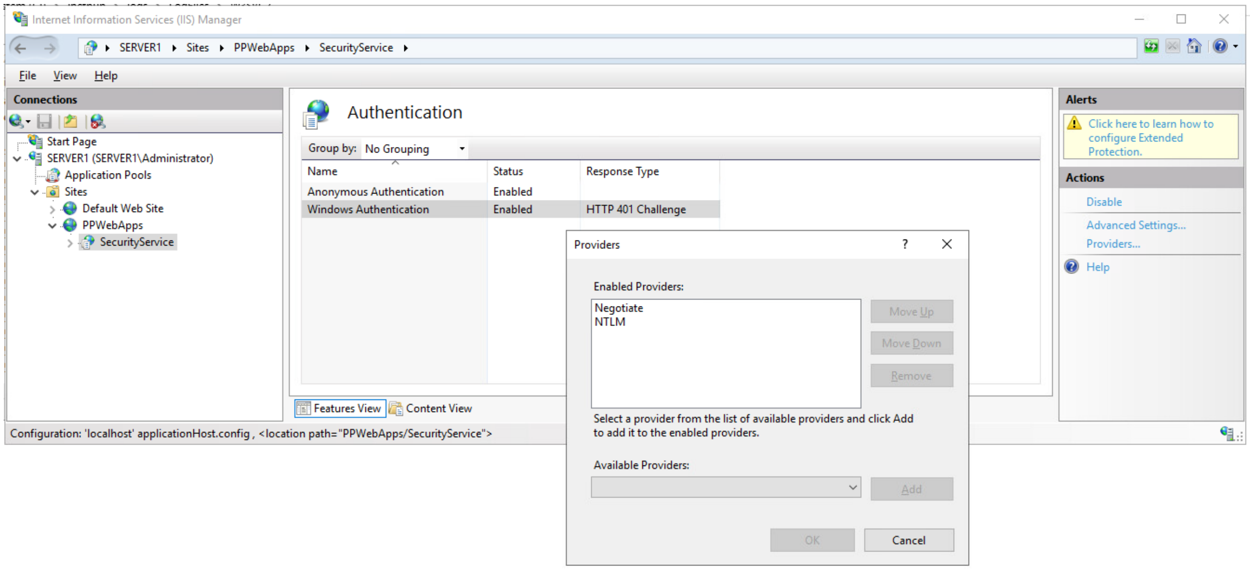
Negotiate

Windows Authentication can happen in different ways, NTLM or Kerberos. Negotiate is the protocol that decides which one to use. Negotiate is also known as “Simple and Protected GSSAPI Negotiation Mechanism” (SPNEGO).

NTLM is an older protocol. For security reasons, we recommend that you use Kerberos instead.

To set this up:

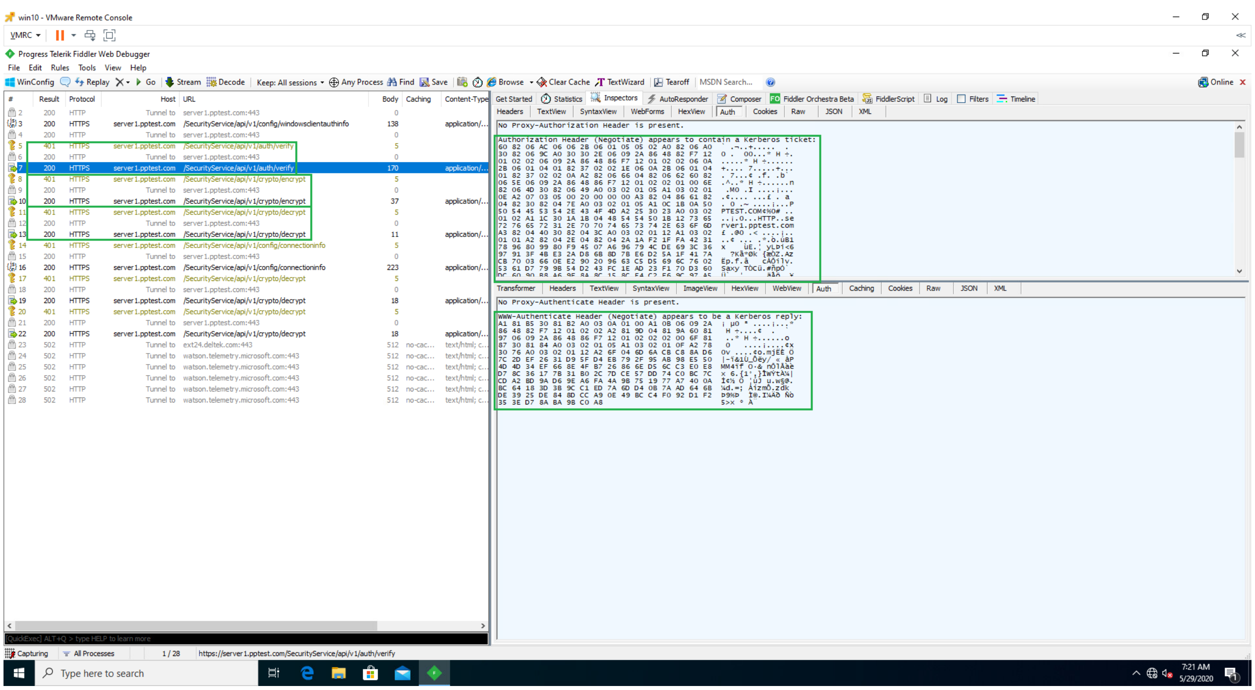
1. Double-click on Windows Authentication.
2. Click on **Providers…** to open the Providers window.
3. Rearrange the providers such that Negotiate is the first item and NTLM is second.



