SIEMENS

Opcenter Reporting 2401.0001

Installation Manual

04/2024

PL20240130630874732

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.

Report-/Print engine List & Label ® Version 28: Copyright combit® GmbH.

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.

Security information

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

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement - and continuously maintain - a holistic, state-of-the-art industrial security concept. Siemens' products and solutions 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 security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

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 Security RSS Feed under https://www.siemens.com/cert.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

PL20240130630874732
20240409_160639

Table of Contents

ID	Opcenter_Reporting_InstallationManual
Title	Installation Manual
Product Title	Opcenter Reporting
Version Title	2401.0001
Product Version	Opcenter_Reporting_2401.0001
Category	Installation, Configuration
Summary	Provides detailed information on how to install and configure Opcenter Reporting.
Audience	System Integrator, Commissioning Engineer, Support Engineer, Project Engineer
Revision	PL20240130630874732
State	Published
Author	Siemens AG
Language	en-US

1 Before you Start

Before you install Opcenter Reporting, 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 who will perform them.
- Verify that all prerequisites are satisfied.
- Follow 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.

⚠ 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.

Installation Options

Opcenter Reporting can be installed in either of the following ways:

- After the installation of Opcenter Intelligence, whose ISO root folder contains the **OpcenterReport** subfolder including Opcenter Reporting setup files.
- As a stand-alone application, directly launching the **Start.exe** program file from the **OpcenterReport** subfolder.

For more information, see Installing Opcenter Reporting.

Virtual Infrastructure Support

Opcenter Reporting supports VMware ESXi 6.7 Update 3 infrastructure, although the possibility cannot be excluded that Opcenter Reporting 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 Reporting hardware requirements and allocate resources (RAM, vCPU and so on) to guarantee the maximum performance level of VMWare operations.

1.1 Managing Licenses, Users and Roles for Opcenter Reporting

Starting from version 3.2, a new licensing model is applied. According to this new model, license types are based on the number of users (seats) that can access the application at the same time, depending on the type of purchased license. A seat is consumed for each logged-in user, unless this user has been assigned the **No role** role.

While in previous versions the creation of analytical solutions and the use of the Manufacturing Data Warehouse and ETLs were allowed to customers who purchased the Opcenter Reporting license, starting from version 3.5 the purchase of an additional Opcenter Intelligence license is required to use these functionalities.

✓ See *Opcenter Reporting User Manual* for details on how to configure users and assign roles, check the number of available seats and release seats.

The following licenses can be purchased for Opcenter Reporting:

License	Description
Opcenter Reporting	Server-based license that allows users to perform the following operations: • Open Combit® List & Label Designer • Design reports • View reports • Move reports to a different folder • Delete reports • Manage data sources
Opcenter Reporting Client	Client-based license, which includes the number of allowed seats, to be added to the Server-based license.

Users and Roles

If the **Can perform administrative functions** check box is selected for a user, he can perform the following operations:

Permission (check box selected)	Actions
Can perform administrative functions	• Manage data sources • Manage user roles (including assigning roles to users) • Import and export reports

The following roles can be associated with users in the **Access Control** page.

Role	Description
Report Author	Can perform the following operations: • Open Combit® List & Label Designer • Design reports • View reports • Move reports to a different folder • Delete reports • Manage data sources • Import and export reports
Report Viewer	Can view reports.
No role	This role cannot perform any of the operations that the Report Author and Report Viewer roles can execute, nor consumes any seats.

1.2 Prerequisites

The following prerequisites are required before you install Opcenter Reporting.

- Software Requirements
- Hardware Requirements

> The system must use UTC time to synchronize client and server machines so that the time difference between clients and servers can be based on UTC time and not on the time zone.

1.2.1 Software Requirements

Operating Systems

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 10
- 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 aforementioned Operating Systems.

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 data source product.

> Opcenter Reporting can only be connected to the databases of Siemens MOM products. The connection to third-party databases is not allowed.

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

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.

Oracle

Product	Edition	Language
Oracle Database 12c Release 2	Enterprise	English
Oracle Database 18c	Enterprise	English
Oracle Database 19c	Enterprise	English

> ⚠ Starting from Oracle ODAC 18, the machine-wide configuration has changed.
> For more details see *Checking Oracle Installation Requirements*:
> - version 19c
> - previous versions

User Management Component (UMC)

- Opcenter Reporting is compatible with User Management Component (UMC) 2.6 and higher.

  > ⚠ If a previous version of UMC has already been installed on your system with another product on the same machine as Opcenter Reporting, you must upgrade it to version 2.9 SP2.
  > A previous version of UMC does not require an upgrade if Opcenter Reporting and UMC are running on different machines.

- Opcenter Reporting is not compatible with UMC 1.9.1.

For more information on UMC prerequisites, see *User Management Component Installation Manual*.

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 is required for Opcenter Reporting configuration and can be installed either on an Opcenter Reporting machine or on a separate machine where Opcenter Reporting 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**)

Other Third-Party Software

- Either Internet Information Services 8.5 or 10 enabling ASP.NET Modules and IIS Role Services
- Microsoft .NET Framework 4.7.2. This software can be downloaded at https://dotnet.microsoft.com/download/dotnet-framework/net472

Internet Browsers

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

- Microsoft Edge (based on Chromium) 123
- Google Chrome 123
- Mozilla Firefox 124

No Longer Supported Software

- Windows Server 2012 R2 x64
- Microsoft Internet Explorer

1.2.2 Hardware Requirements

The minimum hardware requirements for Opcenter Reporting are the following:

Installation Type	Processor	CPU	RAM	Free Disk Space
Single Server	64-bit	4 physical cores 2.0 GHz or higher	16 GB	50 GB

⚠ At least one printer or the Microsoft Print to PDF virtual printer must have been enabled in your system.

ⓘ 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.

1.3 Security Strategies

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

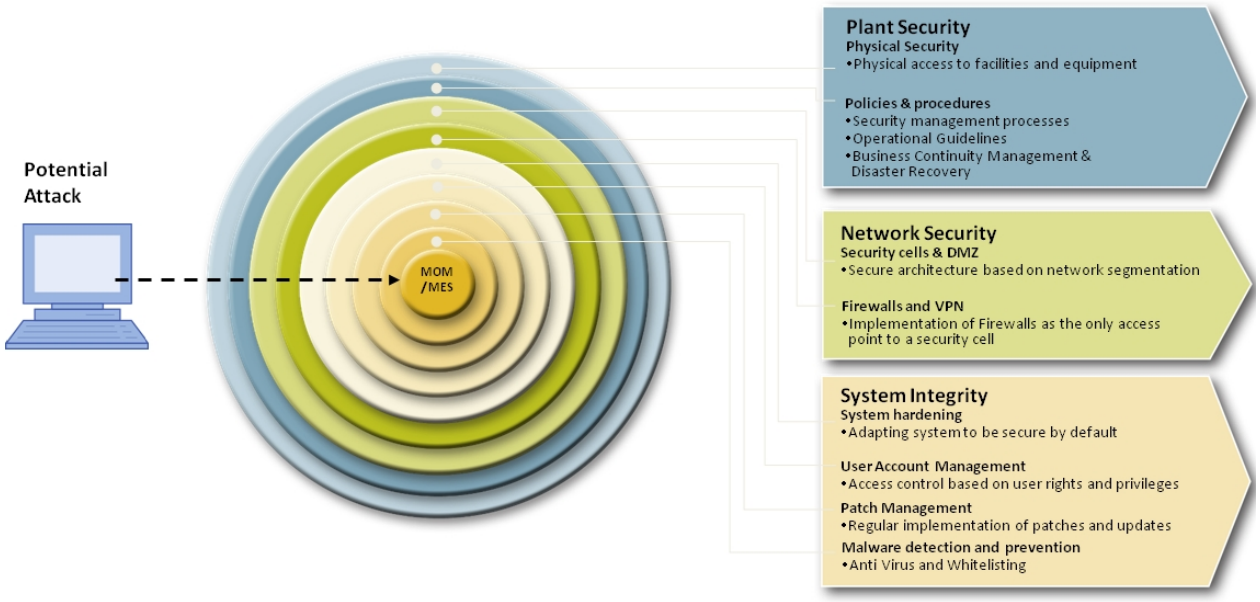
Computer systems and networks are inherently vulnerable to a wide variety of security threats that can be prevented or reduced by adopting specific security countermeasures.

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

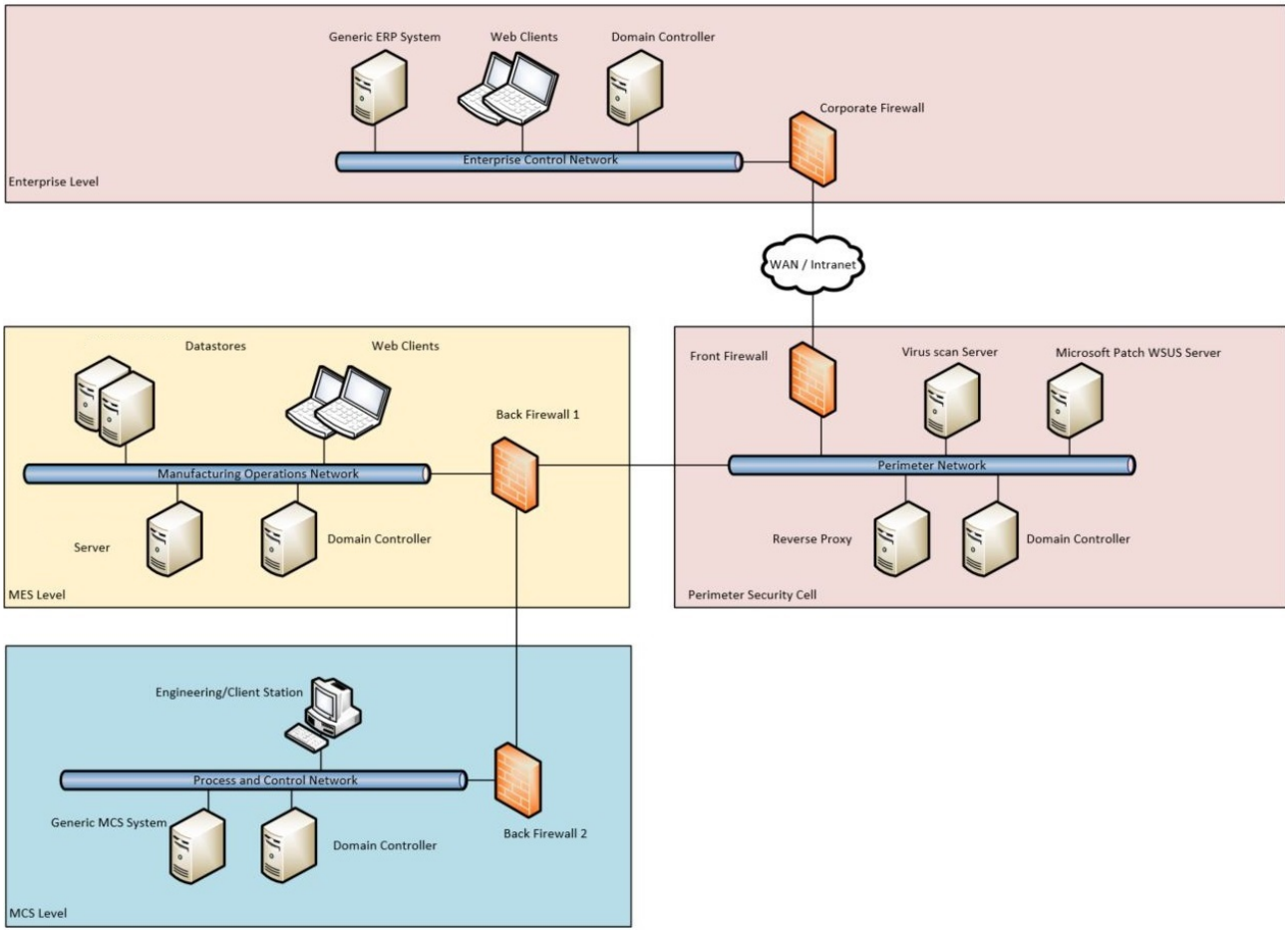
When designing and implementing a complex network scenario, the following rules should be followed to enhance security:

- 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.
- The communication protocols that have to be applied in order to guarantee network security.

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

Communication between different Security Cells

	Opcenter Reporting Server	**Reverse Proxy (*)**	**Data source**	**UMC**	**License Server**
Web Client	Blocked (*)	→ (https)	Blocked (*)	Blocked (*)	Blocked (*)
Opcenter Reporting 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.

	Opcenter ReportingServer	**Data source**	**UMC**	**License Server**
Web Client	→ (https)	Not Applicable (*)	→ (https)	Not Applicable (*)
Opcenter Reporting Server	→ (https)	Database Secure Communication	→ (https)	→ (tcp)

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

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
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 Reporting 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 Reporting 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 data sources (only for data reading)

Opcenter Reporting can be configured to resolve data queries on multiple data sources. It may be necessary to render the communication channel with these data sources secure, according to customer requirements.

Secure communication between Opcenter Reporting application server and an external system

All communication that makes it possible to join Opcenter Reporting 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 Reporting 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.

> ⚠ Customization 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
- 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
ProgramData\Siemens\Opcenter\Intelligence\Report\Server\App_Data	IIS AppPool\Opcenterrppool	Full control

> ⚠
> - 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 Reporting, 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, see: https://msdn.microsoft.com/en-us/library/ms187048.aspx.
- 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 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

1.3.2.1.3 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

1.3.2.1.4 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

1.3.2.1.5 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

1.3.2.1.6 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/

1.3.2.1.7 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 Patch Management

In general, office PC systems are protected against malware. Any weak points that are discovered in the operating system or in the user software 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 Reporting, 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.

1.3.2.3 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 Reporting, you should perform a number of preliminary steps:

- Install the License Server if it is not installed on your environment yet.
- Install the User Management Component (UMC) if it is not already installed on your environment. You can also install UMC during Opcenter Reporting setup.
- After UMC has been installed and before running Opcenter Reporting, you must configure UMC. For instructions on how to execute this operation, see *UMC documentation*.
- (*only if you want to use Oracle database management system*) Install Oracle following some specific requirements: version 19c - versions previous to 19c.
- Configure IIS and ASP.NET settings

⚠ If you execute these operations after you have installed Opcenter Reporting, you must either restart the machine or Run **IISRESET** from the command prompt.

