



P2[®] P2 Security 4.0
Installation Guide

P2 SECURITY

Installation Guide

First Edition (October 2014)

This edition applies to Version 4.0 of P2 Security and to all subsequent releases and modifications until otherwise indicated in new editions.

© P2 2014. All rights reserved.

40 Hasler Road, Osborne Park, WA, 6017, Australia
PO Box 1313, Osborne Park BC, Osborne Park, WA, 6916, Australia
Phone +61 8 9241 0300 • Fax +61 8 9242 8121

Reference herein to P2ES Holdings, LLC shall also include any affiliates thereof (collectively, "P2").

Use of this product and accompanying documentation is subject to the terms and conditions set out in the P2ES Holdings, LLC standard Master Agreement terms and conditions. All information contained in these Release Notes is the confidential and proprietary property of P2ES Holdings, LLC.

The products of P2 are not a primary alarming, machine health, or asset protection system. This function must be performed by low level SCADA / Control Systems or machine monitoring equipment. P2 products are provided for advisory, informational, optimisation and diagnosis purposes.

This information may change without notice. The information and intellectual property contained herein remains the exclusive property of P2. If you find any problems in the documentation, please report them to us in writing. P2 does not warrant that this document is error-free.

Through product maintenance, P2 endeavours to keep its applications up to date with major platform version changes as these platform changes are adopted by our customers. Examples include Internet Explorer 9, Oracle 11g, Microsoft Server 2008 R2. Whilst we cannot test our products against every service pack and patch within a whole third party version release, we publish minimum required major version number, and offer support in the event that a minor patch released by a third party vendor causes an issue.

For licensing and compliance purposes, P2 may track usage of this product by capturing the following details: IP address, date/time, action (such as login, logout, timeout). No personal data such as user ID or passwords are tracked or recorded in this process.

P2 Production Operations and the P2 Production Operation logos are either registered trademarks or trademarks of P2 (and/or its affiliates) in Australia and/or other countries.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

ActiveX, Active Directory, Authenticode, Excel, Internet Explorer, Microsoft, SharePoint, SQL Server, Visual Studio, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.



Contents

Preface	1
Who Should Read This Guide	1
Related Documentation	1
Help and Support	1
About P2 Security	3
Component Overview.....	3
Quick Start Cheat Sheet	4
Planning the Installation	5
Required Information.....	5
Hardware Requirements	5
Network and Hardware Setup	6
Supported Technologies	7
Software Prerequisites.....	8
Supplied Software	8
Installation	9
Fresh Installation.....	9
Step 1. Review Installation Requirements	9
Step 2. Install Prerequisites	9
Step 3. Install P2 Security	9
Upgrading.....	13
Upgrade Procedure	13
Rollback Procedure	14
Uninstall	14
Appendix A. Connecting to P2 Security	16
Appendix B. Running the Create Database Scripts.....	17
Appendix C. Dropping a Database.....	18
Appendix D. How to Select Features in IIS 8.5	19
Appendix E. Troubleshooting.....	22



Preface

This installation guide is provided to assist with the installation of P2 Security.

This document outlines:

- How to install the P2 Security components.
- How to configure P2 Security for use.

Who Should Read This Guide

This guide is intended for P2 analysts and developers, who need to install P2 Security. It assumes working knowledge of:

- Microsoft® Windows® operating system
- Microsoft® Internet Explorer®

Related Documentation

Documents in the P2 Security documentation suite are:

Title	Description
P2 Security Release Notes	Release notes for the current version of P2 Security.
P2 Security Installation Guide	How to install and configure P2 Security.
P2 Security User's Guide	How to use P2 Security to connect to applications and configure access for users of those applications.
P2 Security Developer's Guide	How to add support for P2 Security in various types of applications.

You may also find the following documents useful:

- ISS Log Viewer User's Guide

These documents are available from P2 Customer Support.

Help and Support

P2 Customer Support provides a central point of contact for software assistance and the resolution of software issues. As part of this, P2 offers a variety of professional services, online resources, and access to experienced product specialists who are able to assist with your service requests. For support and information regarding our products, the following resources are provided:

FREE DOCUMENTATION RESOURCES

- PDF documentation supplied in the installation directory.
- Online help provided with the product (if supplied).

ONLINE SUPPORT PORTAL

The P2 Support Portal (<http://p2energysolutions.com/support>) provides access to online support, where you can raise service requests for P2 software, track defects, get product information, and communicate with P2 Customer Support.



CUSTOMER COMMUNITIES

P2's customer communities offer a networking environment for you and other P2 users. Our boards and user groups offer an informal setting to exchange information and discuss issues relevant to today's oil and gas companies. P2 is confident that together, we can create an interactive venue that will provide value by allowing our customers to communicate, collaborate and connect at multiple levels. For details, see www.p2energysolutions.com/services/customer-communities.

TRAINING

P2 offers a variety of standard and customised training courses (ranging from introductory courses through to administrator courses) to help you learn how to use P2 products.

