SIEMENS

Opcenter Intelligence 2501.0001

Installation Manual

04/2025

PL20250213460107832

Guidelines

This manual contains notes of varying importance that should be read with care; i.e.:

Important:

Highlights key information on handling the product, the product itself or to a particular part of the documentation.

Note: Provides supplementary information regarding handling the product, the product itself or a specific part of the documentation.

Trademarks

All names identified by ® are registered trademarks of Siemens AG.

The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Cybersecurity Information

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity concept. Siemens products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit https://www.siemens.com/cybersecurity-industry.

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

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS feed under https://www.siemens.com/cert.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

PL20250213460107832
20250407_142715

Table of Contents

ID	OpcenterIN_InstallationManual
Title	Installation Manual
Product Title	Opcenter Intelligence
Version Title	2501.0001
Product Version	OpcenterIN_2501_0001
Category	Installation, Configuration
Summary	Provides detailed information on how to install and configure Opcenter Intelligence.
Audience	System Integrator, Commissioning Engineer, Support Engineer, Project Engineer
Revision	PL20250213460107832
State	Published
Author	Siemens AG
Language	en-US

1 Before you Start

Before you install Opcenter Intelligence, you must:

- Choose the license type that better satisfies your requirements, depending on the operations you want to execute and on the number of users you need.
- Choose the scenario to install and configure and verify that all software and hardware prerequisites are satisfied for the selected scenario.
- Design your scenario following the suggestions on how to implement security strategies so that any risks and threats that may affect your system are successfully mitigated.
- Perform a number of preliminary configurations.
- Verify that the prerequisites for User Management Component (UMC) are satisfied. In particular, the manual configuration including the acquisition of a valid SSL certificate must have been performed. For more details, see *Central User Management UMC Programming and Operating Manual*.

Virtual Infrastructure Support

Opcenter Intelligence supports VMware ESXi 6.7 Update 3 infrastructure, although the possibility cannot be excluded that Opcenter Intelligence can run on other Cloud environment types.
For the configuration of virtual infrastructure resources there are no constraints on the type of storage, vCPU, RAM, or network board type. However, before configuring the infrastructure, it is recommended that you keep in mind Opcenter Intelligence hardware requirements and allocate resources (RAM, vCPU and so on) to guarantee the maximum performance level of VMWare operations.

1.1 How to Manage Licenses, Users and Roles

According to the licensing model introduced starting from Opcenter Intelligence 3.2:

- License types are based on the number of users that can be configured for each role.
- Assigning roles to user groups is no longer allowed.

The previous licensing model based on the Opcenter Intelligence - Site and Opcenter Intelligence - Enterprise licenses is still available and can be used for existing installations.

> ⚠ Starting from version 2501, Opcenter Intelligence Analytics (Tableau® OEM) is no longer included in Opcenter Intelligence ISO. The license file is not incorporated in the setup either. Tableau® Server and Tableau® Desktop can be downloaded from the Tableau® website by a registered user.
> Customers who installed Opcenter Intelligence Analytics (Tableau® OEM) can migrate to the standard Tableau® Server by following a specific procedure.

Available License Types

- Licenses for Opcenter Intelligence
- Licenses for Tableau® Server

1.1.1 Managing Licenses, Users and Roles for Opcenter Intelligence

You can choose one of the following licenses according to your requirements:

- Opcenter Intelligence Admin User
- Opcenter Intelligence Desktop User for Analytics
- Opcenter Intelligence Explorer User for Analytics
- Opcenter Intelligence Viewer User for Analytics

Opcenter Intelligence Admin User License

Description	This license allows you to configure the user who has full access to the application and can perform analytical solution engineering and configuration tasks.
Number of licensed users (seats)	The number of users that can be configured depends on the number of seats purchased for this license.

⚠ This license does not allow you to create, publish or view analytical dashboards using Tableau®. For more information, see Managing Users and Roles for Tableau® Server.

Opcenter Intelligence Desktop User for Analytics

Description	This license allows you to configure users who can create dashboards using Tableau® Server and perform publish operations from Tableau® Desktop.
Number of licensed users (seats)	The number of users that can be configured depends on the number of seats purchased for this license.

Opcenter Intelligence Explorer User for Analytics

Description	This license allows you to configure users who can create dashboards using Tableau® Server.
Number of licensed users (seats)	The number of users that can be configured depends on the number of seats purchased for this license.

Opcenter Intelligence Viewer User for Analytics

Description	This license allows you to configure users who can only view published dashboards created using Tableau® Server.
Number of licensed users (seats)	The number of users that can be configured depends on the number of seats purchased for this license.

Users and Roles

The following table shows the list of Opcenter Intelligence user roles and the corresponding license types necessary for each role. The number of users you can configure depends on their roles. The Administrator role does not have a seat count on the basis of purchased licenses: you can configure any number of Administrator users irrespective of the purchased licenses.

Opcenter Intelligence User Roles	Opcenter Intelligence Admin User License	Opcenter Intelligence Desktop User for Analytics License	Opcenter Intelligence Explorer User for Analytics License	Opcenter Intelligence Viewer User for Analytics License
Administrator	N/A	N/A	N/A	N/A
Solution Engineer	X			
SmartView Engineer	X			
Desktop Explorer		X		
Analytics Explorer			X	
Analytics Viewer				X

The Desktop Explorer, Analytics Explorer and Analytics Viewer roles are not available for Opcenter Intelligence (Enterprise or Site) licenses.

No Longer Supported Roles

The following roles are related to the no longer supported Legacy Tableau® and reporting functionalities:

- Dashboard Contributor
- Dashboard Viewer
- Report Contributor
- Report Viewer

1.1.2 Managing Users and Roles for Tableau Server

The following roles are available and can be assigned to users after you have installed Tableau® Server. The association of these roles creates corresponding users in Tableau® Server.

Tableau® Server Roles

Role	Permissions
Desktop Explorer	This role grants you the following permissions: • Access the **Analytical Dashboards** page, where Tableau® Server is embedded. • Open Tableau® Server to create new dashboards. • Perform publish operations from Tableau® Desktop.
Analytics Explorer	This role grants you the following permissions: • Access the **Analytical Dashboards** page, where Tableau® Server is embedded. • Open Tableau® Server to create new dashboards.
Analytics Viewer	Can only access the **Analytical Dashboards** page to view published dashboards.

Opcenter Intelligence Roles and Corresponding Tableau® Server Users

Each time the Desktop Explorer, Analytics Explorer or Analytics Viewer role is assigned to a user in Opcenter Intelligence, a Tableau® Server user is created with the roles corresponding to the roles assigned in Opcenter Intelligence.

Opcenter Intelligence Roles	Tableau® Server Users
Solution Engineer OR **Smart View Engineer**	No Tableau® Server user is created.
Desktop Explorer	**Tableau® Explorer (Can Publish)** user - can publish from Tableau® Desktop (password authentication required).
Analytics Explorer	**Tableau® Explorer** user - cannot publish from Tableau® Desktop.
Analytics Viewer	**Tableau® Viewer** user.

Important Notes

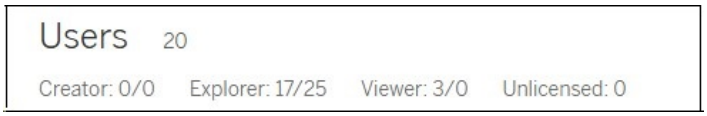
- You cannot assign the Desktop Explorer, Analytics Explorer and Analytics Viewer roles to the same user. If for example you want to upgrade a user from Analytics Viewer to Analytics Explorer, you must first remove the Analytics Viewer role from the user and then assign him the new one.
- When a user is removed from the Desktop Explorer, Analytics Explorer or Analytics Viewer role, the corresponding Tableau® Server user is deleted from Tableau® Server. If the Tableau® Server user is the owner of any dashboards, projects or workbooks, the operation is aborted. The corresponding user is deleted from Tableau® Server only after these resources have been reassigned.

Checking Tableau® Server Role Capacity

Adding or deleting users is managed by Tableau® Server directly, without any license check for Opcenter Intelligence with respect to Tableau® Server roles. You can log in to Tableau® Service Manager/Gateway portal with administrative permissions and check for the number of role capacity available for the current license. To do so:

1. Open a browser and type the URL of Tableau Service Manager (for example: http/https://*<machine name>*:8085) to log in.
2. On the **Configuration** tab, select **Licensing**. The following information is shown:

3. You can also check the assigned users against roles in Tableau® Gateway with Server Administrator role. To do so, select Users from left-hand panel and on top of the page the total users assigned against specific role are shown as follows:



If an added user violates the role capacity of Tableau® Server license, Opcenter Intelligence shows the following error to avoid adding unlicensed users to Tableau® Server:
"An error occurred while adding the Tableau Server user due to exceeding the license role capacity. Please review your current license allocation and consider upgrading your license or removing unused users to free up role capacities."

1.2 Supported Scenarios and Prerequisites

Opcenter Intelligence can be installed and used on the following supported scenarios:

- All-In-One Scenario
- Distributed Scenario

Any hardware or software configuration not expressly mentioned in the documentation is unsupported. For further information, it is recommended that you open an Incident Request to Siemens DI SW Support Services.

Opcenter Intelligence Components

- The **Core** is a Web API self-hosted server that includes the business logic.
- The **Application Server** includes the business logic to interact with the User Management Component (UMC) and redistributes the calls to the Core component.
- The **Client** represents the Single Page Application Client.
- **Opcenter Intelligence Configurator** is the stand-alone application that performs all the post-setup configuration actions.

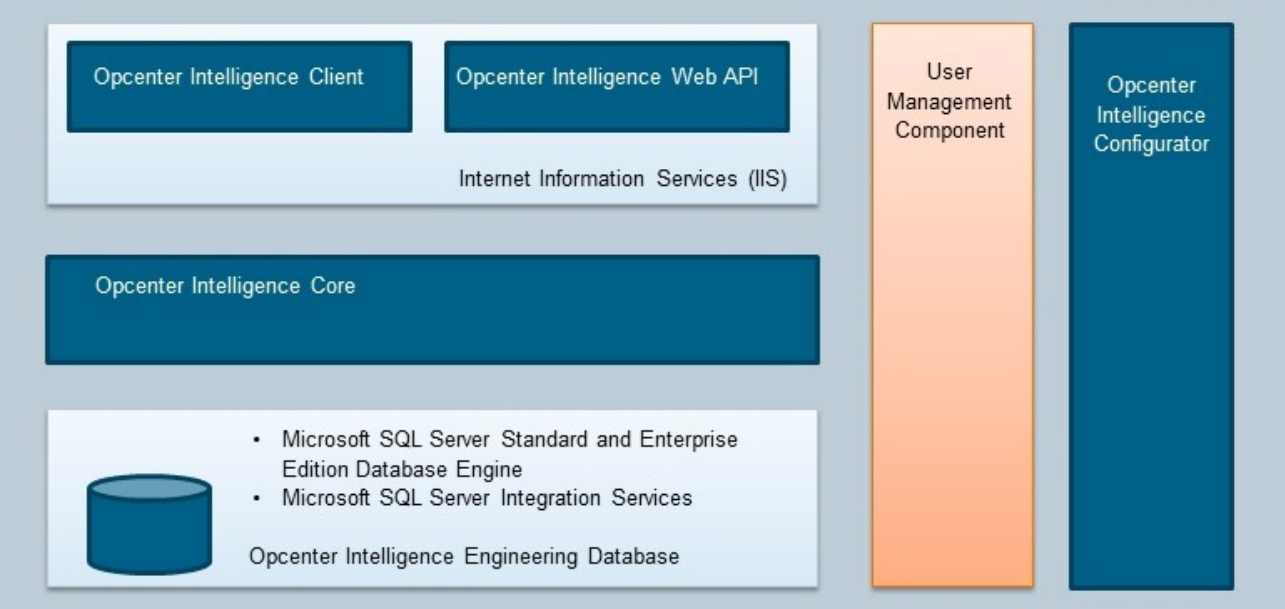
It is highly recommended that you configure your scenarios in a secure way by setting the communication protocol to HTTPS.

User Management Component (UMC)

Starting from version 3.3 the User Management Component (UMC) is the default identity provider for Opcenter Intelligence. For more details, see User Management Component as Default Identity Provider.

1.2.1 All-In-One Scenario

In this scenario all components and Microsoft SQL Server are installed on the same computer. Access to this computer can be performed from one or more Web Client computers.



Any hardware or software configuration not expressly mentioned in the documentation is unsupported. For further information, it is recommended that you open an Incident Request to Siemens DI SW Support Services.

Prerequisites

The following prerequisites are required before you install Opcenter Intelligence on an all-in-one scenario:

- Software Requirements
- Hardware Requirements

1.2.1.1 Software Requirements

Operating Systems

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Maintenance services, according to General SISW Maintenance Services Terms, are extended to the updates and the patches (excluding full Service Packs) that are officially released by Microsoft for the above Operating Systems.

Database Management Systems: Microsoft SQL Server

The following versions of Microsoft SQL Server are a mandatory prerequisite

Product	Architecture	Edition	Language
Microsoft SQL Server 2022	x64	Standard or Enterprise	English
Microsoft SQL Server 2019	x64	Standard or Enterprise	English
Microsoft SQL Server 2017	x64	Standard or Enterprise	English

Maintenance services, according to General SISW Maintenance Services Terms, are extended to the Successive Service Packs of these SQL Server versions, if and only if Microsoft declares their compatibility with it.

- If you are using **SQL Server 2022**, Microsoft OLE DB Driver for SQL Server (MSOLEDBSQL) is required. This new driver is necessary because SQL Server Native Client used in previous versions has been removed from SQL Server 2022 and it is not recommended to use it for new development work.
- If you are using **SQL Server 2019** versions previous to Cumulative Update 9, random issues may occur during flow execution. The installation of the latest SQL Server version is therefore recommended.
- Support for **SQL Server 2016 SP2** is guaranteed only for customers who are already using it. However, it is strongly recommended that you update it to a higher version, as Microsoft supports SQL Server 2016 SP2 only in Extended Mode.

For more information on Microsoft SQL Server configuration and components, see Microsoft SQL Server Installation and Configuration Tips.

Source Database Management Systems

Depending on the data source version, some SQL Server versions may not be supported. For more details see the documentation of the source product.

Microsoft SQL Server

Product	Edition	Language
Microsoft SQL Server 2022	Standard or Enterprise	English
Microsoft SQL Server 2019	Standard or Enterprise	English
Microsoft SQL Server 2017	Standard or Enterprise	English
Microsoft SQL Server 2016	Standard or Enterprise	English
Microsoft SQL Server 2014	Standard or Enterprise	English
Microsoft SQL Server 2012	Standard or Enterprise	English

Oracle

Product	Edition	Language
Oracle Database 12c Release 2 or higher	Enterprise	English

Oracle Data Provider for .NET (ODP.NET) must be installed on the same computer where Opcenter Intelligence Core Service is running.

Other Third-Party Software

- Either Internet Information Services 8.5 or 10 enabling ASP.NET Modules and IIS Role Services. This configuration can be executed automatically or manually.
- Microsoft .NET Framework 4.7.2. This software can be downloaded at https://dotnet.microsoft.com/download/dotnet-framework/net472.
- Microsoft .NET Framework 4.7.2 Developer Pack. This software can be downloaded at https://dotnet.microsoft.com/download/visual-studio-sdks.
- Microsoft Visual C++ 2015-2019 Redistributable packages.
- (Optional) Tableau® Server and Tableau® Desktop 2024.2.4, which can be downloaded from the Tableau® website by a registered user. If you want to install a higher version of Tableau®, ask the Opcenter Intelligence Support Team if that version is supported or not.

User Management Component (UMC)

User Management Component (UMC) 2.15 SP1. This software is distributed with Opcenter Intelligence and is installed by the setup.

For more information on UMC, see *Central User Management UMC Programming and Operating Manual*.

If a previous version of UMC has already been installed on your system with another product, you must upgrade it to version 2.15 SP1.

Licensing software

Siemens License Server (SLS)

This software is available on Support Center at the link https://support.sw.siemens.com/en-US/product/1586485382/downloads.

It can be installed either on an Opcenter Intelligence machine or on a separate machine where Opcenter Intelligence is not installed.

Siemens License Server installation and usage are documented in the following manuals:

- *Siemens Digital Industries Software License Server Installation Instructions* (**sw_siemens_license_server_install.pdf**).
- *Siemens Digital Industries Software Licensing Manual for PLM Products* (**sw_siemens_licensing_plm.pdf**).

Internet Browsers

The web client machine has been tested on the following browsers and versions:

- Microsoft Edge (based on Chromium) 134
- Google Chrome 134
- Mozilla Firefox 136

External Data Sources

Opcenter Intelligence supports:

- SQL Server 2012 or higher
- Oracle Database 12c Release 2 Enterprise Edition or higher

No Longer Supported Software

- Windows Server 2012 R2 x64
- Legacy Tableau®
- Microsoft SQL Server Reporting Services
- Microsoft Power BI
- Microsoft Internet Explorer

1.2.1.2 Hardware Requirements

The minimum hardware requirements for Opcenter Intelligence all-in-one scenario are the following:

CPU	RAM	Recommended Disk Drives
Processor: 4 physical cores x 2.0 GHz or higher	Main memory capacity 32 GB, DDR3 SDRAM or higher	• Solid-state drive 160 GB for the operating system • Solid-state drive 160 GB for temp and log database files • Hard disk drive 1 TB for data files

- Disk space depends on the data source and on the number of plants you are collecting data from. It is therefore recommended that you carry out a preliminary analysis of your requirements with the help of Siemens presales consultants to find the best solution for your project.
- To avoid any failure of flows to load data (ETLs) it is strongly recommended that you do not reserve all the available RAM to SQL Server but set a memory limit for each SQL Server instance.
- To ensure an adequate performance, it is strongly recommended that you dedicate a drive (solid-state drive or faster) to the **tempdb**.

Tableau® Server Hardware Requirements

These requirements are recommended if you have purchased a Tableau® license and want to navigate through the items you have created in Tableau® and view the resulting dashboards embedded in Opcenter Intelligence.

Check if Tableau® Server and Desktop hardware and software requirements are met on the machine where you want to install the two applications. For details, you can refer to Tableau® official documentation at the following links:

- https://help.tableau.com/current/server/en-us/requ.htm#hardware-requirements
- https://help.tableau.com/current/server/en-us/requ.htm#operating-system-requirements
- https://help.tableau.com/current/server/en-us/requ_diskspace.htm
- https://www.tableau.com/products/techspecs

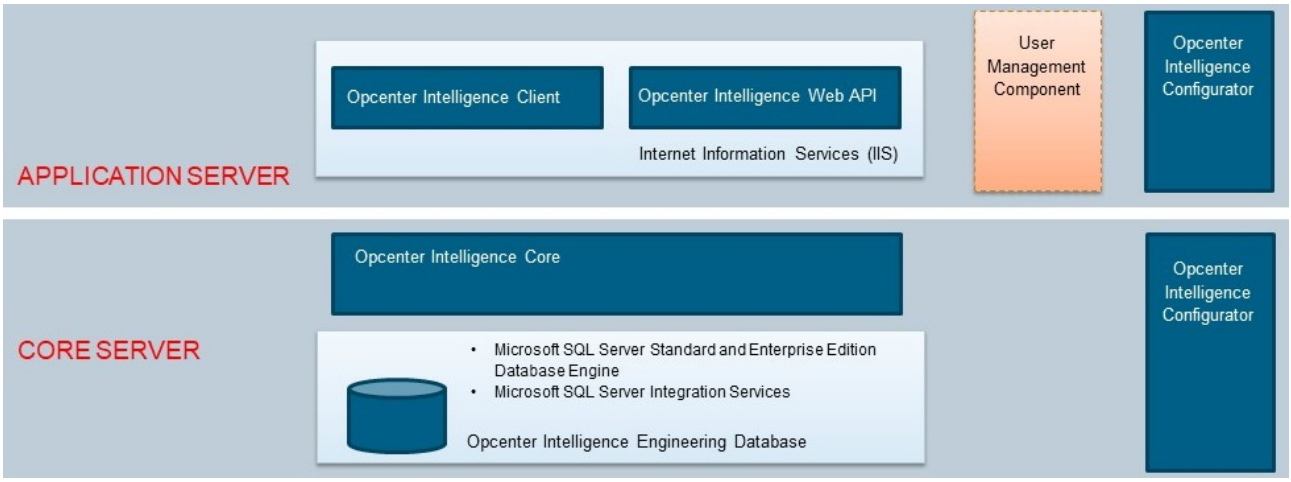
Please note that the RAM required for Tableau® Server has increased from the previous Opcenter Intelligence Analytics (Tableau® OEM) requirement.

1.2.2 Distributed Scenario

In this scenario the components and Microsoft SQL Server are distributed over the following computers:

- Core Server
- Application Server

Access to these computers can be performed from one or more Web Client machines.



> ⚠ Any hardware or software configuration not expressly mentioned in the documentation is unsupported. For further information, it is recommended that you open an Incident Request to Siemens DI SW Support Services.

Important Recommendations

- **Microsoft SQL Server Integration Services** installation is mandatory and must be installed on the same machine where Opcenter Intelligence Core is running.
- **Opcenter Intelligence Configurator** must be run first on the **Core Server** and then on the **Application Server** (so that the MIStudio database is created and the **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost** service is present in the Windows Services).
- The **User Management Component (UMC)** may have already been installed with another product on the same machine as the Application Server or on another machine. If it has not already been installed, it can be installed by the setup; in that case, it must be installed on the same computer where Internet Information Services (IIS) is running. If a previous version of UMC has already been installed on your system with another product, you must upgrade it to version 2.15 SP1.
- If in the distributed scenario the machines do not belong to any domain, the Windows user who will configure the Application Pools of Gateway Services must be the same and must have the same password on all machines.
- If your scenario is configured in HTTPS, in the Opcenter Intelligence Core machine you must configure the HTTPS protocol. To do so, follow the procedure described on the Configuring HTTPS Protocol for Opcenter Intelligence Components page.

Prerequisites

The following prerequisites are required before you install Opcenter Intelligence on a distributed scenario:

- Software Requirements
- Hardware Requirements

1.2.2.1 Software Requirements

Software prerequisites vary according to the computers that make up the scenario you want to install:

- Core Server
- Application Server
- Web Clients

External Data Sources

Opcenter Intelligence supports the following Source Database Management Systems:

Microsoft SQL Server

Depending on the data source version, some SQL Server versions may not be supported. For more details see the documentation of the source product.

Product	Edition	Language
Microsoft SQL Server 2022	Standard or Enterprise	English
Microsoft SQL Server 2019	Standard or Enterprise	English
Microsoft SQL Server 2017	Standard or Enterprise	English
Microsoft SQL Server 2016	Standard or Enterprise	English
Microsoft SQL Server 2014	Standard or Enterprise	English
Microsoft SQL Server 2012	Standard or Enterprise	English

Oracle

Product	Edition	Language
Oracle Database 12c Release 2 or higher	Enterprise	English

Oracle Data Provider for .NET (ODP.NET) must be installed on the same computer where Opcenter Intelligence Core Service is running.

1.2.2.1.1 Prerequisites for the Core Server

Operating Systems

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Maintenance services, according to General SISW Maintenance Services Terms, are extended to the updates and the patches (excluding full Service Packs) that are officially released by Microsoft for the above Operating Systems.

Microsoft .NET Framework

- Microsoft .NET Framework 4.7.2 This software can be downloaded at https://dotnet.microsoft.com/download/dotnet-framework/net472
- Microsoft .NET Framework 4.7.2 Developer Pack This software can be downloaded at https://dotnet.microsoft.com/download/visual-studio-sdks

Database Management Systems

Microsoft SQL Server

The following editions of Microsoft SQL Server are supported:

Product	Architecture	Edition	Language
Microsoft SQL Server 2022	x64	Standard or Enterprise	English
Microsoft SQL Server 2019	x64	Standard or Enterprise	English
Microsoft SQL Server 2017	x64	Standard or Enterprise	English

Maintenance services, according to General SISW Maintenance Services Terms, are extended to the Successive Service Packs of these SQL Server versions, if and only if Microsoft declares their compatibility with it.

- If you are using **SQL Server 2022**, Microsoft OLE DB Driver for SQL Server (MSOLEDBSQL) is required. This new driver is necessary because SQL Server Native Client used in previous versions has been removed from SQL Server 2022 and it is not recommended to use it for new development work.
- If you are using **SQL Server 2019** versions previous to Cumulative Update 9, random issues may occur during flow execution. The installation of the latest SQL Server version is therefore recommended.
- Support for **SQL Server 2016 SP2** is guaranteed only for customers who are already using it. However, it is strongly recommended that you update it to a higher version, as Microsoft supports SQL Server 2016 SP2 only in Extended Mode.

For more information on Microsoft SQL Server configuration and components, see Microsoft SQL Server Installation and Configuration Tips.

Licensing Software

Siemens License Server (SLS)

This software is available on Support Center at the link https://support.sw.siemens.com/en-US/product/1586485382/downloads.

It can be installed either on an Opcenter Intelligence machine or on a separate machine where Opcenter Intelligence is not installed.

Siemens License Server installation and usage are documented in the following manuals:

- *Siemens Digital Industries Software License Server Installation Instructions* (**sw_siemens_license_server_install.pdf**).
- *Siemens Digital Industries Software Licensing Manual for PLM Products* (**sw_siemens_licensing_plm.pdf**).

Internet Browsers

Opcenter Intelligence has been tested on the following browsers and versions:

- Microsoft Edge (based on Chromium) 134
- Google Chrome 134
- Mozilla Firefox 136

Other Third-Party Software

Microsoft Visual C++ 2015-2019 Redistributable packages

No Longer Supported Software

- Windows Server 2012 R2 x64
- Microsoft Internet Explorer
- Microsoft Kerberos: as a consequence of the migration to UMC as Identity Provider, the installation and configuration of Microsoft Kerberos in a distributed scenario is no longer required.

1.2.2.1.2 Prerequisites for the Application Server

Operating Systems

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Maintenance services, according to General SISW Maintenance Services Terms, are extended to the updates and the patches (excluding full Service Packs) that are officially released by Microsoft for the above Operating Systems.

Internet Information Services

Either IIS 8.5 or 10 enabling ASP.NET Modules and IIS Role Services. This configuration can be executed automatically or manually.

Microsoft .NET Framework

- Microsoft .NET Framework 4.7.2 This software can be downloaded at https://dotnet.microsoft.com/download/dotnet-framework/net472
- Microsoft .NET Framework 4.7.2 Developer Pack This software can be downloaded at https://dotnet.microsoft.com/download/visual-studio-sdks

User Management Component (UMC)

User Management Component (UMC) 2.15 SP1. This software is distributed with Opcenter Intelligence and is installed by the setup.

For more information on UMC, see *Central User Management UMC Programming and Operating Manual*.

If a previous version of UMC has already been installed on your system with another product, you must upgrade it to version 2.15 SP1.

Internet Browsers

Opcenter Intelligence has been tested on the following browsers and versions:

- Microsoft Edge (based on Chromium) 134
- Google Chrome 134
- Mozilla Firefox 136

Other Third-Party Software

- Microsoft Visual C++ 2015-2019 Redistributable packages
- (Optional) Tableau® Server and Tableau® Desktop 2024.2.4, which can be downloaded from the Tableau® website by a registered user. If you want to install a higher version of Tableau®, ask the Opcenter Intelligence Support Team if that version is supported or not.

No Longer Supported Software

- Windows Server 2012 R2 x64
- Legacy Tableau®
- Microsoft SQL Server Reporting Services
- Microsoft Power BI
- Microsoft Internet Explorer
- Microsoft Kerberos: as a consequence of the migration to UMC as Identity Provider, the installation and configuration of Microsoft Kerberos in a distributed scenario is no longer required.

1.2.2.1.3 Prerequisites for Web Clients

Web Clients are used to access the product UI to perform engineering and runtime operations. Opcenter Intelligence is not installed on these machines.

Operating Systems

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 10 x64
- Windows 11

Maintenance services, according to General SISW Maintenance Services Terms, are extended to the updates and the patches (excluding full Service Packs) that are officially released by Microsoft for the above Operating Systems.

Internet Browsers

The Web Client machine has been tested on the following browsers and versions:

- Microsoft Edge (based on Chromium) 134
- Google Chrome 134
- Mozilla Firefox 136

No Longer Supported Software

- Windows Server 2012 R2 x64
- Legacy Tableau®
- Microsoft SQL Server Reporting Services
- Microsoft Power BI
- Microsoft Internet Explorer

1.2.2.2 Hardware Requirements

The minimum hardware requirements for Opcenter Intelligence distributed scenario are the following:

	Core Server	**Application Server**	**Web Client Computer**
CPU	Processor: 4 physical cores x 2.0 GHz or higher.	Processor: 4 physical cores x 2.0 GHz or higher.	Processor: 4 physical cores x 2.0 GHz or higher.
RAM	Main memory capacity 32 GB, DDR3 SDRAM or higher	Main memory capacity 16 GB, DDR3 SDRAM or higher	4 GB or higher
Recommended disk drives	• Solid-state drive 160 GB for the operating system • Hard disk drive 500 GB for data files	• Solid-state drive 160 GB for the operating system • Hard disk drive 200 GB for data files	Hard disk: 40 GB
Minimum screen resolution	N/A	N/A	1024 x 768

- Disk space depends on the data source and on the number of plants you are collecting data from. It is therefore recommended that you carry out a preliminary analysis of your requirements with the help of Siemens presales consultants to find the best solution for your project.
- To avoid any failure of flows to load data (ETLs) it is strongly recommended that you do not reserve all the available RAM to SQL Server but set a memory limit for each SQL Server instance.
- To ensure an adequate performance, it is strongly recommended that you dedicate a drive (solid-state drive or faster) to the **tempdb**.

Tableau® Server Hardware Requirements

These requirements are recommended if you have purchased a Tableau® license and want to navigate through the items you have created in Tableau® and view the resulting dashboards embedded in Opcenter Intelligence.

Check if Tableau® Server and Desktop hardware and software requirements are met on the machine where you want to install the two applications. For details, you can refer to Tableau® official documentation at the following links:

- https://help.tableau.com/current/server/en-us/requ.htm#hardware-requirements
- https://help.tableau.com/current/server/en-us/requ.htm#operating-system-requirements
- https://help.tableau.com/current/server/en-us/requ_diskspace.htm
- https://www.tableau.com/products/techspecs

Please note that the RAM required for Tableau® Server has increased from the previous Opcenter Intelligence Analytics (Tableau® OEM) requirement.

1.2.3 User Management Component as Default Identity Provider

Starting from version 3.3 the default identity provider for Opcenter Intelligence is User Management Component (UMC).

> Windows Authentication is no longer supported starting from version 3.5.

Either of the following scenarios is possible:

- If you are installing Opcenter Intelligence for the first time, only the UMC authentication is supported.
- If you are upgrading from a previous version of Opcenter Intelligence and you are using Windows Authentication, you must migrate to UMC as Identity Provider.

Workflow

1. Apply specific settings in Opcenter Intelligence Configurator. In particular, you have to define:
    - The full computer name of the machine where UMC Server is running and the corresponding port.
    - The user who will configure the Application Pools of Gateway Services in IIS.
2. Configure Gateways and Web Sites in Internet Information Services (IIS). For details, see Checking Authentication Keys in IIS.
3. Define users in UMC. A manual operation must then be executed to add the Opcenter Intelligence Administrator to UMC. For more details, see How to Define Users.

    > As a consequence of the migration to UMC as Identity Provider, the installation and configuration of Microsoft Kerberos in a distributed scenario is no longer required.