1.4.1 Installing the License Server

Starting from version 2307, Opcenter Intelligence is migrating to Siemens Advanced Licensing Technology (SALT).

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

Installation File and Documentation

The installation file and 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**)

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. For more details, see *Opcenter Intelligence Installation Manual*;
    - specify a destination folder for the installation;
    - select the **I don't want this feature** check box.
7. Click **Done** to quit the installer.

⚠ Make sure the **Siemens License Server** service is running.

1.4.2 Checking Oracle 19c Installation Requirements

For details on Oracle installation, please refer to *Oracle official documentation*.

Starting from Opcenter Reporting 3.3, ODAC 19c is also supported.

When you install and configure Oracle, you must make sure to select the **Oracle Data Provider for .NET component** check box during installation.

Installing Oracle using a Private Configuration

This is an example on how to install Oracle using a private configuration using version 19.3.1.0:

1. Install **ODT** with **ODAC 19.3.1.0** on the same machine where Opcenter Reportingis running.
2. In the **C:\app\client\Administrator\product\19.0.0\client_1\odp.net\managed\x64** folder, select **configure.bat**.
3. Open the command prompt as Administrator.
4. Type **cd** C:\app\client\Administrator\product\19.0.0\client_1\odp.net\managed\x64
5. Launch the **configure.bat** file.
6. In **C:\app\client\Administrator\product\19.0.0\client_1\odp.net\managed\common** copy the **Oracle.ManagedDataAccess.dll** file.
7. Paste it to **C:\Program Files\Siemens\Opcenter\Intelligence\Report\Server\bin**
8. Modify the **Web.config** file that you can find in **C:\Program Files\Siemens\Opcenter\Intelligence\Report\Server** adding the following nodes:

```
<configuration>
    <configSections>
        <section name="oracle.manageddataaccess.client" type="OracleInternal.Co
mmon.ODPMSectionHandler, Oracle.ManagedDataAccess, Culture=neutral,
PublicKeyToken=89b483f429c47342" />
    </configSections>
    <runtime>
        <assemblyBinding>
```

```
            <dependentAssembly>
                <publisherPolicy apply="no" />
                <assemblyIdentity name="Oracle.ManagedDataAccess"
 publicKeyToken="89b483f429c47342" culture="neutral" />
            </dependentAssembly>
        </assemblyBinding>
    </runtime>
    <system.data>
        <DbProviderFactories>
            <remove invariant="Oracle.ManagedDataAccess.Client" />
            <add name="ODP.NET, Managed Driver" invariant="Oracle.ManagedDataAc
cess.Client" description="Oracle Data Provider for .NET, Managed Driver" type="
Oracle.ManagedDataAccess.Client.OracleClientFactory, Oracle.ManagedDataAccess,
Culture=neutral, PublicKeyToken=89b483f429c47342" />
        </DbProviderFactories>
    </system.data>
    <oracle.manageddataaccess.client>
        <version number="*">
        </version>
    </oracle.manageddataaccess.client>
</configuration>
```

The resulting **web.config** file should look as in this example:

```
<!--
  For more information on how to configure your ASP.NET application, please visit
  http://go.microsoft.com/fwlink/?LinkId=301880
  -->
<configuration>
  <configSections>
    <section name="oracle.manageddataaccess.client" type="OracleInternal.Common.ODPMSectionHandler, Oracle.ManagedDataAccess, Culture=neutral,
    PublicKeyToken=89b483f429c47342"/>
  </configSections>
  <appSettings>
    <add key="webpages:Version" value="3.0.0.0"/>
    <add key="webpages:Enabled" value="false"/>
    <add key="ClientValidationEnabled" value="true"/>
    <add key="UnobtrusiveJavaScriptEnabled" value="true"/>
    <add key="FlexLicenseServer" value="28000@VM-TEST2"/>
    <add key="EnableSwagger" value="false"/>
    <add key="CreationTimeMaxDiff" value="60"/>
    <add key="IdentityProviderUrl" value="http://VM-TEST2/umc-sso/"/>
  </appSettings>
  <!--
      For a description of web.config changes see http://go.microsoft.com/fwlink/?LinkId=235367.

      The following attributes can be set on the <httpRuntime> tag.
        <system.Web>
          <httpRuntime targetFramework="4.7.2" />
        </system.Web>
    -->
  <system.web>
    <!--  adapt request parameters to support upload of large files -->
    <httpRuntime targetFramework="4.7.2" maxRequestLength="200000" executionTimeout="600"/>
    <compilation targetFramework="4.7.2"/>
    <identity impersonate="false"/>
    <!--  <authentication mode="Windows" /> -->
    <authentication mode="Forms">
      <forms name="MRAuth" slidingExpiration="true" timeout="120" loginUrl="~/Login/Login"/>
    </authentication>
    <authorization>
      <deny users="?"/>
    </authorization>
    <browserCaps userAgentCacheKeyLength="256"/>
  </system.web>
  <location path="api/Authenticate">
    <system.web>
      <authorization>
        <allow users="*"/>
      </authorization>
    </system.web>
  </location>
  <location path="AnalyticTool">
    <system.web>
      <authorization>
        <allow users="*"/>
      </authorization>
    </system.web>
  </location>
  <location path="Errors">
    <system.web>
      <authorization>
        <allow users="?"/>
      </authorization>
    </system.web>
  </location>
  <runtime>
    <assemblyBinding>
      <dependentAssembly>
        <publisherPolicy apply="no"/>
        <assemblyIdentity name="Oracle.ManagedDataAccess" publicKeyToken="89b483f429c47342" culture="neutral"/>
      </dependentAssembly>
    </assemblyBinding>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="combit.ListLabel24" publicKeyToken="a7a30592cb4a94be" culture="neutral"/>
        <bindingRedirect oldVersion="0.0.0.0-26.1.7689.17853" newVersion="26.1.7689.17853"/>
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" culture="neutral"/>
        <bindingRedirect oldVersion="0.0.0.0-12.0.0.0" newVersion="12.0.0.0"/>
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Web.Http" publicKeyToken="31bf3856ad364e35" culture="neutral"/>
        <bindingRedirect oldVersion="0.0.0.0-5.2.7.0" newVersion="5.2.7.0"/>
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Net.Http.Formatting" publicKeyToken="31bf3856ad364e35" culture="neutral"/>
        <bindingRedirect oldVersion="0.0.0.0-5.2.7.0" newVersion="5.2.7.0"/>
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Web.Http.WebHost" publicKeyToken="31bf3856ad364e35" culture="neutral"/>
        <bindingRedirect oldVersion="0.0.0.0-5.2.7.0" newVersion="5.2.7.0"/>
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Web.Cors" publicKeyToken="31bf3856ad364e35" culture="neutral"/>
        <bindingRedirect oldVersion="0.0.0.0-5.2.7.0" newVersion="5.2.7.0"/>
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Web.Helpers" publicKeyToken="31bf3856ad364e35"/>
        <bindingRedirect oldVersion="1.0.0.0-3.0.0.0" newVersion="3.0.0.0"/>
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Web.WebPages" publicKeyToken="31bf3856ad364e35"/>
        <bindingRedirect oldVersion="0.0.0.0-3.0.0.0" newVersion="3.0.0.0"/>
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Web.Mvc" publicKeyToken="31bf3856ad364e35"/>
        <bindingRedirect oldVersion="0.0.0.0-5.2.7.0" newVersion="5.2.7.0"/>
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
```

```
<system.data>
  <DbProviderFactories>
    <remove invariant="Oracle.ManagedDataAccess.Client"/>
    <add name="ODP.NET, Managed Driver" invariant="Oracle.ManagedDataAccess.Client" description="Oracle Data Provider for .NET, Managed Driver"
    type="Oracle.ManagedDataAccess.Client.OracleClientFactory, Oracle.ManagedDataAccess, Culture=neutral, PublicKeyToken=89b483f429c47342"/>
  </DbProviderFactories>
 </system.data>
<oracle.manageddataaccess.client>
   <version number="*"> </version>
 </oracle.manageddataaccess.client>
<system.webServer>
  <modules runAllManagedModulesForAllRequests="true">
    <remove name="WebDAVModule"/>
  </modules>
  <handlers>
    <remove name="WebDAV"/>
    <remove name="ExtensionlessUrlHandler-Integrated-4.0"/>
    <remove name="OPTIONSVerbHandler"/>
    <remove name="TRACEVerbHandler"/>
    <add name="ExtensionlessUrlHandler-Integrated-4.0" path="*." verb="*" type="System.Web.Handlers.TransferRequestHandler"
    preCondition="integratedMode,runtimeVersionv4.0"/>
  </handlers>
  <validation validateIntegratedModeConfiguration="false"/>
 </system.webServer>
</configuration>
<!-- ProjectGuid: D1E4F286-C3B3-4B54-811A-0DC87498E20A -->
```

9. Run **IISRESET** from the command prompt.

> ⚠ If you have applied modifications to elements contained in the release folder, remember that they will not be removed when you uninstall Opcenter Reporting and you will need to remove them manually.

1.4.3 Checking Oracle Installation Requirements (versions previous to 19c)

For details on Oracle installation, please refer to *Oracle official documentation*.

Starting from Opcenter Reporting 3.2 Update1, ODAC 18 is also supported.

When you install and configure Oracle, you must make sure that the following requirements are met:

- During installation, select the **Oracle Data Provider for .NET component** check box.
- In the **ODP.NET** step of the installation, select the **Configure ODP.NET and/or Oracle Providers for ASP.NET at machine-wide level** check box. The machine-wide configuration may cause other applications to stop working. If that is the case, please refer to *Oracle documentation*.
  To overcome this issue, you can execute the following procedure, which is an example on how to install Oracle using a private configuration using version 12.2.010.

Installing Oracle using a Private Configuration

If the machine-wide configuration is not a suitable option, you can install Opcenter Reporting using a private configuration. To do so, perform the following procedure:

1. Install **ODT** with **ODAC 12.2.010**.
2. In the **C:\app\client\Administrator\product\12.2.0\client_1\odp.net\managed\x64** folder, select **configure.bat**.
3. Open the command prompt as Administrator.
4. Type **cd** C:\app\client\Administrator\product\12.2.0\client_1\odp.net\managed\x64
5. Launch the **configure.bat** file.
6. In **C:\app\client\Administrator\product\12.2.0\client_1\odp.net\managed\common** copy the **Oracle.ManagedDataAccess.dll** file.
7. Paste it to **C:\Program Files\Siemens\Opcenter\Intelligence\Report\Server\bin**
8. Modify the **Web.config** file that you can find in **C:\Program Files\Siemens\Opcenter\Intelligence\Report\Server** adding the following nodes:

```
<configuration>
    <configSections>
        <section name="oracle.manageddataaccess.client" type="OracleInternal.Co
mmon.ODPMSectionHandler, Oracle.ManagedDataAccess, Culture=neutral,
PublicKeyToken=89b483f429c47342" />
    </configSections>
    <runtime>
        <assemblyBinding>
            <dependentAssembly>
                <publisherPolicy apply="no" />
                <assemblyIdentity name="Oracle.ManagedDataAccess"
 publicKeyToken="89b483f429c47342" culture="neutral" />
            </dependentAssembly>
        </assemblyBinding>
    </runtime>
    <system.data>
        <DbProviderFactories>
            <remove invariant="Oracle.ManagedDataAccess.Client" />
            <add name="ODP.NET, Managed Driver" invariant="Oracle.ManagedDataAc
cess.Client" description="Oracle Data Provider for .NET, Managed Driver" type="
Oracle.ManagedDataAccess.Client.OracleClientFactory, Oracle.ManagedDataAccess,
Culture=neutral, PublicKeyToken=89b483f429c47342" />
        </DbProviderFactories>
    </system.data>
    <oracle.manageddataaccess.client>
        <version number="*">
        </version>
    </oracle.manageddataaccess.client>
</configuration>
```

The resulting **web.config** file should look as in this example:

9. Run **IISRESET** from the command prompt.

> ⚠ If you have applied modifications to elements contained in the release folder, remember that they will not be removed when you uninstall Opcenter Reporting and you will need to remove them manually.

1.4.4 Configuring IIS and ASP.NET Role Services

Once you have installed Internet Information Services, ASP.NET Module and IIS Roles and Features must be enabled manually.

The actual layout of the configuration panels, the ordering of the options and the specific version of ASP.NET 4.x may vary according to the Operating System, updates and patches installed.

Procedure

1. Select: **Start > Administrative Tools > Server Manager**.
2. Select the **Manage > Add Roles and Features** command.
3. Under **Roles** install the following options.
4. Under **Features** install the following options.

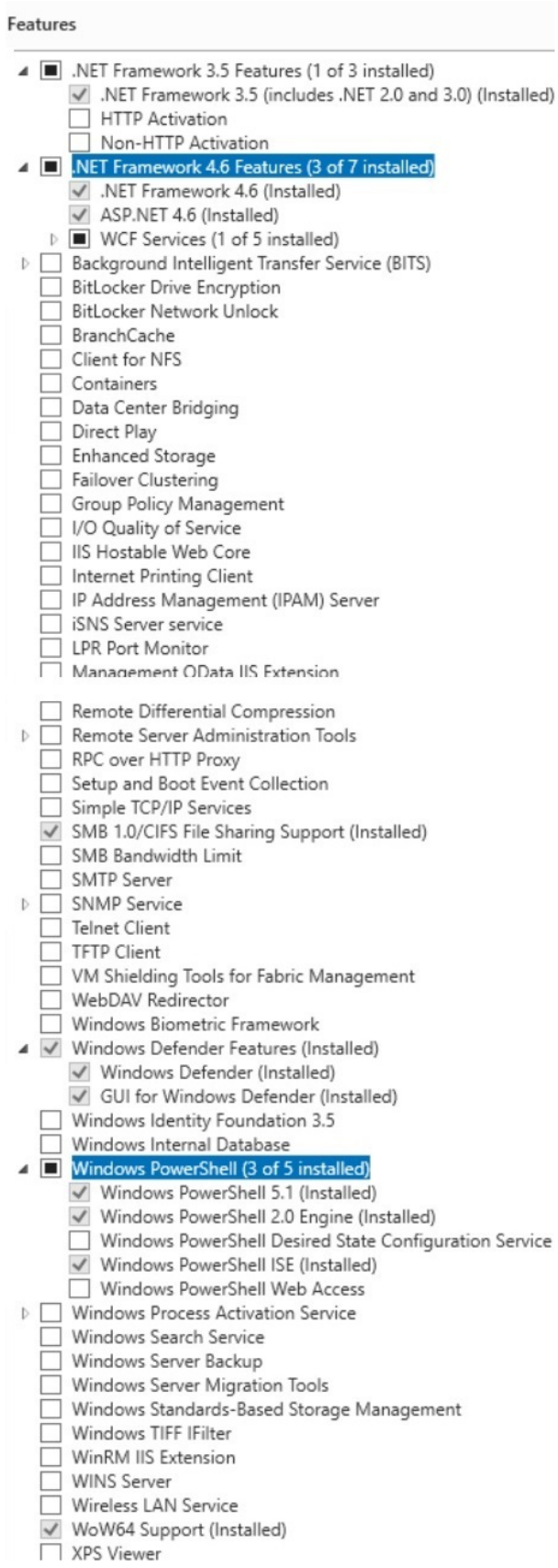
1.4.4.1 Roles

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 screenshots. In this case, select the top node to automatically install all the related sub-features.