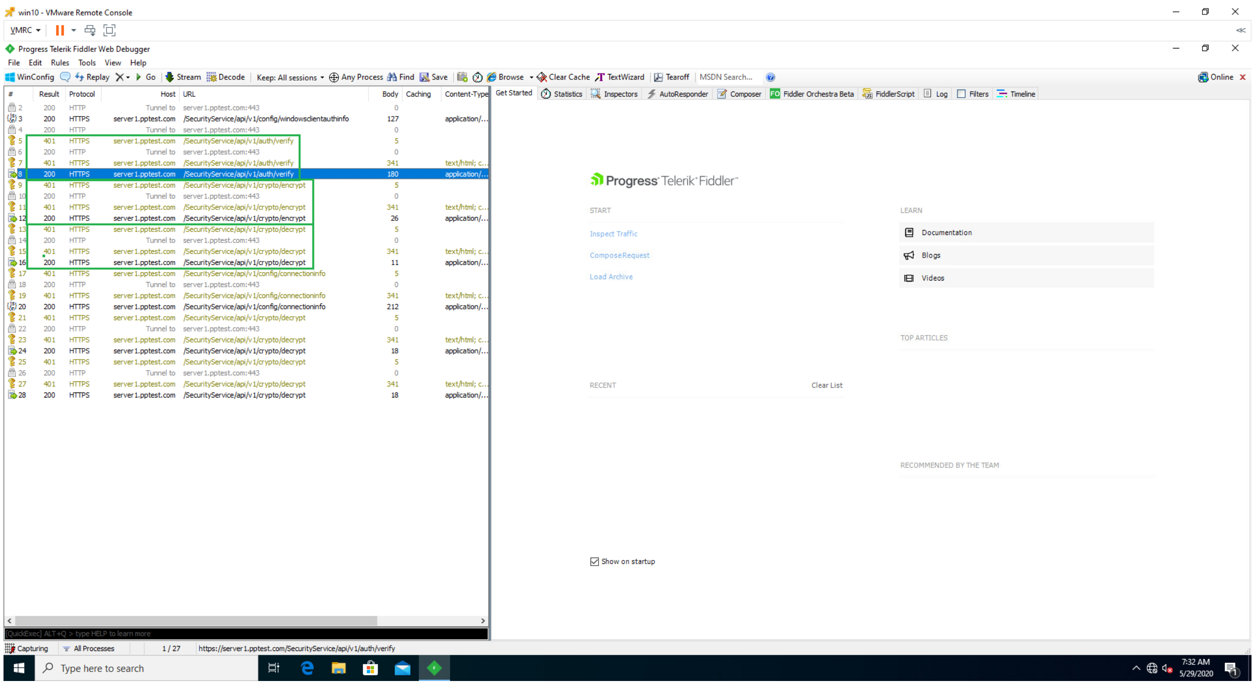
With this setup, the authentication will first attempt to use Kerberos Authentication, and if it fails, it will fall back to using NTLM.

A fall back happens fully transparent to the user, so how do you verify that the authentication does in fact use Kerberos and did not silently fall back to using NTLM? If you install a tool, like Postman or Fiddler, and use it to inspect the HTTP-traffic, you should see the following behavior:

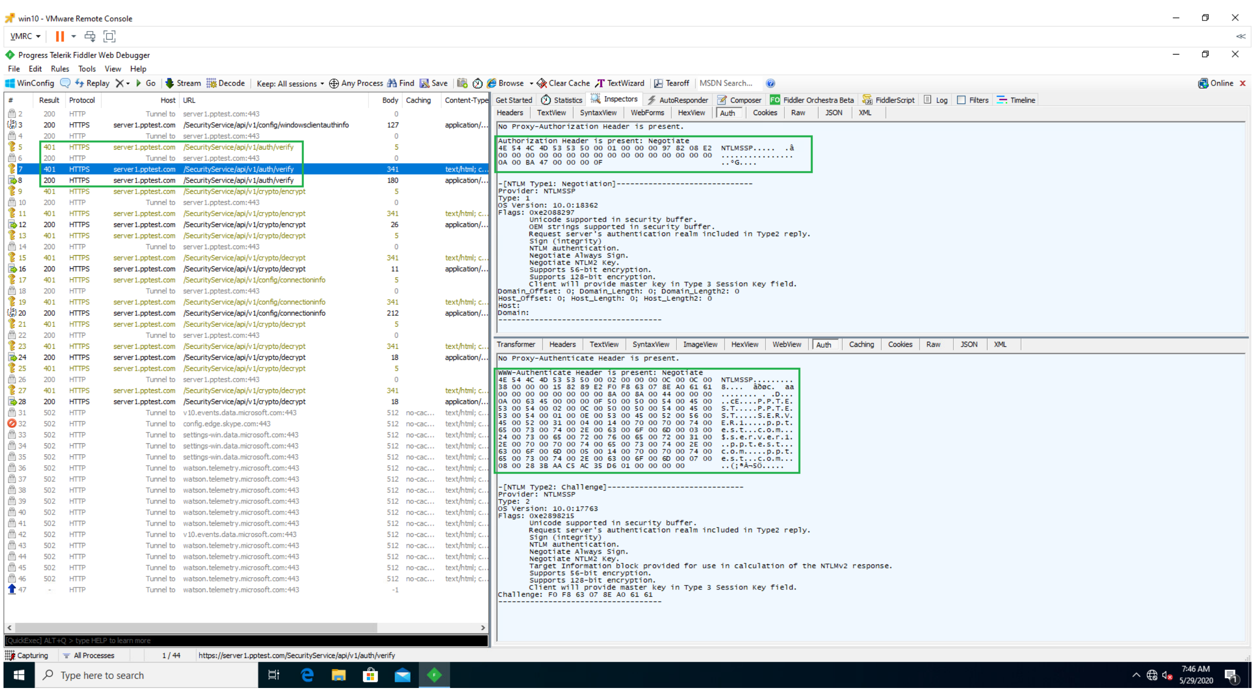
If the authentication is using Kerberos, you will see every request come in pairs of two, the first time with status-401, and the second time with status-200. If you inspect the authentication, you should see the Kerberos tickets.



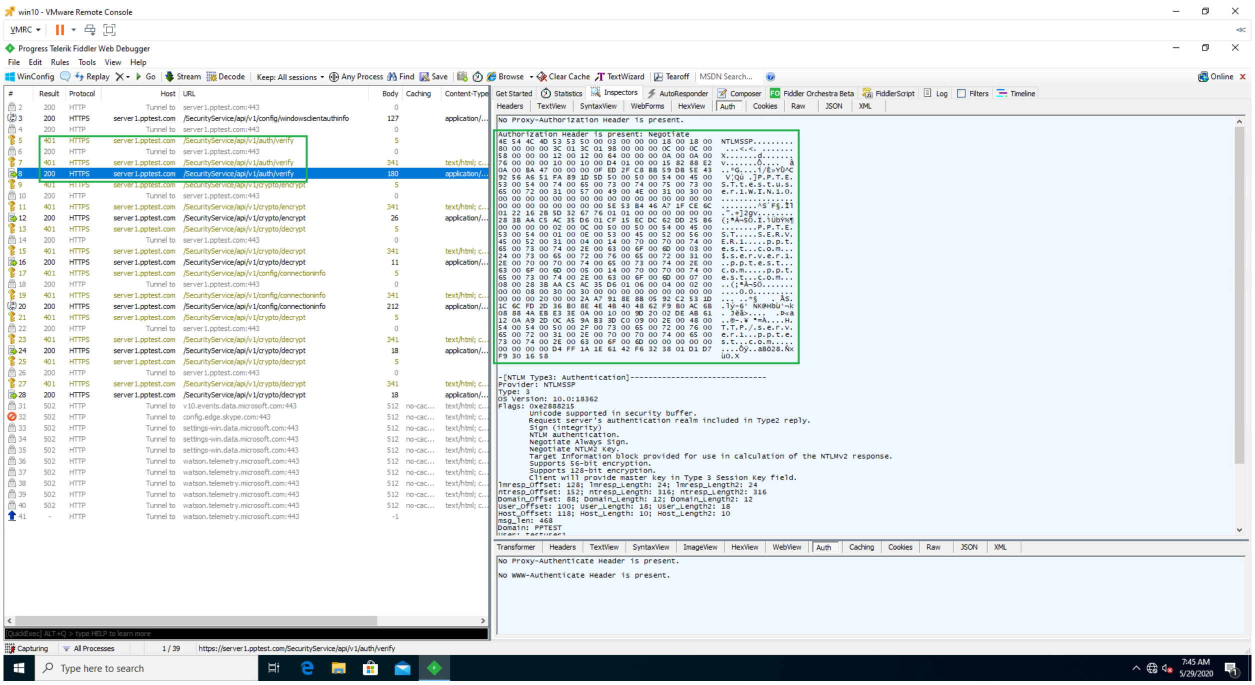
If the authentication is instead using NTML, you will see every request in triplets; First, two status-401 and then a status-200.