PERFORMANCE TUNING

P2 offers a series of system checks to make sure your P2 systems are running as efficiently as possible.

YOUR FEEDBACK

To help improve what we offer you, P2 would like your feedback about this guide. Please send your comments by email to P2 Customer Support, specifying the name of the guide, as well as section headings or page numbers for our reference.

CONTACT DETAILS

You can contact P2 Customer Support via phone or email for technical support on any aspect of P2's products. Please also contact P2 Customer Support for further information on the Customer Communities, access to the online support portal, Performance Tuning services, and information on available training courses. Feedback on our products or user guides can also be sent to P2 Customer Support.

Phone: 1300 739 969 (Australia only)
+61 8 9241 0314 (outside Australia)

Email: support@issgroup.com.au or iss.support@p2energysolutions.com

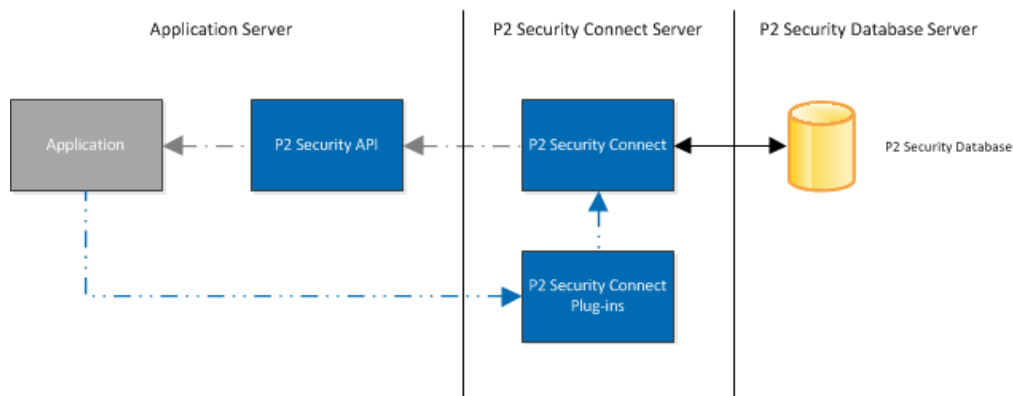
About P2 Security

P2 Security is a common component that provides consistent user authorisation functionality for applications developed by P2.

The security mechanisms are provided to handle user authentication, verification of privileges of individual users and user groups, and to limit users' access to specific business areas or dialog windows within applications.

Component Overview

There are three main components provided in P2 Security.



P2 Security Database

The centralized database which stores connection information.

P2 Security Connect

The web application or Windows service which is responsible for performing operations on the database.

P2 Security API

The client-side P2 Security API libraries allow other applications to communicate with P2 Security Connect.

Quick Start Cheat Sheet

Here is a rundown of the installation process for those who wish to view a summary of the main instructions.

Note: If you encounter any issues during installation, refer to the complete linked instructions.

- ☐ Collect your [database connection information](#).
- ☐ [Review](#) and [install](#) the prerequisites.
- ☐ Ensure [IIS](#) is correctly configured.
- ☐ Install [P2 Security](#).

Planning the Installation

This section describes the requirements for installing and configuring P2 Security. Before you start the installation, make sure your system will support P2 Security.

Required Information

You need the following information to install P2 Security. Complete the table below with the parameter values needed for this installation. You will need these values to complete the database configuration.

Information required	Scripts Parameter	Example
Database instance	DBServer	(local)
DBA user name	DBAUser	sa
DBA user's password	DBAUserPassword	password
Database catalog	Database	SEC
Database user	DatabaseUser	SEC_OWNER
Database user's password	DatabaseUserPassword	password

Hardware Requirements

The following hardware infrastructure is required for P2 Security:

- Database server
- Application server
- Client system

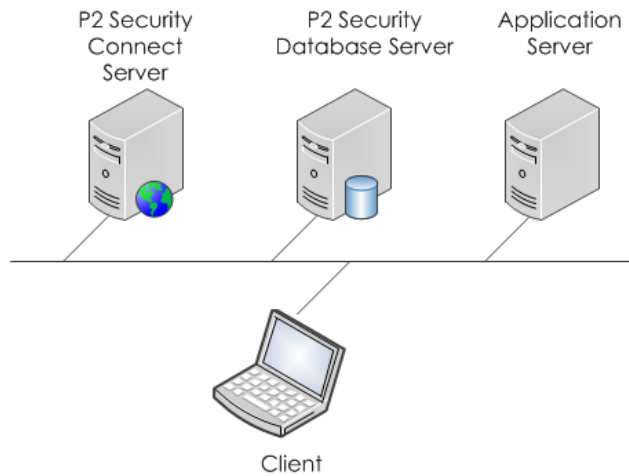
All of these systems can utilize the same physical or virtual machine. P2 Security does not have any specific requirements and it can share a single environment with other products.