Roles
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 (Installe
Digest Authentication (Installed)
IIS Client Certificate Mapping Authentication (Insta
IP and Domain Restrictions (Installed)
URL Authorization (Installed)
Windows Authentication (Installed)
Application Development (8 of 11 installed)
.NET Extensibility 3.5 (Installed)
.NET Extensibility 4.6 (Installed)
Application Initialization (Installed)
ASP
ASP.NET 3.5 (Installed)
ASP.NET 4.6 (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 Essentials Experience
Windows Server Update Services

1.4.4.2 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 screenshots. In this case, select the top node to automatically install all the related sub-features.


Features
.NET Framework 3.5 Features (1 of 3 installed)
.NET Framework 3.5 (includes .NET 2.0 and 3.0) (Installed)
HTTP Activation
Non-HTTP Activation
.NET Framework 4.6 Features (3 of 7 installed)
.NET Framework 4.6 (Installed)
ASP.NET 4.6 (Installed)
WCF Services (1 of 5 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
iSNS Server service
LPR Port Monitor
Management OData IIS Extension
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 (Installed)
SMB Bandwidth Limit
SMTP Server
SNMP Service
Telnet Client
TFTP Client
VM Shielding Tools for Fabric Management
WebDAV Redirector
Windows Biometric Framework
Windows Defender Features (Installed)
Windows Defender (Installed)
GUI for Windows Defender (Installed)
Windows Identity Foundation 3.5
Windows Internal Database
Windows PowerShell (3 of 5 installed)
Windows PowerShell 5.1 (Installed)
Windows PowerShell 2.0 Engine (Installed)
Windows PowerShell Desired State Configuration Service
Windows PowerShell ISE (Installed)
Windows PowerShell Web Access
Windows Process Activation Service
Windows Search Service
Windows Server Backup
Windows Server Migration Tools
Windows Standards-Based Storage Management
Windows TIFF IFilter
WinRM IIS Extension
WINS Server
Wireless LAN Service
WoW64 Support (Installed)
XPS Viewer

2 How to Install Opcenter Reporting

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

Available Operations

- Install Opcenter Reporting Interactively
- Install Opcenter Reporting via Command Line

2.1 Installing Opcenter Reporting Interactively

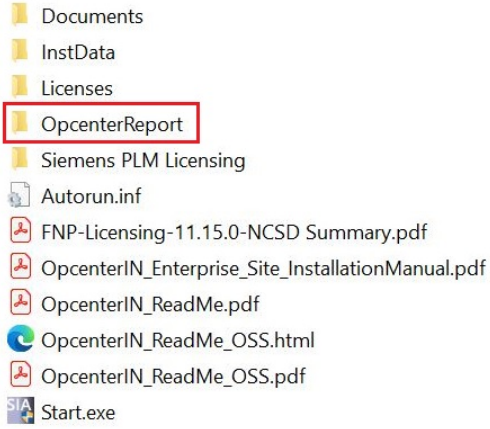
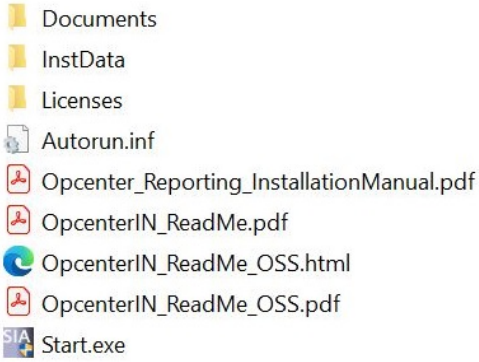
Prerequisites

Verify that all prerequisites required by Opcenter Reporting are satisfied.

Where to find Opcenter Reporting Installation Folder

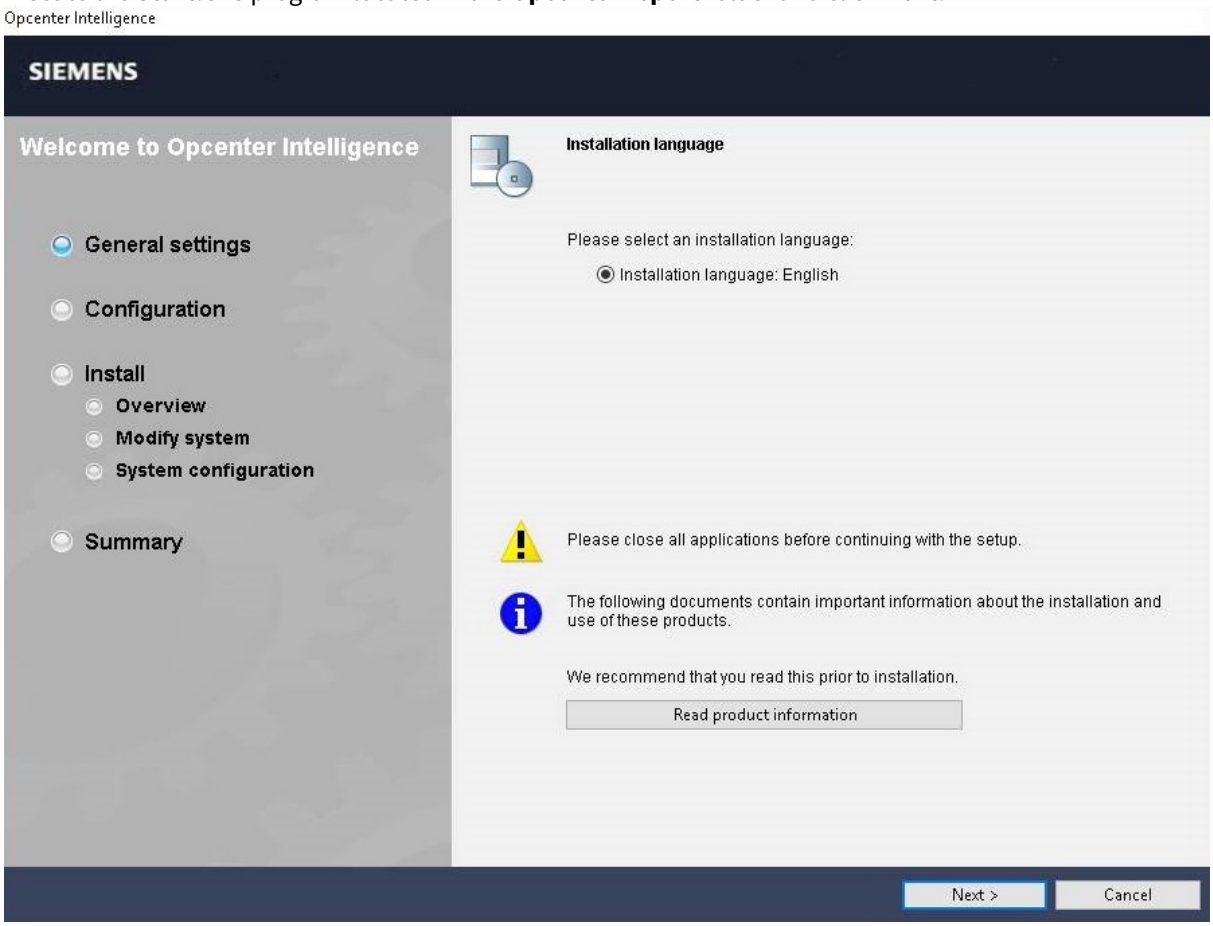
The **OpcenterReport** folder, which contains Opcenter Reporting installation files, is a subfolder of the **Opcenter Intelligence** ISO root folder.

The path of the **Start.exe** file to be launched is: **\OpcenterReport\Start.exe**

