EOS System Manual

Table of Contents

Prerequisites

Microsoft SQL Server 2008 or later

The Ecrion Omni System platform requires to be connected to a **Microsoft SQL Server database.**

> Before proceeding to install the EOS software, you must create a Database (the default name used in the installer is “EOSDB4”) and ensure that the user under which the Authentication will be made has Database Admin rights.

.Net Framework 4.5

The .Net Framework 4.5 can be downloaded from the Microsoft website, from this download link.

For important information about this release, see the .Net Framework 4.5 Readme File.

IIS 7.0 or later with URL Rewrite module

The Internet Information Services (IIS) for Windows® Server is a flexible, secure and manageable Web server for hosting anything on the Web. You can read more on installing IIS 7 here.

The URL Rewrite module is also a requirement. It is a free extension provided by Microsoft for IIS 7 or later. See this link for overview and installation steps.

Software and Hardware Requirements

Hardware Requirements

Minimum	**Recommended**
1 CPU/4 Cores i5 @ 2 GHZ	2 CPU/8 Cores XEON @ 3 GHZ
4 GB of RAM	16 GB of RAM
10 GB disk space	1 TB disk space

Software Requirements

Minimum	**Recommended**
Windows Vista SP2 x86	Windows Server 2012 R2 x64 or later

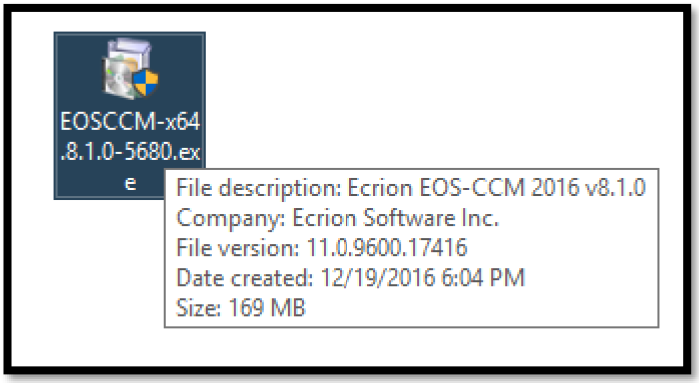
Installation Guide

This section is a step by step guide to installing EOS using the installer.

Naming Conventions

The setup name has the following structure: **Product Name** – **Architecture** – **Build Version** – **Build Number**. In the example below, we can identify the details mentioned as follows:

- **Product Name**: EOSCCM
- **Bit Version:** x64
- **Build Version**: 8.1.0
- **Build Number**: 5680



EOSCCM-x64.8.1.0-5680.exe

File description: Ecrion EOS-CCM 2016 v8.1.0
Company: Ecrion Software Inc.
File version: 11.0.9600.17416
Date created: 12/19/2016 6:04 PM
Size: 169 MB

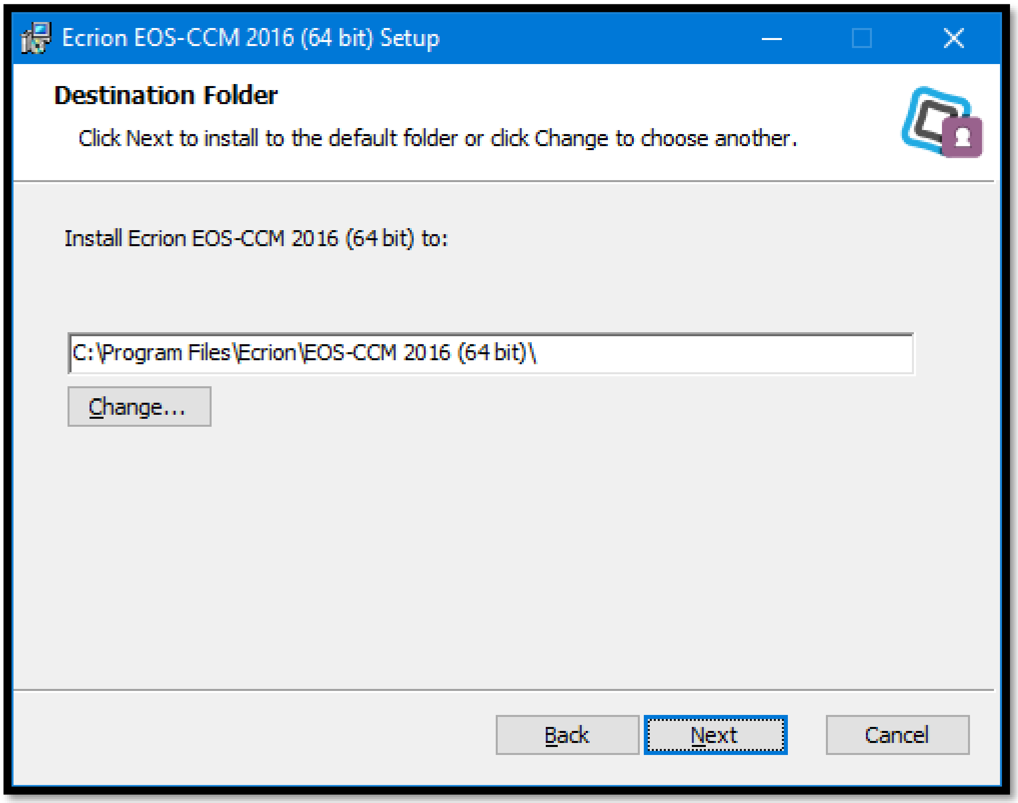
Run the installer to begin the process.

Step - Destination Folder

After initialization and accepting the license agreement, this step lets you set the location where the EOS software will be installed.

To modify the path, select the “Change” button in the middle-left side of the window and provide the destination folder for the installation.

Once you have the folder set, click on “Next” to continue with the installation.



Ecrion EOS-CCM 2016 (64 bit) Setup

Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Ecrion EOS-CCM 2016 (64 bit) to:

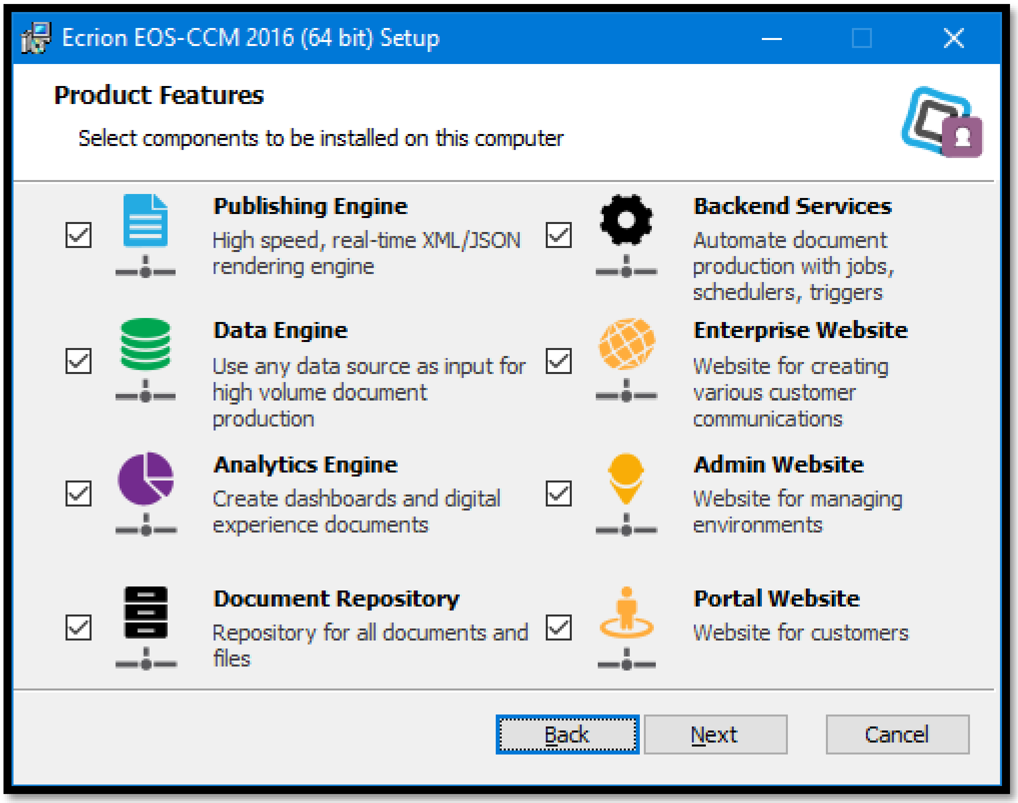
C:\Program Files\Ecrion\EOS-CCM 2016 (64 bit)\

Next, you will decide which Product Features will be installed on the machine.

Step - Product Features Selection

Ecrion Omni System provides a series of features which can be chosen during this step of the installation. Each component is provided with a short description on its functionality.

By default, all features are selected. You can decline the installation of a component by de-selecting the associated check-box. Not selecting a component will render the user unable to finish the installation.



Ecrion EOS-CCM 2016 (64 bit) Setup

Product Features

Select components to be installed on this computer

☑ **Publishing Engine**
High speed, real-time XML/JSON rendering engine

☑ **Backend Services**
Automate document production with jobs, schedulers, triggers

☑ **Data Engine**
Use any data source as input for high volume document production

☑ **Enterprise Website**
Website for creating various customer communications

☑ **Analytics Engine**
Create dashboards and digital experience documents

☑ **Admin Website**
Website for managing environments

☑ **Document Repository**
Repository for all documents and files

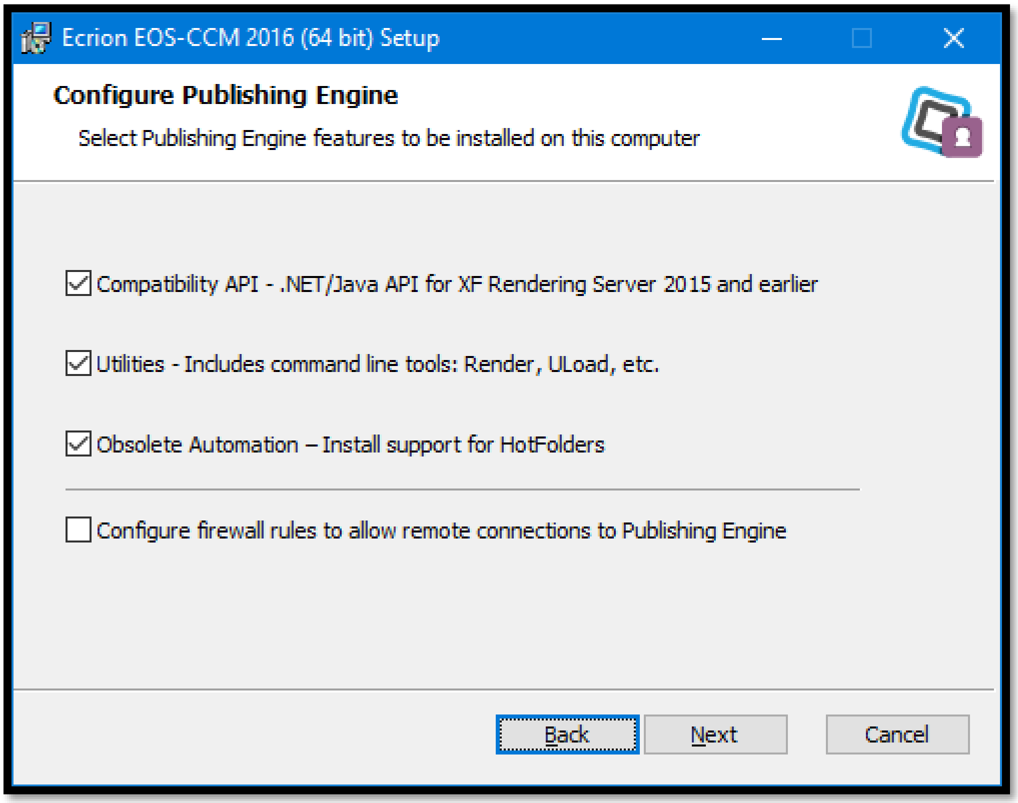
☑ **Portal Website**
Website for customers

Note: The components can be installed all on the same machine, or on separate boxes, but you will need to ensure that the IPs of the machines where you installed components are set correctly in the "Dependent Services Settings" step.

Once you select the needed components, select "Next" to proceed with configuring the required settings for each component.

Step - Publishing Engine & Data Engine

Several features are available for the Publishing Engine, including the ability to configure firewall rules via this Setup Wizard.



Ecrion EOS-CCM 2016 (64 bit) Setup

Configure Publishing Engine

Select Publishing Engine features to be installed on this computer

☑ Compatibility API - .NET/Java API for XF Rendering Server 2015 and earlier

☑ Utilities - Includes command line tools: Render, ULoad, etc.