The following hardware configuration is recommended. Particular requirements depend on the applications that use P2 Security:

Component	Recommended
CPU	2 x Intel® Xeon® class E or L5000/7000 series or better
RAM	16 GB+
Disk	4x 146GB 15000 rpm SAS, configured in RAID 5,10
NIC	1000 MBit/sec +

Network and Hardware Setup

The following diagram illustrates the recommended server configuration.



The servers as show in the diagram are:

P2 Security Connect Server

This is the application server on which P2 Security is installed. This may be located on the same machine as the P2 Security database, or other P2 products, depending on the site configuration.

P2 Security Database Server

This is the machine on which the P2 Security database is created. This may be the same physical machine as the P2 Security Connect Server, or other P2 product databases, depending on the site configuration.

Application Server

Other P2 products that use P2 Security must be installed on the same network as P2 Security.


Client

Workstations on which a browser is installed, for access to the P2 Security web interface, which is where administrators can configure security permissions.


Supported Technologies

The following list displays the technologies currently supported in P2 Security, and the planned support and deprecation in future releases. We recommend that all customers keep their databases and operating systems current with patches and security fixes for the supported versions.















KEY:

 P2 does not warrant or support these platforms, this usually includes the very new and the very old.















 P2 does formal testing on these platforms and warrants and fully supports these installations.

 P2 generally supports these platforms/technologies outside of product maintenance; however no exhaustive testing is performed by P2 and if any major issues arise then it is recommended that only supported technologies are used.

CLIENTS

Technology / Version	3.0	4.0
Windows 7		
Windows 8		
Internet Explorer 8.0 (32-bit)		
Internet Explorer 9.0 (32-bit)		
Internet Explorer 10.0 (32-bit)		
Internet Explorer 11.0 (32-bit)		
Google Chrome 36 and later		

SERVERS

Technology / Version	3.0	4.0
Windows Server 2008 R2		
Windows Server 2012 R2		
SQL Server 2008 R2		
SQL Server 2012 R2		
Oracle 11g R2		
IIS 7.5		
IIS 8.5		

Software Prerequisites

Software prerequisites are as follows:

SERVER MACHINE

- ☐ Microsoft® Windows® Server® 2012
- ☐ Microsoft® IIS 8.5
*See [Appendix D](#) for roles and features that need to be installed.
- ☐ Microsoft® .NET Framework 4.5
- ☐ Microsoft® SQL Server® 2012
- ☐ ISS Logger 2.0.26
- ☐ ISS Log Viewer 2.0.26

CLIENT MACHINE

- ☐ Microsoft® Internet Explorer® 11

Note: We recommend that the latest version updates of any software is installed where possible to take advantage of improved functionality. Check the software's release notes for any compatibility issues.

Supplied Software

With this installation, the following items are present on the installation disc. No other software is required from third party vendors.

DOCUMENTS

- P2 Security Installation Guide
- P2 Security User's Guide

BINARIES

- P2 Security installer (*P2 Security.exe*)

Installation

This section describes the procedure for installing the P2 Security components, and how to install and configure the databases required.

Fresh Installation

Installing P2 Security consists of the following steps:

- Step 1.** Review the installation requirements.
- Step 2.** Install the prerequisites.
- Step 3.** Install P2 Security.

These steps are described in the following sections.

Step 1. Review Installation Requirements

- 1. Gather the [required database information](#).
- 2. Review the [software prerequisites](#).

Step 2. Install Prerequisites

The following software is included in the P2 Security installation package and must be installed on the web server before installing P2 Security.

Install the following software:

- 1. ISS Logger 2.0.26 API (**LoggerAPI.msi**)
- 2. ISS Log Viewer 2.0.26 or later (**ISSLogViewerSetup.msi**)

Note: Refer to the [ISS Logger User's Guide](#) for further information.

Step 3. Install P2 Security

The P2 Security installer installs the P2 Security software and database.