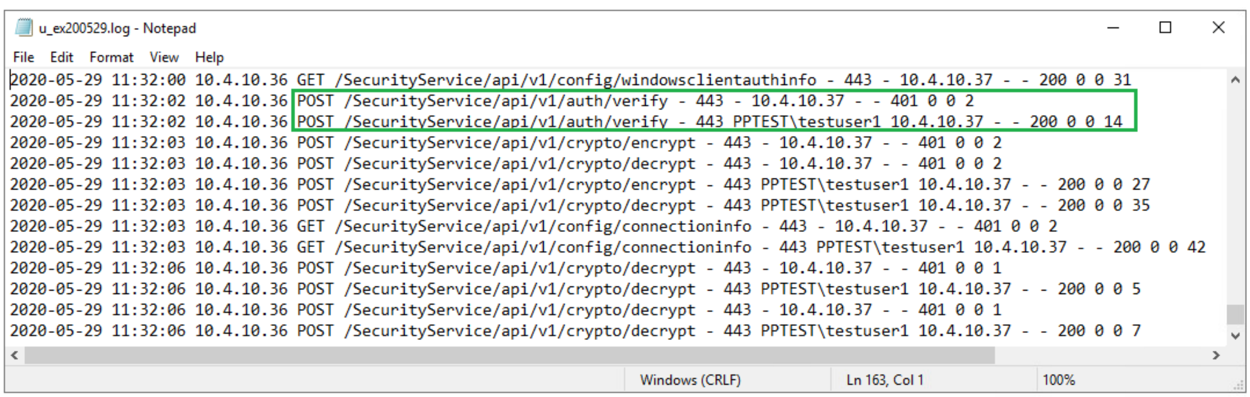
If you inspect the authentication, you will see the NTLM-tickets.



And:



Note: Regardless of whether you are using Kerberos or NTLM, the IIS log will only show two hits.




```
2020-05-29 11:32:00 10.4.10.36 GET /SecurityService/api/v1/config/windowsclientauthinfo - 443 - 10.4.10.37 - - 200 0 0 31
2020-05-29 11:32:02 10.4.10.36 POST /SecurityService/api/v1/auth/verify - 443 - 10.4.10.37 - - 401 0 0 2
2020-05-29 11:32:02 10.4.10.36 POST /SecurityService/api/v1/auth/verify - 443 PPTEST\testuser1 10.4.10.37 - - 200 0 0 14
2020-05-29 11:32:03 10.4.10.36 POST /SecurityService/api/v1/crypto/encrypt - 443 - 10.4.10.37 - - 401 0 0 2
2020-05-29 11:32:03 10.4.10.36 POST /SecurityService/api/v1/crypto/decrypt - 443 - 10.4.10.37 - - 401 0 0 2
2020-05-29 11:32:03 10.4.10.36 POST /SecurityService/api/v1/crypto/encrypt - 443 PPTEST\testuser1 10.4.10.37 - - 200 0 0 27
2020-05-29 11:32:03 10.4.10.36 POST /SecurityService/api/v1/crypto/decrypt - 443 PPTEST\testuser1 10.4.10.37 - - 200 0 0 35
2020-05-29 11:32:03 10.4.10.36 GET /SecurityService/api/v1/config/connectioninfo - 443 - 10.4.10.37 - - 401 0 0 2
2020-05-29 11:32:03 10.4.10.36 GET /SecurityService/api/v1/config/connectioninfo - 443 PPTEST\testuser1 10.4.10.37 - - 200 0 0 42
2020-05-29 11:32:06 10.4.10.36 POST /SecurityService/api/v1/crypto/decrypt - 443 - 10.4.10.37 - - 401 0 0 1
2020-05-29 11:32:06 10.4.10.36 POST /SecurityService/api/v1/crypto/decrypt - 443 PPTEST\testuser1 10.4.10.37 - - 200 0 0 5
2020-05-29 11:32:06 10.4.10.36 POST /SecurityService/api/v1/crypto/decrypt - 443 - 10.4.10.37 - - 401 0 0 1
2020-05-29 11:32:06 10.4.10.36 POST /SecurityService/api/v1/crypto/decrypt - 443 PPTEST\testuser1 10.4.10.37 - - 200 0 0 7
```


SPNs

One reason why Kerberos might fail, and the authentication falls back to NTLM, is missing a **Server Principal Name (SPN)** on the server.

Note: In a security model such as Kerberos, a “Principal” represents an entity that needs authentication. For example, this could be a user that needs to log on. The Server Principal Name is a (unique) represents the service – which also needs authentication.