1.3 Security Strategies

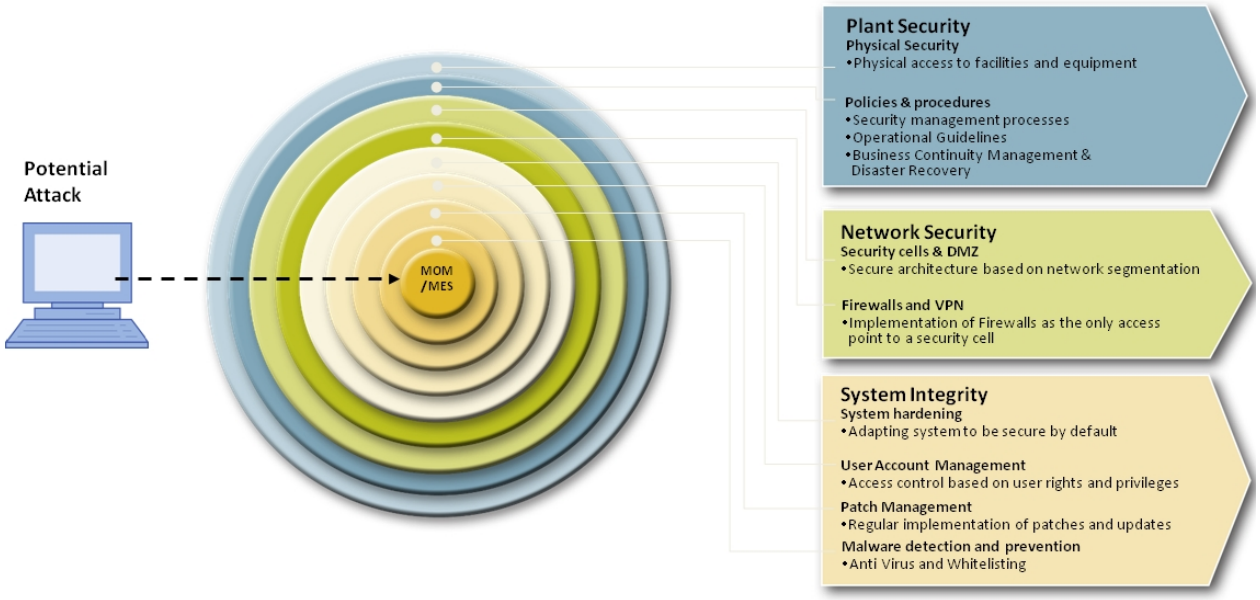
> This section refers only to Opcenter Intelligence security. For concepts related to the security of other Opcenter products or third-party products, please refer to their documentation.

Computer systems and networks are inherently vulnerable to a wide variety of security threats that can be prevented or reduced by adopting specific security countermeasures.

Each of these technical measures is specific to a certain attack (viruses cannot be prevented with firewalls) and can cover only a subset of the necessary protection goals. Nevertheless, only an overall strategy can provide effective protection.
The Siemens Industrial Security concept corresponds to a multi-layer defense, known as defense-in-depth concept. This strategy consists of several defense layers that protect a system, in this case the MOM/MES system:

- **Plant Security Layer**: Plant security ensures that technical IT security measures cannot be bypassed somehow. This includes physical-access protection measures (such as fences, turnstiles, cameras or card-readers) and organizational measures (in particular, a security management process) for ensuring long-term plant security.
- **Network Security Layer**: The core of the Industrial Security concept is network security. This includes protecting automation networks from unauthorized access and checking all interfaces towards other networks, such as an office network and, in particular, remote access to the Internet. Network security also encompasses protecting communication from interception and manipulation (for example, encryption during data transfer and authentication of the respective communication nodes). For more information, see Overview of Network Security.
- **System Integrity Layer**: Securing system integrity should be regarded as the third pillar of a balanced security concept. This is ensured by using automation systems and controller components that are protected against unauthorized access and malware or meet special requirements, such as know-how protection. For more information, see *Overview of System Integrity*.

Adopting a defense-in-depth approach allows you to achieve comprehensive and reliable protection of an automated system.



1.3.1 Overview of Network Security

Network security represents the core of the Industrial Security concept.
This includes protecting automation networks from unauthorized access and checking all interfaces towards other networks, such as an office network and, in particular, remote access to the Internet. Network security also encompasses protecting communication from interception and manipulation (for example, encryption during data transfer and authentication of the respective communication nodes).
One strategy used for increasing overall system availability that can effectively mitigate security risks is the segmentation of the network into a set of so-called security cells.
Each cell is conceived to cover a specific business function and has a dedicated protected network.
As a result, devices within a cell can be protected from unauthorized access from the outside without affecting real-time capabilities, performance or other functions. Security threats that result in failure can thus be restricted to the immediate area.
A particular type of security cell is the Demilitarized Zone (DMZ), which can be used to isolate certain applications from external networks.
For more information on how to set up a secure network by managing safe communications between security cells, see:

- Security Cells and DMZs
- Firewall and VPN
- Secure Communication between Security Cells

1.3.1.1 Security Cells and DMZs

Dividing networks and connected plants into security cells consists in dividing up a large corporate network into separate networks, each used for a specific business function. This strategy increases the availability of the overall

system and is an effective way to mitigate security risks. In the implementation of this approach parts of a network, e.g. an IP subnet, are protected by a security appliance and the network is secured by segmentation. Thus, devices within this 'cell' can be protected from unauthorized access from outside without affecting real-time capabilities, performance or other
functions. Security threats that result in failure can thereby be restricted to the immediate vicinity.
The different ISA95 levels can be used to identify security cells, for example by keeping ERP (Enterprise Resource Planning) functions separate from MES (Manufacturing Execution System) functions.

According to the ISA-95 levels, the following levels can be identified:

- Enterprise Resource Planning Level
- Manufacturing Execution Systems Level
- Manufacturing Control Systems Level

Each level includes one or more networks. In addition we identify also perimeter networks.
When creating security cells, you should follow some design rules.
In this section we present also the example configuration organized in different security cells.

For more information, see https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security.html

Enterprise Resource Planning Level

The Enterprise Resource Planning Level is where the ERP Systems are managed. The network connecting the ERP Systems may need to communicate with both MES and Process Control Systems located in other networks. This network is generally the outermost network used in a plant: as a result, it is the most exposed to potential security risks. For this reason, it is recommended to make this network to connect to other networks via Perimeter Network, instead of direct connection.

Manufacturing Execution System Level

The Manufacturing Execution System Level is where the data exchange among Manufacturing Execution System devices is managed. The network includes MES/MOM servers and can be directly connected to a Process Control Network.

Manufacturing Control System Level

The Manufacturing Control System Level hosts the control-layer software systems, such as generic DNC systems, SIMATIC WinCC or SIMATIC PCS7, and is where the data exchange among Manufacturing Control System devices is

managed. Since this network is very close to the field, it is important to keep it as separate as possible from the external networks, to mitigate security risks and to protect the plant production.

Perimeter Network

In addition to the networks listed above, we have also Perimeter Networks in our scenarios, sometimes called DMZs (Demilitarized Zones). These are networks used to isolate certain applications from outside networks, thereby mitigating security risks.
Typically, Web Servers are placed in this network, so that they can collect data from low level networks and, at the same time, they can provide web pages to outer networks (for example an Enterprise Control Network).
If you are planning to connect using the Remote Desktop Service, the Remote Desktop Service Server should be placed in this network.

Design Rules

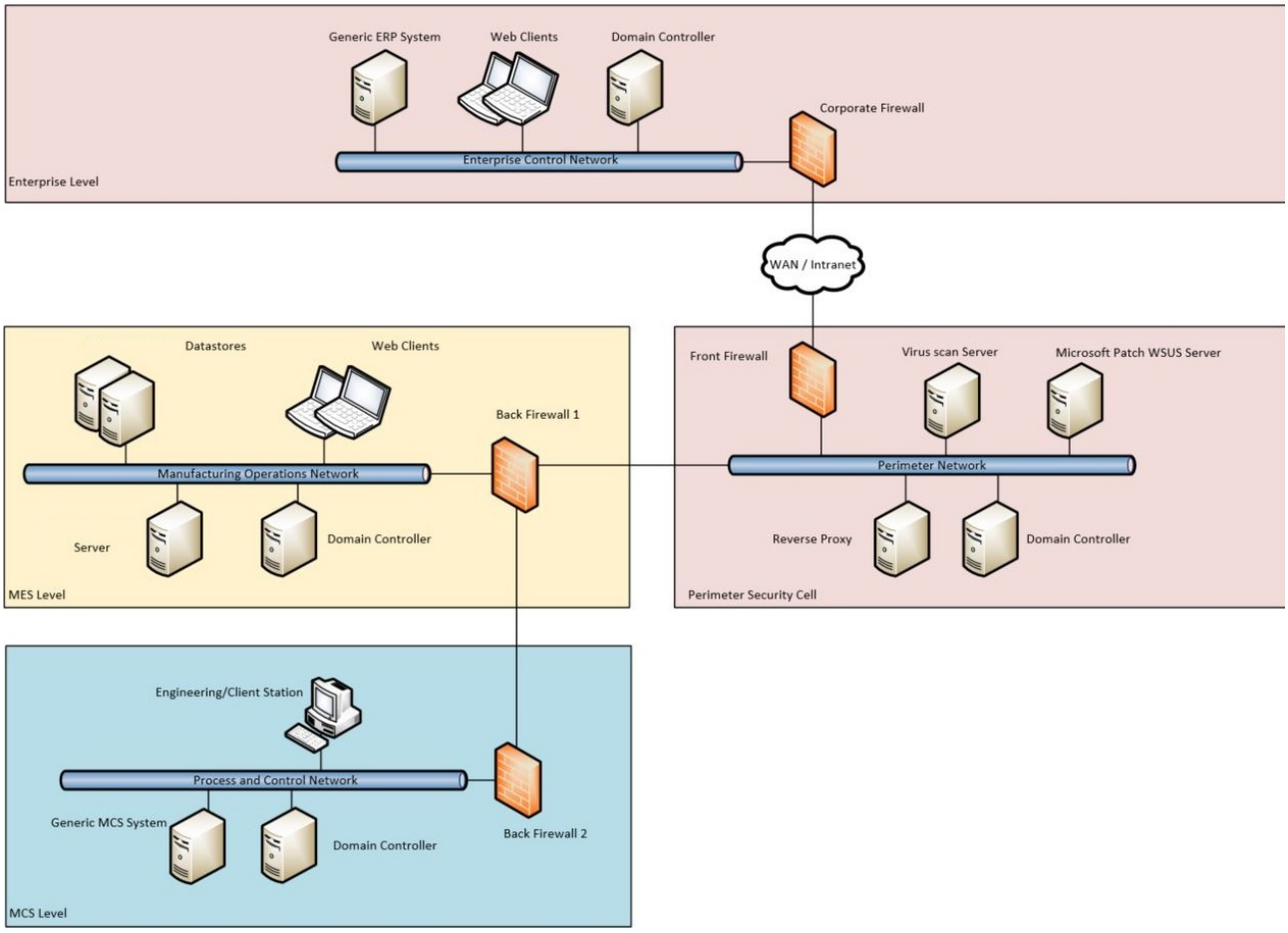
When designing and implementing a complex network scenario, the following rules should be followed to enhance security:

- All devices and hardware that are used to run production should be physical and located in the Manufacturing Control Systems Network.
- All devices with access to external non-secure networks or that can be accessed from external non-secure networks should be placed in a Perimeter Network.
- All devices that collect data from or provide input to Manufacturing Control Systems Networks, but that could also be disconnected for a certain time, should be placed in a Manufacturing Operations Network.

When creating security cells, you should follow some common guidelines and implementation best practices, such as:

- A security cell is an independent part of the plant.
- All participants inside the cell trust each other.
- Access to the security cell is permitted only through clearly-defined access points.
- Access points are monitored and access is logged (data traffic, user, hardware).
- All participants of a security cell are directly connected (no bypass to the outside).
- Participants with a high network load will be integrated into a security cell to avoid bottlenecks.

Example Configuration with Security Cells



1.3.1.2 Firewall and VPN

In order to grant network security, access points to security cells and communication between the different access points have to be secured.

Access Points to Security Cells

It is a good practice to permit access to security cells only through clearly-defined access points: security cells should have a single access point.
The access through access points is permitted only after having verified the legitimacy of the access request (people and/or devices must be authenticated and authorized). Furthermore, it is advisable to log any access.
Access points should prevent unauthorized data traffic to security cells while permitting authorized traffic necessary for smooth system operation. The access point to a security cell can be designed according to configuration and functionality requirements.
A network in which all data traffic is protected by a firewall represents an example of a security cell with a security access point.

⚠ Firewalls must be configured with rules to mitigate DDoS attacks.

Access Points: Configuration Example

In the configuration example, the access points to the different security cells are protected by firewalls. The tables below show:

- the communication direction for the machine roles in the example scenario and
- the communication protocols that have to be applied in order to guarantee network security.

These tables refer only to Opcenter Intelligence connections; for other products refer to their specific documentation.

Communication between different Security Cells

	Application Server	**Reverse Proxy**	**Core Server**	**UMC**	**License Server**
Web Client	Blocked (*)	→ (HTTPS)	Blocked (*)	Blocked (*)	Blocked (*)
Application Server	Not Applicable (**)	← (HTTPS)	Not Applicable (**)	Not Applicable (**)	Not Applicable (**)
UMC	Not Applicable (**)	← (HTTPS)	Not Applicable (**)	Not Applicable (**)	Not Applicable (**)

(*) Typically the direct communication to the server has been blocked.

(**) The involved machines belong to the same security cell.

Communication inside a Manufacturing Security Cell

In general, a firewall is not used within a security cell, but this schema can convey an idea on the communications and corresponding protocols between the different system components.

	Application Server	**Core Server**	**UMC**	**Data Source**	**License Server**
Web Client	→ (HTTPS)	Not Applicable (*)	→ (HTTPS)	Not Applicable (*)	Not Applicable (*)
Application Server	Not Applicable (*)	→ (https)	→ (HTTPS)	Not Applicable (*)	Not Applicable (*)
Core Server	← (HTTPS)	Not Applicable (*)	→ (HTTPS)	Database Secure Communication	→ (tcp) (**)

(*) The involved machines belong to the same security cell.

(**) TCP connections are always established towards two ports (see table below). For more details, see Installing the License Server.

⚠ It is recommended that you use the HTTPS protocol for all configurations.

You can configure the ports used by the different protocols, but the most commonly used ports are:

Protocol	Port Number
HTTP	80
HTTPS	443
License Server TCP	• 29000 • vendor daemon port
SQL Server	1433 (for Default Instance)
Oracle	1521

1.3.1.3 Secure Communication between Security Cells

In order to grant network security, the access points to security cells and the communication, among the various access points, must be rendered secure. In this section, we are going to see how this goal can be reached. In many cases, data exchange among components, that are located in different areas, is required for the correct operation of a plant. The following sections illustrate how to secure communication channels between the cells.

Secure communication between Enterprise and MES Security Cells

The communication between ERP (enterprise) level and MES level must be filtered by using a specific security cell, known as perimeter cell, in order to decouple the plant network from the external network.
Opcenter Intelligence communications are based on HTTP protocol: therefore, in order to grant a good level of security, it is necessary to configure the HTTPS between the ERP cell and the perimeter cell, as well as the same protocol between the perimeter cell and the MES security cell.
It is mandatory to configure the channels between:

- the Enterprise Security Cell and the Perimeter Security Cell using SSL/TLS with a server certificate
- the Perimeter Security Cell to the MES security Cell using SSL/TLS with a server and client certificate.

To enable secure communication, it is necessary to create an HTTPS protocol binding on the site hosting Opcenter Intelligence and the Virtual directories, following the relative IIS procedure at http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis.

Secure Communication between MES and Process and Control Security Cell

Communication between applications deployed in the MES Security Cell and the Process and Control Security Cell must be established following the guidelines provided by back-end applications.
All information required on the Siemens Process and Control system can be found at http://w3.siemens.com/mcms/automation/en/process-control-system/Pages/Default.aspx.

Additional notes on MES Security Cell communication

It is highly recommended that you deploy the components related to manufacturing on the same security cell. Furthermore, it is advisable to apply additional countermeasures to increase communication security.

These suggestions are mandatory if the components or databases are deployed in different security cells.

Secure communication with Opcenter Intelligence database server

The connection between Opcenter Intelligence applications and the database must be secured following the indications provided in the Microsoft SQL Server documentation found at https://msdn.microsoft.com/en-us/library/bb283235.aspx.

Secure communication with third-party databases (only for data reading)

Opcenter Intelligence can be configured to resolve data queries on multiple data sources (the Opcenter Intelligence database, as well as other third-party databases). It may be necessary to render the communication channel with these third-party databases secure, according to customer requirements.

Information about securing the supported database server can be found for Microsoft SQL Server at https://msdn.microsoft.com/en-us/library/bb283235.aspx.

Secure communication between Opcenter Intelligence application server and an external system

All communication that makes it possible to join Opcenter Intelligence applications deployed in the Manufacturing network with other external systems must be based on either application secure protocols that guarantee the goals of confidentiality/integrity or alternative secure solutions provided by your IT department (not contemplated in this document).

In case Opcenter Intelligence Clients are located in different geographic areas, it is necessary to properly setup and configure a firewall between your network and the network where the clients are located. In this scenario, it is recommended to use VPNs (Virtual Private Networks), to protect communications between the different plants from external attacks.

1.3.2 Overview of System Integrity

System Integrity is ensured by using automation systems and controller components that are protected against unauthorized access and malware or meet special requirements, such as know-how protection.

Customizations can be performed by System Integrators. However, you must consider that the effects of the product and of the custom code must be distinguished. This distinction can be implemented via auditing custom code execution and deployment, or providing coding guidelines and making customers responsible for compliant code and/or tracking execution.

At the following links, you can find some general indications on how to ensure system integrity.

- System Hardening
- User Account Management
- Patch Management
- Malware detection and prevention

Some security configurations related to group settings and file/directory permissions will be automatically applied by the installation (that is, from the Security Controller step of the installation wizard).

Access Control on Files and Directories

Folder Path	Users	Role
C:\Program Files\Siemens\Opcenter\Intelligence\IN\ApolloMIStudio	IIS_User and <*Domain*>\Users	Read & Execute
C:\Program Files\Siemens\Opcenter\Intelligence\IN\MIStudioServer	IIS_User	Read & Execute
C:\Program Files\Siemens\Opcenter\Intelligence\IN\CoreService	The domain user inserted in Opcenter Intelligence Configurator who is going to run the Core Service and must have Administrator privileges.	Read & Execute

- When changing the plant configuration or changing the user roles, be aware that local group memberships must be adapted accordingly.
- Settings must be reapplied if a change is made to the work environment.

1.3.2.1 System Hardening

The term *hardening* summarizes all those measures and settings that aim to:

- reduce opportunities to exploit vulnerabilities in software;
- minimize potential methods of attack;
- limit the tools available for a successful attack;
- minimize the available rights following a successful attack;
- increase the probability of detecting a successful attack.

This is intended to increase local security and the resilience of a computer to withstand attacks.
Consequently, a system can be described as "hardened" if:

- the software components and services installed are limited to those that are required for the actual operation;
- restrictive user management is implemented;
- the local Windows Firewall is enabled and is restrictively configured.

System Hardening Recommendations

Before installing Opcenter Intelligence, you must make your system safe by hardening:

- The Computer BIOS.
- The Operating System by:
  - uninstalling programs and Windows components that are not required;
  - disabling unnecessary services;
  - using a whitelisting application to prevent the execution of unauthorized programs;
  - making backups on a regular basis.

    For more information, see Federal Office for Information Security website.
- The databases used in your scenario. For Microsoft SQL Server databases, refer to https://msdn.microsoft.com/en-us/library/bb283235.aspx and https://technet.microsoft.com/en-us/library/bb510663(v=sql.110).aspx. It is recommended that you follow a maintenance plan. In addition, it is recommended that you make back up your

databases on a regular basis, to avoid critical data loss. For the backup-restore procedure using Microsoft SQL Server 2016 SP2, see: https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/back-up-and-restore-of-sql-server-databases?view=sql-server-ver15
- The file system (for example, by encrypting it).

In addition, it is recommended that you remediate the following vulnerabilities:

- Prevent Microsoft IIS Tilde Directory Enumeration
- Disable the SSL v3 Protocol on IIS
- Install the Windows Update to Disable RC4
- Disable Debugging for ASP.NET
- Remove Unwanted HTTP Response Headers
- Prevent Version Disclosure ASP.NET

1.3.2.1.1 Security Controller

The Security Controller (SeCon) is a program, integrated by default in User Management Component (UMC) that configures application-specific security settings during the installation.
SeCon can automatically configure the following settings:

- Group settings
- Registry settings
- Windows Firewall exceptions
- DCOM settings
- File and/or directory permissions settings

These settings are configured depending on the installation (package selection).

1.3.2.1.2 Whitelisting

Opcenter Intelligence has been tested using McAfee Application Control as a whitelisting application, locally on a computer system (standalone). This implies that the local administration is handled exclusively by means of command line inputs that are intelligible and self-explanatory. McAfee Application Control can be also easily handled using batch files or scripts. McAfee provides excellent reference material.

However, McAfee Application Control can also be administered Centrally using McAfee ePolicy Orchestrator (ePO). Decisions in favor of central or local administration should be made based on the number of systems to be maintained.
Once McAfee Application Control has been installed on the computer, you must execute the "solidify" function on every hard disk and partition. The function scans all the connected drives in order to detect the presence of executable files. After the function execution, only the detected executable files are protected against manipulation (renaming, deletion, etc.) and can be executed. Files that are stored in the computer after the execution of "solidify" function cannot be executed.
The execution of the "solidify" function can last several hours, depending on the volume of data and on the performance of the computer.
In the following section you can find how to install McAfee Application Control and execute Solidify Function.

1.3.2.1.2.1 Installing McAfee Application Control and Executing Solidify Function

You should follow the instructions below during integration of the McAfee Application Control, or prior to its installation. Performing this procedure, all components signed by selected certificates can make changes to the binaries on the system and launch new applications.

Procedure

1. Install and configure the operating system.
2. Install all the necessary programs and components.
3. Install all the security updates that are available both for the operating system, program and components.
4. Install a virus scanner and update it with the latest virus signature files.
5. Set up the system architecture according to the recommendations contained in the Installing Opcenter Intelligence Interactively and Security Strategies chapters, in order to keep malware risks to the absolute minimum prior and during the integration of McAfee Application Control.
6. Disconnect the machine from external/third party networks (e.g. at the frontend Firewall).
7. Run a complete virus scan on the machine.
8. Install the McAfee Application Control locally.
9. Open the McAfee Application Control command line (**Start > Programs > McAfee > Solidifier > McAfee Solidifier Command Line**).
10. Start Solidification by typing the **sadmin solidify** or **sadminso** command, and wait for the process to complete.
11. Enable the configuration by typing **sadmin enable** (the McAfee Solidifier Control will be activated when the machine is rebooted).

Result

All partitions and local hard disks of the computer system are scanned for the presence of executable files (applications), e.g. exe, com, bat, dll, as well as Java, Active-X control elements, and scripts. The McAfee Application Control signs and authorizes all files found during the scan for future use. It also protects the files against manipulation such as deletion, or renaming. On successful completion of the "solidification" process, the Solidifier command line reports the number of files scanned per partition or hard disk, including the number of files that have been authorized. After the restart, you can query the status of McAfee Solidifier by entering the **sadmin status** command in the Solidifier command line.

1.3.2.1.3 Preventing Microsoft IIS Tilde Directory Enumeration

It is possible to detect short names of files and directories which have an 8.3 file naming scheme equivalent in Windows by using some vectors in several versions of Microsoft IIS. For instance, it is possible to detect all short-names of ".aspx" files as they have 4 letters in their extensions. This can be a major issue especially for the .Net websites which are vulnerable to direct URL access as an attacker can find important files and folders that are not normally visible.

Recommended Action

For more details, see: https://technet.microsoft.com/en-us/library/cc959352.aspx

1.3.2.1.4 Disabling the SSL v3 Protocol on IIS

Some versions of Windows Server allow SSL 2.0 and SSL 3.0 by default. Unfortunately, these are insecure protocols. Depending on how your Windows servers are configured, you may need to disable SSL v3.

Recommended Action

For more details, see: https://docs.microsoft.com/en-us/security-updates/securityadvisories/2015/3009008

1.3.2.1.5 Installing Windows Update to Disable RC4

A Windows update is available to disable RC4. It is highly recommended that you download and install this update.

Recommended Action

For more details, see: https://docs.microsoft.com/en-us/security-updates/securityadvisories/2013/2868725

1.3.2.1.6 Disable Debugging for ASP.NET

ASP.NET supports compiling applications in a special debug mode that facilitates developer troubleshooting. This mode, however, may affect the application performance.

Recommended Action

It is recommended that you disable ASP.NET debugging before deploying a production application on the web server.

For more details, see: https://support.microsoft.com/en-us/help/815157/how-to-disable-debugging-for-asp-net-applications

1.3.2.1.7 Remove Unwanted HTTP Response Headers

The HTTP responses returned by the web application may include a header named Server. The value of this header includes the version of Microsoft IIS server.

Recommended Action

Configure Microsoft IIS to remove unwanted HTTP response headers from the response. For more details, see: https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

1.3.2.1.8 Prevent Version Disclosure ASP.NET

The HTTP responses returned by the web application may include a header named X-AspNet-Version.

Recommended Action

Apply needed changes to the web.config file to prevent information leakage. For more details, see: https://msdn.microsoft.com/en-us/library/system.web.configuration.httpruntimesection.enableversionheader.aspx

1.3.2.2 User Account Management

Configuring access controls on the basis of user rights and privileges contributes to System Integrity.
A safe user account management foresees that specific users may access only specific parts of the system, devices or applications. Some users have administrator rights, whereas others have only read and/or write access rights. Managing user and operator permissions involves the:

- Assignment of permissions in the Windows environment.
- Assignment of roles to users and user groups.
- Application of the UMC Security Concept.

These procedures are rigorously separated from each other, but both are strictly applied under the principle of minimum required rights.

1.3.2.2.1 Assignment of Permissions in the Windows Environment

> ⚠ Starting from version 3.5, Windows Authentication is no longer supported. The default identity provider is User Management Component (UMC).

The strategy of role-based access control includes restriction to minimally required rights and functions for users, operators, devices, network and software components.
The users to be created in the operating system environment can be managed in distributed mode or from a central location.

In accordance with the distributed management of users in groups of the ALP (Add User Account to Local Group and Assign Permission) principle recommended by Microsoft, local users must be grouped first so that the required permissions (folder, releases, etc.) can be assigned to these groups.
If management is performed centrally from a domain, the AGLP (Access Global Local Permission) principle should be observed. According to this principle, user accounts are initially assigned to the domain-global groups in the Active Directory. These groups are then assigned to local computer groups, which, in turn, receive permissions to the objects.
The generation of Opcenter Intelligence Windows groups, as well as the configuration of file permissions, are automatically performed during product setup.

Opcenter Intelligence Windows Local Groups

Opcenter Intelligence requires that some predefined Windows Local Groups are present either on a single machine when an all-in-one scenario has been chosen, or on both the application machine and the database machine in the case of a distributed scenario (see Supported Scenarios and Prerequisites).

These Windows Local Groups are used to:

- Manage file system permissions on Opcenter Intelligence folders.
- Manage permissions on other Windows low-level resources.
- Protect access to Opcenter Intelligence back-end.
- Access SQL Server using the Windows Authentication connection.

These groups are created by the Opcenter Intelligence setup automatically.

If the database is stored on a dedicated database machine, they must be created manually on the SQL Server machine.

1.3.2.2.2 Assignment of Roles to Users and User Groups

All MES data and related functionalities must be exposed in conditions that do not present problems regarding security. Systems or people that need to access the functionalities must be authenticated and authorized.
Authentication means that the system knows the identity of the external system or user that is going to access some functionalities. In the case of users, the typical user credentials are user name and password. The user accesses the system providing these credentials: if authentication is successful, the user is granted access.
Authorization defines the actions that authenticated users/systems can perform in the system. A typical way to implement authorization is by defining groups and roles that summarize the rights a user can have for system resources.

Authentication

In enterprise environments, there is a growing need to guarantee a high level of interoperability among the various systems making up the enterprise itself, without neglecting important qualitative attributes, such as security.
The excerpt from *A Guide to Claims-Based Identity and Access Control (2nd Edition)* at http://msdn.microsoft.com/en-us/library/hh446528.aspx illustrates that MES/MOM service applications (based on REST - REpresentational State Transfer) are typically consumed in a "session-less" flow and each request is an independent operation.
No session cookies are handled within this type of communication because there is no concept of a sequence of operations.
Typically, Web Services expect each request to provide the necessary authentication details and treat them in two possible ways:

- **Unauthorized requests** are rejected and trigger a response with HTTP code 401 containing one or more WWW-Authenticate headers, each specifying the details of the required authorization scheme and realm. Clients must analyze these headers to understand how to obtain a token to be included in a valid request.
- **Authorized requests** carry the authorization header containing the authentication token issued by the Identity Provider STS.

As a consequence of this architectural choice, Opcenter Intelligence does not implement identification and authentication functionalities.
Opcenter Intelligence relies on the User Manager Component to implement these functionalities.

Authorization

Opcenter Intelligence access control is guaranteed by:

- the predefined role *SysAdmin*, which is created to grant the access to the system for initial engineering.
- additional pre-defined operational roles, which are associated by default with a set of operations on a collection of objects.

> ⚠ If you are correctly authenticated in the system, but do not possess the necessary privileges to perform a particular action, the system rejects your attempt to perform the operation, triggering a response with HTTP code 403 Forbidden.

1.3.2.2.3 UMC Security Concept for Opcenter Intelligence

Distribution: UM Server Roles

Opcenter Intelligence supports only the following UMC roles:

- UM ring server.
- UM server (UM agents are not supported).

The TCP port 4002 of the machine where UMC is running should be protected by a firewall.

UMC Security Controller Settings

See Security Controller for detailed information about this topic.

Physical Protection

To ensure security levels in UMC, the primary prerequisite is that the target system that hosts the UMC Server (in this case, Opcenter Intelligence) be correctly configured. In particular, it is mandatory:

- To use the administrative account only for administrative operations.
- To protect the folders used by the UM Server:
  - %ProgramData%\Siemens\UserManagement\CONF
  - %ProgramData%\Siemens\UserManagement\CERT

> ⚠ Do not modify the files contained in these folders. They can only be modified using the tools provided by UMC.

- To use a dedicated account for the UM Server launcher (this account must belong to the Windows Group UM Service Account created by UMC setup).

Administrator Group (root) and Least Privilege

The UMC built-in Administrator role is used to grant "root" privileges to a specific user. Use this role only for installation and disaster recovery purposes. In addition, apply a strong password policy for users associated with this role and revoke this role when it is no longer necessary.
The lowest privileges should be used to administer UMC functionalities using operation accounts in order to

perform administrative operations. To follow this principle, assign a specific UMC user to the UMC provisioning service (see the specific command in the *Central User Management UMC Programming and Operating Manual*).

HTTPS Configuration

UMC works with either HTTP and HTTPS protocol. It is strongly recommended that you enable the HTTPS protocol in a plant environment. For more details on UMC configuration, see *Central User Management UMC Programming and Operating Manual*.