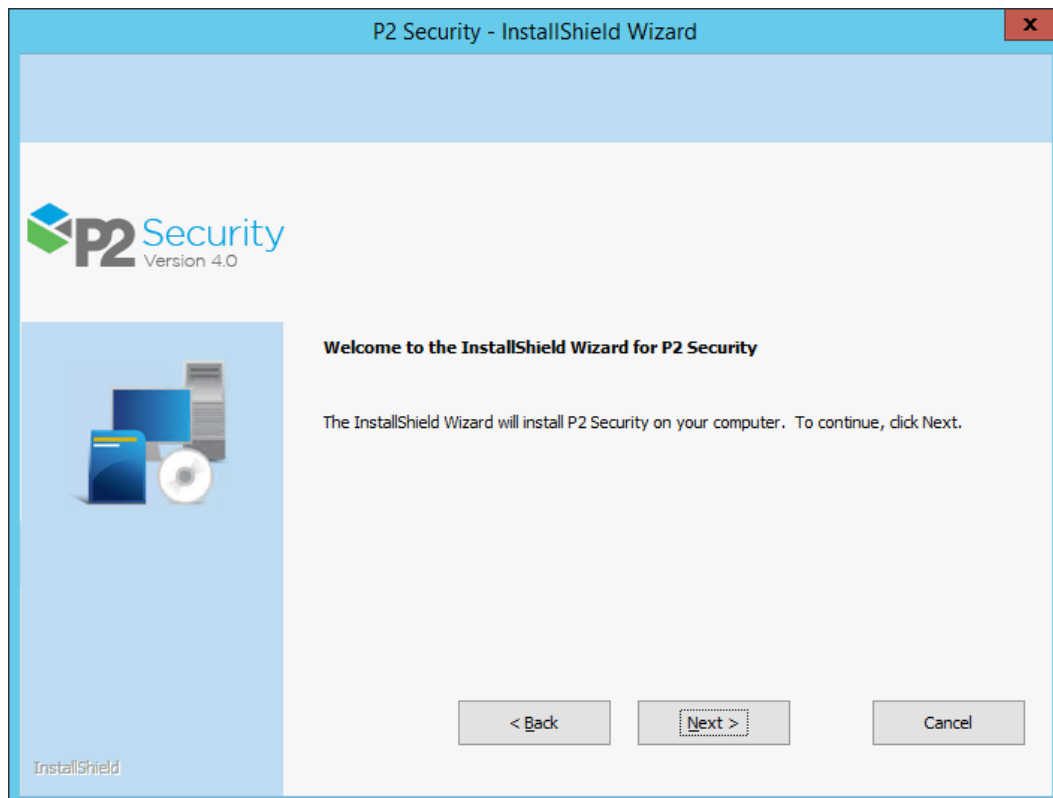
Note: You can install multiple instances of P2 Security on the one machine using the same installer. The installer must have administrative rights to the local machine.

To run the installer:

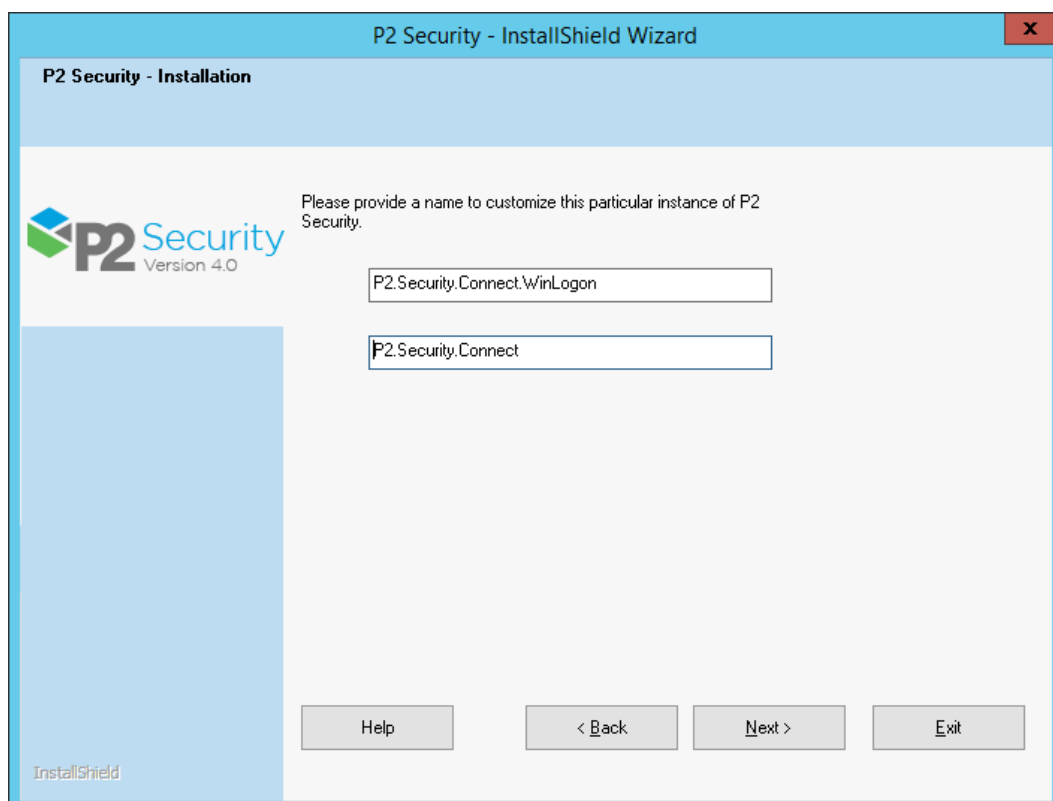
- 1. Double-click **P2 Security.exe**.

The InstallShield Wizard prepares the setup, and then displays the welcome page.