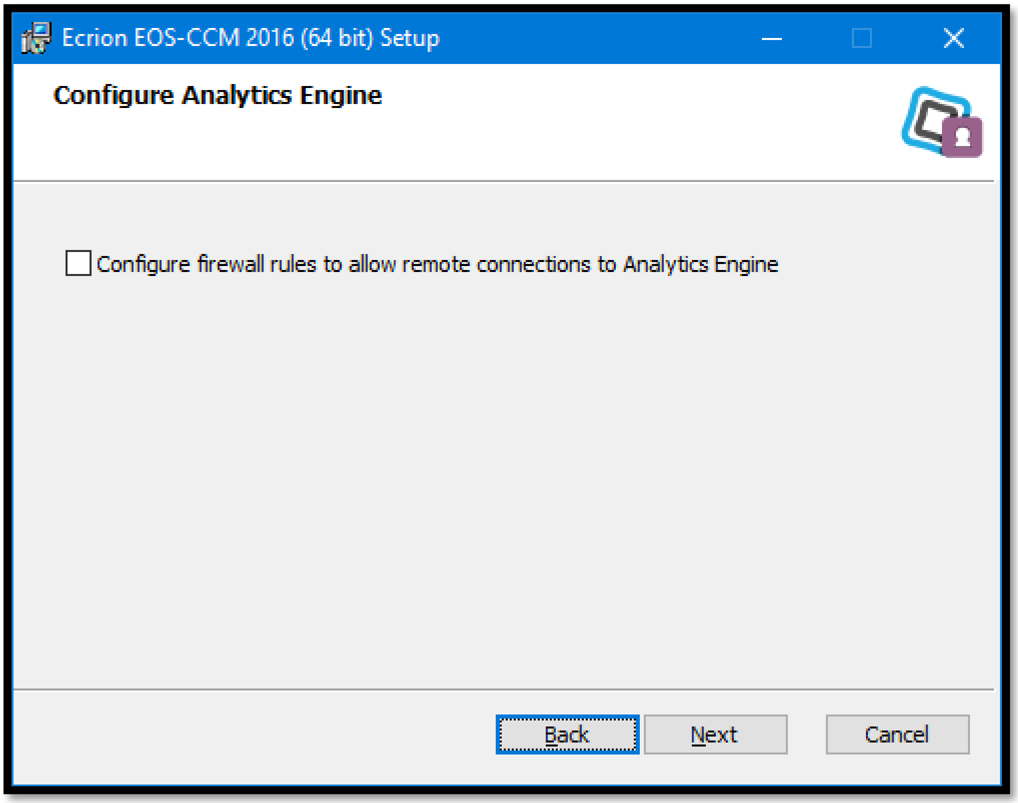
☑ Obsolete Automation – Install support for HotFolders

☐ Configure firewall rules to allow remote connections to Publishing Engine

Selecting the last checkbox will automatically add a firewall rule to allow the incoming requests to connect to the Publishing Engine.

The Data Engine has the same settings and can be configured in a similar fashion.

Step - Analytics Engine



Configure Analytics Engine

□ Configure firewall rules to allow remote connections to Analytics Engine

The analytics Engine can only be set to add automatically a rule for the firewall to allow incoming requests.

Step - Database Settings

In the next step, you will need to select a database provider.
You have two options: either use a previous configuration, or create a new SQL connection.

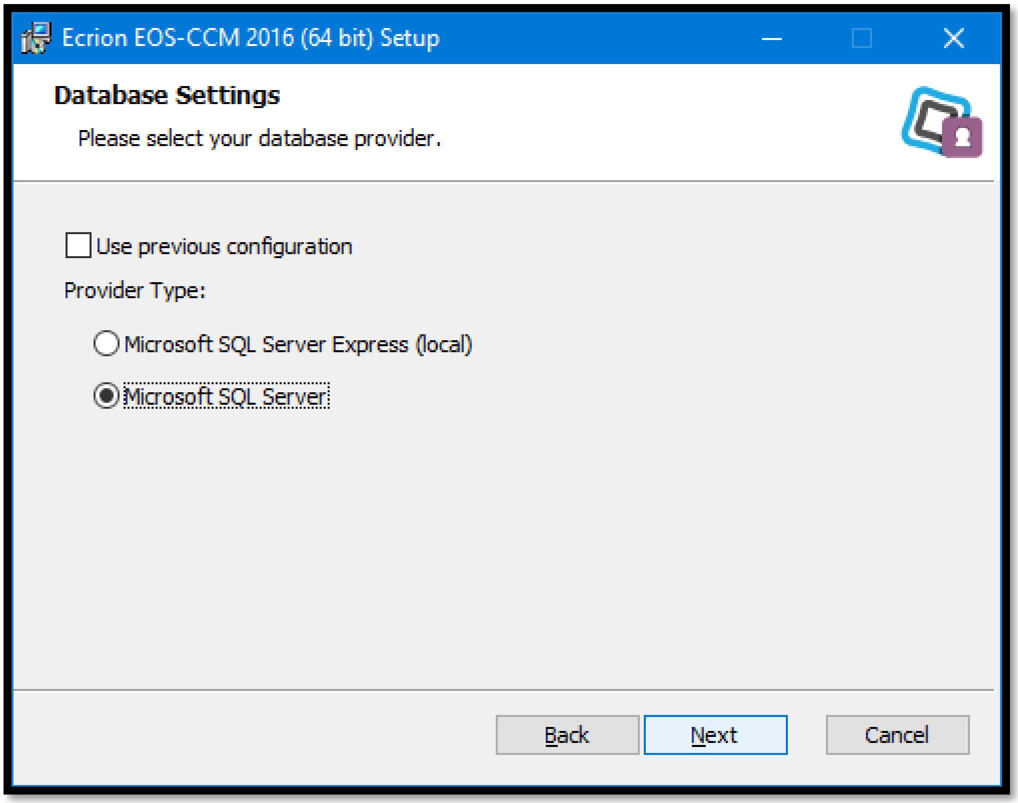
Using Existing SQL Database

If you choose the “Use previous configuration” button, then the settings made in a previous install of the EOS software will be used.

Using New SQL Database

If you un-check the option “Use previous configuration”, then you must choose the Provider Type out of two options:

- **Microsoft SQL Server Express** (local)
- **Microsoft SQL Server**



Ecrion EOS-CCM 2016 (64 bit) Setup

Database Settings

Please select your database provider.

□ Use previous configuration

Provider Type:

○ Microsoft SQL Server Express (local)

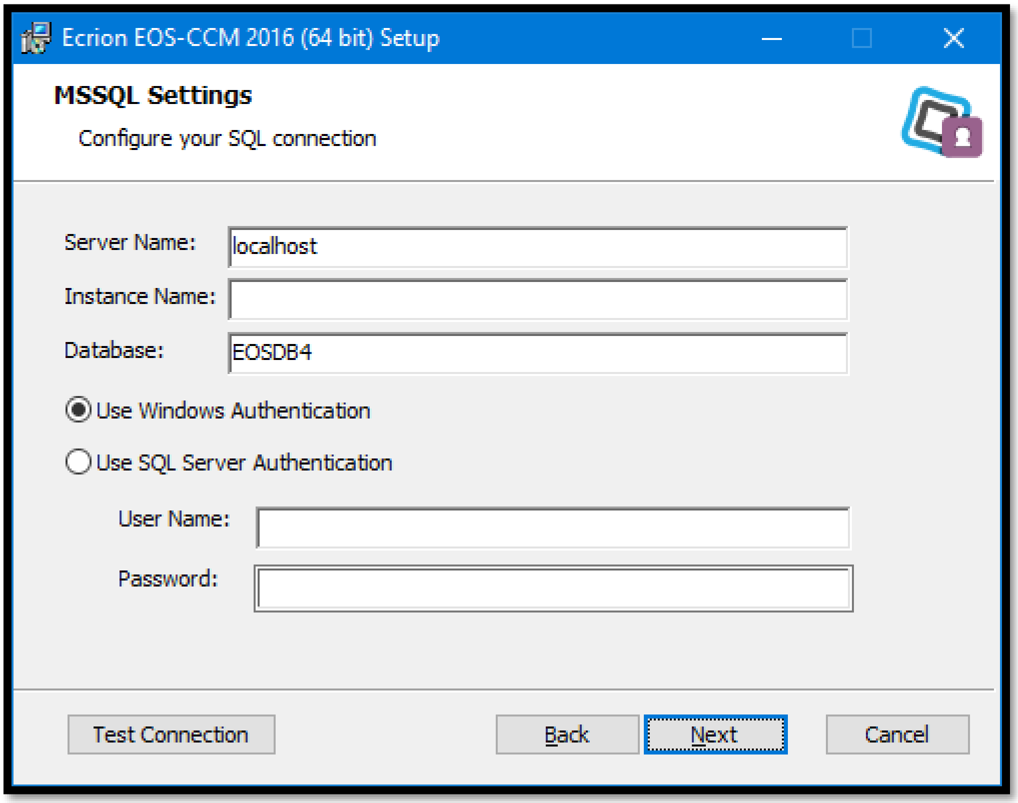
● Microsoft SQL Server

Microsoft SQL Server

If you choose the **Microsoft SQL Server**, then you need to provide the following information:

- **The Server Name** – the IP of the machine where the Microsoft SQL Server is installed
- **The Database Name** – the name of the database previously created
- **The Authentication Type** – Windows or SQL Server. Note: the user must have *db_owner* rights.
- [Optional] **Instance Name**, if you have the Microsoft SQL Server installed as a named instance.

Once you provide all the necessary data, you can test the connection to ensure that all fields have been set up properly, by clicking the “Test Connection” button.



Ecrion EOS-CCM 2016 (64 bit) Setup

MSSQL Settings

Configure your SQL connection

Server Name: localhost

Instance Name:

Database: EOSDB4

● Use Windows Authentication

○ Use SQL Server Authentication

User Name:

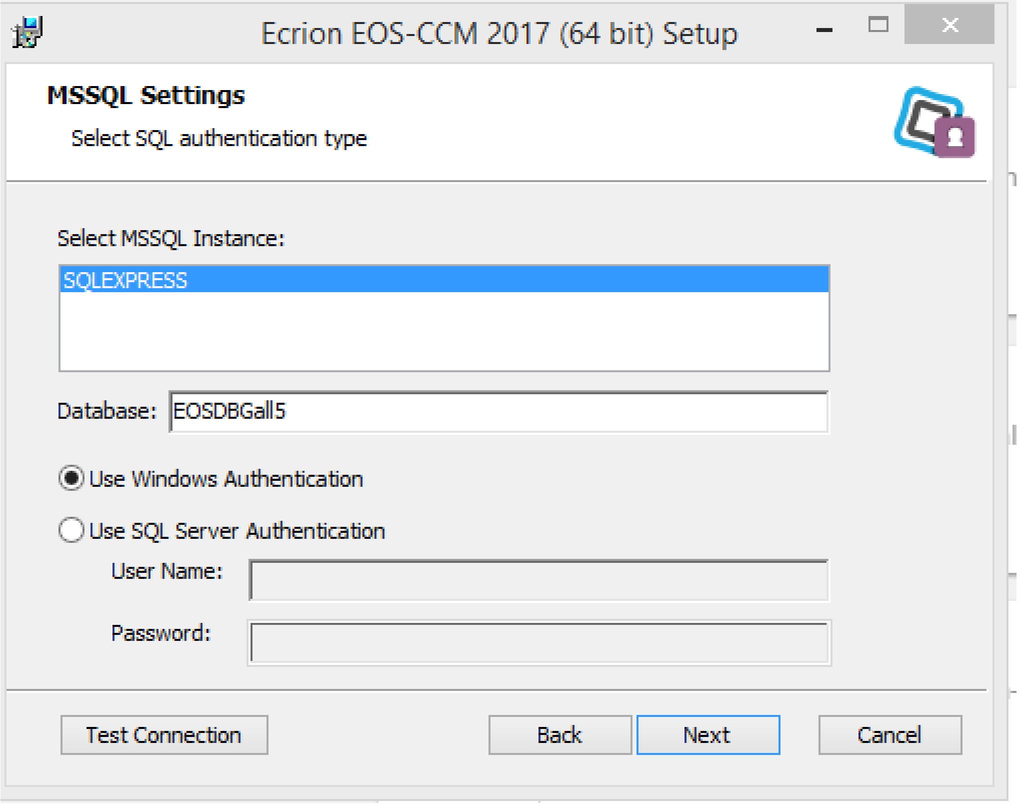
Password:

Microsoft SQL Server Express (local)

If you choose the **Microsoft SQL Server Express (local)**, then you need to provide the following information:

- **The MSSQL Instance**
- **The Database Name** – the name of the database previously created (default is **EOSDB4**)
- **The Authentication Type** – Windows or SQL Server. Note: the user must have *db_owner* rights.

