

IBM Enterprise Content Management System Monitor

Installation Guide



IBM Enterprise Content Management System Monitor

Version 5.8.0

Installation Guide

SC27-9241-09

Table of Contents

Preface	2
About this document	2
Who should read this guide?	2
Before you start	2
Feedback on documentation	3
Platform Support with ESM 5.8.0	4
Platforms and releases supported for ESM Server and ESM Agent - Operating Systems	4
Platform Support for ESM 5.8.0 - Managed Middleware	4
Browser Support with ESM 5.8.0	6
Hardware Requirements of ESM	7
Before you start	8
Preposition	8
Consideration	8
SLM tag files	9
Preparation before executing the installation	10
Database Preparation	10
Installing with internal database (H2)	10
Installing with external databases (MSSQL or DB2)	10
Preparing the databases	10
Ports	11
X11 (Unix/Linux)	12
Diskspace and filesystem	12
Tips and Tricks	13
Important information before starting any installation	14
When updating an existing installation	14
Before	14
After	15
Virus Scanners	17
Known Issues when executing the installers	18
Windows	18
Installer does not start due to unsecured location	18
Installation using GUI mode	20
Windows based server	20
Linux based server	30
Windows based agent	40
Linux based agent	48
AIX based agent	55
Installation using silent mode	64

Windows based server	64
Windows based agent	65
Linux based server	66
Linux based agent	67
AIX based agent	68
Tests for a successful installation	70
Security hints	71
How to create a systemd service for ESM on Linux-s390x	72
Motivation	72
Prerequisites	72
Procedure	72
New reload script	72
Make the file executable with	73
Scenario: No service installed	73
Scenario: Existing – but not working service installation	73
Service test	74
Example service configuration	74
De-installation of the software	76
Windows based systems	76
Linux based systems	79
AIX based systems	82
Running the ESM server with https - Using self-signed or authority signed certificates	86
Create a self-signed certificate	86
Use an authority signed certificate	86
ESM 5.8.0 Docker Deployment	88
Overview	88
How can ESM be used with Docker?	88
Which Docker images are available (as of version ESM 5.8.0)?	88
Import Docker Images into the Local Repository	88
Deploying ESM Server (<code>esmserver</code>)	89
Deployment Samples	89
Simple Deployment	90
Simple Deployment with Port Mapping	91
Deployment with Data Volume	91
Deployment with TLS/SSL Security (HTTPS)	92
Configuration Variables	94
Deploy ESM Server Container With IBM DB2 databases	95
Deploy ESM Server Container With SQL Server	97
Deploying ESM Agent (<code>esmagent</code>)	99
Prepare Docker Network	99
Connect a running <code>esmserver</code> container to the network	100

Run a <code>esmagent</code> container	100
Installation on a Container Orchestration Platform	102
Appendix A: Copyright notice	103
IBM Enterprise Content Management System Monitor	103
Appendix B: Notices	104
Appendix C: Trademarks	106

This document contains installation and configuration instructions for the IBM Enterprise Content Management System Monitor server and agent systems. The target audience for this guide are those who install or maintain ESM environments.

Preface

About this document

This document is written as plain text document and provided as html / pdf. The newest ESM related documents can be found in the help section of the console.

Who should read this guide?

The target audience for this guide are those who install or maintain ESM environments.

Every effort has been made to provide you with complete installation instructions. If information becomes available after the creation of the installation media from which you accessed this guide, we will provide an updated version of the guide on the IBM Customer Service and Support web site (<https://www.ibm.com/support>). As a general rule, you should refer to the IBM web site to obtain the current version of this guide.

This guide provides instructions for installing and/or upgrading IBM Enterprise Content Management System Monitor, and identifies the IBM/FileNet and 3rd Party products that are certified for the current release. Be aware that each release of IBM Enterprise Content Management System Monitor may have multiple Interim Fixes, or Fix Packs available for installation, each with potentially different dependencies and installation requirements. Therefore, before you attempt to install or upgrade IBM Enterprise Content Management System Monitor, review the list of releases and their associated dependencies on the IBM Support web site (<https://www.ibm.com/support>).

Before you start

Users of the guide should have knowledge about Unix and/or Microsoft Windows® operating system, web servers, database systems and middleware platforms. The configuration of managed systems (clients) requires advanced knowledge of all IBM ECM systems that should be monitored.

You should read the Upgrade Notes section below!

If you lack the requisite skill sets it is strongly recommended to have IBM Lab Services or a certified ValueNet Partner in order to install this product.

TIP

For tips and tricks regarding the configuration and maintenance of IBM Enterprise Content Management System Monitor please check the CENIT Field Guides at [IBM ESM Field Guides](#).

The PDFs of the eGA documentation can be found on the [IBM support pages](#). In the installed product you will always find the newest documentation.

Feedback on documentation

Send your comments by e-mail to comments@us.ibm.com. Be sure to include the name of the product, the version number of the product, and the name and part number of the book (if applicable). If you are commenting on specific text, include the location of the text (for example, a chapter and section title, a table number, a page number, or a help topic title)

Platform Support with ESM 5.8.0

Platforms and releases supported for ESM Server and ESM Agent - Operating Systems

Table 1. Platform Support for ESM 5.8.0 - Management Infrastructure (Operating Systems)

Product/Platform	Release	Component
Windows	2019, 2022, 2025	ESM Server
RHEL (x86_64)	8.6, 8.7, 9.0-9.5	ESM Server
SLES (x86_64)	15 SP5	ESM Server
Windows	2012 R2 (deprecated), 2016 SR4 (deprecated), 2019, 2022, 2025	ESM Agent
AIX	7.2 TL5 (deprecated), 7.3 TL0, 7.3 TL1	ESM Agent
RHEL (x86_64)	8.6, 8.7, 9.0-9.5	ESM Agent
RHEL (s390x / Z64)	8.6, 8.7, 9.0-9.5	ESM Agent
SLES (x86_64)	12 SP5, 15 SP4, 15 SP5	ESM Agent
SLES (s390x / Z64)	15 SP4, 15 SP5	ESM Agent
Ubuntu (s390x / Z64)	22.04, 24.04, 26.04	ESM Agent

NOTE

The supported platform architectures (aka hardware) are listed at https://www.ibm.com/support/pages/semeru-runtimes-support/#platforms_version_11.

Platform Support for ESM 5.8.0 - Managed Middleware

NOTE

In the following x equals to the maximum version number available at July 24, 2025.

Table 2. Platform Support for ESM 5.8.0 - Managed Middleware

Product/Platform	Release	Component
DB2	11.5, 12.1	ESM Server
DB2	11.1, 11.5, 12.1	ESM Agent
H2	2.3.232	ESM Server (included in the product, will be updated automatically, if necessary)
MSSQL	2019, 2022, 2025	ESM Server
MSSQL	2017 (deprecated), 2019, 2022, 2025	ESM Agent
Oracle	18c (deprecated), 19c, 21c, 23ai	ESM Agent
PostgreSQL	14, 15, 16	ESM Agent
WebSphere Application Server	8.5.x, 9.0.x	ESM Agent
WebLogic	11.0, 12.x, 14c	ESM Agent
TSM/Spectrum Protect	7.x, 8.x	ESM Agent

Table 3. Platform Support for ESM 5.8.0 - Managed Business Automation Engines

Product/Platform	Release	Component
FileNet Image Services	4.1.x, 4.2.x	ESM Agent
IBM Content Navigator	3.0.x, 3.1.x, 3.2.0	ESM Agent
IBM Content Collector	4.0.x	ESM Agent
IBM Content Cortex Content Platform Engine	26.0	ESM Agent
IBM FileNet Content Platform Engine	5.5.x, 5.6.0, 5.7.0	ESM Agent
IBM Case Manager	5.3.x	ESM Agent
IBM Business Automation Workflow	22.0.x, 23.0.x, 24.0.x, 25.0.x	ESM Agent
IBM Enterprise Records	5.2, 5.2.1	ESM Agent
IBM Content Manager (CM8)	8.6, 8.7	ESM Agent
IBM Content Manager on Demand	10.1, 10.5	ESM Agent
IBM OperationalDecisionManager	8.10.x, 8.11, 8.12	ESM Agent
IBM Datacap	9.1.x	ESM Agent
Daeja ViewONE Virtual	5.0.x	ESM Agent
IBM BA Containers (CP4BA)	Corresponding Standalone Versions - see above	remote ESM Agent
Cloud Pak for Business Automation	24.0.x, 25.0.x	remote ESM Agent

Browser Support with ESM 5.8.0

- Google Chrome 130+
- Mozilla FireFox 130+
- Microsoft Edge 130+

NOTE

Safari is unsupported. The ESM console can be used with Safari, but some features might not work as expected.

NOTE

Microsoft IE 11 not supported!

Hardware Requirements of ESM

Table 4. Container Version of ESM

Container	CPU (min)	CPU (max)	Memory (min)	Memory (max)	Diskspace
Server	2 core	4 cores	8 GB	16GB	10 GB + 40 GB shared location if internal H2 is used as Database
Agent	2 core	4 cores	4 GB	16GB	2 GB

NOTE

Images are based on Red Hat UBI10-minimal. So all requirements of UBI10-minimal do also apply to the ESM images as well.

Table 5. Install Version of ESM

Type	CPU (min)	CPU (recommended)	Memory (min)	Memory (recommended)	Diskspace
Agent on monitored Server (additionally plan)	10 %	-	10 %	-	2 GB
Agent stand alone	1 core	2 cores	4 GB	8 GB	2 GB
Server	2 core	4 cores (no SMT)	8 GB	16GB	10 GB + 40 GB if internal H2 is used as Database

NOTE

The load on the agent always depends on the amount of running probes and their schedules.

Before you start

Preposition

ESM provides an inbuilt database (H2) and an inbuilt http server (Jetty). Both are maintained within software updates and can be seen as a black box. No administration or maintenance must be done.

IMPORTANT

There can be some restrictions when updating an H2 based installation from one major version to another. Please read the Release Notes for the release version you are targetting to update to and please also read the chapter about the H2 update below.

Consideration

There are some important things you need to think about before you start with the installation.

Installation directory

For security reasons, it is mandatory to restrict access to the installation directory and its contents to a minimum number of accounts.

We therefore recommend that only the account under which the program is executed and the account responsible for installation management have access.

Windows server / agent installation user

The account that is used for the installation of a Windows server or agent must have local admin rights (member of the local administrator group).

Service User

Before you install the server or agent, you should decide which account should be used to run it. On Windows the service can run as local system. Nevertheless, you might want to use a service account. On Unix / Linux a user that has access / execute rights for the monitored application tools should be used.

Root rights

Root access is needed e.g. for the creation of autostart links for the agent.

HA environment (Active/Passive)

If an agent should be installed as HA resource, the virtual IP and the virtual hostname must be used for the installation. Furthermore, a shared drive or filesystem must be used.

On Windows based systems the installation must be repeated on the second node. All services have to be specified in the cluster administration tool.

For Unix / Linux based systems the startup and shutdown of processes have to be specified in the cluster administration tool (e.g. HACMP). There is no need to repeat the installation on the second node.

HA environment (Active/Active)

This is only possible for an agent installation. There must be a separate agent installation on each

active node. The local hostname should be used for better classification of the event.

Automatic start

Normally the software is started during start up of the server. In some cases e.g.HA on Active/Passive servers the automatic startup might not be useful. Therefore, the start-up procedure can be changed.

Eventforwarding

During the configuration process you can decide if you want to forward events via logfile.

Reporting

ESM offers basic reporting functions.

Firewall

The following ports are used as defaults in ESM and need to be opened in the firewall. The port numbers can be changed in the installation process.

- 80 (Default http port for Console URL on ESM Server)
- 443 (Default https port for Console URL on ESM Server)
- 1883 (MQTT based Agent / Server communication)

SSL

The ESM console can be installed using SSL.

The console initially uses a self-signed certificate. It is strongly recommended to replace this by a trusted certificate provided by the customer. See chapter "Running the ESM server with https - Using self-signed or authority signed certificates" for details.

LDAP Login

The most commonly used LDAP Services are supported and can be configured within the ESM console. (See configuration guide)

SLM tag files

IBM Enterprise Content Management System Monitor (ESM) creates so-called Software License Metric (SLM) tag files in the installation process for ESM Server and ESM Agent.

SLM tag files provide a standardized capability for a product to report its consumption of license metrics (resources that are related to the use of the software asset). The SLM tag files are based on the ISO/IEC 19770-4 standard draft for Resource Utilization Measurement.

The SLM tag files are stored in XML format, and new metric records are appended to the end of the file when updating an existing installation. For IBM Enterprise Content Management System Monitor, the SLM tag files (*.slmtag) are stored in the <Installation-Dir>/slm folder.

Preparation before executing the installation

Database Preparation

Installing with internal database (H2)

No preparation is needed in this case. For updates see the related Release Notes.

Installing with external databases (MSSQL or DB2)

NOTE

Only MSSQL (Enterprise and Standard only) and DB2 (Advanced and Standard Edition only) as external databases are supported. Oracle has some restriction which momentarily cause issue in ESM.

IMPORTANT

We strongly advise against entering passwords in JDBC URLs, although some databases support this. This is a serious security risk and should not be used at all, especially in production environments.

If ESM should be installed with external databases, such as MSSQL or DB2, that databases must be prepared in advance.

Create two databases (e.g. ESMConf and ESMMon, one for the configuration and one for the monitoring data) with the information from the "Preparing the databases" chapter below.

The configuration database will have less data and will not grow after the setup and configuration of the environment is complete. The monitoring database size depends on the amount of data that should be stored. Per default the cleanup is set to delete old entries after 1.5 million sets of samples and incidents. This is approx 5 to 8 GB of data but can vary.

Preparing the databases

MSSQL preparation

MS SQL Server General installation parameters The MS SQL Server must be configured for SQL Server Authentication or Mixed Mode Authentication. To change the authentication mode, see MS SQL Server

documentation.

- Create a database to use with ESM Server. Assign the Latin1_General_CI_AS collation to the database.
- Create a database user. Assign the just created ESM Server database as Default database and assign the db_datareader, db_datawriter, db_owner and public roles within the database role membership.

NOTE

Make sure, the database schema, that you will use, is the Default Schema of your specified database user, which will be used to connect to your ESM Server database and for database initialization and import, otherwise database initialization for instance will fail.

DB2 preparation

IBM DB2 General installation parameters

- Create a ESM database (use codeset UTF-8 and database Page size 32k). Smaller Page size settings are not supported and cause installation errors.
- Create the ESM technical DB user on your operating system (select a name, e.g. webadmin).
- Create the ESM technical DB user on your previously created ESM database with at least the rights "Connect to database", "Create tables" and "Create schema implicitly"

Ports

ESM uses several ports on the systems. Please make sure to use ports that are not in use during the installation. Precheck the availability of the ESM default ports with the following command:

```
ss -an | grep <Port> (Linux/Unix)
or
netstat -an | findstr <Port> Windows)
```

The default ports are:

```
ESM Server: 1099,1883,5555,8101,80,443,9092,44444
ESM Agent: 1180,1543,1883,2099,5556,9093,9202,55555
```


X11 (Unix/Linux)

The installer can be started in silent / console mode, but InstallAnywhere sometimes still tries to address X11 libraries. We have found the necessary libraries are installed if X11 forwarding can be used by ssh connections to the host the installer is executed at.

Diskspace and filesystem

Diskspace and / or file systems on Unix / Linux must be prepared. The server and agent installation take about 500MB each after installation. The server can grow more because of the internal event database then the agent.

Please see above under 'Hardware Requirements of ESM' for the recommended disk space requirements.

On Unix / Linux we recommend to create a separate file system for both.

Tips and Tricks

For tips and tricks regarding the configuration and maintenance of ESM please check the CENIT Field Guides at https://www.cenit.com/en_EN/solutions-services/software-solutions/ibm-ecm-system-monitor.html#c11350

Important information before starting any installation

All information given during the installation are stored in the file `installer.properties`. As long as the file exists in the same location, an IA installer will pick up the information from there. In case the agent and server installer is started from the same location, this will also happen and the settings might be incorrect.

Please avoid this by starting the server and agent installer from different locations or removing the file prior an installation.

When updating an existing installation

Before updating make sure you have made a backup of your current installation.

NOTE

If you have a scanner tool that checks the file system, it is possible, your scanner will find an older `log4j` or `log4j2` JAR file after you have deployed older external API JARs from other products. This is not a fault of ESM. Keep in mind to update these external JARs if necessary.

Before

IMPORTANT

When updating **directly** from 5.7.0 on MS Windows the service will always be re-installed although service re-installation was disabled in the installation/update process. Installers starting with 5.7.0.0-001 will fix this problem for the **following** updates.

- It is not recommended to mix GUI based and console mode based installations. This can lead to configuration settings erroneously enclosed with double quotes, e.g. "1883" instead of plain 1883. This is a technical limitation of InstallAnywhere.
- Check if there is an `installer.properties` file in the same directory where the installer binary was copied to.
 - If so, remove this file from the directory before starting the installer. If not, this will damage your installation.
- If you the installation uses an H2 database (ESM Server only), check the JDBC-URLs for the configuration and the monitoring database contain the following options:
`LOCK_TIMEOUT=10000;DB_CLOSE_DELAY=-1.`
 - If not, append them at the end of the each JDBC-URL by separating them with a `;` from the existing URL.

Server

- We recommend to stop the ESM server.
- Proceed with the update guided by the installer.
- Due to a 3rd-party limitation whitespace in the installation path are currently not supported under Unix/Linux.

Agent

NOTE

We strongly advise against changing an agent's identifier (aka name) with an update. If there is the need to rename an agent, please remove it and reinstall it again later.

If an agent's identifier is changed with an update, that agent will be handled as a new agent by the server. You must then manually switch the probe assignments to that new agent if you want to use the situations that were deployed to the agent before the update and renaming took place. Also keep in mind, the automatic base monitoring deployment will be executed for that new agent if it was not disabled in the server's settings.

NOTE

If you are updating an agent via the ESM web-UI, under rare conditions it is possible an already existing `<agent-installation-directory>/update` directory causes issues that will prevent the update to proceed. If so, please delete that `update` directory and try again.

- Manual update via GUI or console
 - Due to a 3rd-party limitation whitespace in the installation path are currently not supported under Unix/Linux.
 - We recommend to stop the ESM agent.
 - Proceed with the update guided by the installer.

After

- Modern browsers tend to cache data to enhance the responsiveness of web-UIs. We have found this can lead to complications after updates. Sometimes the browser does not recognize or simply ignores updates of the UI and its underlying data stores. That caching will even survive a browser restart. This all depends on the specific settings of each browser. So after an update it is recommended to explicitly clear the web browser's caches to trigger a fresh update of the UI and its components. Normally pressing Ctrl and F5 when the focus is in the tab of the ESM's UI should clean the cache. But we have found this is not always sufficient. That is why we recommend to use the browser's settings to clear stored website data and the browser's cache.
- The PortCheck-probe now uses `ss` instead of `netstat` on Linux systems. `netstat` is no longer the recommended tool but is replaced by `ss`. So it is no longer necessary to install `netstat` only for ESM. `ss` should be part of the standard installation. `ss` has a similar but not always identical output as

`netstat`. It is very likely you have to edit the entries in the IP address field in your PortCheck-probe configurations. For an example see the probe's documentation.

- Check if there are any Listener probe instances that contain masked slashes (combination of backslash and slash: `\`/`/`) in their path parameter.
 - In these probe instances, remove the masking backslashes as they are no longer necessary.
 - Affected probe types:
 - Listener
 - ListenerCpu
 - ListenerDisk
 - ListenerNetwork
 - ListenerUser
 - ListenerUserServer
 - ListenerUserStatic
- Database clean-up setting for max incidents count pruning
 - After an update the setting 'Database Max Incidents Per Situation Count' stored in `<installation_dir>/server>/karaf/etc/de.cenit.phoenix.server.dbcleanup.cfg` is removed from the file. It is not possible to redefine the setting via the UI before following the instructions of the workaround.
 - To fix this, edit the `cfg`-file (see above) and add the following entry at its end:
`cleanup.incidents.remaining.per.situation.count = <desired value>`. Then restart the server. Only after that you can change the setting via the UI again.

Virus Scanners

We strongly advise to exclude the karaf folder of the server from virus scans and from access by other external programs that potentially can lead to file locks. This can lead to database corruption.

Known Issues when executing the installers

Windows

Installer does not start due to unsecured location

Sometimes it happens that the installer does not start and report the following:

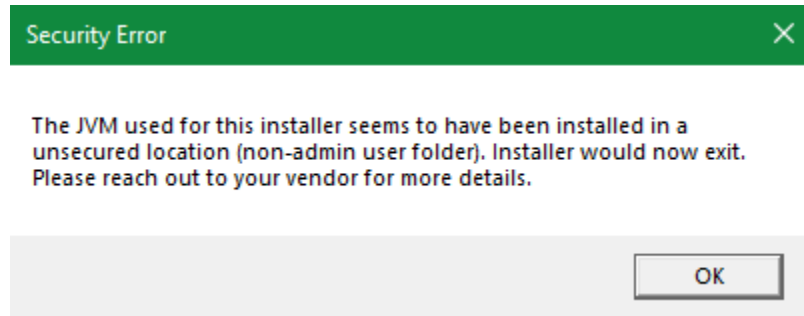
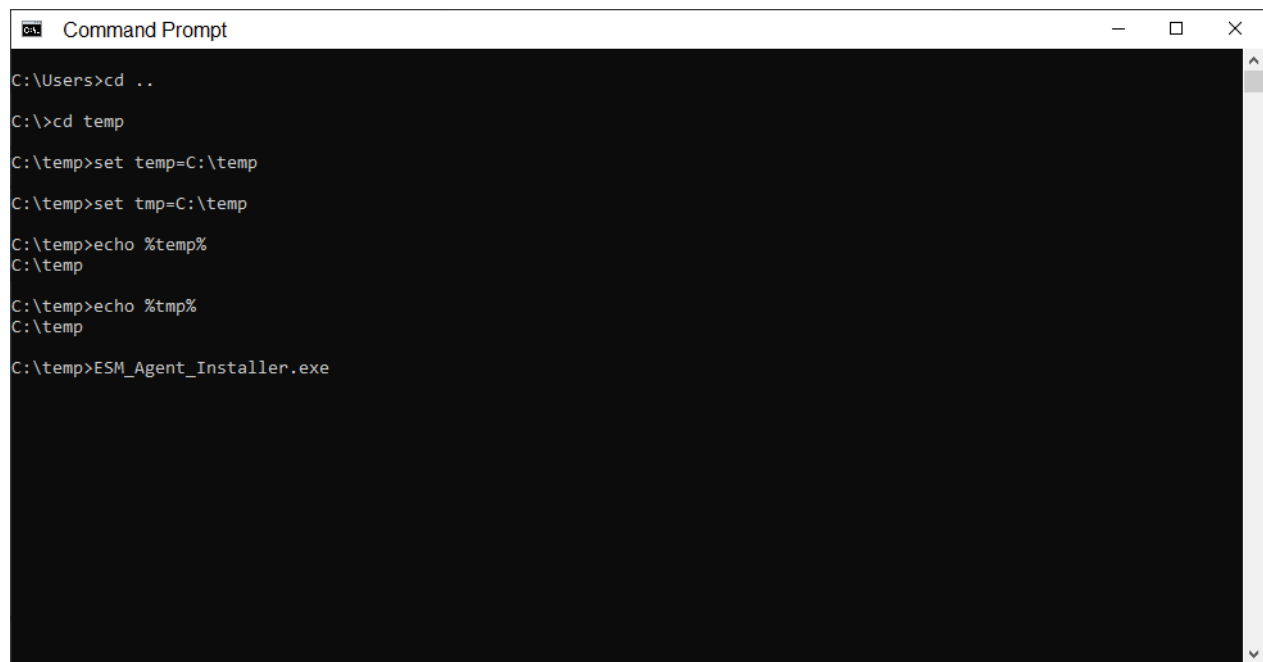


Image of Unsecure Location Error

This can be solved by changing tmp and temp environment variable to other than default in a cmd prompt and executing the installer from there:

- Open CMD prompt window.
- Set tmp and temp to a different location that exists – e.g. C:\temp
- Run the ESM installer from this CMD prompt.



```
Command Prompt
C:\Users>cd ..
C:\>cd temp
C:\temp>set temp=C:\temp
C:\temp>set tmp=C:\temp
C:\temp>echo %temp%
C:\temp
C:\temp>echo %tmp%
C:\temp
C:\temp>ESM_Agent_Installer.exe
```

Image of CMD Prompt for Unsecure Location Error

Installation using GUI mode

For the installation an InstallAnywhere package is provided. The installation offers 3 different modes: GUI, console and silent mode (See chapter [Installation using silent mode](#) for examples). This chapter shows the installation in GUI mode. The console mode is equivalent to the GUI mode, the only difference is that the input must be provided in the console and not in a GUI interface.

Windows based server

- Start the installation by executing the file "ESM_Server_Installer.exe" as administrator
- The "Software License Agreement" window is loaded. Accept the license agreement and proceed with "Next".

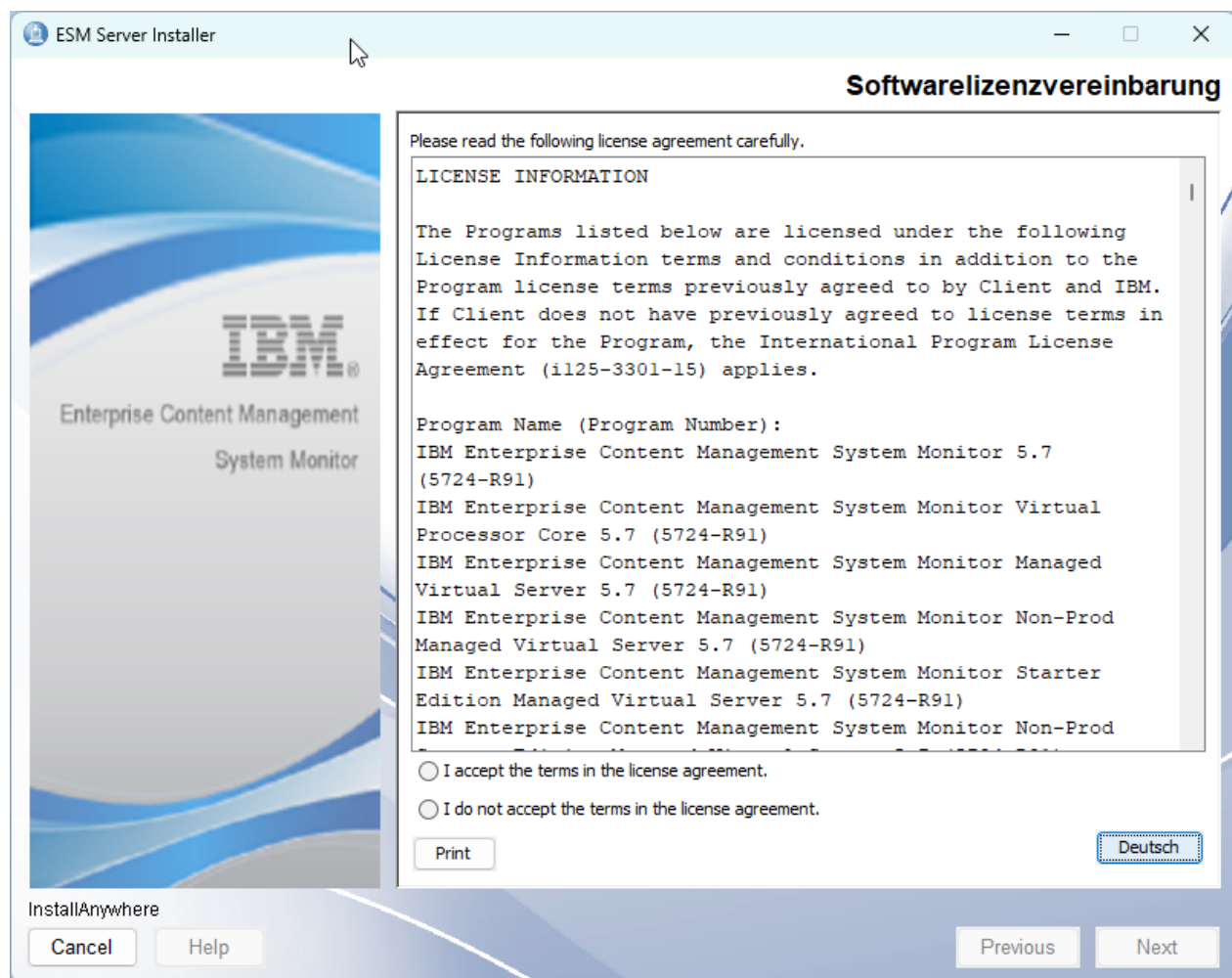


Image of Software License Agreement

- The next window is "Welcome to ESM Server". It shows some information about the installation. Click "Next" to proceed.

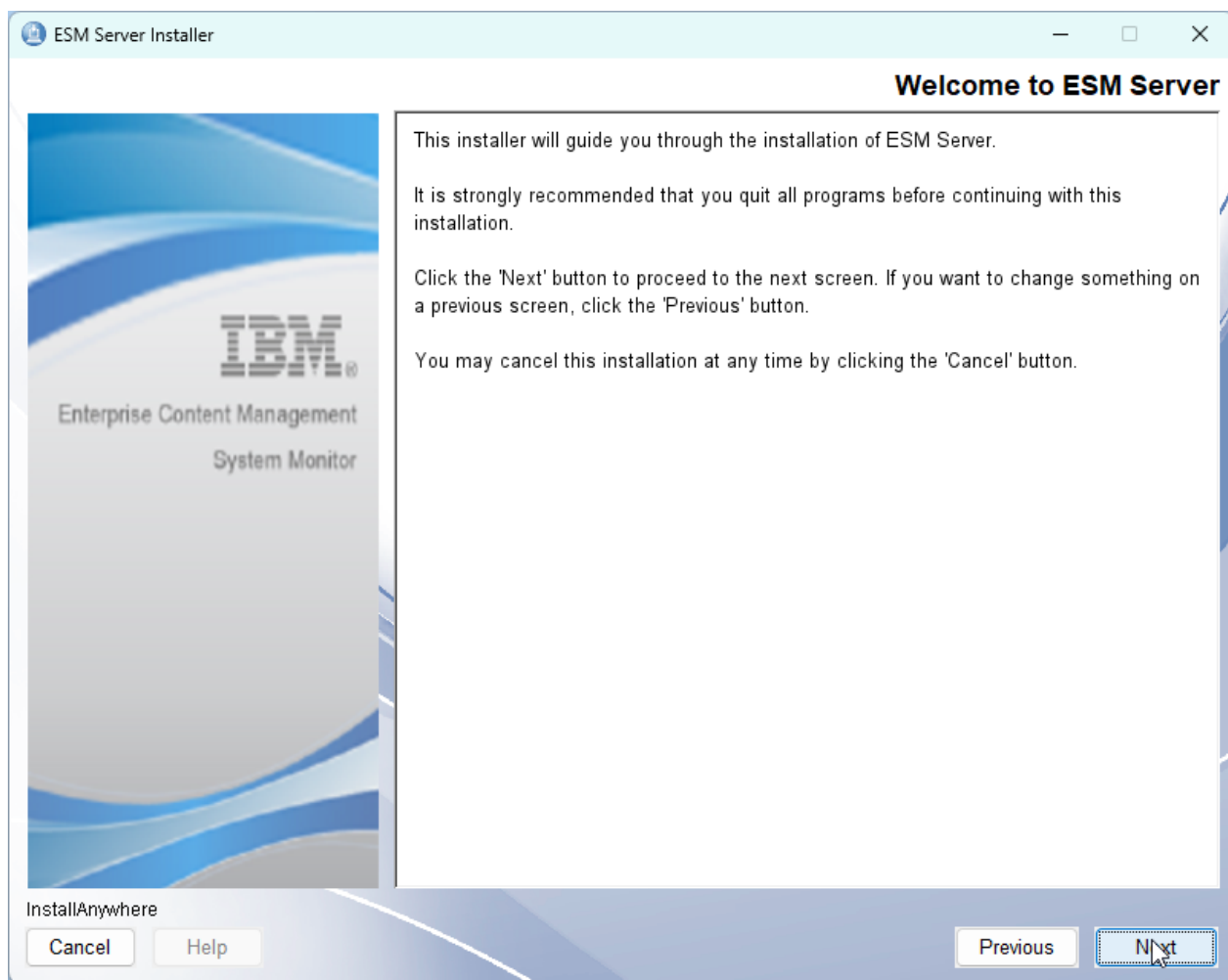


Image of Welcome to ESM Server

- The next window is "Choose Installation Folder". Specify your path for the installation here. The default is `C:\Program Files\IBM\ESM\Server`. Click "Next" to proceed.