Password Strength

UMC provides the following default values for the user global account policy:

Name	Description	Default Value
SL_PWD_MIN_LEN	Minimum password length (number of characters).	8
SL_PWD_MAX_LEN	Maximum password length (number of characters).	120
SL_PWD_MIN_LOW_CHAR	Minimum number of lower case characters allowed in the password.	1
SL_PWD_MIN_UP_CHAR	Minimum number of upper case characters allowed in the password.	1
SL_PWD_MIN_ALPHA_CHAR	Minimum number of alphanumeric characters allowed in the password.	1
SL_PWD_MIN_NUM_CHAR	Minimum number of numeric characters allowed in the password.	1
SL_PWD_MIN_OTHER_CHAR	Minimum number of special characters allowed in the password.	0

These recommendations should be followed:

- Maintain at least the default values for password account policies or to make them more restrictive.
- Force the user to change the password at first login, if the password assigned to a new user does not satisfy the password account policies.
- Force the user to change the password, if the password has been reset and does not satisfy the password account policies.
- Do not store passwords in user stores. If you need to verify passwords, it is not necessary to store the passwords. Instead, store a one-way hash value and then recompute the hash using the user-supplied passwords. To mitigate the threat of dictionary attacks against the user store, use strong passwords, and incorporate a random salt value within the password.

Access Control

The following UMC roles are used by Opcenter Intelligence:

Name	Description
UMC Viewer	Can access the user management configuration without making modifications.

1.3.2.3 Patch Management

In general, office PC systems are protected against malware. Any weak points that are discovered in the operating system, in Microsoft SQL Server instances or in any other installed component must be eliminated by installing updates and patches. Likewise, industrial PCs and PC-based control systems in the plant network require corresponding protective measures.
Systems should be updated and patched on a regular basis to address potential security risks and known exploits. To accomplish this, Microsoft removes security gaps in its products and provides these corrections to its customers via official updates/patches.
To ensure secure and stable operation in Opcenter Intelligence, the installation of "Security patches" and "Critical patches" is recommended. Siemens will provide customer support only if these updates have been installed and solely for problems that are unrelated to such updates.
You can find information on Microsoft updates and the Windows Server Update Services (WSUS) on the following Microsoft pages:

- http://technet.microsoft.com/en-us/
- http://www.microsoft.com/wsus

The support for implementing patch management in your system is available from the Industrial Security Services. You can find additional information and the corresponding contacts at http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/default.aspx.

1.3.2.4 Malware Detection and Prevention

This section focuses on protecting the automation system and its computers against malicious software. Malicious software and malicious programs (malware) refer to computer programs that have been developed to execute undesirable and possible damaging functions. There are various types of malware available:

- computer viruses
- computer worms
- trojan horses
- other potentially-dangerous programs, such as:
    - backdoor
    - spyware
    - adware
    - scareware
    - grayware

A virus scanner or antivirus program is a software that detects, blocks and, if necessary, removes malware.
The use of a virus scanner on the computers of an automation plant must not interfere with the plant's process mode. The following two examples illustrate two situations which may arise on a production system where a virus scanner is used:

- Even when infected with malware, a computer might not be switched off by a virus scanner, this could then lead to losing control of the production system (for example, for an OS server).
- A project file "infected" by malware (for example, a database archive) might not be automatically moved to quarantine, blocked or deleted.

It is advisable to use a virus scanner with server-client configuration where:

- The virus scanner server is a computer that centrally manages virus scan clients, downloads virus signature files (virus patterns) from the virus scanner vendor sites and distributes them to the virus scanner clients.
- The virus scanner client is a computer that is checked for malware and managed by the virus scanner server.

In accordance with the rules for distributing components into security cells, the virus scanner server must be singled out in a separate network (Perimeter network / DMZ).

⚠ Although there are no known compatibility issues at the moment, the current release officially supports only Trend Micro OfficeScan 11.0.

1.4 Preliminary Configurations

Before installing Opcenter Intelligence, you must perform the following preliminary steps:

- Install ASP.NET and IIS Role Services
- Install Microsoft SQL Server
- Install the License Server

Depending on your data sources:

- Enable Support in SIMATIC IT MOSC
- Configure QMS or Opcenter Quality Database

Additional Configurations

Temp Folder

The *C:\\Temp* folder is the default folder in which temporary cache files used by ETLs are saved. This folder must be created if it does not exist. You can create it in any accessible and writable directory of your file system and give it a different name. Its path must be specified during the creation of the environment.

HTTP Strict Transport Security (HSTS)

Make sure that in IIS Manager > **Sites** > **Default Web Site**, HTTP Strict Transport Security (HSTS) is disabled. For more details, see Troubleshooting: Opcenter Intelligence.

1.4.1 Installing ASP.NET and IIS Role Services

This operation can be executed either automatically or manually.

Prerequisites

Internet Information Services is installed.

✓ Check whether a MIME Type exists in IIS. If not, you should add it by following the procedure described at the following links:
- https://technet.microsoft.com/en-us/library/cc725608(v=ws.10).aspx
- https://www.iis.net/configreference/system.webserver/staticcontent/mimemap

Executing the procedure manually

1. Select **Start > Administrative Tools > Server Manager**.
2. Select the **Manage > Add Roles and Features** command.

3. Under **Server Roles** install the following options.
4. Under **Features** install the following options.

> The actual layout of the configuration panels, the ordering of the options and the specific version of ASP.NET may vary according to the Operating System, updates and patches installed.

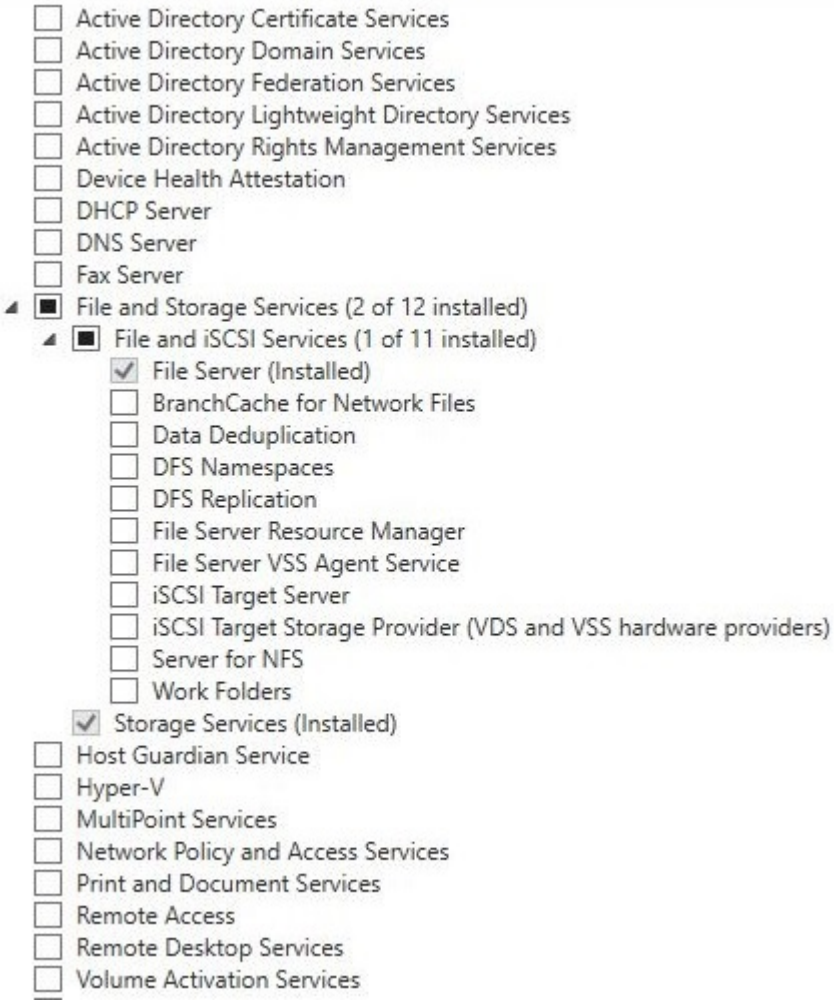
Executing the procedure automatically

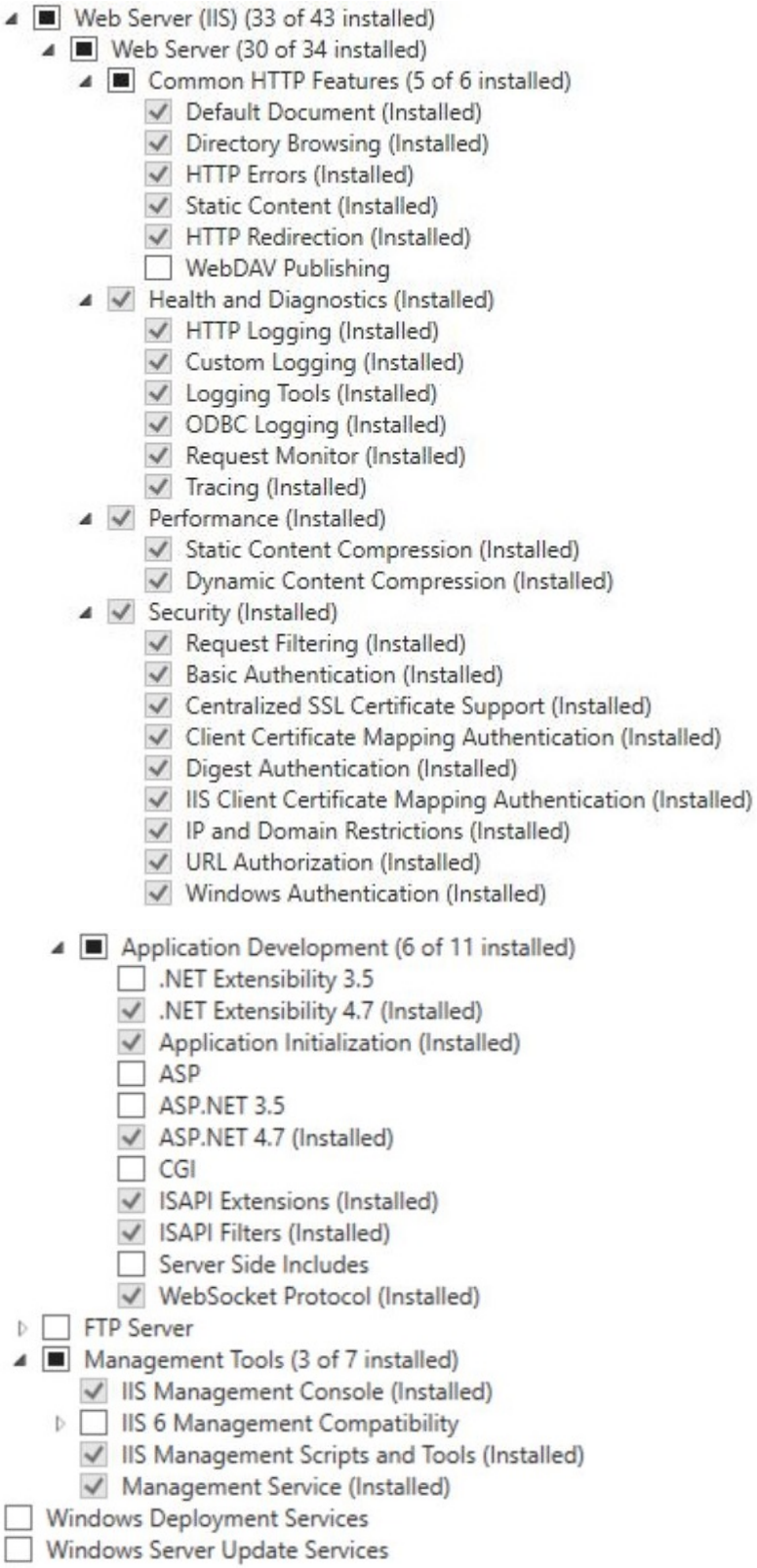
Launch the **EnableRolesAndFeatures.ps1** script that you can find in the ISO root folder in the **ConfigurationScripts** folder.

If the script fails, a message is returned advising you to execute the operation manually following the instructions contained in the procedure below.

1.4.1.1 Server Roles

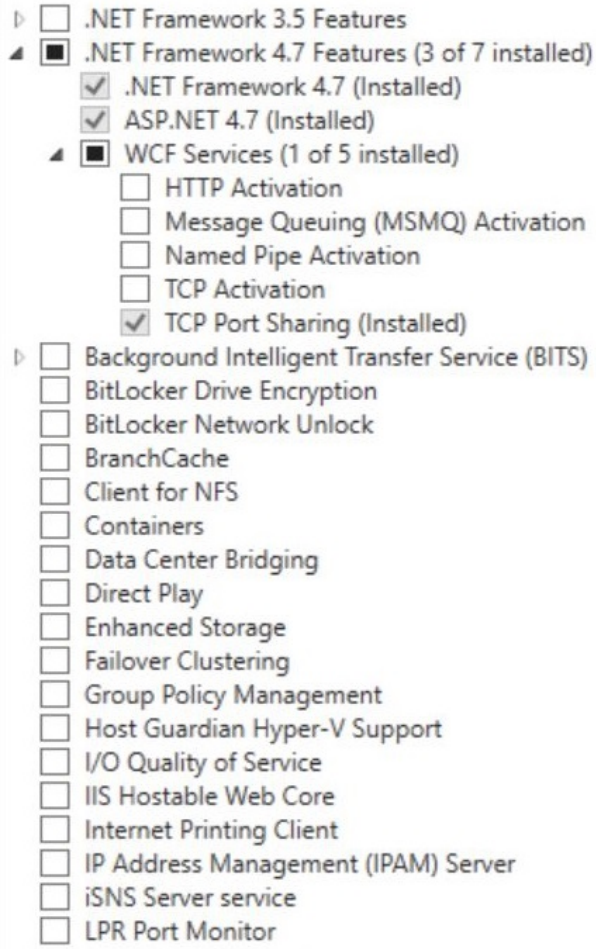
> When you are configuring the ASP.NET Module and IIS Role Services for the first time, not all the nodes can be expanded as displayed in the following screenshots. In this case, select the top node to automatically install all the related sub-features.



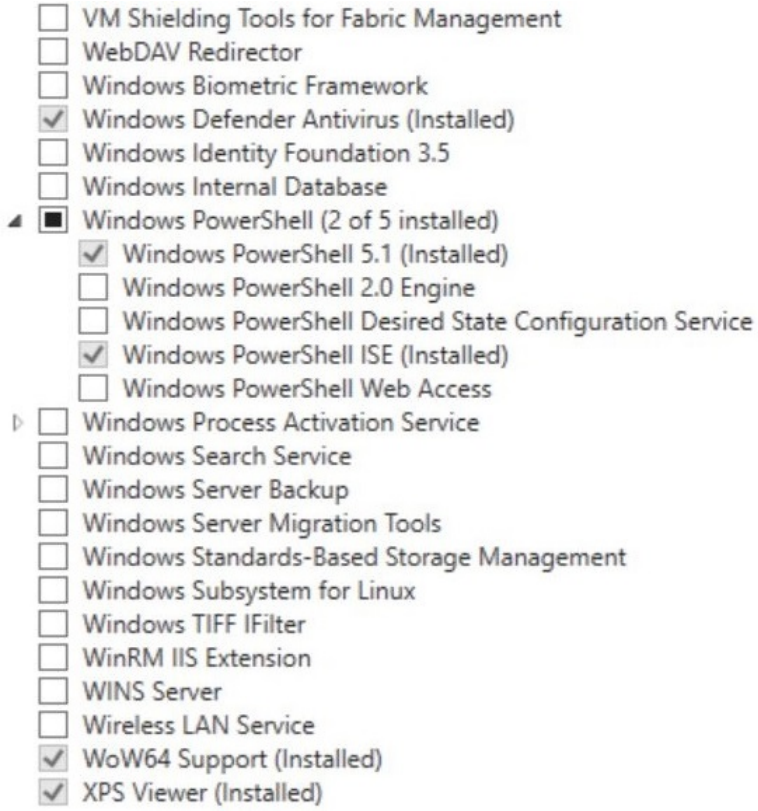

Web Server (IIS) (33 of 43 installed)
Web Server (30 of 34 installed)
Common HTTP Features (5 of 6 installed)
Default Document (Installed)
Directory Browsing (Installed)
HTTP Errors (Installed)
Static Content (Installed)
HTTP Redirection (Installed)
WebDAV Publishing
Health and Diagnostics (Installed)
HTTP Logging (Installed)
Custom Logging (Installed)
Logging Tools (Installed)
ODBC Logging (Installed)
Request Monitor (Installed)
Tracing (Installed)
Performance (Installed)
Static Content Compression (Installed)
Dynamic Content Compression (Installed)
Security (Installed)
Request Filtering (Installed)
Basic Authentication (Installed)
Centralized SSL Certificate Support (Installed)
Client Certificate Mapping Authentication (Installed)
Digest Authentication (Installed)
IIS Client Certificate Mapping Authentication (Installed)
IP and Domain Restrictions (Installed)
URL Authorization (Installed)
Windows Authentication (Installed)
Application Development (6 of 11 installed)
.NET Extensibility 3.5
.NET Extensibility 4.7 (Installed)
Application Initialization (Installed)
ASP
ASP.NET 3.5
ASP.NET 4.7 (Installed)
CGI
ISAPI Extensions (Installed)
ISAPI Filters (Installed)
Server Side Includes
WebSocket Protocol (Installed)
FTP Server
Management Tools (3 of 7 installed)
IIS Management Console (Installed)
IIS 6 Management Compatibility
IIS Management Scripts and Tools (Installed)
Management Service (Installed)
Windows Deployment Services
Windows Server Update Services

1.4.1.2 Features

When you are configuring the ASP.NET Module and IIS Role Services for the first time, not all the nodes can be expanded as displayed in the following screenshots. In this case, select the top node to automatically install all the related sub-features.




Management OData IIS Extension
Media Foundation
Message Queuing
Multipath I/O
MultiPoint Connector
Network Load Balancing
Network Virtualization
Peer Name Resolution Protocol
Quality Windows Audio Video Experience
RAS Connection Manager Administration Kit (CMAK)
Remote Assistance
Remote Differential Compression
Remote Server Administration Tools
RPC over HTTP Proxy
Setup and Boot Event Collection
Simple TCP/IP Services
SMB 1.0/CIFS File Sharing Support
SMB Bandwidth Limit
SMTP Server
SNMP Service
Storage Migration Service
Storage Migration Service Proxy
Storage Replica
System Data Archiver (Installed)
System Insights
Telnet Client (Installed)
TFTP Client



1.4.2 Microsoft SQL Server Installation and Configuration Tips

For details on Microsoft SQL Server installation and configuration, please refer to *Microsoft SQL Server official documentation*.

Opcenter Intelligence does not support side by side installations of different versions of Microsoft SQL Server on the same computer.

Microsoft SQL Server Components

- The supported versions of Microsoft SQL Server do not include **SQL Server Management Console**, whose installation is however recommended.
- **SQL Server Integration Services** installation is mandatory and must be installed on the same machine where Opcenter Intelligence Core is running.
- **SQL Server Agent** installation is mandatory.

(*Only for SQL Server versions previous to SQL Server 2019*) After you have installed SQL Server, check if the **Microsoft.SqlServer.Smo.dll** is installed in the GAC_MSIL folder of Global Assembly Cache (GAC). If it is not installed, you can install it from the SDK or the Feature Pack.

SQL Server Agent Account

The account that the SQL Server Agent service runs as must be a member of the ***sysadmin*** fixed server role. For details on how to configure SQL Server Agent account, see https://docs.microsoft.com/en-us/sql/ssms/agent/select-an-account-for-the-sql-server-agent-service?view=sql-server-ver15. This user must also have the roles

required to read data sources, which are described in the *Prerequisites* section of each data source page (see *How to Configure a Project* > *Selecting Sources* in *Opcenter Intelligence User Manual*).

⚠ If you want to configure the Core Service user without the ***sysadmin*** role, see Configuring Opcenter Intelligence without SQL Server sysadmin role. This configuration is not recommended nor supported.

Configuring the Integration Services Catalog Automatically

This operation can be executed automatically by launching the **CreateSSISCatalog.ps1** script that you can find in the **ConfigurationScripts** folder in the ISO root folder. Make sure that the user who is going to run the script has the **sysadmin** role in SQL Server. When running the script, make sure to enter a password, otherwise a generic error is returned. If the script fails, a message is returned advising you to execute the operation manually by following the procedure below.

Configuring the Integration Services Catalog Manually

After SQL Server installation and before installing Opcenter Intelligence, do the following:

1. Verify if the SQL Server common language runtime (CLR) integration feature is enabled, otherwise enable it and then in SQL Server Management Studio, right-click the server and select the **Restart** command. For more information, see http://msdn.microsoft.com/en-us/library/ms254498(v=vs.110).aspx.
2. In SQL Server Management Studio, right-click the **Integration Services Catalog** node and then select the **Create Catalog** command.
3. Select the **Enable CLR Integration** checkbox.
4. Select the **Enable automatic execution of Integration Services stored procedure at SQL Server startup** checkbox.
5. In the available edit boxes type a password to protect the SSISDB database.
6. Click **OK**: the **SSISDB** folder is displayed in the tree list.
7. Right-click the **SSISDB** folder and then select the **Create Folder** command.
8. Type **Siemens** in the **Folder name** edit box.

   ℹ Make sure to write the name of the **Siemens** folder correctly (the first letter is capitalized and the other letters are lower-case) as it is case-sensitive.
9. Click **OK**.

⚠ When the SQL Server SSISDB is created, the snapshot isolation level is disabled by default. This can cause a deadlock during the parallel execution of two ETL flows. It is suggested that you enable the snapshot isolation level on this database and set it as default for all transactions.

1.4.3 Installing the License Server

Siemens Advanced Licensing Technology (SALT) is a prerequisite for Opcenter Intelligence.

The License Server should be installed before installing Opcenter Intelligence either on an Opcenter Intelligence machine or on a separate machine where Opcenter Intelligence is not installed.

Installation File and Documentation

The installation file and the documentation manuals are available on Support Center at the link https://support.sw.siemens.com/en-US/product/1586485382/downloads

Siemens License Server installation and usage are documented in the following manuals:

- *Siemens Digital Industries Software License Server Installation Instructions* (**sw_siemens_license_server_install.pdf**)
- *Siemens Digital Industries Software Licensing Manual for PLM Products* (**sw_siemens_licensing_plm.pdf**)

The Siemens License Server installer and manuals have been removed from Opcenter Intelligence ISO.

Prerequisites

You have obtained a valid license file.

Procedure

1. Save the license file (with **.lic** extension) in a directory accessible to the license server host.
2. Download the Siemens License Server installation file from Support Center.
3. Copy the file to a temporary directory on your local hard drive.
4. Launch the setup program.
5. Follow the instructions contained in the *Siemens Digital Industries Software License Server Installation Instructions* manual.
6. In particular, do the following:
    - Provide the location of the license file. If you are upgrading from a previous version of the product, you do not need a new license file, you can use the same license file you used for the previous version.
    - Configure the correct port:
        - If you are installing the product for the first time, leave the license server default port (29000).
        - If you are upgrading from a previous version of the product, you may want to keep the previously configured port number.
    - Specify a destination folder for the installation.
    - Select the **I don't want this feature** checkbox.
7. Click **Done** to quit the installer.

Make sure the **Siemens License Server** service is running. When you restart the server, the license check is executed after a delay of five minutes. To reduce this delay, as a workaround you can restart the **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost** service.

1.4.4 Enabling Support in SIMATIC IT MOSC

If your data source is one of the following:

- SIMATIC IT Production Suite 7.0 SP1 - 7.0 SP2 - 7.1 - 7.2 - 8.0
- SIMATIC IT Historian 7.2
- SIMATIC IT Line Monitoring System 2.2 SP2 HF1 - 2.3 - 2.4 - 2.5 - 2.6 - 2.7
- SIMATIC IT Unified Architecture Discrete Manufacturing 1.0 - 1.1 - 1.2 - 1.3 - 2.3 - 2.4 - 2.5

you must activate the integration with Opcenter Intelligence by enabling the **Opcenter Intelligence support** in SIMATIC IT MES Option Servers Configuration (MOSC).

For more details on how to perform this operation, see *SIMATIC IT Production Suite documentation*.

1.4.5 Configuring QMS or Opcenter Quality Database

The following procedure is required in order to execute a deploy operation in Opcenter Intelligence if you are using QMS as a SQL Server data source. It must be executed during the installation of QMS Professional or Opcenter Quality.

Prerequisite

The program **DBchange.exe** is required to configure the database.

Procedure

1. Navigate to the installation directory **...\QMSxxxx\Bin** and execute the **dbchange.exe** file.
2. In **DBchange** startup window, select **System > Prepare Incremental Load Support**.
3. In the window that opens, select the following database tables where the **DTUPDATE** column needs to be added:
    - ARTIKEL
    - EINHEIT
    - FEHLER
    - MANDANT
    - MM_KOPF
    - PERS_USER
    - PP_KOPF
    - RQMS_FEHLER
    - RQMS_MASS
    - RQMS_MAS
    - RQMS_POS
    - RQMS_STAMM
    - RQMS_TXT_ZUW
    - SPA_KOPF
    - SPE_VAR
    - STICHPROBE
    - WERK
4. Launch the procedure: the tables are updated and a trigger is created to keep the value up-to-date on inserting or updating.

For more information, see *QMS Professional or Opcenter Quality documentation*.

2 How to Install Opcenter Intelligence

You can install Opcenter Intelligence either by launching the installation file from the ISO folder or via Command Line.

Available Operations

- Install Opcenter Intelligence Interactively
- Install Opcenter Intelligence via Command Line

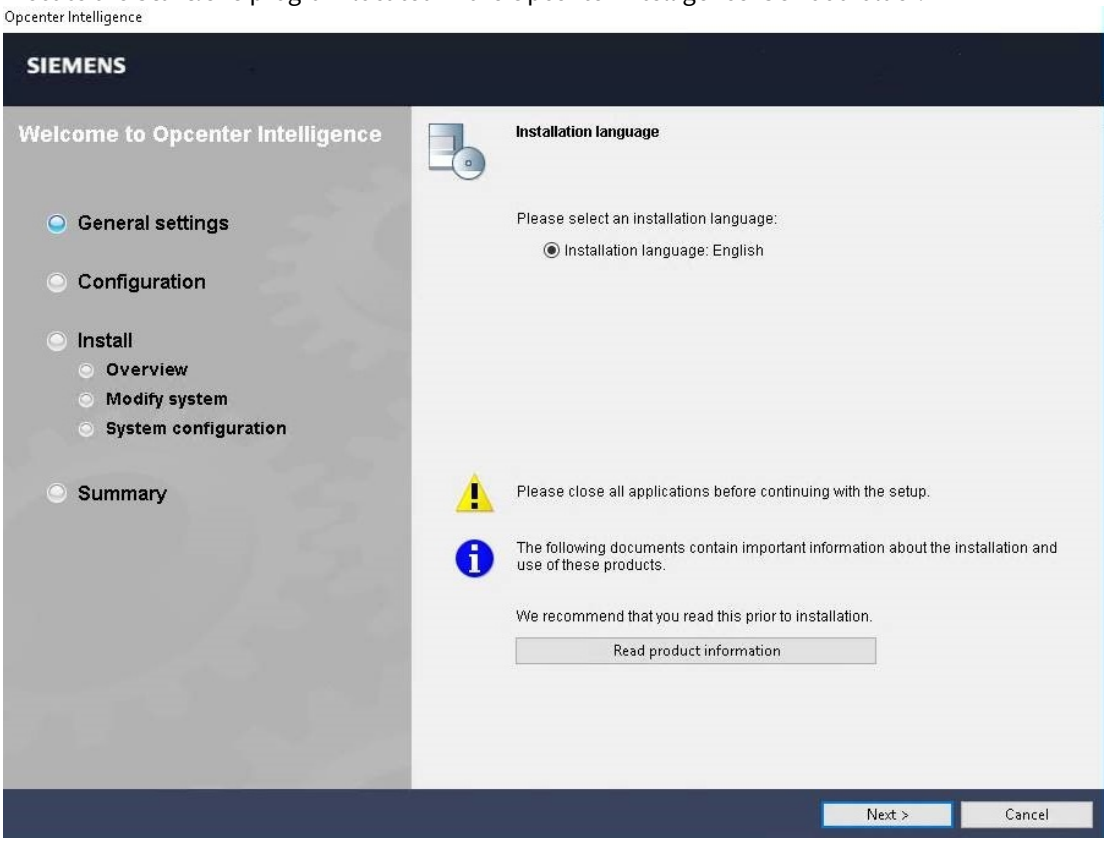
2.1 Installing Opcenter Intelligence Interactively

Prerequisites

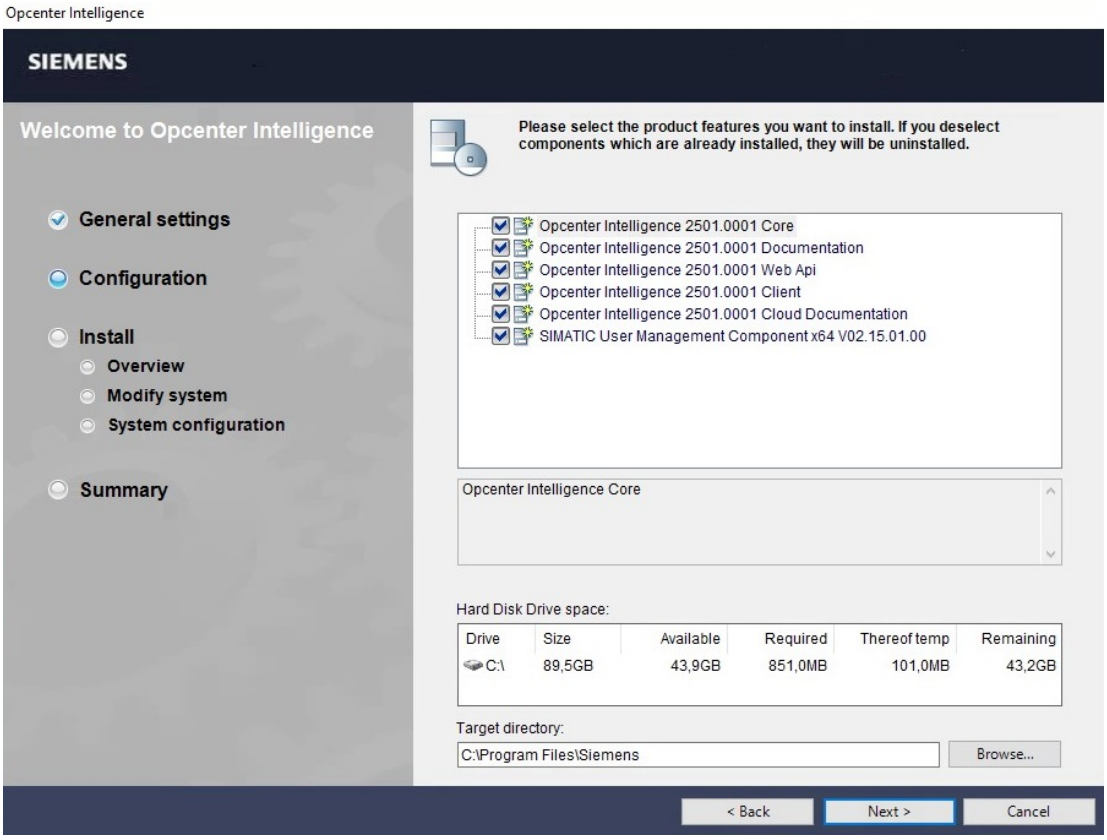
Verify that all required prerequisites are satisfied, depending on the selected scenario.