Once you provide all the necessary data, you can test the connection to ensure that all fields have been set up properly, by clicking the “Test Connection” button.



Ecrion EOS-CCM 2017 (64 bit) Setup

MSSQL Settings

Select SQL authentication type

Select MSSQL Instance: SQLEXPRESS

Database: EOSDBGall5

● Use Windows Authentication

○ Use SQL Server Authentication

User Name:

Password:

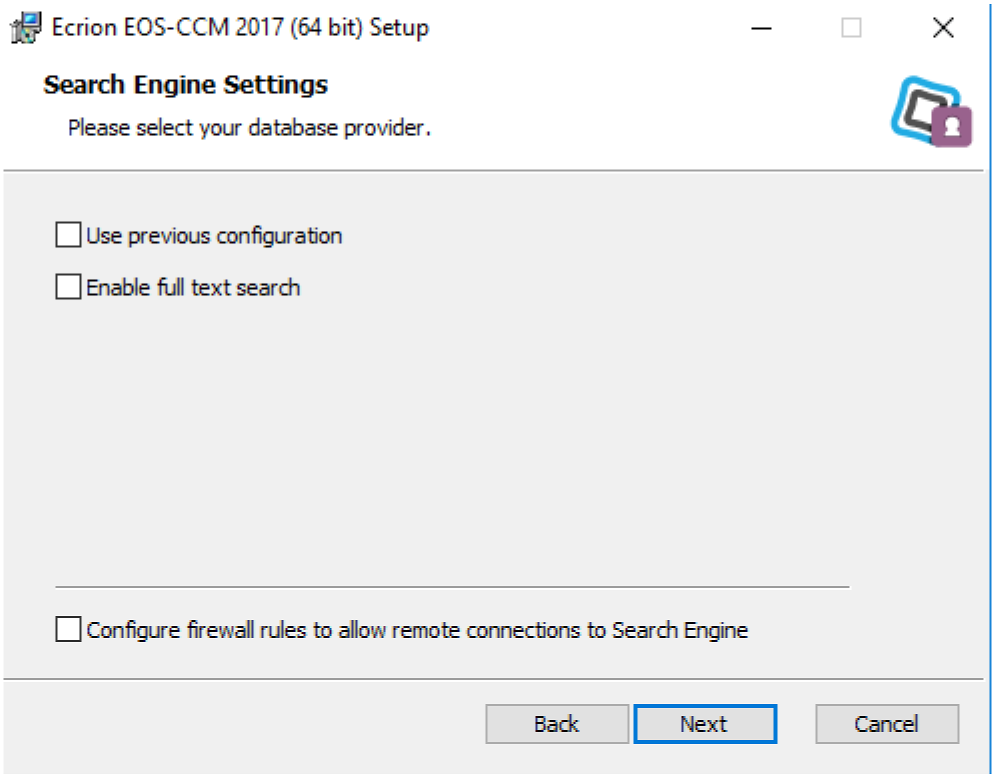
Step – Configure Search

The next step allows you to configure search, specifically the search database. There is an option to use the previous configuration, similar to the main database, but you can also use a different database.

There are a few considerations regarding the database:

- The database must exist and the user must have *db_owner* rights.
- If it's a Windows user (as opposed to a SQL Server user), then **the user must be the same one used for the EOS database**.
- In order to enable full text search, the MS SQL Server hosting the database must have the "Full Text and Semantic Extractions for Search" feature enabled. You also need to check "Enable full text search" in the EOS setup.

At this screen, you may also check the last box to configure the firewall so as to allow remote connections to the search engine. Do this if the machine you are currently running the installer on is going to be separate from the machines where the other components are installed.



Ecrion EOS-CCM 2017 (64 bit) Setup

Search Engine Settings

Please select your database provider.

□ Use previous configuration

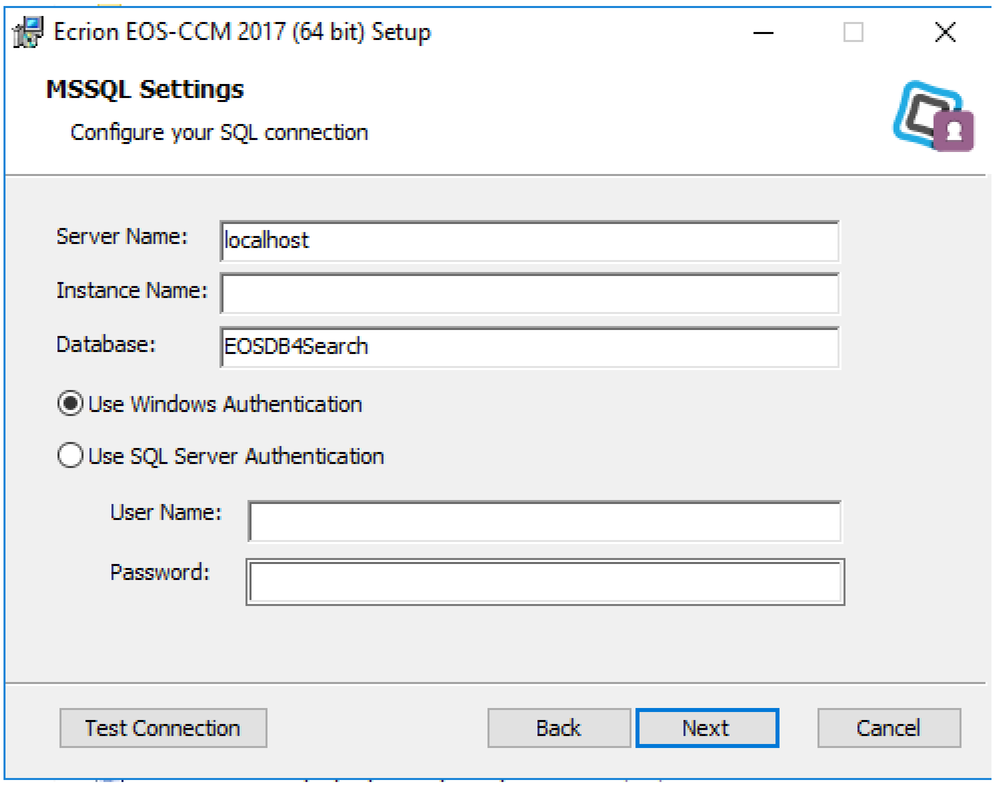
□ Enable full text search

□ Configure firewall rules to allow remote connections to Search Engine

Next, you will need to provide the following information:

- **The Server Name** – the IP of the machine where the Microsoft SQL Server is installed
- **The Database Name** – the name of the database previously created
- **The Authentication Type** – Windows or SQL Server. Note: the user must have *db_owner* rights. If it's a Windows user (as opposed to a SQL Server user), then **the user must be the same one used for the EOS database**.
- [Optional] **Instance Name**, if you have the Microsoft SQL Server installed as a named instance.

Once you provide all the necessary data, you can test the connection to ensure that all fields have been set up properly, by clicking the "Test Connection" button.



Ecrion EOS-CCM 2017 (64 bit) Setup

MSSQL Settings

Configure your SQL connection

Server Name: localhost

Instance Name:

Database: EOSDB4Search

● Use Windows Authentication

○ Use SQL Server Authentication

User Name:

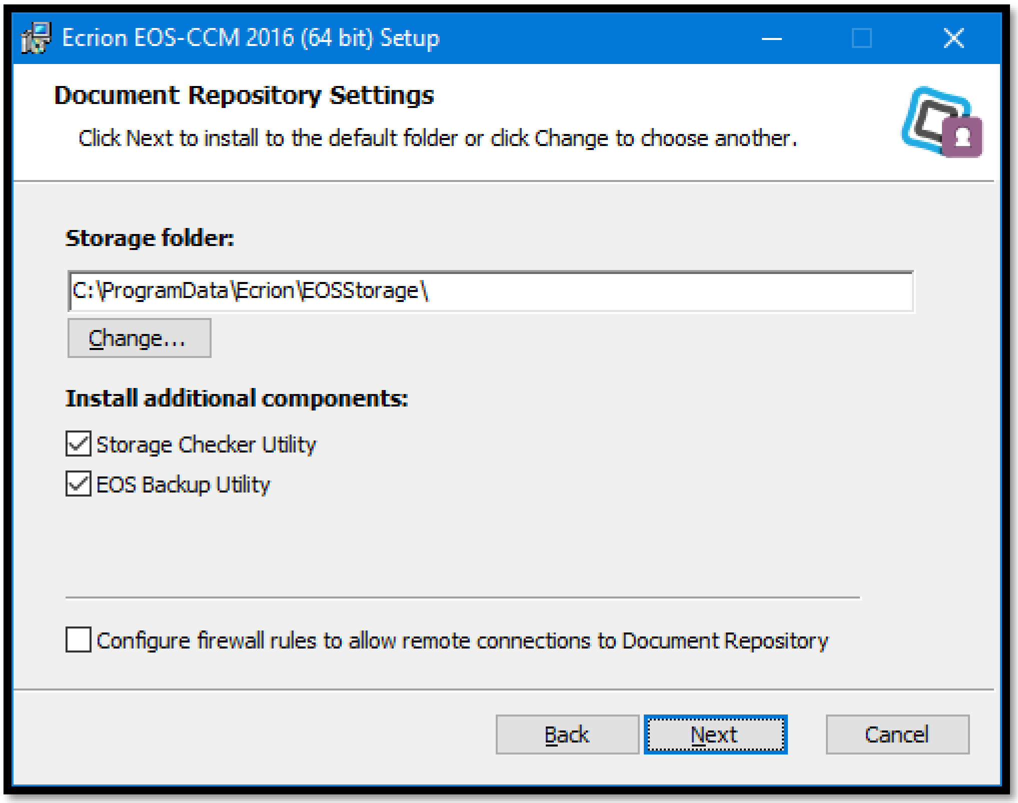
Password:

Step - Document Repository

After you finish configuring your Database Settings, you must proceed to set the EOS Repository folder and components.

You can also check an option for firewall rules on remote connections to the Document Repository.

You can also choose to install the "**Storage Checker Utility**" and "EOS Backup Utility" which are checked by default and we strongly recommend that they be installed.



Ecrion EOS-CCM 2016 (64 bit) Setup

Document Repository Settings

Click Next to install to the default folder or click Change to choose another.

Storage folder:

C:\ProgramData\Ecrion\EOSStorage\

Install additional components:

☑ Storage Checker Utility

☑ EOS Backup Utility

□ Configure firewall rules to allow remote connections to Document Repository

Step - Backend Services

During this phase of the Install Wizard, you can choose the additional components that come with the Backend Services component:

- **DITA** – Optionally install DITA Open Toolkit. Read more about DITA-OT here. The version of DITA that ships with EOS contains additional plugins for compatibility with our product suite.
- **Pre-Production Test Utility** – Performs a smoke check of all the functionality of the system

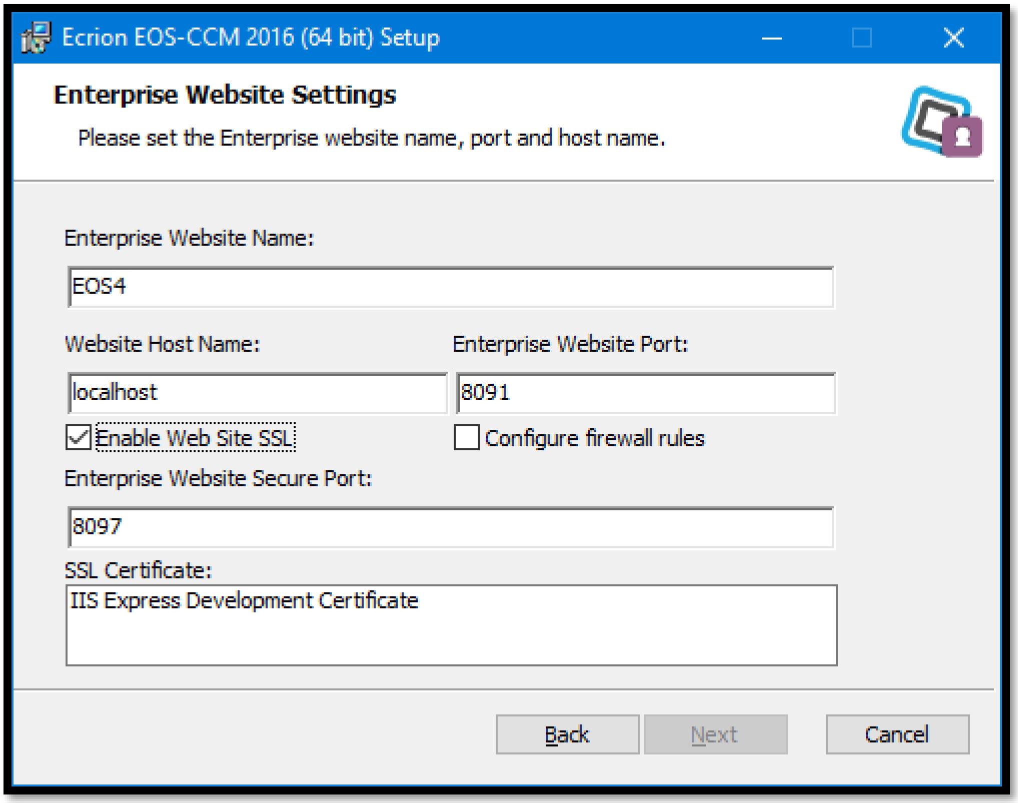
You can select if a firewall rule should be added to allow incoming requests to the Backend Services.