For more information about SPNs, refer to:

https://docs.microsoft.com/en-us/windows/win32/ad/service-principal-names

Running the **setspn** command with the -L switch, will give you the list of SPNs for a given host. For example, the SPNs for server1 could look something like this:

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> setspn -L server1
Registered ServicePrincipalNames for CN=SERVER1,CN=Computers,DC=pptest,DC=com:
        HOST/server1.pptest.com
        HOST/SERVER1
        RestrictedKrbHost/SERVER1
        RestrictedKrbHost/server1.pptest.com
        MSSQLSvc/server1.pptest.com
        MSSQLSvc/server1.pptest.com:1433
        TERMSRV/SERVER1
        WSMAN/server1
        WSMAN/server1.pptest.com
        TERMSRV/server1.pptest.com
PS C:\Users\Administrator>
```

Below, we will discuss the SPNs that relates to the People Planner Security Service. For a comprehensive list of SPNs, you can refer to this document:

https://adsecurity.org/?page_id=183

HOST/…

When a host is joined to a domain, these two SPNs are created automatically. They are used for the services that comes built-in with Windows.

Both a "SERVER1" and a "server1.pptest.com" are created because you need separate SPNs for the NetBIOS name and the Fully Qualified Name (FQDN).

HOST is used as a default when a specific service is not specified; in fact, the SPNs for "LDAP" and "HTTP" are simply aliases for the HOST SPN. When a client asks for a Kerberos ticket for "HTTP/xyz", Active Directory will search through its accounts for the exact SPN, "HTTP/xyz", and if it cannot find this, it then searches for "HOST/xyz".

You might sometimes see a HTTP SPN that represents an IIS. This is not the case here, and is not absolutely necessary, as the HTTP would just be an alias for HOST anyway.

If the HOST SPNs are missing, you can use the setspn command with the -R switch to repair them:

```
setspn -R server1
```

See also for a longer discussion of HOST:

http://msdn.microsoft.com/en-us/library/ff649429.aspx

MSSQLSrv/…

The two MSSQLSrv SPNs are for the Microsoft SQL Server running on server1. The one with a port is used with TCP traffic, and the one without is used for other traffic.

In this case, the SQL Server is installed as a Default Instance, not a Named Instance. For a Named Instance the name would be part of the SPN.

In case these two SPNs are missing, they will automatically be recreated if the server is restarted.

For further reading, you should see:

https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/register-a-service-principal-name-for-kerberos-connections

Adding and removing SPNs

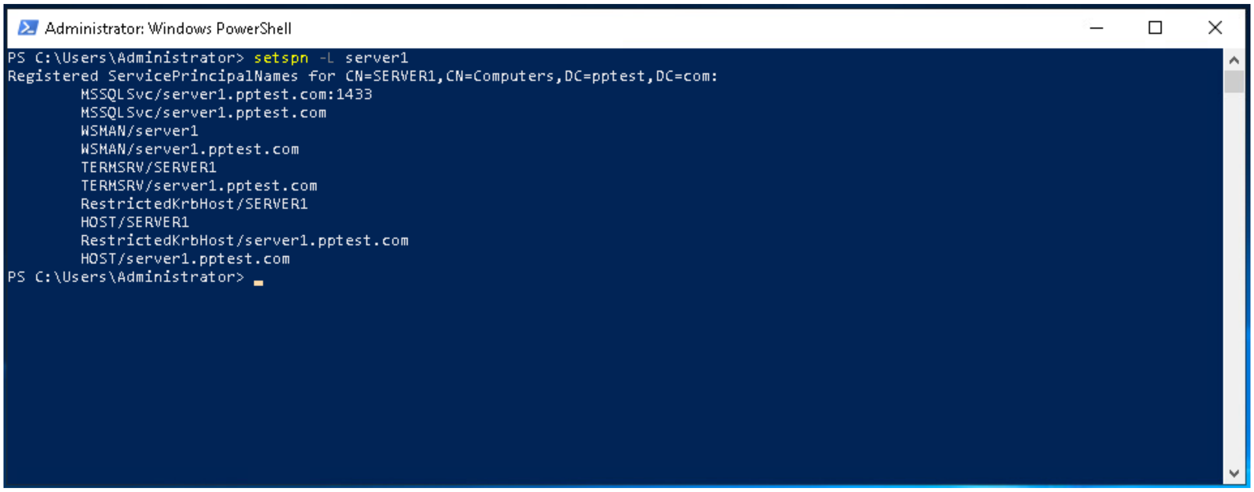
You can use the setspn-command to work with SPNs.

List the SPNs

To see a list of SPNs, use the setspn command with the -L switch:

```
setspn -L server1
```

The -L switch takes a single argument, the accoutname. If you want to see the SPNs relating to server1 you should use that as the accountname.

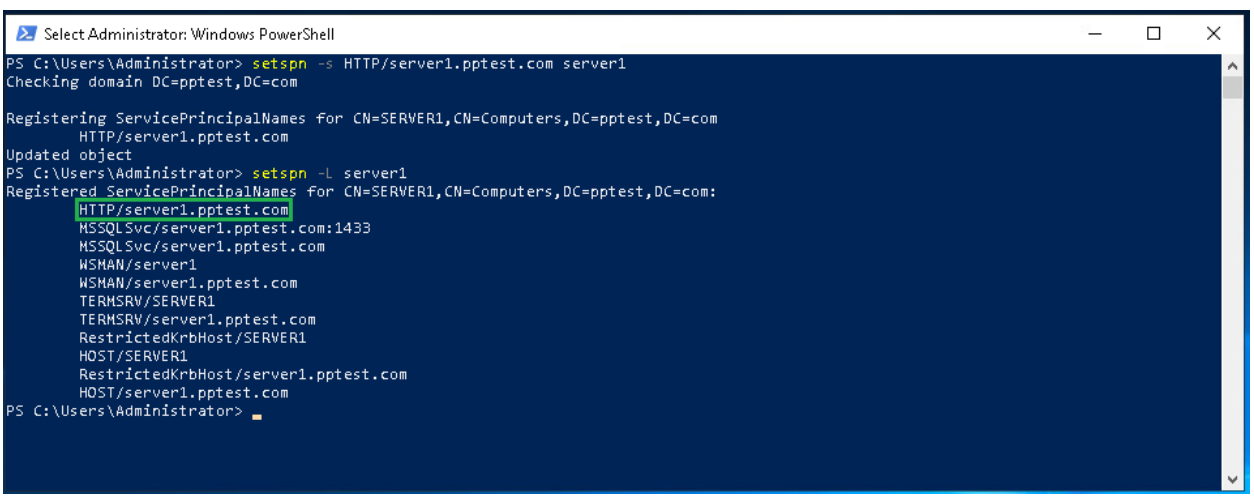


Add a SPN

To add a new SPN, you can use the setspn command with the -S switch:

```
setspn -S HTTP/server1.pptest.com server1
```

The -S switch takes two arguments, where the first, HTTP/server1.pptest.com, is the SPN and the second, server1, is the accountname.



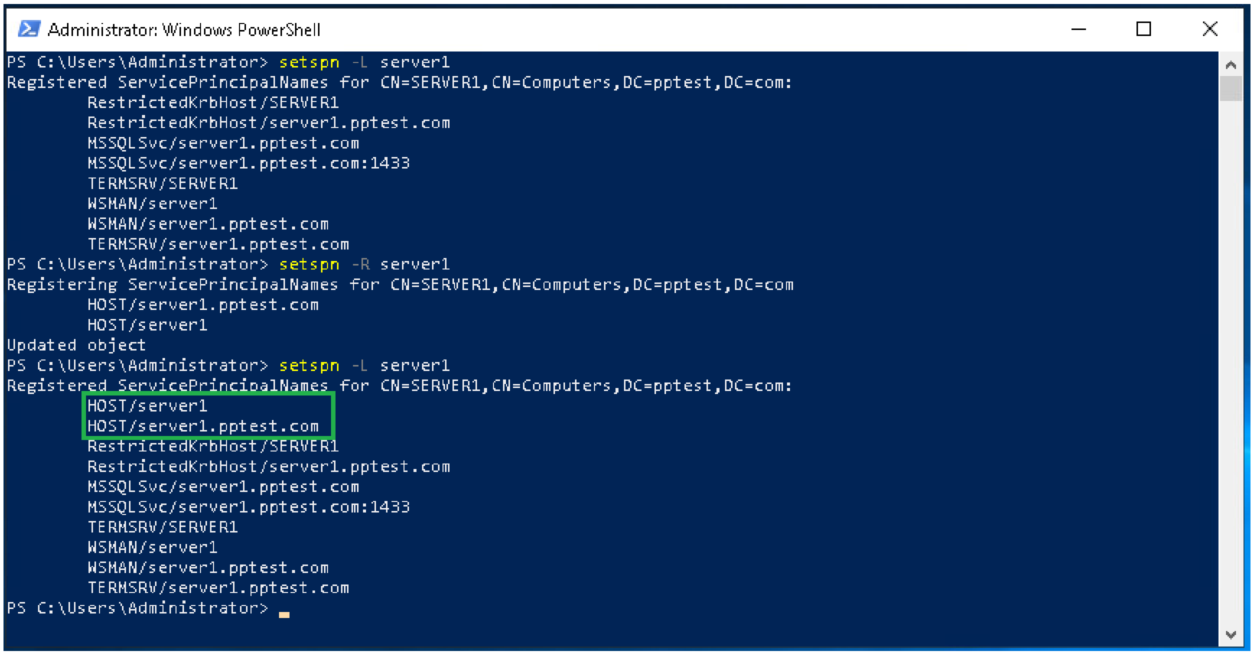
Repairing SPNs

The two HOST SPNs are vital to the Kerberos-authentication.

If they are missing, you can add them using the setspn command with the -S switch. However, you can also add them using the repair switch instead (-R):

```
setspn -R server1
```

The -R switch takes a single argument, the accoutname.

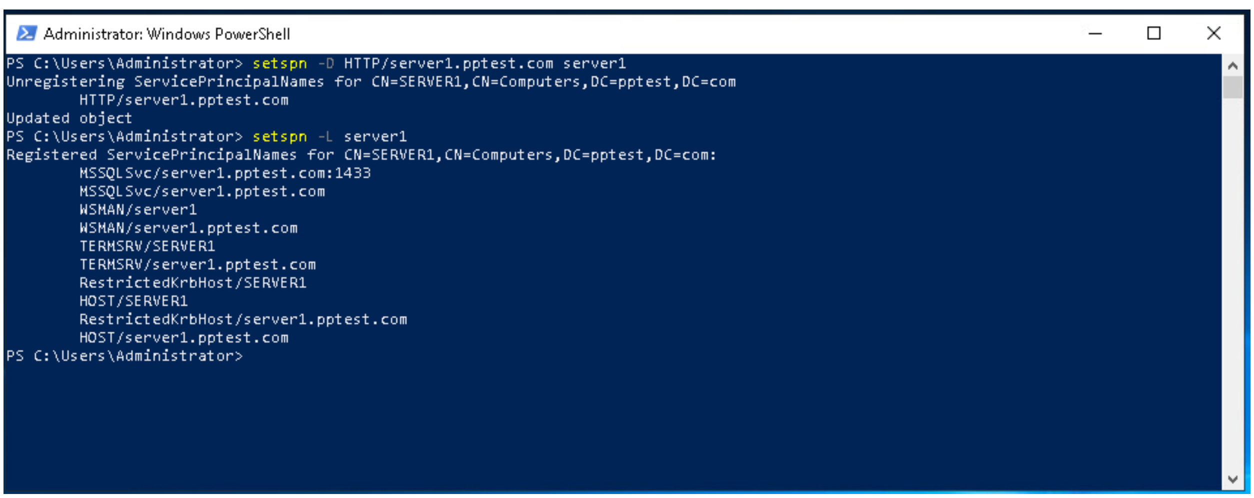


Remove a SPN

To remove an existing SPN, use the setspn command with the -D switch:

```
setspn -D HTTP/server1.testpp.com server1
```

The -D switch takes two arguments, where the first, HTTP/server1.pptest.com, is the SPN and the second, server1, is the accountname.



Restarting the client

If the HOST SPNs are missing, Kerberos will fail. Adding the missing SPNs should fix this.

After the SPNs has been added, the client must be restarted in order to pick-up the changes.

Kerberos error logging

If Kerberos authentication is not working, and you want to investigate what the issue is, you can enable logging of Kerberos-errors.

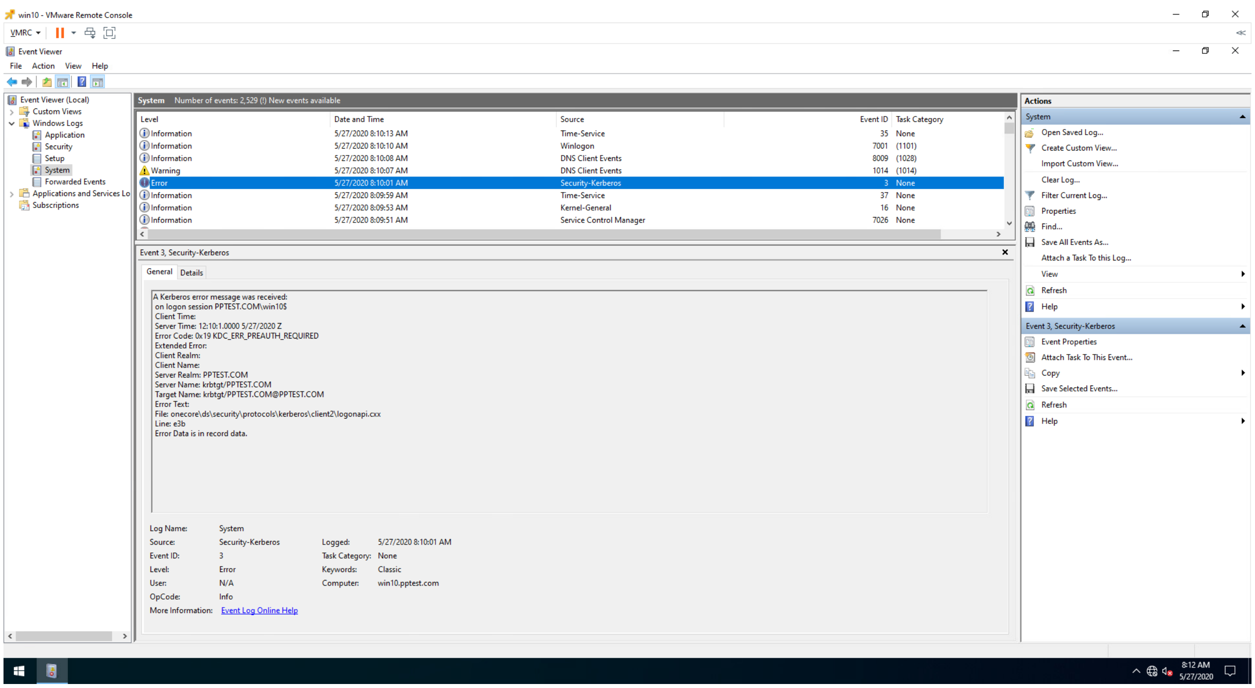
You enable logging of Kerberos errors by editing the Windows registry database:

1. Start the Registry Editor.
2. Add the following registry value:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters
   Registry Value: LogLevel
   Value Type: REG_DWORD
   Value Data: 0x1

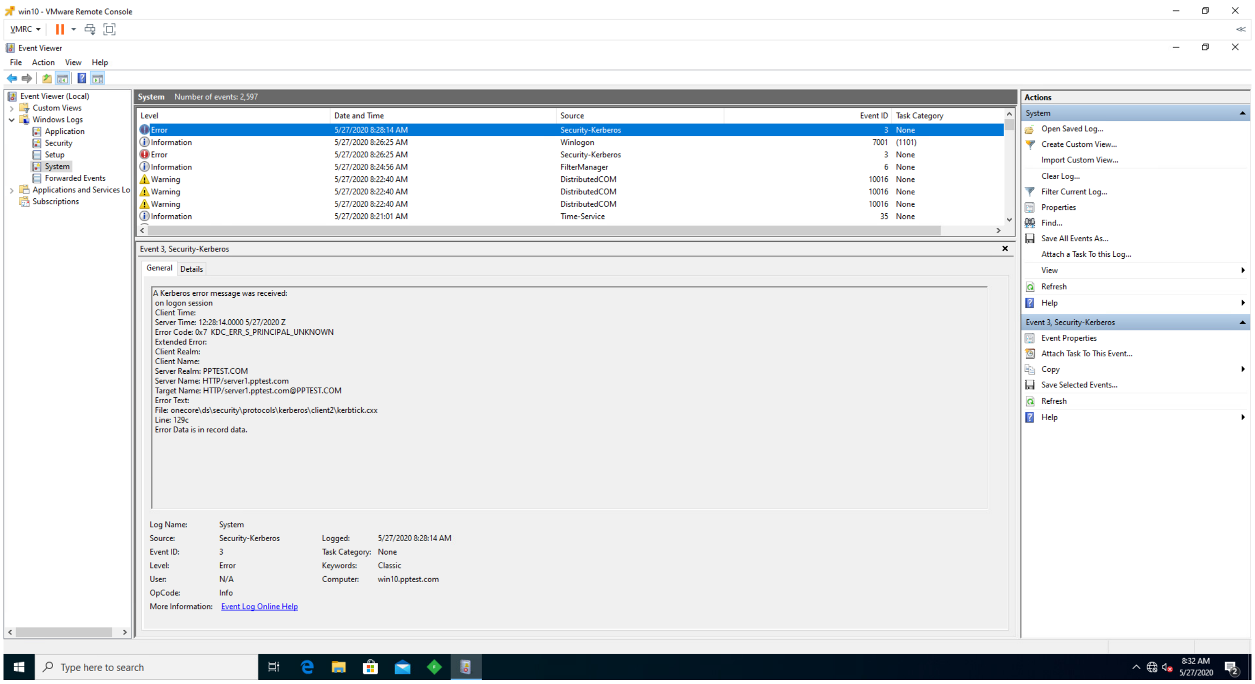
If the Parameters subkey does not exist, you must first create it.

Any Kerberos errors will now be written to the Windows event-log under System and with the Source Security-Kerberos.

Not all Kerberos errors are in fact actual errors, and in a system that functions correct with Kerberos, you should expect to see some “errors” that are an integral part of the login-process, such as KDC_ERR_PREAUTH_REQUIRED:



If Kerberos authentication fails because of missing SPN, we get a KDC_ERR_S_PRINCIPAL_UNKNOWN error:



Alternatively, KDC_ERR_C_PRINCIPAL_UNKNOWN, if it is the client that does not exist in the Kerberos database.

Appendix D: Multiple People Planner Systems

You use the People Planner Security Service to determine which DataConnection.xml file the People Planner Window Application should use.

Sometimes you want your users to be able to choose between several setups. This could be the case when you have both a test- or a training-system as well as the live production-system.

You can achieve this by installing one or more Security Services, or you can have one or more connection-sections in the DataConnection.xml-file, and you can combine both methods.

Breaking it down:

1. You can have one or more Security Services installed.
2. Each Security Service can have one or two DataConnection.xml files.
3. Each DataConnection.xml file can have one or more connection-sections.

Single People Planner Security Server

First, we consider the case with a single Security Service installed:

The People Planner Windows Application need to know where to call the Security Service.

The Security Service need to know where to find the People Planner Database.

Configuring the URL of the People Planner Security Service

When the software have been installed, the Windows Application needs to know the URL of the Security Service.

This is configured in the PeoplePlanner.exe.config file – which is found in the installation-directory of the Windows Application.

You should look for the PeoplePlannerSecurityService section:

```
<!-- Configure the URLs for the People Planner security service here -->
<PeoplePlannerSecurityService hideUrls="true" hideTestButton="true">
  <Services>
    <Service name="Default" url="https://INSERT_SECURITY_SERVICE_URL_HERE/SecurityService"/>
  </Services>
</PeoplePlannerSecurityService>
```

In this section, you should replace the URL with the one for where you installed the Security Service, e.g. to something like this:

```
<!-- Configure the URLs for the People Planner security service here -->
<PeoplePlannerSecurityService hideUrls="true" hideTestButton="true">
  <Services>
    <Service name="Default" url="https://10.4.9.173:5000/SecurityService"/>
  </Services>
```