Procedure

1. Execute the **Start.exe** program located in the Opcenter Intelligence ISO root folder.



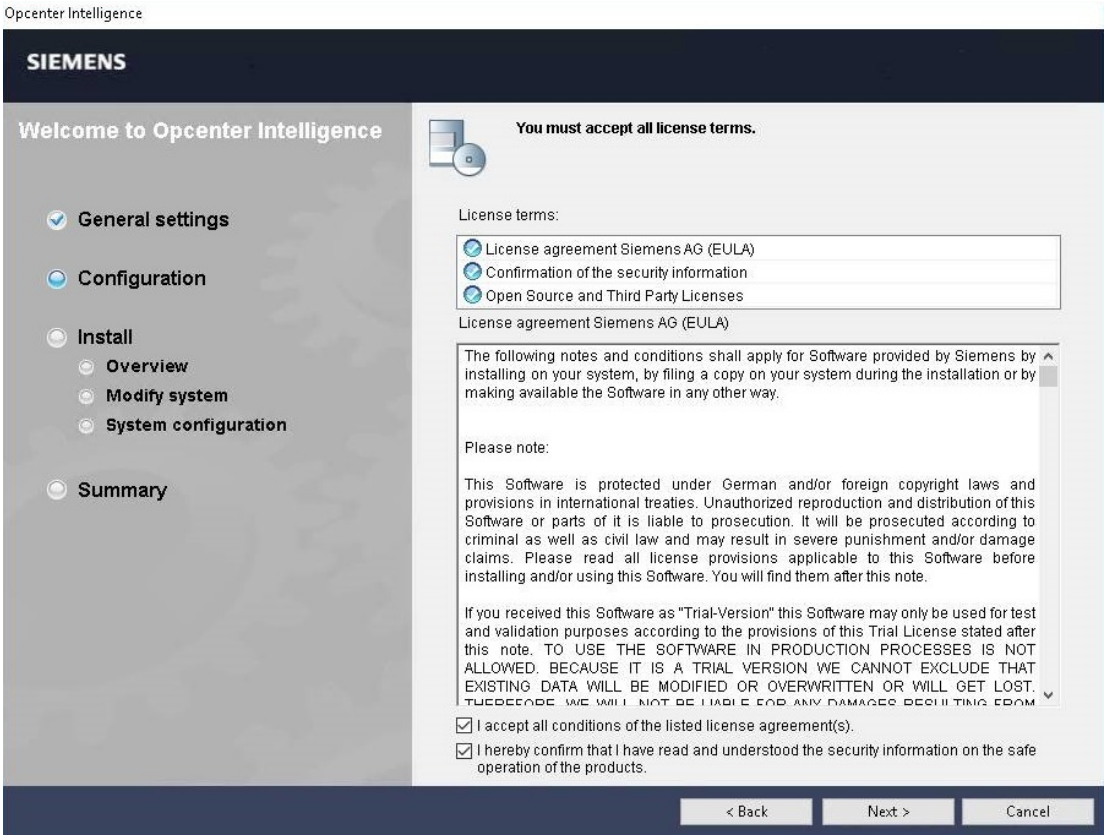
2. Click **Next**.



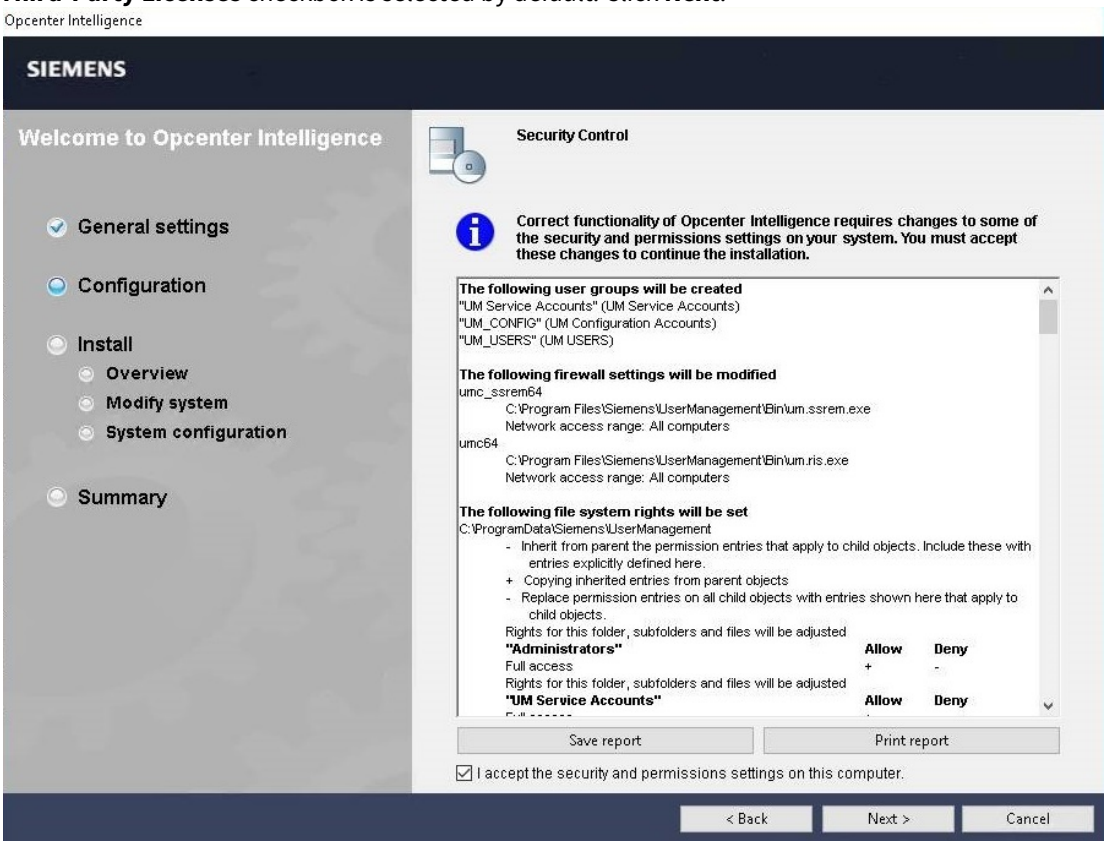
3. Select which product features you want to install depending on the scenario you have chosen to implement and click **Next**. If you clear the checkbox for components that are already installed, they will be uninstalled.

> If you are installing Opcenter Intelligence on the same machine where User Management Component (UMC) is running, UMC 2.15 SP1 is mandatory. If a previous version of UMC has already been installed on that machine, it will be upgraded to version 2.15 SP1.
> Do not clear the **SIMATIC User Management Component x64 V02.15.01.00** checkbox, otherwise the existing UMC will be uninstalled.

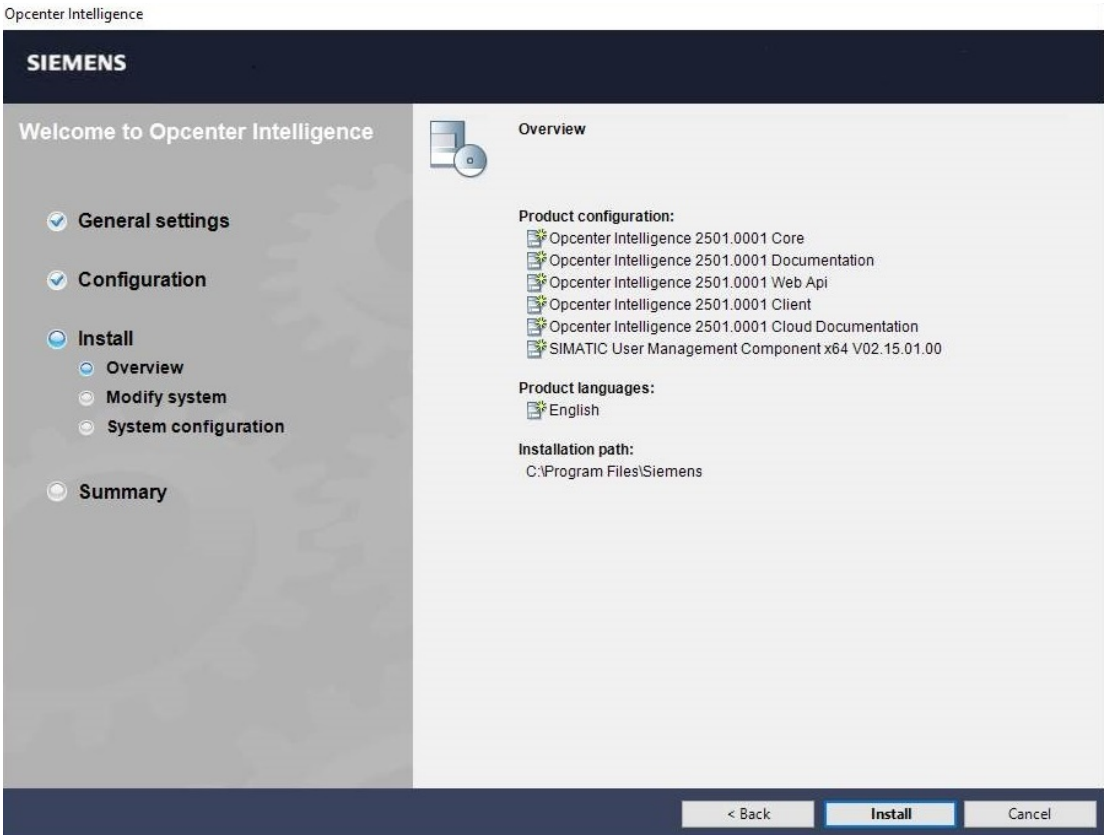
> The **Opcenter Intelligence V.x.x Cloud Documentation** checkbox must be selected if you want to install the entity mapping files in the **<setup drive>Program Files\Siemens\Opcenter\Intelligence\IN\Documentation\MappingFiles** folder. For more details, see the *Manufacturing Data Warehouse Documentation* section in *Opcenter Intelligence Release Notes* > *Documentation* chapter.


Opcenter Intelligence
SIEMENS
Welcome to Opcenter Intelligence
General settings
Configuration
Install
Overview
Modify system
System configuration
Summary
You must accept all license terms.
License terms:
License agreement Siemens AG (EULA)
Confirmation of the security information
Open Source and Third Party Licenses
License agreement Siemens AG (EULA)
The following notes and conditions shall apply for Software provided by Siemens by installing on your system, by filing a copy on your system during the installation or by making available the Software in any other way.
Please note:
This Software is protected under German and/or foreign copyright laws and provisions in international treaties. Unauthorized reproduction and distribution of this Software or parts of it is liable to prosecution. It will be prosecuted according to criminal as well as civil law and may result in severe punishment and/or damage claims. Please read all license provisions applicable to this Software before installing and/or using this Software. You will find them after this note.
If you received this Software as "Trial-Version" this Software may only be used for test and validation purposes according to the provisions of this Trial License stated after this note. TO USE THE SOFTWARE IN PRODUCTION PROCESSES IS NOT ALLOWED. BECAUSE IT IS A TRIAL VERSION WE CANNOT EXCLUDE THAT EXISTING DATA WILL BE MODIFIED OR OVERWRITTEN OR WILL GET LOST.
I accept all conditions of the listed license agreement(s).
I hereby confirm that I have read and understood the security information on the safe operation of the products.
< Back
Next >
Cancel

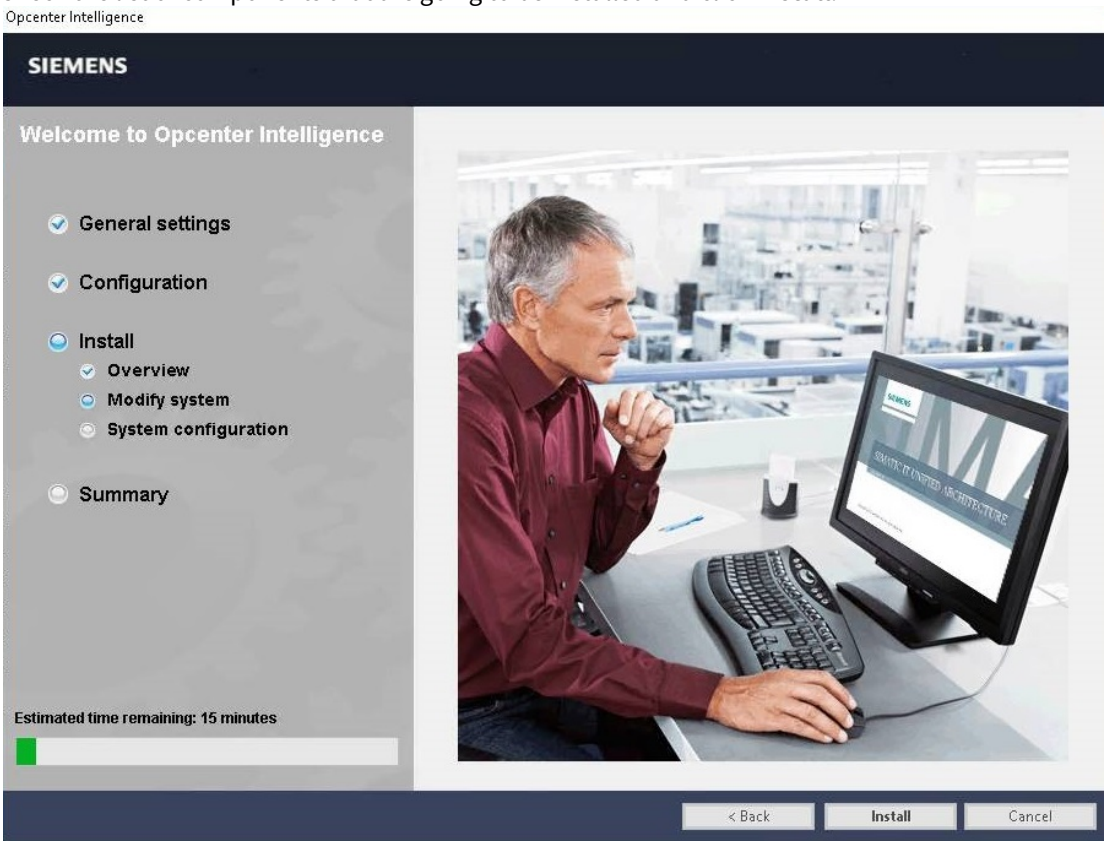
4. Accept the conditions of the license agreement and confirm the security information. The **Open Source and Third-Party Licenses** checkbox is selected by default. Click **Next**.



5. Accept the security and permission settings related to the User Management Component installation and click **Next**.



6. Check the list of components that are going to be installed and click **Install**.



7. Click **Install** again and when the setup is completed, click **Finish**.

2.2 Installing Opcenter Intelligence via Command Line

Opcenter Intelligence allows you to install the product via command line. In this page you can find a description of the operations to be executed when you are installing the system from scratch.

> ⚠ The procedures to install Opcenter Intelligence via command line must be applied bearing in mind that an incorrect usage of scripts may cause system unavailability. Administrative rights are required to perform these operations.

Prerequisites

- All prerequisites required by Opcenter Intelligence are satisfied.
- Hardware and software of the programming device or PC meet the system requirements.
- You have Administrator privileges on your computer.
- All running programs are closed.

Procedure

To start the installation with the desired options directly via the command interface, proceed as follows:

1. Open the Windows command prompt with **Start > Run > cmd**.
2. Switch to the directory that contains the **Start.exe** file.
3. In the command prompt, enter one of the following commands:
    - Installation with visible installation information: **Start.exe /qb <*Parameter*>**

- Installation without visible installation information: **Start.exe /qn <*Parameter*>** or **Start.exe /silent <*Parameter*>**

  > Installation with the **/qb** or **/qn** parameters has the effect that no alarm windows are displayed, even if an error occurs. You can only evaluate the results via the return value. When using the option "REBOOT=Suppress", note that you need to evaluate the return value yourself and possibly restart the system and then restart the installation manually after the system restart in order to make evaluation of the return value possible.

4. Press the <**Return**> key to confirm your entry.

> By default, all setup components are installed. If you want to customize the installation process, see Customizing the Installation for instructions on how to execute the Starting Recording and Playing the Recording procedures.

Examples

See some examples of automated installation via the command line

Available Information

- Parameters for Automated Installation
- Return Values from the Installation Process

2.2.1 Examples of Automated Installation via the Command Line MI

Example of a typical installation with REBOOT=AUTO

The following example shows a typical installation via the command line:

```
Start.exe /qb REBOOT=Auto
```

At the end of the installation, the system is restarted automatically without the request for a confirmation ("REBOOT=Auto").

Example of a complete installation with REBOOT=Suppress

The following example shows a complete installation via the command line:

```
Start.exe /qb REBOOT=Suppress
```

At the end of the installation, restart of the system is suppressed ("REBOOT=Suppress"). This means that you must evaluate the return value yourself and possibly restart the system manually.

Example of querying the return value per batch file

The following example shows you how to query the return value per batch file:

```
SET SetupSuccess=%ERRORLEVEL%
if '%SetupSuccess%' EQU '0' (
```

```
echo Setup successful. Return code: %SetupSuccess%
) else (
if '%SetupSuccess%' EQU '3010' (
echo Setup successful. A reboot is needed! Return code:
%SetupSuccess%
) else (
echo "ERROR during Setup! Return code: %SetupSuccess%
)
)
Pause
```

The return code "1641" also documents successful completion of the installation and that restart has already been initiated. Restart occurs, however, only if "/REBOOT=Auto" is used and for this reason was not evaluated in the batch file. You can find all possible return values under Return Values from the Installation Process.

2.2.2 Parameters for Automated Installation

The following table shows the parameters available for an automated installation:

Parameter	Description
/qb [1]	You can use this parameter to perform an automated installation. During the installation, you receive information on the installation currently being performed. • Without the parameter **qb** or **qn**, you cannot perform an automated installation. • The parameters **qn** and **qb** cannot be used together within one call. • The information during the installation appears in the set installation language. This means that this information matches the texts in the log files. You need these log files, for instance, if you need to contact Product Support. • You can take the results of the installation from the return values.
/qn or **/silent** [1]	You can use this parameter to perform an automated installation. During the installation, you will receive no information on the installation currently being performed. • Without the parameter **qb** or **qn**, you cannot perform an automated installation. • The parameters **qn** and **qb** cannot be used together within one call. • You can take the results of the installation from the return values.
/record	You can use this parameter to start the Record mode. It creates the **autoinstall.rec** file for automated installation.

Parameter	Description
/play	You can use this parameter to start the Play mode. In this mode, you need the configuration file that was created in the Record mode. **Example** /play="c:\siemensconfiguration\autoinstall.rec"
REBOOT	You can use this parameter to specify the restart characteristics during the installation. **Possible Values** • **Auto**: A restart, if necessary, is performed automatically at the end of installation. • **Suppress** [2]: The restart is suppressed at the end of installation. If a restart would have been necessary, the calling process must initiate the restart. Continuation of the installation is also suppressed if this is necessary after the restart (in the case of return value 13010). **Example** REBOOT=Suppress

[1] Installation with the **/qb** or **/qn** parameters has the effect that no alarm windows are displayed, even if an error occurs. You can only evaluate the results via the return value.

[2] If the installation is not yet finished (return value 13010), you first need to restart the system and then the installation in order to make evaluation of the return value possible.

2.2.3 Return Values from the Installation Process

The following table shows the return values from an automated installation along with their descriptions:

Return value	Technical fault description	Description
?	OtherError	Any return value that is not described in the following table generally indicates an error. Detailed information on all errors can always be found in the installation log. Open the most recent log file whose name begins with "SIA".
0	Success	The installation was successful. No errors have occurred.
5	AccessDenied	You do not have appropriate rights. The installation requires administrator's rights.
112	DiskFull	Not enough free space on the target media.

Return value	Technical fault description	Description
1601	InstallServiceFailure	An internal error has occurred during initialization.
1602	UserExit	Cancellation by user occurs most often as the result of Cancel being selected in a dialog.
1603	InstallFailure	An error has occurred while performing the installation.
1605	UnknownProduct	An internal error has occurred during product configuration.
1610	BadConfiguration	An internal error has occurred during product configuration.
1618	InstallAlreadyRunning	Another installation is already running. A simultaneous installation is not possible.
1622	InstallLogFailure	An error has occurred while writing the log.
1627	FunctionFailed	An internal error has occurred.
1633	InstallPlatformUnsupported	This operating system is not supported.
1639	InvalidCommandline	There is an error in the indicated command line.
1641	SuccessRebootInitiated	The installation was successful. A restart has already been initiated to complete the operation.
3010	SuccessRebootRequired	The installation was successful. A restart is absolutely necessary to complete the operation.
5001	PrerequisitesFailure	The installation conditions have not been fulfilled. For more information, you can restart the installation by double-clicking **start.exe**.
5002	InvalidIEVersion	Internet Explorer is not installed or an unsupported version is installed.

Return value	Technical fault description	Description
5003	ResourcesFailed	An internal error has occurred during initialization.
5004	ProductInitFailed	An internal error occurred (the installation media may be defective).
5005	ProductInitNewerVersionInstalled	A newer version of the product is already installed.
5006	ProductInitMoreValuableEditionInstalled	A more complete edition of the product is already installed (e.g. if you are attempting to install a basic version although a professional version is installed).
5007	ProductInitOptionalWithoutMain	You are attempting to install an optional package without the main software.
5008	ProductIncompatibility	A product that is incompatible with the product to be installed is already present.
5009	AutoinstallFileNotFound	The file required for the Play mode could not be found.
5010	AutoinstallUnexpectedContent	The file for the Play mode cannot be read (wrong format, wrong version or unsuitable installation media).
11641	NotCompleteReboot	Setup is not complete and must be continued after restarting. Restarting has already begun. After restarting, you must restart installation.
13010	NotCompleteRebootRequired	Setup is not complete and must be continued after restarting. You must initiate a restart and then restart the installation again.

2.2.4 Customizing the Installation

If you want to customize your installation, you can save your choice using the recording functionality.

Prerequisites

- Hardware and software of the programming device or PC meet the system requirements.
- You have administrator privileges on your computer.
- All running programs are closed.

- To play the recording, the previously recorded file ("*.rec") must be present.

Workflow

To do so, you can execute the following operations:

1. Start Recording
2. Play the Recording

Starting Recording

To record the installation, proceed as follows:

1. Open the Windows command prompt with **Start > Run > cmd**.
2. Switch to the directory that contains the **Start.exe** file.
3. In the command prompt, enter the following command: **Start.exe /record**
4. Press the <**Return**> key to confirm your entry.

Result

The installation dialog opens with the information that you are in Record mode and the system will not be changed. During the recording operation, a configuration file is generated, which can be played in the next step.

Playing the Recording

To play the installation, proceed as follows:

1. Open the Windows command prompt with **Start > Run > cmd**.
2. Switch to the directory that contains the **Start.exe** file.
3. In the command prompt, enter the following command:

```
Start.exe /play=<Drive>:\<Directory>\<File name>
e. g. "Start.exe /play=c:\siemensconfiguration\autoinstall.rec"
```

4. Press the <**Return**> key to confirm your entry.

If no license key is found during the installation, the license transfer is skipped and you can take care of this later with the Automation License Manager.

Result

Installation takes place automatically using the settings recorded in the configuration file.

3 How to Configure Opcenter Intelligence

After installing Opcenter Intelligence, you must perform a number of operations before accessing the working environment.

Workflow

1. Configure Opcenter Intelligence with Opcenter Intelligence Configurator.
2. Configure the HTTPS Protocol for Opcenter Intelligence Components.
3. Check Authentication Keys in IIS.
4. (If you are loading data from an Oracle data source) Configure Oracle Authentication.
5. (If you are loading data from an Oracle data source) Configure the connection between Opcenter Intelligence and Oracle Server.
6. Define Users.
7. *(*Optional*)* Configure the User Management Component Ring Servers.

Additional Operations

- Configure Opcenter Intelligence via Command Line.
- Configure Opcenter Intelligence without SQL Server sysadmin role.

3.1 Configuring Opcenter Intelligence with Opcenter Intelligence Configurator

Opcenter Intelligence Configurator is the stand-alone application that performs the post-setup configuration actions.

- In a distributed scenario, Opcenter Intelligence Configurator must be run on both the Core Server and on the Application Server.
- The user who is going to run Opcenter Intelligence Configuratormust have the **sysadmin** role in SQL Server or be a member of a **sysadmin** group in SQL Server.

Accessing the Configurator

You can run the Configurator in either of the following ways:

- Right-click the Opcenter Intelligence Configurator desktop icon and run the tool as local administrator.
- From **<*target directory*>\Siemens\SimaticIT\Unified\UAMI\SETUP**, run as Administrator the **Siemens.SimaticIT.UAMI.MIStudio20.PostSetup.exe** file. <*target directory*> is either the default folder **C:\Program Files\Siemens** or the target directory you have specified during the installation.

Preliminary Check on Server Connectivity

When you launch the Configurator, a preliminary validation process is executed to check server connectivity and inform you about any connection issue before starting the configuration. The connection check is performed on SQL Server for the engineering database, on Opcenter Intelligence Core Service and Web API Service, on UMC Server and License Server. A check is also performed on Gateways' Services availability. If no issue is found, the configuration process is started. In case of connection issues, a pop-up window shows the list of unreachable servers. You are then prompted to choose if you want to continue anyway (bearing in mind that the configuration may fail) or to try solving the issues before proceeding.

Available Options

After you have launched the Configurator, you are prompted to choose one the following options:

- Manage Configuration - to be selected the first time you run the Configurator and every time you want to change the configuration settings.
- Upgrade Configuration - to be selected when you need to update the configuration in case of an upgrade from a previous version of the product.
- Tableau Server Connection Configuration - to perform the configuration needed to navigate through the items created in Tableau® Server and view the resulting dashboards embedded inOpcenter Intelligence. Ignore this option if you do not need to configure Tableau® Server.

Opcenter Intelligence Configurator Log File and XML Files

Opcenter Intelligence Configurator log file is called **Siemens.SimaticIT.MIStudio20.PostSetup.log**. The default location of this file is **C:\ProgramData\Siemens\Opcenter\Intelligence\IN\LogFiles\SetUp**.

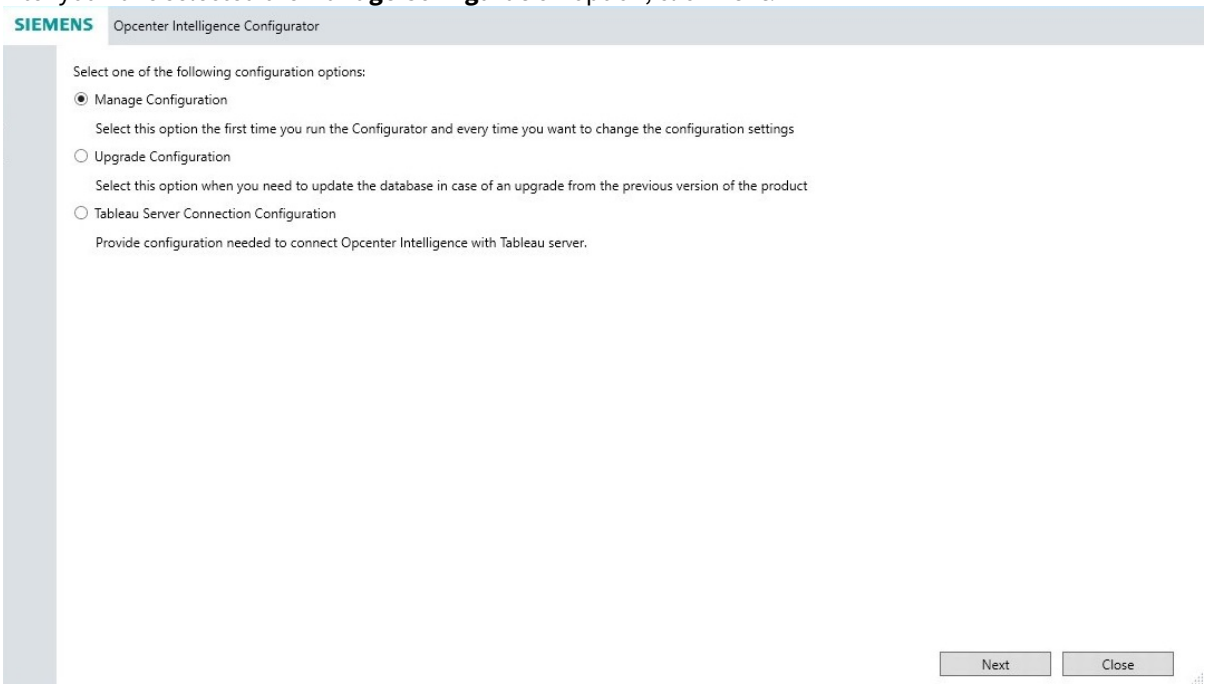
Alternatively, if logs are not present in the default location, you can find it in **C:\Users\<*username*>\AppData\Local\Temp**

The Configurator XML files are stored at the following path: **C:\ProgramData\Siemens\Opcenter\Intelligence\IN\Setup\SetupParameters.xml**

3.1.1 Manage Configuration

Procedure

1. After you have selected the **Manage Configuration** option, click **Next**.



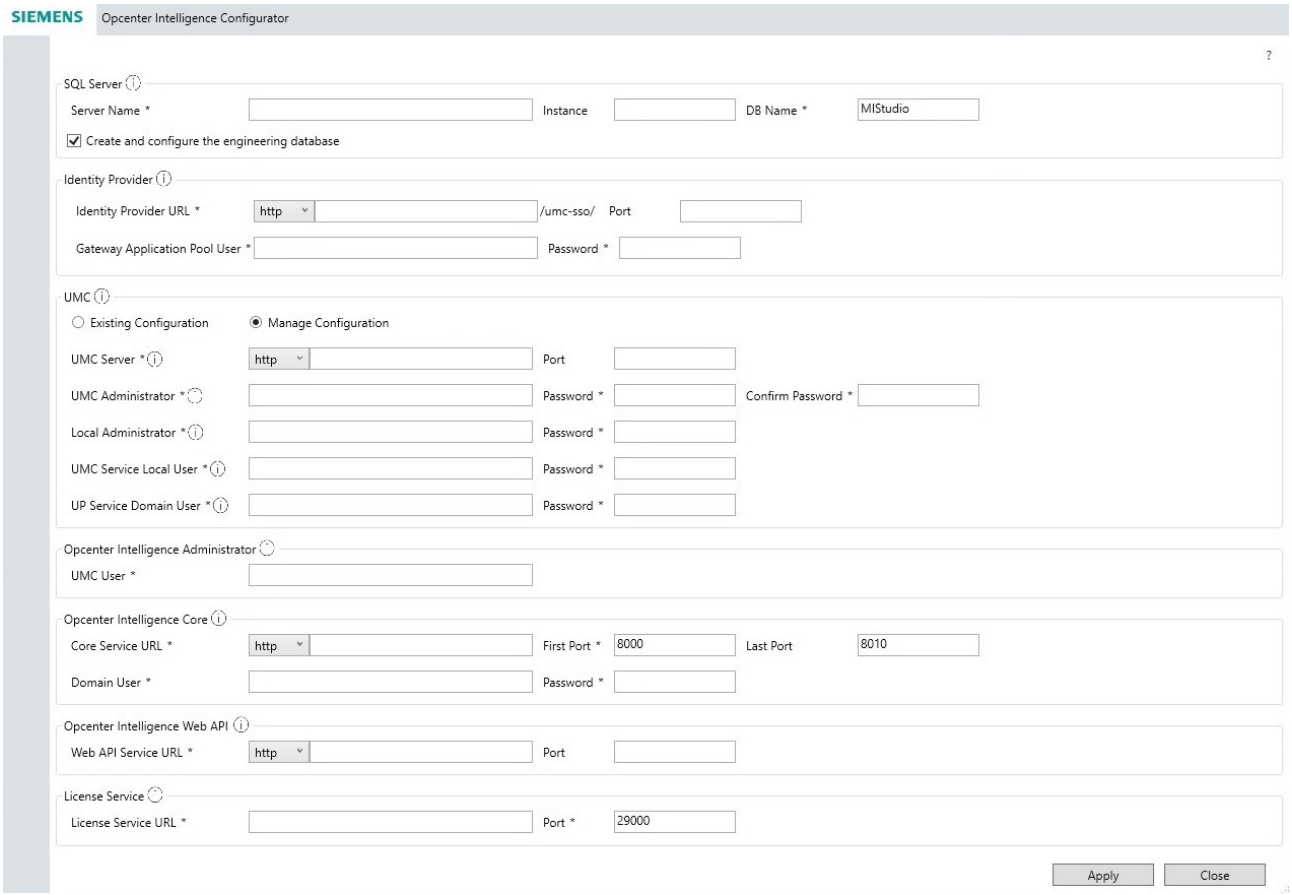
2. Insert the required information as explained in the tables below. The fields marked with an asterisk are mandatory.