Opcenter Intelligence ISO root folder	**Opcenter Reporting installation folder**
	

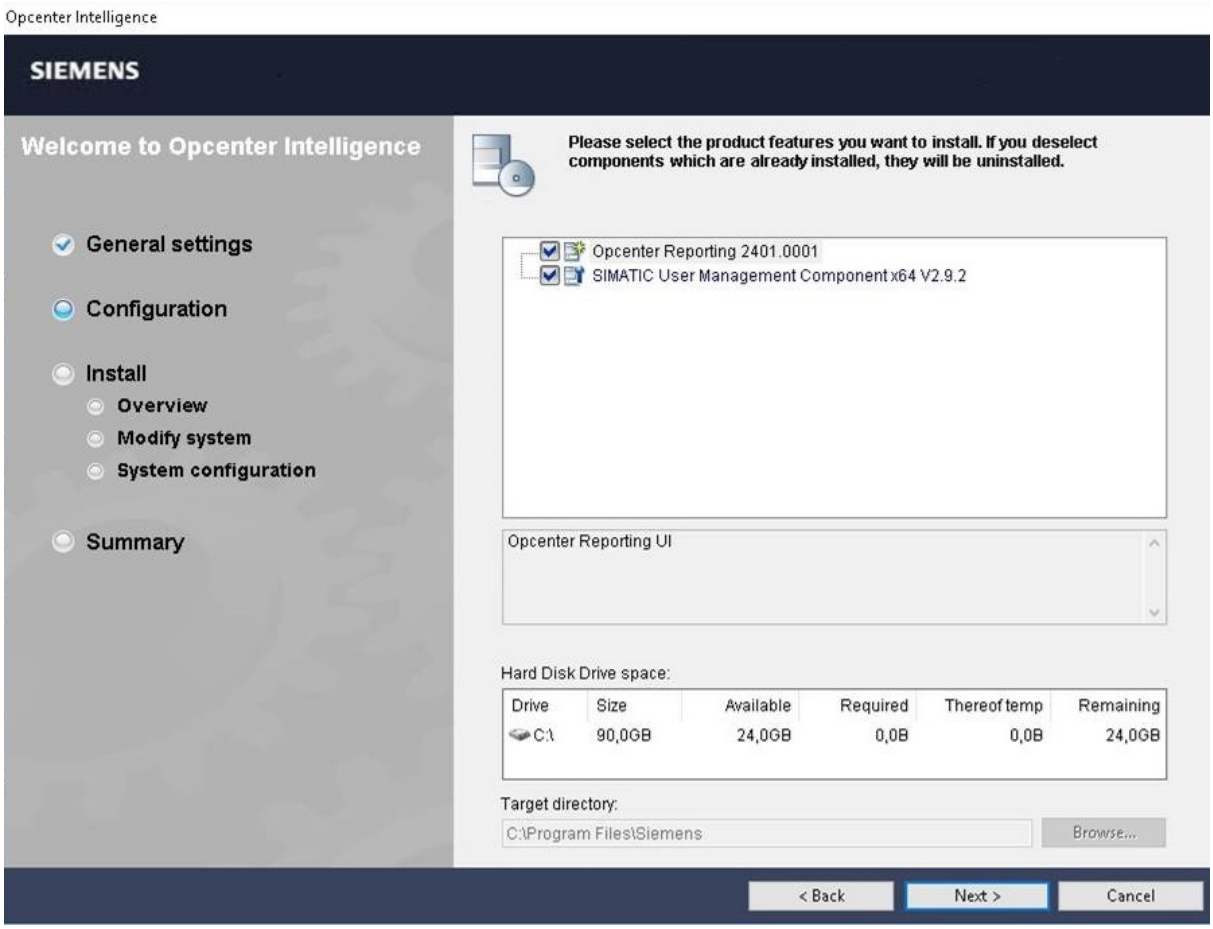
Procedure

1. Execute the **Start.exe** program located in the **OpcenterReport** folder and click **Next**.

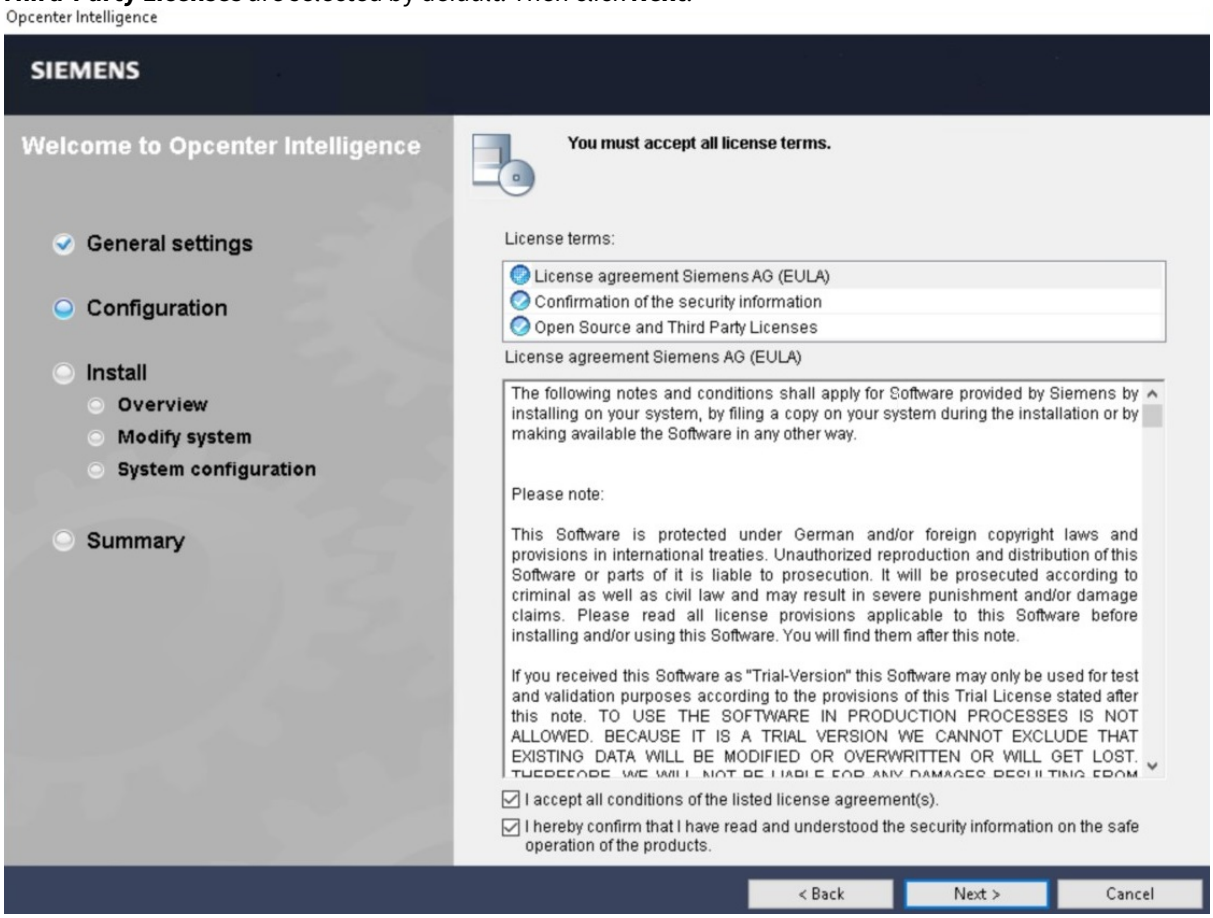


2. Select which product features you want to install and click **Next**.

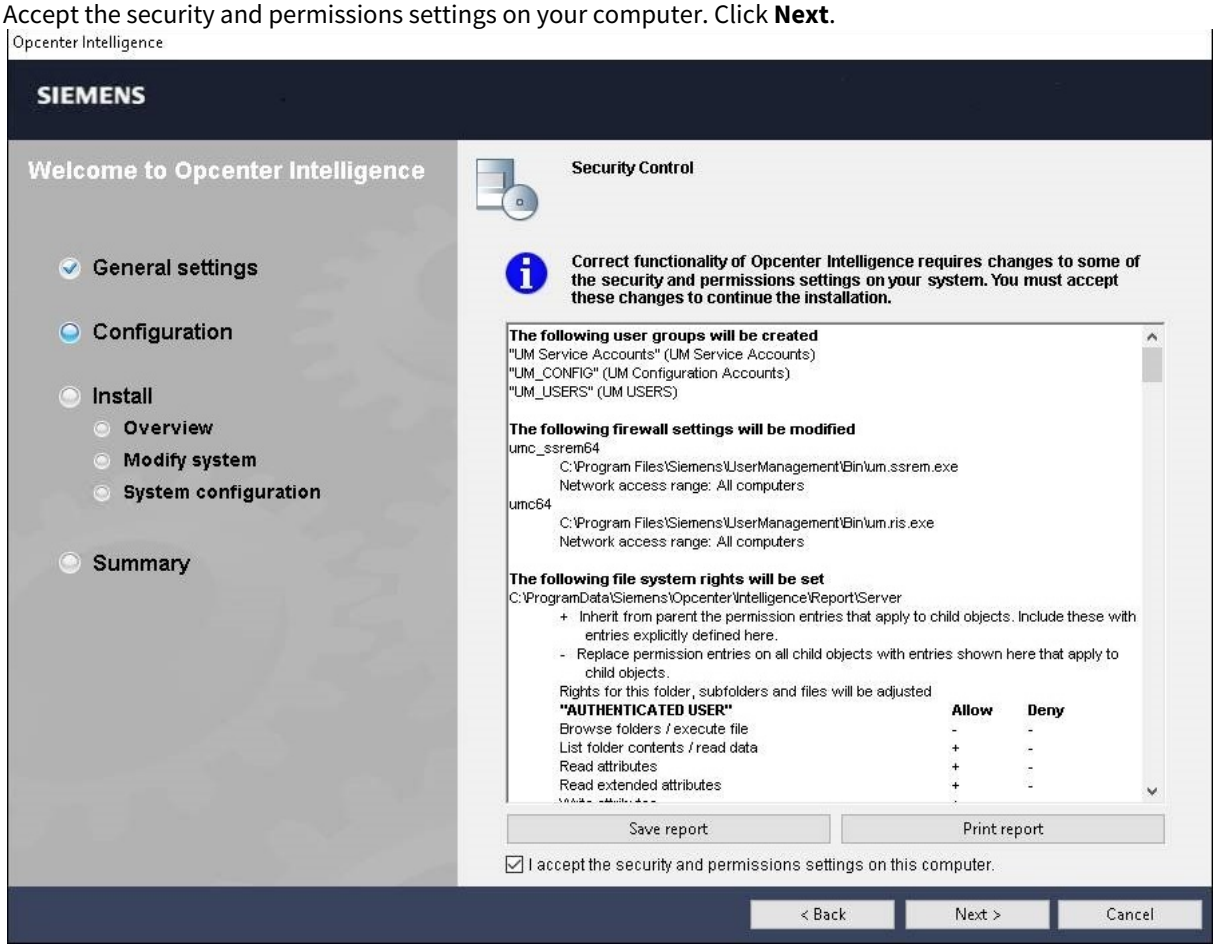
> ⚠ If you are installing Opcenter Reporting on the same machine where User Management Component (UMC) is running, UMC 2.9 SP2 is mandatory. If a previous version of UMC has already been installed on that machine it will be upgraded to version 2.9 SP2.
> Do not deselect the **SIMATIC User Management Component x64 V2.9.2** check box, otherwise the existing UMC will be uninstalled.


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 Reporting 2401.0001
SIMATIC User Management Component x64 V2.9.2
Opcenter Reporting UI
Hard Disk Drive space:
Drive
Size
Available
Required
Thereof temp
Remaining
C:\
90,0GB
24,0GB
0,0B
0,0B
24,0GB
Target directory:
C:\Program Files\Siemens
Browse...
< Back
Next >
Cancel

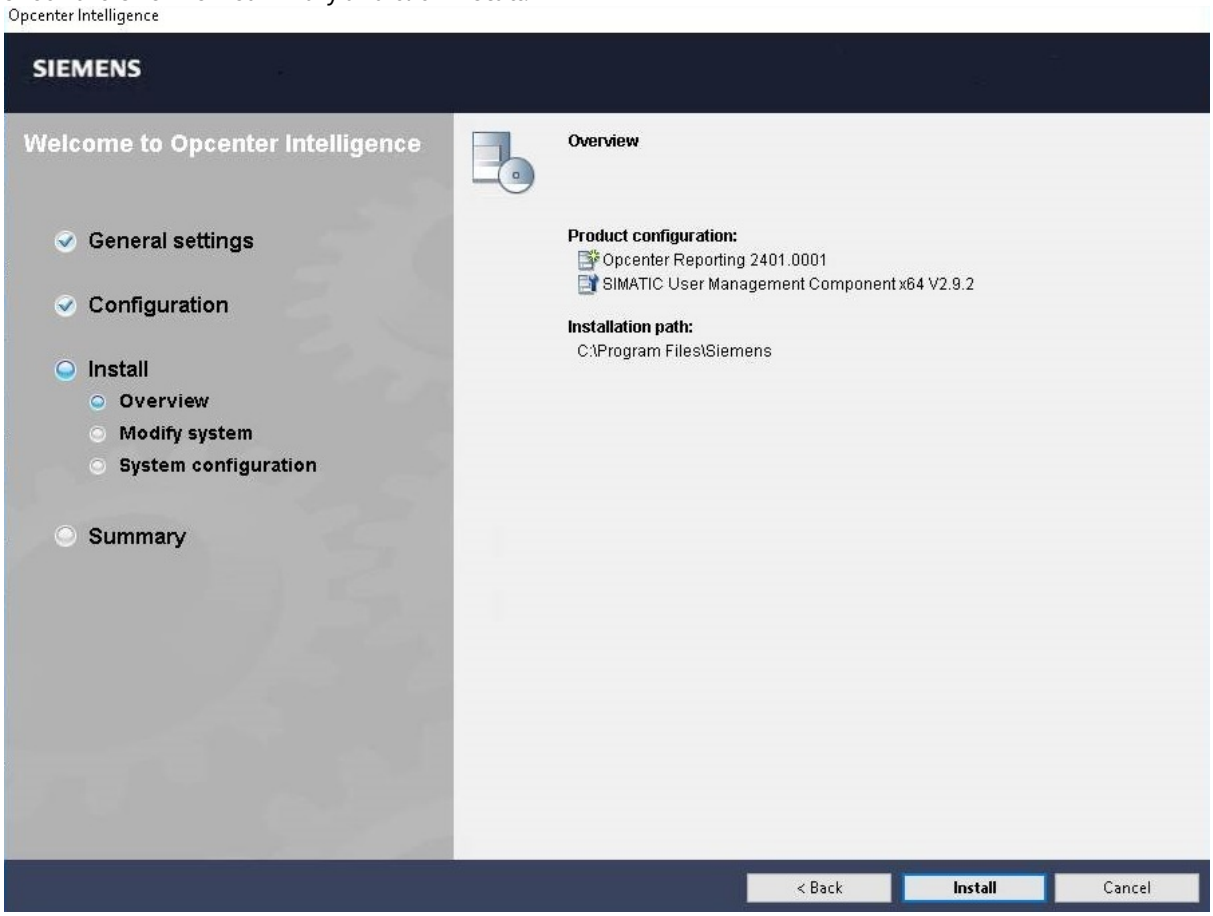
3. Accept the conditions of the license agreement and confirm the security information. **Open Source and Third-Party Licenses** are selected by default. Then click **Next**.



4. Accept the security and permissions settings on your computer. Click **Next**.



5. Check the **Overview** summary and click **Install**.



6. When the setup is completed successfully, click **Finish**.

2.2 Installing Opcenter Reporting via Command Line

Opcenter Reporting 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 for installing Opcenter Reporting 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 Reporting 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

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 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 Reporting

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

To help you set the configuration, at this link you can find a schema of TCP/UDP ports to be opened on Opcenter Reporting server.

Workflow

1. (Optional) Create the UMC user who will be used as Administrator for Opcenter Reporting.
2. Configure Opcenter Reporting Interactively with Opcenter Reporting Configurator
3. Perform Additional Configuration Operations

Additional Configurations

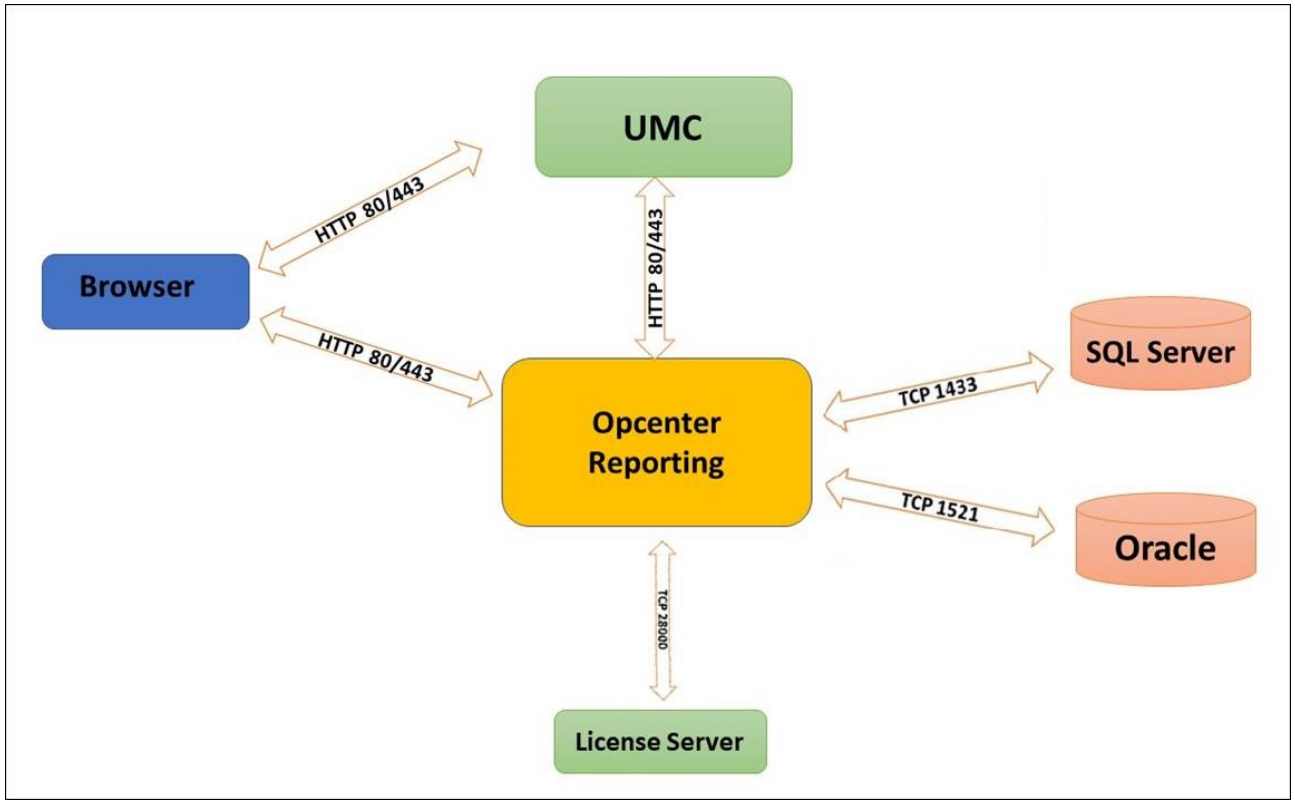
- Configure Opcenter Reporting via Command Line
- Integrate Opcenter Reporting with other products
- Configure Microsoft ARR as Reverse Proxy

Backup Strategy

To prevent data loss if an incident occurs (for example a malware infection or storage device failure), an appropriate backup strategy is highly recommended. Database backup has to be planned to save Opcenter Reporting database, in particular because it stores the reports you have created. A regular backup of the **ProgramData\Siemens\Opcenter\Intelligence\Report\Server\App_Data** folder is therefore strongly recommended.