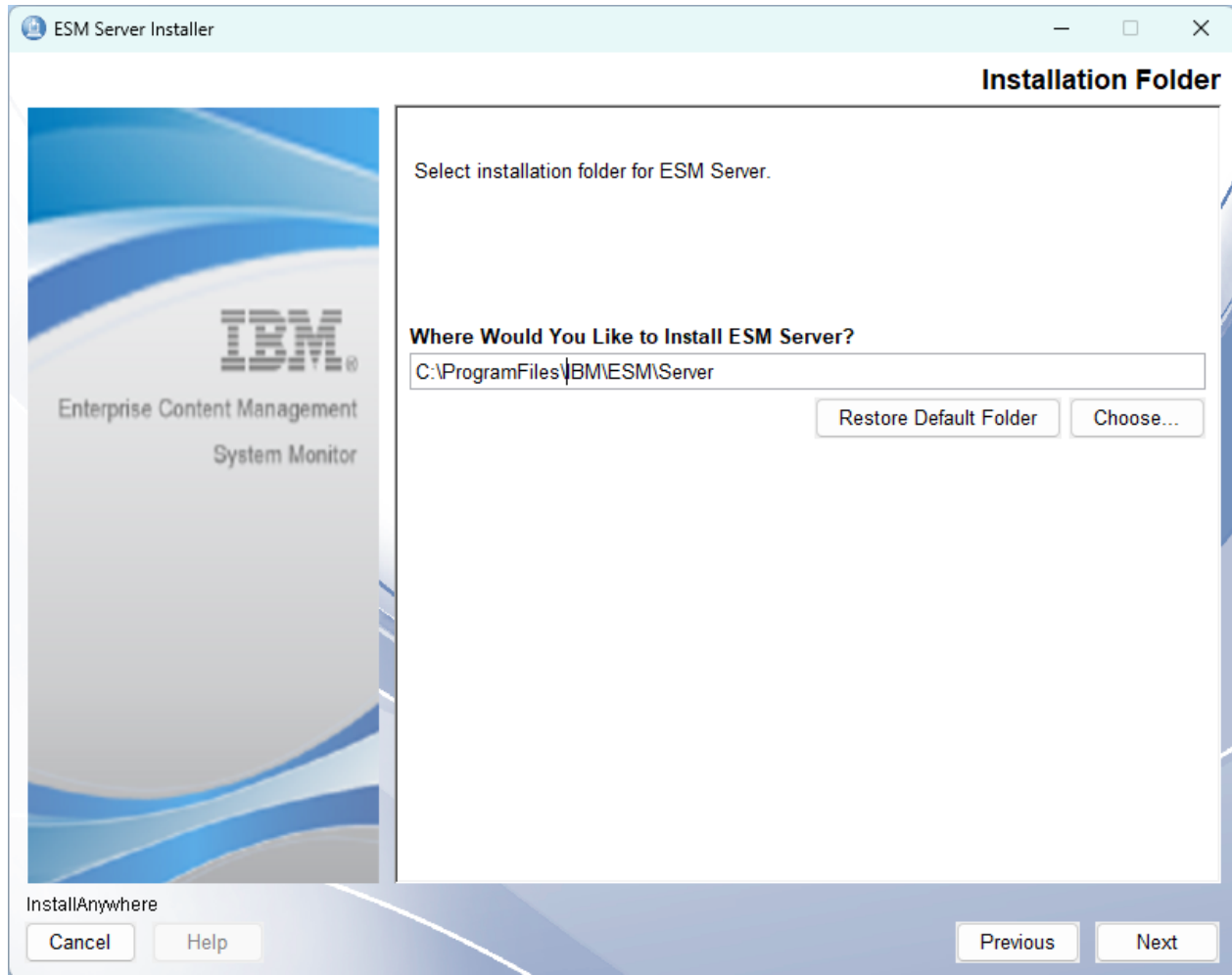


Image of Choose Installation Folder

- The next window is "Server Settings". The following parameters can be specified. Click "Next" to proceed. We recommend to keep https enabled.

Hostname

Default: `<server name>`

Server IP

Default: `0.0.0.0`

MQTT Port

Default: `1883`

HTTP Port

Default: `80`

HTTPS

Default: `Enabled`

HTTPS Port

Default: `443`

RMI Registry Port

Default: 1099

RMI Server Port

Default: 44444

SSH Port

Default: 8101

SSL KEY PASSWORD

Default: =password

SSL KEYSTORE PASSWORD

Default: =password

SSL TRUSTSTORE PASSWORD

Default: =password

ESM Server Installer

ESM Server Settings

Please enter ESM Server hostname and port numbers.

Please only change the passwords for SSL key and stores if you want to use a custom key- or truststore. Changes to the file path or store type must be made directly in the corresponding configuration file.

Hostname
localhost

IP Address
0.0.0.0

MQTT Port
1883

HTTP Port
80

HTTPS
☒ Enabled ☐ Disabled

HTTPS Port
443

RMI Registry Port
1099

InstallAnywhere

Cancel Help Previous Next

Image of Server Settings

- The next window is "Configuration Database Settings". The default settings are for usage with the internal H2 DB. DB2 and MSSQL is possible as well.

IMPORTANT

If the installation is done with DB2 or MSSQL, copy a suitable jdbc driver to <Installation-Dir>/karaf/deploy after a successful installation. In addition, if the connection is established with an LDAP account. The service needs to be started with this account and for MSSQL the matching auth.dll must be copied to <Installation-Dir>/karaf/lib/wrapper. Start the software afterwards. The default settings must be changed to fit your MSSQL or DB2 database.

JDBC Url

Default:

`jdbc:h2:./configuration;AUTO_SERVER=TRUE;AUTO_RECONNECT=TRUE;LOCK_TIMEOUT=10000;MODE=LEGACY`

Database Driver Class Name

Default: `org.h2.Driver`

Database Username

Default: `db`

Database Password

Default: `pw is hidden`

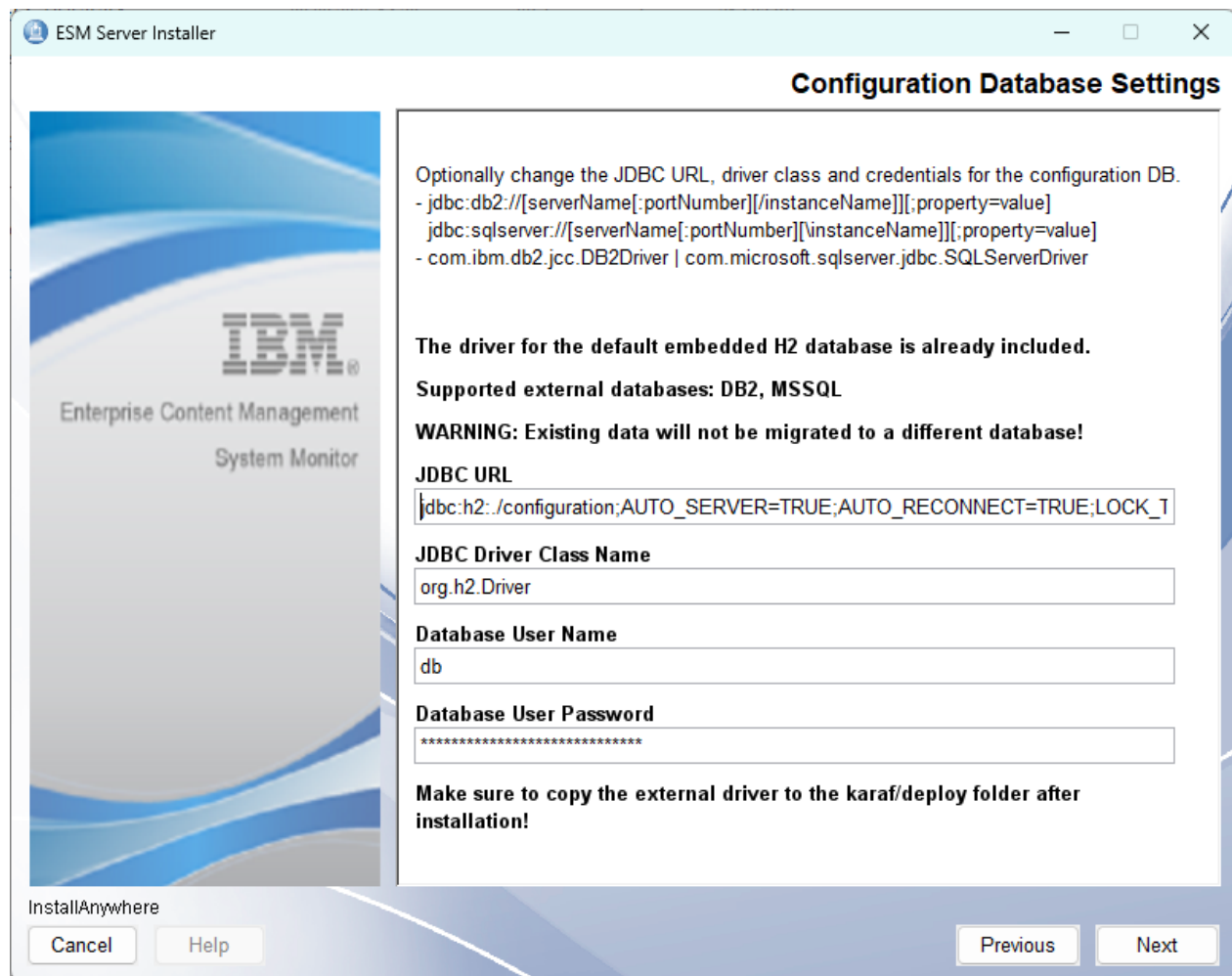


Image of Configuration Database Settings

- The next window is "Monitoring Database Settings". The default settings are for usage with the internal H2 DB. DB2 and MSSQL is possible as well.

IMPORTANT

If the installation is done with DB2 or MSSQL, copy a suitable jdbc driver to <Installation-Dir>/karaf/deploy after a successful installation. In addition, if the connection is established with an LDAP account. The service needs to be started with this account and for MSSQL the matching auth.dll must be copied to <Installation-Dir>/karaf/lib/wrapper. Start the software afterwards. The default settings must be changed to fit your MSSQL or DB2 database.

JDBC Url

Default:

`jdbc:h2:./monitoring;AUTO_SERVER=TRUE;AUTO_RECONNECT=TRUE;LOCK_TIMEOUT=10000;MODE=LEGACY`

Database Driver Class Name

Default: `org.h2.Driver`

Database Username

Default: *db*

Database Password

Default: *pw is hidden*

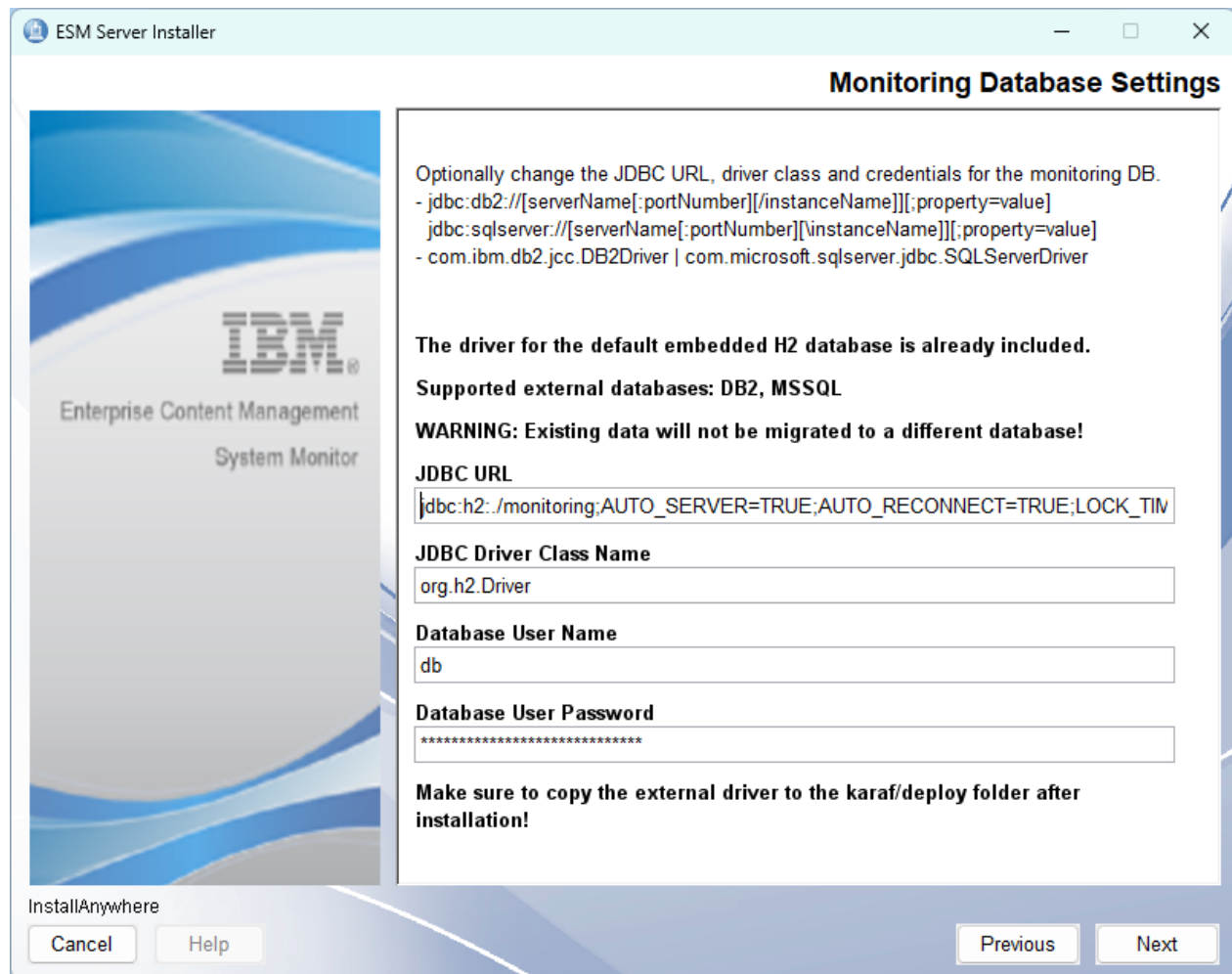


Image of Monitoring Database Settings

- The next window is "Autostart and Systemstart". The following parameters can be specified. Click "Next" to proceed.

Start ESM Server after Installation

Default: Yes = checked

Start ESM Server at OS Start

Default: Yes = unchecked

NOTE

If unchecked, the service will be installed with manual startup type.

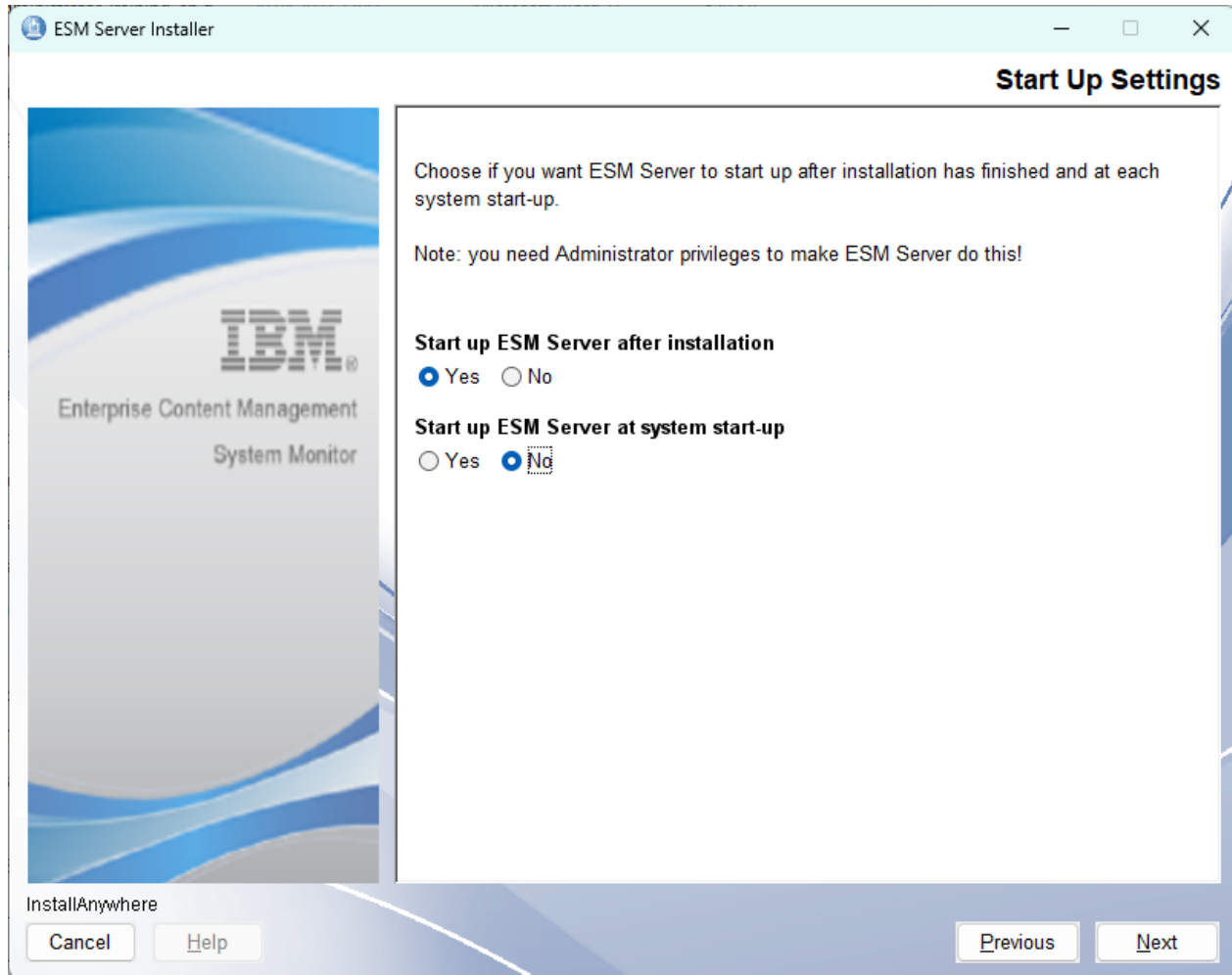


Image of Autostart and Systemstart

- The next window is "Service Installation". The following parameters can be specified. Click "Next" to proceed.

Re-Install ESM Server Service

Default: No = checked

NOTE

This Window will only be shown if the OS is Windows, the installation is an update installation and a service is used in the previous installation already.

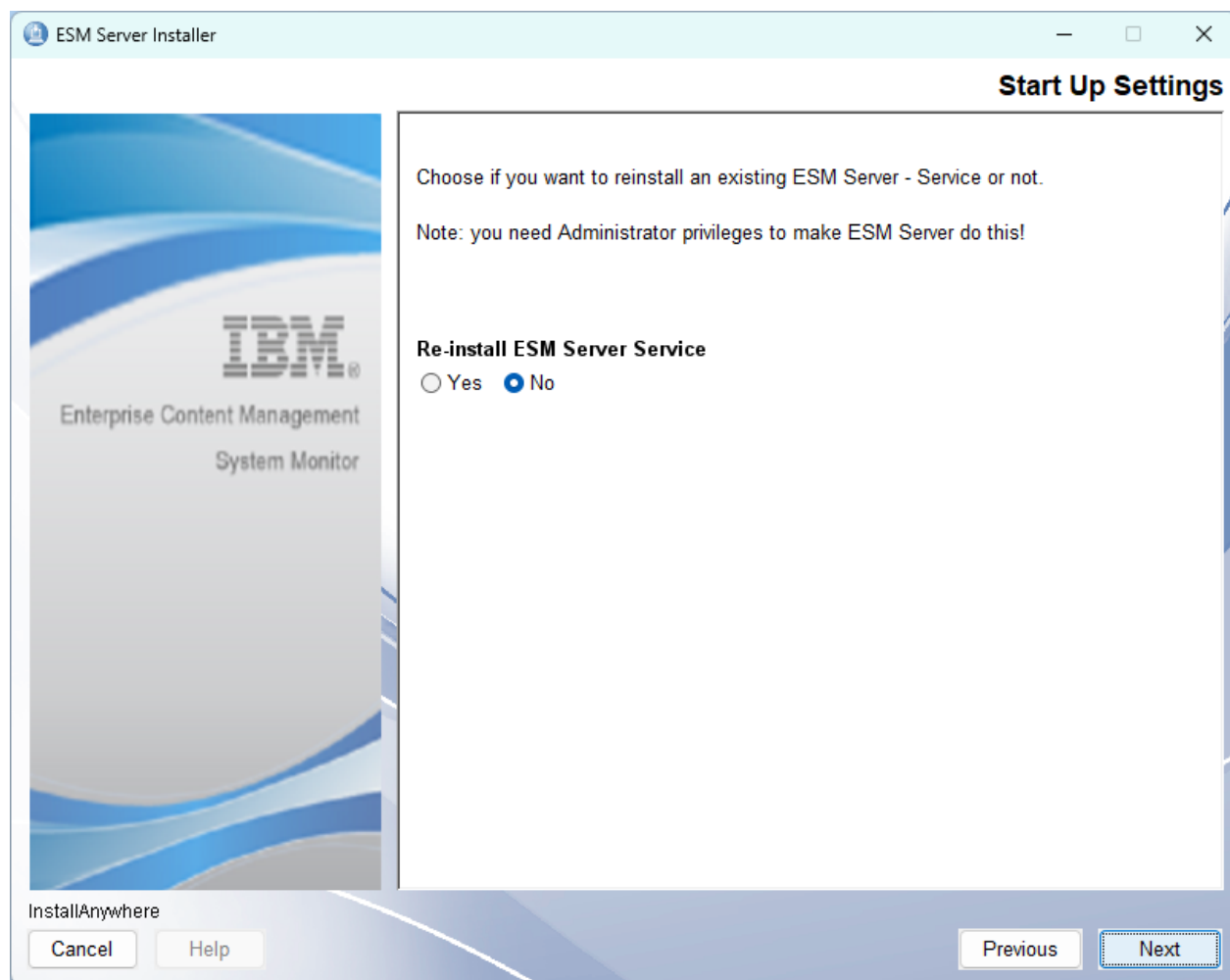


Image of Service Installation

- The next window is "Pre-Installation Summary". Click "Install" to proceed.

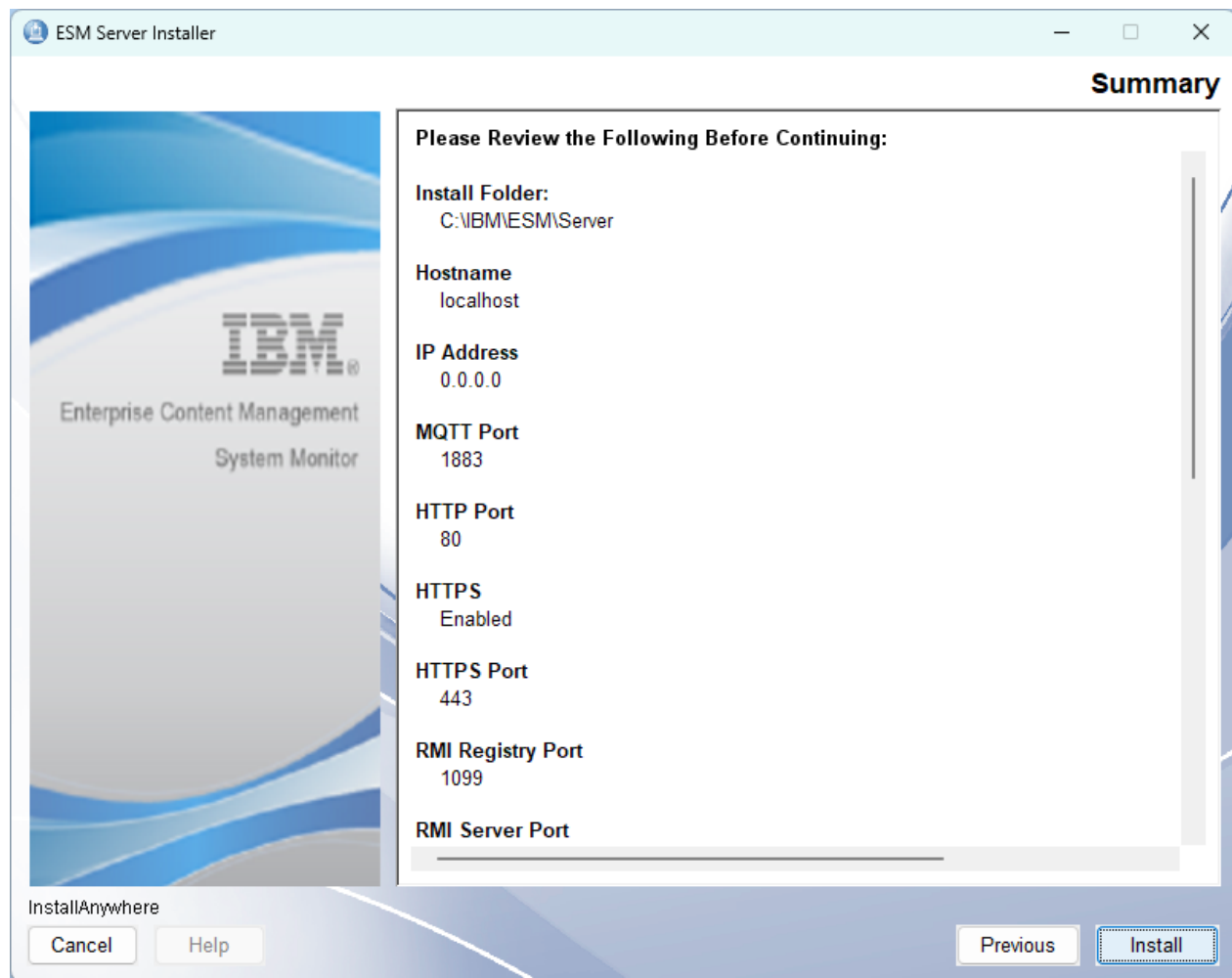


Image of Pre-Installation Summary

- The installation starts and finishes with the window "Install Complete". Click "Done" to close and finish the installation procedure.

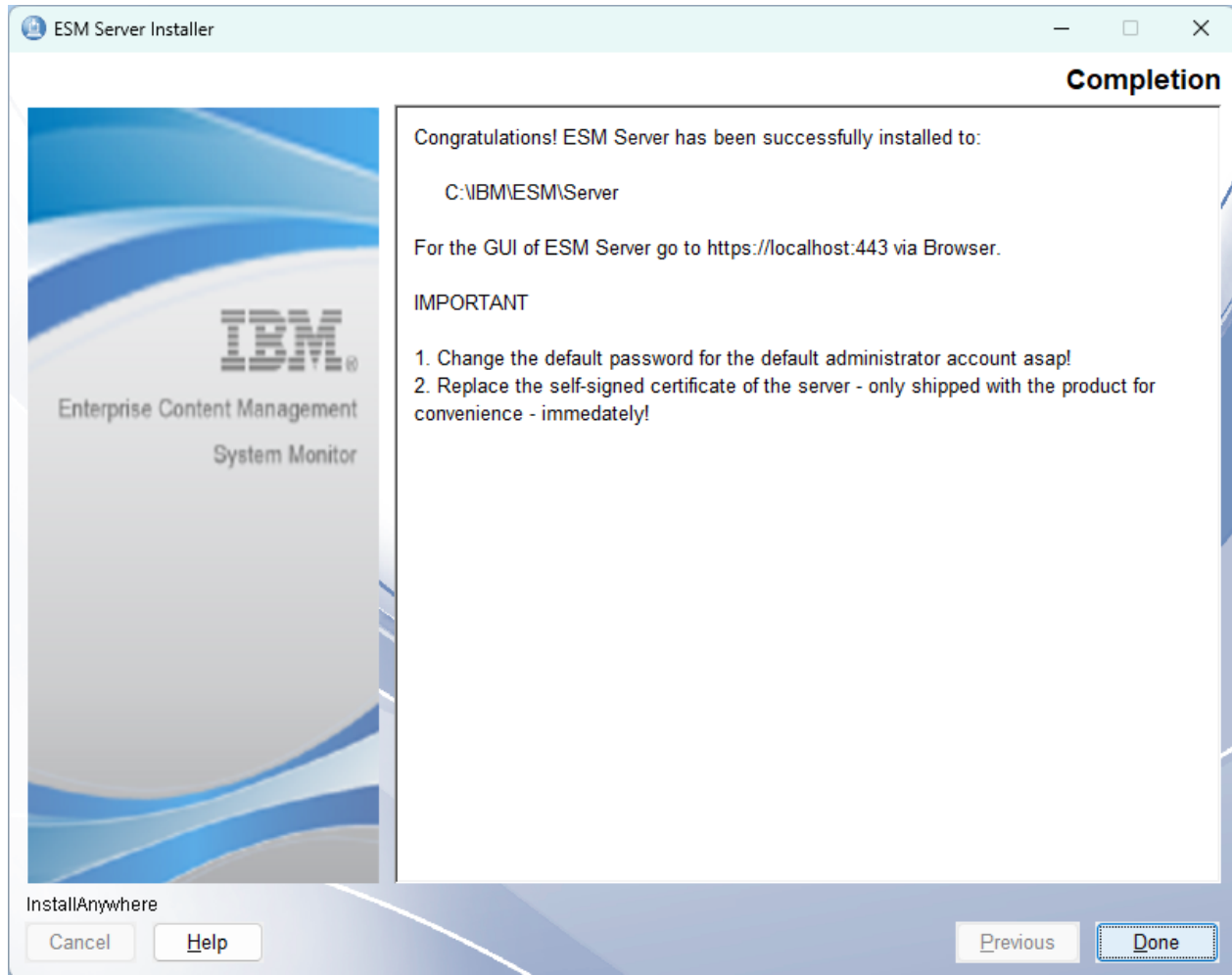


Image of Installation Complete

Linux based server

IMPORTANT | Ports < 1000 will only work for root based installations

- Start the installation by executing the file "ESM_Server_Installer.bin"
- The "Software License Agreement" window is loaded. Accept the license agreement and proceed with "Next".

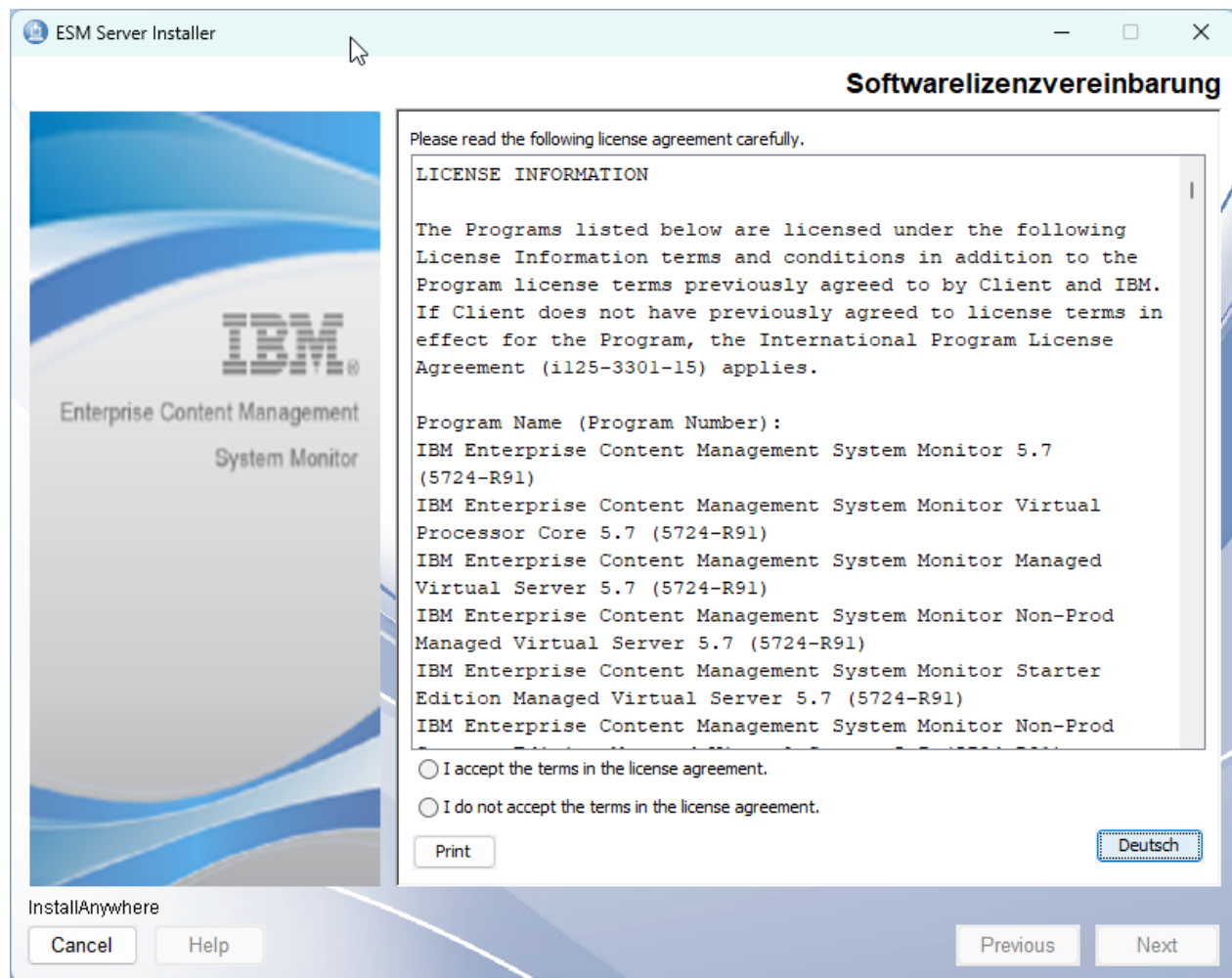


Image of Software License Agreement

- The next window is "Welcome to ESM Server". It shows some information about the installation. Click "Next" to proceed.