- Click the ⓘ icon next to field names to quickly get information on how the fields should be configured.
- The selected communication protocol (either HTTP or HTTPS) must be the same in all configuration sections.

3. When you have completed the configuration, click **Apply** and wait for the notification that confirms the successful completion of the configuration.

   If you have inserted the number of one or more ports that are already being used by other processes, a warning message appears and the configuration is aborted.

4. Click **Close**.
5. To ensure that UMC functions correctly, add the following URL to UMC allowlist: **http(s)://*<machine name>*/UserGateway/Login/Login**. For more details, see *Create allowlist entry* in *Central User Management UMC Programming and Operating Manual*.
6. Check that the **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost** service is in **Running** status. If not, start this service.



By clicking the **?** button in the upper right corner of the Configurator you can open the *Opcenter Intelligence Installation Manual* or the *Release Notes*.

SQL Server

Field	Action
Server Name	Insert the name or IP address of the computer where SQL Server is running. This name is mandatory even if you do not want to create and configure the database.
Instance	Insert the SQL Server instance name. If you have not created an instance, this field can be left empty.
DB Name	Insert the name of the database (the default name is **MIStudio**). This name is mandatory even if you do not want to create and configure the database.
Create and configure the engineering database	Select this checkbox if you want the Configurator to create and configure the engineering database.

Identity Provider

Field	Action
Identity Provider URL	Select the protocol for the UMC identity provider and insert the <*Full computer name*> of the machine where UMC Server is running and the **Port** number. This computer name must match with the name to be inserted in the **UMC Server** field in the **UMC** configuration section. ⚠ The protocol for UMC Server can be either HTTP or HTTPS. To avoid security issues, it is strongly recommended that you enable the HTTPS protocol.
Gateway Application Pool User	Insert the <*computer name*>\<*user name*> of a Windows user who can configure the Application Pools of Gateway Services and the corresponding password. ⚠ In a distributed scenario where the machines do not belong to any domain, you must insert **.\<*user name*>** in this field; this user name must be present with the same password in both machines of the scenario. You can also use a Windows user present in both machines: for example: **.\Administrator**

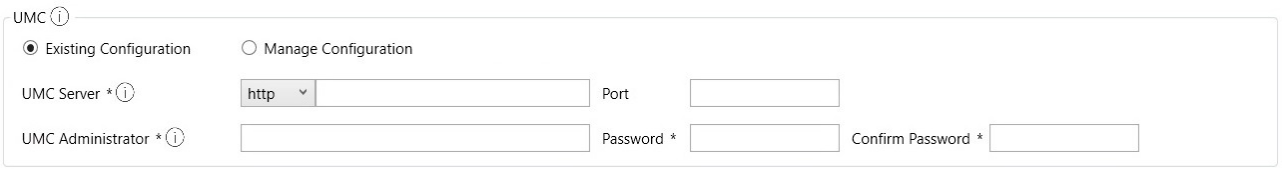
UMC

Select one of the two radio buttons according to the UMC settings required for your scenario. See the table below for the detailed description on how to fill the different fields.

Existing Configuration

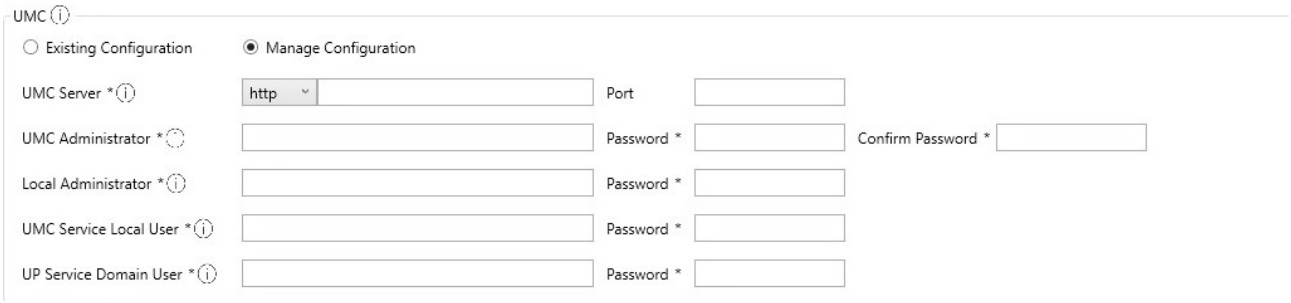
Select this radio button if UMC is already present and does not need to be configured by Opcenter Intelligence Configurator.

Note that reconfiguring UMC entails the execution of a set of complex operations. For more information, see *Central User Management UMC Programming and Operating Manual*.



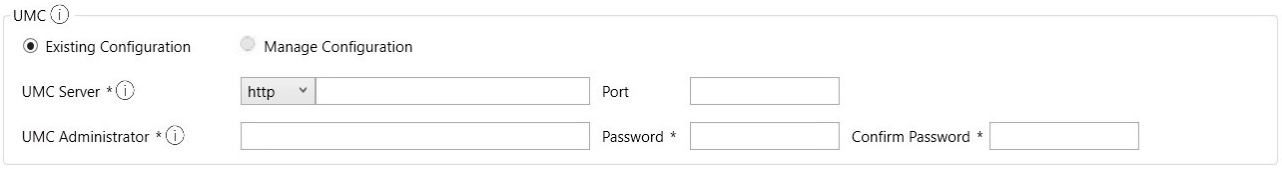
Manage Configuration

Select this radio button if UMC has been installed by the Opcenter Intelligence setup and needs to be configured for the first time.



Manage Configuration option not selected

When UMC is not installed on the local machine, the **Manage Configuration** option is not selected because UMC was configured on a different machine.



Field	Action
UMC Server	Select the protocol for the UMC server and insert the <*Full computer name*> of the machine where UMC Server is running and the **Port** number. This computer name must match with the name to be inserted in the **Identity Provider** section. The protocol for UMC Server can be either HTTP or HTTPS, but HTTPS is recommended. If you want to use the HTTP protocol, see *Central User Management UMC Programming and Operating Manual*.

Field	Action
UMC Administrator	This user has the privileges of Administrator with full control of UMC. For example, he is the only user able to import all other users from the domain directory into UMC. Two situations may occur: • You are configuring UMC for the first time: this user is created by the Configurator. Insert the <*user name*> you want to assign to this UMC user. • UMC has already been configured: insert the correct <*user name*> of the existing UMC user. Insert the corresponding **Password** and confirm it. This password is mandatory even if you have selected the **Existing configuration** radio button and do not need to configure UMC.
Local Administrator	Insert the <*computer name*>\<*user name*> of the local machine administrator and the corresponding **Password**.
UMC Service Local User	Insert the <*domain name*>\<*user name*> of the existing domain user with local Administrator privileges who is going to run UMCService. Insert the corresponding **Password**.
UP Service Domain User	Insert the <d*omain name*>\<*user name*> of a domain user who has Active Directory access rights and who is going to run UPService. Insert the corresponding **Password**. For more details on UMC and UP Service users, see *Central User Management UMC Programming and Operating Manual*.

Opcenter Intelligence Administrator

Field	Action
UMC User	Insert the <*user name*> of the UMC user who is going to be the Opcenter Intelligence Administrator. This is the user who will be able to grant access to other users. This user is not created automatically, but will have to be created manually in UMC with exactly this name. This user must be added to the list of User Management Component (UMC) users (see Creating Opcenter Intelligence Users in UMC).

Opcenter Intelligence Core

Field	Action
Core Service URL	Select the protocol for the Core Server and insert the name of the computer where the Core Server is running. Insert the number of the **First Port** (the default is 8000) of a series made up of 11 ports. The **Last Port** number is automatically inserted by the system. ⚠ Before configuring these fields, check that all the ports included in the list between first port and last port are not used by other processes.
Domain User	Insert the <*domain name*>\<*user name*> of the user who is going to run the Core Service. He must be a domain user with local Administrator privileges. This is the user who will run Opcenter Intelligence flows and who will therefore connect to the different data sources and write data on the Manufacturing Data Warehouse. Insert the **Password** for this user. ⓘ If your scenario is made up of different machines including data source machine(s), and you are using local Windows users, the Windows user who will run the Core Service and access data sources must be the same on all machines and use the same password. **Important Notes on Core Service Domain User** • The first time this user is configured in Opcenter Intelligence Configurator you must assign the **Log on as a service** user right to the service account, using **Local Security Settings** (**Secpol.msc**) under **Local Policies** > **User Rights Assignments**. • These credentials will also be used in **SQL Server Security > Logins** to create the login. • This user must have the roles required to read data sources. • This user can be configured without the ***sysadmin*** role. For details, see Configuring Opcenter Intelligence without SQL Server sysadmin role. ⚠ The following special characters are not supported in the **Domain User** field: " / [ ] : ; | = , + * ? < > @ and space

Log file for Opcenter Intelligence Core Service

The log file for Opcenter Intelligence Core Service is called **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost.log** and is stored in **C:\ProgramData\Siemens\Opcenter\Intelligence\IN\LogFiles\CoreService**

Opcenter Intelligence Web API

Field	Action
WebAPI Service URL	Select the protocol for Opcenter Intelligence Server and insert the name of the computer where the Server is running. Insert the Port number. If you are using the default port (80 for HTTP and 443 for HTTPS), this field can be left empty.

License Server Configuration

Field	Action
License Service URL	Insert the computer name of the License Server and the **Port** number (default 29000). For more details, see Installing the License Server. If you are upgrading Opcenter Intelligence from a previous version of the product, see Upgrading from previous versions of Opcenter IN to Opcenter IN 2501.0001 to find recommendations on configuring the proper port number for the license server.

Running Opcenter Intelligence Configurator after the first time

The Configurator (**Manage Configuration** option) can be run more than once, for example if you want to split the configuration into different steps or if you want to change your settings after the first configuration.

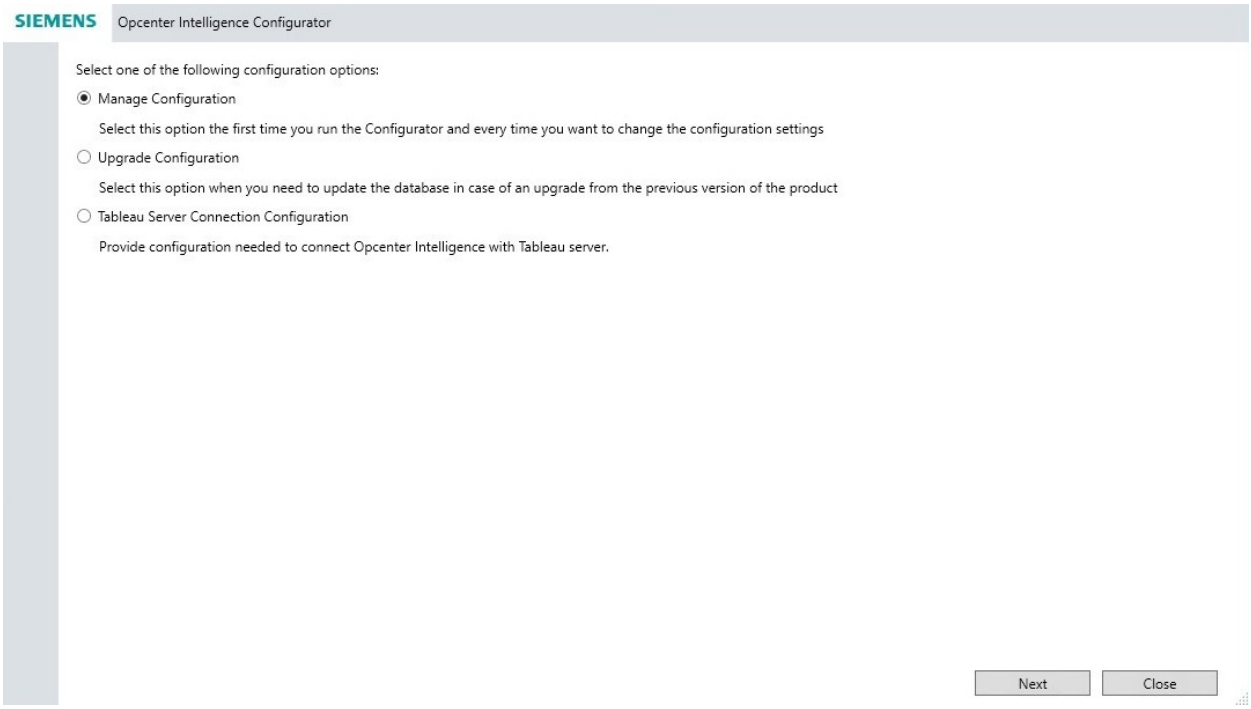
Every time you run the Configurator after the first time, you must always restart the **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost** service.

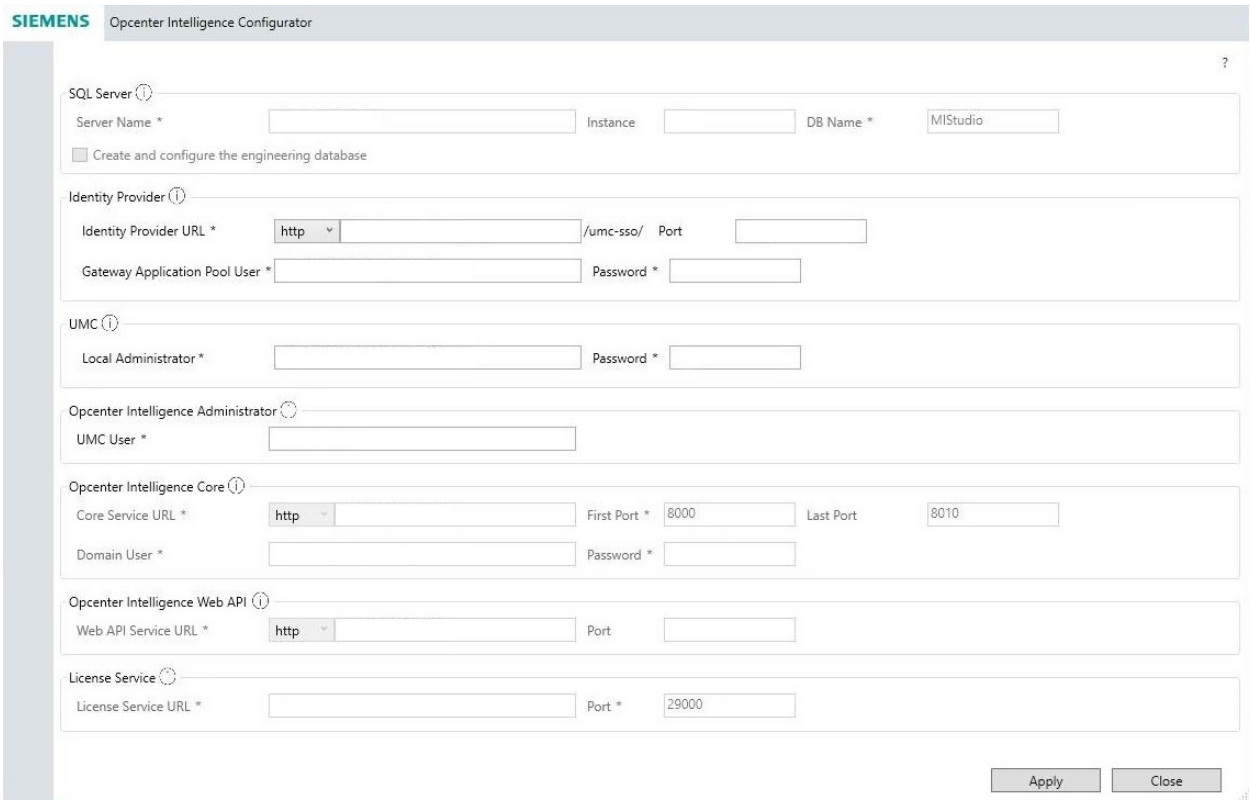
3.1.2 Upgrade Configuration

You must select this option when you are upgrading from the previous version of the product. This operation, which is mandatory, performs the migration of the system configuration to the new version. You cannot edit the Configurator fields except for the Identity Provider area. For more details, see Upgrading from previous versions of Opcenter IN to Opcenter IN 2501.0001.

Procedure

1. After you have selected **Upgrade Configuration**, click **Next**. Ignore the **Tableau Server Connection Configuration** option if you do not need to configure Tableau® Server.





2. Insert the required information in the **Identity Provider** area as explained in the table below. The fields marked with an asterisk are mandatory. Click the ⓘ icon next to field names to quickly get information on how the fields should be configured.

> ⚠ If you are upgrading from a version of Opcenter Intelligence prior to 3.3 you must migrate to UMC as Identity Provider, as Windows Authentication is no longer supported starting from version 3.5.
> In that case, add the following URL to UMC allowlist: **http(s)://<machine name>/UserGateway/Login/Login**. For more details, see *Create allowlist entry* in *Central User Management UMC Programming and Operating Manual*.

Identity Provider

Field	Action
Identity Provider URL	Select the protocol for the UMC identity provider and insert the <*Full computer name*> of the machine where UMC Server is running and the **Port** number. ⚠ The protocol for UMC Server can be either HTTP or HTTPS. To avoid security issues, it is strongly recommended that you enable the HTTPS protocol.
Gateway Application Pool User	Insert the <*computer name*>\<*user name*> and password of a Windows user who can configure the Application Pools of Gateway Services. ⚠ In a distributed scenario where the machines do not belong to any domain, you must insert **.\<*user name*>** in this field; this user name must be present with the same password in both machines of the scenario. You can also use a Windows user present in both machines: for example: **.\Administrator**

UMC

Field	Action
Local Administrator	Insert the <*computer name*>\<*user name*> and password of the local machine administrator.

3. Check the other configuration settings, click **Apply** and then **Close**.
4. Check that the **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost** service is in **Running** status. If not, start this service.

3.1.3 Tableau Server Connection Configuration

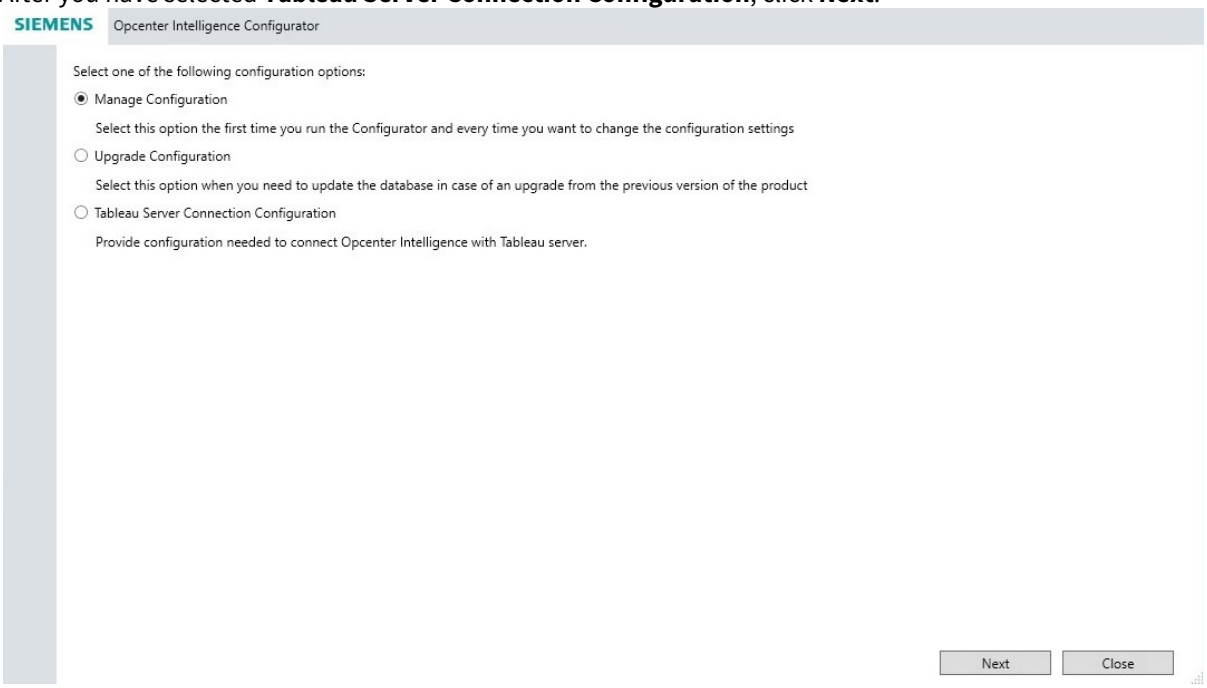
You must select this option when you have purchased a Tableau® Server license and you need to navigate through the items created in Tableau® Server and view the resulting dashboards embedded in Opcenter Intelligence.

Prerequisites

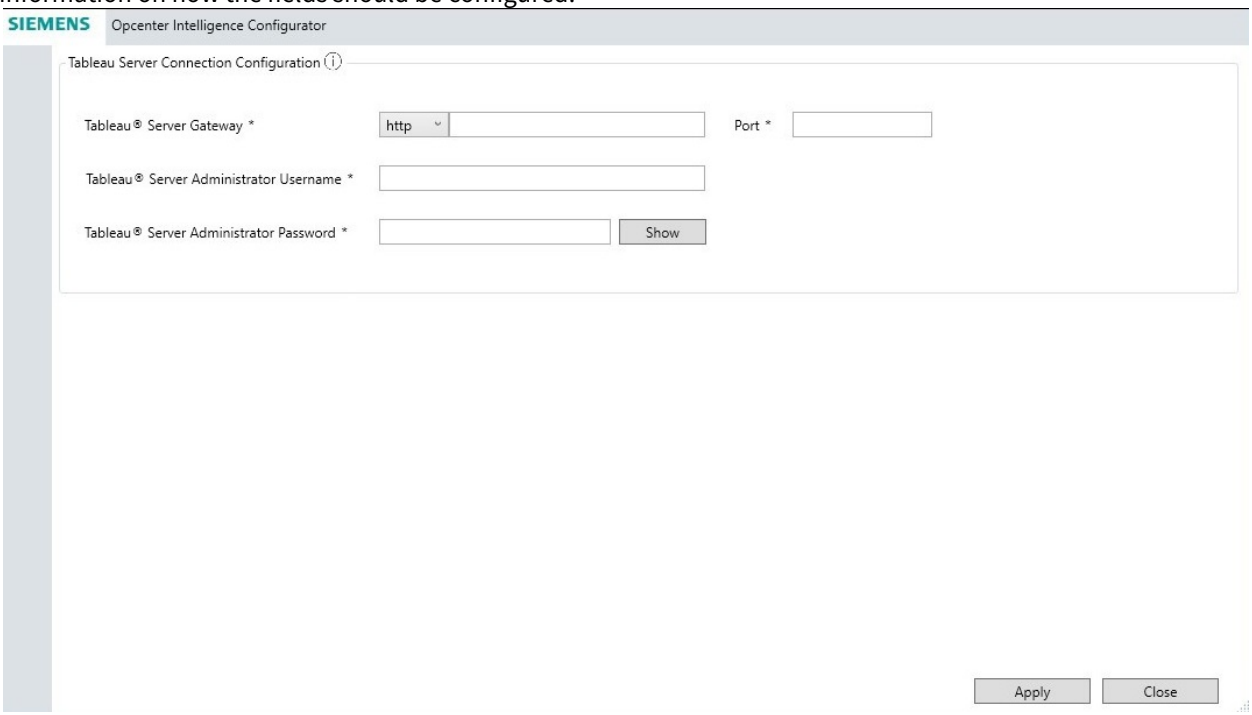
Tableau® Server is already installed on your system.

Procedure

1. After you have selected **Tableau Server Connection Configuration**, click **Next**.



2. Insert the required information in the **Tableau Server Connection Configuration** area as explained in the table below. The fields marked with an asterisk are mandatory. Click the ⓘ icon next to field names to quickly get information on how the fields should be configured.



Field	Action
Tableau® Server Gateway	This field allows the user to input the URL for Tableau® Server. It defines the address to which the system will connect for all Tableau® Server-related activities. Select the protocol for Tableau® Server and insert the <*server name*> of the machine where Tableau® Server is running (for example http/https://<*machine name*>:8085).
Port	This field must contain the Gateway port number for Tableau® Server. It defines the network port used for communication between the system and Tableau® Server, typically set to the default Tableau® Server port or custom port configured for the environment (for example: http/https//<*machine name*>:<*configured port*>).
Tableau® Server Administrator Username	This field must contain Tableau® Server Administrator's username. The administrator is responsible for managing the Tableau® Server environment, and this credential is necessary for performing administrative actions. It must match with the username used while configuring TSM Administrative account.
Tableau® Server Administrator Password	This field must contain the password for the Tableau® Server Administrator account. It is required to authenticate the user and enable access to the administrative functions on Tableau® Server. It is the same password used while configuring TSM Administrative account.

3. Click **Apply** and wait for the notification that confirms the successful completion of the configuration. Then click **Close**.
4. Check that the **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost** service is in **Running** status. If not, start this service.

3.2 Configuring Opcenter Intelligence via Command Line

Opcenter Intelligence allows you to customize the configuration via command line. In this page you can find a description of the commands and a list of the operations to be executed in the described order when you are installing and configuring the system from scratch.

> ⚠ The procedures for configuring Opcenter Intelligence via command line must be applied bearing in mind that an incorrect usage of scripts may cause system unavailability. Administrative rights are required to perform these operations.

Prerequisites

Verify that all prerequisites required by Opcenter Intelligence are satisfied.

Procedure

Follow these steps to launch a configuration from scratch for Opcenter Intelligence:

1. Open the **Command Prompt** with administrative privileges.
2. Move to **C:\Program Files\Siemens\Opcenter\Intelligence\IN\SETUP**
3. Run the following command line. In the next paragraphs you can find details on the configuration of the different parameters.

```
Siemens.SimaticIT.UAMI.MIStudio20.PostSetup.exe database create
-sqlinstance=<sqlinstance> umcconfiguration create -url=<UMCServerURL>
-adminuser=<UMCAdminUser> -adminuserpassword=<password>
-localadminuser=<LocalAdmin> -localadminuserpassword=<password>
-serviceuser=<UMCServiceLocalUser> -serviceuserpassword=<password>
-upuser=<UPServiceDomainUser> -upuserpassword=<password> service configure
-serviceuser=<ServiceUserName> -password=<password> identityprovider configure
-type=umc -url=<machine name> administrator create -domainuser=<DomainUser>
gateway configure -url=<MIStudioWebAPIURL>
-applicationpooluser=<domainName\UserName> -applicationpooluserpassword=<password>
core configure -url=<CoreURL> -domainuser=<domainUser>
-domainuserpassword=<password> -firstport=<FirstPort> flex configure
-url=<FlexURL> shortcuts create service start
```

SQL Server Configuration

Use this command to create and configure the engineering database.

```
database create -sqlinstance=<sqlinstance>
```

Use this command to update the database.

```
database update
```

Parameter	Description
sqlinstance	Insert the SQL Server instance name.

UMC Configuration

Use the following command line if UMC is already present and does not need to be configured:

```
umcconfiguration configure -url=<UMCServerURL> -admin=<UMCAdminUser>
-password=<password>
```

Use the following command line if UMC needs to be configured for the first time:

```
umcconfiguration create -url=<UMCServerURL> -adminuser=<UMCAdmin>
-adminuserpassword=<password> -localadminuser=<LocalAdmin>
-localadminuserpassword=<password> -serviceuser<UMCServiceLocalUser>
-serviceuserpassword=<password> -upuser=<UPServiceDomainUser>
-upuserpassword=<password>
```

Parameter	Description
UMCServerURL	Insert the <*Full computer name*> of the machine where UMC Server is running, including the Port number.
UMCAdmin *password*	This user is going to be created by the Configurator. Insert the user name for this user who will have the privileges of Administrator with full control of UMC. For example, he will be the only user able to import all other users from the domain directory into UMC. Insert the corresponding password.
LocalAdmin *password*	Insert the <*computer name*>\<*user name*> of the local machine administrator and the corresponding password.
UMCServiceLocalUser *password*	Insert the <*domain name*>\<*user name*> of the domain user with Administrator privileges who is going to run UMCService and the corresponding password.
UPServiceDomainUser *password*	Insert the <*domain name*>\<*user name*> of a domain user who has Active Directory access rights and who is going to run UPService. Insert the corresponding password.

Identity Provider Configuration

```
identityprovider configure -type=umc -url=<machine name>
```

Parameter	Description
type	The identity provider mode, in this case UMC.
url	The <*Full computer name*> of the machine where UMC Server is running.

Opcenter Intelligence Administrator Configuration

```
administrator create -domainuser=<DomainUser>
```

Parameter	Description
DomainUser	Insert the <*domain name*>\<*UMC user name*> of the UMC user who is going to be the Opcenter Intelligence Administrator. This is the user who will be able to grant access to other users.

Host Service Configuration

Use the first command line to create the **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost** service.

Use the other commands to start/stop or remove the service.

```
service configure -serviceuser=<ServiceUserName> -password=<password>

service start

service stop

service remove
```

Opcenter Intelligence Core Configuration

```
core configure -url=<CoreURL> -domainuser=<domainUser> -domainuserpassword=<password>
-firstport=<FirstPort>
```

Parameter	Description
CoreURL	Insert the name of the computer where the Core Server is running.
domainUser *password*	Insert the <*domain name*>\<*user name*> of the user who is going to run the Core Service. He must be a domain user with Administrator privileges. Insert the password for this user.
FirstPort	Insert the number of the First Port (the default is 8000) of a series made up of 11 ports. The Last Port number is automatically inserted by the system.

Opcenter Intelligence Web API Configuration

```
gateway configure -url=<MIStudioWebAPIURL> -applicationpooluser=<domainName\UserName>
-applicationpooluserpassword=<password>
```

Parameter	Description
MIStudioWebAPIURL	Insert the name of the computer where the Server is running and the Port number.
applicationpooluser *applicationpooluserpassword*	Insert the <*domain name*>\<*user name*> of the user who can configure the Application Pools of Gateway Services. Insert the password for this user.

License Server Configuration

```
flex configure -url=<FlexURL>
```

Parameter	Description
FlexURL	Insert the computer name of the License Server and the Port number.

