Siemens Opcenter Advanced Planning and Scheduling (Opcenter APS) 18.5

Installation Guide

Website

Revision 74920

Table of Contents

Siemens Opcenter Advanced Planning and Scheduling (Opcenter APS) 18.5 ..... **1**

Installation Guide 1

Table of Contents **2**

Installing **3**

Introduction 3

Installation Options 3

Installing SQL Express 3

Local Instance 4

Remote Instance 4

Installing Opcenter Advanced Planning and Scheduling (Opcenter APS) 4

Upgrading Opcenter Advanced Planning and Scheduling (Opcenter APS) 4

Customization Upgrades 5

Repairing Opcenter Advanced Planning and Scheduling (Opcenter APS) 5

Uninstalling Opcenter Advanced Planning and Scheduling (Opcenter APS) 5

System Requirements **6**

License Warning **7**

Security Information **8**

Data Protection by Design Aspects of DI SW MOM Products and Solutions **9**

Installing

Introduction

This guide provides information on the process for installing and running Opcenter Advanced Planning and Scheduling (Opcenter APS).

Whether running a trial version of Opcenter APS or have purchased a license, the installation package is the same. When using a trial of Opcenter APS, trial mode will only run for 30 days from its first run. When a license has been purchased, you will need to have that license activated.

In order to install a full version of Opcenter APS for the first time,the following steps need to be taken:

1. Ensure prerequisite SQL Server instance is available from Microsoft - the minimum required version is **SQLEXPRESS 2008R2**.
2. Install Opcenter APS by opening the installation package and following the on-screen instructions.

At this point Opcenter APS can be run in trial mode for up to 30 days.

3. Order and obtain an Activation Code.
   This can be for a single user/system, or a multi-user network license.
4. If a **Network License** has been purchased, download and install the **Network License Manager**.
5. Use the license utility to enter the activation code.
   If you are using a trial, you will be prompted by the license utility every time Opcenter APS is run. Alternatively you can enter the activation code by opening the license utility from the **Start Menu**. For network license servers, the activation code should be entered on the server using the network license utility.

   Opcenter APS is now able to be run.

If the 32-bit version of Opcenter APS is required, it is available on request from the Support Website.

Installation Options

This installation guide will walk you through the simplest deployment scenario where Opcenter Advanced Planning and Scheduling (Opcenter APS) is installed locally. No knowledge of Microsoft SQL Server is required in this scenario.

For deployment scenarios where the SQL Server and/or SQL Server Reporting Services are to be accessed over the network, please contact your IT department.

Installing SQL Express

Opcenter Advanced Planning and Scheduling (Opcenter APS) requires a connection to a SQL Server instance in order to deploy databases and to use as a persistent store. You may use a pre-existing instance of SQL Server either locally or on the network. If you have downloaded a stand-alone installation of Opcenter APS, or if you prefer to use a later version of SQL Express, you may download it from the SQL section of the Microsoft Website.

Tip: Please see the Microsoft SQL Documentation: Install SQL Server from the Installation Wizard (Setup) for detailed guidance installing and configuring SQL Express.

Local Instance

The default deployment case for Opcenter APS is a local instance of SQL Server Express Edition. For this type of deployment, the default server configuration options are suitable.

Remote Instance

Any supported edition of SQL Server may be used and can also be deployed remotely. Remote deployment of SQL Server should be performed according to best practices and should only be done where compliant with network and organization policy.

Note: When deploying SQL Server for use with Opcenter APS on a remote server, in order to ensure integrity of data and deny any possibility of data being compromised or tampered with, due care and consideration should be taken to ensure that all communications between the Opcenter APS application and the SQL Server are encrypted.

Installing Opcenter Advanced Planning and Scheduling (Opcenter APS)

Opcenter APS can be installed by downloading from the web site. This install does not include any prerequisite software, which must be downloaded separately if required.

- Installing from the Web Installer:

1. In Windows Explorer, double-click the .exe file.
2. Follow the on screen instructions.

If upgrading, the upgrade is recognized when Opcenter APS is run and some additional options are available to the user at that point.

When (re)installing or upgrading, any existing configuration will be maintained. Upgrading the configuration is done by Opcenter APS when it is run. See "Upgrading Opcenter Advanced Planning and Scheduling (Opcenter APS)" below.