Image of Welcome to ESM Server

- The next window is "Choose Installation Folder". Specify your path for the installation here. The default is `/opt/IBM/ESM/Server`. Click "Next" to proceed.

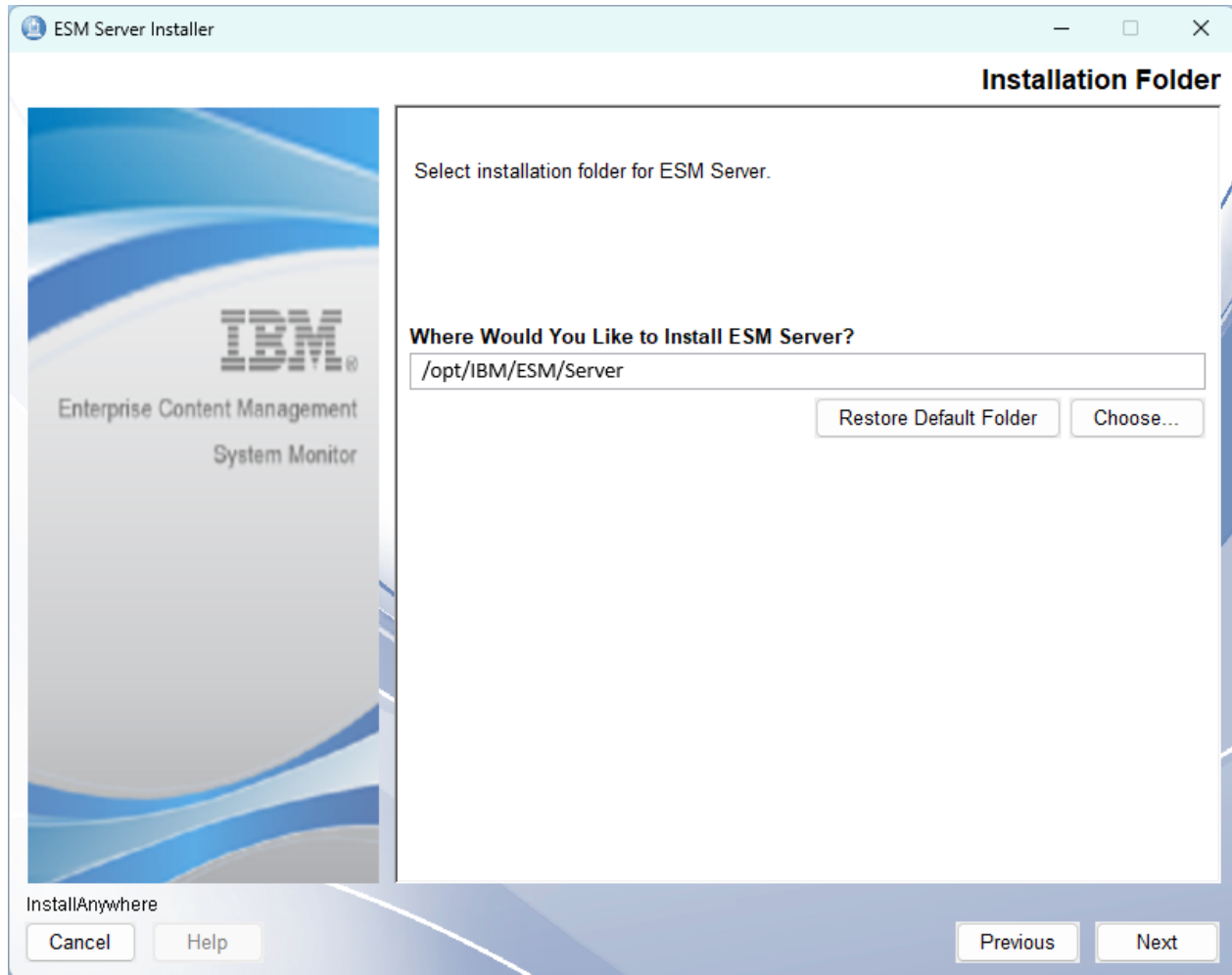


Image of Choose Installation Folder

- The next window is "Server Settings". The following parameters can be specified. Click "Next" to proceed. We recommend to keep https enabled.

Hostname

Default: `<server name>`

Server IP

Default: `0.0.0.0`

MQTT Port

Default: `1883`

HTTP Port

Default: `80`

HTTPS

Default: `Enabled`

HTTPS Port

Default: `443`

RMI Registry Port

Default: 1099

RMI Server Port

Default: 44444

SSH Port

Default: 8101

SSL KEY PASSWORD

Default: =password

SSL KEYSTORE PASSWORD

Default: =password

SSL TRUSTSTORE PASSWORD

Default: =password

ESM Server Installer

ESM Server Settings

Please enter ESM Server hostname and port numbers.

Please only change the passwords for SSL key and stores if you want to use a custom key- or truststore. Changes to the file path or store type must be made directly in the corresponding configuration file.

Hostname
localhost

IP Address
0.0.0.0

MQTT Port
1883

HTTP Port
80

HTTPS
☒ Enabled ☐ Disabled

HTTPS Port
443

RMI Registry Port
1099

InstallAnywhere

Cancel Help Previous Next

Image of Server Settings

- The next window is "Configuration Database Settings". The default settings are for usage with the internal H2 DB. DB2 and MSSQL is possible as well.

IMPORTANT

If the installation is done with DB2 or MSSQL, copy a suitable jdbc driver to <Installation-Dir>/karaf/deploy after a successful installation and start the software afterwards. The default settings must be changed to fit your MSSQL or DB2 database.

JDBC Url

Default:

`jdbc:h2:./configuration;AUTO_SERVER=TRUE;AUTO_RECONNECT=TRUE;LOCK_TIMEOUT=10000;MODE=LEGACY`

Database Driver Class Name

Default: `org.h2.Driver`

Database Username

Default: `db`

Database Password

Default: `pw is hidden`

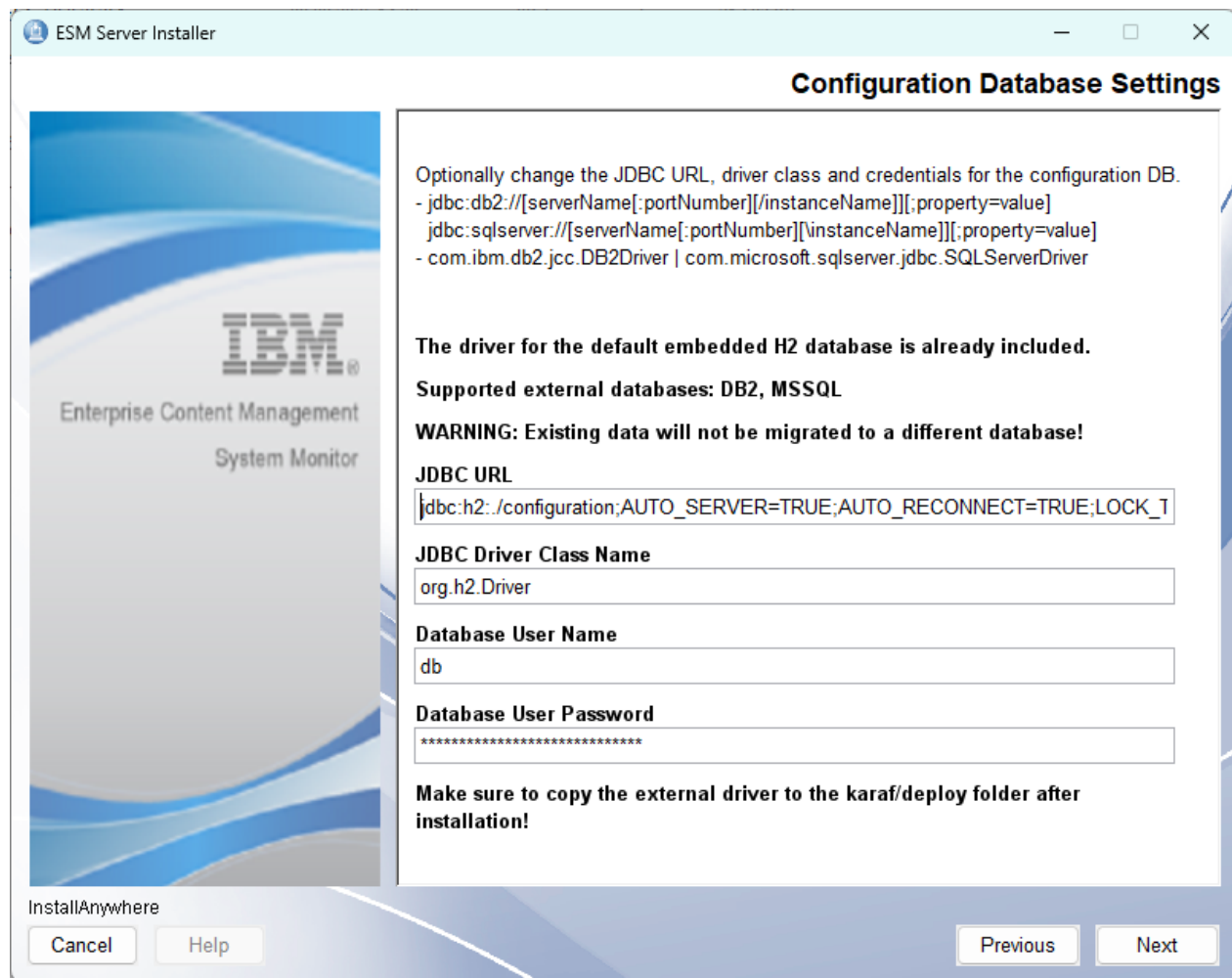


Image of Configuration Database Settings

- The next window is "Monitoring Database Settings". The default settings are for usage with the internal H2 DB. DB2 and MSSQL is possible as well.

IMPORTANT

If the installation is done with DB2 or MSSQL, copy a suitable jdbc driver to <Installation-Dir>/karaf/deploy after a successful installation and start the software afterwards. The default settings must be changed to fit your MSSQL or DB2 database.

JDBC Uri

Default:
`jdbc:h2:./monitoring;AUTO_SERVER=TRUE;AUTO_RECONNECT=TRUE;LOCK_TIMEOUT=10000;MODE=LEGACY`

Database Driver Class Name

Default: `org.h2.Driver`

Database Username

Default: *db*

Database Password

Default: *pw is hidden*

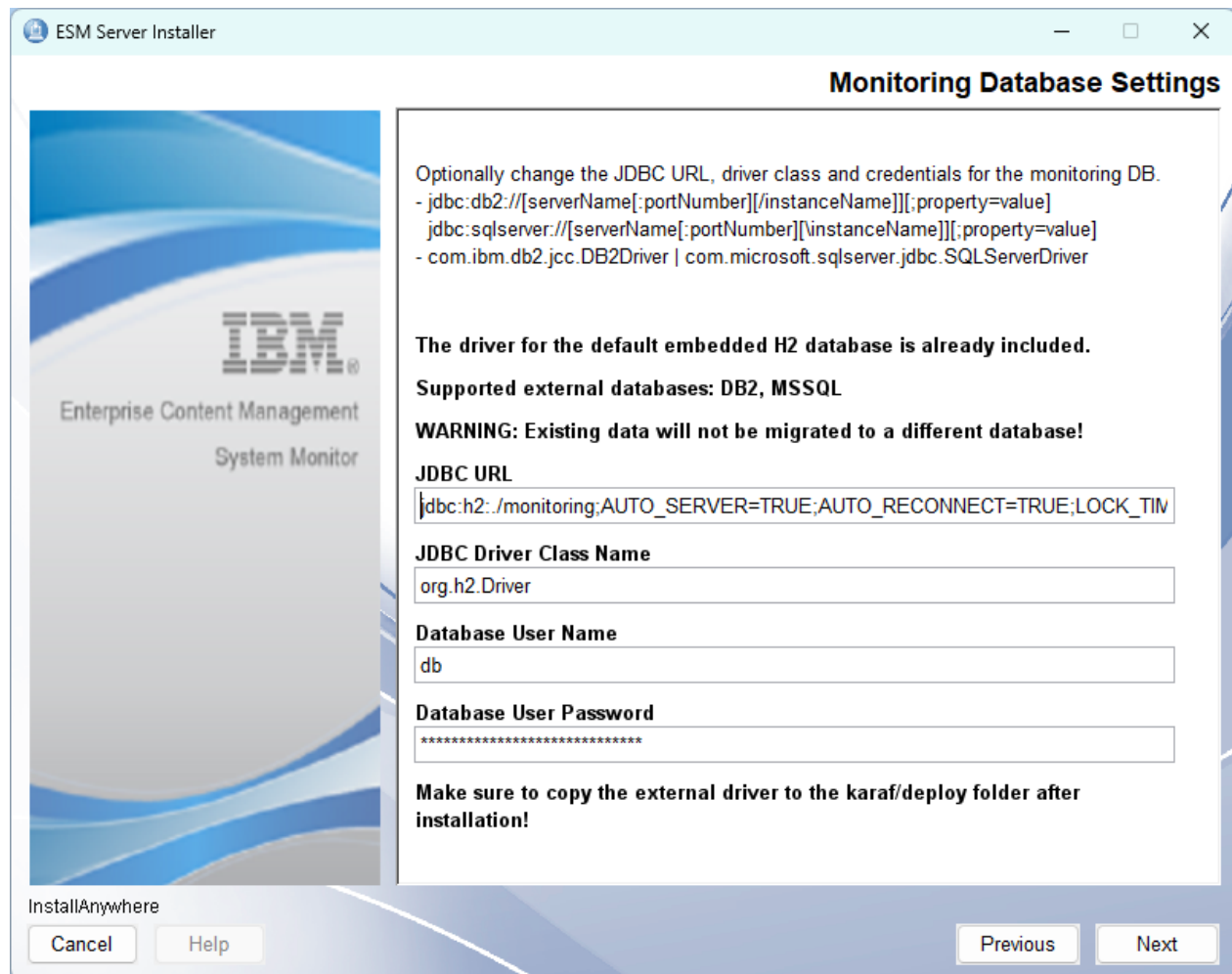


Image of Monitoring Database Settings

- The next window is "Autostart and Systemstart". The following parameters can be specified. Click "Next" to proceed.

Start ESM Server after Installation

Default: Yes = checked

Start ESM Server at OS Start

Default: Yes = unchecked

NOTE

If unchecked, the no service entry is created in inittab or systemctl. Also root rights are needed for this.

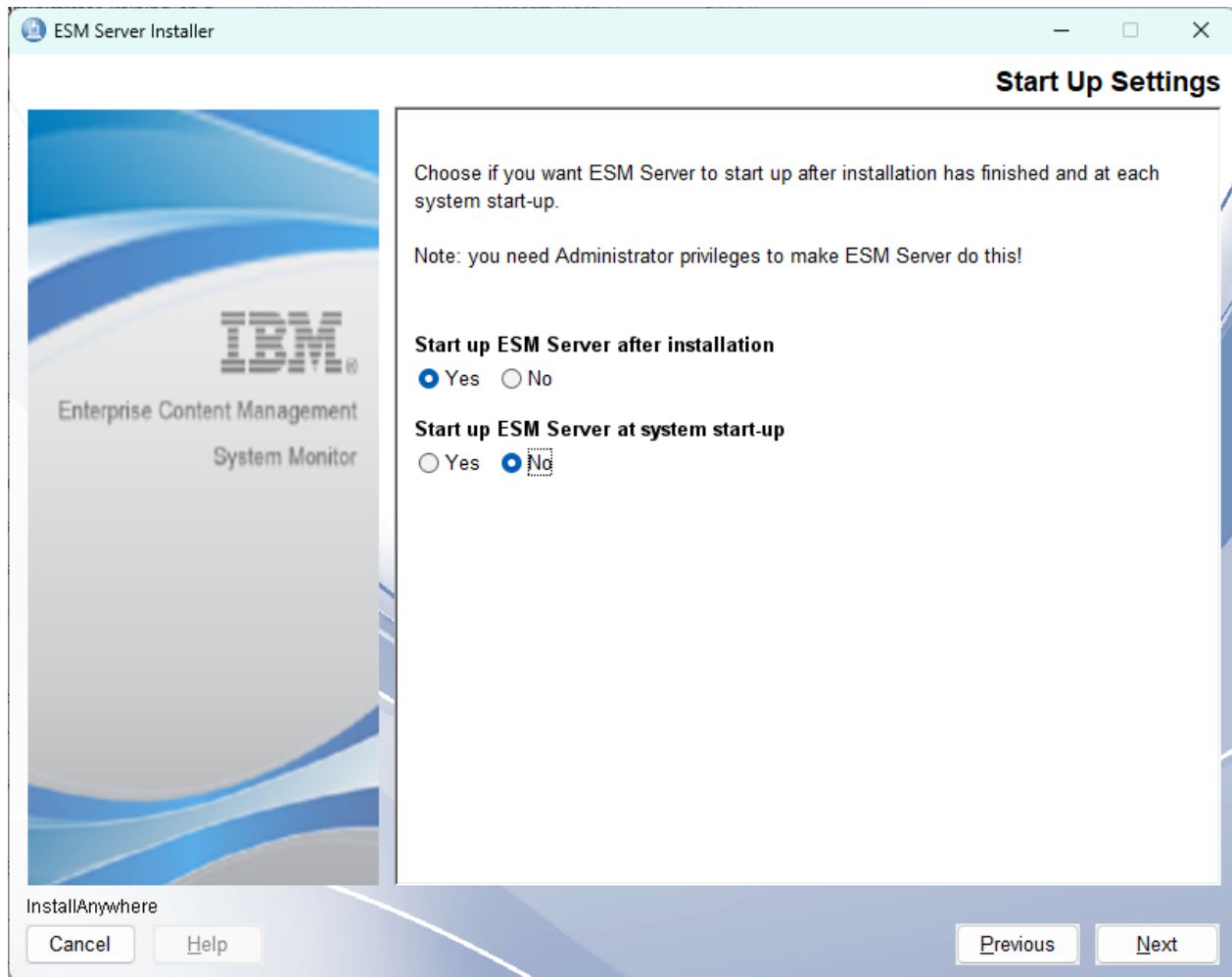


Image of Autostart and Systemstart

- The next window is "Pre-Installation Summary". Click "Install" to proceed.

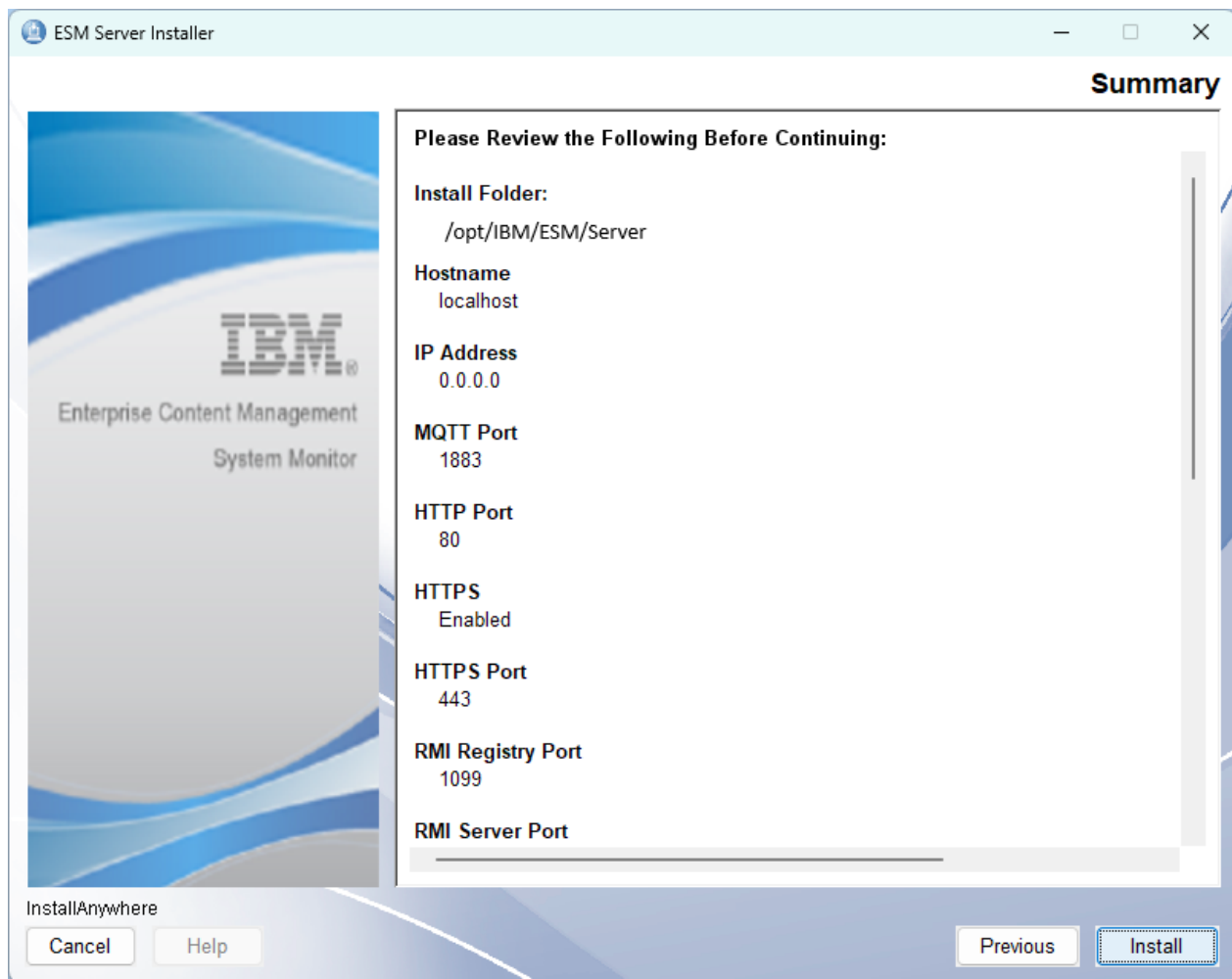


Image of Pre-Installation Summary

- The installation starts and finishes with the window "Install Complete". Click "Done" to close and finish the installation procedure.

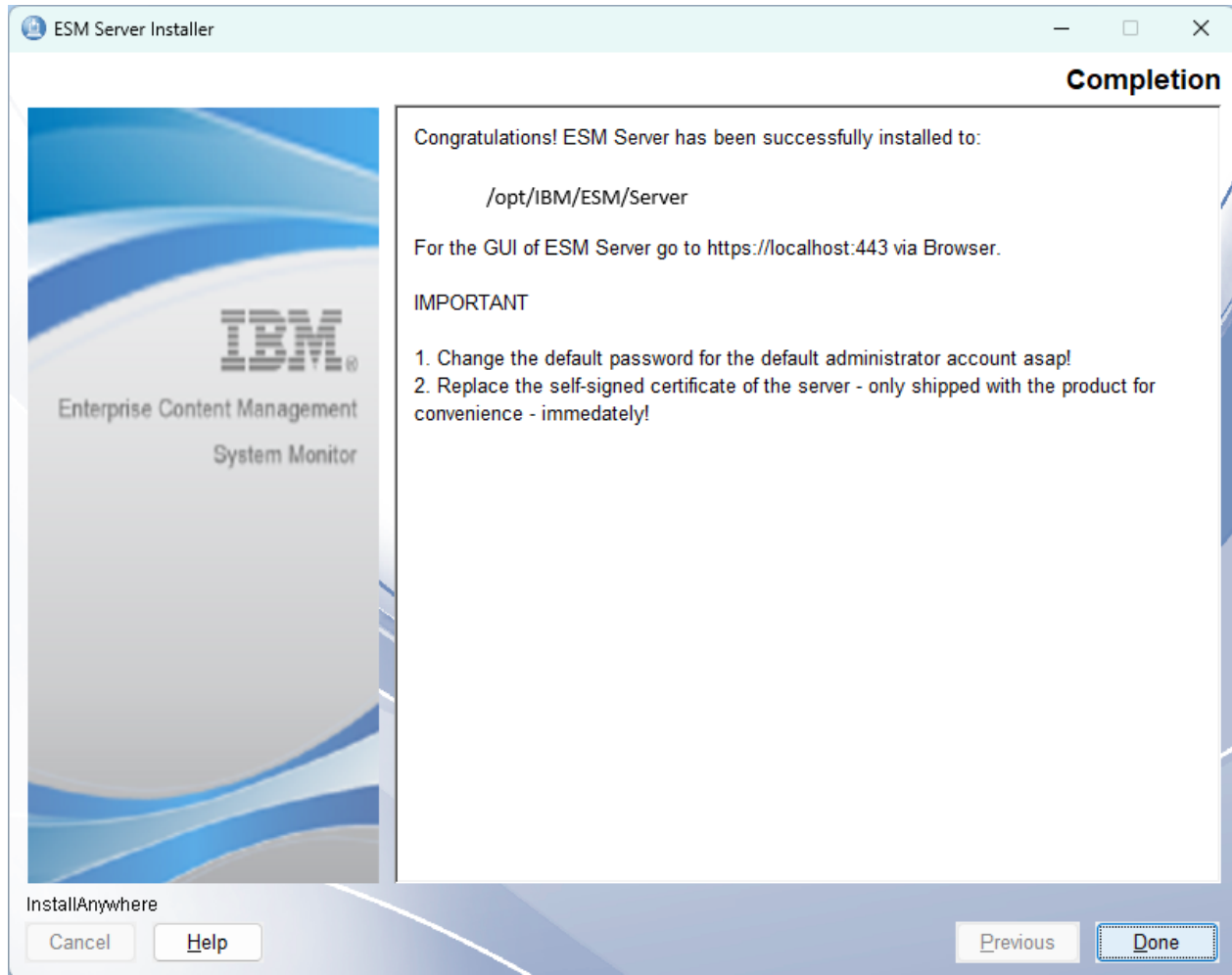


Image of Installation Complete

IMPORTANT

If the installation was done with DB2, copy a suitable jdbc driver to <Installation-Dir>/karaf/deploy and start the software afterwards.

Windows based agent

- Start the installation by executing the file "ESM_Agent_Installer.exe" as administrator.
- The "Software License Agreement" window is loaded. Accept the license agreement and proceed with "Next".

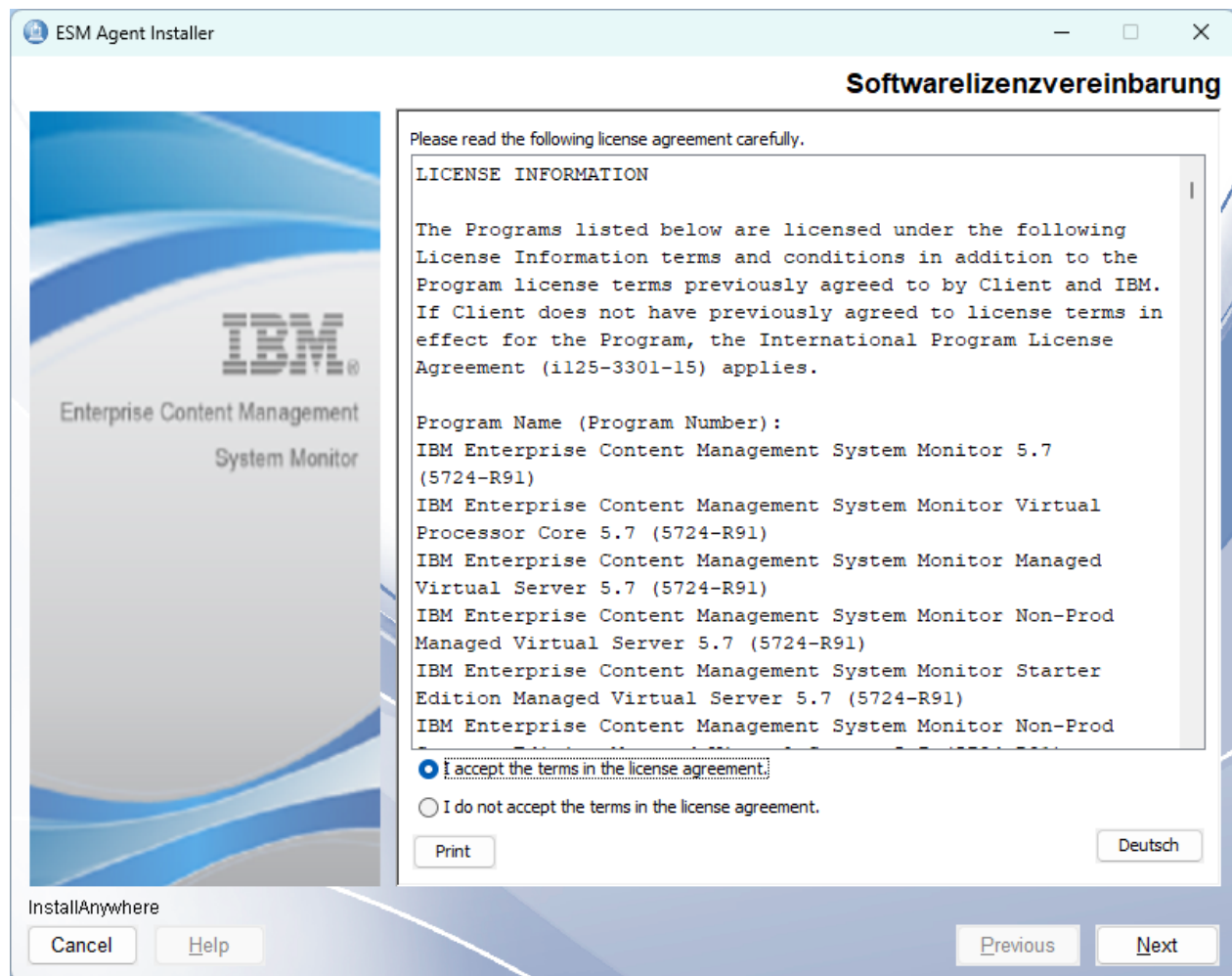


Image of Software License Agreement

- The next window is "Welcome to ESM Agent". It shows some information about the installation. Click "Next" to proceed.