Help

```
help
```

This command displays a guide that contains instructions on how to use the different commands.

Shortcut Configuration

```
shortcuts create
```

This command creates shortcuts on the Desktop and in the Start Menu to access Opcenter Intelligence.

Adding URL to UMC whitelist

To ensure that UMC functions correctly, add the following URL to UMC whitelist: **http(s)://<machine name>/UserGateway/Login/Login**. For more details, see *Create Whitelist Entry* in *UMCONF User Manual*.

```
C:\Program Files\Siemens\UserManagement\BIN> umconf -c -w -d http(s)://<machine name>/UserGateway/Login/Login
```

3.3 Configuring HTTPS Protocol for Opcenter Intelligence Components

To configure the HTTPS protocol for Opcenter Intelligence Core, do the following to enable HTTPS with self-hosted ASP.NET Web API.

> ⚠ The certificate must be imported into the machine local store. If the certificate is installed in the **Personal** store folder, you do not have to specify the *certstorename* (as in the example below).
> Otherwise, please refer to *Microsoft documentation* at the link: https://docs.microsoft.com/en-us/windows-server/networking/technologies/netsh/netsh-http#add-sslcert

Prerequisites for Certificates

Common Certificates

- The Key Usage certificate extension must have the Digital Signature value.

- In the Subject or Subject Alternative Name, the name used during Opcenter Intelligence configuration must be used. For example, if Opcenter Intelligence was configured using the FQDN of the machine (or machines, depending on the type of installation), the certificate must contain the FQDN.

Self-Signed Certificates

Self-Signed Certificates are autogenerated and therefore are not automatically recognized by operating systems. In order to let them be trusted, they must be installed on the machine where they are used. For example, in a distributed scenario including a Core machine, a Gateway machine and a Client machine where the browser you are using to connect to Opcenter Intelligence is installed, you must:

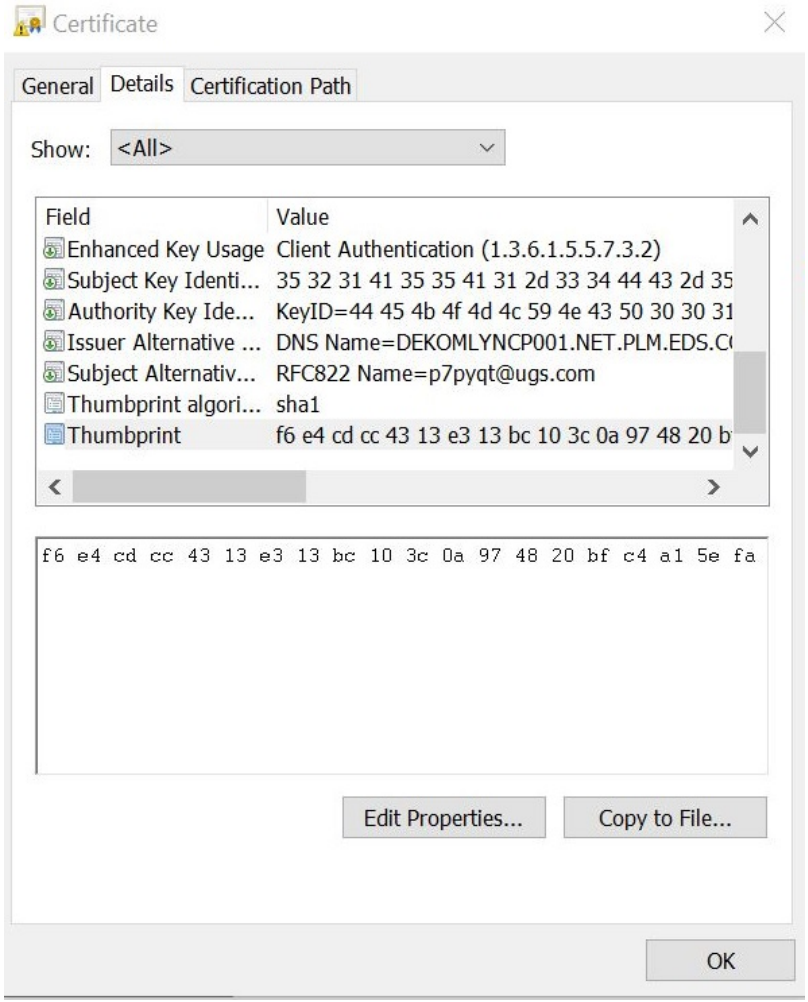
- Install the certificate used in the Core machine on the Gateway machine.
- Install the certificate used in the Gateway machine on all the client machines from where you want to connect to Opcenter Intelligence .

Procedure

1. To register the certificate, run:

   ```
   netsh http add sslcert ipport=0.0.0.0:port appid={app-guid} certhash=thumbprint
   ```

   where you need to configure the following parameters:
   - **ipport**: the special IP address 0.0.0.0 matches any IP address for the local machine.
   - **port**: the numbers of the listening ports that make up a series of 11 ports.
   - **app-guid**: any valid GUID. You can use the GUID specified in the example below.
   - **thumbprint**: the certificate SHA-1 hash, represented in hexadecimal, which can be retrieved as shown in this image (remember to remove spaces between characters).



2. For Opcenter Intelligence Client, refer to *Microsoft Internet Information Services (IIS) documentation* for instructions on how to configure a certificate on the website.

Example

This example shows a standard configuration (ports from 8000 to 8010):

```
netsh http add sslcert ipport=0.0.0.0:8000 appid={f571c5de-ef36-40a4-
b2ea-030470971f87} certhash=f6e4cdcc4313e313bc103c0a974820bfc4a15efa

netsh http add sslcert ipport=0.0.0.0:8001 appid={f571c5de-ef36-40a4-
b2ea-030470971f87} certhash=f6e4cdcc4313e313bc103c0a974820bfc4a15efa

netsh http add sslcert ipport=0.0.0.0:8002 appid={f571c5de-ef36-40a4-
b2ea-030470971f87} certhash=f6e4cdcc4313e313bc103c0a974820bfc4a15efa

netsh http add sslcert ipport=0.0.0.0:8003 appid={f571c5de-ef36-40a4-
b2ea-030470971f87} certhash=f6e4cdcc4313e313bc103c0a974820bfc4a15efa
```

```
netsh http add sslcert ipport=0.0.0.0:8004 appid={f571c5de-ef36-40a4-
b2ea-030470971f87} certhash=f6e4cdcc4313e313bc103c0a974820bfc4a15efa

netsh http add sslcert ipport=0.0.0.0:8005 appid={f571c5de-ef36-40a4-
b2ea-030470971f87} certhash=f6e4cdcc4313e313bc103c0a974820bfc4a15efa

netsh http add sslcert ipport=0.0.0.0:8006 appid={f571c5de-ef36-40a4-
b2ea-030470971f87} certhash=f6e4cdcc4313e313bc103c0a974820bfc4a15efa

netsh http add sslcert ipport=0.0.0.0:8007 appid={f571c5de-ef36-40a4-
b2ea-030470971f87} certhash=f6e4cdcc4313e313bc103c0a974820bfc4a15efa

netsh http add sslcert ipport=0.0.0.0:8008 appid={f571c5de-ef36-40a4-
b2ea-030470971f87} certhash=f6e4cdcc4313e313bc103c0a974820bfc4a15efa

netsh http add sslcert ipport=0.0.0.0:8009 appid={f571c5de-ef36-40a4-
b2ea-030470971f87} certhash=f6e4cdcc4313e313bc103c0a974820bfc4a15efa

netsh http add sslcert ipport=0.0.0.0:8010 appid={f571c5de-ef36-40a4-
b2ea-030470971f87} certhash=f6e4cdcc4313e313bc103c0a974820bfc4a15efa
```

3.4 Checking Authentication Keys in IIS

After you have completed the configuration in Opcenter Intelligence Configurator, follow these procedures to check the configuration of Gateways and Web Sites in Internet Information Services (IIS).

> The **AnalyticsConfiguratorGateway** and **UserGateway** have different configurations from the other Gateways. Please check the correct settings described in the procedure below.

Procedure

1. In **IIS Manager** > **Sites** > **Default Web Site**, select one of the following Gateways:
   - **DeployerGateway**
   - **EnvironmentGateway**
   - **ImportExportGateway**
   - **MonitoringOnPremGateway**
   - **ProjectGateway**
   - **ScenarioGateway**
   - **TimeGateway**
   - **UserViewGateway**
   - **ViewerGateway**
2. Double-click **Authentication** from the area on the right.
3. Check if the authentication keys of each Gateway are configured as follows:
   - **Anonymous Authentication** must be set to **Disabled**
   - **ASP.NET Impersonation** must be set to **Disabled**
   - **Basic Authentication** must be set to **Disabled**
   - **Digest Authentication** must be set to **Disabled**
   - **Forms Authentication** must be set to **Enabled**
   - **Windows Authentication** must be set to **Disabled**
4. Repeat steps 1, 2 and 3 for each Gateway.
5. Select the **AnalyticsConfiguratorGateway** and check if the authentication keys are configured as follows:

- **Anonymous Authentication** must be set to **Disabled**
- **ASP.NET Impersonation** must be set to **Enabled**
- **Basic Authentication** must be set to **Disabled**
- **Digest Authentication** must be set to **Disabled**
- **Forms Authentication** must be set to **Disabled**
- **Windows Authentication** must be set to **Enabled**

6. Select the **UserGateway** and check if the authentication keys are configured as follows:
   - **Anonymous Authentication** must be set to **Enabled**
   - **ASP.NET Impersonation** must be set to **Disabled**
   - **Basic Authentication** must be set to **Disabled**
   - **Digest Authentication** must be set to **Disabled**
   - **Forms Authentication** must be set to **Enabled**
   - **Windows Authentication** must be set to **Disabled**
7. In **IIS Manager** > **Sites** > **Default Web Site**, select the **MISignal** and **MIStudio** web sites.
8. Double-click **Authentication** from the area on the right.
9. Check if the authentication keys for both web sites are configured as follows:
   - **Anonymous Authentication** must be set to **Disabled**
   - **ASP.NET Impersonation** must be set to **Disabled**
   - **Basic Authentication** must be set to **Disabled**
   - **Digest Authentication** must be set to **Disabled**
   - **Forms Authentication** must be set to **Enabled**
   - **Windows Authentication** must be set to **Disabled**
10. Run **IISRESET** from the Command Prompt.

3.5 Configuring Oracle Authentication

For more details on Oracle configuration concerning authentication, please refer to *Oracle documentation*.

For the connection to an Oracle data source, Opcenter Intelligence supports both the native Windows authentication and the Oracle authentication.

Windows Authentication

For Windows authentication, the local users of the Windows machine or of the Active Directory are used. This procedure creates the user in Oracle for the connection and grants this user all the required rights.

Prerequisites

- Check whether in the Windows user groups the group **ORA_DBA** has been created (this group should contain the Windows user who installed Oracle).
- Windows authentication must be enabled. To perform this check, in <*Oracle installation path*>\network\admin, open the **sqlnet.ora** file and check if the row **SQLNET.AUTHENTICATION_SERVICES= (NTS)** is present.
- Verify that in Windows system variables, the **TNS_ADMIN** variable is present with the value <*Oracle installation path*>\network\admin
- <*OPS$domain\user*> has been created in the *domain* domain.

If you apply any change after the above checks, you must restart the computer to make your changes effective.

Procedure

This procedure creates the user and assigns the grants required for the creation of the contract database and the execution of readings.

1. Launch the "Run SQL Command Line" application.
2. Execute the following commands:

```
CONNECT / AS SYSDBA;
CREATE USER "OPS$domain\user" IDENTIFIED EXTERNALLY;
GRANT CREATE SESSION TO "OPS$domain\user";
GRANT CREATE session, connect, resource TO OPS$domain\user;
GRANT CREATE any view TO OPS$domain\user;
GRANT CREATE procedure TO OPS$domain\user;
GRANT CREATE any procedure TO OPS$domain\user;
GRANT ALTER any procedure TO OPS$domain\user;
GRANT CREATE view TO OPS$domain\user;
GRANT DROP any view TO OPS$domain\user;
GRANT EXECUTE any procedure TO OPS$domain\user;
GRANT SELECT any table TO OPS$domain\user;
GRANT CREATE any type TO OPS$domain\user;
GRANT CREATE type TO OPS$domain\user;
GRANT DROP any type TO OPS$domain\user;
GRANT ALTER any type TO OPS$domain\user;
GRANT EXECUTE any type TO OPS$domain\user;
GRANT DROP any procedure TO OPS$domain\user;
DISCONNECT;
```

Oracle Database Authentication

This procedure creates the user in Oracle for the connection and grants this user all the required rights.

Procedure

1. Launch the "Run SQL Command Line" application.
2. Execute the following commands:

```
CONNECT / AS SYSDBA;
CREATE USER "<OCIN Username>" IDENTIFIED BY "<pwd>";
GRANT CREATE session, connect, resource TO <OCIN Username>;
GRANT CREATE any view TO <OCIN Username>;
GRANT CREATE procedure TO <OCIN Username>;
GRANT CREATE any procedure TO <OCIN Username>;
GRANT ALTER any procedure TO <OCIN Username>;
GRANT CREATE view TO <OCIN Username>;
GRANT DROP any view TO <OCIN Username>;
GRANT EXECUTE any procedure TO <OCIN Username>;
GRANT SELECT any table TO <OCIN Username>;
GRANT CREATE any type TO <OCIN Username>;
GRANT CREATE type TO <OCIN Username>;
GRANT DROP any type TO <OCIN Username>;
GRANT ALTER any type TO <OCIN Username>;
GRANT EXECUTE any type TO <OCIN Username>;
GRANT DROP any procedure TO <OCIN Username>;
```

```
DISCONNECT;
```

3.6 Configuring the connection between Opcenter Intelligence Client and Oracle Server

If you want to load data from an Oracle data source, the following procedure must be executed on the computer where Opcenter Intelligence Core Service is running.

⚠ Both 32-bit and 64-bit drivers must be installed.

Procedure

1. Install the 64-bit OLEDB driver (to be downloaded from the Oracle website): extract the **ODAC121024Xcopy_x64.zip** package and execute **install.bat all c:\oracle odac** from the command prompt (Run as administrator).
2. Install the 32-bit OLEDB driver (to be downloaded from the Oracle website): extract the **ODAC121024Xcopy_32bit.zip** package and execute **install.bat all c:\oracle\odac32 odac32** from the command prompt (Run as administrator).
3. Copy the **sqlnet.ora** file (contained in C:\oracle\network\admin\samples) to C:\oracle\network\admin
4. Copy the **sqlnet.ora** file (contained in C:\oracle\odac32\network\admin\samples) to C:\oracle\odac32\network\admin
5. Add the following paths to the **PATH** system variable:
   - c:\oracle
   - c:\oracle\bin
   - c:\oracle\odac32
   - c:\oracle\odac32\bin
6. Restart the computer.

3.7 How to Define Users

After you have installed and configured Opcenter Intelligence, you must open the User Management Component (UMC) Web User Interface to define users.

⚠ Starting from version 3.2, assigning user groups to Opcenter Intelligence roles is no longer supported. The license model now requires a check on the number of configured users against the number of users allowed by the installed licenses. In the **Access Control** page, the **Groups** tab is only maintained for compatibility for existing installations based on previous Opcenter Intelligence versions.

Accessing the UMC Login Page

1. Open a supported Web browser.
2. Access UMC by entering the address **http://*<FullComputerName>*/UMC** or **https://*<FullComputerName>*/UMC** depending on the configuration, and in the **User UMC Administrator** field log in with the user specified during the configuration.

Workflow

1. Manually create users.
2. Grant the access to users by assigning them specific predefined roles. For details on this procedure, see *Managing Access Control* in *Opcenter Intelligence User Manual*.

3.7.1 Creating Opcenter Intelligence Users in UMC

You can skip this procedure if User Management Component has already been installed and configured on your machine and you have already created one or more users in UMC.
If, on the contrary, you have installed UMC during Opcenter Intelligence installation, you must previously configure UMC in Opcenter Intelligence Configurator and then follow this procedure.

Procedure

1. From a supported browser, access UMC by entering the address: **http(s)://<*FullComputerName*>/UMC**
2. Log in with the UMC user who owns the permissions to create other users or groups.
3. In UMC **Users** page, add the user who will be the Administrator for Opcenter Intelligence. This user is the one specified on the Configurator under **Opcenter Intelligence Administrator** > **UMC User**.
4. In the UMC **Users** page, add other users if needed.

3.8 Configuring the User Management Component Ring Servers

Opcenter Intelligence includes among its data sources a number of Opcenter products. As a result, Opcenter Intelligence (and consequently UMC) may be installed in a domain where Opcenter products are installed together with the corresponding UMC version (most likely a different version of UMC).

In that case you may want to join the different UMC servers and make them work as one; this configuration is known as UMC Ring Servers and its main characteristic is that the UMC with the latest version takes control over the other ones and becomes the UMC primary server in the ring, while the other UMC instances become secondary UMC servers.

Opcenter Intelligence Configurator automatically configures UMC server as primary. Then you have to configure other UMC servers (with earlier versions) as secondary UMC servers in the ring.

You can find information on how to configure them in *Central User Management UMC Programming and Operating Manual*.

> ⚠ If the UMC that you set as secondary has already been configured as UMC server (primary) you will need to first delete the existing configuration and then configure it as secondary server joining the ring (for more details, see *Central User Management UMC Programming and Operating Manual*). While running the join procedure, remember to configure the provisioning as well (the [-b] switch must be removed).

3.9 Configuring Opcenter Intelligence without SQL Server sysadmin role

It is possible to avoid configuring the **sysadmin** role for the SQL Server Agent account. To do so, follow the steps described below.

1. Create the Windows AD users
2. Configure the users in SQL Server logins
3. Configure the Core user (Administrator)
4. Set the proper Server Roles for the Administrator user
5. Map the Administrator user to the required database roles
6. Configure SQL Server Agent (sqlUserAgent user)
7. Configure the ETL launcher (SisLaunch user)
8. Map the SisLaunch user to the required database roles
9. Set the credentials in SQL Server
10. Create SQL Server Agent proxies

11. Configure the ETL job flow
12. Run the ETL flow

> ⚠
> - These are the least privileges needed to run SQL Server Integration Services flows and to create the data warehouse.
> - This configuration is reverted every time a deploy operation is executed in Opcenter Intelligence.
> - This configuration is not recommended nor supported.

Creating the Windows AD users

Three different accounts are required for this configuration. In Windows **Computer Management**, create the following users:

- **Administrator**: the user to be configured for the Core service (it must be included in the local Administrator group).
- **SisLaunch**: the user to be configured to run ETL flows.
- **sqlUserAgent**: the user to be configured for the SQL Server Agent service.

> ℹ These three users must be created on the Opcenter Intelligence machine.
> In addition, the **Administrator** and **SisLaunch** users must be created on the source machine as well.

Configuring the users in SQL Server logins

Create three SQL Server logins for the above users. To perform these operations you need to access SQL Server Management Studio with a **sysadmin** user.

Configuring the Core user (Administrator)

This user needs to access the engineering database (MIStudio) to create and manage the data warehouse and to create and manage ETL flows in SSIS. Once the configuration for the Core user is completed, you should be able to perform Opcenter Intelligence configuration and deploy.

> ℹ For more details, see the documentation at the following links:
> - https://docs.microsoft.com/en-us/sql/ssms/agent/configure-a-user-to-create-and-manage-sql-server-agent-jobs?view=sql-server-ver16
> - https://docs.microsoft.com/en-us/sql/ssms/agent/sql-server-agent-fixed-database-roles?view=sql-server-ver16

Setting the proper Server Roles for the Administrator user

1. In SQL Server Management Studio, in the **Security** logins, right-click on the **Administrator** user and select **Properties**.
2. In the **Server Roles** page, select the **public** and **dbcreator** roles. The **dbcreator** role is required to create a data warehouse on the server.
3. Clear the **sysadmin** option if it is selected.

Mapping the Administrator user to the required database roles

1. In the **User Mapping** page on the Opcenter Intelligence machine, select the **SSISDB** database and select the **public**, **ssis_admin** and **db_owner** database role membership. This configuration is required to deploy ETL packages and launch them from the portal.

2. In the **User Mapping** page on the Opcenter Intelligence machine, select the **msdb** database and select the **public**, **SQLAgentOperatorRole** and **db_owner** database role membership. This configuration is required to write the schedule on SQL Server Agent.

Configuring SQL Server Agent (**sqlUserAgent** user)

Run the SQL Server Agent using the **sqlUserAgent** user.

Configuring the ETL launcher (**SisLaunch** user)

This user needs to access ETL flows in SSIS and launch them as well as the deployed contract database and the data source system. In order to use this user from the SQL Server Agent to launch ETL packages, you need to create a proxy user, as described at the following documentation link: https://www.mssqltips.com/sqlservertip/2163/running-a-ssis-package-from-sql-server-agent-using-a-proxy-account/

Mapping the SisLaunch user to the required database roles

On the Opcenter Intelligence machine:

1. In the **User Mapping** page, select the **MIStudio** database and select the **public** and **db_owner** database role membership.
2. In the **User Mapping** page, select the **SSISDB** database and select the **ssis_admin** and **public** database role membership.
3. In the **User Mapping** page, select the **MDW** database and select the **public** and **db_owner** database role membership.

On the source machine:

1. In the **User Mapping** page, select the source database and select the **db_owner** and **public** database role membership.
2. In the **User Mapping** page, select the database view to be created during the deploy and select the **db_owner** and **public** database role membership.

> If the MDW database does not exist yet, deploy the environment to create it and repeat point 3 on the Opcenter Intelligence machine and points 1 and 2 on the source machine.

Setting the credentials in SQL Server

In the **Security** folder of SQL Server Management Studio, right-click on the **Credentials** folder and create a **New Credential**. Provide the required information:

Field	Description
Name	A name for the credential.
Identity	Browse for the **SisLaunch** user.
Password	Type a password and confirm it.

Creating SQL Server Agent proxies

1. In the SQL Server Agent service, under **Proxies**, select **New Proxy** on the **SSIS Package Execution** object to create a new proxy.

2. In the **General** section, configure a name for the proxy, select the previously created credential and leave the **SQL Server Integration Services Package** option selected.
3. In the **Principals** section, select the **Administrator** user configured for the Core service.

For more details, see the documentation at these links:
- https://docs.microsoft.com/en-us/sql/ssms/agent/create-a-sql-server-agent-proxy?view=sql-server-ver15
- https://social.technet.microsoft.com/wiki/contents/articles/32643.ssis-using-proxy-account-to-execute-a-package.aspx

Configuring the ETL job flow

1. On the Job list under SQL Server Agent, select the Opcenter Intelligence ETL schedule and click **Properties**.
2. In the **Steps** tab select **Edit**.
3. In the **Run as** field, select the proxy created above.
4. Under **Proxies**, in **SSIS Package Execution**, check that the **Reference** tab has been added for the proxy.

Running the ETL flow

Now you can run the ETL flow without SQL Server **sysadmin** role.

4 Upgrading from previous versions of Opcenter IN to Opcenter IN 2501.0001

Perform the following procedure if you want to upgrade from one of the previous versions of Opcenter Intelligence to Opcenter Intelligence 2501.0001.

Prerequisite

Before launching the installation of Opcenter Intelligence, manually stop the **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost** service.

Important Recommendations

- It is highly recommended that you make a **backup** of the existing engineering database.
- Before proceeding with the upgrade, it it strongly recommended that you clear the cache of the Internet browser to avoid any unpredictable errors when using Opcenter Intelligence.
- It is suggested that in **SQL Server Management Studio** you set the **Recovery Model** property to **Simple** before starting the deploy and launching the script.
- During database maintenance, use **WITH (DATA_COMPRESSION = PAGE)** in the rebuild index statement to reduce index fragmentation and obtain the best balance between space and speed.
- If you are upgrading from Opcenter Execution Discrete 3.x or 4.0 to Opcenter Execution Discrete 4.1 or higher, you must execute the procedure to migrate the **EquipmentKey** in Opcenter Execution Discrete described in *Opcenter Intelligence User Manual* under the *How to Perform Advanced Operations* > *How to Manage the Update of a Data Source Product Version* chapter. This migration procedure must be executed only when a customer using Opcenter EX DS 3.x or 4.0 upgrades to Opcenter EX DS 4.1 or higher and Opcenter Intelligence 2501.0001.

Upgrading User Management Component (UMC)

The 2.15 SP1 version of User Management Component (UMC) is required by Opcenter Intelligence.

These recommendations are only valid if you are upgrading UMC from any previous version to version 2.15 SP1.

To upgrade UMC, execute the following steps:

1. Run the **Remove_IdP_WebUI_configuration.bat** command.
2. Install Opcenter Intelligence 2501.0001 (points 1 to 5 of the procedure below).
3. Launch Opcenter Intelligence Configurator: a notification is shown informing you that UMC Server is unavailable. Click **Yes** to continue.
4. Follow points 6 to 10 of the procedure below. UMC is automatically configured by Opcenter Intelligence Configurator.

- This update is always executed, even if on the same machine you have already installed UMC with another product that uses UMC as Identity Provider, for example Opcenter Execution Discrete.
- If you are migrating from Windows Authentication (which is no longer supported starting from version 3.5) to UMC as identity provider, and to ensure that UMC functions correctly, add the following URL to UMC allowlist: **http(s)://<machine name>/UserGateway/Login/Login** (see *Create allowlist entry* in *Central User Management Programming and Operating Manual*).
- Before proceeding with the update, please check the compatibility of all the applications that use this instance of UMC.

Upgrading the License Server

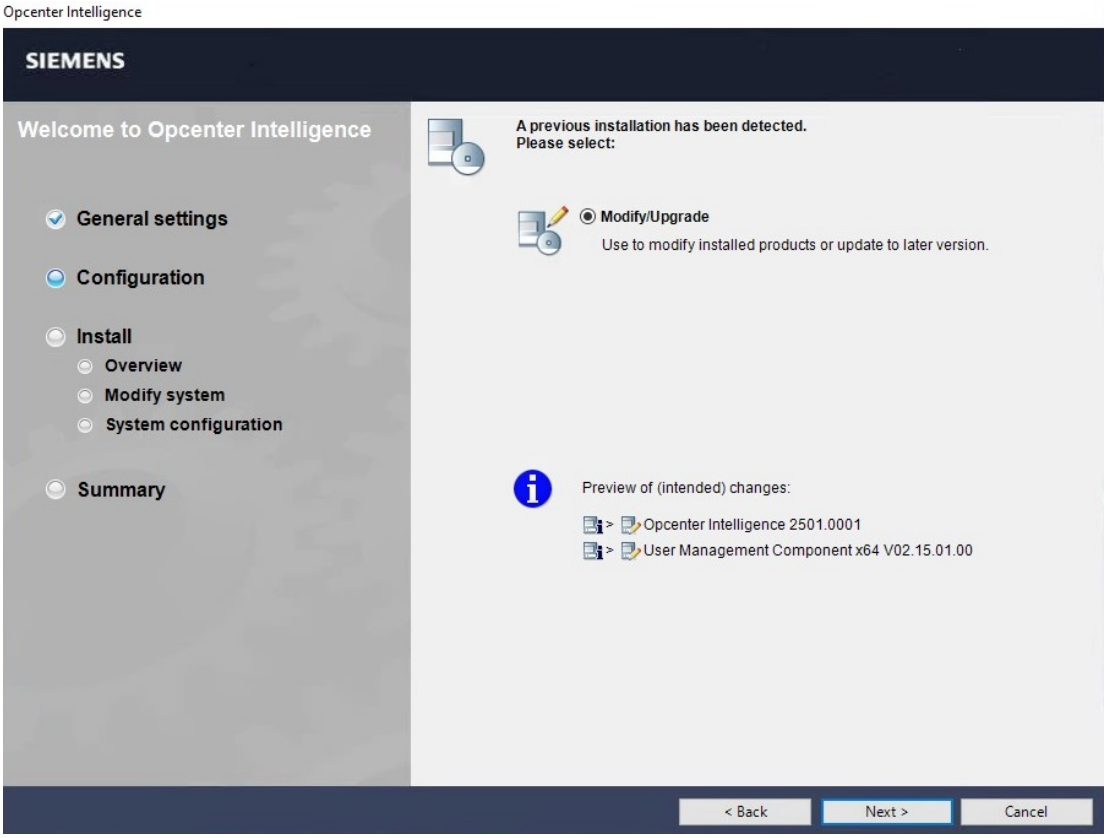
For the current license server, the default port is 29000 (for versions previous to 2307, the port was 28000).

If you want to keep the previously configured port number, you have to change it in the **Port Changes** step of the license installation wizard by selecting the **Advanced Settings** checkbox.

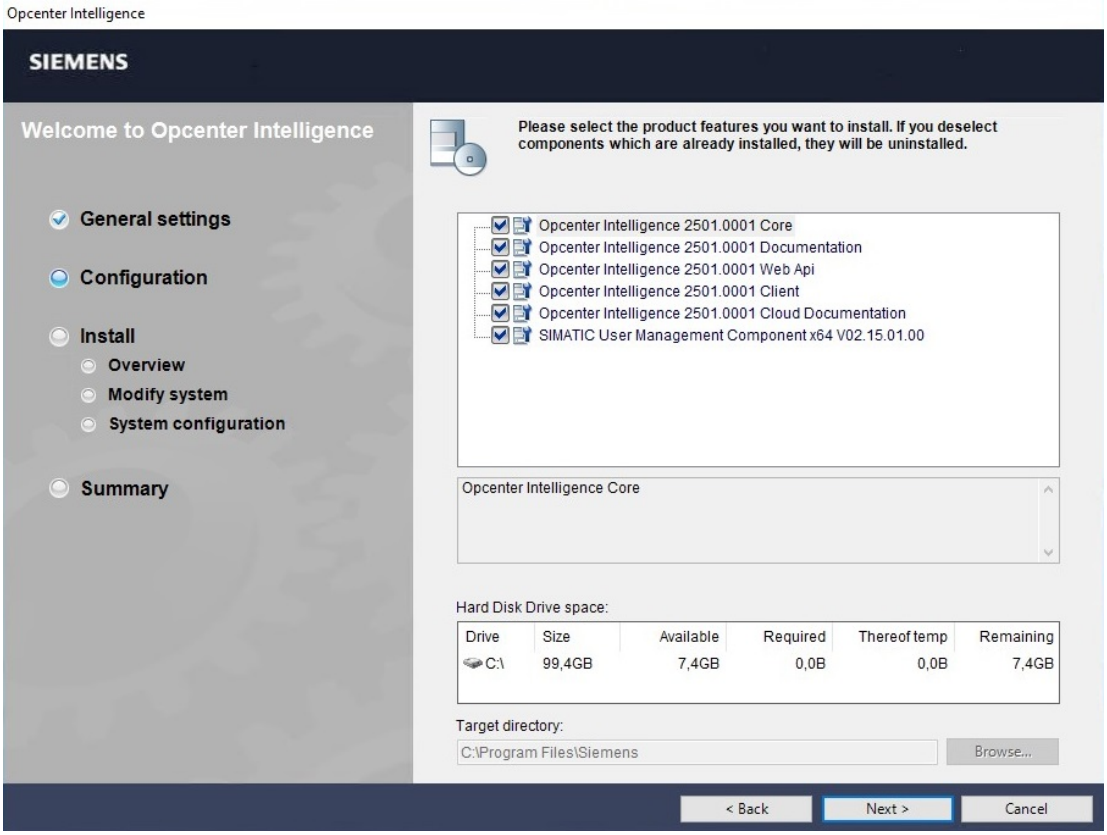
If a previous version of another product (for example Opcenter Execution Discrete) that is using the license server is installed on your system, please make sure that Opcenter Intelligence and the other products are configured to use the same port number.