Step - Enterprise Website

If you choose the "Enterprise Website" component, you will be prompted to choose the Website name, port and host name.

You also have two options that can be checked/un-checked:

- **Enable Web Site SSL** – Makes the site also be accessible via HTTPS (requires a preinstalled SSL certificate)
- **Configure firewall rules** – Configures firewall to allow access to the Enterprise Website via the specified port(s)



Enterprise Website Settings

Please set the Enterprise website name, port and host name.

Enterprise Website Name: EOS4

Website Host Name: localhost

Enterprise Website Port: 8091

☑ Enable Web Site SSL

□ Configure firewall rules

Enterprise Website Secure Port: 8097

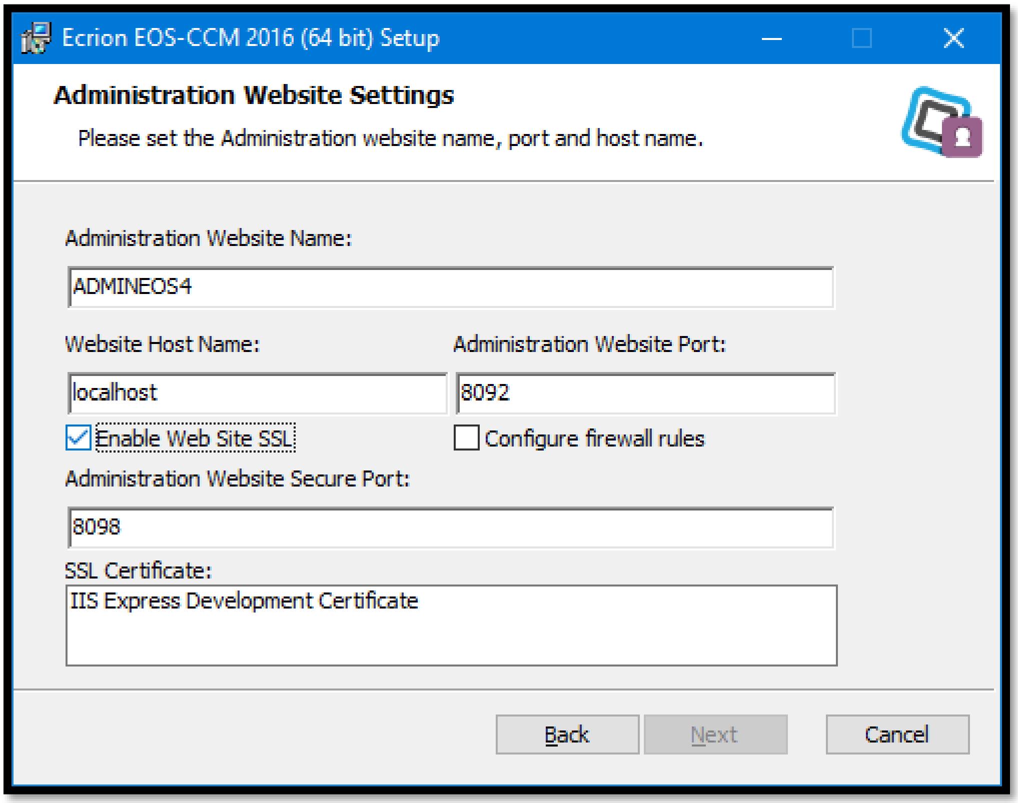
SSL Certificate: IIS Express Development Certificate

If you Enable the Web Site SSL, two additional fields will appear:

- **Enterprise Website Secure Port** – Select the port to use for HTTPS access; this must be different than the HTTP port (and ports used by the other websites). You may disable HTTP access to the website from IIS Manager after running the setup.
- **SSL Certificate** – Select an SSL Certificate for enabling HTTPS access; **this must already be installed on the system, prior to launching the setup.**

Step - Administration Website

Like the "Enterprise Website" component, the Administration Website component needs to be configured by providing the Administration website name, port and host name.



Ecrion EOS-CCM 2016 (64 bit) Setup

Administration Website Settings

Please set the Administration website name, port and host name.

Administration Website Name: ADMINEOS4

Website Host Name: localhost

Administration Website Port: 8092

☑ Enable Web Site SSL

□ Configure firewall rules

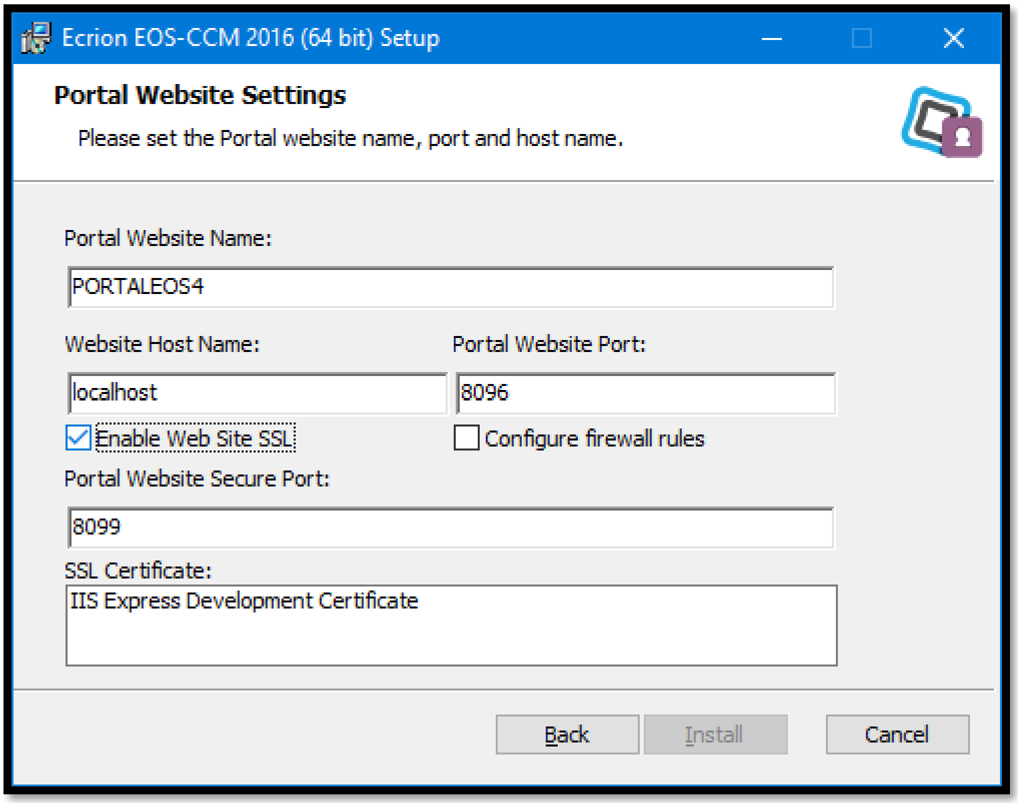
Administration Website Secure Port: 8098

SSL Certificate: IIS Express Development Certificate

You can also enable the Web Site SSL and automatically add firewall rules for incoming requests.

Step - Portal Website

For this component, you must also specify the Portal website name, port and host name. Both firewall rules and Web Site SSL are available settings to enable and configure.



Ecrion EOS-CCM 2016 (64 bit) Setup

Portal Website Settings

Please set the Portal website name, port and host name.

Portal Website Name: PORTALEOS4

Website Host Name: localhost

Portal Website Port: 8096

☑ Enable Web Site SSL

□ Configure firewall rules

Portal Website Secure Port: 8099

SSL Certificate: IIS Express Development Certificate

Once you finish configuring the components, you can click the “Install” button, located in the bottom region of the Setup Wizard window, and the setup will proceed to install the EOS software.

Post-Installation Tasks

Changing Initial Configuration

Some settings like **database**, **storage**, **ports** or **SSL** are configured during installation. To modify these settings, we recommend running the installer again. You might need to first uninstall the product from **Control Panel**.

The installer will automatically detect previous database/storage configurations and offer to use them. We recommend that you use this option. You will still be able to review and modify settings other than the database and storage if you use this option.

If you need to specify database and storage explicitly, read below. Note that this is **NOT recommended** when there is a previous configuration available.

If you point the installer explicitly to a database previously used by EOS, the installer will upgrade the database to the current version while preserving its contents.

If you point the installer explicitly to a storage folder previously used by EOS, the installer will use the contents of that folder without deleting them.

Note: The database and storage are deeply linked with each other and cannot function properly if they are out of sync. It's **critical** that the database and storage selected have been used by **EOS** in the same configuration and have not been altered since the last time they were used.

Updating IIS Bindings

Follow these steps for each of the EOS websites that you want accessible remotely:

1) Open **IIS Manager**.
2) Navigate to the website exhibiting the problem.
3) On the right-side panel, click **Bindings**.
4) Edit the existing binding and change **localhost** to *****.
5) Click **OK**.

Note: If you do this, the website will be accessible from the intranet if the firewall allows it. Make sure that this is the intended functionality and that website access (especially for System Administration) is properly secured before making the change.

Installing and Activating Licenses

Finding Your Licenses

To find your licenses, log in to https://accounts.ecrion.com (the **Sign In** link on the main website) and navigate to the **Product Keys** section. Here you can see all your licenses and on which machines they have been activated.

To view details for a license, click its ID on the first column. The ID should be a 5-digit numeral. A dialog will appear.

In the dialog, click **Install License** and a new dialog will appear, containing a license key consisting of digits and letters – this is what we will use to install the license.

License Administrator

On the server, open the **Management Console** by clicking **Start** and typing "Management Console". Click on **License Administrator** on the left. On older installations, **License Administrator** might be a separate executable.

Both executables should be located under **C:\Program Files\Ecrion\EOS-CCM 2017 (64 bit)\Engines\Bin**.

Note: If you have multiple Ecrion products installed, you might find multiple versions of these applications on your machine. You can safely use any instance of either **Management Console** or **License Administrator** to manage licenses for any Ecrion product.

Installing Licenses

In the **License Administrator**, click **Install**. In the wizard that appears, paste the license key from the website, click **Next** and **Finish**.

The next step will be to activate the license. The license will not be usable until activated.

If you skip this step now, you can activate the license by selecting it in the list and clicking **Activate**. The activation dialog will prompt you to choose between either online or offline activation.

Online Activation

If your server has internet access, we recommend using online activation. Select **Online** in the activation wizard.

When prompted for a username and password, use the same credentials as on the Ecrion website (i.e. from https://accounts.ecrion.com – your EOS credentials will not work here). Continue the wizard until the end, waiting for activation at the corresponding step. Your license should now be activated.

Note: If there was a problem activating the license, the wizard will automatically prompt for offline activation.

Offline Activation

If your server is offline or cannot otherwise communicate with our licensing server, we recommend using offline activation. Select **Offline** in the activation wizard.

The wizard will generate an activation key. Copy the activation key.

On a machine with internet access, go back to the website and find the license you are trying to activate. Click on the license ID and click **Install License**.

A new dialog will appear, with an empty textbox. Paste the activation key there and click **Installs**.

The website will reply with a response key. Copy the response key.

On the server, paste the response key in the textbox below the activation key. Continue the wizard until the end. Your license should now be activated.

Uninstalling Licenses

The uninstall process is very similar to the install process, providing both an online and offline method.

In the **License Administrator**, click on the license you want to uninstall and go through the wizard.

You will be prompted for a user name and password. Use the same Ecrion website credentials used during activation.

If online activation fails, the wizard will switch to offline uninstallation. It will provide an uninstall key which you need to use on the website.