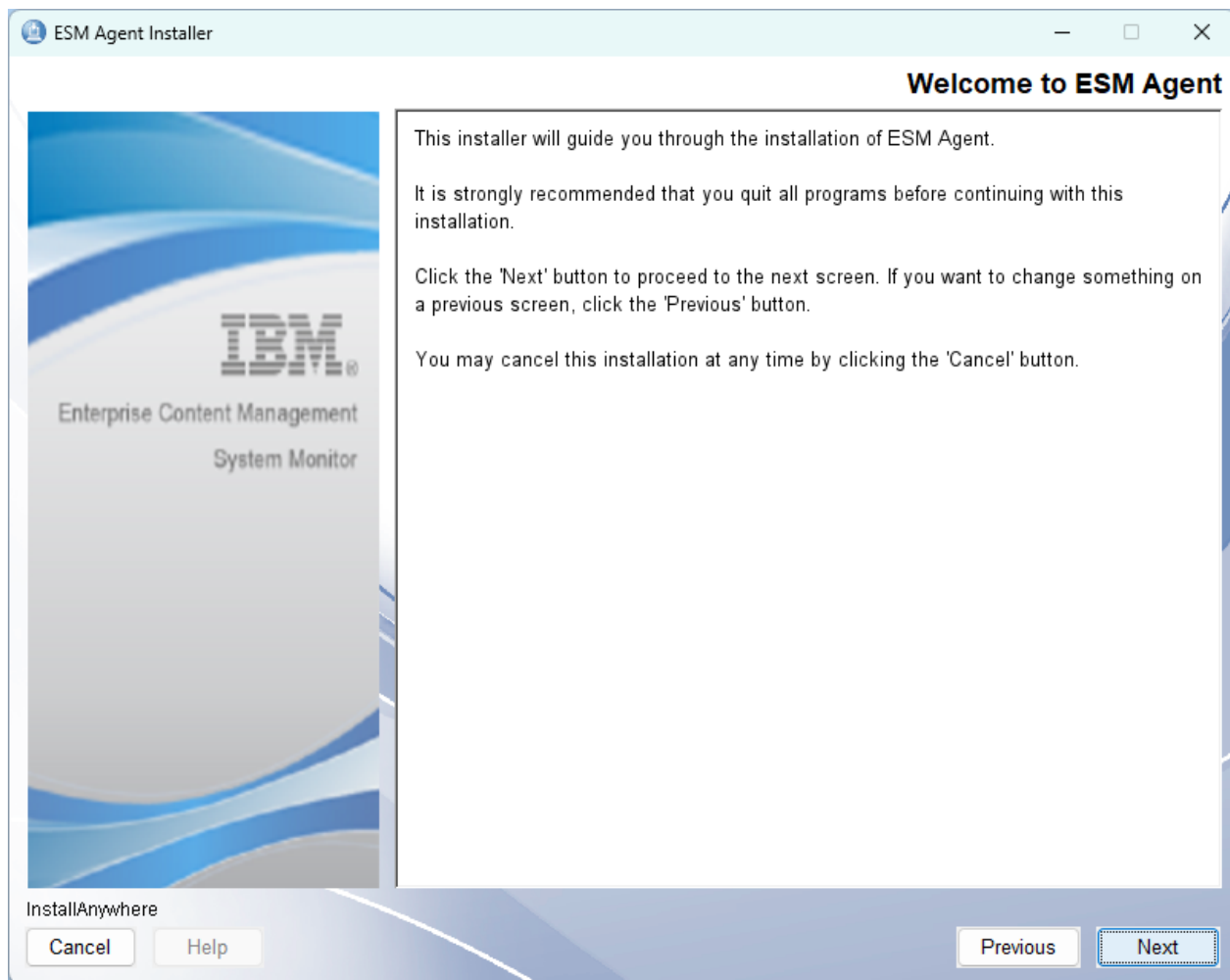


Image of Welcome to ESM Agent

- The next window is "Choose Installation Folder". Specify your path for the installation here. The default is `C:\Program Files\IBM\ESM\Agent`. Click "Next" to proceed.

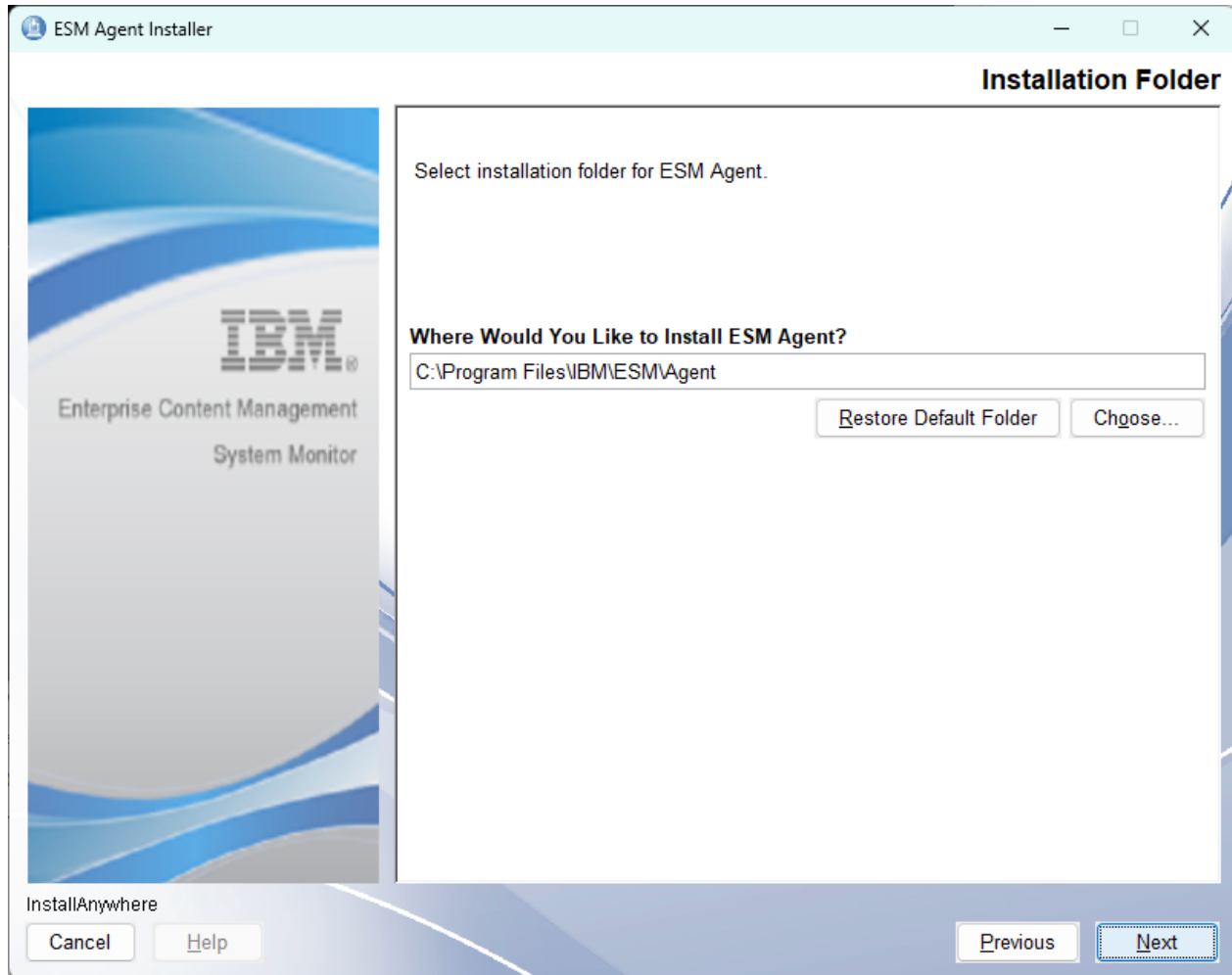


Image of Choose Installation Folder

- The next window is "Enter Agent Name, Hostname and Ports". The following parameters can be specified. Click "Next" to proceed. We recommend to keep https enabled.

Unique Agent Name

Default: *EsmAgent*

ESM Server Name

Default: *localhost*

Server Port

Default: *1883*

Http Port

Default: *1180*

Https Port

Default: *1543*

RMI Registry Port

Default: *2099*

RMI Server Port

Default: 55555

SSH Port

Default: 9202

SSL KEY PASSWORD

Default: =password

SSL KEYSTORE PASSWORD

Default: =password

SSL TRUSTSTORE PASSWORD

Default: =password

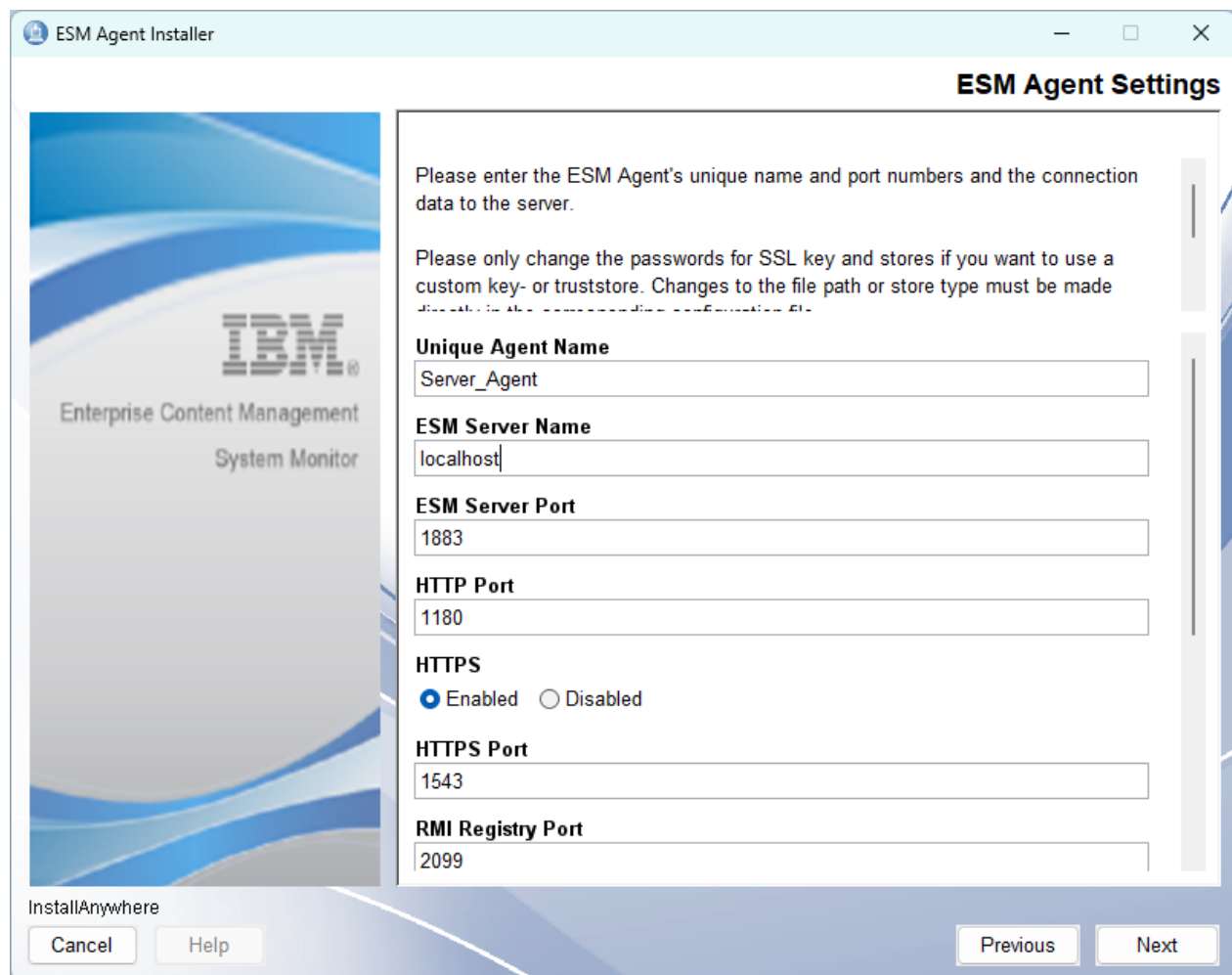


Image of Agent Settings (1)

- The next window is "Autostart and Systemstart". The following parameters can be specified. Click "Next" to proceed.

Start ESM Agent after Installation

Default: Yes = checked

Start at OS Start

Default: Yes = unchecked

NOTE | If unchecked, the service will be installed with manual startup type.

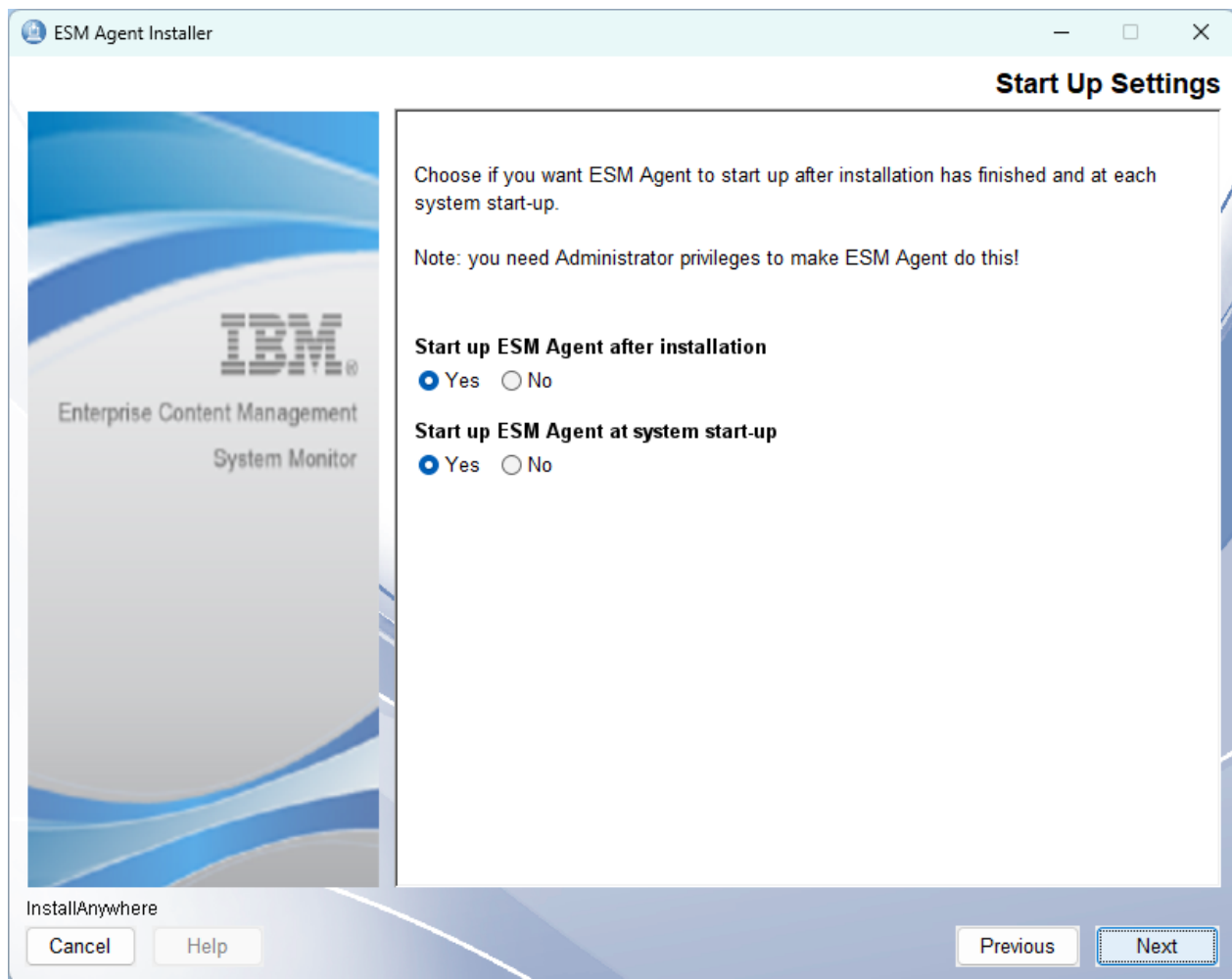


Image of Autotstart and Systemstart

- The next window is "Service Installation". The following parameters can be specified. Click "Next" to proceed.

Re-Install ESM Agent Service

Default: No = checked

NOTE

This Window will only be shown if the OS is Windows, the installation is an update installation and a service is used in the previous installation already.

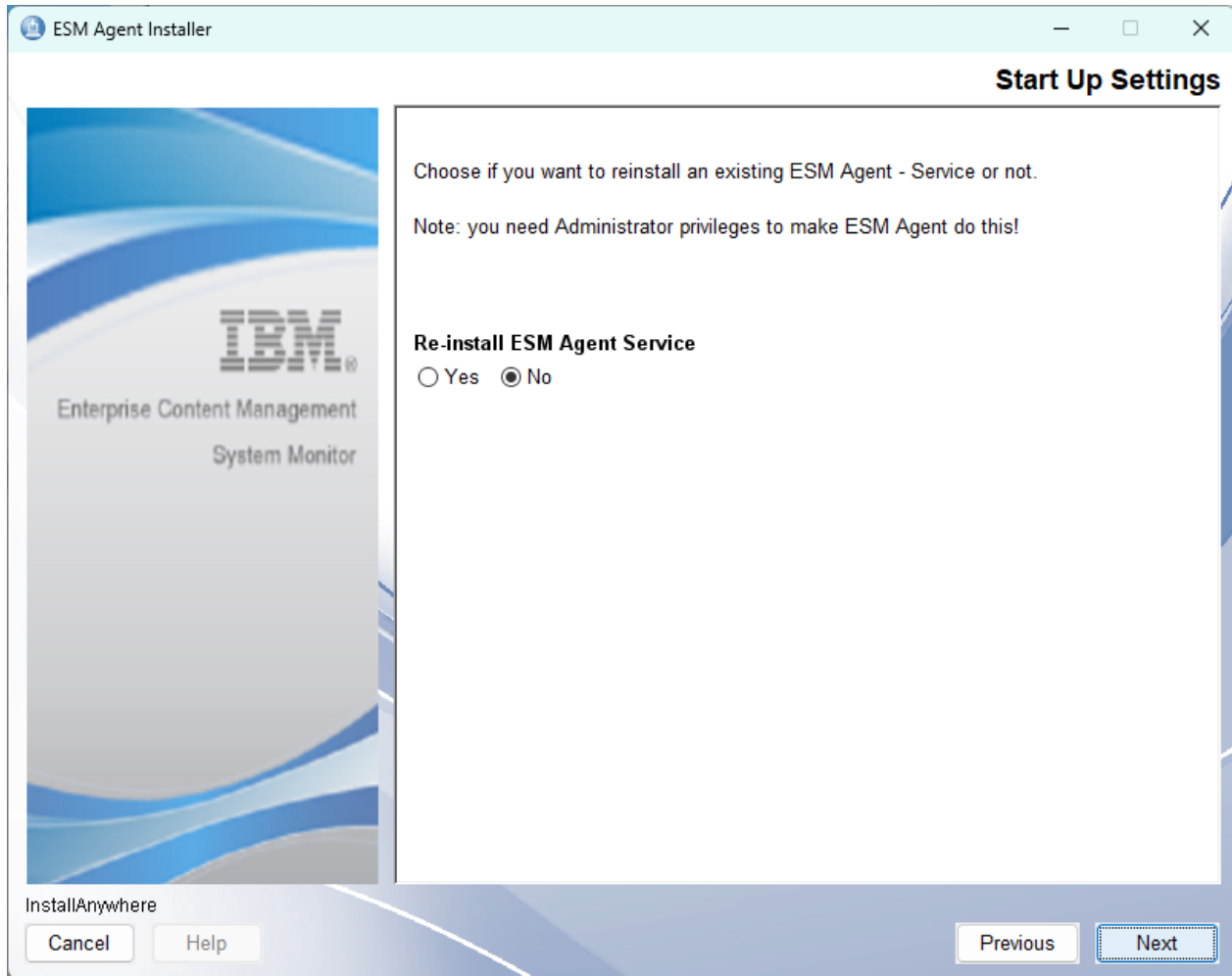


Image of Service Installation

- The next window is "Pre-Installation Summary". Click "Install" to proceed.

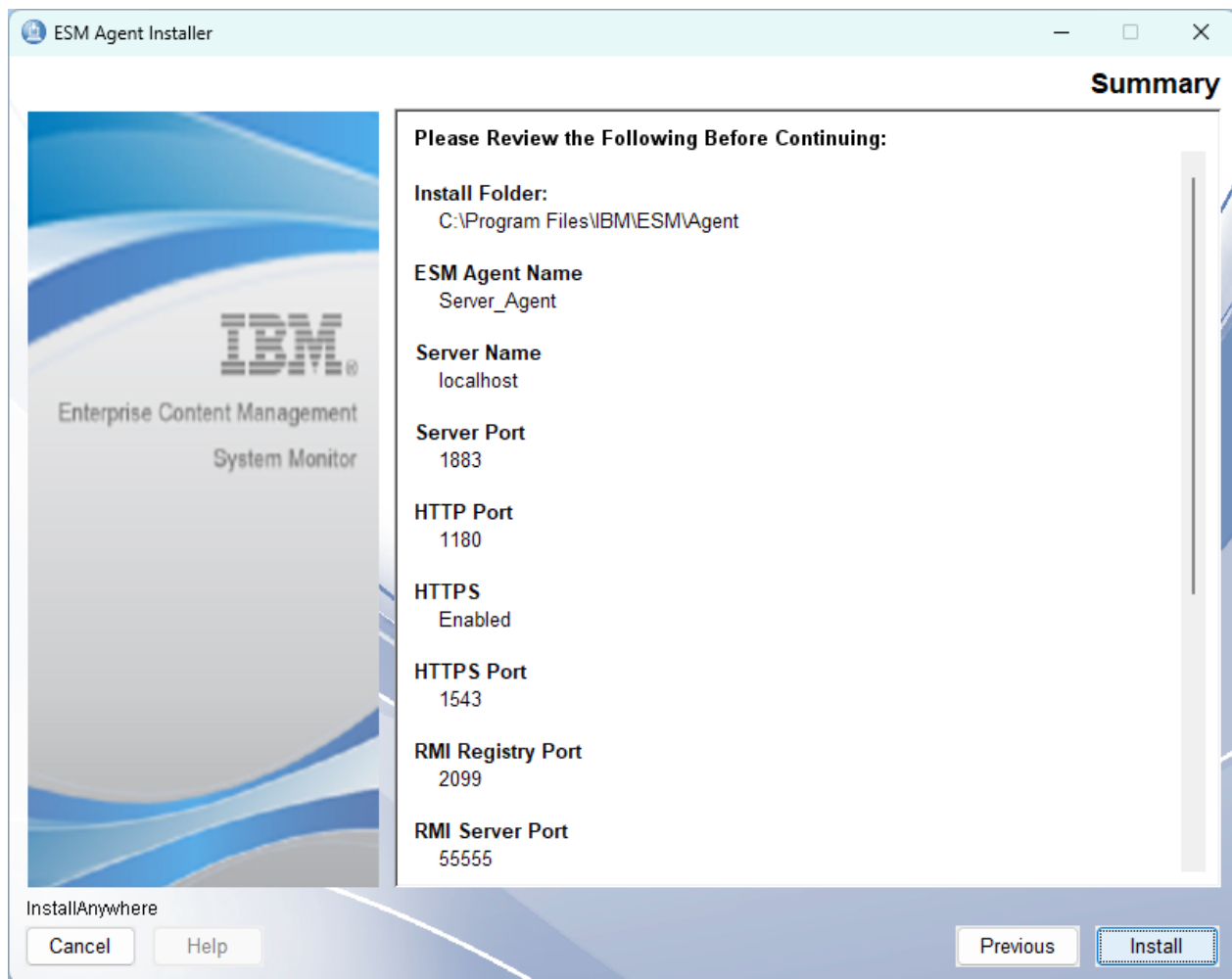


Image of Pre-installation Summary

- The installation starts and finishes with the window "Install Complete". Click "Done" to close and finish the installation procedure.

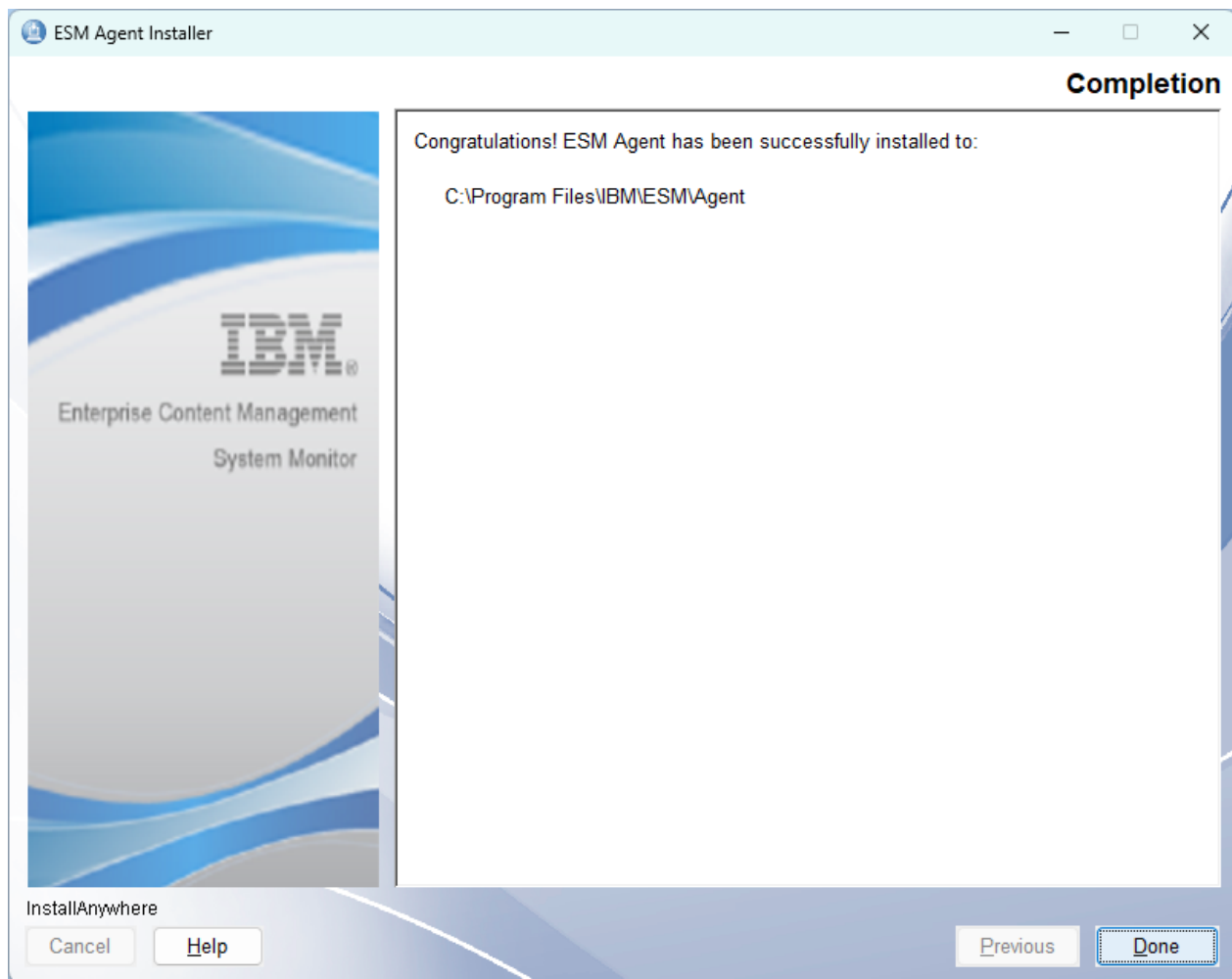


Image of Installation Complete

NOTE

Every Agent that connects to an ESM server for the first time, will automatically have basic monitoring activated. Per default 3 probes (cpu, memory and disk space) will run. For more details see the Probes and Situation Guide chapter "Default (standard) base probes for all agent".

Linux based agent

- Start the installation by executing the file "ESM_Agent_Installer.bin"
- The "Software License Agreement" window is loaded. Accept the license agreement and proceed with "Next".

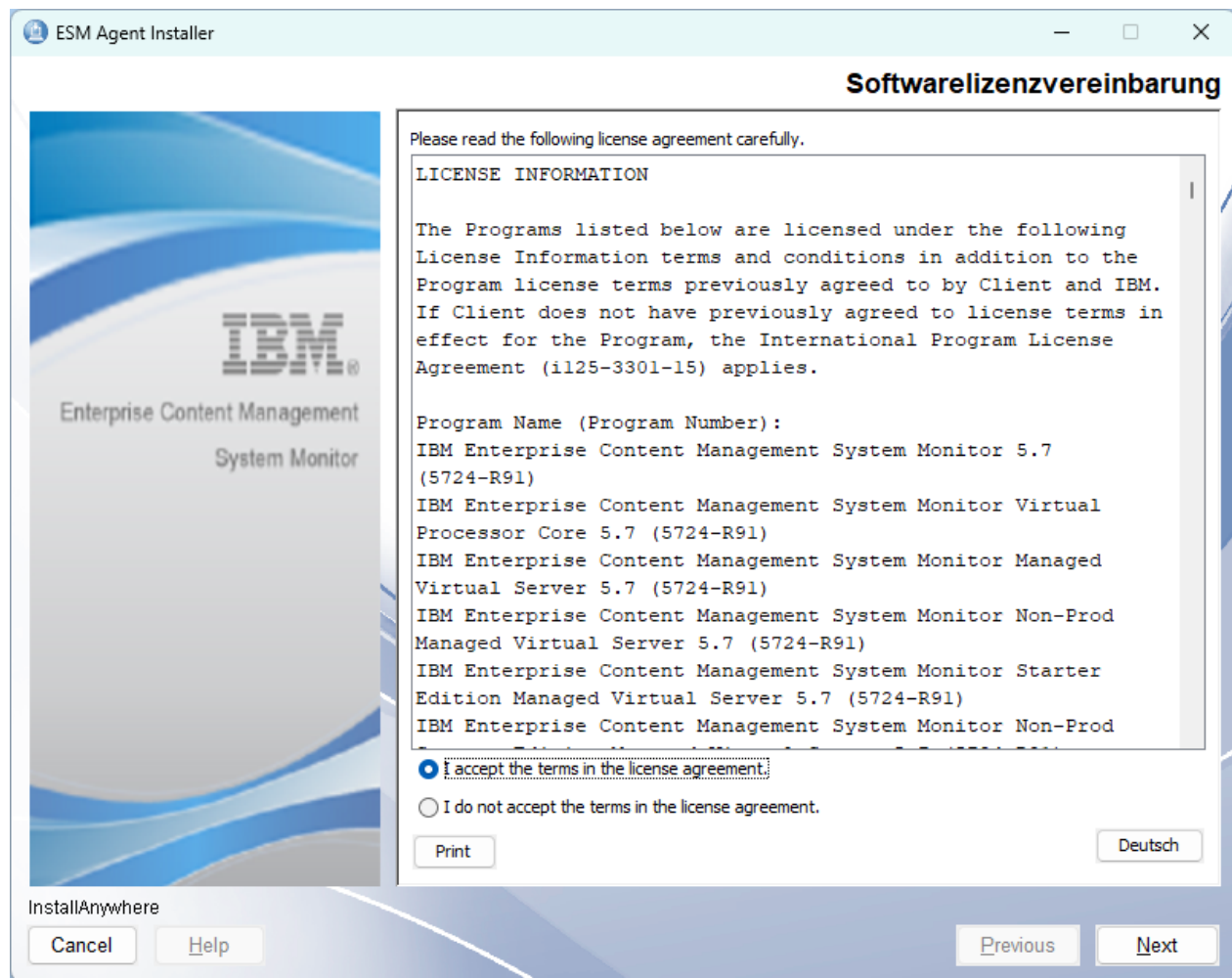


Image of Software License Agreement

- The next window is "Welcome to ESM Agent". It shows some information about the installation. Click "Next" to proceed.