```
</PeoplePlannerSecurityService>
```

> **Note:** It is important that the Security Service is installed under SSL (such as HTTPS) and not respond to HTTP – or else it does not provide any additional security as intended. See Appendix B: Securing the People Planner Security Service for details on how to do this.

Configuring the File Path of the DataConnection.xml File

The Security Service needs to know where the People Planner database is located, and it does this by looking up the information in the DataConnection.xml file.

As part of the introduction of the People Planner Security Service, the DataConnection.xml file was moved away from being in the Settings-folder under the People Planner Windows Application. Instead, you will now find it together with the installation of the Security Service (and the other People Planner web applications) on a path similar to the following:

C:\inetpub\People Planner Web Apps 3.9.2-3 \DataConnection.xml

> **Note:** The point of this is that the file has been moved away from the client-machines and over on the server-machine instead.

You do not necessarily have to place the file at the indicated path; if desired, you can place the DataConnection.xml file in a different location.

Therefore, the Security Service has its own configuration-file where you configure where it can find the DataConnection.xml file(s). Go to where the People Planner Security Service is installed, such as:

C:\inetpub\People Planner Web Apps 3.9.2-3\People Planner Security Service\

Edit the appsettings.Production.json file. This file has two settings, ServerDataConnectionFile and ClientDataConnectionFile:

```
"DataConnections": {
        "ServerDataConnectionFile": "..\\DataConnection.xml",
        "ClientDataConnectionFile": "..\\DataConnection.xml"
}
```

Normally these two settings will point at the exact same DataConnection.xml file (as in the above case), and in a location one folder over the installation folder of the Security Service itself. If this is where you want the file to be placed, then you do not need to do anything further.

Note: Only in very special cases would you need to have a different ServerDataConnectionFile- and ClientDataConnectionFile-version of the DataConection.xml.

The ServerDataConnectionFile-file holds the connection-information that the Security Service itself use to connect to the People Planner database and the ClientDataConnectionFile likewise holds the connection-information that that the People Planner Windows Application use.

So if:

- You need to have multiple connection-sections in the DataConnection-file, and …

- If you have two different DataConnection.xml files

Then, the connection-sections would have to go into the ClientDataConnectionFile-version of the DataConection.xml.

The DataConnection.xml file itself is exactly as it always has been, and it is created in the usual manner, using the Admin Tool.

Multiple People Planner Security Servers

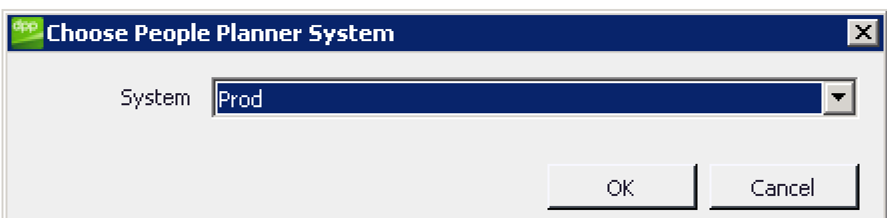
If needed, you can install multiple Security Servers, and each of their configurations would then be as described above.

Two or more Security Servers would operate independent of each other, and the only required change is that the People Planner Windows application would need a URL for each Security Server.

Edit the PeoplePlanner.exe.config file, and add each URL:

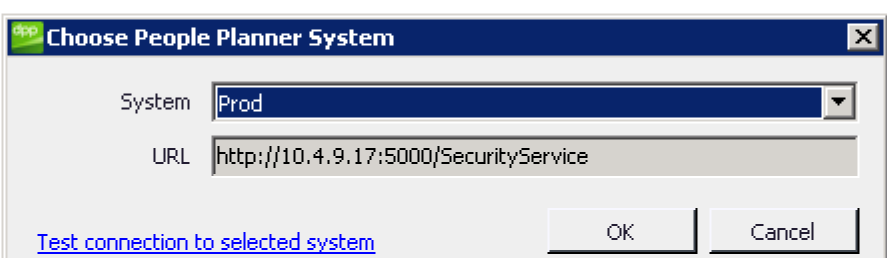
```
<PeoplePlannerSecurityService hideUrls="true" hideTestButton="true">
    <Services>
        <Service name="Prod" url="http://10.4.9.17:5000/SecurityService" />
        <Service name="Test" url="http://10.4.9.19:5010/SecurityService" />
    </Services>
</PeoplePlannerSecurityService>
```

In a setup with multiple Security Servers, the user (when starting the Windows application) would first be prompted about which Security Server to connect to.



Next, the selected Security Server would look in its ClientDataConnectionFile-version of the DataConection.xml file, and if multiple connection-section are present, it would now prompt the user for which one to connect the Windows application to.

You can use the settings, hideUrls and hideTestButton, to control whether the URL and Test connection buttons should be displayed in the dialog. For example, set hideURLs to false if you want to display the URLs:



Appendix E: People Planner MyPlan and Web Components Error Codes

A user can access MyPlan and the Web Components from the Maconomy WSC and from the Maconomy web client.

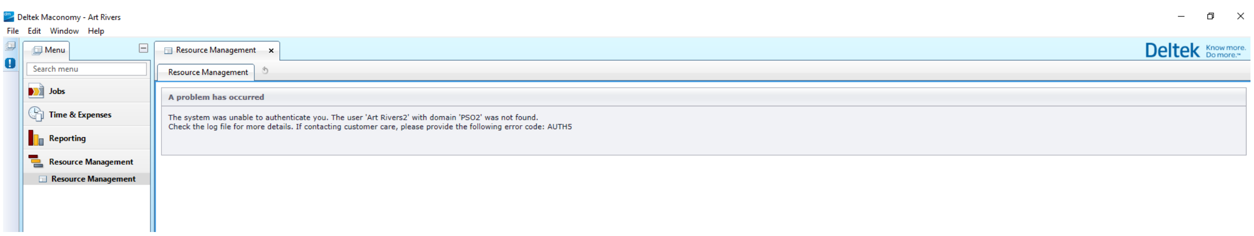
When a user tries to access either the embedded MyPlan or the embedded People Planner Web Components from the Maconomy Workspace Client, People Planner will try to authenticate the user through People Planner Silent Sign In (SSI).

> **Note:** See the *People Planner Integration Guide* for further information on how SSI works.

Likewise, when a user tries to access the MyPlan native in the Maconomy web client, or the embedded People Planner Web Components from the Maconomy web client, People Planner will try to authenticate the user using a JSON Web Token (JWT).

This appendix discusses the various error codes you might see in either the SSI- or the JWT-case.

If SSI or JWT fails, the user will be presented with an error message. The error-message consist of an error-code, and a message.



In addition to this, an error-message is written to the People Planner log, and should be accessible in the log-file of the People Planner Web Components or MyPlan. This error-message contains some of the more technical details about the problem.

This section lists the various error-codes, the error-message, and the technical error-message that is only available through the log-files.

SSI and JWT

AUTH1

The system was unable to authenticate you. The token passed to People Planner is either missing or invalid.

"Missing or invalid token (does not contain user and domain name). This error usually means that a token was expected but not found in the querystring. Another common issue is if the Maconomy user does not have the network user and domain names filled out."

AUTH2

The system was unable to authenticate you. User and domain name is invalid.

This error means that People Planner is configured to use UPN authentication, but the username and domain ('UserDomainName') in the token is malformed, as it must only contain one backslash. If integrating with Maconomy, check the user setup in Maconomy.

AUTH3

The system was unable to authenticate you. UPN user and domain name is missing.

UPN only error. This error means that People Planner is configured to use UPN authentication, but the username and domain ('UserDomainName') in the token is empty. If integrating with Maconomy, check the user setup in Maconomy.

AUTH4

The system was unable to authenticate you. UPN user and domain name is invalid.

UPN only error. This error means that People Planner is configured to use UPN authentication, but the username and domain ('UserDomainName') in the token is malformed, as it must only contain one ampersand. If integrating with Maconomy, check the user setup in Maconomy.

AUTH5

The system was unable to authenticate you. The user '{Username}' with domain '{Domain}' was not found.

This error means that the user could not be found in the People Planner database. If you get this error in the Web Components (WSC), it could mean that the token sent contains incorrect user information, or master data has not been imported recently. Check the network user and domain settings for the user in Maconomy.

AUTH6

The system was unable to authenticate you. The user session cookie value is invalid.

This error means that the session cookie value is used by a non-authenticated user trying to access the application.

Specific to JWT

JWT1

The system was unable to authenticate you. The JWT contains an invalid issuer.

This error means that the issuer in the JWT from Maconomy does not match the expected issuer in People Planner.

JWT2

The system was unable to authenticate you. The JWT contains an invalid audience.

This error means that the audience in the JWT from Maconomy does not match the expected audience in People Planner.

JWT3

The system was unable to authenticate you. The JWT has expired.

This error means that the JWT passed to People Planner has expired.

JWT4

The system was unable to authenticate you. The JWT is not valid yet.

This error means that the JWT passed to People Planner is not yet valid.

JWT5

The system was unable to authenticate you. Unable to validate the signature of JWT.

This error means that the signature of JWT passed to People Planner is not valid.

JWT6

The system was unable to authenticate you. Invalid JWT. See log for details.

This error means that the JWT failed validation.

JWT7

The system was unable to authenticate you. General exception trying to validate the JWT. See log for details.

This error means that an error occurred while validating the token.

JWT8

The system was unable to authenticate you. The JWT does not contain a valid name identifier claim.

This error means that the JWT received from Maconomy does not contain an identifier claim. This is normally due to missing Network UserName and Domain on the User in Maconomy.

JWT9

The system was unable to authenticate you. The format of the JWT 'sub' claim is invalid. It must contain exactly one '@').

This error means that the identifier claim in the JWT received from Maconomy does not contain an identifier claim. This is normally due to missing Network UserName and Domain on the User in Maconomy.

JWT10

The system was unable to authenticate you. The format of the JWT 'sub' claim is invalid. It is missing either user or domain name.

This error means that the JWT received from Maconomy does not contain a username and/or a domain name. This is normally due to missing Network UserName and Domain on the User in Maconomy.

Specific to SSI

TOK1

The system was unable to authenticate you. Unable to read security token.

Invalid token. This error means that the token cannot be used with this People Planner installation. Usually this indicates a wrong secret key configuration in either People Planner or Maconomy.

TOK2

The system was unable to authenticate you. Incorrect security token type.

Invalid token. This error means that a 'Request Token' was sent to People Planner instead of a 'Response Token'.

TOK3

The system was unable to authenticate you. Your session has expired, please refresh.

This error means that the security token passed to People Planner has expired. If this issue continues to impact you on a regular basis, the token validity period can be changed in the People Planner configuration.

TOK4

The system was unable to authenticate you. Missing user or domain name.

This error means that the token received from Maconomy does not contain both a username and a domain name. This is normally due to a missing Network UserName and Domain on the User in Maconomy.

OIDC

If People Planner MyPlan is configured to use OAuth 2 and OpenId Connect (OIDC), you may encounter the following error-codes.

OIDC1

The system was unable to authenticate you.

Unable to parse the response received from Maconomy REST. This error means that People Planner was unable to get the authorization URL because the response data from Maconomy could not be parsed.

OIDC2

The system was unable to authenticate you.

Failed to get a successful response from Maconomy REST. This error means that People Planner was unable to get the authorization URL because Maconomy REST did not respond successfully.

OIDC3

The system was unable to authenticate you.

General error trying to communicate with Maconomy REST. This error means that People Planner was unable to get the authorization URL because communication with Maconomy REST failed.

OIDC4

The system was unable to authenticate you.

Unable to parse the response received from Maconomy REST. This error means that People Planner was unable to get a PP JWT token from Maconomy because the response data from Maconomy could not be parsed.

OIDC5

The system was unable to authenticate you.

Failed to get a successful response from Maconomy REST. This error means that People Planner was unable to get PP JWT token from Maconomy because Maconomy REST did not respond successfully.

OIDC6

The system was unable to authenticate you.

General error trying to communicate with Maconomy REST. This error means that People Planner was unable to get PP JWT token from Maconomy because communication with Maconomy REST failed.

OIDC7

The system was unable to authenticate you.

This error means that the state param returned by the auth provider did not match the state param we sent to them. This is used to guard against certain types of attacks. Make sure that the auth provider is configured to support the state param.

OIDC8

The system was unable to authenticate you.

This error means that the auth provider did not return a state param or that the auth URL we got from Maconomy did not contain a state param. This is used to guard against certain types of attacks. Make sure that both the auth provider and Maconomy are configured to support the state param.

OIDC9

The system was unable to authenticate you.

Maconomy SSO OIDC authentication is not enabled. This error means that People Planner has not been configured to use Maconomy SSO OIDC. Enable it in People Planner settings using the AdminTool.

About Deltek

Better software means better projects. Deltek is the leading global provider of enterprise software and information solutions for project-based businesses. More than 23,000 organizations and millions of users in over 80 countries around the world rely on Deltek for superior levels of project intelligence, management and collaboration. Our industry-focused expertise powers project success by helping firms achieve performance that maximizes productivity and revenue. www.deltek.com