3.1 Summary of Port Numbers required for Opcenter Reporting Configuration

The following schema summarizes the TCP/UDP ports to be opened on Opcenter Reporting server.



If you want to use non-default configuration, please check vendor documentation. For example, if you are using a named instance in SQL Server, you also need to open the UDP port 1434 for SQL Server Browser Service.

3.2 Creating Opcenter Reporting 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 Reporting installation, you must previously configure UMC (see the *How to Configure UMC* chapter in *UMC Installation Manual*) and then follow this procedure.

Procedure

1. From a supported browser, access UMC by entering one of the following addresses depending on the configuration:
   - http://<*FullComputerName*>/UMC
   - https://<*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 Reporting.

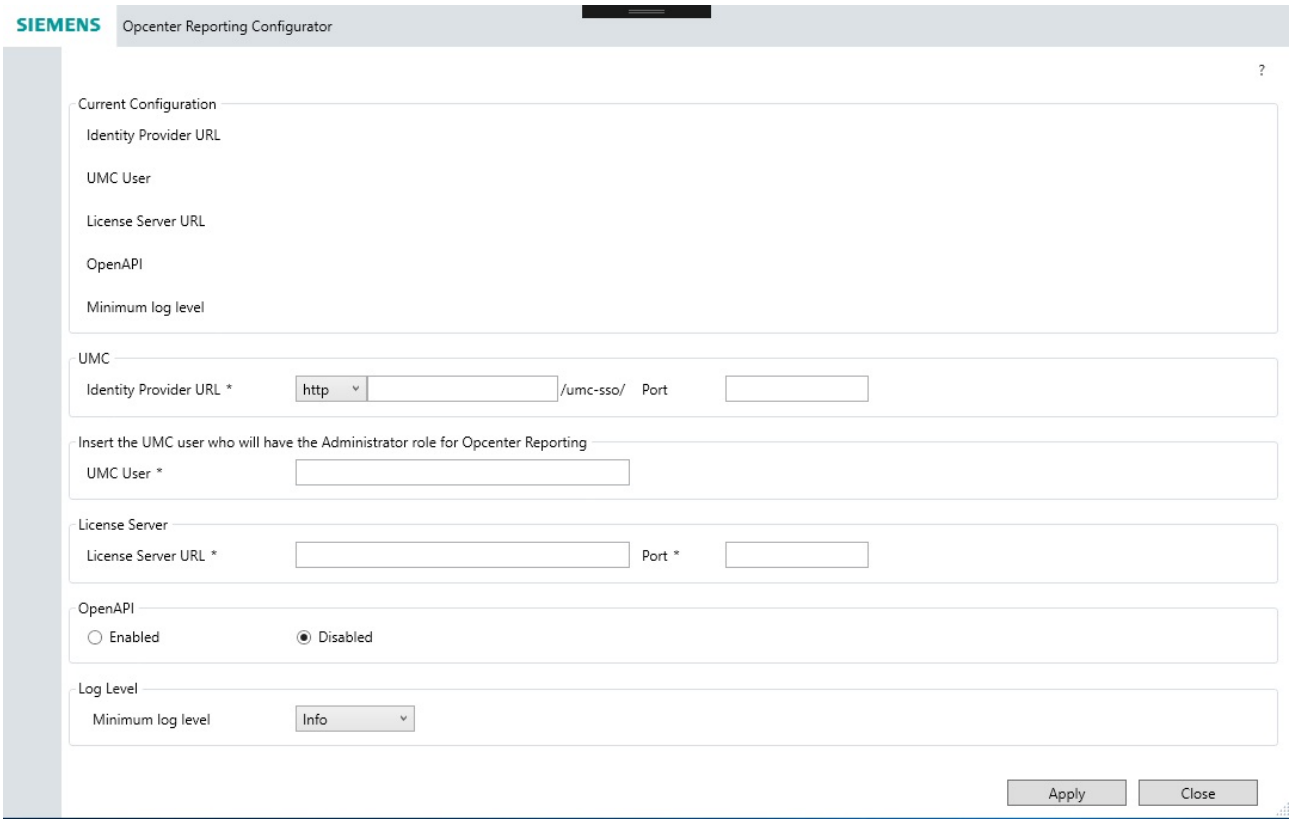
3.3 Configuring Opcenter Reporting Interactively with Opcenter Reporting Configurator

Opcenter Reporting is the stand-alone application that performs the post-setup configuration actions. The Configurator can be run more than once if you want to change your settings after the first configuration.

Procedure

1. Double-click the desktop icon to run the Opcenter Reporting.
2. Insert the required information as explained in the tables below. The fields marked with an asterisk are mandatory.
3. When you have completed the configuration, click **Apply** and wait for the popup that confirms the successful completion of the configuration.
4. Click **Close**.
5. To ensure that UMC functions correctly, add the following URL to UMC whitelist: **http(s)://<machine name>/opcenterrp/Login/Login**. For more details, see *Create a Whitelist Entry* in *UMCONF User Manual*.
6. Restart IIS Application Pool.

> The structure containing the application database and runtime log files is created in **ProgramData\Siemens\Opcenter\Intelligence\Report\Server\App_Data**



Current Configuration

The **Current Configuration** area shows a summary of the settings you have previously applied.

User Management Component (UMC) Configuration

Field	Actions
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.
UMC User	Insert the name of the UMC user who will have the Administrator role for Opcenter Reporting and that you have created in UMC Web User Interface.

License Server Configuration

Field	Actions
License Server URL	Insert the full computer name of the License Server and the **Port** number.

OpenAPI

OpenAPI Specification (formerly Swagger Specification) is an API description format for REST APIs.

Enable or disable **OpenAPI** by selecting the corresponding radio button.

Log Level

The Configurator log file is called **Siemens.OpcenterRP.PostSetup.log** and can be found in **Program Files\Siemens\Opcenter\Intelligence\Report\Setup**

Each log entry has a level and each logger is configured to include or ignore certain levels. In this section you can specify the minimum level where that level and higher levels are included. For example, if the minimum level is Info, then Info, Warning and Error are logged, but Debug and Trace are ignored.

Field	Action
Minimum log level	Select a log level to categorize the information to be included in the log file. The log levels, in descending order, are as follows: • **Error** • **Warning** • **Info** • **Debug** • **Trace**

3.4 Configuring Opcenter Reporting via Command Line

Opcenter Reporting 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 or after an update.

> ⚠ The procedures for configuring Opcenter Reporting 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 Reporting are satisfied.

Procedure

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

```
Siemens.OpcenterRP.WebApi.ReportingServer.PostSetupCLI.exe umcconfiguration
configure -url=<UMCServerURL> administrator configure -umcuser=<umcuser> flex
configure -url=<FlexURL>
```

UMC Configuration

Use the command line to specify the UMC URL.

```
umcconfiguration configure -url=<UMCServerURL>
```

Parameter	Description
UMCServerURL	Type the <*Full computer name*> of the machine where UMC Server is running, including the Port number. **Sample**: https://<*Full computer name*>/umc-sso/

Opcenter Reporting Administrator Configuration

```
administrator configure -umcuser=<umcuser>
```

Parameter	Description
umcuser	Insert the <*umc user*> who is going to be the Opcenter Reporting Administrator. This is the user who will be able to grant access to other users.

License Server Configuration

```
flex configure –url=<FlexURL>
```

Parameter	Description
FlexURL	Insert the computer name of the Flex Server and the Port number. FlexURL: port@<*Full computer name*> **Sample**: 28000@ReportingMachine.Domain.TST

Sample

```
Siemens.OpcenterRP.WebApi.ReportingServer.PostSetupCLI.exe umcconfiguration configure
–url=https://mireporting.swqa.tst/umc-sso/ administrator configure
–umcuser=ConfiguredUser flex configure –url=28000@mireporting.swqa.tst
```

Error Codes

The following error codes may be returned:

Error	Code
GENERIC_ERROR	-1
CMD_SUCCESS	0
CMD_LINE_WRONG_INPUT	1
CMD_NO_ADMIN	2
FAIL_DB_CREATION	100
FAIL_DB_UPDATE	101

Error	Code
FAIL_WEBCONFIG_UPDATE	200
FAIL_INITIALIZATION_ENGINE	1000

Log File

A log file named **Siemens.OpcenterRP.PostSetup.log** is available in **C:\Program Files\Siemens\Opcenter\Intelligence\Report\Setup**

3.5 Performing Additional Configuration Operations

Perform the following operations to complete the configuration of Opcenter Reporting:

- (Optional) Configure IIS Application Pool
- (Optional) Configure https Protocol
- Check Authentication Keys in IIS

Configuring IIS Application Pool to use Windows Authentication

Opcenter Reporting setup installs a default application and an IIS application pool named **opcenterrpPool**. The user must be granted read access to SQL Server in order to use Windows Authentication to access the DB. To do so, click on **Application Pool Identity** and insert a domain service user that can run also in remote SQL Server machine.

Configuring https Protocol for Opcenter Reporting

To configure the https protocol for **opcenterrp** (application contained in IIS Default Web Site), refer to *Microsoft Internet Information Services (IIS) documentation* for instructions on how to configure a certificate on the web site.

Checking Authentication Keys in IIS

In IIS, follow this procedure to verify if authentication keys have been set correctly.

1. In **IIS Manager > Sites > Default Web Site**, select **opcenterrp**.
2. Double-click **Authentication** from the area on the right.
3. Check that only the two following keys have been set to **Enabled**. The other keys must be set to **Disabled**.
    - **Anonymous Authentication**
    - **Forms Authentication**
4. Run **IISRESET** from the command prompt.

3.6 How to Configure Microsoft ARR as Reverse Proxy

These guidelines deal with Microsoft Application Request Routing (ARR) used as a reverse proxy. This application has been officially tested: however we are not aware of any problems in using other reverse proxy/load balancing applications, provided that they support the WebSocket protocol.

- The configuration of Microsoft ARR used as Reverse Proxy is supported starting from Opcenter Reporting version 3.3 Update1.

- Opcenter Reporting does not support the load balancer configuration mode on more than one node. To maintain uniformity with the configurations suggested by other products (for example Opcenter Execution Foundation) these pages describe how to configure ARR as load balancer on one node.

ARR exposes a unique URL that web clients use for sending and receiving requests and redirects these requests to Opcenter Reporting and UMC hosts. Consequently web clients only need to know the ARR server to which they must connect.

These pages describe the procedures to be followed to create a basic configuration of load balancing using Microsoft Application Request Routing (ARR) when Opcenter Reporting is running in a DMZ network.
If you want to configure ARR in HTTPS, you must first configure Opcenter Reporting and UMC in HTTPS and then follow the procedures to configure ARR described in these pages.

User Management Component Limitation

To properly configure the reverse proxy to use multiple web servers, you must increase the value of the query string length on all web servers via IIS Manager. For more information, see *High Availability/Reliability General Issues* in *UMC Installation Manual*.

Prerequisites

- The host containing ARR is a separate host that must not contain Opcenter Reporting.
- Microsoft ARR add-on is installed on IIS.
- You have applied the basic endpoint configuration, which is the default in Opcenter Reporting.
- If you do not configure ARR in High Availability, the host containing ARR must never be shut down.
- If you want to use ARR and the entire environment using HTTPS:
  - you must have modified the ARR default site binding and assigned a valid certificate as documented on *Microsoft documentation*;
  - you must have configured Opcenter Reporting in HTTPS.

Workflow

ⓘ These steps must be executed before you start using web clients.

1. Create the web farms
2. Configure the redirection rules
3. Configure the redirection rule order
4. Increase the default proxy timeout
5. Configure the maximum allowed content length for file processing
6. Set the recycle time to zero
7. Configure the connection from web clients

3.6.1 Creating the Web Farms

In this step of the ARR Load Balancer configuration, you are creating the web farms and assigning the servers of the Opcenter Reporting environment.

Procedure

1. In **IIS Manager**, under **Server Farms**, create the following web farm for Opcenter Reporting:

Field	Value
Server Farm Name	REPORTING_SVC
Status	online
Server address	RP SERVER IP or FQDN

2. If the UMC web farm has not already been created and configured in another product (for example Opcenter EX FN), create it and insert the following values:

Field	Value
Server Farm Name	UMC_SVC
Status	online
Server address	UMC IP or FQDN

3. Click **Finish**.
4. Click **No** to the **Rewrite Rules** request that appears.

3.6.2 Configuring the Redirection Rules

In this step of the ARR Load Balancer configuration, you are configuring the rules to redirect the incoming requests to the required farm.

Procedure

Leave the default settings for all the parameters that are not mentioned in the tables below.

1. In **IIS Manager**, select the root node.
2. Double-click the **URL Rewrite** option.
3. In the **Actions** panel, click **Add Rule(s)...**
4. Select the **Blank rule** template and click **OK**.
5. Create a rule by entering the parameters shown in the following table.

Section	Parameter	Value
	Name	ARR_REPORTING_SVC
Match URL	**Requested URL**	Matches the Pattern
	Using	Regular Expression

Section	Parameter	Value
	Pattern	.*
	Ignore case	checked
Conditions	**Logical Grouping**	Match any
	Condition input	{R:0}
	Check if input string:	Matches the Pattern
	Pattern	^opcenterrp
Action	**Action Type**	Route to Server Farm
	Action Properties	URL: https://reporting_svc/{R:0}
	Append query string	checked
	Stop processing of subsequent rules	checked

6. Click **Apply**.
7. Click **Back to Rules**.
8. Repeat steps 2 to 5 to create the second rule for UMC if it has not been already created and configured for another product.

> ⚠ If you need to set the Opcenter Reporting host name, you can add **Server Variables** in the corresponding section.