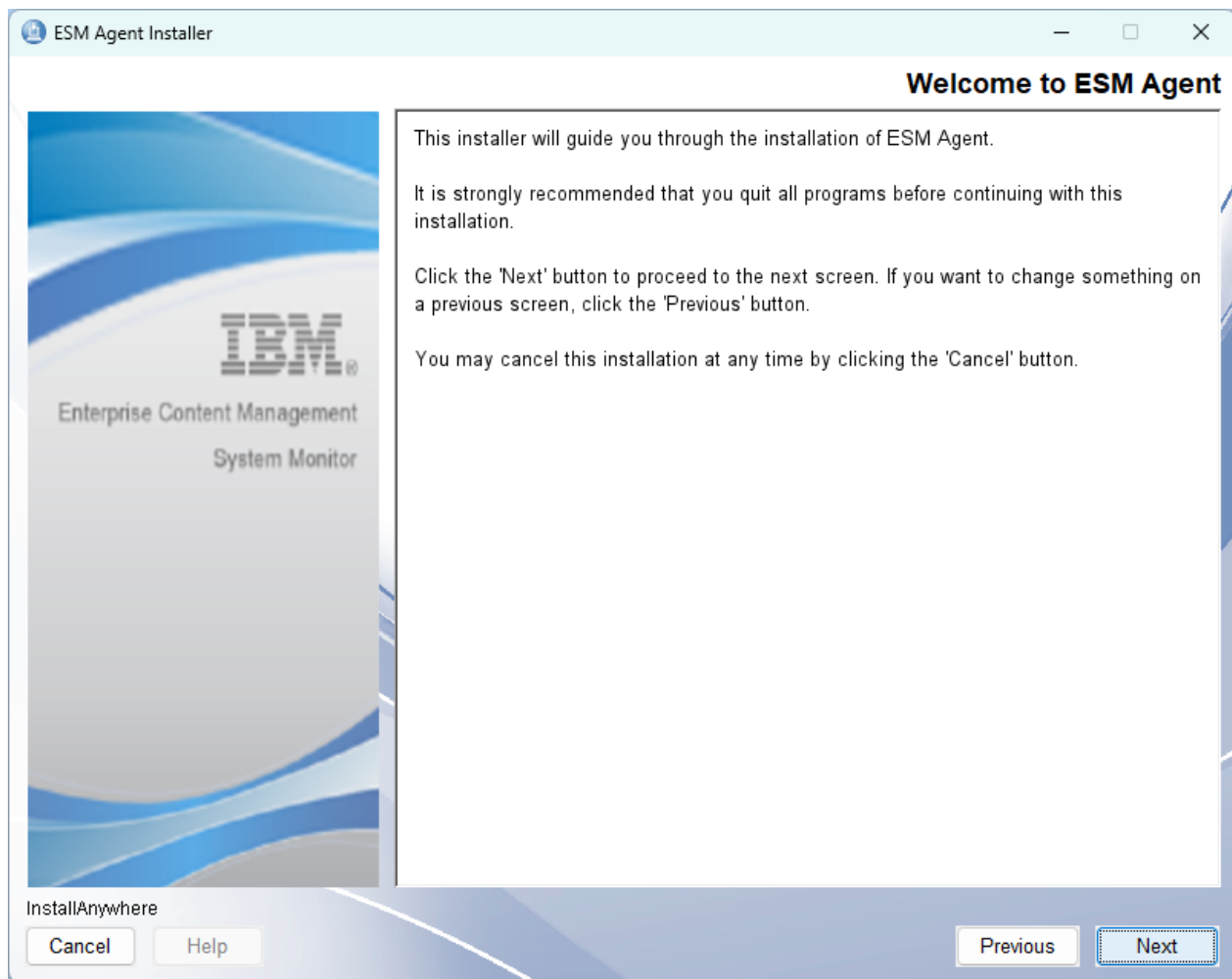


Image of Welcome to ESM Agent

- The next window is "Choose Installation Folder". Specify your path for the installation here. The default is `/opt/IBM/ESM/Agent`. Click "Next" to proceed.

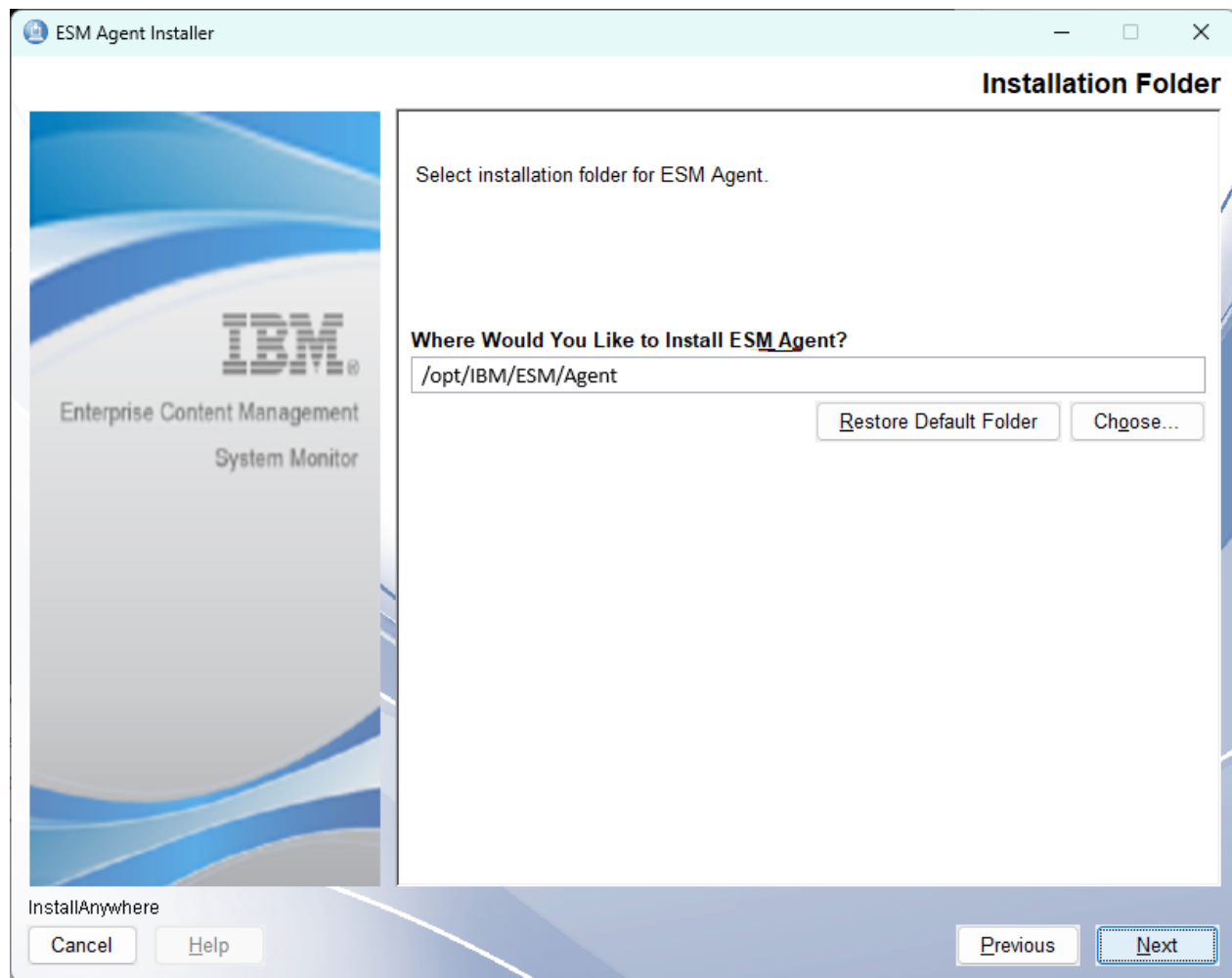


Image of Choose Installation Folder

- The next window is "Enter Agent Name, Hostname and Ports". The following parameters can be specified. Click "Next" to proceed. We recommend to keep https enabled.

Unique Agent Name

Default: *EsmAgent*

ESM Server Name

Default: *localhost*

Server Port

Default: *1883*

Http Port

Default: *1180*

Https Port

Default: *1543*

RMI Registry Port

Default: *2099*

RMI Server Port

Default: 55555

SSH Port

Default: 9202

SSL KEY PASSWORD

Default: =password

SSL KEYSTORE PASSWORD

Default: =password

SSL TRUSTSTORE PASSWORD

Default: =password

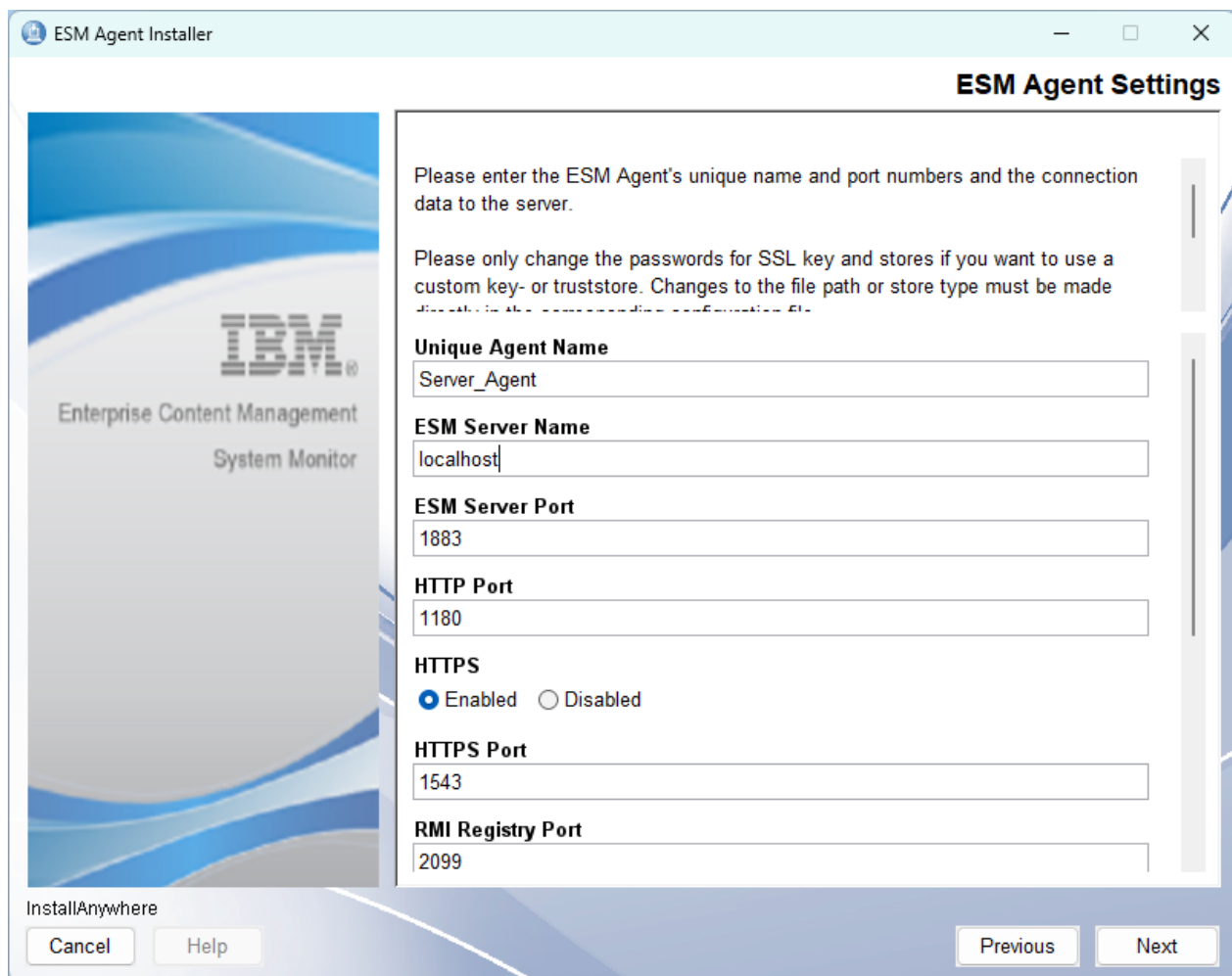


Image of Agent Settings (1)

- The next window is "Autostart and Systemstart". The following parameters can be specified. Click "Next" to proceed.

Start ESM Agent after Installation

Default: Yes = checked

Start at OS Start

Default: Yes = unchecked

NOTE

If unchecked, the no service entry is created in inittab or systemctl. Also root rights are needed for this.

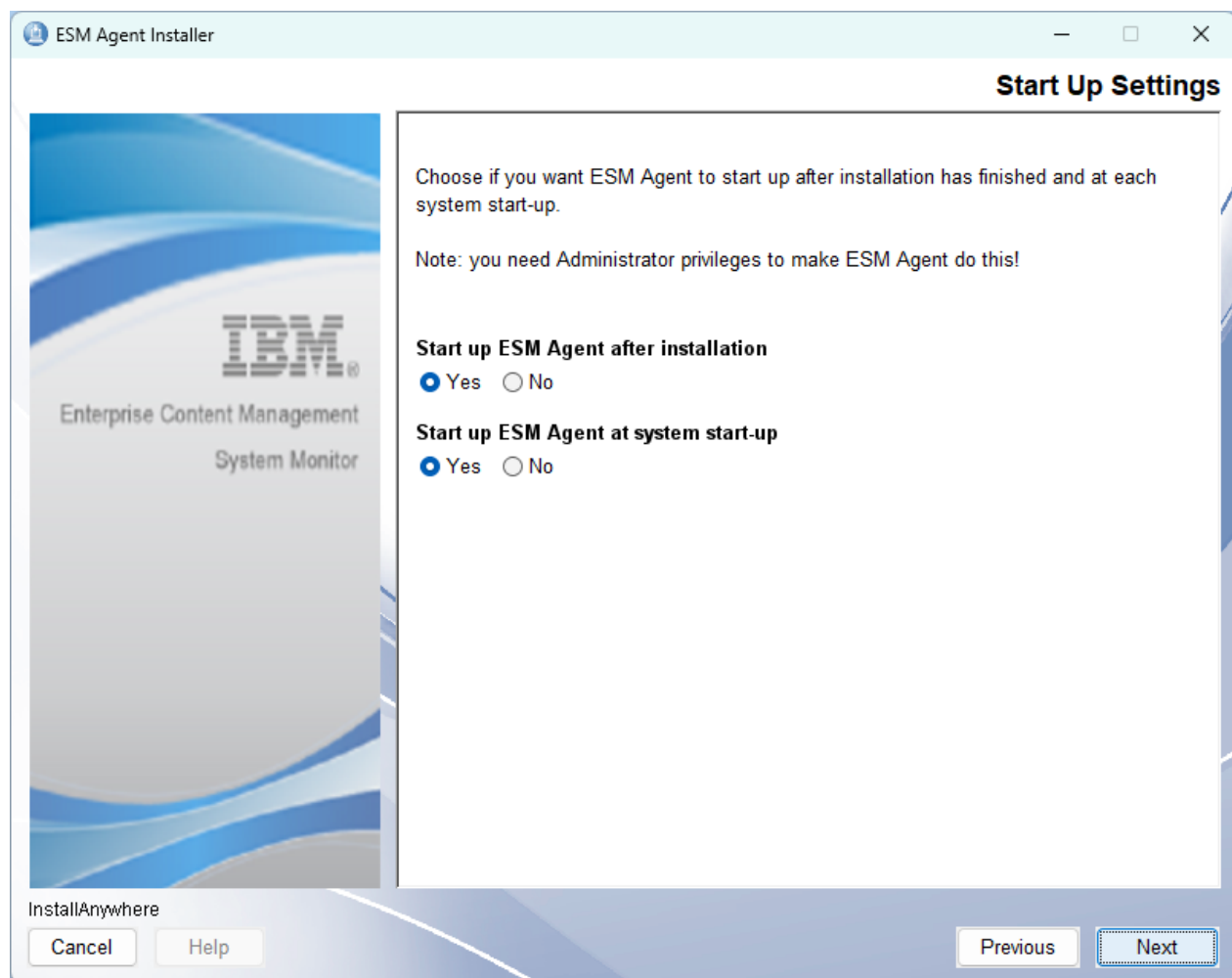


Image of Autotstart and Systemstart

- The next window is "Pre-Installation Summary". Click "Install" to proceed.

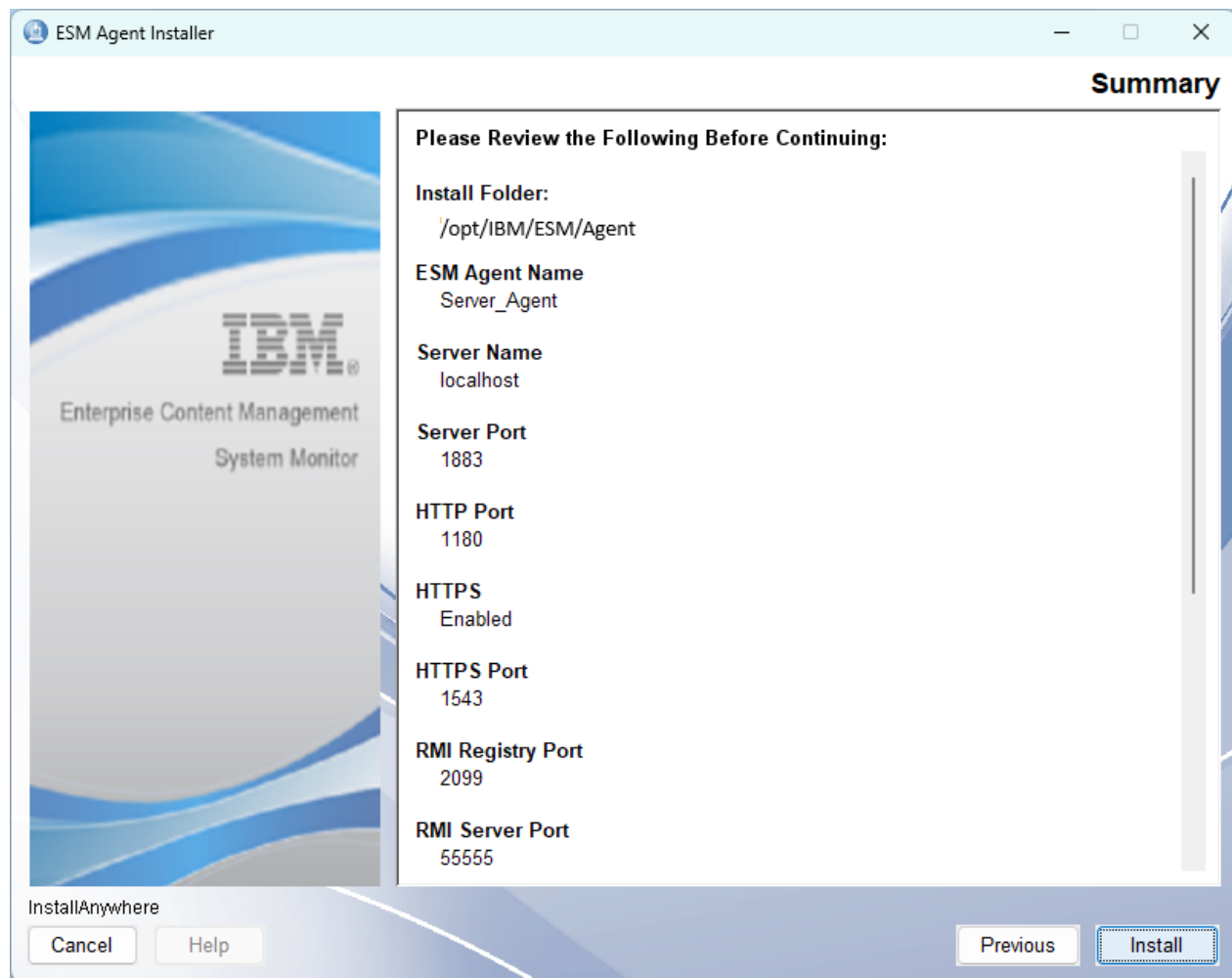


Image of Pre-installation Summary

- The installation starts and finishes with the window "Install Complete". Click "Done" to close and finish the installation procedure.

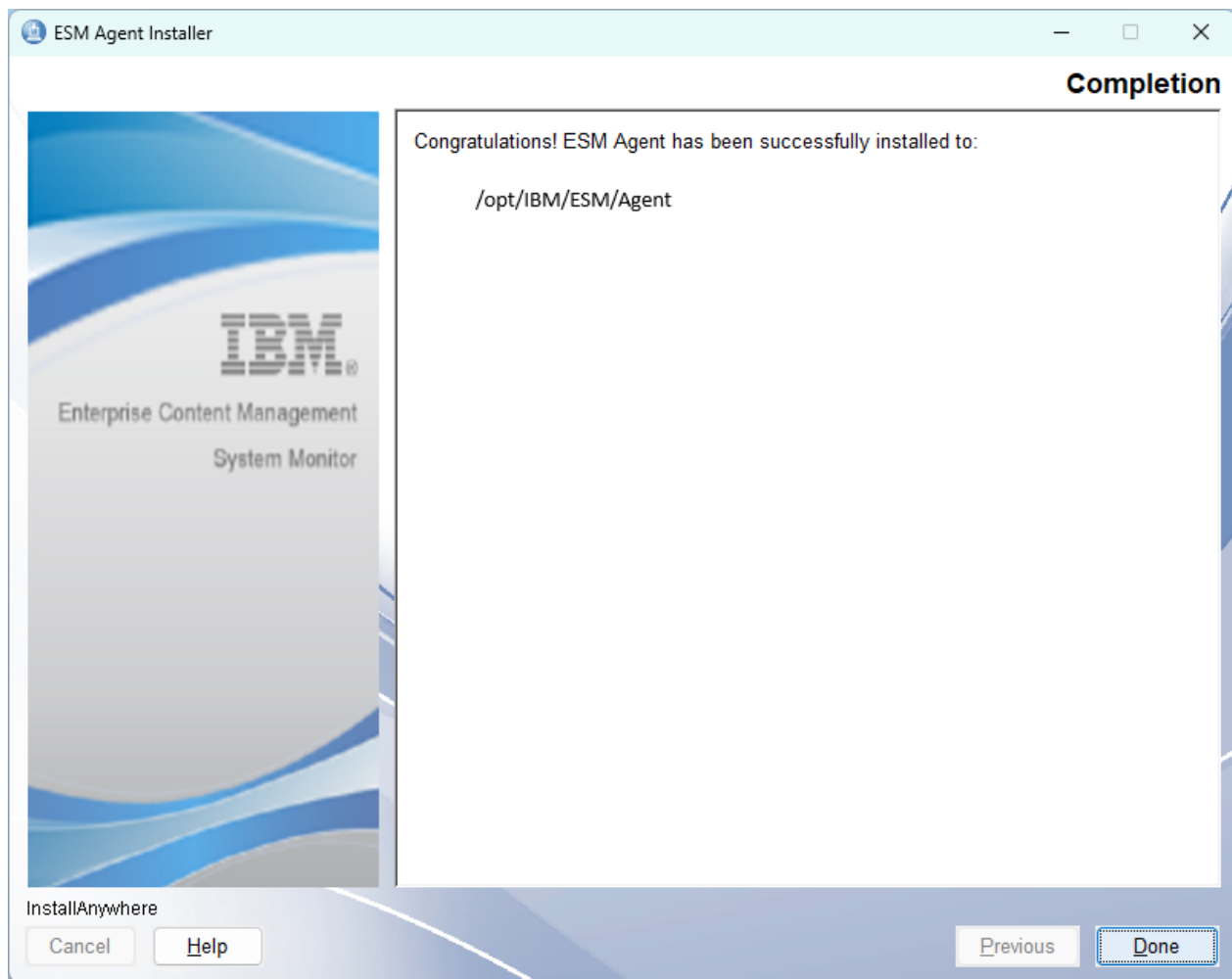


Image of Installation Complete

NOTE

Every Agent that connects to an ESM server for the first time, will automatically have basic monitoring activated. Per default 3 probes (cpu, memory and disk space) will run. For more details see the Probes and Situation Guide chapter "Default (standard) base probes for all agent".

AIX based agent

IMPORTANT

Large page support must be activated before the product can be installed.

NOTE

In some cases we have seen issues when installing on AIX. Typically, you can see an error message that "Graphical Installers are not supported by th VM". This is often combined with the context "User interface mode not supported" and "Unable to load and to prepare the installer in console or silent mode."

If that happens, try to unset the LIBPATH and DISPLAY variable and run the installer in silent or console mode. A typical cause is that the LIBPATH is set to /opt/freeware/lib as first entry.

- Start the installation by executing the file "ESM_Agent_Installer.bin"
- The "Software License Agreement" window is loaded. Accept the license agreement and proceed with "Next".

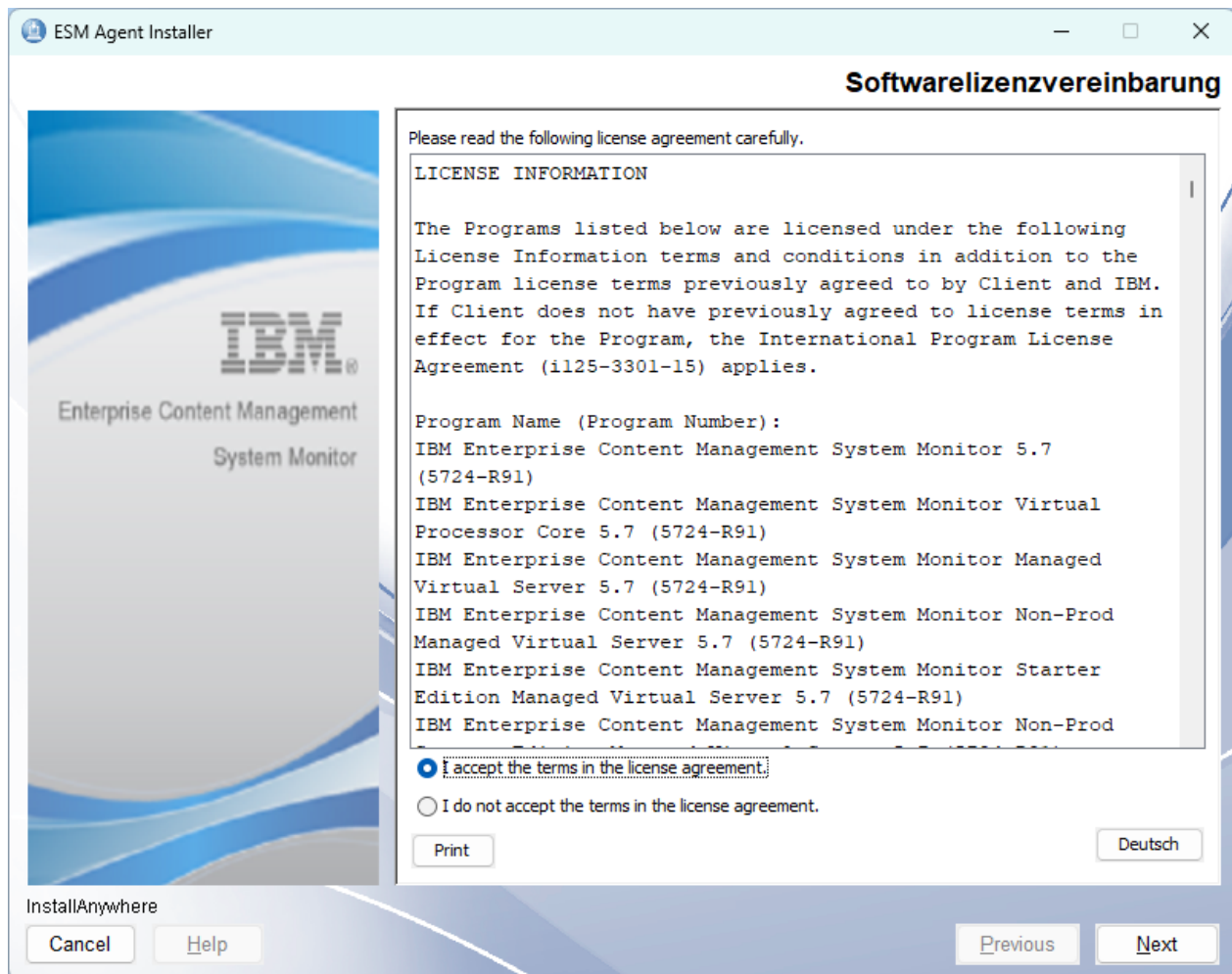


Image of Software License Agreement

- The next window is "Welcome to ESM Agent". It shows some information about the installation. Click "Next" to proceed.

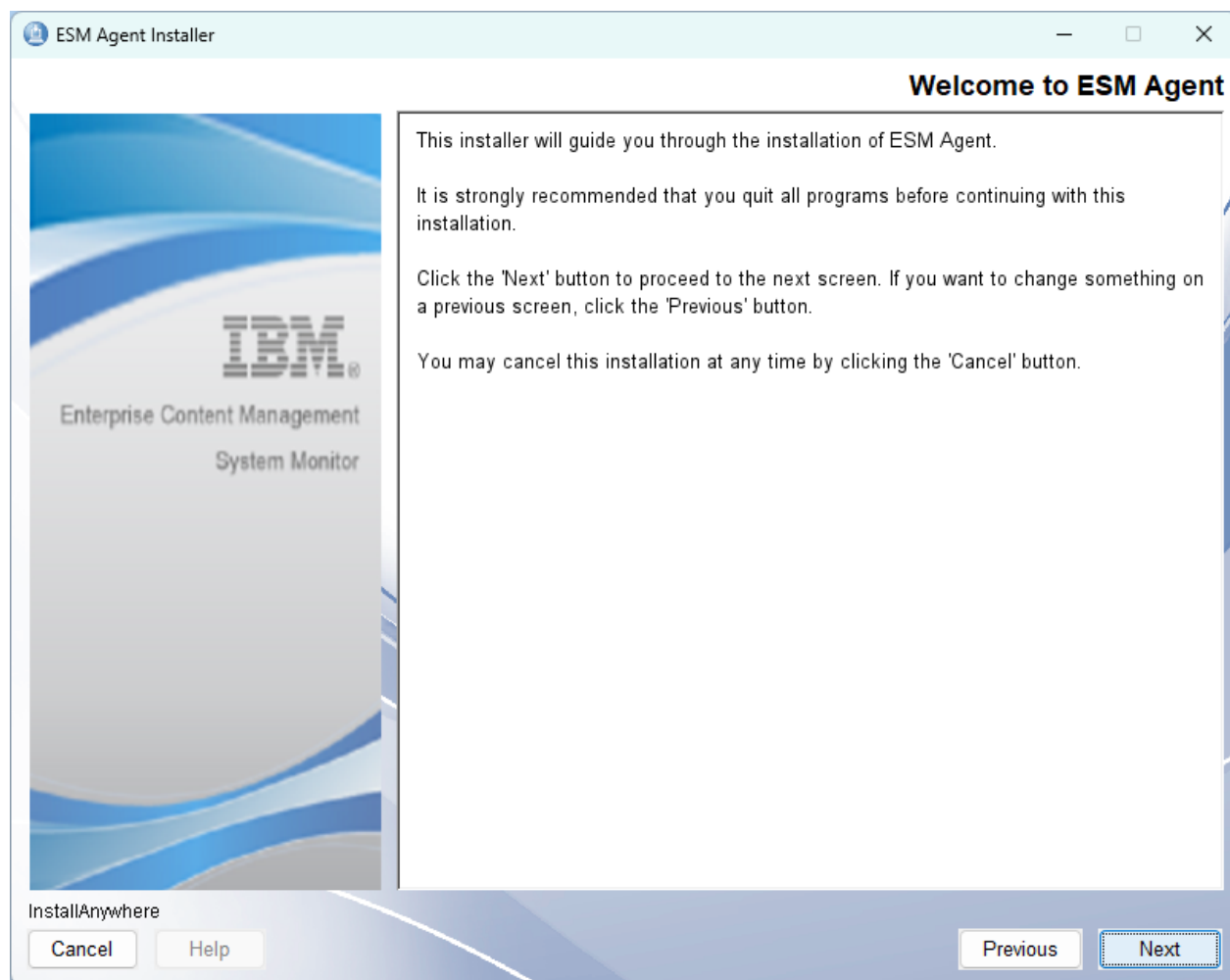


Image of Welcome to ESM Agent

- The next window is "Choose Installation Folder". Specify your path for the installation here. The default is `/opt/IBM/ESM/Agent`. Click "Next" to proceed.