2. Click **Next**.

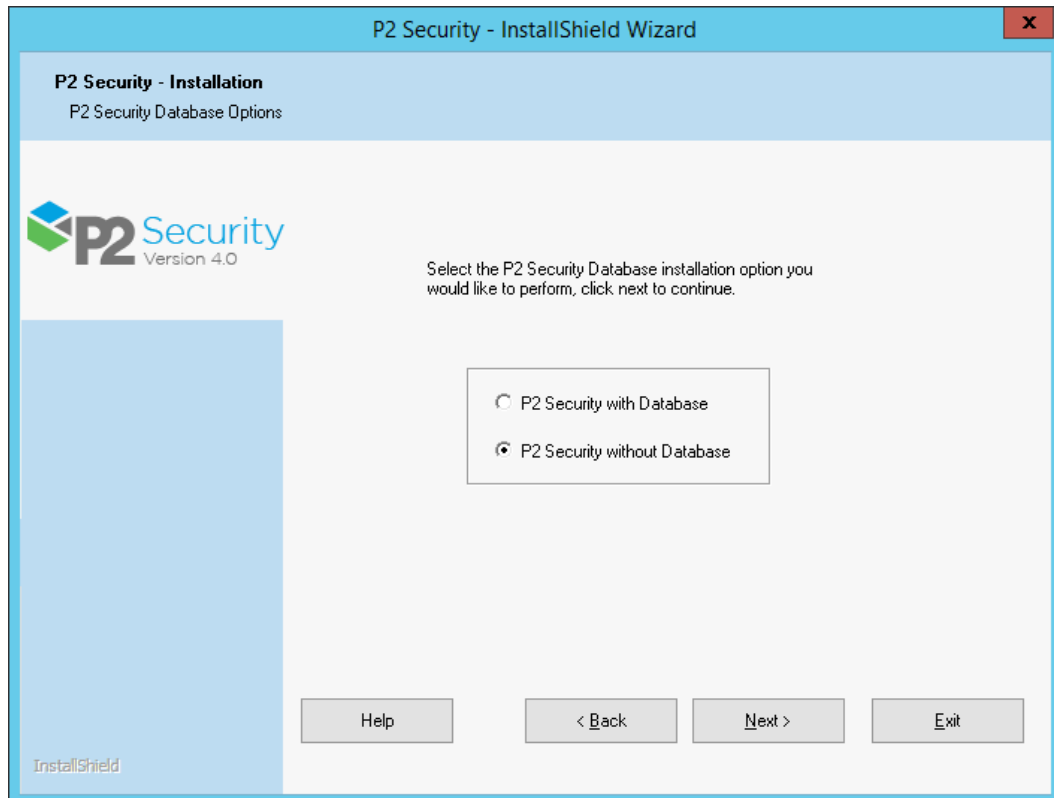


3. In the Installation screen, enter the following:

Authentication page: The first field is the domain authentication page (for Windows authentication), which on successful authentication creates a user session and redirects the user to the other application. **Default.** P2.Security.Connect.WinLogon

Application name: The second field is the name of the main web application of P2 Security Connect (which uses anonymous authentication). This is the name which will form part of the URL that will be used by other applications to connect to P2 Security. **Default:** P2.Security.Connect

4. Click **Next**.



5. In the Database Options screen, choose whether to install both the application and the database, or only the application.

If you do not want to install the database at this point in time, a DBA user with create privileges will need to run the database create scripts after the software has been installed (see [Appendix B](#)).
6. Click **Next**.
7. If you have elected to install the database, specify the following:

Database server you are installing to:

- Type in the name of the database server ; or
- Select the name from the drop-down list. You can choose (local) if the database is to installed on the same machine as the web server; or
- Click **Browse** to select the database.

Connect Using:

Supply the login ID and password to connect to the database.

Name of database catalog:

Type a name for the new catalog to be created.

8. Click **Next**.

FILE DIRECTORY STRUCTURE

When you install P2 Security, the following default file directory structure is created on your computer:

```

..P2 Energy Solutions
 | P2 Security
  
```

Upgrading

- ▶ Before upgrading, make sure you first back up your existing databases, web directories, and other customisations.

Note: You may install multiple instances of P2 Security on the same machine. If you wish to install a new instance using a new database, follow the instructions for [Fresh Installation](#).

Upgrade Procedure

This topic describes the procedure for upgrading an existing P2 Security database.

1. Back up the database and any modified configuration files found in the installation directory.
2. [Uninstall](#) the previous version of the software. You can do this using the new installer.
3. After the software has been uninstalled, run the installer again (double-click **P2 Security.exe**).

The InstallShield Wizard prepares the setup, and then displays the **Installation** page.

4. Click **Next**.
5. In the **P2 Security Instance Name** screen, type the name of the P2 Security instance.

This is the name of the directory that will be created in the destination folder when P2 Security is installed.

6. Click **Next**.

The **Installation Options** screen appears.

The options are:

Create a database: Select this option to create a new database for this version of the software. This option allows you to install multiple instances of the software alongside each other.

Upgrade an existing database: Select this option if you want to perform a standard upgrade, which will install the new version of the software and allow you to specify the database settings at the same time.

Do not select a database: Select this option if you want to install the new version of the software, but you do not have DBA privileges for updating the database. Another user can then make the required database changes at a later time.