Section	Parameter	Value
	Name	ARR_UMC_SVC
Match URL	**Requested URL**	Matches the Pattern
	Using	Regular Expression
	Pattern	.*
	Ignore case	checked

Section	Parameter	Value
Conditions	**Logical Groupings**	Match Any
	Condition input	{R:0}
	Check if input string:	Matches the Pattern
	Pattern	^UMC ^umc-idp ^umc-sso
Action	**Action Type**	Route to Server Farm
	Action Properties	**Scheme**: *http://* or *https://*
		Server Farm: UMC_SVC
		Path: /{R:0}
	Stop processing of subsequent rules	checked

9. Click **Apply** and **Back to Rules**.

3.6.3 Configuring the Redirection Rule Order

In this step of the ARR Load Balancer configuration, you are configuring the execution order of redirection rules.

Procedure

1. In the **URL Rewrite** configuration environment, set the correct order for the rules, which must be:
   - **REPORTING_SVC**
   - **UMC_SVC**
2. To change the order, select a rule and in the **Actions** panel use the **Move Up** or **Move Down** commands.

3.6.4 Increasing the Default Proxy Timeout

In this step of the ARR Load Balancer configuration, you must increase the default proxy timeout for all web farms.

Procedure

1. Select a web farm.
2. In the **Server Farm** pane, click **Proxy**.
3. In the **Timeout** (in seconds) edit box, type 10000 (instead of 30).
4. Select the **Reverse rewrite host in response headers** check box.

5. Click **Apply**.
6. Repeat steps 1 to 5 for each web farm.

3.6.5 Configuring the Maximum Content Length Allowed for File Processing

In this step the ARR Load Balancer configuration, you must increase the default value for the maximum content length allowed to allow the processing of data files with a large amount of data. By default, the limit is set to 30 MB and you can manually modify it as follows:

Procedure

1. In the **Machine Name** pane, click **Request Filtering**.
2. Click the **Edit Feature** settings action link.
3. Set the value of the **Maximum allowed content length (bytes)** edit box according to your requirements (we suggest a value greater than 200 MB).
4. Click **OK** to apply the configuration.

3.6.6 Setting the Recycle Time to Zero

The recycle time of the Application Pool is set by default to 1740 minutes. When the Application Pool is recycled, all active connections (including client-side websockets) are automatically closed. Since the Signal Manager sends information via websocket connections, which are automatically closed after recycling and not reopened, the recycle option may cause data loss.

To solve this problem, you must set the recycle time to zero as follows:

Procedure

1. In the **Connections** pane, select the **Application Pools** node and select the default application pool.
2. In the **Actions** pane, click **Recycling**.
3. Set the **Regular time interval (minutes)** parameter to zero, complete the wizard and save changes.
4. Restart IIS.

3.6.7 Configuring the Connection from Web Clients

To correctly connect from the web clients to Opcenter Reporting hosts using the ARR reverse proxy, some web browser versions need to use an FQDN name (i.e. they must contain a dot character in the URL) to make the client affinity work properly. As a best practice we suggest that you use a DNS record for the ARR host that should be visible from all web clients.

4 How to Integrate Opcenter Reporting with other Products

If you need to embed reports in your application, you can authenticate and perform some operations in Opcenter Reporting by applying the code provided in the following chapters.

The authentication required before the embedding operations can be done using the User Management Component (UMC) or not.

- Products not supporting UMC
- Products supporting UMC

Additional Options

Execute a Report and Save it as PDF without User Interaction

4.1 How to Integrate Opcenter Reporting with Products not supporting UMC

In this scenario Opcenter Reporting trusts users of the application you want to integrate. The permissions required to authorize users remain unchanged.
The following workflow needs to be executed each time you want to access the Opcenter Reporting application by means of a one-time authorization code to be obtained after the generation of private and public RSA keys.

Workflow

1. Generate Public and Private RSA Keys
2. Get the One-Time Authorization Code to perform the following operations:
    - Get Reports from Opcenter Reporting
    - Embed Reports
    - Provide Values for Report Parameters
    - Release a Seat after Report Visualization

4.1.1 Generating Public and Private RSA Keys

The first step to integrate Opcenter Reporting with other products is to generate public and private RSA keys.

The private key will need to be moved to the external system, while the public key will be moved to the Opcenter Reporting machine. As a result, the external user will be able to authenticate into Opcenter Reporting.

> After the generation of these keys, strict measures should be taken to guarantee that they are securely stored and moved between different customer machines.

Procedure

1. Run the **Digital Signature Generator** Console Application (**Siemens.OpcenterRP.DigitalSignatureGenerator.exe**) contained in the folder: **Program Files\Siemens\Opcenter\Intelligence\Report\Setup**
2. To generate a public and a private key, follow the instructions prompted by the application and provide the following details:

Field	Description	Naming Convention
Realm	Name to be used in order to distinguish different systems in case you want to access Opcenter Reporting from more than one system using different keys, for example: *ACME*.	• Minimum length: 3 characters • Maximum length: 15 characters • Available characters: letters (uppercase, lowercase, numbers and underscore)
Scenario	A subgroup of the realm, for example: *test, production, etc.*	• Minimum length: 3 characters • Maximum length: 15 characters • Available characters: letters (uppercase, lowercase, numbers and underscore)

3. The keys are generated in the following folder: **ProgramData\Siemens\Opcenter\Intelligence\Report\DigitalSignatureGenerator**. The keys format will be: **Realm-Scenario-*Public/Private*-Key-Timestamp.xml** where the **Timestamp** field is a record of the time of key generation, for example: *20190905-132018907*.
4. Move the private key to the system you want to integrate with Opcenter Reporting.
5. Move the public key to the following folder: **ProgramData\Siemens\Opcenter\Intelligence\Report\Server\App_Data\PKRepository**

4.1.2 Getting the One-Time Authorization Code

A one-time authorization code (OTC) is a code that is valid to authenticate the user identity for only one session. For example, a web application can use an OTC to securely authenticate in Opcenter Reporting.

⚠ The purpose of the OTC is to create a session cookie. If you are using APIs and a session cookie already exists, the system will not accept the new OTC (i.e. the resulting request for a new session) and will return the error: "HTTP Code 401". If a valid session is present, you can call the API without the **otc** parameter.

ⓘ Please make sure to copy the code correctly and check it carefully before running it (the text may be broken across two different pages of the .pdf manual).

The following "usings" are required for the next code block:

```
using Newtonsoft.Json;
using System;
using System.Collections.Generic;
using System.Net.Http;
using System.Net.Http.Headers;
using System.Text;
using System.Threading.Tasks;
```

The following method is an example to get the one-time code:

```
private async Task<string> getOneTimeCode()
{
    //this user should be a trusted user in the reporting api
    //get username and groups
    string userName = "trusted_user";

    //Used public key REALM1-SCENARIO1-PrivateKey-20190912-121150201.xml
    //Used public key <realm>-<scenario>-PrivateKey-20190912-121150201.xml
    String realm = "REALM1";
    String scenario = "SCENARIO1";
    List<String> groups = new List<string>();

    //get Signature
    UserAndSignature signature = Helpers.GetSign(userName, groups, realm, scenario);
    //call Authenticate Method
    HttpClient client = new HttpClient();
    client.BaseAddress = new Uri("https://full_computer_name/opcenterrp/");
    client.DefaultRequestHeaders.Accept.Clear();
    client.DefaultRequestHeaders.Accept.Add(new MediaTypeWithQualityHeaderValue("appl
ication/json"));
    HttpContent contentPost = new
 StringContent(JsonConvert.SerializeObject(signature), Encoding.UTF8, "application/
json");
    HttpResponseMessage response = await client.PostAsync("api/Authenticate",
contentPost);
    response.EnsureSuccessStatusCode();
    var otc = await response.Content.ReadAsStringAsync();
    return otc.Trim('"');
}

public class UserAndSignature
{
    public string UserName { get; set; }
    public string CreationTime { get; set; }
    public List<string> Groups { get; set; }
    public string Realm { get; set; }
    public string Scenario { get; set; }
    public string Signature { get; set; }
}
```

Helper Methods

The following "usings" are required for the next code block:

```
using System;
using System.Collections.Generic;
using System.Globalization;
using System.Security.Cryptography;
using System.Text;
using WebApi.Models; //namespace of the UserAndSignature class
```

The following methods are used by the one-time code:

```
static class Helpers
{
    public static UserAndSignature GetSign(String userId, List<string> groups, string
 realm, string scenario)
    {
        //Get UtcDate
        string creationDate = DateTime.UtcNow.ToString("yyyy-MM-ddTHH:mm:ssZ",
CultureInfo.InvariantCulture);
        //Get Private key (filename <Realm>-<Scenario>-PrivateKey-<Date><Time>.xml)
        string privateKey = System.IO.File.ReadAllText(@"REALM1-SCENARIO1-
PrivateKey-20190913-081726276.xml");
        //Create String To Sign <UserId><Group1,Group2,...><UTCDateTime>
        string strToSign = String.Format(
            "{0}|{1}|{2}|{3}|{4}",
            userId,
            String.Join(",", groups),
            creationDate,
            realm,
            scenario);
        //Get Signature from String
        string signature = Sign(strToSign, privateKey);
        UserAndSignature userToAuthenticate =
            new UserAndSignature
            {
                UserName = userId,
                Groups = groups,
                CreationTime = creationDate,
                Realm = realm,
                Scenario = scenario,
                Signature = signature
            };
        return userToAuthenticate;
    }

    //Signature of String SHA512 FIPS Compatible
    private static string Sign(string StringToSign, string PrivateKey)
    {
        using (RSACryptoServiceProvider rsaProvider = new RSACryptoServiceProvider())
        {
            rsaProvider.FromXmlString(PrivateKey);
            using (SHA512CryptoServiceProvider hashProvider = new
 SHA512CryptoServiceProvider())
            {
```

```
                UnicodeEncoding unicodeEncoding = new UnicodeEncoding();
                byte[] SignedHashValue = rsaProvider.SignHash(
                    hashProvider.ComputeHash(unicodeEncoding.GetBytes(StringToSign)),
                    "System.Security.Cryptography.SHA512CryptoServiceProvider");
                return System.Convert.ToBase64String(SignedHashValue);
            }
        }
    }
}
```

4.1.3 Getting Reports from Opcenter Reporting

The following example shows how to retrieve a report list through a call to the Opcenter Reporting Web API using the one-time code.

Prerequisites

You have obtained a one-time authorization code.

GetJsonReportList Method

> ⚠ Please make sure to copy the code correctly and check it carefully before running it (the text may be broken across two different pages of the .pdf manual).

The following "usings" are required for the next code block:

```
using System;
using System.Net.Http;
using System.Net.Http.Headers;
using System.Threading.Tasks;
```

This method is an example of how to use the OneTimeCode to call the Web API. In this particular example, the method returns the list of reports.

```
private async Task<string> GetJsonReportList()
{
    var otc = await this.getOneTimeCode();

    HttpClient client = new HttpClient();
    client.BaseAddress = new Uri("https://full_computer_name/opcenterrp/");
    client.DefaultRequestHeaders.Accept.Clear();
    client.DefaultRequestHeaders.Accept.Add(new MediaTypeWithQualityHeaderValue("appl
ication/json"));
    String url = String.Format("api/RepositoryItems?otc={0}&parentItemId={1}", otc,
Guid.Empty.ToString());
    return await client.GetStringAsync(url);
}
```

Example of Return Values

```
[{
        "ItemId": "a235c809-d95f-44b4-b14d-422990e4ec98",
        "cbID": "",
        "ItemName": "Folder1",
        "ItemType": 1,
        "ParentItemId": "00000000-0000-0000-0000-000000000000",
        "DataSourceId": "00000000-0000-0000-0000-000000000000",
        "DataSourceName": "n/a",
        "Description": "",
        "IsEmpty": true,
        "IsValid": false
    },
{
        "ItemId": "a16ecf03-b774-456c-9996-04e660b3118c",
        "cbID": "repository://{E43EA856-C0C7-4E3F-9EAD-99B001758DE4}",
        "ItemName": "Equipment",
        "ItemType": 0,
        "ParentItemId": "00000000-0000-0000-0000-000000000000",
        "DataSourceId": "d9e5bca5-8b54-4773-84ae-dbc0421f7be3",
        "DataSourceName": "LMS_MDW",
        "Description": "",
        "IsEmpty": false,
        "IsValid": true
    }]
```


- the **cbID** parameter is returned in the form required by the viewer repository: //{E43EA856-C0C7-4E3F-9EAD-99B001758DE4}
- the **ItemType** parameter can assume two different values: **0** for a report, **1** for a folder.

4.1.4 Embedding Reports

Prerequisites

You have obtained a one-time authorization code.

Procedure

The following code can be used as an example to embed in a page of your application the reports in ASP.NET MVC created in Opcenter Reporting.

Please make sure to copy the code correctly and check it carefully before running it (the text may be broken across two different pages of the .pdf manual).

ASP.NET MVC

You must insert this **iframe** tag in the View where you want to display the report:

```
/*
Cshtml Code:
```

```
*/
<iframe style="width: calc(100%); height: calc(100% - 0px)" src="@ViewBag.IframeUrl">
</iframe>
```

This method sets the URL of the frame specified in the **src** attributes of the above tag.

```
public async Task<ActionResult> Report(String id)
{
 var otc = await this.getOneTimeCode();

 string formatParameters =
     "{2}Reports/HTML5Viewer?otc={0}&reportRepositoryID=repository://{{{1}}}";

 ViewBag.IframeUrl =
     String.Format(
         formatParameters,
         otc.ToUpper(),
         id,
         "https://full_computer_name/opcenterrp/");
 return View();
}
```

AngularJS + ASP.NET Web API

This method returns the URL required by the **src** attribute of the <**iframe**> tag.

```
[HttpGet]
[ActionName("viewReport")]
public async Task<string> ViewReport(String id)
{
    //id refers to the cbID of the ReportDto class
    var otc = await this.getOneTimeCode();
    var url =
    String.Format("{2}Reports/HTML5Viewer?otc={0}&reportRepositoryID={1}",
        otc.ToUpper(), id, "https://mireporting.swqa.tst/opcenterrp/");
    return url;
}
```

The URL is retrieved by the HTTP method, for example:

```
function GetById(id) {

    return $http.get(
        'http://full_computer_name/WebApi/api/Reporting/viewReport?id=' + id)
        .then(
        function (res)
        {
            return res.data;
        },
        handleError('Error getting report by id'));
}
```

Once the URL has been returned, it must be processed as follows in order to make it work in the **iframe** and generate a contextual reload:

```
ReportService.GetById(vm.reportCbId)
                    .then(function (reportUri) {
                        $scope.reportUri = $sce.trustAsResourceUrl(reportUri);
                    });
```

where **$sce** must be injected into the controller:

```
ReporViewerController.$inject = ['ReportService', '$rootScope', '$routeParams',
'$scope', '$sce'];    function ReporViewerController(ReportService, $rootScope,
$routeParams, $scope, $sce) {
```

The HTML code of the **iframe**, must be as follows in the view:

```
<iframe id="reportFrame" style="width: 1000px; height: 800px" src="{{reportUri}}" ></
iframe>
```

reportUri must have been defined in the **$scope**.