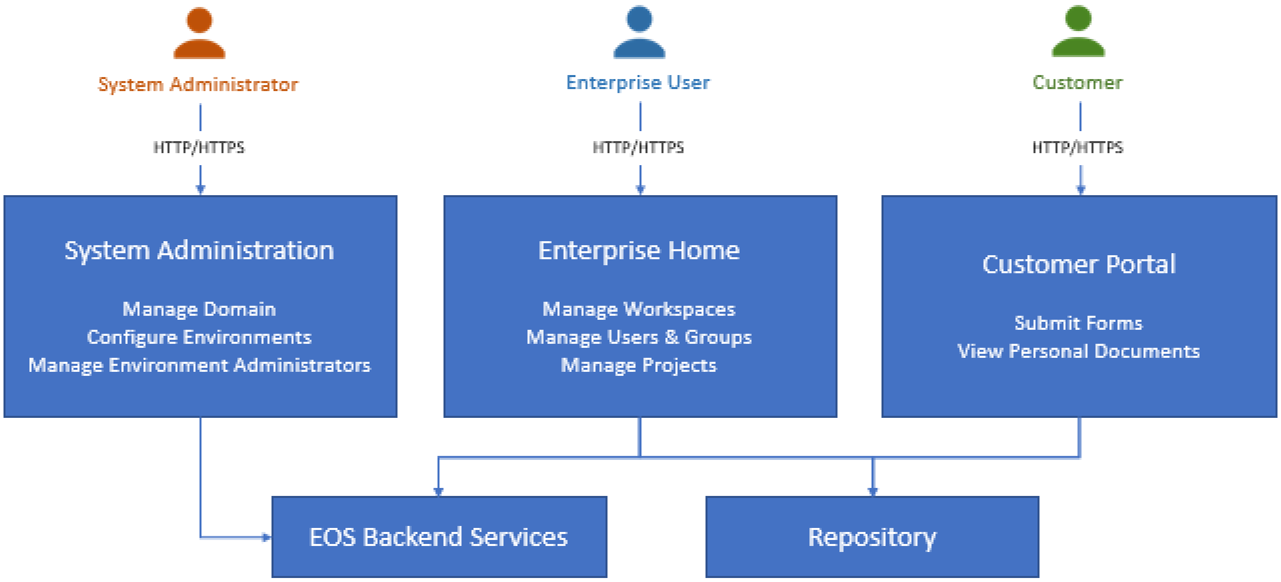
On the website, find the license that you are uninstalling and click on its ID in the list.

Click **Uninstall License** in the dialog that appears and paste the key. Click **Uninstall**.

Note: If you skip this step, the license will continue to appear as being used and be unusable on another machine unless manually freed by Ecrion Support. Contact support@ecrion.com to request freeing a license that is not being used anymore.

System Architecture

Architecture Overview



The main components of EOS are:

- **Enterprise Home / Web Front-End** – IIS website providing access to enterprise users. Default port: 8094
- **Customer Portal Front-End** – IIS website providing access to customers. Default port: 8096
- **System Administration Front-End** – IIS website providing access to administrators. Default port: 8095
- **Backend Services** – Windows services for EOS, Publishing, Data, Analytics, Search

- **Database** – SQL Server database containing system configuration and repository metadata
- **File Storage** – Folder containing repository binary data (file contents)

Each component may reside on a different machine, while the backend services may be further split across multiple machines. The file storage may reside on a SAN/NAS.

Application File Locations

System files for EOS are placed in the following locations:

- **Application Installation Folder** – This is where the product is installed. The directory contains all the binaries for the websites and backend services. In a default installation, this is **C:\Program Files\Ecrion\<Product Name>**.
- **Application Data Folder** – This directory contains the configuration files for the EOS components. It is located under **C:\ProgramData\Ecrion**. The main configuration file is **EOS4.config** and is loaded on start-up by all websites and the EOS service. Any changes made to the main config require a restart of both the EOS service and websites (e.g. using **iisreset**). The Publishing, Data and Analytics services have separate config files named the same as the corresponding executable, respectively **PublisherSvc.config**, **DASSvc.config**, **BISvc.config**. Any changes made to the main config files require a restart of the associated service.
- **Log Folder** – This directory contains the log files for the EOS components. Unless otherwise specified, the default log location is **<ApplicationDataFolder>\Log**, with log files named after their respective executable or website.
- **Storage Folder** – This directory represents the File Storage component, located by default at **<Application Data Folder>\EOSStorage4**
- **Public Folder** – This directory contains public samples for installed Ecrion products. It is deployed during installation, but is not required by EOS to function correctly.

Distributed Configurations

Distributed configurations are possible, but may require the use of additional licenses. Some servers may only require the licenses to enable the functionality provided by the respective website or service.

Distributed Components

It’s possible to have your components distributed across multiple servers. The most distributed setup that is possible without replicating any component has each of the following on a different machine:

- **Enterprise Home / Web Front-End** – “EOS4” in IIS, port 8094
- **Customer Portal Front-End** – “PORTALEOS4” in IIS, port 8096
- **System Administration Front-End** – “ADMINEOS4” in IIS, port 8095
- **EOS Service** – “EOS4Svc.exe”
- **Publishing Service** – “PublisherSvc.exe”
- **Data Service** – “DASSvc.exe”
- **Analytics Service** – “BISvc.exe”
- **Database** – “EOSDB4” in SQL Server (default value)

- **File Storage** – "C:\ProgramData\Ecrion\EOSStorage" (default value)

When installing a website on a different machine than the EOS Service, the main configuration file on the machine hosting the website must be updated with the following information:

```
XFServerAddress=<Publishing Service IP>
DASAddress=<Data Service IP>
BIAddress=<Analytics Service IP>
ESSAddress=<EOS Service IP>
RepositoryAddress=<EOS Service IP>
LogAddress=<EOS Service IP>
WorkAddress=<EOS Service IP>
BackgroundServerAddress=<EOS Service IP>
```

Multiple Workers

Multiple Publishing, Data and Analytics nodes may be used by the same EOS server to boost throughput. The nodes will be selected using round-robin. This functionality is native to EOS and does not require an external load balancer.

Additional workers may be added from the sysadmin interface for each environment using the **Edit Environment** dialog. The settings are located under the **Reporting**, **Data** and **Analytics** tabs respectively.

By default, no nodes are configured, in which case EOS will look for the services at the address specified by the following values specified in the main config:

- **Publishing** – "XFServerAddress" (default "127.0.0.1")
- **Data** – "DASAddress" (default "127.0.0.1")
- **Analytics** – "BIAddress" (default "127.0.0.1")

To add a new worker node, you will need to specify the hostname/IP of the server where that instance resides and the appropriate port. The default ports for each service are listed below:

- **Publishing** – 40017
- **Data** – 40021
- **Analytics** – 40023

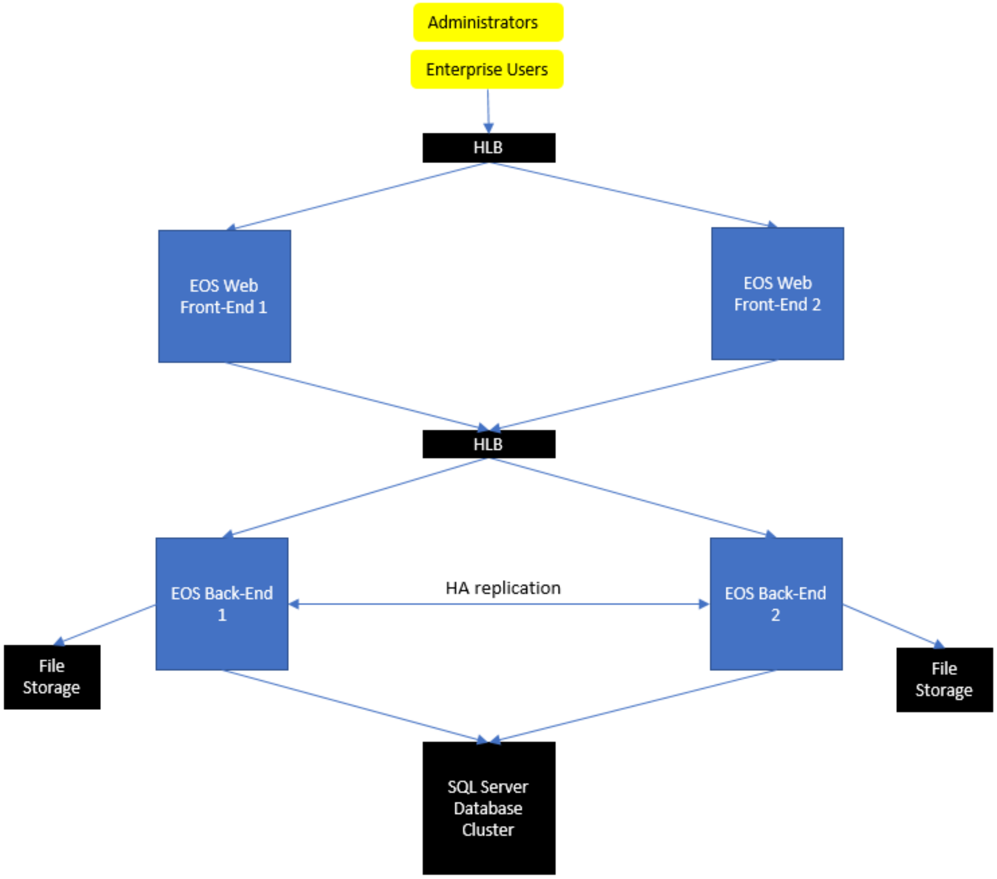
The machine containing the EOS Service will need to have in its main config file the following line:

```
RepositoryAddress=<EOS Service IP>
```

Note: The IP used above must be the IP as seen from the machine(s) where the Publishing, Data and/or Analytics nodes are installed.

High Availability

EOS supports HA Active-Active setups. Replication is possible between multiple front-ends and 2 back-ends. The setup requires a hardware load balancer in front of replicated components. Consider the following architecture:



We will assume that all components have been installed to use the same database and database user.

The file storages of the two back-ends should be distinct.

We recommend turning on logging by adding **LogLevel=Normal** to the main config file on all machines and restarting the EOS services and websites.

Configuring Frontends for HA

The steps to configure the frontend servers:

- Install EOSFrontend1 with default settings. Install only Admin Web Site, Portal Web Site and Enterprise Website components.
- Install Admin, Portal, Enterprise Web Site licenses on EOSFrontEnd1.
- Install EOSFrontend2 with default settings. Install only Admin Web Site, Portal Web Site and Enterprise Website components.
- Install Admin, Portal, Enterprise web site licenses on EOSFrontEnd2.
- In the main configuration file, for both frontend machines, add or change the following values:

```
XFServerAddress=<Backend HLB IP>
DASAddress=<Backend HLB IP>
BIAddress=<Backend HLB IP>
ESSAddress=<Backend HLB IP>
RepositoryAddress=<Backend HLB IP>
LogAddress=<Backend HLB IP>
```

```
WorkAddress=<Backend HLB IP>
BackgroundServerAddress=<Backend HLB IP>
WebSiteHostUrl=http://<Frontend HLB IP>:<Frontend HLB Port>
```

- Restart the websites on EOSFrontEnd1
- Restart the websites on EOSFrontEnd2

Configuring Backends for HA

Follow the instructions below to configure the backend servers for HA:

- Install EOSBackend1 with default settings. Install everything except the websites.
- Install backend licenses (PE, AE, DE, Repository, Backend) on EOSBackend1.
- Stop the Ecrion Omni System Service on EOSBackend1.
- Install EOSBackend2 with default settings. Install everything except the websites.
- Install backend licenses (PE, AE, DE, Repository, Backend) on EOSBackend2.
- Stop the Ecrion Omni System Service on EOSBackend2.
- Update the main config file for each of the both backends with the following values:

```
XFServerAddress=<Backend HLB IP>
DASAddress=<Backend HLB IP>
BIAddress=<Backend HLB IP>
StorageServerEnabled=true
ESSAddress=<Backend HLB IP>
LogAddress=<Backend HLB IP>
RepositoryAddress=<Backend HLB IP>
WebSiteHostUrl=http://<Frontend HLB IP>:<Frontend HLB Port>
ESSPeerAddress=<Peer/Other Backend IP>
ESSPeerPort=40014
StorageEncrypted=true
StorageClustered=true
LogClustered=true
LogPeerAddress=<Peer/Other Backend IP>
LogPeerPort=40018
ClusteredPeerConnectionTimeout=1000
ClusterNodeName=<CustomUniqueNodeName>
BackgroundServiceClustered=true
BackgroundPeerPort=40026
BackgroundPeerAddress=<Peer/Other Backend IP>
```

- **All except one** of the service nodes must contain the below lines, because triggers, schedules and search do not currently support replication:

```
TriggerServerEnabled=false
SchedulerServerEnabled=false
SearchEnabled=false
```