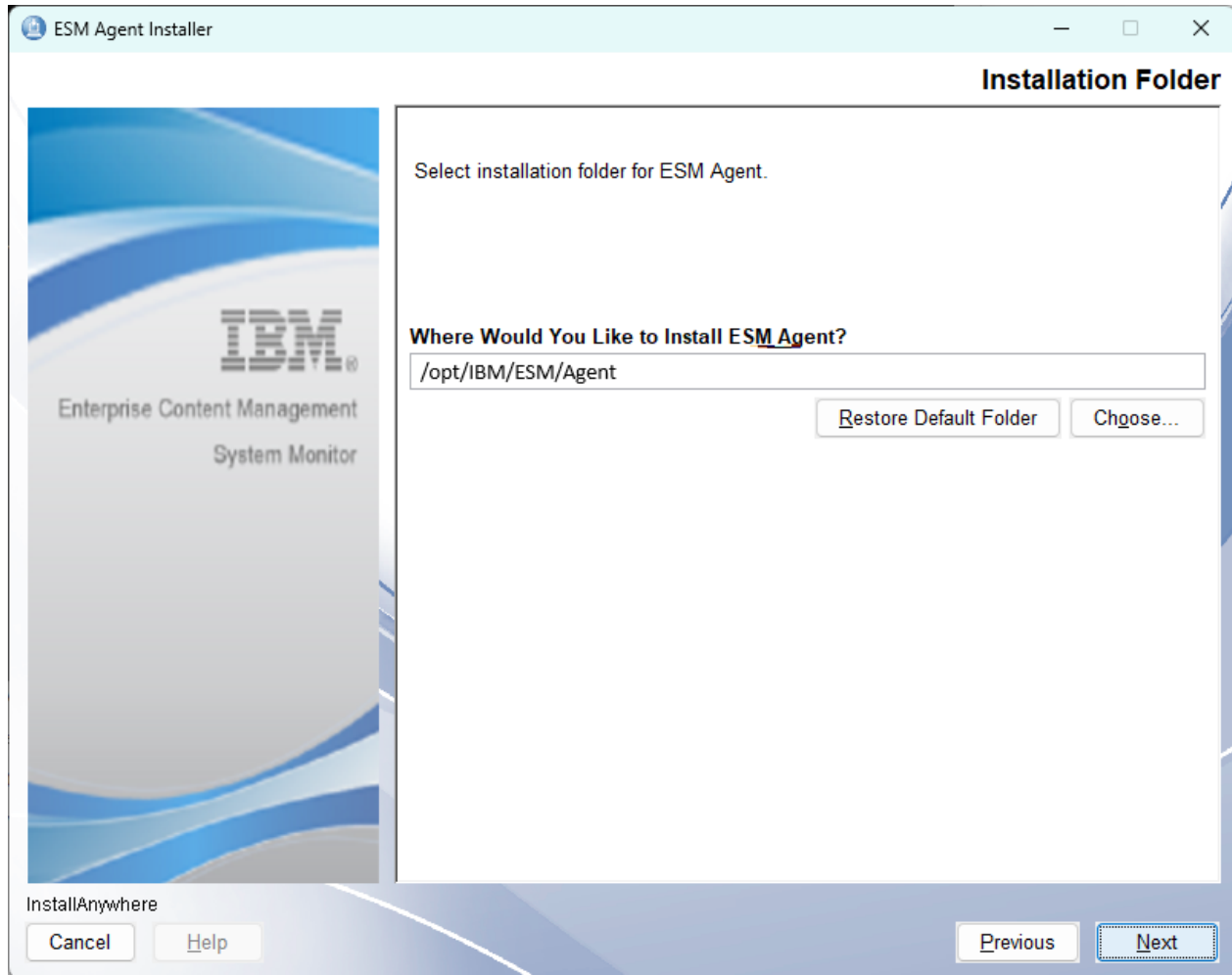


Image of Choose Installation Folder

- The next window is "Enter Agent Name, Hostname and Ports". The following parameters can be specified. Click "Next" to proceed. We recommend to keep https enabled.

Unique Agent Name

Default: *EsmAgent*

IMPORTANT

The agent name on AIX is limited to 8 characters.

ESM Server Name

Default: *localhost*

Server Port

Default: *1883*

Http Port

Default: *1180*

Https Port

Default: *1543*

RMI Registry Port

Default: *2099*

RMI Server Port

Default: *55555*

SSH Port

Default: *9202*

SSL KEY PASSWORD

Default: *=password*

SSL KEYSTORE PASSWORD

Default: *=password*

SSL TRUSTSTORE PASSWORD

Default: *=password*

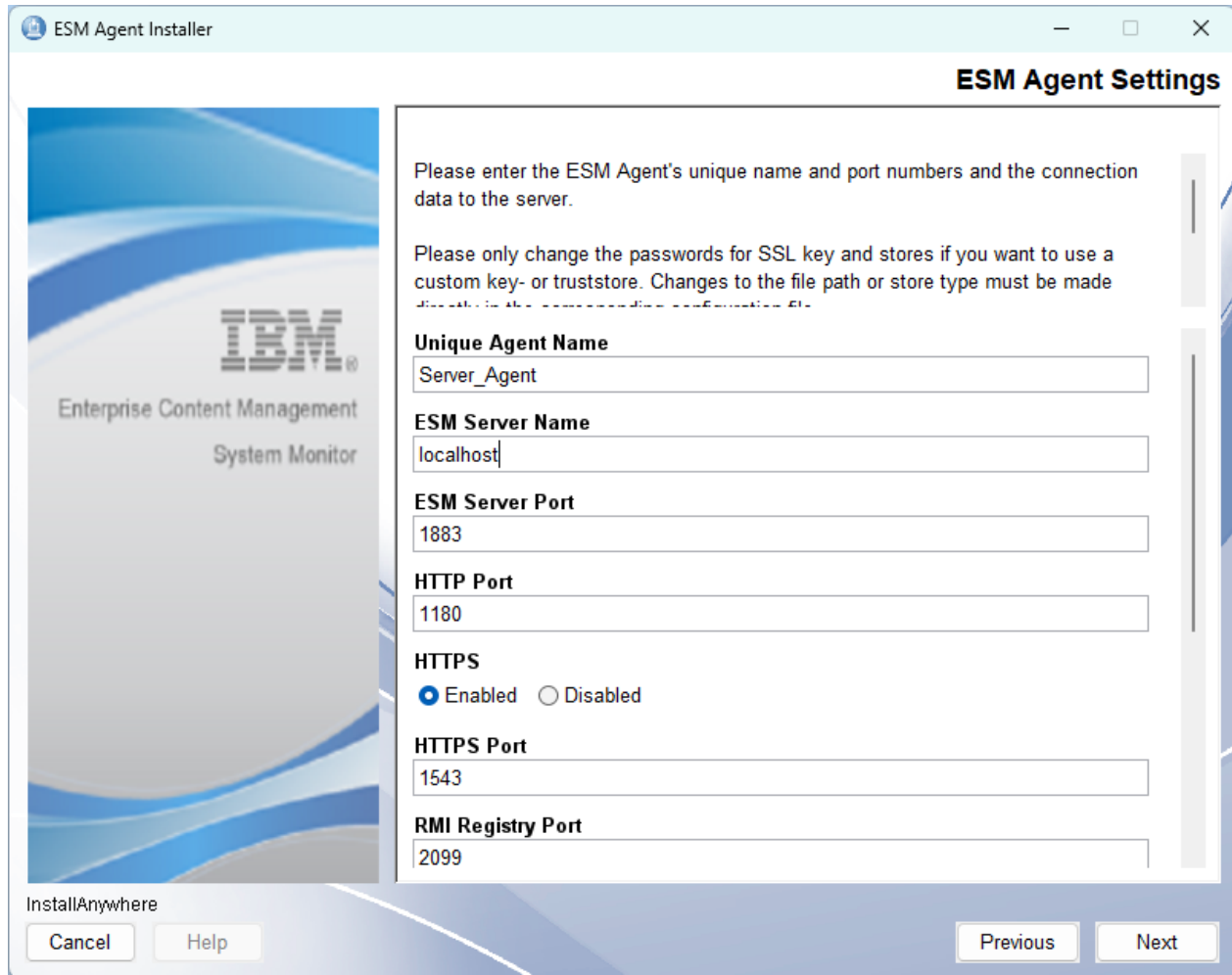


Image of Agent Settings (1)

- The next window is "Autostart and Systemstart". The following parameters can be specified. Click "Next" to proceed.

Start ESM Agent after Installation

Default: Yes = checked

Start at OS Start

Default: Yes = unchecked

NOTE

If unchecked, the no service entry is created in inittab or systemctl. Also root rights are needed for this.

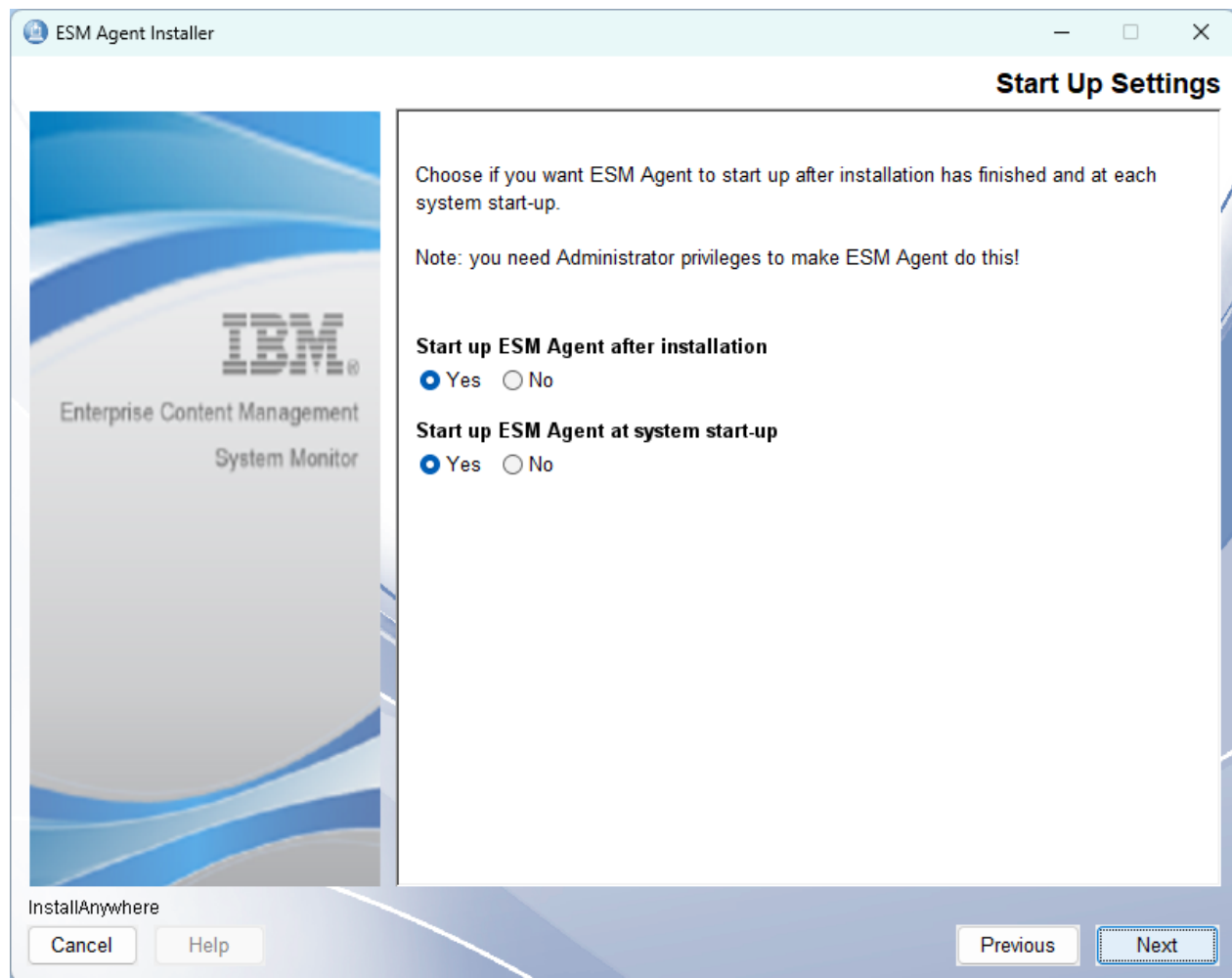


Image of Autotstart and Systemstart

- The next window is "Pre-Installation Summary". Click "Install" to proceed.

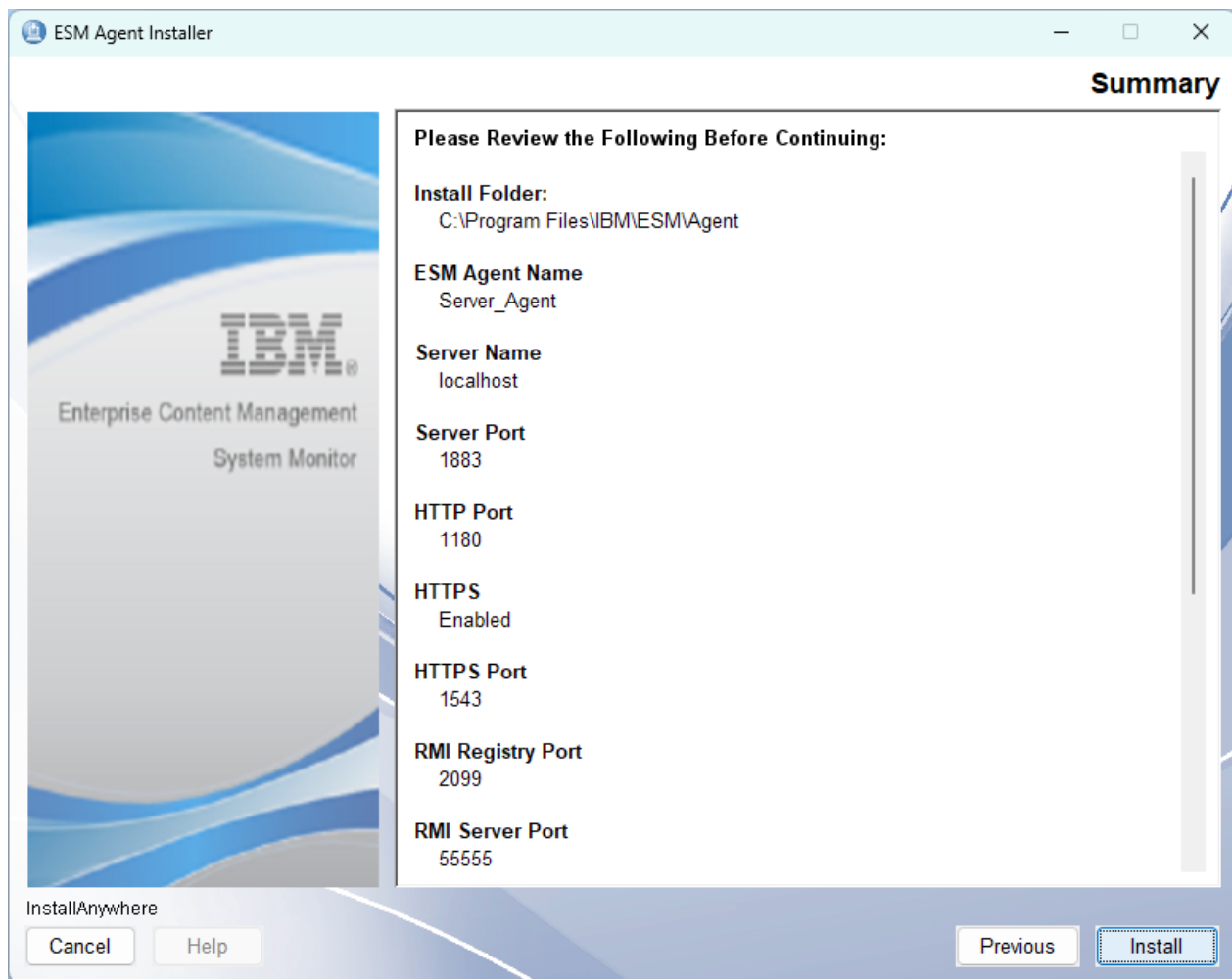


Image of Pre-installation Summary

- The installation starts and finishes with the window "Install Complete". Click "Done" to close and finish the installation procedure.

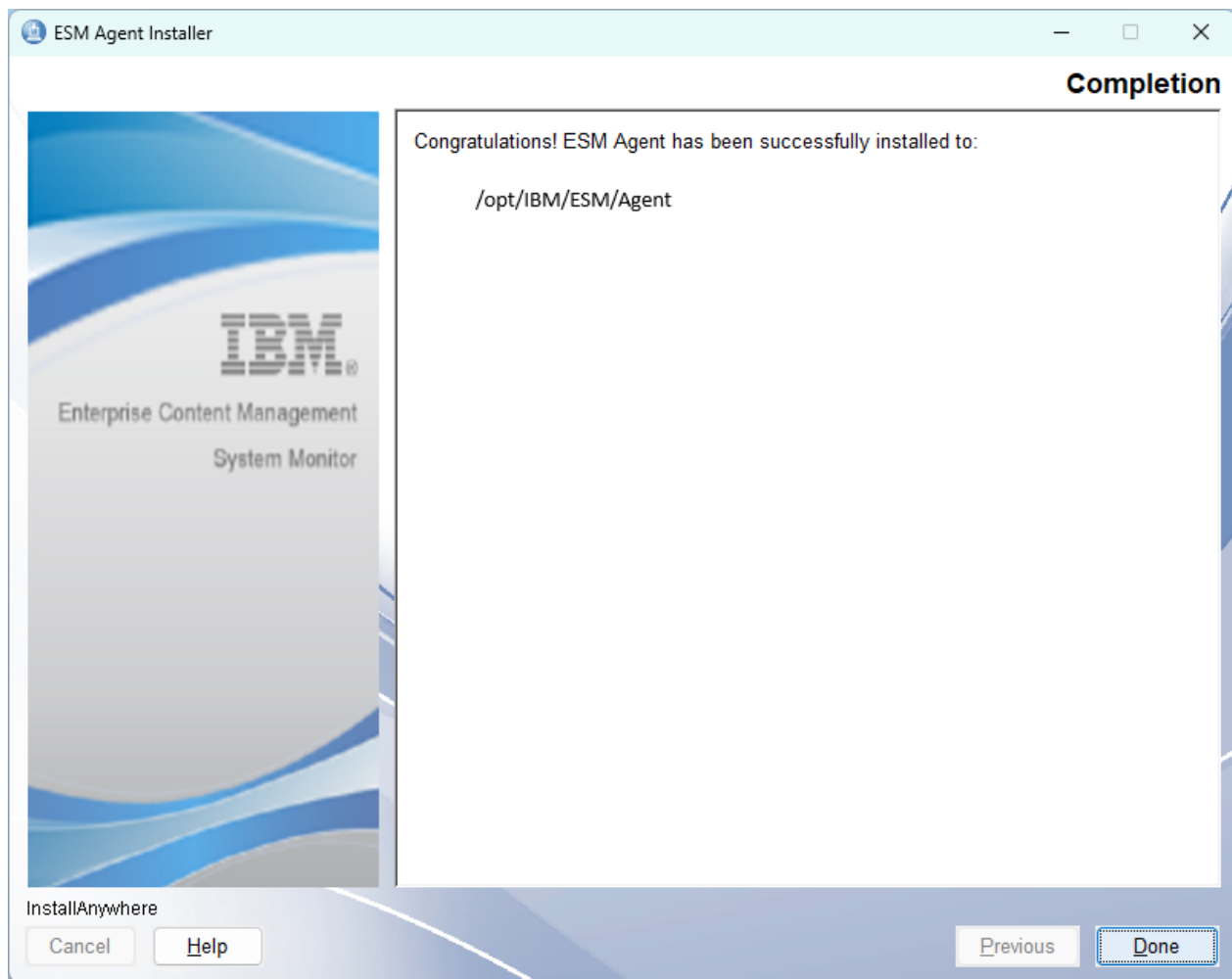


Image of Installation Complete

NOTE

Every Agent that connects to an ESM server for the first time, will automatically have basic monitoring activated. Per default 3 probes (cpu, memory and disk space) will run. For more details see the Probes and Situation Guide chapter "Default (standard) base probes for all agent".

Installation using silent mode

For the silent installation a properties file is needed. An example file will be given for each possible OS and the execution command will be listed.

Windows based server

- Open a "Command Prompt (Admin)" and execute the installation package as shown:

```
<YourPackageLocation>\ESM_Server_Installer.exe      -i      silent      -f  
<YourPropertiesLocation>\installer.properties
```

Example 1. Example for installer.properties file with H2 Database

```
# Thu Aug 10 07:26:01 PDT 2017
# Replay feature output
#
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

#Indicate whether the license agreement been accepted
#-----
LICENSE_ACCEPTED=TRUE

#Choose Installation Folder
#-----
USER_INSTALL_DIR=C:\\Program Files\\IBM\\ESM\\Server

#Server Settings
#-----
SERVER_HOSTNAME=localhost
SERVER_IP=0.0.0.0
SERVER_PORT=1883
JETTY_PORT=80
JETTY_SECURE_ENABLED=true
JETTY_SECURE_DISABLED=false
JETTY_SECURE_PORT=443
RMI_REGISTRY_PORT=1099
RMI_SERVER_PORT=44444
SSH_PORT=8101
SSL_KEY_PASSWORD=ENC(g+R0/aAgGtIjBjQCppBD2Q==)
SSL_KEYSTORE_PASSWORD=ENC(g+R0/aAgGtIjBjQCppBD2Q==)
SSL_TRUSTSTORE_PASSWORD=ENC(g+R0/aAgGtIjBjQCppBD2Q==)

#Configuration Database Settings
#-----
JDBC_URL=jdbc:h2:./configuration;AUTO_SERVER=TRUE;AUTO_RECONNECT=TRUE;LOCK_TIMEOUT=10000;MODE=LEGACY
JDBC_DRIVER_NAME=org.h2.Driver
JDBC_USER=db
JDBC_PASSWORD=ENC(JWvE1aMYXp+TQMRha6gROg==, PasswordEncryptor)

#Monitoring Database Settings
#-----
MONITORING_JDBC_URL=jdbc:h2:./monitoring;AUTO_SERVER=TRUE;AUTO_RECONNECT=TRUE;LOCK_TIMEOUT=10000;MODE=LEGACY
MONITORING_JDBC_DRIVER_NAME=org.h2.Driver
MONITORING_JDBC_USER=db
MONITORING_JDBC_PASSWORD=ENC(JWvE1aMYXp+TQMRha6gROg==, PasswordEncryptor)

#Start Up Settings
#-----
AUTO_START=1
NOT_AUTO_START=0
SYSTEM_START=1
NOT_SYSTEM_START=0
SYSTEM_START_INSTALLATION=0
NOT_SYSTEM_START_INSTALLATION=1

#Install
#-----
-fileOverwrite C:\\Program Files\\IBM\\ESM\\Server\\Uninstall_ESM_Server.lax=Yes
-fileOverwrite C:\\Program Files\\IBM\\ESM\\Server\\resource\\tiawIn64_x64.dll=Yes
-fileOverwrite C:\\Program Files\\IBM\\ESM\\Server\\resource\\iawin32.dll=Yes
-fileOverwrite C:\\Program Files\\IBM\\ESM\\Server\\resource\\win64_32_x64.exe=Yes
-fileOverwrite C:\\Program Files\\IBM\\ESM\\Server\\resource\\remove.exe=Yes
-fileOverwrite C:\\Program Files\\IBM\\ESM\\Server\\resource\\invoker.exe=Yes
Files\\IBM\\ESM\\Server\\version\\ibm.com_IBM_Enterprise_Content_Management_System_Monitor_Server-5.5.2.swidtag.xml=Yes
```

Windows based agent

- Open a "Command Prompt (Admin)" and execute the installation package as shown:

```
<YourPackageLocation>\ESM Agent Installer.exe -i silent -f
<YourPropertiesLocation>\Installer.properties
```

Example 2. Example for installer.properties file

```
# Thu Aug 17 07:54:20 PDT 2017
# Replay feature output
#
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

#Indicate whether the license agreement been accepted
#-----
LICENSE_ACCEPTED=TRUE

#Choose Installation Folder
#-----
USER_INSTALL_DIR=C:\\Program Files\\IBM\\ESM\\Agent

#Agent Settings
#-----
CLIENT_ID=Agent
SERVER_HOSTNAME=localhost
SERVER_PORT=1883
JETTY_PORT=1180
JETTY_SECURE_ENABLED=true
JETTY_SECURE_DISABLED=false
JETTY_SECURE_PORT=1543
RMI_REGISTRY_PORT=2099
RMI_SERVER_PORT=55555
SSH_PORT=9202
SSL_KEY_PASSWORD=ENC(g+R0/aAqGtIjBjQCppBD2Q==)
SSL_KEYSTORE_PASSWORD=ENC(g+R0/aAqGtIjBjQCppBD2Q==)
SSL_TRUSTSTORE_PASSWORD=ENC(g+R0/aAqGtIjBjQCppBD2Q==)

#Start Up Settings
#-----
AUTO_START=1
NOT_AUTO_START=0
SYSTEM_START=1
NOT_SYSTEM_START=0
SYSTEM_START_INSTALLATION=0
NOT_SYSTEM_START_INSTALLATION=1

#Install
#-----
-fileOverwrite C:\\Program Files\\IBM\\ESM\\Agent\\Uninstall_ESM_Agent.lax=Yes
-fileOverwrite C:\\Program Files\\IBM\\ESM\\Agent\\resource\\iawin64_x64.dll=Yes
-fileOverwrite C:\\Program Files\\IBM\\ESM\\Agent\\resource\\iawin32.dll=Yes
-fileOverwrite C:\\Program Files\\IBM\\ESM\\Agent\\resource\\win64_32_x64.exe=Yes
-fileOverwrite C:\\Program Files\\IBM\\ESM\\Agent\\resource\\remov@.exe=Yes
-fileOverwrite C:\\Program Files\\IBM\\ESM\\Agent\\resource\\invoker.exe=Yes
Files\\IBM\\ESM\\Agent\\version\\ibm.com_IBM_Enterprise_Content_Management_System_Monitor_Ag
ent-5.5.2.swidtag.xml=Yes
```

Linux based server

- Open a "shell (root)" and execute the installation package as shown:

```
<YourPackageLocation>./ESM_Server_Installer.bin -i silent -f
<YourPropertiesLocation>\\install@.properties
```

Example 3. Example for installer.properties file with H2 Database

```
# Thu Jan 04 01:40:27 EST 2018
# Replay feature output
#
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

#Indicate whether the license agreement been accepted
#-----
LICENSE_ACCEPTED=TRUE

#Choose Installation Folder
#-----
USER_INSTALL_DIR=/opt/IBM/ESM/Server

#Server Settings
#-----
SERVER_HOSTNAME=localhost
SERVER_IP=0.0.0.0
SERVER_PORT=1883
JETTY_PORT=80
JETTY_SECURE_ENABLED=true
JETTY_SECURE_DISABLED=false
JETTY_SECURE_PORT=443
RMI_REGISTRY_PORT=1099
RMI_SERVER_PORT=44444
SSH_PORT=8101
SSL_KEY_PASSWORD=ENC(g+R0/aAqGtIjBjQCppBD2Q==)
SSL_KEYSTORE_PASSWORD=ENC(g+R0/aAqGtIjBjQCppBD2Q==)
SSL_TRUSTSTORE_PASSWORD=ENC(g+R0/aAqGtIjBjQCppBD2Q==)

#Configuration Database Settings
#-----
JDBC_URL=jdbc:h2:./configuration;AUTO_SERVER=TRUE;AUTO_RECONNECT=TRUE;LOCK_TIMEOUT=10000;MODE=LEGACY
JDBC_DRIVER_NAME=org.h2.Driver
JDBC_USER=db
JDBC_PASSWORD=ENC(JWvElamYXp+TQMRha6gROg==, PasswordEncryptor)

#Monitoring Database Settings
#-----
MONITORING_JDBC_URL=jdbc:h2:./monitoring;AUTO_SERVER=TRUE;AUTO_RECONNECT=TRUE;LOCK_TIMEOUT=10000;MODE=LEGACY
MONITORING_JDBC_DRIVER_NAME=org.h2.Driver
MONITORING_JDBC_USER=db
MONITORING_JDBC_PASSWORD=ENC(JWvElamYXp+TQMRha6gROg==, PasswordEncryptor)

#Start Up Settings
#-----
AUTO_START=1
NOT_AUTO_START=0
SYSTEM_START=1
NOT_SYSTEM_START=0

#Install
#-----
-fileOverwrite /opt/IBM/ESM/Server/karaf/version=Yes
-fileOverwrite /opt/IBM/ESM/Server/Uninstall ESM Server.lax=Yes
-fileOverwrite /opt/IBM/ESM/Server/properties/version/ibm.com IBM_Enterprise_Content_Management_System_Monitor_Server-5.5.2.swidtag.xml=Yes
```

Linux based agent

- Open a "shell (root)" and execute the installation package as shown:

```
<YourPackageLocation>/ESM_Agent_Installer.bin          -i          silent          -f
<YourPropertiesLocation>\installer.properties
```


Example 4. Example for installer.properties file

```
# Thu Jan 04 01:54:20 EST 2018
# Replay feature output
# -----
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

#Indicate whether the license agreement been accepted
#-----
LICENSE_ACCEPTED=TRUE

#Choose Installation Folder
#-----
USER_INSTALL_DIR=/opt/IBM/ESM/Agent

#Agent Settings
#-----
CLIENT_ID=Agent
SERVER_HOSTNAME=localhost
SERVER_PORT=1883
JETTY_PORT=1180
JETTY_SECURE_ENABLED=true
JETTY_SECURE_DISABLED=false
JETTY_SECURE_PORT=1543
RMI_REGISTRY_PORT=2099
RMI_SERVER_PORT=55555
SSH_PORT=9202
SSL_KEY_PASSWORD=ENC(g+R0/aAqGtIjBjQCppBD2Q==)
SSL_KEYSTORE_PASSWORD=ENC(g+R0/aAqGtIjBjQCppBD2Q==)
SSL_TRUSTSTORE_PASSWORD=ENC(g+R0/aAqGtIjBjQCppBD2Q==)

#Start Up Settings
#-----
AUTO_START=1
NOT_AUTO_START=0
SYSTEM_START=1
NOT_SYSTEM_START=0

#Install
#-----
-fileOverwrite /opt/IBM/ESM/Agent/karaf/version=Yes
-fileOverwrite /opt/IBM/ESM/Agent/Uninstall ESM Agent.lax=Yes
-fileOverwrite /opt/IBM/ESM/Agent/properties/version/ibm.com IBM_Enterprise_Content_Manageme
nt_System_Monitor_Agent-5.5.4.swidtag.xml=Yes
```

AIX based agent

- Open a "shell (root)" and execute the installation package as shown:

```
<YourPackageLocation>/ESM Agent Installer.bin          -i          silent          -f
<YourPropertiesLocation>\installer.properties
```

Example 5. Example for installer.properties file

```
# Thu Jan 04 01:54:20 EST 2018
# Replay feature output
# -----
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

#Indicate whether the license agreement been accepted
#-----
LICENSE_ACCEPTED=TRUE

#Choose Installation Folder
#-----
USER_INSTALL_DIR=/opt/IBM/ESM/Agent

#Agent Settings
#-----
CLIENT_ID=Agent
SERVER_HOSTNAME=localhost
SERVER_PORT=1883
JETTY_PORT=1180
JETTY_SECURE_ENABLED=true
JETTY_SECURE_DISABLED=false
JETTY_SECURE_PORT=1543
RMI_REGISTRY_PORT=2099
RMI_SERVER_PORT=55555
SSH_PORT=9202
SSL_KEY_PASSWORD=ENC(g+R0/aAqGtIjBjQCppBD2Q==)
SSL_KEYSTORE_PASSWORD=ENC(g+R0/aAqGtIjBjQCppBD2Q==)
SSL_TRUSTSTORE_PASSWORD=ENC(g+R0/aAqGtIjBjQCppBD2Q==)

#Start Up Settings
#-----
AUTO_START=1
NOT_AUTO_START=0
SYSTEM_START=1
NOT_SYSTEM_START=0

#Install
#-----
-fileOverwrite_/opt/IBM/ESM/Agent/Uninstall_ESM_Agent.lax=Yes
```

Tests for a successful installation

- Check if the services or start up files have been created.
- Login to your console ([http\(s\)://<hostname>:<port>](http(s)://<hostname>:<port>))
- The default login is admin / admin, please change the password.
- See if the console is behaving normal. Switch between dashboards and check if it is working, etc.

Security hints

CAUTION

Do not forget to change the admin password from the default to a more secure one!

CAUTION

When using https, it is strongly recommended to replace the self-signed certificate shipped with the product. See chapter "Running the ESM server with https - Using self-signed or authority signed certificates" for details.

How to create a systemd service for ESM on Linux-s390x

Motivation

The Apache Karaf service wrapper used in ESM does not support Linux-s390x. But it is relatively easy to create a systemd service manually.

Prerequisites

You must have the permission

- To open a terminal.
- To create, delete and edit files below the 'karaf'-directory in the installation directory of ESM Agent.
- To reload systemd service configurations.
- To start and stop systemd services.

Normally this means you must be root or execute all the below commands via sudo as shown.

ESM was installed as a service. This is strictly not necessary but makes things easier as it provides a template for the service configuration and has created the necessary links in /etc/systemd/system/.