4.1.5 Providing Values for Report Parameters

In Opcenter Reporting you can create reports with specific parameters and open these reports from a hosting application by providing the values to be used for such parameters.

Prerequisites

- You have obtained a one-time authorization code.
- You have created and saved a report in Combit® List & Label Designer and configured the following settings:

Settings	Values
Visibility	**False**

Settings	Values
Available Values	If the parameter is single value, select: **Manual Input** If the parameter is multivalued, select: **From Predefined Values**
Default	If you have selected **From Predefined** Values, select **Values**
Value(s)	If you have selected **From Predefined** Values, type **[ ]**
Support Multi Selection	If you have selected **From Predefined Values**, select **Yes**
Available Values Type	This value must be consistent with the allowed filter data type and type.

Procedure

Call the following URL to which you have previously added the required parameters:

https://[FQDN]/opcenterrp/Reports/HTML5Viewer?otc=[*OTCCODE*]&reportRepositoryID=repository://{[*cbID*]}
&reportParams=[*URLencoded keypair value separated by &*]

Parameters	Description
otc	One-time code retrieved by **getOneTimeCode**()
reportRepositoryID	The **Cbid** of the report in the format: repository://{cbID}
reportParams	URLencoded keypair value separated by **&**. The allowed parameter types are: • **string** • **date**: JSON format ISO 8601 • **bool**: true or false • **numeric**: using decimal point as separator • **array**: separated by **;**

Example

1. Create a report that contains the parameters:
   - **@EmployeeID**
   - **@City**
   - **@BirthDate**

2. In the List & Label Designer, set the visibility of these parameters to **False**.
3. Encode the **reportParams** parameter as in this example. The **reportParams** string must be encoded before calling the controller action.

```
var reportParams =
"@EmployeeID=0&@City=Seattle&@BirthDate=1958-09-01T00:00:00Z";
var encodedParams = encodeURIComponent(reportParams);
```

4. Call the URL of the API:
https://FQDN/opcenterrp/Reports/HTML5Viewer?otc=5FD97E21-CCF5-4A04-8A6E-E7D6ECCE6883&reportRepositoryID=repository://{D65A3C2E-A166-40CB-B503-42B9177496DF}&reportParams=%40EmployeeID%3d0%26%40City%3dSeattle%26%40BirthDate%3d1958-09-01T00%3a00%3a00Z

> - The last string of the URL corresponds to: @EmployeeID=0&@City=Seattle&@BirthDate=1958-09-01T00:00:00Z
> - If the report parameter has been set as multivalued in the report, you can set the parameter values separated by **;** (e.g. @City=Seattle;London)

4.1.6 Releasing a Seat after Report Visualization

The following example shows how to release a seat for a specific user before the session expiration time (120 minutes) through a call to the Opcenter Reporting Web API using the one-time code.

Prerequisites

You have obtained a one-time authorization code.

logoutFromReporting Method

> Please make sure to copy the code correctly and check it carefully before running it (the text may be broken across two different pages of the .pdf manual).

The following "usings" are required for the next code block:

```
using System;
using System.Net.Http;
using System.Net.Http.Headers;
using System.Threading.Tasks;
```

This method is an example of how to use the OneTimeCode to call the Web API. In this particular example, the method releases the seats for one or all the browsers listed in the enum for a specific user (All = 4 releases all the seats for all browsers for a specific user).

```
public enum BrowserEnum
 {
 IE = 0,
 Edge = 1,
 Chrome = 2,
 Firefox = 3,
```

```
 All = 4
}

private async Task logoutFromReporting(String otc, BrowserEnum browser)
        {
            try
            {

                HttpClient client = new HttpClient();
                client.BaseAddress = new Uri("https://full_computer_name/opcenterrp/")
;
                client.DefaultRequestHeaders.Accept.Clear();
                client.DefaultRequestHeaders.Accept.Add(
                    new MediaTypeWithQualityHeaderValue("application/json")
                );

                String url = String.Format("api/ReleaseSeat?otc={1}&BrowserId={0}",
browser, otc);
                HttpResponseMessage response = await client.GetAsync(url);

                response.EnsureSuccessStatusCode();

            }
            catch (Exception ex)
            {
                //log error
            }

        }
```

4.2 How to Integrate Opcenter Reporting with Products supporting UMC

A product that uses the User Management Component (UMC) as identity provider can directly invoke the Opcenter Reporting Web API without the need to obtain a one-time authorization code, but only by authenticating on Opcenter Reporting. This can be an alternative for the UMC application to embed Opcenter Reporting without the need to create and distribute the **opcenterrp** certificate.

Authentication

After the authentication in UMC you have to load the Opcenter Reporting URL, which must be on the same domain, within an **iframe** not visible to the user.

Example

```
<iframe src="https://full_computer_name/opcenterrp/" style="width:0px;height:0px;disp
lay:none;"/>
```

The authentication is completed when the **MRAuth** cookie is created within the application domain. As this cookie is set as *HttpOnly*, it is not visibile in JavaScript.

Available Operations

4.2.1 Embedding Reports

To embed reports, you can invoke the Opcenter Reporting Web API in either of the following ways:

- Client-side
- Server-side

> ⚠ Please make sure to copy the code correctly and check it carefully before running it (the text may be broken across two different pages of the .pdf manual).

Invoking the Opcenter Reporting Web API Client-side

Make the call to the API after you have set:

- the Web API URL;
- the method corresponding to the action you want to invoke (GET, POST, PUT, DELETE, UPDATE etc.)

Example

In AngularJS this type of call is managed by a service. In this example, a **config** object containing the UI configuration keys is injected into the service constructor.

The **reportingApi** key contains Opcenter Reporting Web API URL (e.g. https://*full_computer_name*/opcenterrp/)

```
(function () {
    'use strict';

    angular
        .module('app')
        .factory('ReportUmcService', ReportUmcService);

    ReportUmcService.$inject = ['$http','config','$q'];
    function ReportUmcService($http, config, $q) {
        var service = {};

        service.GetAll = GetAll;
        service.GetById = GetById;
        service.QueryReport = QueryReport;


        return service;

        //It returns the list of all items (reports and folders) in the repository at
the root level folder
        function GetAll() {
            return $http.get(config.reportingApi + 'api/RepositoryItems?
parentItemId=00000000-0000-0000-0000-000000000000').then(handleSuccess,
handleError('Error getting all reports'));
        }
```

```
        //It returns the url for the iframe embedding
        function GetById(id) {

            var url = config.reportingApi + 'Reports/HTML5Viewer?reportRepositoryID='
 + id;
            return url;
        }

        //It returns the url for the iframe embedding and also it passes the report
parameters to the report itself
        function QueryReport(id, reportParams) {

            var url = config.reportingApi + 'Reports/HTML5Viewer?reportRepositoryID='
 + id + '&reportParams=' + reportParams;
            return url;
        }


        // private functions

        function handleSuccess(res) {
            return res.data;
        }

        function handleError(error) {
            return function () {
                return { success: false, message: error };
            };
        }
    }

})();
```

Invoking the Opcenter Reporting Web API Server-side

To make a server-side call to the Opcenter Reporting Web API, you have to insert the **MRAuth** cookie retrieved during the call to the API of the application that needs to embed Opcenter Reporting.

Example

```
public class ReportingController : ApiController
{
    //consider an object that contains the configuration of your application
    private ApiConfiguration _config;

    public ReportingController()
    {
        _config = ApiConfiguration.Instance;
    }

    [ActionName("getReports")]
    [HttpGet]
    public async Task<string> GetJSonReports()
```

```
    {
        //this property contains the reporting api url in the same format explained
above
        var reportingUrl = _config.ReportingUrl;
        //this is the rest url you want to call
        var url = $"api/RepositoryItems?parentItemId={Guid.Empty}";

        CookieContainer cookieContainer = new CookieContainer();
        var handler = new HttpClientHandler() { CookieContainer = cookieContainer,
UseCookies = true };
        HttpClient client = new HttpClient(handler)
        {
            BaseAddress = new Uri(reportingUrl)
        };
        client.DefaultRequestHeaders.Accept.Clear();
        client.DefaultRequestHeaders.Accept.Add(new MediaTypeWithQualityHeaderValue
        ("application/json"));

        var requestCookies = this.Request.Headers.GetCookies();
        var cookieCollection = new CookieCollection();
        foreach (var cookieHeaderValue in requestCookies)
        {
            var cookies = cookieHeaderValue.Cookies.Where(c => c.Name == "MRAuth").Se
lect(c => new Cookie(c.Name, c.Value)).ToList();
            foreach (var cookie in cookies)
            {
                cookieContainer.Add(client.BaseAddress, cookie);
            }
        }
        return await client.GetStringAsync(url);

    }
}
```

4.3 Executing and Getting a Report as PDF without User Interaction

In Opcenter Reporting you can execute a report and receive it in PDF format for future use, for example to send it by email or to another application.

Procedure

Call the following URL to which you have previously added the required parameters:

https://FQDN/opcenterrp/api/RepositoryItemActions/ExecuteReportInPdf?cbID=&rpParams=<*encoded report parameter*>&pdfOpt=<*URLencoded pdf parameter*>

Parameters	Description
otc	(*Only if you are authenticating without using UMC*) See Getting the One-Time Authorization Code.

Parameters	Description
cbID	The **Cbid** of the report.
rpParams	(Optional) URLencoded pdf parameter values separated by **&**. The allowed parameter types are: • **string** • **date**: JSON format ISO 8601 • **bool**: true or false • **numeric**: using decimal point as separator • **array**: separated by **;**
pdfOpt	(Optional) URLencoded parameter values separated by **&**. If you use this parameter, all its elements are optional. Valid keys are: • **Conformance**: the PDF version to be used (see table below). • **Title**: string that specifies the title of the generated PDF document (empty by default). • **Subject**: string that specifies the subject of the generated PDF document (empty by default). • **Keywords**: string that specifies the keywords of the generated PDF document (empty by default). • **Author**: string that specifies the Author tag of the PDF file (empty by default).

Examples of pdfOpt parameter configuration

Full form (non-encoded) Configuration

```
Conformance=pdfa1b&Title=TestTitle&Subject=TestSubject&Keywords=TestKeyword&Author=TestAuthor
```

URLencoded Configuration

```
Conformance%3Dpdfa1b%26Title%3DTestTitle%26Subject%3DTestSubject%26Keywords%3DTestKeyword%26Author%3DTestAuthor
```

Possible values for the Conformance parameter

Value	Meaning
pdf10	PDF version 1.0

Value	Meaning
pdf11	PDF version 1.1
pdf12	PDF version 1.2
pdf13	PDF version 1.3
pdf14	PDF version 1.4 (corresponds to Acrobat 5)
pdf15	PDF version 1.5
pdf16	PDF version 1.6 (corresponds to Acrobat 7)
pdf17	PDF version 1.7 (ISO 32000-1)
pdf20	PDF version 2.0 (ISO 32000-2)
pdfa1b	PDF/A-1b (ISO 19005-1, Level B compliance)
pdfa1a	PDF/A-1a (ISO 19005-1, Level A compliance)
pdfa2b	PDF/A-2b (ISO 19005-2, Level B compliance)
pdfa2u	PDF/A-2u (ISO 19005-2, Level U compliance)
pdfa2a	PDF/A-2a (ISO 19005-2, Level A compliance)
pdfa3b	PDF/A-3b (ISO 19005-3, Level B compliance)
pdfa3u	PDF/A-3u (ISO 19005-3, Level U compliance)
pdfa3a	PDF/A-3a (ISO 19005-3, Level A compliance)
Default	pdf17

Limitations

Besides others, the following hints and limitations should be considered:

- Fonts are automatically recognized and dynamically embedded if necessary.
- Not all EMF records can be displayed accurately – if you are using complex EMFs, you should pass them as bitmaps or choose "export as picture" in the designer.

- Lines/Frames that are dashed/dotted in the layout may have a different spacing.
- Note for PDF/A:
    - When using form elements in combination with PDF/A, PDF/A conformity cannot be maintained and the form elements are deactivated.
    - All fonts are always embedded.
    - Encryption is not supported.

5 Upgrading Opcenter Reporting from version 2401 to version 2401.0001

Perform the following procedure if you want to upgrade Opcenter Reporting from version 2401 to version 2401.0001.

Starting from version 3.2 a new licensing model is applied. Before upgrading from a version prior to 3.2 to a higher version, you need to acquire the Opcenter Reporting Client license, which includes the number of allowed seats, to be added to the Server-based license. For more details, see Managing Licenses, Users and Roles for Opcenter Reporting.

User Management Component (UMC) Configuration

To configure UMC 2.9 SP2 correctly, some additional manual steps have to be executed. To do so, follow the procedure described in the *Upgrading UM Priority Ring Server* chapter in *UMC Installation Manual* (point 5 and the first command of point 6 of the procedure, as the steps described in points 1 to 4 are already executed by Opcenter Reporting setup).