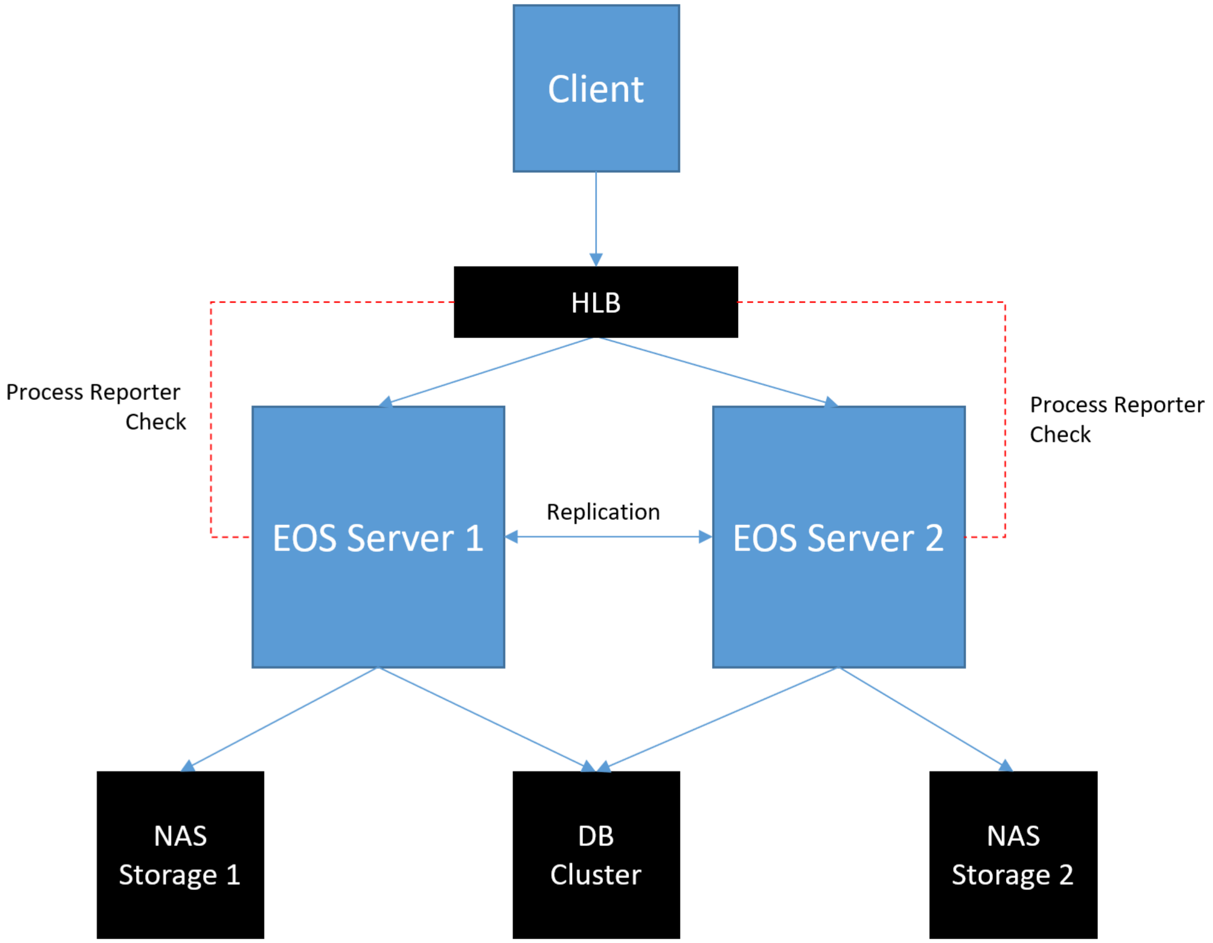
- Start the Ecrion Omni System Service on both machines.
- If logging is enabled and set to at least **Normal** (see **Enabling Logging**), then check **EOS4Svc.log** for confirmation that all storage files are in sync. A message like the following should appear for each file in the Storage Folder:

```
[Storage] Synchronization for file #.dat finished, took #.# seconds
```

Simple HA Scenario Example: Two Servers, Active/Active

This section describes how to set up active/active high availability using two servers, each with a full instance of EOS deployed.

Setup



The diagram above shows the main components of this setup:

- Basic HLB configuration
- Automatic failover/failback with no user interaction
- Both servers are used evenly
- Process reporter can be used if supported & configured in HLB

Deployment Steps

To install and configure the above setup, the following steps must be performed:

1) Install all EOS components on the first machine.

2) Install licenses for the first EOS instance.

3) Stop the Ecrion Omni System service on the first EOS instance.

4) Install all EOS services on the second machine.

5) Install licenses for the second EOS instance.

6) Stop the Ecrion Omni System service on the second EOS instance.

7) Set the following values in the main config file on both instances:

```
ClusteredPeerConnectionTimeout=1000
ClusterNodeName=<CustomUniqueNodeName>
```

8) Configure storage clustering by setting the following values in the main config files on both instances:

```
ESSPeerAddress=<Peer/Other EOS IP>
ESSPeerPort=40014
StorageEncrypted=true
StorageClustered=true
```

9) Configure log service clustering on both instances:

```
LogClustered=true
LogPeerAddress=<Peer/Other EOS IP>
LogPeerPort=40018
```

10) Configure background service clustering on both instances:

```
BackgroundServiceClustered=true
BackgroundPeerPort=40026
BackgroundPeerAddress=<Peer/Other Backend IP>
```

11) Disable trigger, scheduler and search services **on one of the EOS instances** (currently these services can run on only one of the instances, even in HA scenarios) by adding the following lines to the second instance main config file:

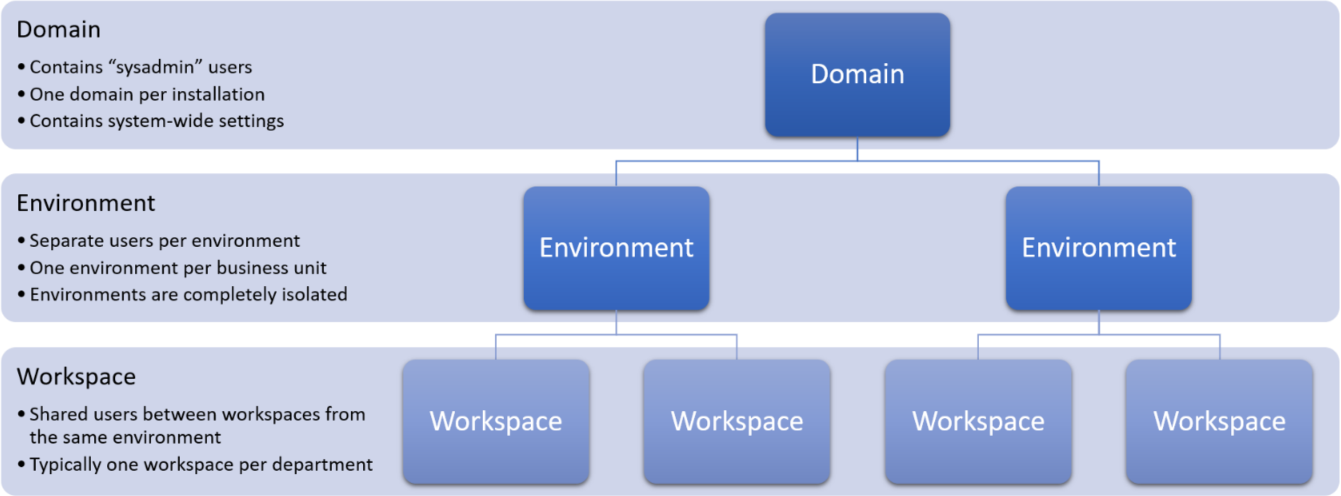
```
TriggerServerEnabled=false
SchedulerServerEnabled=false
SearchEnabled=false
```

12) Start first EOS instance and wait for sync to finish.

13) Start second EOS instance and wait for sync to finish.

System Configuration

System Hierarchy



Domain

- Contains “sysadmin” users
- One domain per installation
- Contains system-wide settings

Environment

- Separate users per environment
- One environment per business unit
- Environments are completely isolated

Workspace

- Shared users between workspaces from the same environment
- Typically one workspace per department

An EOS system is comprised of 3 entities: **domain**, **environment**, **workspace**. The hierarchy is defined as follows:

- The domain contains one or more environments.
- Each environment contains one or more workspaces.

Domain

The domain refers to the entire EOS setup – it is the top-level node. An installation of EOS, whether its across one or multiple machines, will contain a single domain. There is no way to add multiple domains other than having separate EOS installations with no connection to each other.

The domain contains its own system-wide users called **sysadmins**. These users have full access to the **System Administration** website, giving them the following permissions:

- Create, edit or delete environments
- Create, edit or delete users with full access within any environment (also called **environment admins**)
- Change domain-level settings

Sysadmins cannot directly log into any environment; however they can easily gain access to it by creating a new environment admin for that environment. This is because there is no overlap between sysadmin users (stored at the domain level) and regular users (stored at the environment level).

New sysadmin credentials can be added from the **Sysadmins** section of the **System Administration** website.

Environments

The domain contains multiple environments, each with its own distinct set of users and features. This is where enterprise users log into and perform all of their work.

By default, EOS does not require users to specify which environment they want to log into, asking only for a username and password. It does this by enforcing **unique usernames and emails across the system** – this allows EOS to infer the environment name from the user that's currently logging in, as well as be able to reset their password via email should they forget it. This setting can be changed to be more permissive, but will either require a separate box for the environment name or each environment to be mapped to a different URL (see **Environment Selection on Enterprise Login** section).

The main consideration when lifting the uniqueness restriction is that, internally, users are still stored separately within each environment, i.e. user **joe** from environment **test** and user **joe** from environment **prod** are two distinct users which are managed separately, each in their own environment. This has some implications, the most important of which is that **users with the same name using built-in EOS authentication may have different passwords across environments**.

In order to avoid confusion:

- If you intend to share environments between users, we highly recommend using an external system to store user credentials, like **Active Directory**.
- If you want to have separate users per environment, built-in **EOS authentication** is usually more suitable (e.g. using the email as the username).

The purpose of environments is to have completely separate EOS instances within the same installation, which may be useful in some scenarios. Here are some examples when you might consider multiple environments:

- **DTAP (or similar) setups** – a different environment for each stage of the development process (Development, Testing, Acceptance, Production)
    - These environments are more or less clones of each other, with projects being worked on in Development, then being published through Testing, Acceptance and eventually Production.
    - In this type of scenario, a user will likely have access to multiple environments.
    - For performance and stability reasons, it's **highly recommended** that the Production environment is part of a different EOS domain/installation altogether.
- **Multi-tenant setups** – a different environment for each customer (or "tenant")
    - This type of setup is intended to separate your customers into their own environments because it doesn't make sense for any overlap to exist.
    - A good practice is to give each user an account with their corporate email as the username; this way, customers will be naturally separated: ***@company1.com** to the **Company1** environment, ***@company2.com** to the **Company2** environment, etc.
    - Built-in EOS authentication is recommended for this type of setup.
- **Single purpose environments** – a "one-off" environment to try a specific feature, perform a demo or a training session.
    - Creating a new environment for trying out a new feature allows you to properly isolate your work from other operations being performed on the server.

Lastly, each environment has its own **Customer Portal** instance, with its own set of customers, accounts and metadata schema.

Workspaces

Workspaces are subdivisions of an environment, containing files, jobs and settings. They are only visible in the **Enterprise Home** website, to enterprise users logged into an environment.

The purpose of workspaces is to allow you to better organize your assets into meaningful categories, e.g. per department. You can also assign different permissions to workspaces so that certain users or groups will only see the workspaces you allow them to see.

Workspaces mostly **act as top-level folders**, however there are subtle differences. To determine a file, a workspace and a path within that workspace must be provided – the workspace name is not a part of the path, but a different parameter altogether. This pattern rings true for other assets: jobs require a job ID and workspace name, tasks require a task ID and workspace name, etc.

Communications are a special case: while defined at the environment level, each communication references a workflow file internally, which belongs to a specific workspace. Furthermore, a communication will only depend on its workflow's (static) dependencies, which must also belong to that same workspace, thus indirectly associating the communication with a single workspace. This means workspace permissions will affect which communications a user can effectively run, which is why the following security rule is enforced: if a user does not have access to a workspace, then communications referencing that workspace cannot be seen by that user.

In-place review and approval for assets is also enforced at the workspace level, meaning that all the assets in that workspace will be subject to the configured review and approval workflow – except for the workflow file itself, which by design must also belong to that workspace.

Lastly, workspaces may only be **created by environment admins** and will, by default, only be visible to other admins. Permissions may be set so that other users/groups can see or even manage that workspace. When a user has **Manage** rights to a workspace, they will have full control over that workspace, regardless of any permissions enforced on individual assets.

Domain Configuration

The **System Administration** website allows you to configure domain level settings via the **Domain Settings** dialog, accessible via the top-right cogwheel menu.