Procedure

New reload script

Create a new file named reload in <ESM-Installation-directory>/karaf/bin. Its content should be:

```
#!/bin/sh
/opt/IBM/ESM/Server/karaf/bin/stop
sleep 10
/opt/IBM/ESM/Server/karaf/bin/start
```

Make the file executable with

```
$ sudo chmod 755 <ESM-Installation-directory>/karaf/bin/reload
```

Scenario: No service installed

If not installed as a service create the service configuration file - named `IbmESM_<agent-name>.service` - manually in `<ESM-Installation-directory>/karaf/bin/`. Use the example below as a template and change the installation directory to match your environment. That is replace `/opt/IBM/ESM/Agent` with the installation directory of the ESM Agent at your site.

Now you must create a symbolic link in `/etc/systemd/system/` pointing to `IbmEsm_<agent-name>.service`

```
$ sudo ln -s <ESM-Installation-directory>/karaf/bin/IbmEsm_<agent-name>.service  
/etc/systemd/system/
```

Now enable the new service by executing:

```
$ sudo systemctl enable IbmEsm_<agent-name>.service
```

Scenario: Existing – but not working service installation

If installed as a service, open the service configuration named `IbmEsm_<agent-name>.service` located in `<ESM-Installation-directory>/karaf/bin/` in a text editor with administrative privileges; e.g. `sudo vi ...` or `sudo nano ...`

Replace `IbmEsm_<agent-name> start`, `IbmEsm_<agent-name> restart`, and `IbmEsm_<agent-name> stop` by `start`, `reload`, and `stop`.

Remove the complete line starting with `PIDFile=`

Save the file after you have made these changes.

Remove a stale PID-file `<ESM-Installation-directory>/karaf/karaf.pid` if it exists:

```
$ sudo rm <ESM-Installation-directory>/kara/karaf.pid
```

Reload the service configuration by executing:

```
$ sudo systemctl daemon-reload
```

Service test

At the end of both scenarios it should now be possible to start the service for ESM by executing:

```
$ sudo systemctl start IbmEsm_<agent-name>.service
```

Check the status with:

```
$ sudo systemctl status IbmEsm_<agent-name>.service
```

Example service configuration

Here is an example how the files should look like if ESM Agent was installed in /opt/IBM/ESM/Agent:

Example 6. Example service configuration

```
# -----  
# Licensed to the Apache Software Foundation (ASF) under one or more  
# contributor license agreements. See the NOTICE file distributed with  
# this work for additional information regarding copyright ownership.  
# The ASF licenses this file to You under the Apache License, Version 2.0  
# (the "License"); you may not use this file except in compliance with  
# the License. You may obtain a copy of the License at  
#  
# http://www.apache.org/licenses/LICENSE-2.0  
#  
# Unless required by applicable law or agreed to in writing, software  
# distributed under the License is distributed on an "AS IS" BASIS,  
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.  
# See the License for the specific language governing permissions and  
# limitations under the License.  
# -----  
#  
# This script is an Unix systemd script  
#  
[Unit]  
Description=Agent of the IBM Enterprise Content Management System Monitor  
Server  
  
[Service]  
Type=forking  
ExecStart=/opt/ESM/Agent/karaf/bin/start  
ExecReload=/opt/ESM/Agent/karaf/bin/reload  
ExecStop=/opt/ESM/Agent/karaf/bin/stop  
  
[Install]  
Alias=Csm_LocalAgent  
WantedBy=default.target
```


De-installation of the software

InstallAnywhere offers an uninstall method that can be used.

Windows based systems

On Windows based installations the uninstall can be triggered via ControlPanel → Programs → Programs and Features. Select the Software (Server / Agent) you want to uninstall and click on the uninstall button.

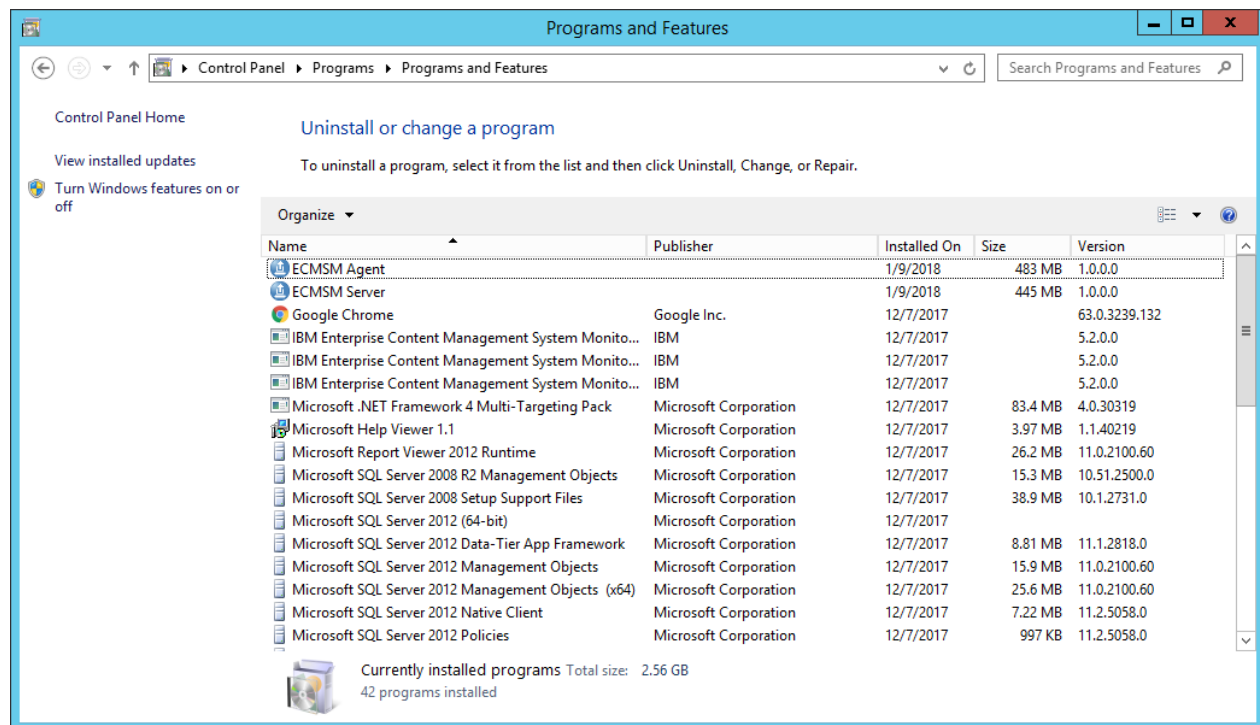


Image of Program and Features

Follow the procedure, the first window will point out that you are about to uninstall the product.

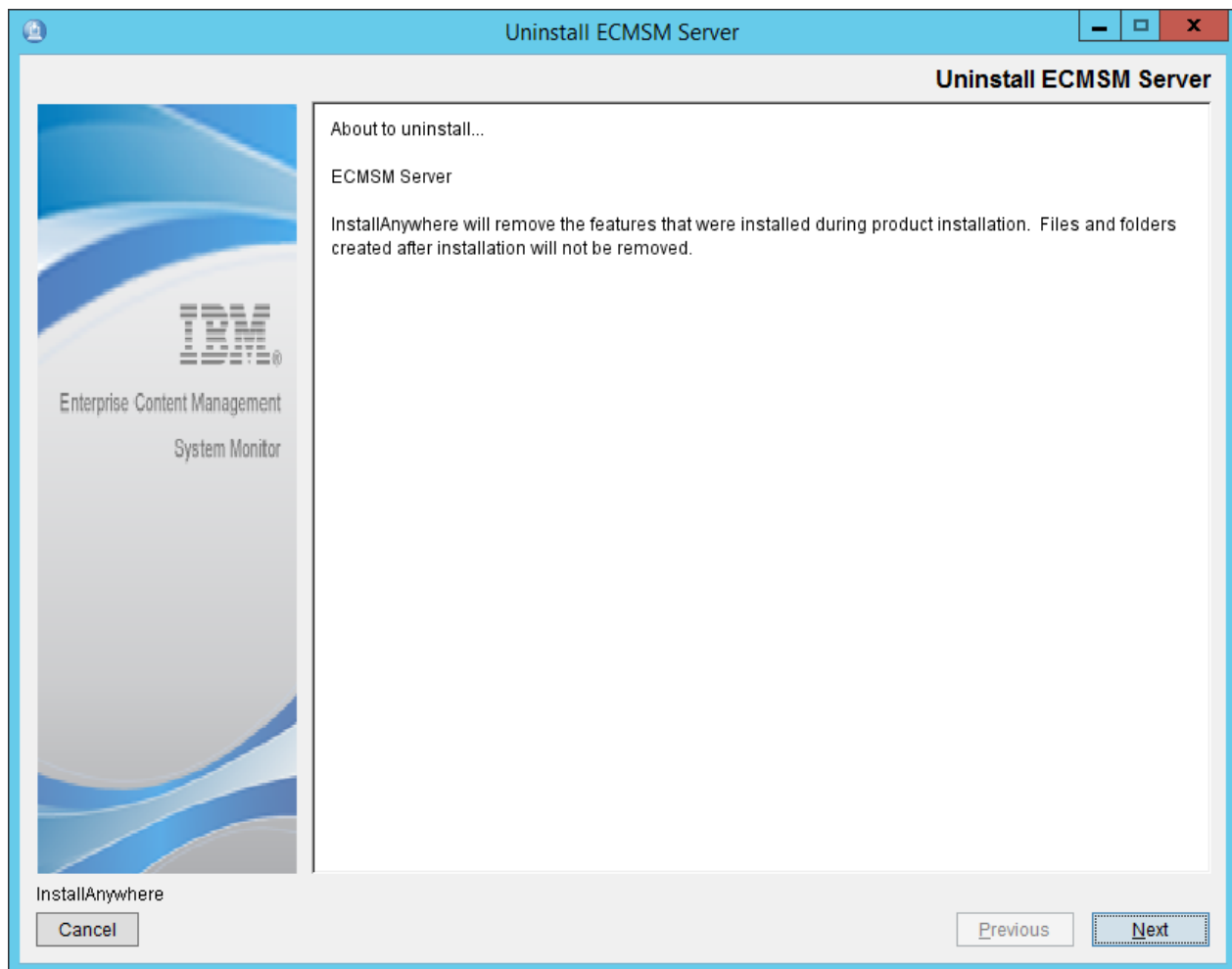


Image of Uninstall ESM Server

Select the Uninstall Option, by default "Complete Uninstall" is selected.

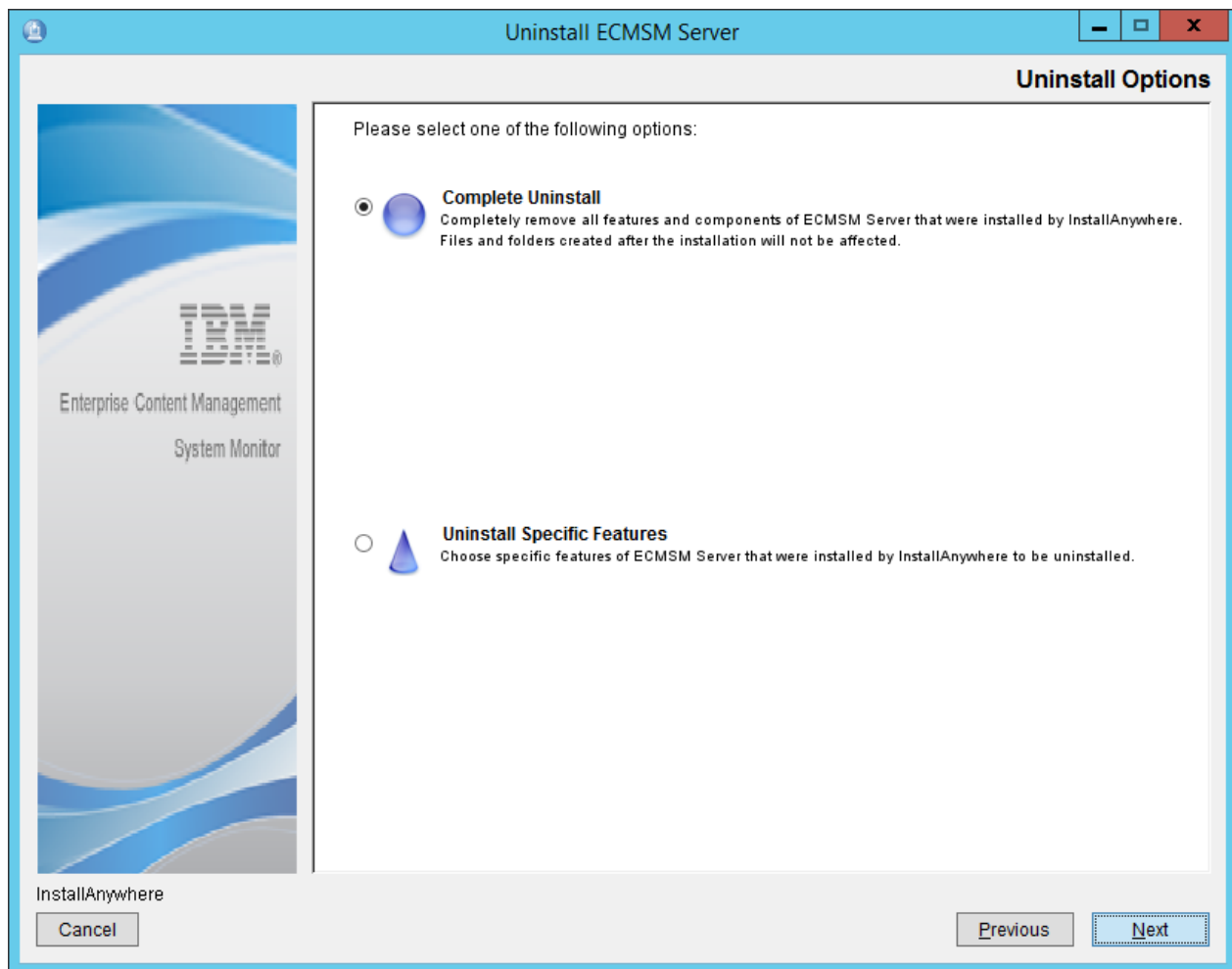


Image of Uninstall Options

The software is getting uninstalled. It can happen that not all files could be removed during uninstall process.

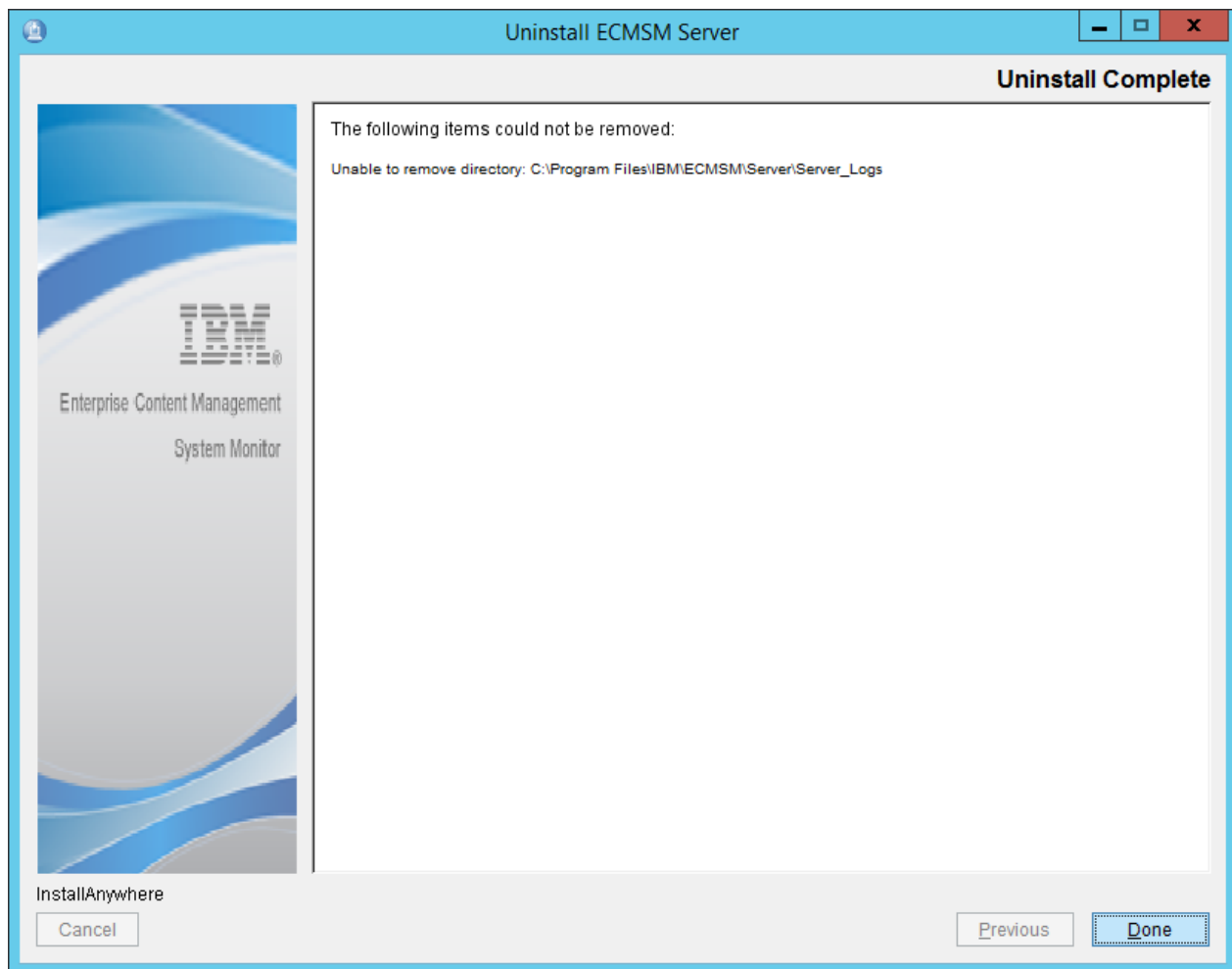


Image of Uninstall Complete

Please review the installation folder afterwards. You can delete any leftover files and folders.

Linux based systems

On Linux based installations the uninstall can be triggered via an uninstall binary (Uninstall_ESM_Agent or Uninstall_ESM_Server both located in the *Installation_Root*). Please make sure that you have the possibility of running a graphical installer (X11 is enabled) otherwise the procedure starts in console mode.

Follow the procedure, the first window will point out that you are about to uninstall the product.

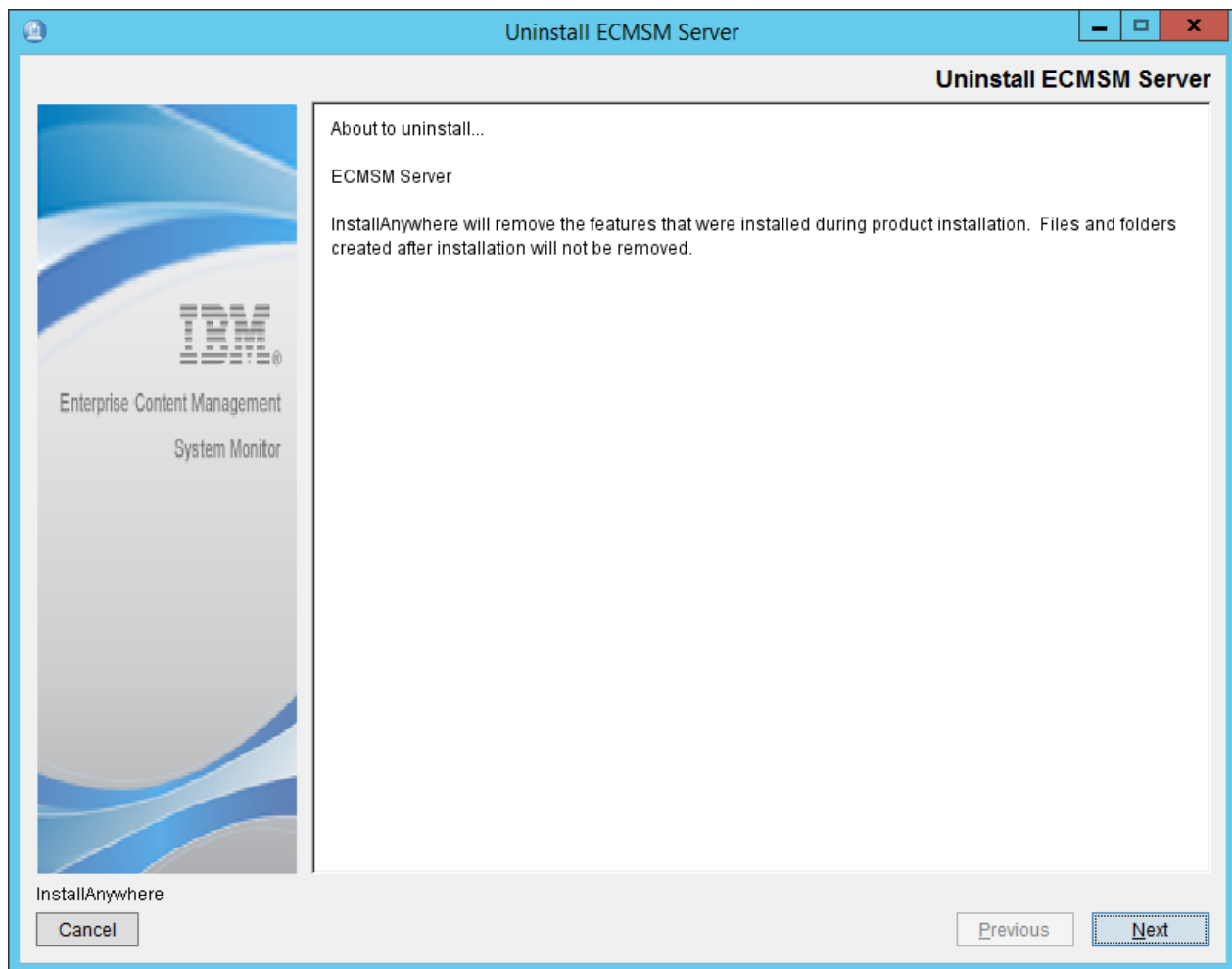


Image of Uninstall ESM Server

Select the Uninstall Option, by default "Complete Uninstall" is selected.

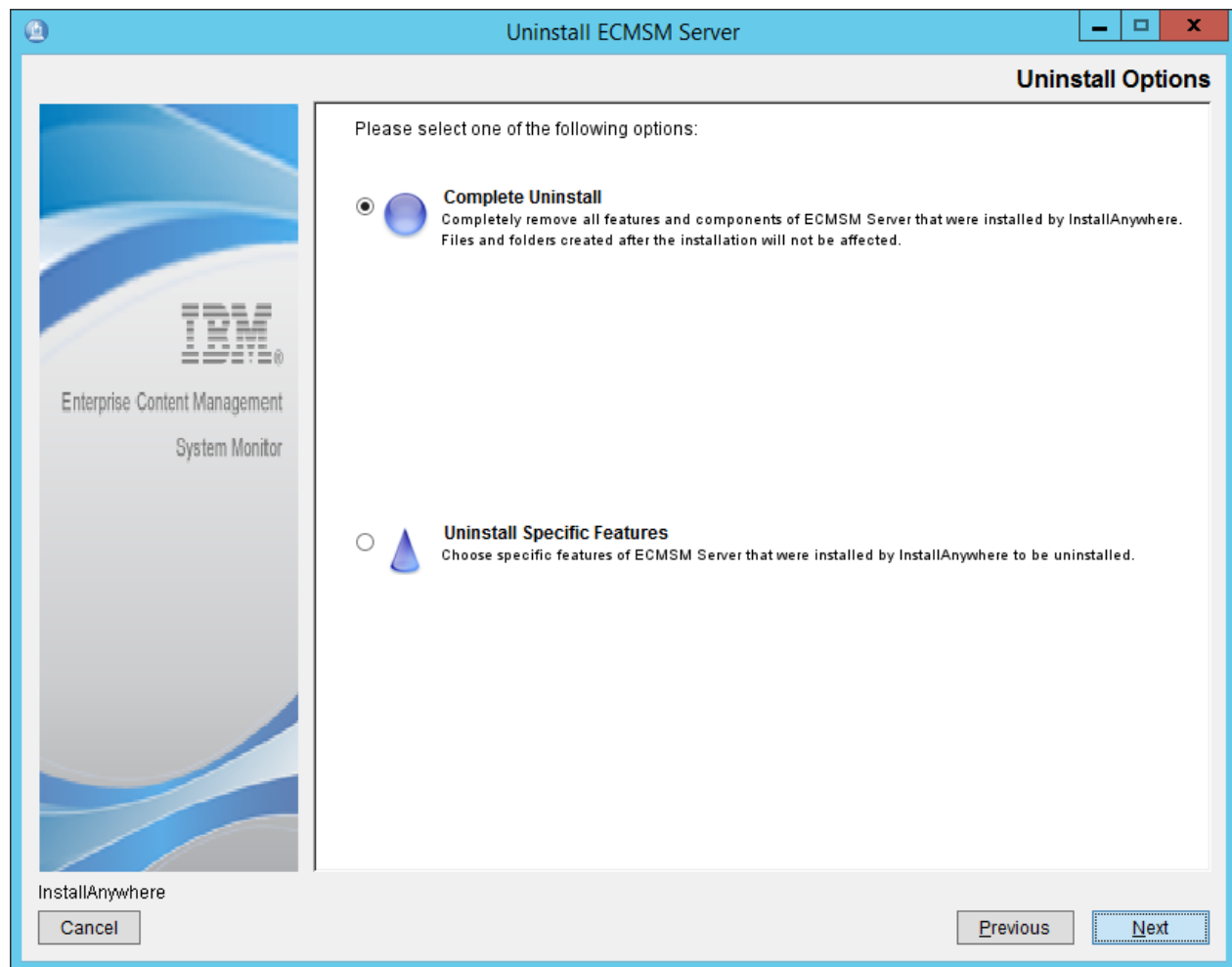


Image of Uninstall Options

The software is getting uninstalled. It can happen that not all files could be removed during uninstall process.

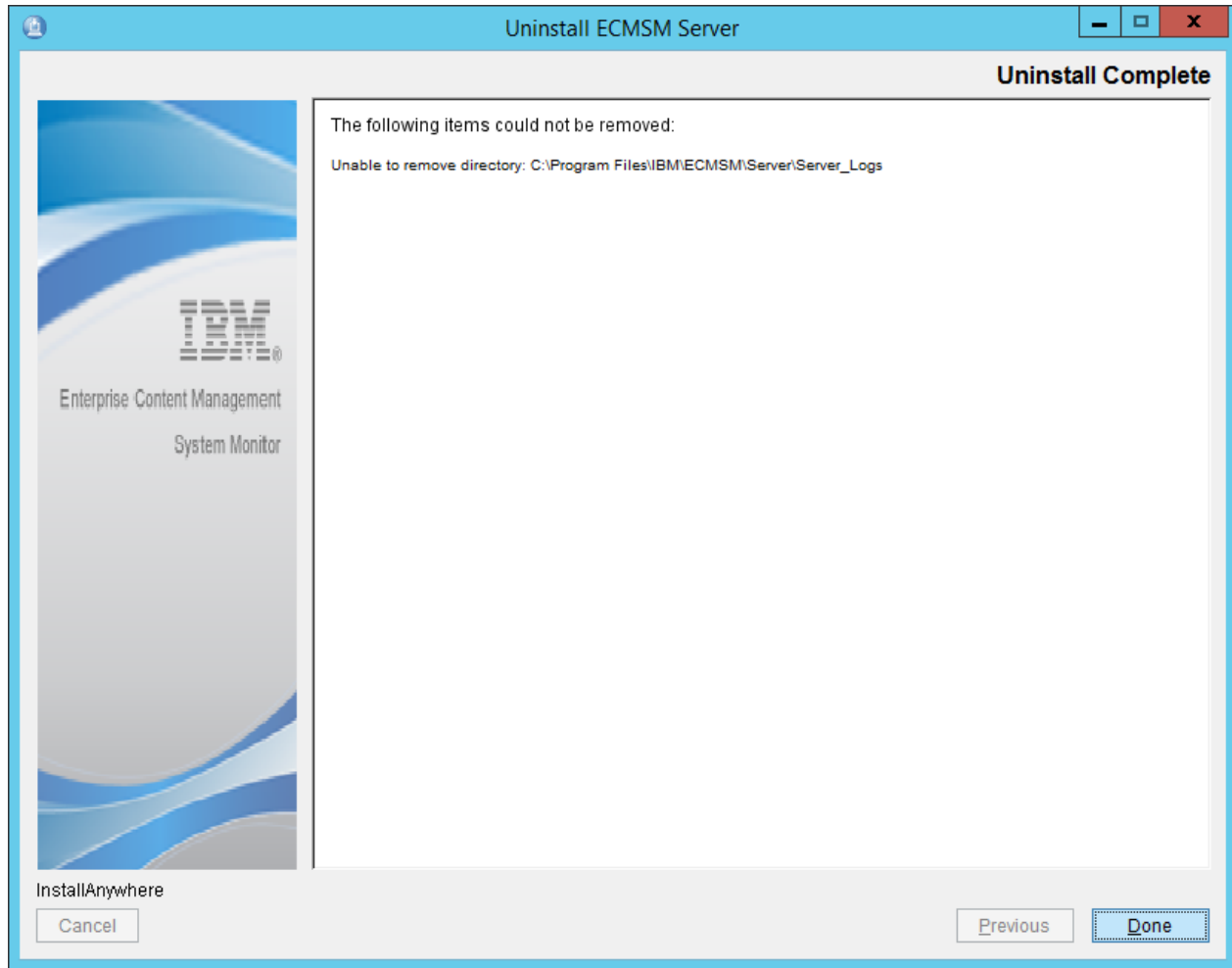


Image of Uninstall Complete

Please review the installation folder afterwards. You can delete any leftover files and folders.

AIX based systems

On AIX based installations the uninstall can be triggered via an uninstall binary (Uninstall_ESM_Agent or Uninstall_ESM_Server both located in the *Installation_Root*). Please make sure that you have the possibility of running a graphical installer (X11 is enabled) otherwise the procedure starts in console mode.

Follow the procedure, the first window will point out that you are about to uninstall the product.

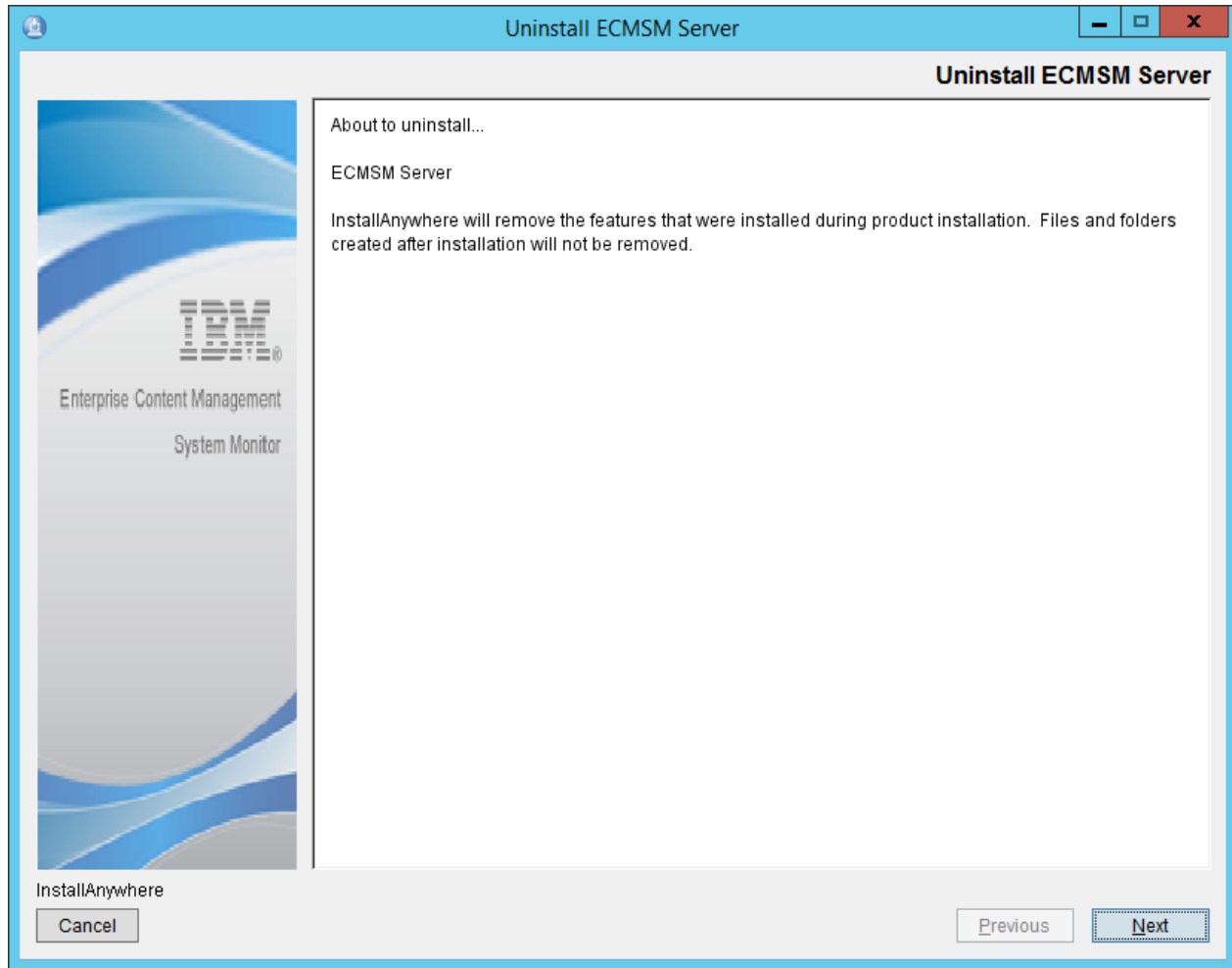


Image of Uninstall ESM Server

Select the Uninstall Option, by default "Complete Uninstall" is selected.