Procedure

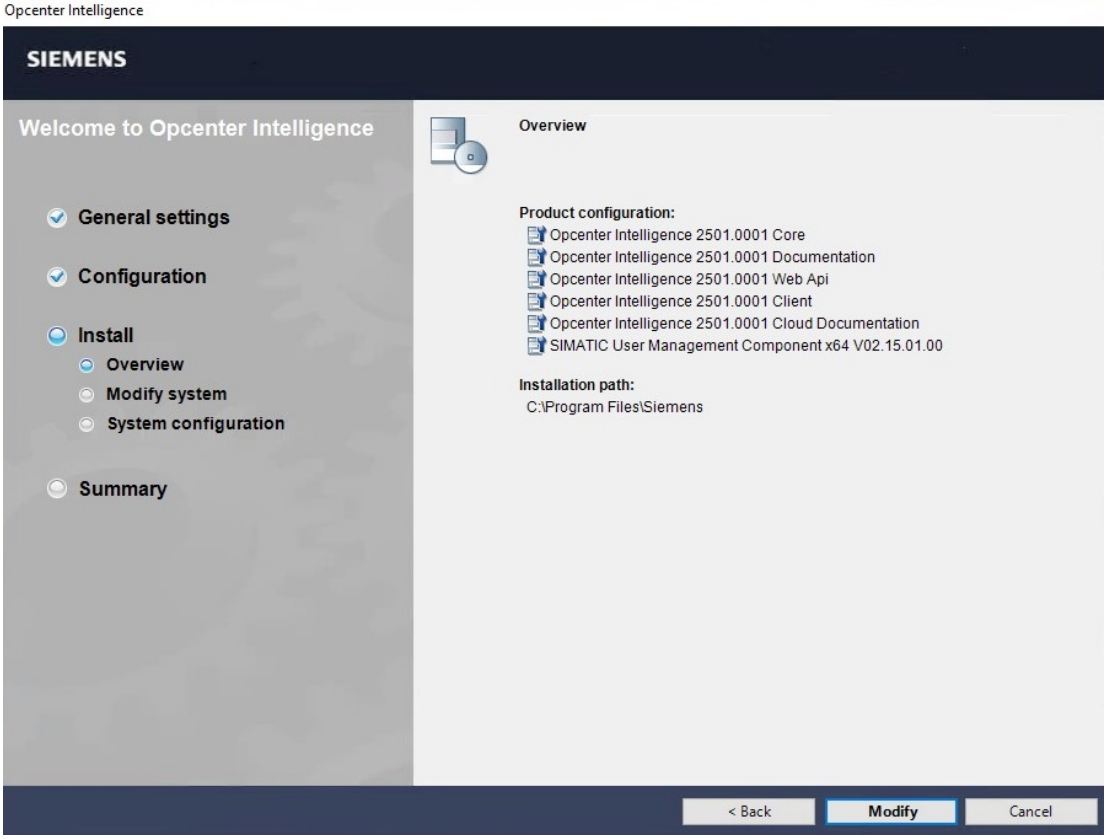
1. Launch the installation of Opcenter Intelligence 2501.0001 by executing the **Start.exe** program located in the ISO root folder.



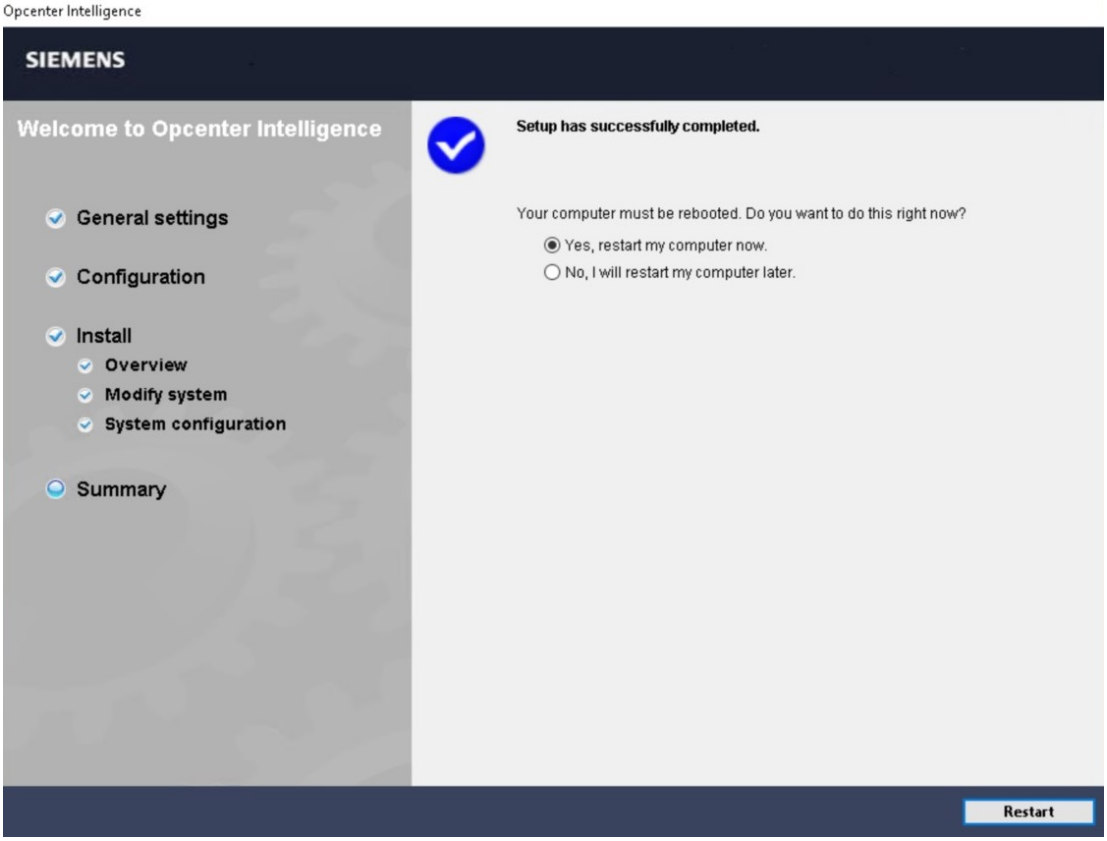
2. Click **Next**.


Opcenter Intelligence
SIEMENS
Welcome to Opcenter Intelligence
General settings
Configuration
Install
Overview
Modify system
System configuration
Summary
Please select the product features you want to install. If you deselect components which are already installed, they will be uninstalled.
Opcenter Intelligence 2501.0001 Core
Opcenter Intelligence 2501.0001 Documentation
Opcenter Intelligence 2501.0001 Web Api
Opcenter Intelligence 2501.0001 Client
Opcenter Intelligence 2501.0001 Cloud Documentation
SIMATIC User Management Component x64 V02.15.01.00
Opcenter Intelligence Core
Hard Disk Drive space:
Drive Size Available Required Thereof temp Remaining
C:\ 99,4GB 7,4GB 0,0B 0,0B 7,4GB
Target directory:
C:\Program Files\Siemens
Browse...
< Back
Next >
Cancel

3. Click **Next**. Please note that if you clear the checkbox for components that are already installed, they will be uninstalled.

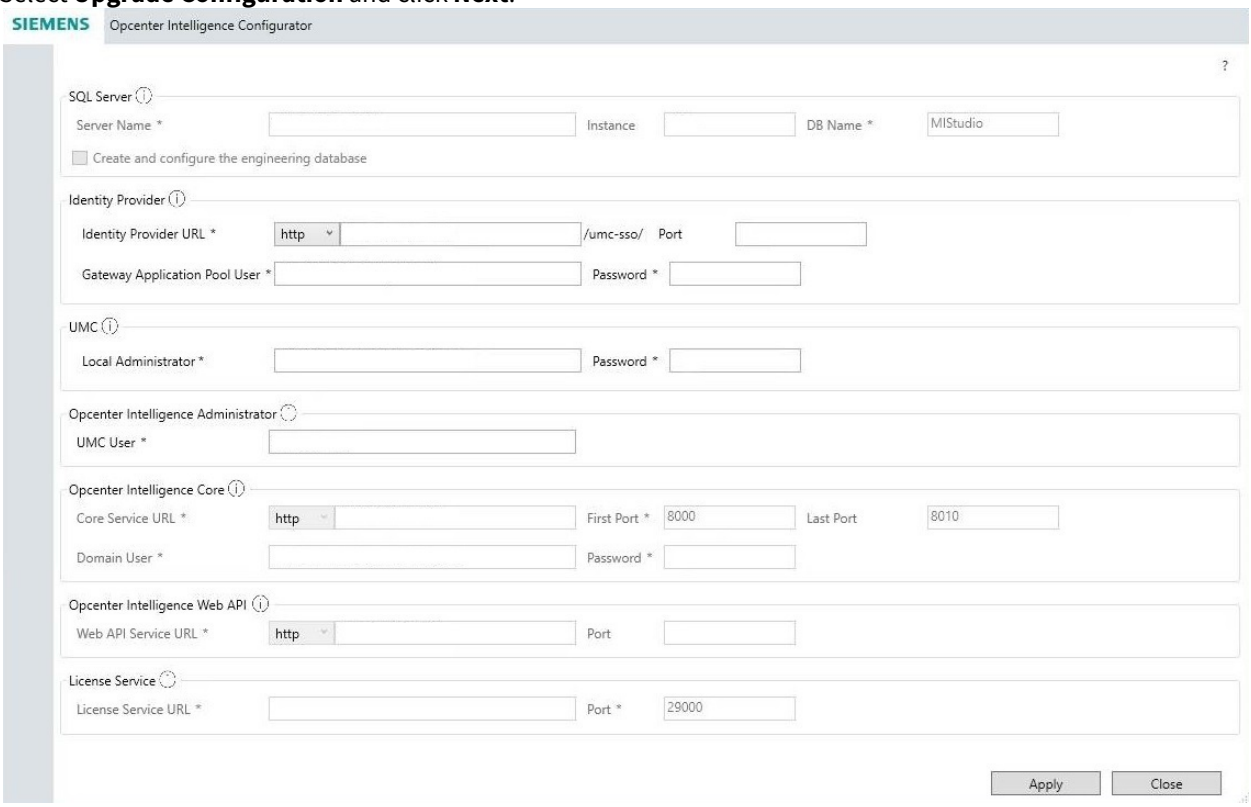


4. Click **Modify**.



5. When the setup is completed click **Restart** to restart the computer.
6. Run Opcenter Intelligence Configurator by double-clicking the corresponding desktop icon.

7. Select **Upgrade Configuration** and click **Next**.



8. Insert the required information in the **Identity Provider** area of the Configurator. For more details, see Upgrade Configuration.

> ⚠ If you are upgrading from a version of Opcenter Intelligence prior to 3.3 and are using Windows Authentication, you must migrate to UMC as Identity Provider. For more details, see Upgrade Configuration and User Management Component as Default Identity Provider.

9. Click **Apply** and wait for the notification that confirms the successful completion of the operation.
10. Click **Close**.
11. Check that the **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost** service is in **Running** status. If not, start this service.
12. Check the configuration of Gateways and Web Sites in Internet Information Services (IIS).
13. Open Opcenter Intelligence. In the **Environments** page, deploy the Environment. The duration of this operation will depend on the size of the data warehouse (up to many hours).
14. After the deploy operation is completed, run the following script from **SQL Server Management Studio** connected to the Manufacturing Data Warehouse.

> ⛔ Please make sure to copy the correct script text and check it carefully before running it (for example the text may be broken across two different pages of the PDF manual).

```
exec sp_MSforeachtable
'IF (OBJECT_SCHEMA_NAME(OBJECT_ID(''?'')) = ''bm20'' OR
OBJECT_SCHEMA_NAME(OBJECT_ID(''?'')) = ''localizedBm20'')
BEGIN
print ''Tablename: ?''
```

```
IF EXISTS (SELECT * FROM SYS.COLUMNS WHERE OBJECT_ID = OBJECT_ID(''?'') AND NAME =
''RowUpdated'')
BEGIN
EXEC(''
WHILE 1=1
    BEGIN
    UPDATE TOP(10000) ? SET RowUpdated = RowInserted WHERE RowUpdated IS NULL
    IF @@ROWCOUNT = 0
        BREAK
END'')
END
END'
```

15. (Optional) If the source is SIMATIC IT LMS or SIMATIC IT Production Suite and you have configured a linked server, change the values of environment properties as follows:
    - Replace **PPA: [linkedserver name].[PPAdbname]** with **PPA: PPAdbname** and **PPA Linked Server: linkedserver name** (without square brackets).
    - Replace **SitMes: [linkedserver name].[SitMesdbname]** with **SitMes: SitMesdbname** and **SitMes Linked Server: linkedserver name** (without square brackets).

5 Migrating from Opcenter Intelligence Analytics (Tableau OEM) to standard Tableau Server

This guide aims at providing a step-by-step procedure to help customers migrating from Opcenter Intelligence Analytics (Tableau® OEM), embedded in Opcenter Intelligence until Tableau® 2410.1 version and no longer supported) and the standard Tableau® Server (compatible with Opcenter Intelligence starting from 2501 version).

⚠ This migration procedure must be performed before **15 February 2025**, because starting from that date Opcenter Intelligence Analytics (Tableau® OEM) will no longer work.

Important Recommendations

- If you installed Opcenter Intelligence Analytics (Tableau® OEM) on a dedicated machine, it is suggested that you setup a new "parallel" machine and then, when the new Tableau® Server is fully operational, remove the old machine.
- If you want to execute the installation on the same machine, keep in mind that the procedure will require multiple restarts of the computer. As a consequence, for an all-in-one scenario, Opcenter Intelligence will experience downtime periods.

Prerequisites

Check if Tableau® Server and Desktop hardware and software requirements are met on the machine where you want to install the two applications. For details, you can refer to Tableau® official documentation at the following links:

- https://help.tableau.com/current/server/en-us/requ.htm#hardware-requirements
- https://help.tableau.com/current/server/en-us/requ.htm#operating-system-requirements
- https://help.tableau.com/current/server/en-us/requ_diskspace.htm
- https://www.tableau.com/products/techspecs

⚠ Please note that the RAM required for Tableau® Server has increased compared with the previous Opcenter Intelligence Analytics (Tableau® OEM) requirement.

Workflow

⚠ Depending on the machine where you want to install the new Tableau® (either on the same machine as Tableau® OEM or on a different machine), the removal of Tableau® OEM must be executed in a different sequence.

1. Download Tableau® Server and Tableau® Desktop.
2. Backup data from Tableau® Server OEM.
3. *If the new Tableau® is going to be installed on the same machine as Tableau® OEM* Remove Tableau® OEM.
4. Install the new Tableau® Server.
5. Restore backed-up data to the new Tableau® Server.
6. Install Tableau® Desktop.
7. Upgrade Opcenter Intelligence and configure Tableau Server.
8. *If the new Tableau® is going to be installed on a different machine (recommended)* Remove Tableau® OEM.

5.1 Downloading Tableau Server and Tableau Desktop

Prerequisites

Before the download you must have registered and signed in to Tableau® web portal.

Procedure

1. Download Tableau® Server and Tableau® Desktop 2024.2.4 from the following URLs and copy them to the destination machine where Tableau® Server and Tableau® Desktop are going to be installed.
    - https://www.tableau.com/support/releases/server/2024.2.4
    - https://www.tableau.com/support/releases/desktop/2024.2.4

⚠ Tableau® license is provided separately and is no longer included in Opcenter Intelligence setup.

5.2 Backing up data from Tableau Server OEM

Important Recommendations

- The backup process can take a long time to run. Since no other jobs can be run while the backup is running, we recommend that you run the backup during non-business hours.
- When backing up Tableau® Server on Windows to a network drive, the machine account, that is the user you have selected while configuring Tableau Server for the Run As Service account (i.e. User Account or Network Service account), must have writing access to the network share where the backup files are written (this is not normally the case and you are responsible for configuring this if you want to back the server up to a network share). For more details, see https://help.tableau.com/current/server/en-us/backup_restore.htm
- Remember to collect any information you may need for the next operations, because Tableau® OEM data will no longer be available after the removal.

Prerequisites

Before backing up Tableau® Server OEM, verify that permissions are configured correctly.

Procedure

1. On the machine where Tableau® Server OEM is installed, open Command Prompt with administrative permissions and launch the backup by typing the following command, where <*filename*> is the name of the backup file (for example **ts_backup.tsbak**).

    ```
    tsm maintenance backup --file <filename>.tsbak
    ```

    ⚠ The default path where the backup file is stored is **C:\Program Files\Siemens\Tableau\Tableau Server\data\tabsvc\files\backups**. After running the above command, make sure that the backup file is created. For more information, see https://help.tableau.com/current/server/en-us/cli_maintenance_tsm.htm#tsm-maintenance-restore

2. Back up server topology and configuration data by launching the following command, where <*filename*> is the name of the backup file (for example **tsexport.json**):

```
tsm settings export -f <filename>.json
```

5.3 Installing the new Tableau Server

It is recommended that you install Tableau® Server on a new VM.

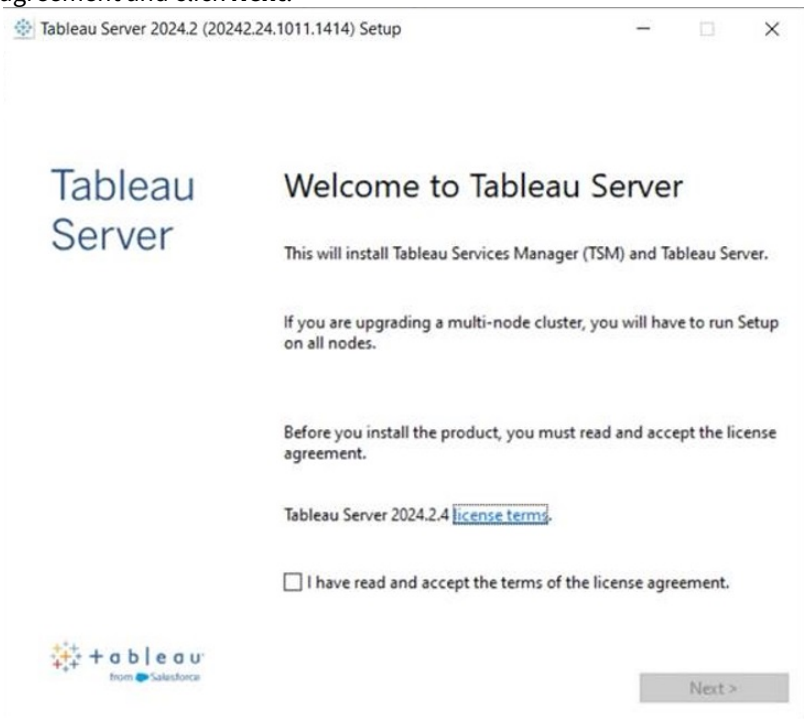
> ⚠ If the new Tableau® is going to be installed on the same machine as Tableau® OEM, you must remove Tableau® OEM before executing this installation procedure.
> If that is the case, remember to collect any information you may need for the next operations, because Tableau® OEM data will no longer be available after the removal.

Prerequisites

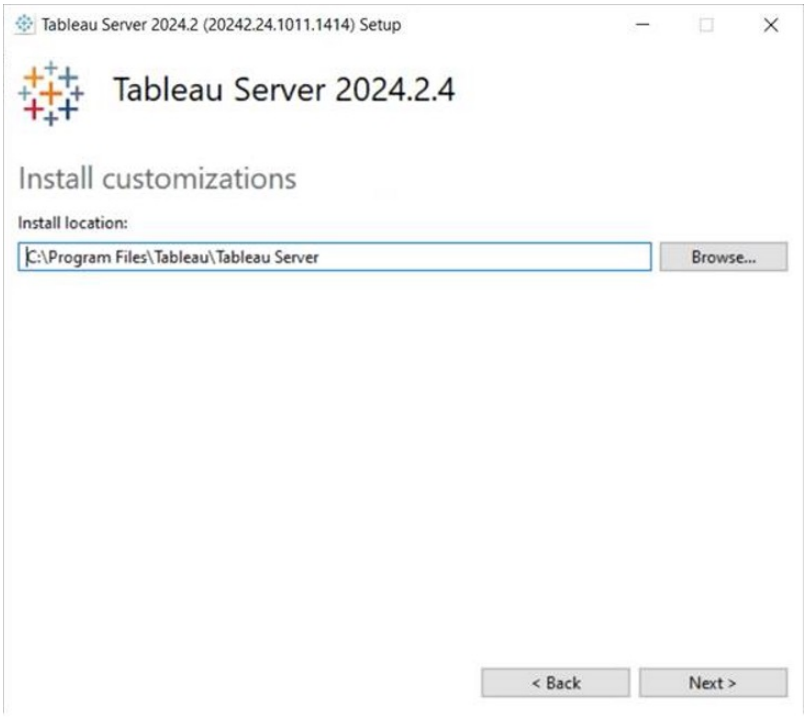
You have executed the backup of Tableau® OEM data.

Procedure

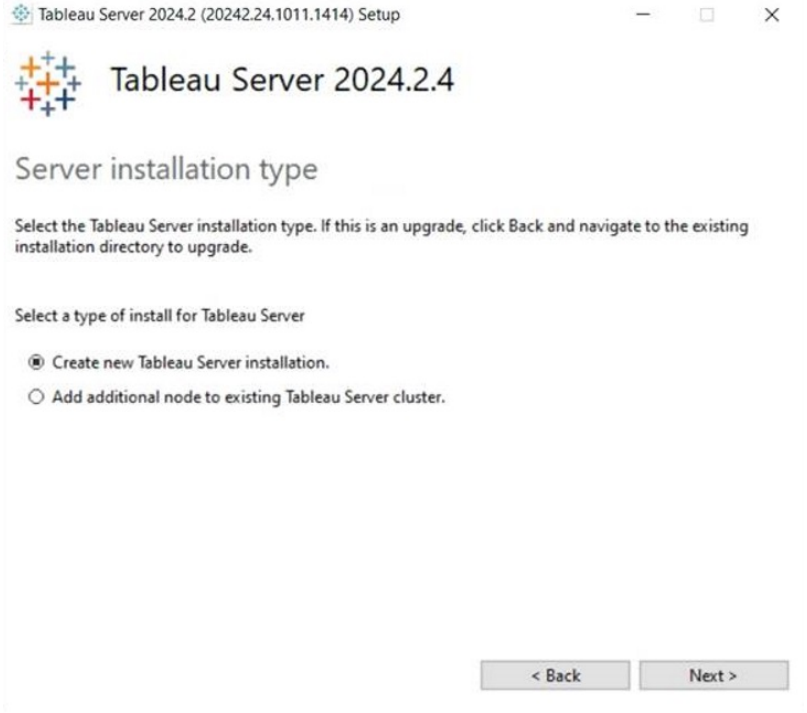
1. Execute the **TableauServer-64bit-2024-2-4.exe** file as an Administrator. Accept the terms of the license agreement and click **Next**.



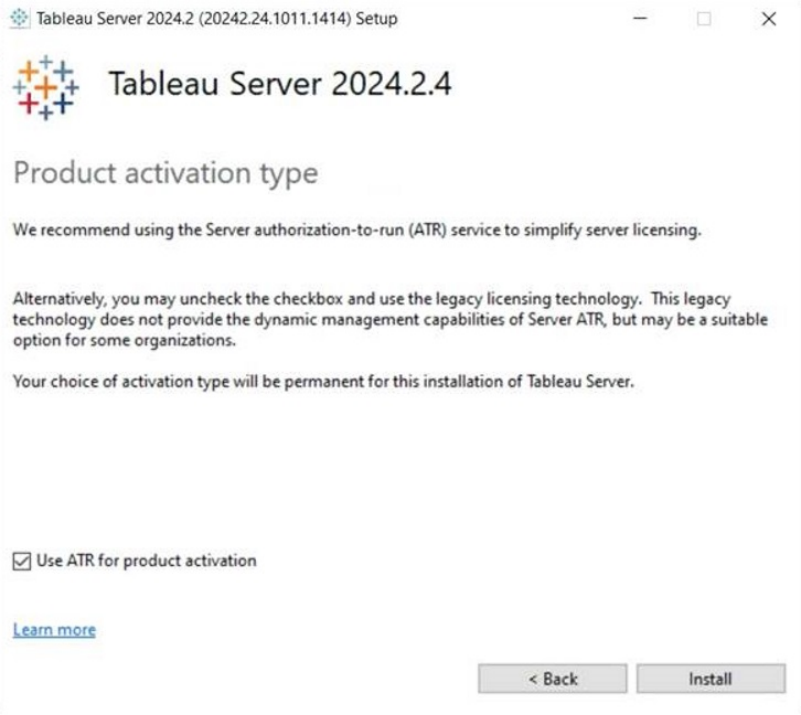
2. Browse for the install location and click **Next**.



3. Select **Create new Tableau Server installation** as type of install and click **Next**.

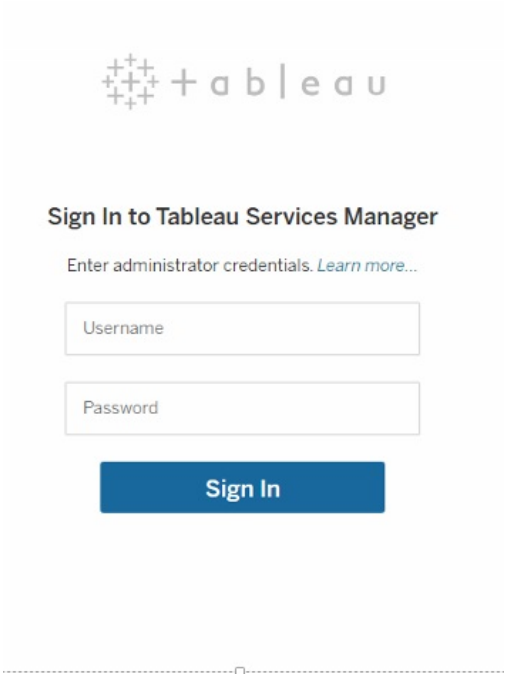


4. Select **Use ATR for product activation** and click **Install**.

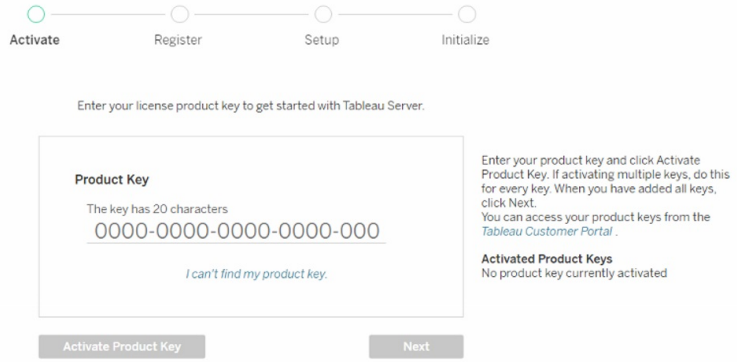


5. Restart the computer.

6. After the installation, open a browser and type the URL of Tableau Service Manager (for example: http/https://<*machine name*>:8850) to be redirected to the **Tableau Services Manager** login page, where you need to log in with the Windows system credentials (the username and password you use to log in to the Windows machine). The default port number for TSM is 8850.



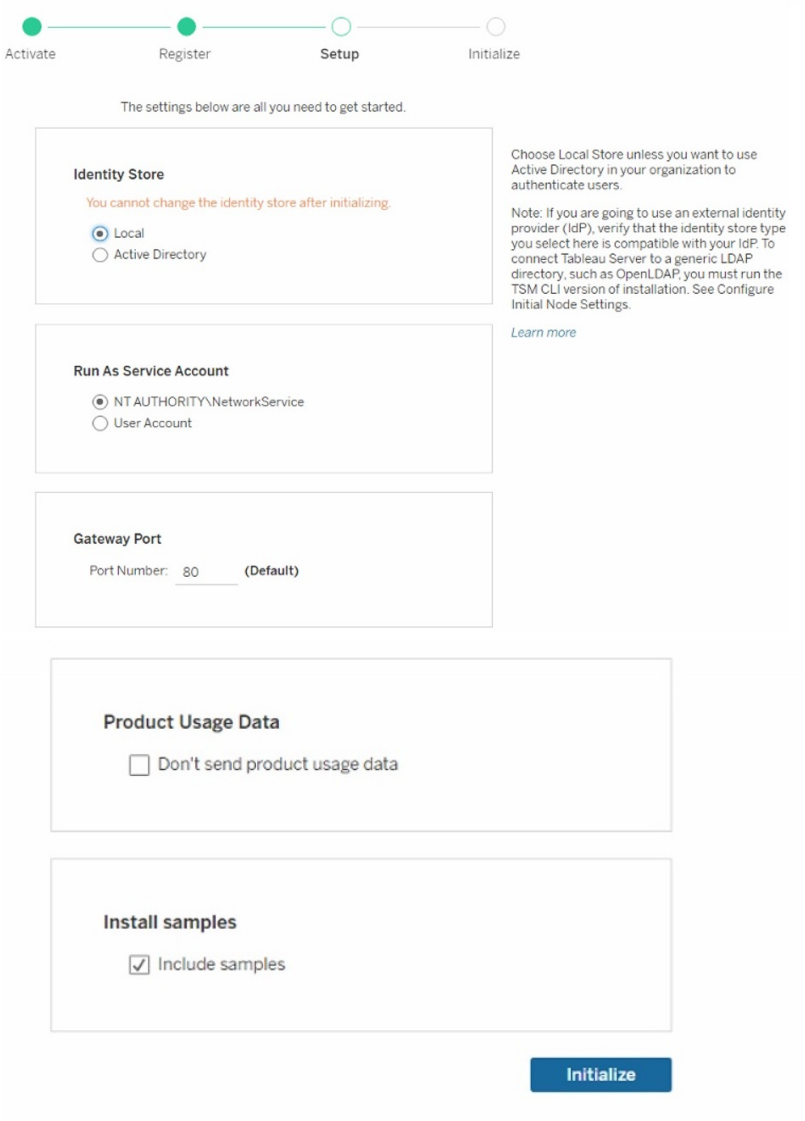
7. In the **Activate Product Key** step, insert the product key received from Siemens, click **Activate Product Key**, then click **Next** and wait for the process to complete.



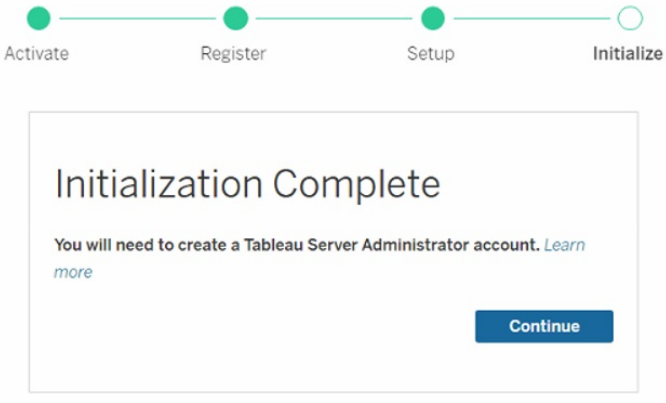
8. Configure the following settings:
   - **Identity Store**: select the **Local** option.
   - **Run As Service Account**: see https://help.tableau.com/current/server/en-us/runas.htm

     If you want to create dashboards with data stored in the Manufacturing Data Warehouse using the integrated security and SQL Server is installed on a different machine than Tableau®, it is suggested that you configure a User Account specifically created on your domain (Active Directory).