Environment Selection on Enterprise Login

This setting lets you control how EOS picks which environment to log an enterprise user into. The possible values are:

- **Autodetect environment** – This requires unique usernames across all environments, i.e. each user will only have access to exactly one environment. This is the default. If you have changed this value and have granted access to multiple environments to certain users, then you should not revert the setting to this value, because users will again be limited to just one environment.
- **Use subdomains** – This setting allows you to map subdomains to environments, thus using the URL to identify which environment the user wants to log into.

- **Allow user to select environment** – This setting will allow the user to simply type in the environment name manually at login. The drawback is that all users will need to fill in 3 fields (username, password, environment) instead of 2 (username, password).

Tip: When granting a user access to multiple environments (options #2 and #3), it's recommended to use an AD user instead of an EOS user, because EOS users are essentially duplicated when given access to a new environment, which makes user data (like passwords) more difficult to maintain.

Enterprise Login with Active Directory

This setting allows you to toggle Active Directory logins to the system. Users will still need to be added to each environment manually or via synchronization with AD. Both EOS and AD users can coexist in the system.

AD users are added using the **Domain\User** syntax.

Synchronize Active Directory Users with Enterprise Users

This setting allows you to map AD groups to EOS groups. Once an AD group has been mapped to an environment in the system, users from that AD group will automatically be added to the EOS group and inherit the group's permissions.

You can map multiple groups across multiple environments. When a user first logs into an environment, they will be made a member of all the corresponding groups in that environment.

This setting does not work with the **Autodetect environment** value.

Managing Environments and Environment Administrators

Environments can be added, edited or deleted from the **Environments** section of the **System Administration** website. This operation requires a sysadmin account.

For each environment, you can configure the following:

- Environment features – you may disable features like communications, channels or analytics so that your users only have access to the features they need within the environment
- Environment admins – add, edit or delete users with full access to the environment
- Resource allocation for EOS services – configure the maximum number of threads and additional worker nodes for the Publishing, Data & Analytics services
- Single Sign-On – optionally enable single sign-on for the environment, at the **Enterprise Home** and/or **Customer Portal** level
- Search – enable/disable, what to crawl, etc.

Single Sign-On Support

Single sign-on (SSO) is a user authentication process that allows a user to enter one set of credentials to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a session.

An EOS environment can be configured to use Single Sign-On with **SAML** or **WSFed**.

Please reach out to support@ecrion.com for instructions on how to setup SSO for your configuration.

Search Configuration

In the System Administration, for each environment, you may enable or disable search from the **Search** tab. In a new environment, search will be off and the **Search** tab will be empty. Click the **Configure** button to begin configuring search.

First, select the backend:

- **Database** – use the database configured during installation for search
- **Elastic Search** – use an Elastic Search instance.

Next, configure additional crawling options:

- **Crawl Job Output** – will crawl the generated files, i.e. the files under **Jobs**; this could significantly increase crawl time if you generate many documents;
- **Crawl Document Content** – will also use full text search, so as to crawl the contents of documents; having a large corpus of documents will significantly increase crawl time.

Note: Long crawl times don't affect the system's performance. Instead, what this means is that new and modified items will take longer to appear in the search results due to the fact that the service takes a longer time to index them.

Last, check the connection using the **Test Connection** button.

After configuring search, a full crawl must be run. Click on the **Full Crawler** dropdown next to the **Configure** button and select **Start**. Information about the current configuration, crawler status and indexed items will appear on the page. When the dropdown says **Full Crawler (finished)**, your search is configured. Users logging into the environment (on the **Enterprise Home** website) will now see the search bar at the top right of each page, on the navigation bar.

Environment Configuration

Most of the configuration for an environment will be performed by an **environment admin**. Environment admins are enterprise users, so this configuration will be done through the **Enterprise Home** website as opposed to **System Administration**.

Environment admins have unlimited permissions in their own environment. By design, **it's impossible to enforce restrictions on an environment admin** within the environment they are managing. Typically, environment admins are created by being added to the **Administrators** group of that environment, but it's possible to provide this level of access to user-created groups as well.

Environment admins are the only users who have access to the **Settings** page, which can be accessed via the cogwheel icon on the navigation bar (top-right of any Enterprise page). This page controls the settings for the current environment, notably:

- Users, groups, profiles and permissions
    - Only admins can manage users, groups and define permissions for them – they can also create new environment admins.

    - They are also able to set a profile for each user/group to control their welcome page experience.
- Connections
    - Only admins can see and configure connection strings and other sensitive information related to the data sources relevant to the environment.
    - They are also the only ones who can manage email connections or connections to third party services (Amazon, DocuSign, CRMs, etc.)
- Views
    - Admins may create and configure views which shall be seen by all users.
- Task Types
    - Admins can create different tasks and configure their states, outcomes and transitions.
- Time zone
    - Admins can enforce the time zone for all users.

Environment admins can also manage access and publish assets to the **Customer Portal** website, change the accounts and customers schema, design new communications and share them (with enterprise users or customers).

Environment configuration is detailed online in the **EOS User Guide**, available at: http://help.ecrion.com/EOSUserGuide/

Main Configuration File

The main config file (**EOS4.config**) contains system settings which enable additional functionality, including distributed configurations and high availability. Any changes to the main config require a restart of the EOS service and websites (e.g. via **iisreset**).

Main Website URLs

The **External URLs** for each website are specified via the main **config file**. These should be set to the URLs that are used when accessing the system from the intranet, on each corresponding website and on the machine(s) hosting the EOS Service component:

```
WebSiteHostUrl=http://<Enterprise Website IP>:<Enterprise Website Port>
PortalURL=http://<Portal Website IP>:<Portal Website Port>
SysadminURL=http://<Sysadmin Website IP>:<Sysadmin Website Port>
```

Service IPs for Distributed/HA Scenarios

Important Note: All of the IP values mentioned throughout should be taken to mean “the IP through which this service can be accessed”. Usually, this is the intranet IP of the machine hosting the component. If a component is load balanced, then it’s the IP of the load balancer. Essentially, if someone were to specify all IPs explicitly on each machine, the list of IPs should be the same across all the machines.

EOS Service IPs

The EOS service executable (EOS4Svc.exe) hosts multiple sub-services which can be hosted at different addresses. If the service and the websites are hosted on different machines, the main config file of the website machines must contain the following information:

```
ESSAddress=<EOS Service IP>
```

```
RepositoryAddress=<EOS Service IP>
LogAddress=<EOS Service IP>
WorkAddress=<EOS Service IP>
BackgroundServerAddress=<EOS Service IP>
TriggerAddress=<EOS Service IP>
SchedulerAddress=<EOS Service IP>
DistributionAddress=<EOS Service IP>
AlertsAddress=<EOS Service IP>
CrawlerServerAddress=<EOS Service IP>
```

Splitting EOS Services

Services running under EOS4Svc.exe can be further divided into two components which can be selected during installation time:

- Document Repository, which contains the Storage Service, Log Service and Repository Service;
- Backend Services which contains Worker Service (for running jobs), Background Service (for health-check, search, analytics, etc.), Trigger, Scheduler, Distribution, Alerts and Crawler.

```
ESSAddress=<Document Repository IP>
RepositoryAddress=<Document Repository IP>
LogAddress=<Document Repository IP>
WorkAddress=<Backend Services IP>
BackgroundServerAddress=<Backend Services IP>
TriggerAddress=<Backend Services IP>
SchedulerAddress=<Backend Services IP>
DistributionAddress=<Backend Services IP>
AlertsAddress=<Backend Services IP>
CrawlerServerAddress=<Backend Services IP>
```

Publishing Service IP

If the Publishing Service is hosted on a different machine, the IP must be specified in the main config files of the EOS Service and all EOS websites:

```
XFServerAddress=<Publishing Service IP>
```

Data Service IP

If the Data Service is hosted on a different machine, the IP must be specified in the main config files of the EOS Service and all EOS websites:

```
DASAddress=<Data Service IP>
```

Analytics Service IP

If the Analytics Service is hosted on a different machine, the IP must be specified in the main config files of the EOS Service and all EOS websites:

```
BIAddress=<Analytics Service IP>
```

Peer EOS Service IPs

In an HA scenario (see **High Availability** section), each EOS Service must know of its peer (replicated) component:

```
ESSPeerAddress=<Peer/Other Service IP>
LogPeerAddress=<Peer/Other Service IP>
BackgroundPeerAddress=<Peer/Other Service IP>
```

Captcha Settings

For servers not connected to the internet, you will want to disable captcha, which uses Google's ReCaptcha over the internet.

The following flags control captcha settings:

```
CaptchaEnabled=<true | false>
LoginNumberOfRetries=<number>
RecaptchaSiteKey=<string>
RecaptchaSecretKey=<string>
```

Other Settings

This section describes various other system settings.

Enabling HTTPS

Enabling HTTPS can be done in two ways:

- Automatically, by re-running the installer,
- Manually, by changing bindings in IIS and updating the main config file.

Note that both these methods require that a valid and appropriate SSL certificate is installed on the server hosting the website(s) that you wish to enable HTTPS for.

Important Note: In a multi-server setup, regardless which of the methods described below (automatic or manual) is used, the steps must be performed **on all servers in the multi-server setup**. This includes HA scenarios.

Enabling HTTPS Automatically

To enable HTTPS automatically, simply re-run the installer and choose "Enable Web Site SSL" for each of the websites that you wish to make accessible through HTTPS. When ticking the box, make sure to select the correct certificate from the list that appears.

Enabling HTTPS Manually

First, the appropriate bindings in IIS must be added:

- Open **IIS Manager**.
- Navigate to the website that you wish to enable HTTPS for.
- On the right-side panel, click **Bindings**.
- Add a new binding or edit the existing binding and change **http** to **https**.
- Click **OK**.

Afterward, the corresponding host URL in the main config file must be updated:

- For the Enterprise Home website, set the following value:
  ```
  WebSiteHostUrl=https://<hostname>:<port>
  ```
- For the System Administration website, set the following value:
  ```
  SysadminURL=https://<hostname>:<port>
  ```

- For the Customer Portal website, set the following value:
  `PortalURL=https://<hostname>:<port>`

Note: Usually, this only means changing "http" to "https" in the config file, with the hostname and port (if present) left the same.

After making the changes, perform the following actions so that the new configuration values are loaded:

- Restart the Ecrion Omni System service.
- Restart the IIS service either from **IIS Manager** or by opening an administrator command prompt and running the **iisreset** command.

Note: This procedure can also be applied in reverse, to change from HTTPS to HTTP.

Maintenance

Run Health Check

If you suspect there may be something wrong with your system (data corruption, service crashes, etc.), the first recommended step is running a health check **for each environment**.

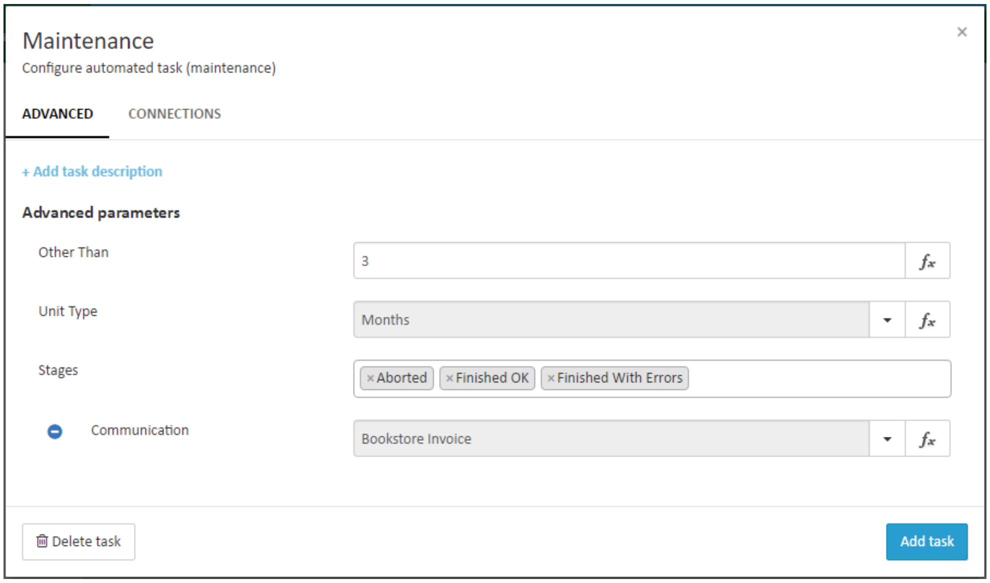
This can be done from **System Administration**, in the **Edit Environment** dialog, by clicking the **Run Health Check** button on the first tab.

Delete Old Jobs

To create policies on deleting older jobs, you will need to create a maintenance workflow and run it either manually or using EOS Scheduler.

Create a new workflow and add a **Maintenance** task. You can configure this task to delete jobs older than a certain amount of time, allowing to filter by job status (stage) and, optionally, by communication.