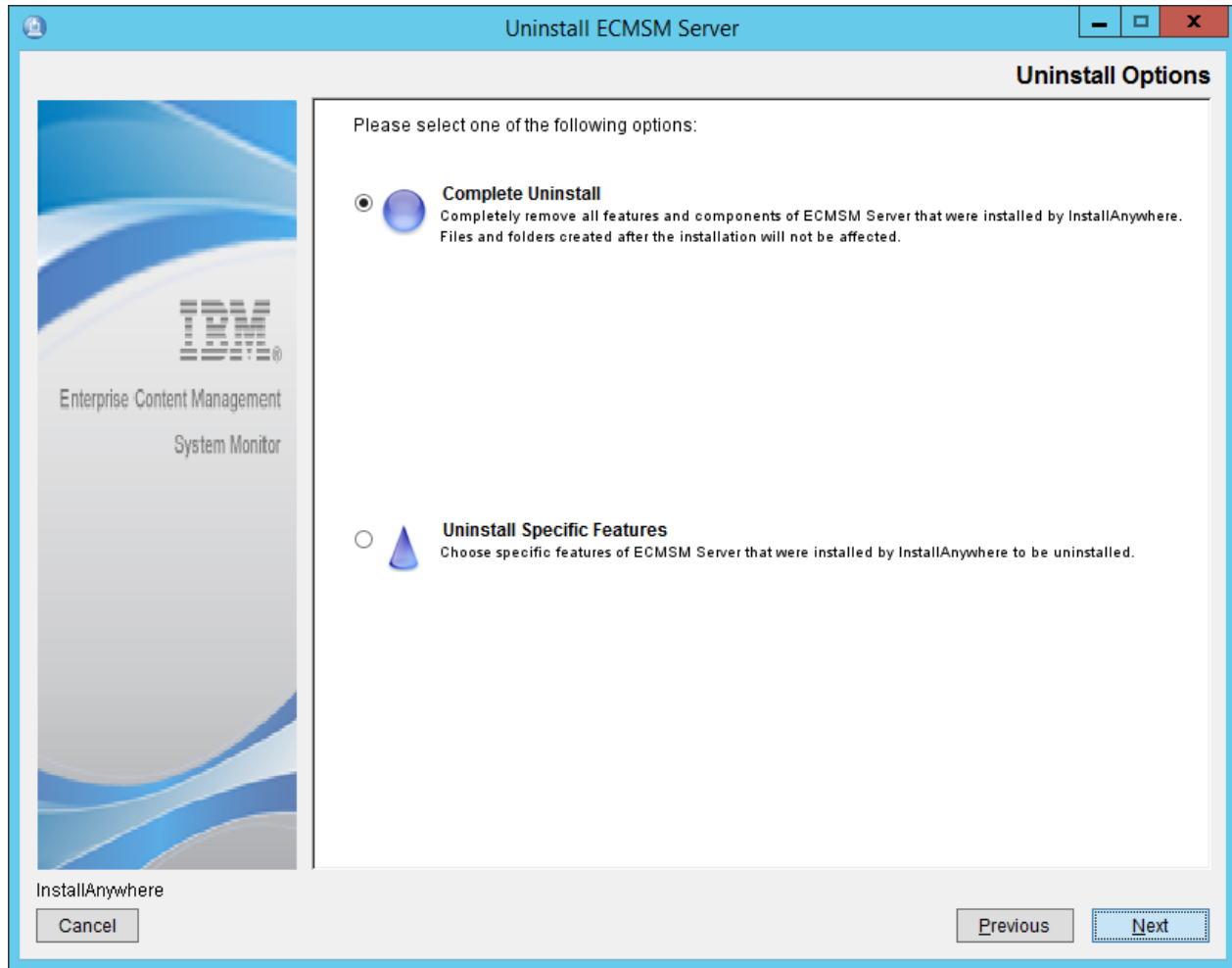


Image of Uninstall Options

The software is getting uninstalled. It can happen that not all files could be removed during uninstall process.

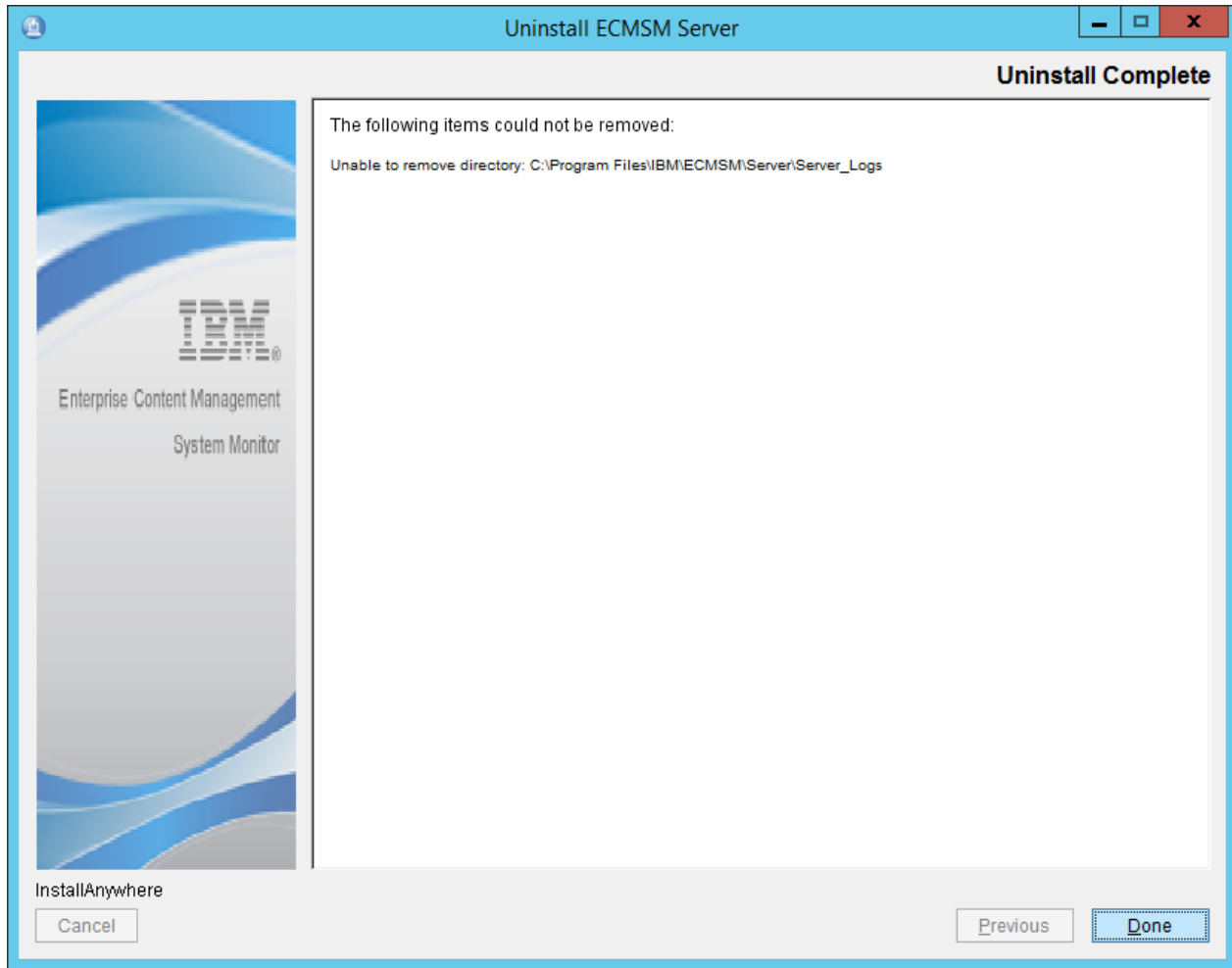


Image of Uninstall Complete

Please review the installation folder afterwards. You can delete any leftover files and folders.

Running the ESM server with https - Using self-signed or authority signed certificates

The configuration for starting the ESM gui https based is located in the file org.ops4j.pax.web.cfg. The file can be found in <Installation-Root>/karaf/etc. The file also contains a java command which can be executed to create a self-signed certificate. The keystore file is located in the subdirectory ssl and named keystore and per default just contains a dummy certificate.

Create a self-signed certificate

Delete or rename the keystore file before running the command. The ESM server must be stopped.

Example 7. Java Command

```
$JAVA_HOME/bin/keytool -genkey -keyalg RSA -alias selfsigned -keystore keystore -storepass password -validity 9999 -sigalg SHA256withRSA -keysize 2048 -storetype jks
```

To create a new self-signed certificate open a cmd or shell and switch to <Installation-Root>/karaf/etc/ssl. Execute the following command:

Windows

(CMD with full admin rights) ..\..\jre\bin\keytool -genkey -keyalg RSA -alias selfsigned -keystore keystore -storepass password -validity 9999 -sigalg SHA256withRSA -keysize 2048 -storetype jks

Unix/Linux

../../jre/bin/keytool -genkey -keyalg RSA -alias selfsigned -keystore keystore -storepass password -validity 9999 -sigalg SHA256withRSA -keysize 2048 -storetype jks

Answer the question for username with FQDN of the ESM server. Leave the rest empty or answer if you like.

Restart the ESM - The GUI is available via https on port 443 (default) now.

Use an authority signed certificate

- Request a certificate and private key for the certificate. The certificate must contain all possible subject alternative names like alias, hostname and hostname + domain.
- Make sure you have the password for the private key, best is if the password is already password.
- Create a keystore with the name keystore from type jks.
- As password for the keystore use password.
- Add the server certificate and the private key to this keystore.
- The private key password must be password within the keystore.
- Replace the keystore file in <Install-Dir>/karaf/etc/ssl on the ESM Server

- Restart the ESM Server afterwards - The GUI is available via https on port 443 (default) now and uses the new certificate.

NOTE

Use a tool like keystore explorer for this procedure. It can be used to export and import certificates and private keys with password change etc.

IMPORTANT

The keystore file is not maintained and is overwritten during the update process, please keep a copy and replace the file again after the update.

ESM 5.8.0 Docker Deployment

This section is intended for administrators and developers who want to operate ESM in a Container environment or customize the existing Docker Container Images provided by IBM. The instructions explain the exemplary container-based deployment on a standard Docker environment (Docker Community Edition).

Overview

How can ESM be used with Docker?

As of today, a Docker Image for the server component of ESM is available. The image provides the following capabilities:

- Full-featured ESM Server (as compared to a non-containerized installation)
- Usage of internal H2 database. No external database is required.
- System configuration and monitoring data can be persisted onto a Data Volume.
- Full support for encrypted communication (for Jetty Web Frontend and communication with agents, including transmission of monitoring data from the Agents to the Server)

Which Docker images are available (as of version ESM 5.8.0)?

The provided Docker image supports x64 Linux Container environments. There are two images provided:

- **esmserver**
 - The Server component of ESM. Includes the possibility to use the built-in H2 database. To be deployed once per environment.
 - Only single instance containers are supported. If more than one Server container is deployed, each of the containers will have to persist a separate state into a database on an own data volume that will contain system configuration and monitoring data.
- **esmagent**
 - The Agent component of ESM. If necessary, the Agent container can be deployed multiple times in one environment.

Import Docker Images into the Local Repository

To be able to conduct the deployment, the required image needs to be present in your local Docker Image Registry. There are two options to obtain the image:

- Pull the image from a registry (`docker pull`)
- Import a downloaded TAR.GZ archive containing the esmserver Image

This documentation will describe the latter of the two options.

Once you downloaded the image (referred to as esmserver.tgz), the image can be imported using the docker load command:

```
> docker load --input esmserver.tgz
2526d0d696da: Loading layer [=====>]
18.94kB/18.94kB
07a99fe71645: Loading layer [=====>]
19.85MB/19.85MB
90753dda1777: Loading layer [=====>]
172.3MB/172.3MB
d35cf5469510: Loading layer [=====>]
156.6MB/156.6MB
1e78a80e2127: Loading layer [=====>]
14.34kB/14.34kB
e2d8e94d1295: Loading layer [=====>]
19.46kB/19.46kB
abe65828e320: Loading layer [=====>]
26.11kB/26.11kB
97796f99b62a: Loading layer [=====>]
249.3kB/249.3kB
Loaded image: esmserver:latest
```

To verify that the image has been properly imported into the local repository, check the images using docker images:

```
> docker images
REPOSITORY    TAG       IMAGE ID       CREATED        SIZE
esmserver     latest    b2df3672c490  About an hour ago  455MB
```

To import esmagent.tgz, repeat the steps above for this file.

Deploying ESM Server (esmserver)

Deployment Samples

This chapter shows several examples for deployments of the esmserver Docker Image. It assumes that the esmserver Image is available in your local Docker Registry and is tagged with version tag "latest".

```
> docker images
REPOSITORY    TAG       IMAGE ID       CREATED        SIZE
esmserver     latest    6a6d011c6c60  5 minutes ago  437MB
```

Depending on from which registry the image has been pulled or whether it has been locally imported, the prefix of the "Repository" name might vary.

```
> docker images
REPOSITORY          TAG          IMAGE ID          [...]
some-repository/esmserver latest       6a6d011c6c60     [...]
```

For simplification the explanations in this documentation use the short syntax (esmserver:latest).

URLs for accessing the Web UI stated in the examples are using a placeholder for the hostname. The hostname needs to be replaced by the hostname or IP that fits your Docker host system.

Furthermore, please note that longer commands are masking linebreaks with a backslash.

Simple Deployment

A default deployment with no specific options can be achieved with this command:

```
> docker run -d --name myesmserver \
-p 8080:8080 \
-p 1883:1883 \
esmserver:latest
```

It is important to understand the characteristics of this type of deployment:

- All passwords of built-in user ids are set to their default values.
- All changes to the system configuration (User Management, Situations etc.) are ephemeral, as the database files used to store this information are residing inside the container. Recreating the container (docker run) or tasks in Container Frameworks (i.e. restarting a Kubernetes Pod) will revert any changes made subsequently to the initial container deployment. In order to safely persist data using Data Volumes, refer to the example in chapter "Deployment with Data Volume and Password Protection".

NOTE

The last argument given in the command line of a `docker run` command is the name of the Docker image. If you have pulled the image from a remote repository, it is tagged with the name of this repository and you need to replace `esmserver:latest` with the full image path (i.e.: `some-repository/esmserver:latest`).

A successful start of the container is indicated by the container's status:

```
> docker ps -a
CONTAINER ID        IMAGE               COMMAND
b38b387c0075       esmserver:latest   "/opt/sm/server/..."
\
CREATED            STATUS
51 seconds ago     Up 50 seconds
\
PORTS              NAMES
0.0.0.0:1883->1883/tcp, 8443/tcp, 0.0.0.0:8080->8080/tcp   myesmserver
```

The Web UI for the resulting container can be accessed via the default port 8080: <http://dockerhost:8080>

Although the container is showing status "up", it could still be possible, that the application cannot be accessed, as the ESM Server is still starting up inside the container.

The first attempt for troubleshooting is the usage of the docker logs command:

```
> docker logs -tf myesmserver
2018-03-02T13:24:51.503902773Z /opt/IBM/ESM/Server/bootstrap.sh - INFO: Startup
procedure of IbmEsmServer initiated.
[...]
```

The option -t will show timestamps for each log message, the option -f will follow the log.

Simple Deployment with Port Mapping

In case it is required to use specific ports for incoming connections to the container, you can make use of the Docker Port Mapping capabilities. The following example shows how to use port mapping for the Web UI port:

```
> docker run -d --name myesmserver \
-p 80:8080 \
-p 1883:1883 \
esmserver:latest
```

The Web UI for the resulting container can be accessed via the default port 80, but container-internally, the application will bind to the default port 8080: <http://dockerhost:80> (respectively: <http://dockerhost> as 80 is the default HTTP port)

It is not necessary to set the associated environment variables when mapping ports (i.e. JETTY_PORT, JETTY_SECURE_PORT, SERVER_PORT or SERVER_SECURE_PORT).

Deployment with Data Volume

The following example will show how to deploy the container with a Data Volume for the purpose of

persisting application data.

PREPARATION OF DATA VOLUME

To persist application data on a Data Volume outside the container the Data Volume needs to be created and mounted in the container. The container-internal target path for the application data cannot be changed.

To create a local Docker Volume, use the following command:

```
> docker volume create esm-vol  
esm-vol
```

To make use of remote File Storage or Network Shares, refer to the documentation of Docker or the Framework in place.

DEPLOYMENT

```
> docker run -d --name myesmserver \  
-p 80:8080 \  
-p 1883:1883 \  
-v esm-vol:/opt/sm/server/karaf/db \  
esmserver:latest
```

NOTE

`${PWD}` refers to the current working directory and could be replaced by a full-qualified path. The part left of the colon in a volume argument (-v) points to a fixed path on the Docker host or a Data Volume on the Docker host managed by the Docker daemon. The right part points to the targeted mount path inside the container.

In comparison to the other samples, there is no difference in the port configuration, which is why the Web UI for the resulting container can be accessed via the default port 80: <http://dockerhost:80>

Deployment with TLS/SSL Security (HTTPS)

The following example will be based on the sample in chapter "Deployment with Data Volume and Password Protection", but additionally, SSL security will be enabled.

NOTE

In case the ESM Server UI shall be provided to multiple users in a Kubernetes clusters, it is possible to run the ESM Server container in HTTP mode and to terminate TLS on an Ingress controller or a Load Balancer.

INTRODUCTION ON KEYSTORES

The `esmserver` container requires appropriate a Java keystore for enabling SSL security. The keystore

has to be provided for the deployment or a supplied store with self-signed certificate is used.

PREPARING A SELF-SIGNED JAVA KEYSTORE FOR TLS CONFIGURATION

IMPORTANT

Do not use self-signed certificates for other purposes than testing the configuration procedure. Rather than self-signed certificates, obtain certificates signed by a Certificate authority.

For the following sample deployment, the passwords which were used for `-storepass` and `-keypass` are written into the text files `./keystores/store_pw.txt` and `./keystores/key_pw.txt`

BUILDING A JAVA KEYSTORE FROM AN EXISTING PKCS12 KEYSTORE

Many organizations provide a prepared PKCS12 package, containing private key, public certificate and all required root certificates. In this case, the keystore can be converted into a Java keystore. For this purpose, the store password and the key password have to be provided by the Certificate Authority.

```
keytool -importkeystore -srckeystore ./keystores/server_keystore.p12 \  
-srcstorepass secret012 \  
-srcstoretype pkcs12 \  
-destkeystore server_keystore.jks \  
-storepass secret123
```

DEPLOYMENT

The following command will deploy the container with

- the Web UI on the external port 443
- SSL enabled for the Web UI
- SSL enabled for the Server (ActiveMQ Broker)
- the same keystore (as well as key and store password) for Web UI and Server
- a Data Volume for persistence of application data

The keystore is provided to the container as direct file mount.

```
docker run -d --name myesmserver \  
-p 443:8443 \  
-p 1883:1883 \  
-e JETTY_SECURE_ENABLED="true" \  
-v esm-vol:/opt/sm/server/karaf/db \  
-v ${PWD}/keystores/server_keystore.jks:/opt/sm/server/karaf/etc/ssl/keystore \  
esmserver:latest
```

The Web UI for the resulting container can be accessed via the default SSL port 443, but container-internally, the application will bind to the default port 8443: <https://dockerhost:443> (respectively: <https://dockerhost> as 443 is the default HTTPS port)

Configuration Variables

The configuration of the ESM Server is controlled by Environment Variables. The following chapters document the available variables grouped by topic.

General Configuration

- **TZ**
 - Default value: None. Depends on Container host.
 - Description: Native Linux environment variable which allows enforcing a specific timezone to be set inside the container. For possible values, please refer to https://en.wikipedia.org/wiki/List_of_tz_database_time_zones
- **LOG_LEVEL**
 - Default value: **INFO**
 - Description: Log level for messages forwarded to the Docker Logging (`docker logs`). The following values are supported:
 - **OFF**
 - **ALL**
 - **DEBUG**
 - **ERROR**
 - **FATAL**
 - **INFO**
 - **TRACE**
 - **WARN**

SSL Security

JETTY CONFIGURATION VARIABLES (WEB UI)

- **JETTY_SECURE_ENABLED**
 - Default value: false
 - Description: Value true activates SSL security of the Web UI.
- **SSL_KEYSTORE_FILE**
 - Default value: `/opt/sm/server/karaf/etc/ssl/keystore.jks`
 - Description: File path to Java keystore for the Web UI
- **SSL_KEYSTORE_PASSWORD**
 - Default value: password
 - Description: Password of the keystore for the Web UI.
- **SSL_TRUSTSTORE_FILE**

- Default value: /opt/sm/server/karaf/etc/ssl/truststore.jks
- Description: File path to Java truststore for the Web UI
- **SSL_TRUSTSTORE_PASSWORD**
 - Default value: password
 - Description: Password of the truststore for the Web UI.
- **SSL_KEY_PASSWORD**
 - Default value: password
 - Description: Password of the key for the Web UI.

SERVER CONFIGURATION VARIABLES (ACTIVEMQ BROKER)

- **SSL_KEYSTORE_FILE**
 - Default value: /opt/sm/server/karaf/etc/ssl/keystore.jks
 - Description: File path to Java keystore for the Web UI

Deploy ESM Server Container With IBM DB2 databases

ESM provides support for IBM DB2 databases to store monitoring data and configuration data. With this option, collected monitoring data are stored in a DB2 database, instead of the built-in H2 database.

NOTE

ESM Server needs access to an *existing*, but empty database. ESM Server will not create the database itself. Hence, the user id for accessing the database does not require permissions to create a database, but only to create database objects.

Run IBM DB2

As a requirement a DB2 Server (container or on prem) must be running and the planed ESM Server container must have acces through the network to it. The server needs to host the databases (two) for the ESM Server software. For this example the db names are confdb and mondb.

NOTE

ESM Server requires a Db2 database with a page size of 32768.

Provide Db2 JDBC Driver

It is required to provide a JDBC driver for IBM Db2. JDBC drivers required for ESM to establish connections to a DB2 database are not delivered with the ESM Container Images. Suitable JDBC drivers can be obtained from [IBM's website](#) or the [Maven repository](#).

The JDBC driver has to be provided to the container on a volume. This is accomplished by creating a new volume and copying the driver into a volume, which will then later be used during the creation of the ESM

Server container.

Example 8. Example for downloading the Db2 JDBC driver

```
wget -O db2jdbc.jar  
https://repo1.maven.org/maven2/com/ibm/db2/jcc/11.5.5.0/jcc-11.5.5.0.jar
```

To make the JDBC driver accessible to the ESM Server it needs to be copied to the `smdeploy` volume.

Example 9. Example for copying the Db2 JDBC driver to the "smdeploy" volume

```
# Create a temporary container  
docker container create \  
  --name temp \  
  -v smdeploy:/data \  
  esmserver:5.8.0.0-000  
  
# Use the container to copy the driver to the volume  
docker cp db2jdbc.jar temp:/data  
  
# Remove the temporary container  
docker rm temp
```

Run ESM Server Container

In addition to running the container with a built-in database, using a Db2 database requires passing of JDBC parameters to the container:

- `JDBC_DRIVER_NAME`: Most likely `com.ibm.db2.jcc.DB2Driver`. May differ for future versions of DB2 JDBC drivers.
- `JDBC_URL`: URL including host, port, and database name. In a container context, make sure a to use a valid IP or DNS name that resolves to the remote DB2 database or a local DB2 container.
- `JDBC_USER` and `JDBC_PASSWORD`: Credentials for accessing the database.
- `JDBC*` variables without prefix `MONITORING_` refer to the ESM configuration database. Variables including the prefix `MONITORING_` refer to the ESM monitoring database.

The following example shows how to start the ESM Server container based on the Db2 preparations accomplished previously:

Example 10. Example for using the local Db2 container with ESM Server

```
docker run -d --name smserver \  
  --net=smnet \  
  -p 8080:8080 \  
  -p 1883:1883 \  
  -v smdeploy:/opt/sm/server/karaf/deploy \  
  -e JDBC_DRIVER_NAME='com.ibm.db2.jcc.DB2Driver' \  
  -e JDBC_URL='jdbc:db2://mydb2:50000/confdb' \  
  -e JDBC_USER='db2inst1' \  
  -e JDBC_PASSWORD='MyDb2Database!' \  
  -e MONITORING_JDBC_DRIVER_NAME='com.ibm.db2.jcc.DB2Driver' \  
  -e MONITORING_JDBC_URL='jdbc:db2://mydb2:50000/mondb' \  
  -e MONITORING_JDBC_USER='db2inst1' \  
  -e MONITORING_JDBC_PASSWORD='MyDb2Database!' \  
  esmserver:5.8.0.0-000
```

Deploy ESM Server Container With SQL Server

ESM provides support for Microsoft SQL Server databases to store monitoring data and configuration data. With this option, collected monitoring data are stored in a DB2 database, instead of the built-in H2 database. Configuration data originating from configuration procedures in the Web UI cannot be stored in a DB2 database, but are still written to a built-in H2 database.

NOTE

ESM Server needs access to an *existing*, but empty database. ESM Server will not create the database itself. Hence, the user id for accessing the database does not require permissions to create a database, but only to create database objects.

Run a SQL Server

As a requirement a SQL Server (container or on prem) must be running and the planned ESM Server container must have access through the network to it. The server needs to host the databases (two) for the ESM Server software. For this example the db names are confdb and mondb.

NOTE

ESM Server requires a SQL database with Latin1_General_CI_AS collation. Also, assign the db_datareader, db_datawriter, db_owner and public roles within the database to the db user used for the deployment.

Provide SQL Server JDBC Driver

It is required to provide a JDBC driver for Microsoft SQL Server. JDBC drivers required for ESM to establish connections to a Microsoft SQL Server database are not delivered with the ESM Container Images. Suitable JDBC drivers can be obtained from [Microsoft's website](#) or the [Maven repository](#).

The JDBC driver has to be provided to the container on a volume. This is accomplished by creating a new volume and copying the driver into a volume, which will then later be used during the creation of the ESM Server container.

Example 11. Example for downloading the SQL Server JDBC driver

```
wget -O sqljdbc.jar  
https://repo1.maven.org/maven2/com/microsoft/sqlserver/mssql-  
jdbc/13.2.0.jre11/mssql-jdbc-13.2.0.jre11.jar
```

To make the JDBC driver accessible to the ESM Server it needs to be copied to the `smdeploy` volume.

Example 12. Example for copying the SQL Server JDBC driver to the "smdeploy" volume

```
# Create a temporary container  
docker container create \  
  --name temp \  
  -v smdeploy:/data \  
  esmserver:5.8.0.0-000  
  
# Use the container to copy the driver to the volume  
docker cp sqljdbc.jar temp:/data  
  
# Remove the temporary container  
docker rm temp
```

Run ESM Server Container

Example 13. Example for using the local SQL Server container with ESM Server

```
docker run -d --name smserver \
  --net=smnet \
  -p 8080:8080 \
  -p 1883:1883 \
  -v smdeploy:/opt/sm/server/karaf/deploy \
  -e JDBC_DRIVER_NAME='com.microsoft.sqlserver.jdbc.SQLServerDriver' \
  -e JDBC_URL='jdbc:sqlserver://sqlserver:1433;databaseName=confdb' \
  -e JDBC_USER='sa' \
  -e JDBC_PASSWORD='MySQLServerDatabase!' \
  -e \
  MONITORING_JDBC_DRIVER_NAME='com.microsoft.sqlserver.jdbc.SQLServerDriver' \
  -e MONITORING_JDBC_URL='jdbc:sqlserver://sqlserver:1433;databaseName=mondb' \
  \
  -e MONITORING_JDBC_USER='sa' \
  -e MONITORING_JDBC_PASSWORD='MySQLServerDatabase!' \
  esmserver:5.8.0.0-000
```

Deploying ESM Agent (`esmagent`)

In contrast to the `esmserver` container, the `esmagent` container does not need to persist configuration or event data. Configuration data is loaded from the ESM Server during startup and runtime of the Agent process.

Prepare Docker Network

In order to enable communication inbetween the ESM Server container and the ESM Agent container, in a standard Docker environment, both containers have to be part of the same "Docker Network".

NOTE

Connecting container using the `--link` argument is considered deprecated. Visit the official Docker documentation for more details ([Legacy container links](#)).

Create a Docker Network of type "Bridge":

```
> docker network create -d bridge esmnet
```

To verify the creation of the network and list all networks present in the environment, use the `docker network list` command:


```
> docker network list
NETWORK ID          NAME          DRIVER          SCOPE
362392273c1a       bridge       bridge         local
9c8d425blea9       esmnet       bridge         local
2ce2cd9f0b96       host        host          local
392ae2b9ed33       none        null          local
```

IMPORTANT

To use ESM (`esmagent`) to monitor applications in the same Docker environment, it is required for the container to be able to connect to the application containers in order to acquire monitoring information from the applications.

Connect a running `esmserver` container to the network

To join the previously created `esmserver` container in the network, the `docker network connect` command can be used:

```
> docker network connect esmnet myesmserver
```

Example for joining in `esmserver` container into the network on container start:

```
> docker run -d --name myesmserver \
--net=esmnet \
-p 80:8080 \
-p 1883:1883 \
esmserver:latest
```

Run a `esmagent` container

To run a `esmagent` container, two container parameters are required:

- **SERVER_HOSTNAME**
 - Default value: `localhost`
 - Description: Use the name of the ESM Server container the agent shall be connected to. In the previous examples this name is `myesmserver`. To obtain the name of your deployed container, use the command `docker ps` in order to show all running containers.
- **CLIENT_ID**
 - Default value: `ESMAgent`

- Description: Each individual Agent container needs to be configured with a unique `CLIENT_ID`. Otherwise the ESM Server will not be able to distinguish event data from different Agent containers.

```
docker run -d \  
--net=esmnet \  
--name MyESMAgent \  
-e SERVER_HOSTNAME="myesmserver" \  
-e CLIENT_ID="myfirstagent" \  
esmagent:latest
```

After this deployment, the Agent will connect to the ESM Server and will show up in the list of connected agents.

Installation on a Container Orchestration Platform

For deploying ESM on a Kubernetes or OpenShift Cluster see the available field guides at [Cenit's Field Guide website](#).

Appendix A: Copyright notice

IBM Enterprise Content Management System Monitor

© Copyright CENIT AG 2000, 2026, © Copyright IBM Corp. 2005, 2026 including this documentation and all software.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without prior written permission of the copyright owners. The copyright owners grant you limited permission to make hard copy or other reproductions of any machine-readable documentation for your own use, provided that each such reproduction shall carry the original copyright notice. No other rights under copyright are granted without prior written permission of the copyright owners. The document is not intended for production and is furnished as is without warranty of any kind. *All warranties on this document are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.*

NOTE

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Appendix B: Notices

This information was developed for products and services offered in the U.S.A.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Appendix C: Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others



Product Number: 5724-R91

Printed in USA

SC27-9241-09