7. For standard upgrades, choose **Existing Database**, and then click **Next**.

The **Database Server Login** screen appears.

8. Specify the following (refer to [Required Information](#)):

Database server you are installing to:

- Type in the name of the existing database; or
- Select the name from the drop-down list. You can choose (local) if the database is to be installed on the same machine as the web server; or
- Click **Browse** to select the database.

Connect Using:

This is the authentication method used to log in to the database.

- Windows authentication; or
- SQL Server authentication. If this is selected, provide the DBA user name and password.

Name of database catalog:

Type the name of the existing catalog, or click **Browse** to choose one from a list. If you type a name that is different to the existing database catalog, a new database will be created.

9. Click **Next**.

By default, P2 Security installs to `C:\P2\P2.Security\`.

The last folder will be named the same as the instance name specified above.

10. Click **Change** to select a different destination folder, if your previous installation was on a different path.
11. Click **Next**.
12. In the next screen, select the **Website Name** from the drop-down list. E.g. P2.Security.Connect
13. Click **Next**.
14. Click **Install**.

P2 Security installs. The installation will usually only take a few seconds.

15. When the installer has finished, click the **P2 Security** link to launch P2 Security.
16. Click **Finish** to close the wizard.

You should not need to change anything, but be aware of any new objects that may appear.

Rollback Procedure

1. [Uninstall P2 Security](#).
2. [Install the previous version of P2 Security](#).
3. Restore the database from backup.
4. Restore the configuration files from backup.

Uninstall

After you have run the **P2 Security.exe** installer, running this again offers you the options of changing your installation, repairing your installation, and removing your installation.

To run the installer:

1. Double-click **P2 Security.exe**.

The InstallShield Wizard prepares the setup, and then displays the **Existing Installed Instances Detected** screen.

Note: You can bypass the InstallShield wizard through the **Program Features** utility (**Start > Control Panel > Programs and Features**). Double-click **P2 Security** in the list of installed programs to completely remove the application.

2. Select the “**Maintain or update**” option, and then select the instance that you want to uninstall.
3. Click **Next**.

InstallShield prepares the setup and displays a welcome screen.

The following options appear:

- **Modify:** The Modify option allows you to change the installed components. Since the P2 Security installation requires a complete installation of all components, this option is not applicable.
 - **Repair:** Repair allows you to fix any errors that may have occurred in the most recent installation. It fixes missing and corrupt files, shortcuts, and registry entries.
 - **Remove:** Remove allows you to remove P2 Security and all associated files and features from your computer. You should not do this until you have spoken to P2 Customer Support.
4. To uninstall P2 Security, select **Remove** and then click **Next**.
 5. At the confirmation prompt, click **Yes**.
- The InstallShield wizard removes P2 Security.
6. When the uninstall has been completed, click **Finish**.

Note: The installer will not remove the P2 Security database. If you want to remove the database, you must do this manually, following the instructions in [Appendix C](#).

Appendix A. Connecting to P2 Security

Other P2 products (such as P2 Explorer) will need to connect to P2 Security in order to set permission access levels for users.

Those products will require the following information in order to connect.

URL

- ▶ In the following URL, replace the [servername] placeholder with the name of the machine on which P2 Security is installed.

URL Required	Description	Value
P2 Security	The URL used to open the P2 Security web interface. You will also need the password to connect to P2 Security.	https://[servername]/P2.Security.Connect Note: This is the default value. Refer to point 3 in Step 3 to check if the path is different to the default.

CONNECTION STRINGS

Applications using P2 Security must specify a connection string for P2 Security using ODBC format. Below is an example of a connection string using the configuration details from [Required Information](#):

SQL Server

```
Driver={SQL Server};Server=(local);Database=SEC;  
Uid=ISS_OWNER;Pwd=password;
```

Appendix B. Running the Create Database Scripts

If you did not create a database during initial installation, you will need a DBA user to run the scripts required to create the database and tables. These scripts will be located in the following folder:

`C:\Program Files (x86)\P2 Energy Solutions\P2 Security\SQL Scripts`

You must match the settings specified in [Required Database Information](#).

For a Microsoft SQL Server database, the default file location is:

`C:\Program Files (x86)\P2 Energy Solutions\P2 Security\SQL Scripts\Microsoft SQL Server\CreateDatabase.bat`

The **CreateDatabase.bat** file expects the following command-line arguments:

InstanceName

Name of the database server instance where the P2 Security database has to be created.

DBAUser

Name of the DBA user which will be used to create the P2 Security database.

DBAUserPassword

Password of the DBA user.

Database

Name of the P2 Security database to create.

DatabaseUser

Name of the P2 Security user accessing the database to create.

DatabaseUserPassword

Password of the P2 Security user accessing the database to create.

For example:

```
CreateDatabase.bat (local) sa sa_password SEC SEC_OWNER password
```

After the script has run successfully, the database installation is complete.