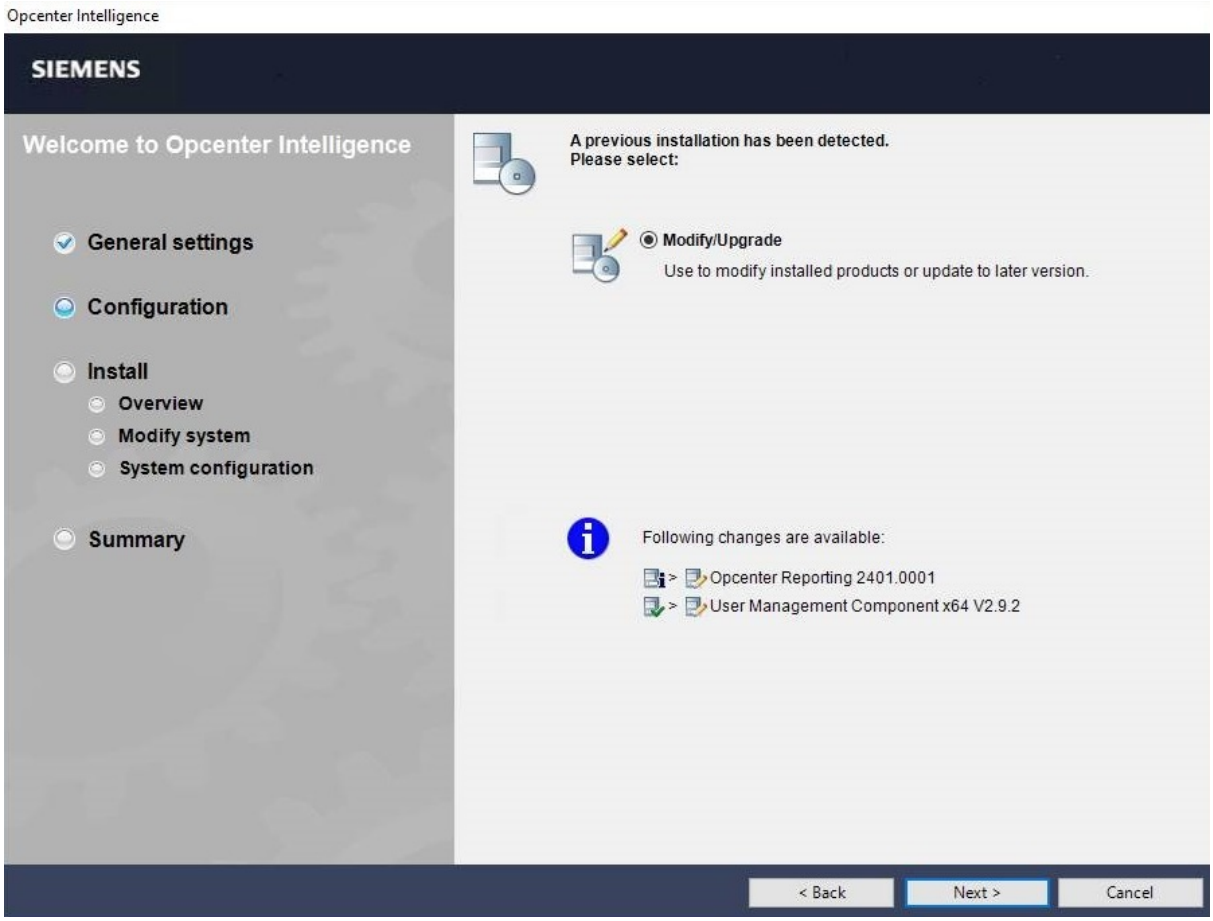
Before executing the procedure, check the compatibility of all the applications that use this instance of UMC.

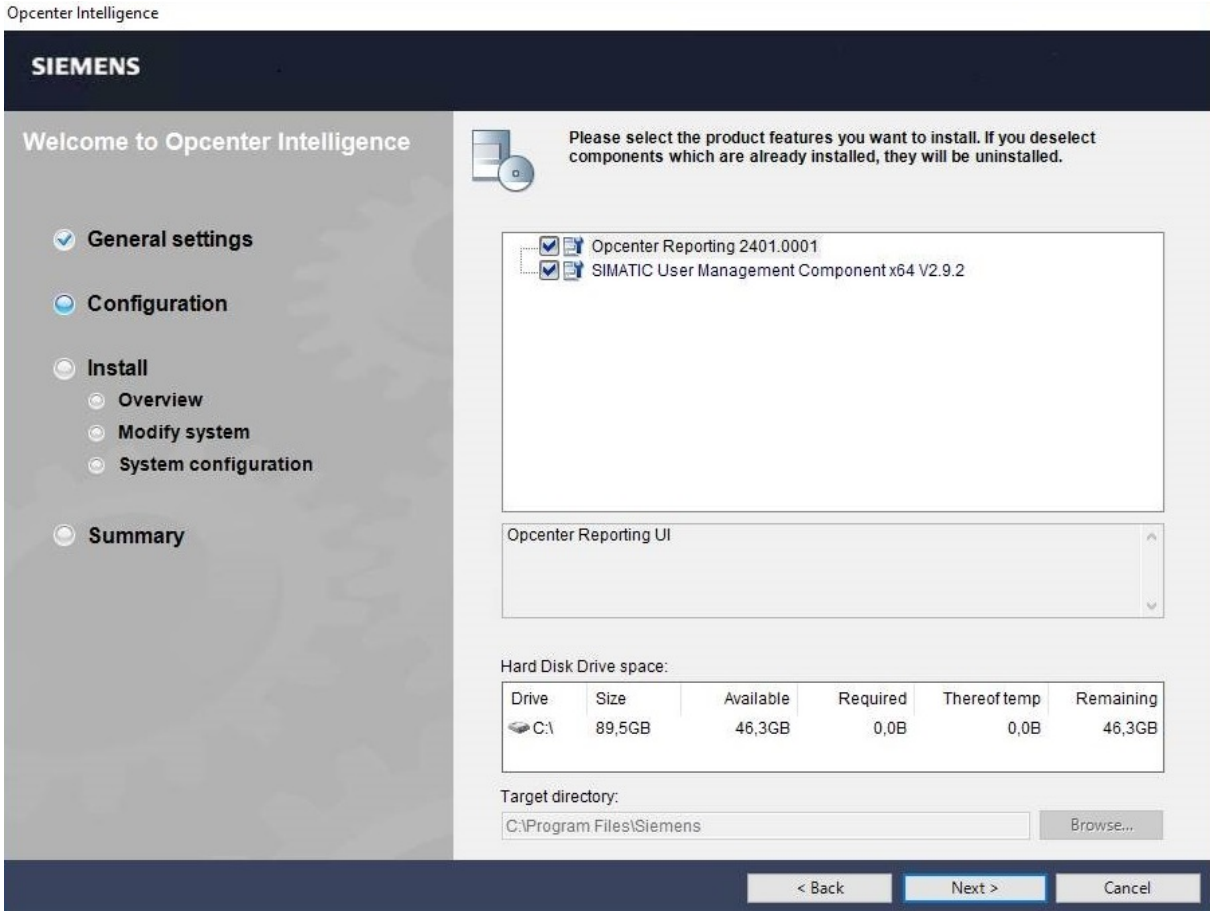
Important Recommendations

- 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 Reporting.
- It is recommended that you include in your database maintenance plan a backup of the existing repository database located in the folder: **ProgramData\Siemens\Opcenter\Intelligence\Report\Server\App_Data**
- In particular, you should make a regular backup of the **repository.db** file, which is stored in the above folder and contains all the reports you have created.

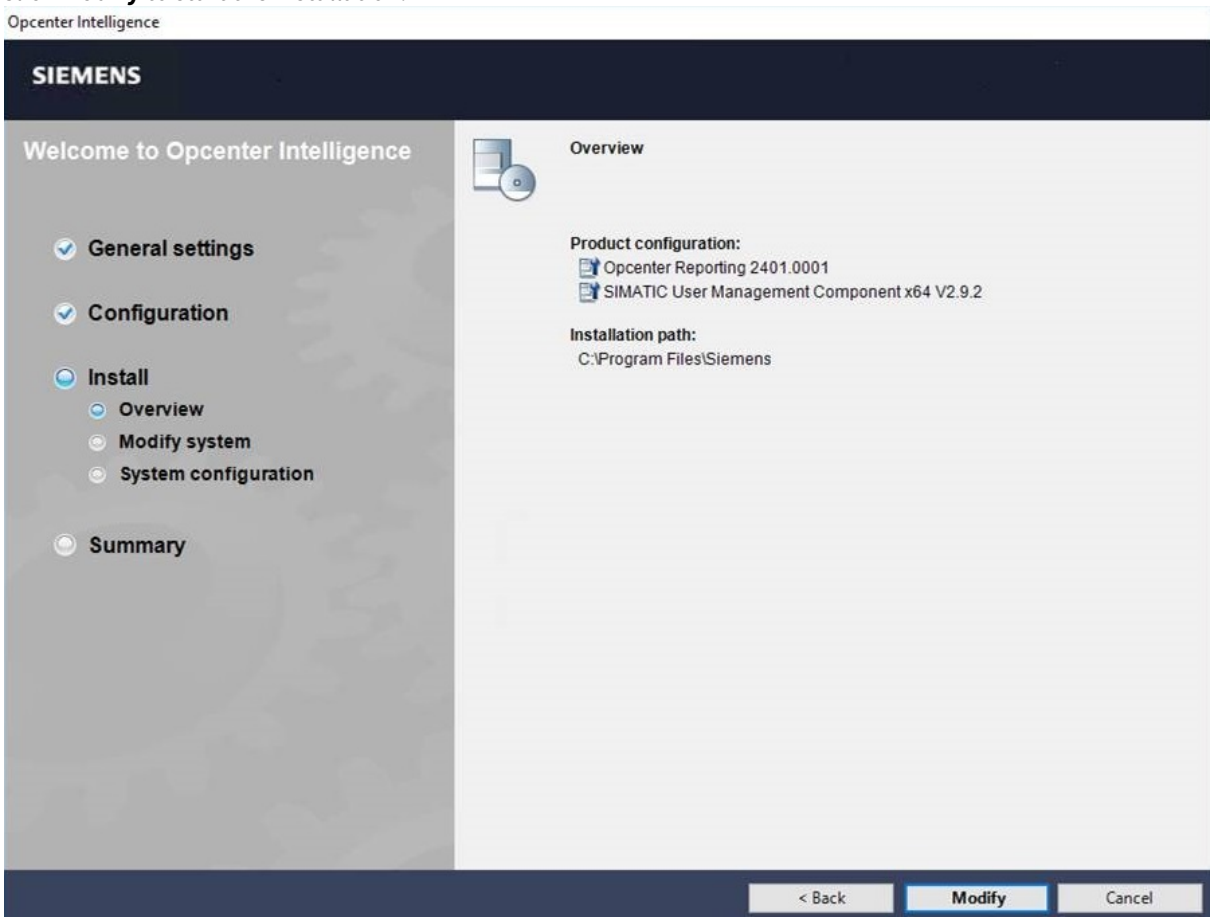
Procedure

1. Launch the installation of Opcenter Reporting 2401.0001 by executing the **Start.exe** program located in the **OpcenterReport** subfolder contained in Opcenter Intelligence ISO root folder and follow the wizard instructions. In particular, in the following steps select **Modify/Upgrade**, click **Next** and select the products to be installed.


Opcenter Intelligence
SIEMENS
Welcome to Opcenter Intelligence
General settings
Configuration
Install
Overview
Modify system
System configuration
Summary
A previous installation has been detected.
Please select:
Modify/Upgrade
Use to modify installed products or update to later version.
Following changes are available:
> Opcenter Reporting 2401.0001
> User Management Component x64 V2.9.2
< Back
Next >
Cancel


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 Reporting 2401.0001
SIMATIC User Management Component x64 V2.9.2
Opcenter Reporting UI
Hard Disk Drive space:
Drive
Size
Available
Required
Thereof temp
Remaining
C:\
89,5GB
46,3GB
0,0B
0,0B
46,3GB
Target directory:
C:\Program Files\Siemens
Browse...
< Back
Next >
Cancel

2. Click **Modify** to start the installation.



3. After the installation is completed, run the Opcenter Reporting Configurator by double-clicking the corresponding desktop icon.
4. A warning message appears to remind you that the UMC configuration needs to be completed and suggests that you follow the instructions contained in *UMC Installation Manual*.
5. Click **Apply** and wait for the pop-up message that confirms the successful completion of the configuration.
6. Click **Close**.
7. Clear the cache of the Internet browser.

6 Uninstalling Opcenter Reporting

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

Important Recommendations

- Uninstalling User Management Component requires a number of additional actions. For more details on how to uninstall UMC properly, see *User Management Component Installation Manual*.
- If you have applied modifications to elements contained in the installation folder, remember that they will not be removed when you uninstall Opcenter Reporting and you will need to remove them manually.
- All data generated by the application (application database, log files and public keys you have used) need to be removed from **ProgramData\Siemens\Opcenter\Intelligence\Report\Server\App_Data** if you want to totally uninstall Opcenter Reporting. However, if you are upgrading to a new version of the product, these items may be maintained in the same folder.

  > Please bear in mind that this folder contains the **repository.db** file, which contains all the reports you have created. If the folder is deleted and a regular backup of this file has not been made, your reports will be lost.

Procedure

1. From **Windows Control Panel > Programs and Features** environment, select Opcenter Reporting and click **Uninstall**.
2. Restart the computer.

7 Troubleshooting

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

Issue	Tips	See also
Combit® List & Label Designer does not open.	Check that the https protocol has been configured correctly in IIS.	Performing Additional Configuration Operations
Combit® List & Label Designer automatic update fails.	1. In Windows **Settings** > **Apps** > **Apps & features**, uninstall the Web Designer. 2. Go to the **Reports** page and open a report using the Web Designer. A message should prompt you to download the new version.	*Authoring Reports* page in *Opcenter Reporting User Manual*.
A message requesting to update the Web Designer continues to appear even if the update has been completed.	1. In Windows **Settings** > **Apps** > **Apps & features**, uninstall the Web Designer. 2. Go to the **Reports** page and open a report using the Web Designer. A message should prompt you to download the new version.	*Authoring Reports* page in *Opcenter Reporting User Manual*.
When an update of Combit® List & Label Designer is available and you open a report in Opcenter Reporting using the Designer, you are prompted to modify, repair or remove the program but the **Modify** option is not visible.	You must select the **Remove** option to uninstall the Web Designer (the **Repair** option would not update the program), then open the report again to be prompted to download and install the updated version of the Web Designer.	*Authoring Reports* page in *Opcenter Reporting User Manual*.