Upgrading Opcenter Advanced Planning and Scheduling (Opcenter APS)

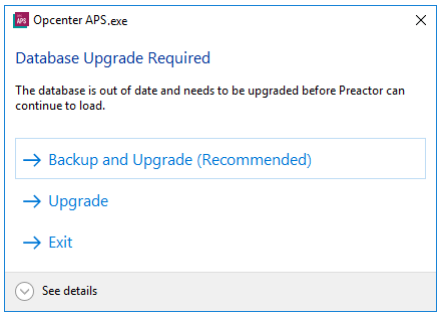
The procedure for upgrading Opcenter APS is the same as for an initial install. "Installing Opcenter Advanced Planning and Scheduling (Opcenter APS)" above.

Any configuration that works with Preactor 10.0 or later can be upgraded to this release.

Note: It is strongly advised that you take a backup of your configuration before upgrading (i.e. create a configuration package).

Once Opcenter APS is installed, any existing configuration may be opened. To do so, start Opcenter APS in the normal way, selecting the required configuration.

At this point, it is likely that a set of upgrade tasks need to be performed. The greater the difference between the version of Opcenter APS last used with the configuration selected and the version being used now, the greater the number of upgrade steps that will be performed. Before the upgrade steps are executed the following options are offered:



- Backup and Upgrade
  Opens the Configuration Package Manager, allowing a configuration backup to be taken before the upgrade steps are performed.
- Upgrade
  Performs the upgrade steps without taking a backup of the configuration.
- Exit
  Close Opcenter APS without performing any upgrade steps.

Warning: Once an upgrade step has been performed, it may not be undone. Taking a backup of a configuration prior to performing any upgrade steps is recommended for this reason.

Customization Upgrades

Where additional work may be required due to customization, refer to your partner for support.

Repairing Opcenter Advanced Planning and Scheduling (Opcenter APS)

If the files installed with an application have been altered in some way, it is possible that the application will be rendered inoperable or will exhibit unexpected behavior. For this reason many applications, including Opcenter APS, include a repair facility to return the installed application to its expected state.

To repair an existing installation of Opcenter APS, either re-run the installation wizard from the installation media and choose the Repair option or select the repair option presented when selecting Opcenter APS from the list of installed programs in the 'Programs and Features' control panel application.

Repairing an existing installation will replace any missing or corrupt files and re-create any shortcuts.

Uninstalling Opcenter Advanced Planning and Scheduling (Opcenter APS)

Opcenter APS is uninstalled using the Windows utility, found under **Start ►Control Panel ►Program and Features**, or by running the Opcenter APS executable downloaded from the Opcenter APS web site, selecting the option to remove the software.

Uninstalling Opcenter APS does not removed any of the configuration files.

No configuration files will be overwritten by the (re)installation of Opcenter APS.

Be sure to take a back-up copy of any configurations you wish to keep.

System Requirements

Your computer should meet the following system requirements for running Opcenter Advanced Planning and Scheduling (Opcenter APS).

Operating System	Windows® 7 SP1[1] Windows® 8.1[1] Windows® 10[1, 2] Windows Server® 2012 Windows Server® 2012 R2 Windows Server® 2016 Windows Server® 2019
Supported Platforms	x86[3], x64
Microsoft® .NET Framework Version	4.8[4]
Microsoft® SQL Server	2008 R2 or later(any edition including Express)[5]
Microsoft® Visual C++ Runtime	Visual C++ Runtime 2017[6]
Processor	2 GHz or better
Memory	1 GB RAM (2 GB recommended)
Disk Space	A minimum of 1 GB free disk space is required for installation A minimum of 2 GB free disk space is required for .NET Framework version 4 installation on a 64 bit platform.

1. Opcenter APS can be installed on any edition of Windows, but an SQL Server Reporting Services (SSRS) server may only be installed on editions where Internet Information Services (IIS) is supported.
2. Windows® 10 version 1607 or later.
   On editions that do not support IIS, only local reporting is possible.
3. x86 (32-bit) is available from the Support Website.
4. Microsoft® .NET Framework Version 4.8 will be installed by the Opcenter APS installation program if it is not already installed.
5. Microsoft® SQL Server will need to be downloaded and installed. It is not provided with the Opcenter APS installation.
6. Microsoft® Visual C++ Runtime will be installed by the Opcenter APS installation program if it is not already installed.