   - For **Gateway Port**, **Product Usage Data** and **Install Samples** settings you must keep the same settings configured for Tableau® OEM Server. Click **Initialize**.



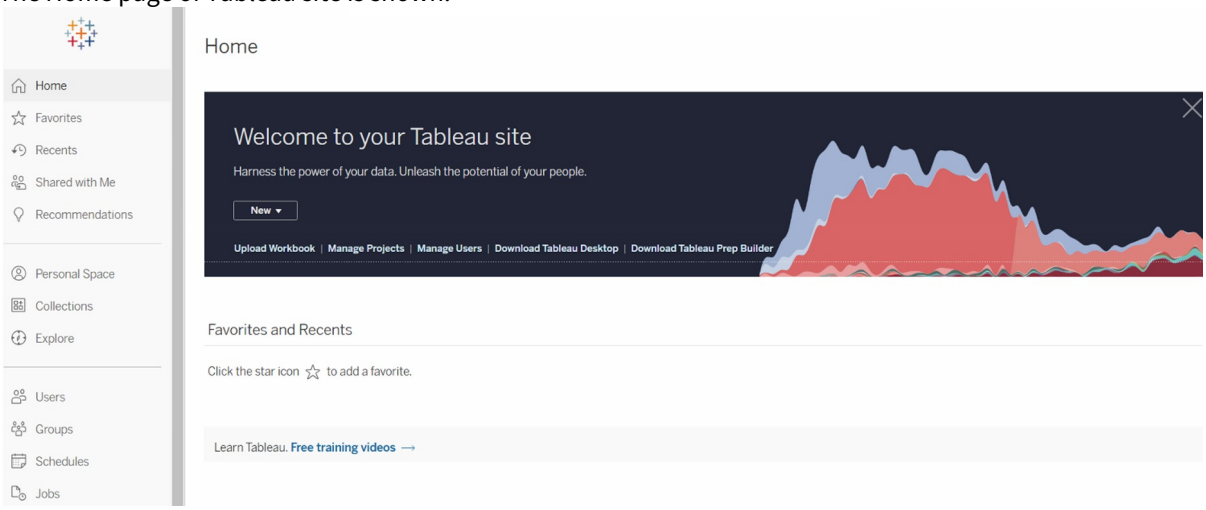
9. Wait for the initialization process to complete and then click **Continue**.



10. Create a **Tableau Server Administrator Account**. This Administrator Account is temporary. Please make note of username and password, which will be required while running the initializing user TSM command after the

restore process is completed.

11. The Home page of Tableau site is shown.



5.4 How to Restore backed-up data to the new Tableau Server

Prerequisites

- You have backed up data from Tableau Server OEM.
- You have installed the new Tableau® Server.

Workflow

1. Restore backed-up data
2. Performing post restore operations

5.4.1 Restoring backed-up data

Prerequisites

The following files must be ready to be used:

- Topology and configuration data **.json** file generated during the backup procedure by the "tsm settings export" command (for example **tsexport.json**).
- Repository backup **.tsbak** file generated during the backup procedure by the "tsm maintenance backup" command (for example **ts_backup.tsbak**).

Procedure

1. Import topology and configuration data. Copy the topology and configuration **.json** backup file to the computer where Tableau® Server is currently installed.
2. On the same machine, open Command Prompt with administrative permissions and import the **.json** file by running the following command.

```
tsm settings import -f <filename>.json
```

3. Apply pending changes by running the following command.

```
tsm pending-changes apply
```

4. Restart Tableau® Server by running the following command.

```
tsm restart
```

5. Restore Tableau® Server by running the following command using the specified **.tsbak** backup file generated during the previous backup procedure.

```
tsm maintenance restore --file <filename>.tsbak
```

5.4.2 Performing post restore operations

Prerequisites

The procedure to restore backed-up data to the new Tableau® Server is complete.

Procedure

1. Log in to Tableau Services Manager (TSM): open a browser, enter the Tableau Server URL, and append the dedicated TSM web UI port (the default port is 8085).
2. Create the initial administrative user for Tableau® Server by running the following commands in Command Prompt with administrative permissions. You have to set the same Administrator User Name and password used while configuring Tableau® Server. For Gateway Port settings you must keep the same settings configured for Tableau® OEM Server. Example of Tableau Gateway Url: http/https//*<machine name>*:*<configured port>*.

```
tsm reset
```

```
tabcmd initialuser --server <TableauGatewayUrl> --username <UserName> --password
<password>
```

3. On the **Configuration** tab, select **User Identity & Access**.
4. On the **Trusted Authentication** tab, in **Trusted Hosts**, insert all the IP addresses of Web API Server. These IP addresses are required to whitelist Web API server to communicate with Tableau Gateway. Please remember to collect all the information you need before Tableau® OEM removal.
5. Click **Save Pending Changes**.

> ⚠ Steps from 6 to 9 must only be executed if you want to configure the new Tableau® Server in HTTPS.

6. On the **Configuration** tab, select the **Security** option and click **External SSL**.
7. Under **External web server SSL**, select **Enable SSL for server communication**.
8. Upload the certificate and key files.
9. Click **Save Pending Changes**.
10. Set up access with unrestricted tickets by running the following command.

```
tsm configuration set -k wgserver.unrestricted_ticket -v true
```

11. Select **Pending Changes** on top of the page and click **Apply Changes and Restart**. As an alternative, you can run the following commands.

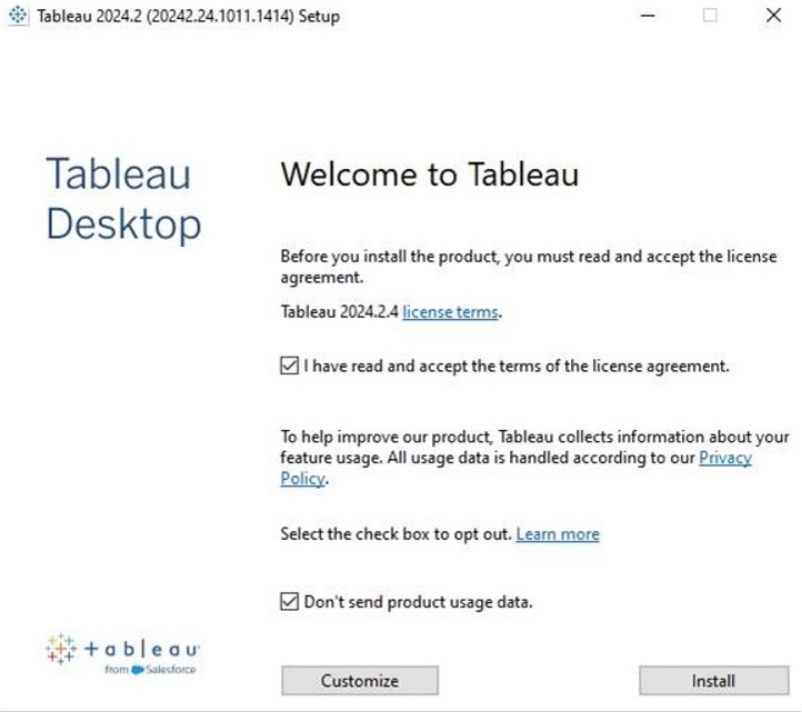
```
tsm pending-changes apply
tsm restart
```

> ℹ Tableau® Server restart might take some time. Once the server is restarted, try to log in with the existing users and check whether all required data was migrated using the Gateway URL.

5.5 Installing the new Tableau Desktop

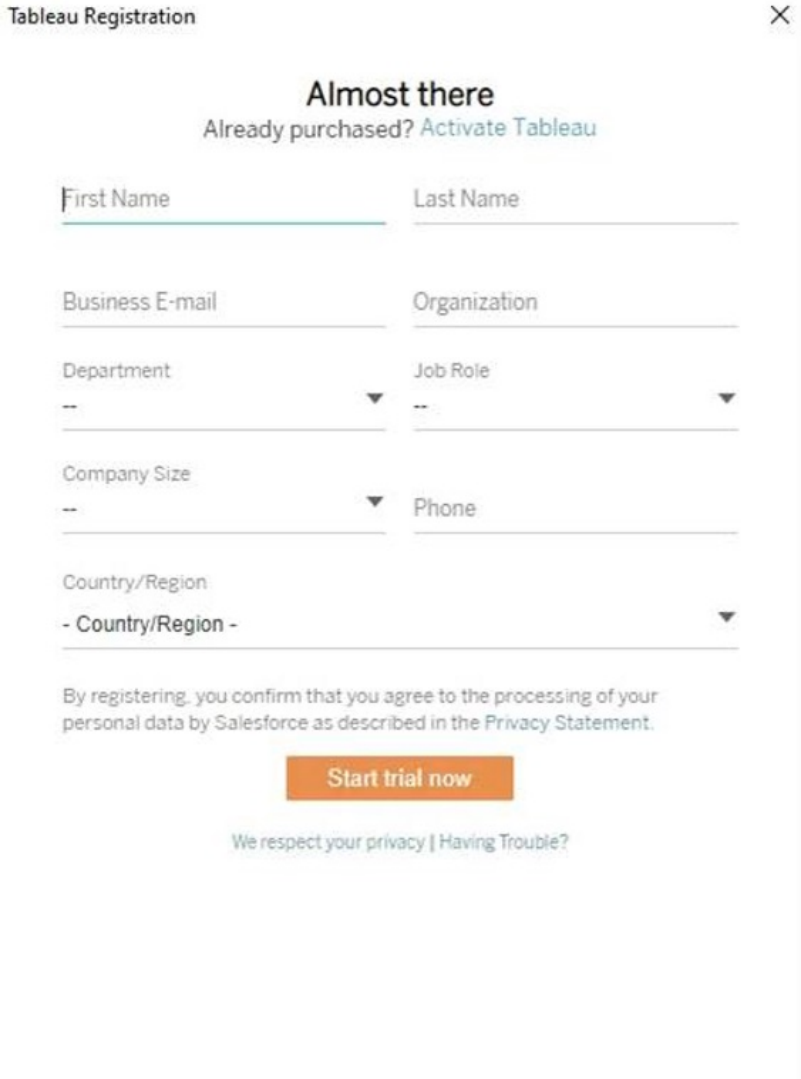
Procedure

1. Execute **TableauDesktop-64bit-2024-2-4.exe** as an Administrator. Click **Install**.

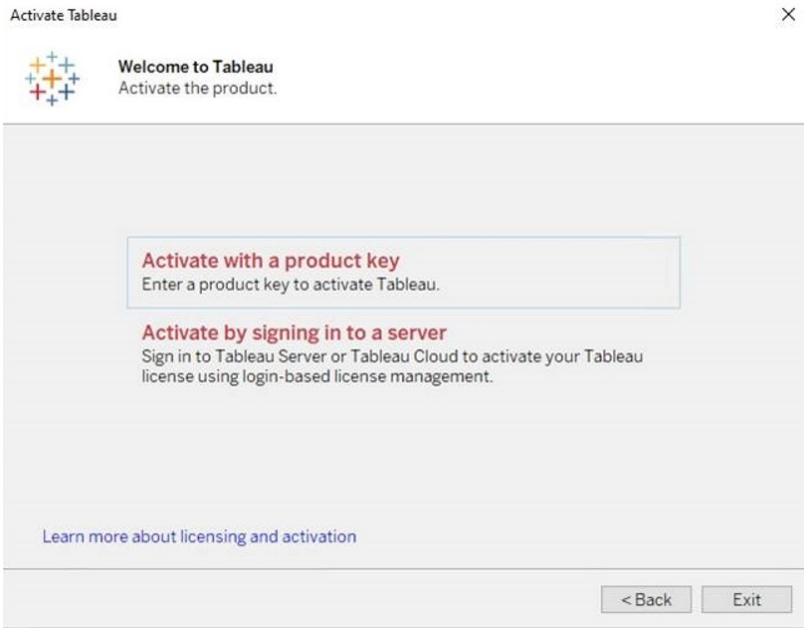


2. After the installation is completed, open Tableau Desktop application from the machine.

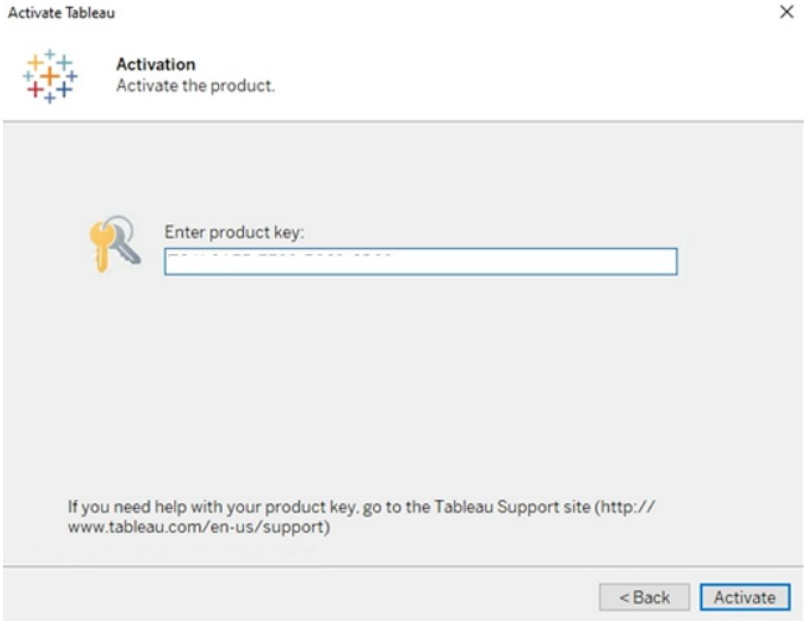
3. Click the **Activate Tableau** link instead of filling the form.



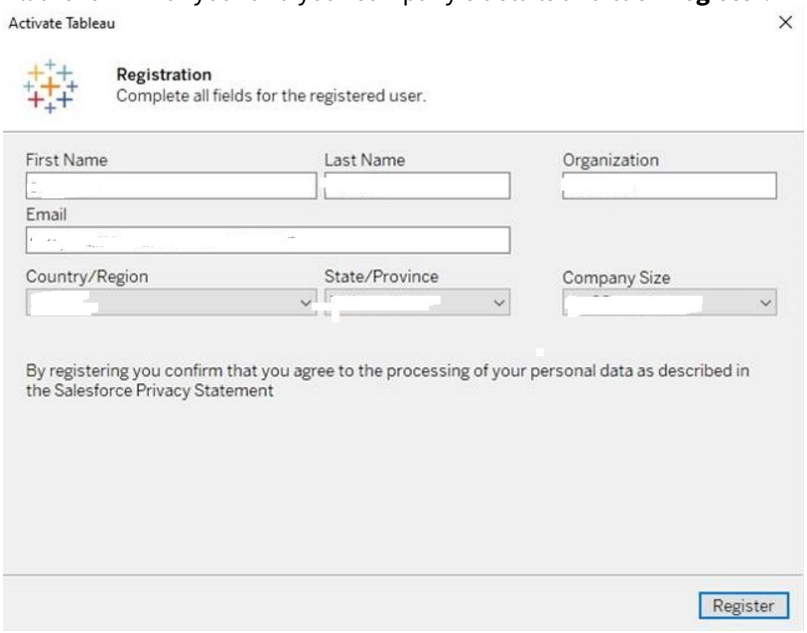
4. Select **Activate with a product key**.



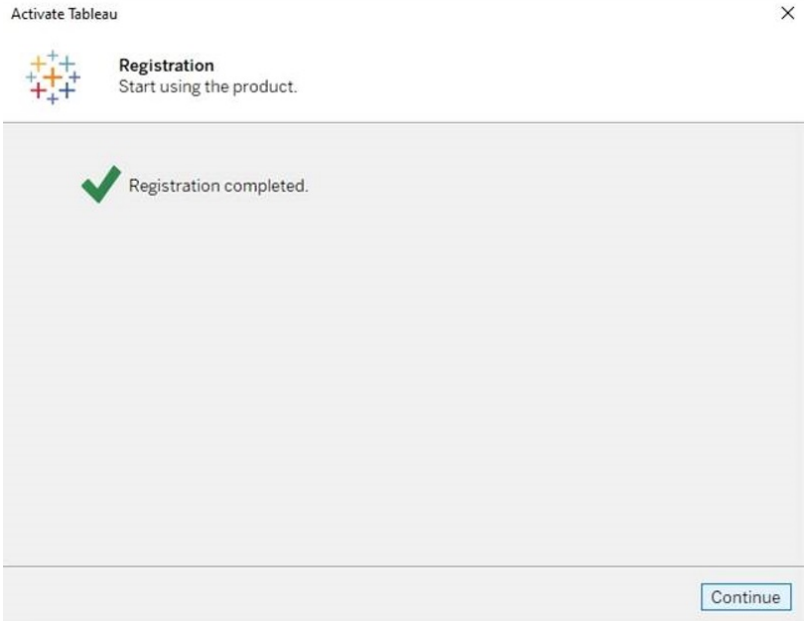
5. Type the product key provided by Siemens.



6. Fill the form with your and your company's details and click **Register**.



7. When the registration is completed, click **Continue** and check if Tableau Desktop is working as expected.



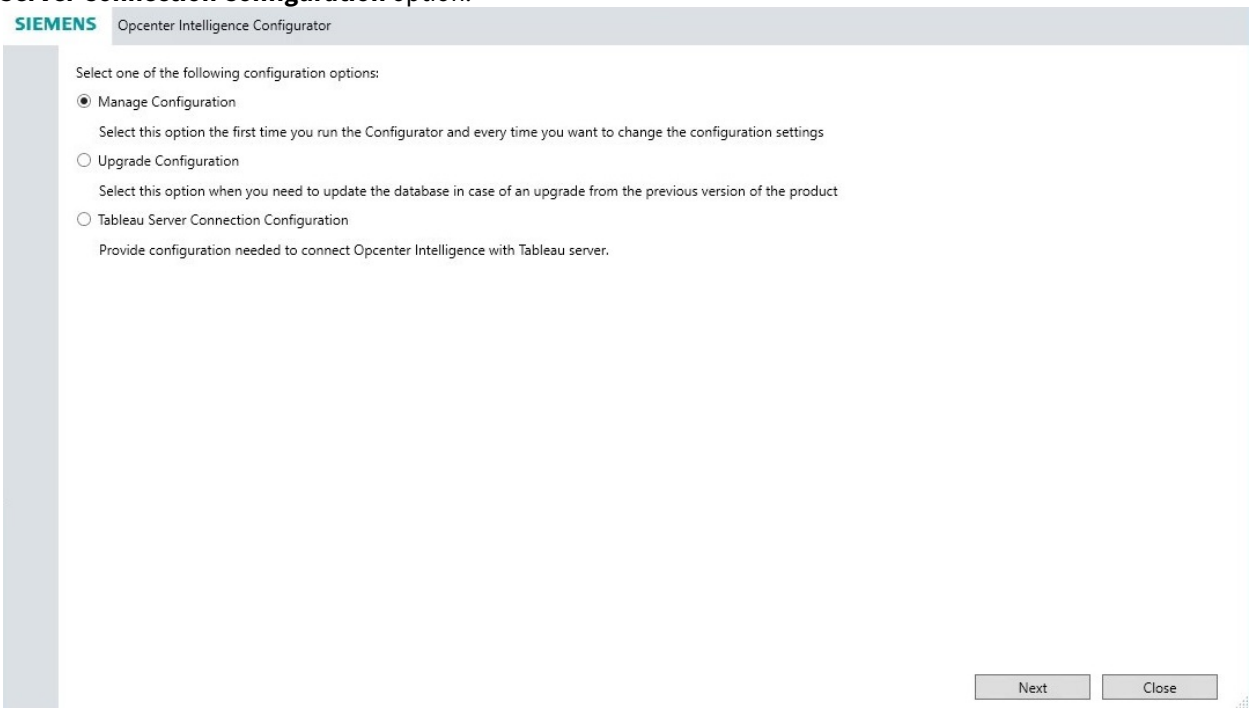
5.6 Upgrading Opcenter Intelligence and Configuring Tableau Server

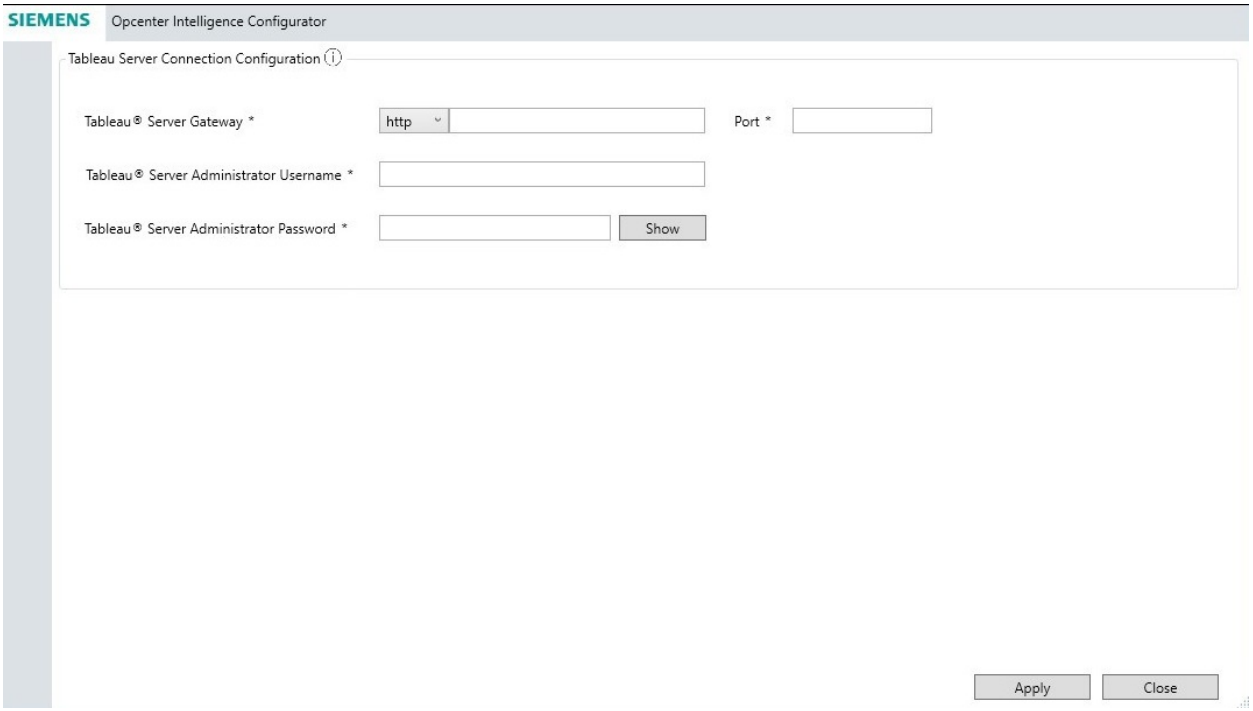
Prerequisite

- You have performed the procedure to upgrade Opcenter Intelligence described in Upgrading from previous versions of Opcenter IN to Opcenter IN 2501.0001.
- The new Tableau® Server has been installed successfully.

Procedure

1. To navigate through the items created in Tableau® Server and view the resulting dashboards embedded in Opcenter Intelligence, run Opcenter Intelligence Configurator as an Administrator and choose the **Tableau Server Connection Configuration** option.





2. Configure the following settings:

Field	Description
Tableau® Server Gateway	This field allows the user to input the URL for Tableau® Server Gateway. It defines the address to which the system will connect for all Tableau® Server-related activities. Select the protocol for Tableau® Server and insert the <*server name*> of the machine where Tableau® Server is running (for example http/https://<*machine name*>:8085).
Port	This field must contain the Gateway port number for Tableau® Server. It defines the network port used for communication between the system and Tableau® Server, typically set to the default Tableau® Server port or custom port configured for the environment. For Gateway Port settings you must keep the same settings configured for Tableau® OEM Server (example: http/https//<*machine name*>:<*configured port*>.
Tableau® Server Administrator Username	This field must contain Tableau® Server Administrator's username. The administrator is responsible for managing the Tableau® Server environment, and this credential is necessary for performing administrative actions. It must match with the username used while configuring TSM Administrative account.
Tableau® Server Administrator Password	This field must contain the password for the Tableau® Server Administrator account. It is required to authenticate the user and enable access to the administrative functions on Tableau® Server. It is the same password used while configuring TSM Administrative account.

3. Click **Apply** and wait for the notification that confirms the successful completion of the configuration. Then click **Close**.
4. Log in to Opcenter Intelligence.

5.7 Removing Tableau OEM

⚠ This operation is not reversible: after this activity, Tableau OEM data will no longer be available.

Procedure

1. Uninstall Tableau® Desktop and Tableau® Server. You can use the Control Panel remove/uninstall option to perform this operation. After completing this process, please check in Control Panel if Tableau OEM Server and Desktop were removed. If not, remove them manually.
2. Run the following TSM commands to remove Tableau OEM Server from the system.

```
tableau-server-obliterate.cmd -y -y -l -a
refresh-environment-variables.cmd
```

3. Manually delete any existing Tableau folders present in the **C:\ProgramData** and **C:\ Program Files\Siemens** folders.

   For more information, please refer to:
   - https://help.salesforce.com/s/articleView?id=001471574&type=1
   - https://help.tableau.com/current/server/en-us/remove_tableau.htm#running-the-tableauserverobliterate-script

6 Upgrading from Opcenter Intelligence 2.x to Opcenter Intelligence 2501.0001

Perform the following procedure if you want to migrate a solution created in Opcenter Intelligence 2.x to Opcenter Intelligence 2501.0001.

Prerequisites

- You have executed a deploy operation in Opcenter Intelligence 2.x.
- You have exported and saved a solution in Opcenter Intelligence 2.x.
- You have stopped old flows from SQL Server Agent.
- You have manually stopped the **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost** service.
- It is suggested that you make a backup of the existing engineering database.

Procedure

1. After you have exported the 2.x solution, uninstall Opcenter Intelligence 2.x (you do not need to uninstall the User Management Component).
2. In **Microsoft SQL Server Management Studio**, delete the **MIStudio** database manually (this step is optional if you mean to assign a different name to the new engineering database).
3. Install Opcenter Intelligence 2501.0001.
4. Run Opcenter Intelligence Configurator.
5. Select the **Manage Configuration** option and click **Next**.
6. Select the **Create and configure the engineering database** checkbox in the **SQL Server** area of the Configurator to create and configure a new engineering database.
7. If UMC is already installed, select the **Existing configuration** option in the **UMC** area.
8. Click **Apply** and wait for the notification that confirms the successful completion of the operation.
9. Click **Close**.
10. Check that the **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost** service is in **Running** status. If not, start this service.
11. Import the previously exported Opcenter Intelligence 2.x solution.
12. Check the environment details of the imported solution.

    > It is highly recommended that you check that server, environment, database and other properties are exactly the same as those of the previous version.

13. (Optional) If the source is SIMATIC IT LMS or SIMATIC IT Production Suite and you have configured a linked server, change the values of environment properties as follows:
    - Replace **PPA: [*linkedserver name*].[*PPAdbname*]** with **PPA: *PPAdbname*** and **PPA Linked Server: *linkedserver name*** (without square brackets).
    - Replace **SitMes: [*linkedserver name*].[*SitMesdbname*]** with **SitMes: *SitMesdbname*** and **SitMes Linked Server: *linkedserver name*** (without square brackets).
14. Deploy the environment: this operation will update the data warehouse to the new version.
15. Execute an initial flow to reinitialize the flow between the source and the data warehouse:
    - Select the **Manual** start mode and insert the date and time when you have started the upgrade as **Start Date and Time** and the present date and time as **End Date and Time** in order to avoid loading data already present in the MDW and only load data from the time when old flows have been removed from SQL Server Agent.
    - Enable the automatic incremental flows manually or in SQL Server.

7 Uninstalling Opcenter Intelligence

To completely uninstall Opcenter Intelligence, you must perform the following procedure.

Important Recommendations

- Uninstalling UMC requires a number of additional actions. For more details on how to uninstall UMC properly, see *Central User Management UMC Programming and Operating Manual*.
- If your configuration requires a new database for the next installation, in Microsoft SQL Server Management Studio delete the **MIStudio** database manually. If on the contrary you want to maintain the existing database, you must clear the **Create and configure the engineering database** checkbox in Opcenter Intelligence Configurator so that the database will not be created and configured.

Procedure

1. From **Windows Control Panel > Programs and Features** environment, select **User Management Component** and click **Uninstall**.
2. From **Windows Control Panel > Programs and Features** environment, select Opcenter Intelligence and click **Uninstall**.
3. Stop and delete the **Siemens.SimaticIT.UAMI.MIStudio20.ServiceHost** service manually.
4. Restart the computer.

8 Troubleshooting

The following information can help you overcome common issues that you may encounter during the installation or configuration of Opcenter Intelligence.

Issue	Possible Cause	Possible Solution
When you launch the setup the following error is returned: **Opcenter Intelligence Core Locked by:** **Opcenter Intelligence setup cannot start: SQL Server is not installed properly (check installation manual)**.	SQL Server Integration Services was not installed.	Check that all requirements described in the **Installation Manual** are fulfilled. See also: https://support.sw.siemens.com/en-US/knowledge-base/PL8690302
After the successful execution of the Configurator , when you try to log in to OCIN for the first time and insert the credentials of the user configured at the previous step, the following error message is displayed by the application on the **User Login** panel: **The validation of the parameter 'service' failed**.	Opcenter Intelligence URL was not added to UMC whitelist.	Add the URL: **http(s)://<machine name>/UserGateway/Login/Login** to UMC whitelist. To do so: 1. Navigate to **C:\Program Files\Siemens\UserManagement\BIN** and open the Command Prompt. 2. Execute the command: **umconf -c -w -d http(s)://<machine name>/UserGateway/Login/Login** 3. Restart UMC service. 4. Recycle the application pool of the Identity Provider in IIS Manager. ⚠ If UMC is used by another product (for example Opcenter EX DS) in a production environment, all sessions are deleted. ℹ For more details, see *Create allowlist entry* in *Central User Management UMC Programming and Operating Manual*. See also: https://support.sw.siemens.com/en-US/knowledge-base/PL8688159

Issue	Possible Cause	Possible Solution
When you try to connect to UMC or OCIN using the HTTP protocol, the URL is automatically redirected to HTTPS and the following error is returned: **Error: This site can't be reached – ERR_CONNECTION_REFUSED**	One of the possible causes is that in **IIS Manager > Sites > Default Web Site**, HTTP Strict Transport Security (HSTS) is **Enabled** and the **Redirect Http to Https** option is selected.	In IIS Manager, disable HSTS: 1. Start IIS Manager. 2. Navigate to **Sites** and click on **Default Web Site**. 3. In the **Actions** menu select **HSTS...** 4. Uncheck all directives, set the max-age directive to 0 and finally uncheck the **Enable** checkbox. 5. Run IISRESET. See also: https://support.sw.siemens.com/en-US/knowledge-base/PL8698654

Opcenter Intelligence and User Management Component (UMC) manuals are available after you have installed Opcenter Intelligence in the following folders:

- **<setup drive>Program Files\Siemens\Opcenter\Intelligence\IN\Documentation**
- **<setup drive>Program Files\Siemens\UserManagement\Documentation**

or on Support Center at the link: https://support.sw.siemens.com/en-US/