Appendix C. Dropping a Database

The P2 Security database and user account can be dropped by using the **DropDatabase.bat** batch file, located in:

`C:\Program Files (x86)\P2 Energy Solutions\P2 Security\SQL Scripts`

For a Microsoft SQL Server database, the default file location is:

`C:\Program Files (x86)\P2 Energy Solutions\P2 Security\SQL Scripts\Microsoft SQL Server\DropDatabase.bat`

The **DropDatabase.bat** file expects the following command-line arguments:

InstanceName

Name of the database server instance where the P2 Security database has to be dropped.

DBAUser

Name of the DBA user which will be used to drop the P2 Security database.

DBAUserPassword

Password of the DBA user.

Database

Name of the P2 Security database to drop.

DatabaseUser

Name of the P2 Security user accessing the database to drop.

For example:

```
DropDatabase.bat (local) sa sa_password SEC SEC_OWNER
```

After the script has run successfully, the database removal is complete.

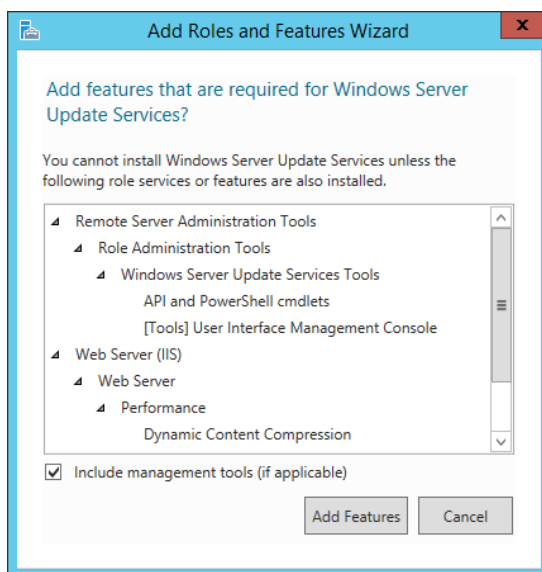
Appendix D. How to Select Features in IIS 8.5

In Windows Server 2012, the default IIS settings have changed. When installing P2 Security onto a newly installed server, ensure the following IIS roles and features are **turned on**.

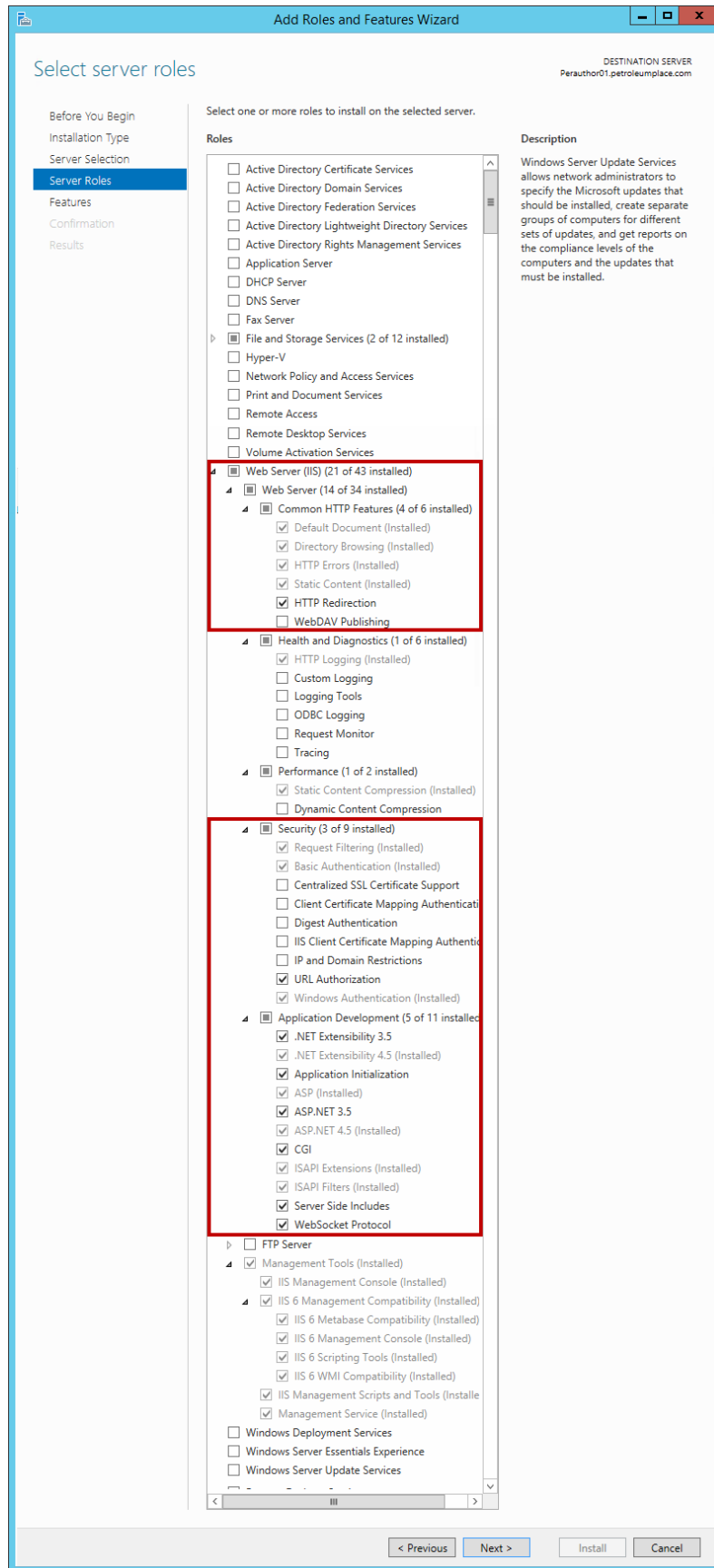
To turn the IIS roles and features on:

1. In the Server Manager, click **Add roles and features** in the Dashboard.
2. In the **Add Roles and Features Wizard**:
 - a. On the Before You Begin Page (if displayed), click **Next**.
 - b. On the Installation Type page, select **Role-based or feature-based installation**, and then click **Next**.
 - c. On the Server Selection page, select the server you are installing onto, and then click **Next**.
 - d. On the **Server Roles** page, select **Web Server (IIS)**.

Note: As you select some roles, an additional dialog box may appear, prompting for installation of additional features. In each case, click **Add Features** to accept. The dialog box will look something like this example below (note this example is not a required feature).

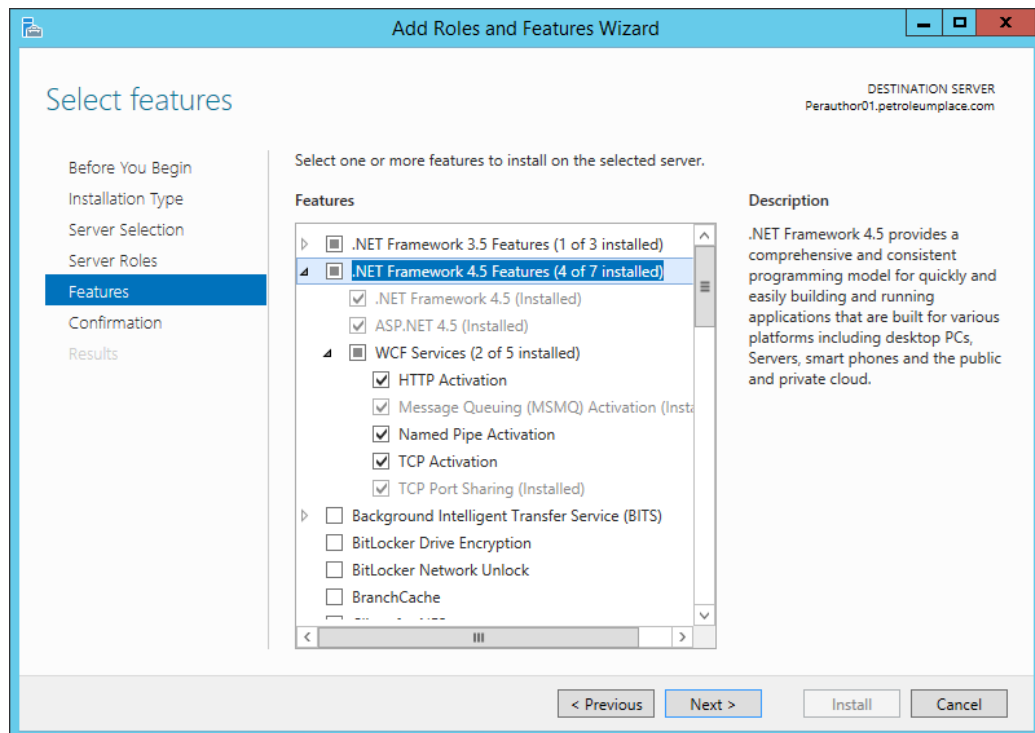


- e. Select the following roles:
 - **Web Server (IIS) > Web Server > Common HTTP Features:** select all options except WebDAV
 - **Web Server (IIS) > Web Server > Security:**
 - Request Filtering
 - Basic Authentication
 - URL Authorization
 - Windows Authentication
 - **Application Development:** select all options.
 - **Management Tools:** select all options



f. Click **Next**.

- g. In the **Features** screen, select ALL of the **.NET Framework 4.5 Features**, and then click **Next**.



- h. In the **Confirmation** screen, check that you have selected all the required features, and then click **Install**.

The installation may take a few minutes.

- i. Click **Close** when the installation has finished.
3. In the Server Manager toolbar, click **Tools > Services**.
 4. Change the **Startup Type** of the **Net.Tcp Port Sharing Service** to **Automatic**.

Appendix E. Troubleshooting

There are no troubleshooting topics at this time.