License Warning

Opcenter Advanced Planning and Scheduling (Opcenter APS) is licensed using a system that entitles the user to execute the software. While every effort has been made to ensure the continued operation of your Opcenter APS software, it is the case that certain operations may compromise the integrity of the license entitlement and render the system inoperable.

Such operations include, but are not limited to, amending system or installation files, deleting or moving those files or imposing policies that restrict access to those files and / or the system registry.

In order to avoid such issues, you must perform all operations on your license entitlement using the included License Utility, or Server License Utility for network licenses. Under no circumstances should you attempt to duplicate, move or remove a license entitlement by any other means, and any attempt to tamper with license entitlements is strictly prohibited. Any such attempts will render the system inoperable.

In the event that the integrity of the license entitlement is compromised, a manual administrative procedure must be performed. For customers not under current maintenance there is an administrative charge associated with this service.

Although Flexnet licenses can be installed on Virtual Machines, it is strongly recommended that the Server License Utility and network licenses are installed on a physical machine. Due to the nature of virtual environments, changes to the environment can cause a license to become inoperable.

For instructions on the correct procedures for removing and returning licenses, refer to Move a License and Return a License.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement - and continuously maintain - a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.-com/industrialsecurity.

Version 4.5 - 17-04-2019- Siemens AG, I IA L CG, Nuremberg

Data Protection by Design Aspects of DI SW MOM Products and Solutions

In the course of development of DI SW MOM Products and Solutions, DI SW MOM follows the

“Data protection by design” as foreseen in Article 25 of the General Data Protection Regulation (“GDPR”). This means that data protection and privacy issues are taken into account starting from the commencement of product development or solution engineering.

In general, within Siemens, the following processes are implemented:

- Data Protection by Design approach is a part of the principles actively adopted by Siemens and integrated in the secure lifecycle development of products.
- Siemens solutions adopt Threat and Risk Analysis (TRA), a Siemens-wide standardized methodology that is used for product, solution and service business during product development, engineering or service projects. This methodology is intended to support Siemens teams in identifying typical security weaknesses and vulnerabilities, analyzing any threats that might exploit these weaknesses or vulnerabilities and evaluating any resulting risks.

Specifically for DI SW MOM products and solutions, in all data collection and processing activities that potentially involve personal data in the intended customer use case, DI SW MOM considers appropriate technical and/or organizational measures, with the goal of adequately addressing the data protection principles and safeguarding individual rights.

For Opcenter APS, the following applies:

- Opcenter APS has obtained the TÜV SÜD certification of security in the development process (based on IEC 62443-4-1). This standard specifies process requirements for the secure lifecycle development of products used in an Industrial Automation and Control System (IACS). The lifecycle includes:
  - the definition of security requirements;
  - secure design,
  - secure implementation (including coding guidelines), verification and validation,
  - secure defect management, patch management, and product end-of-life.
- The following personal data is processed by the Opcenter APS solution:
  - Usernames
  - Windows Security Identifiers

Specific attention is dedicated to the processing of personal data belonging to special categories, relevant for the purpose of detecting the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, health, sexual orientation or conduct, criminal convictions and offenses or related security measures of the persons concerned. No such personal data is processed by Opcenter APS.

- The personal data processed by Opcenter APS is required for authorization, logging, and personalization purposes. Therefore, such personal data processed by Opcenter APS cannot be anonymized or pseudonymized. Such data is stored solely for these reasons, as it is necessary to provide a mechanism to control access to application data.
- Opcenter APS adopts hashing and encrypting (at rest and in transit).
- In Opcenter APS, personal data can be deleted when no longer necessary for the designated purpose. In detail, the Opcenter APS Security Module can be used to remove users from the application.
  On the other hand, personal data may appear in the solution’s data repositories as database’s records, product file and log files, which are necessary for diagnostic or logging purposes. This information generated by Opcenter APS has different retention periods based on their different purposes: Dataset ‘last saved by’ information can be removed by deleting that dataset. Personalization data can be removed with the assistance of Customer Support.

- Opcenter APS Solution makes use of least privilege access control and policies and using appropriate roles and authorization concepts as individual user Read/Write permission.
- Regular review is performed to validate necessity for the purposes for which the personal data was collected and test the design against purpose limitation.