For example, the task below will delete all jobs older than 3 months, which have either finished ok, finished with errors or have been terminated forcefully, and belonging to the communication "Bookstore Invoice":



Maintenance

Configure automated task (maintenance)

Advanced parameters

Other Than: 3

Unit Type: Months

Stages: × Aborted × Finished OK × Finished With Errors

Communication: Bookstore Invoice

If the “Communication” parameter is not set, then the task will consider all jobs in the current workspace.

If the “Communication” parameter is set, then the task will consider all jobs belonging to that communication, regardless of workspace.

Storage Integrity Check & Compacting

Storage Utility

The Storage Checker tool, can be found in: **<Installation Folder>\Windows Service\EOS Utility\StorageChecker\StorageUtility.exe.**

The usage is as follows:

```
StorageUtility.exe
        [-command checkStorage|compactStorage]
        [-u <sysadmin username>]
        [-p <sysadmin password>]
        [-logLevel None|Normal|Debug]
        [-outputFilePath <Path>]
```

The tool has two functionalities: check and compact.

Check Storage

Check Storage command verifies if there are any invalid <<version of>> documents present in the storage.

Usage example for checking storage:

```
-command checkStorage -u sysadmin -p sysadmin -logLevel Normal -outputFilePath D:\output\Checkstorage.txt
```

Compact Storage

Compact Storage command verifies the storage for files marked as deleted by **EOS** (either from UI or API) and will release the disk space that was previously allocated to those files. The tool also defragments the storage.

Note: This operation is performed **automatically** at the end of each day. However, if you would like to perform this operation **manually**, please see below:

Usage example for compacting storage:

```
-command compactStorage -u sysadmin -p sysadmin -logLevel Normal -outputFilePath D:\output\Compactstorage.txt
```

Backup & Cloning

Backing Up an EOS Server

Backup Frequency

We strongly recommend backing up your EOS system as often as possible. Daily backups with a retention policy should be implemented, if possible.

Before Backing Up

Backing up your EOS system is safe to do at any time without impacting users. However, as a best practice, we recommend disabling user access to the system by stopping all **EOS websites** for the duration of the backup. We recommend this practice for two reasons:

- It's preferable for administrators that large jobs are not running during the backup operation;
- Users should be made aware if and when administrative tasks are being performed on the server.

Since the procedure will put extra load on the DB and EOS services, it's recommended scheduling backups at a time when system load is lower than average, for example at night, so as to minimize the impact on overall performance.

Automatic Backup

Note: This tool requires .NET Framework 4.5 and SQL Server Command Line Utilities.

Note: For remote backup, you will need an existing main config file with the correct addresses specified for all the services, the database and the storage folder.

The recommended way of backing up EOS is with the storage backup tool, located under: **<Installation Folder>\Windows Service\EOS Utility\EOSBackup\Tools.EOSBackup.exe**. The tool will backup and restore EOS Database, EOS Storage, EOS Windows Service logs. It can backup and restore files in/from a shared network folder or an Amazon S3 folder.

The shared network folder should be specified as a UNC path. The SQL Server should also have read/write access to the folder.

The tool writes logs to the master log, specified in the main config file. It can also be used to restore backups (see **Automatic Restore** section).

Important Note: If EOS was configured with Windows Authentication to connect to the database, then the backup tool will attempt logging in to the database as the current user. Please make sure that you run the Command Prompt as the correct domain user.

The usage is as follows:

```
Tools.EOSBackup.exe
        [-backup|-restore|-examples]
        [-backUpFolder <localFolderPath>]
        [-AWSAccessKeyId <AWSAccessKeyId>]
        [-AWSSecretAccessKey <AWSSecretAccessKey>]
        [-AWSRegion <AWSRegion>]
        [-AWSRegion <AWSRegion>]
        [-S3Bucket <S3Bucket>]
        [-S3Folder <S3Folder>]
        [-configFile <configFileToUse>]
```

Usage example that backs up to a local folder:

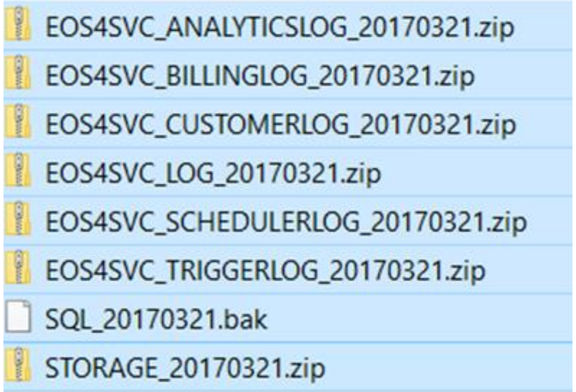
```
Tools.EOSBackup.exe -backup -backUpFolder "D:\BackUp Folder"
```

Usage example that backs up to an Amazon S3 folder:

```
Tools.EOSBackup.exe -backup -backUpFolder "D:\BackUp Folder" -AWSAccessKeyId "******" -AWSSecretAccessKey "******"
-AWSRegion "USEast1" -S3Bucket "eos4backup" -S3Folder "Backup"
```

Note: The **EOS4.config** file can also be referenced by the backup tool to perform remote backup or restore using the **-configFile** flag.

After running the backup tool, you should see 8 files in the backup folder:



EOS4SVC_ANALYTICSLOG_20170321.zip
EOS4SVC_BILLINGLOG_20170321.zip
EOS4SVC_CUSTOMERLOG_20170321.zip
EOS4SVC_LOG_20170321.zip
EOS4SVC_SCHEDULERLOG_20170321.zip
EOS4SVC_TRIGGERLOG_20170321.zip
SQL_20170321.bak
STORAGE_20170321.zip

Manual Backup

Important Note: Before attempting a manual backup, you will need to stop all EOS services and websites.

To perform a manual backup, follow the steps below instead of running the backup tool:

- Back up the **Storage Folder**, located by default at **<Application Data Folder>\EOSStorage4**

- Back up the **EOS Database**
- Back up the EOS logs:
  - EOS logs, located by default at: **<Application Data Folder>\EOS4Log**
  - Analytics logs, located by default at: **<Application Data Folder>\EOS4AnalyticsLog**
  - Billing logs, located by default at: **<Application Data Folder>\EOS4BillingLog**
  - Customer logs, located by default at: **<Application Data Folder>\EOS4CustomerLog**
  - Discussions logs, located by default at: **<Application Data Folder>\EOS4DiscussionsLog**
  - Scheduler logs, located by default at: **<Application Data Folder>\EOS4SchedulerLog**
  - Trigger logs, located by default at: **<Application Data Folder>\EOS4TriggerLog**

This will essentially yield the same result, but we recommend using the tool as it offers more predictability and flexibility.

Note: The default locations for all of the above folders may be changed using the config file. Please double check if the values have been overridden to custom locations.

Important Note: Please use the appropriate guidelines for backing up a database on your version of SQL Server.

Note: We **strongly** recommend saving a copy of your main config files (**EOS4.config**, **PublisherSvc.config**, **DASSvc.config**, **BISvc.config**) along with the backup for future reference.

Decommissioning an EOS Server

If you're backing up a server with the goal of decommissioning it, then you must uninstall the licenses on that server before proceeding (see **Uninstalling Licenses** section). This operation should be performed as a last step, after backing up.

Restoring a Backup

Before Restoring

Restoring requires that all user access is disabled, meaning all the **EOS websites** must be stopped.

Automatic Restore

Note: This tool requires .NET Framework 4.5 and SQL Server Command Line Utilities.

Note: For remote restore, you will need an existing main config file with the correct addresses specified for all the services, the database and the storage folder.

Before proceeding, it's important to know that the automatic restore operation requires the **EOS services** to be up and running on the backend. In case the services are not running properly and/or cannot be started, you must perform a manual restore instead.

Use the backup tool (see **Automatic Backup** section) to restore a previously created backup. The tool will automatically wait for any operations on the database and storage to finish before beginning, then prevent any other reads or writes until it is finished.

Usage example that restores from a local folder:

```
Tools.EOSBackup.exe -restore -backUpFolder "D:\BackUpFolder"
```

Usage example that restores from Amazon S3:

```
Tools.EOSBackup.exe -restore -AWSAccessKeyId "******" -AWSSecretAccessKey "******" -AWSRegion "USEast1" -S3Bucket
"eos4backup" -S3Folder "Backup\20160810"
```

Manual Restore

Important Note: Before attempting a manual restore, you will need to stop all **EOS services and websites**.

Follow the steps below:

- Restore the **Storage Folder** from a previously created backup.
- Restore the **EOS Database** from a previously created backup.
- Restore the **EOS Logs** from a previously created backup to their respective folders.

Note: The correct folders can be found in the main config file. If a folder name is not present in the config file, then it will use the default value, specified in the **Manual Backup** section.

Important Note: Please use the appropriate guidelines for restoring a database backup on your version of SQL Server.

Automatic Backup & Restore from a Remote Machine

Backup and restore operations using the backup tool can also be performed from a remote machine.

First, you will need to copy the backup tool itself from one of the EOS servers. This is located at **<Installation Folder>\Bin\Windows Service\EOS Utility\EOSBackup**. The contents of the entire folder must be copied to the remote machine.

The backup tool will require reading its settings from a main config file in order to run. This should be a copy of the main config file from a machine running one of the **EOS websites**.

You must point the tool to the config file via the **-configFile** flag – the file provided will tell the tool which database and storage folder it should back up.

Important Note: If EOS was configured with Windows Authentication to connect to the database, then the backup tool will attempt logging in to the database as the current user. Please make sure that you run the Command Prompt as the correct domain user.

Important Note: When doing backup or restore from a remote machine, that machine needs to have access to:

- The **EOS Database**;
- The **EOS Backend Services** listed in the config file copy;
- The backup folder.

Essentially, the remote machine must be located in the same intranet as the EOS setup.

The backup folder must be a shared network folder and should be specified as a UNC path. The SQL Server should also have read/write access to the folder.

Automatic Backup from a Remote Machine

Note: All considerations in the **Automatic Backup** section apply here as well.

Usage example, assuming the config file is copied to the same folder as the backup tool:

```
Tools.EOSBackup.exe -backup -backUpFolder "\\Remote Storage\EOS Backup Folder" -configFile EOS4Production.config
```

Automatic Restore from a Remote Machine

Note: All considerations in the **Automatic Restore** section apply here as well.

Usage example, assuming the config file is copied to the same folder as the backup tool:

```
Tools.EOSBackup.exe -restore -backUpFolder "\\Remote Storage\EOS Backup Folder" -configFile EOS4Production.config
```

Cloning an EOS Server

To clone an EOS server from a source to a target machine, you will need to do the following:

- Back up the source machine (see **Backing Up an EOS Server** section).
- On the target machine, run the installer for the same EOS version as the source machine. Make sure the settings specified during installation, e.g. the IP addresses, the database connection, etc., are correct.
- Restore the backup on the target machine (see **Restoring a Backup** section for details).

Note: Some configuration on the target machine may need to be done by manually adding settings to the main config file(s), e.g. enabling cross-environment logins. We recommend reviewing the main config file(s) from the source machine.

Note: License info will not be preserved. New licenses will need to be installed and activated on the target machine.

Rolling Back an Installation

To roll EOS back to a previous version:

- Uninstall the newer version.
- Run the installer for the older version, using previous configuration.
- Restore a compatible backup on the EOS server (see **Restoring a Backup** section for details).

Note: The backup must belong to the specific older EOS version that is being rolled back to. Ignoring this may lead to data loss. Please contact support@ecrion.com if your rollback scenario cannot accommodate these requirements.

Upgrading EOS

To upgrade the system, simply run the installer of the newer EOS version. You may need to uninstall the existing version from **Control Panel** first.

It’s important to make sure that there is no activity on the system while running the upgrade to preserve system integrity. We recommend to ensure that:

- No users are performing any operations or generating documents. One way to do this is to stop the IIS websites.
- Make sure there are no active jobs. One way to do this is to stop the “Ecrion Omni System” service.
- Make sure no operations are performed on the EOS database (by default named “EOSDB4”). The installer process may alter the database to accommodate for new features or enhancements.

Note on using previous configurations: To preserve repository integrity, we highly recommend using the same storage location that was previously used with the selected database.

Note on High Availability: In HA scenarios:

- For minor patches, it’s sufficient to remove the current server where you are performing the upgrade from the HA setup, using the procedure above.
- For major upgrades, the entire HA setup needs to be taken offline for the duration of the upgrade, otherwise there is a risk of corrupting the integrity to the database and/or storage.

Troubleshooting

This section lists troubleshooting tips for common encountered problems.

400 Bad Request

Symptoms

When accessing an EOS website, you receive a **400 Bad Request** error. This can manifest in a number of ways, depending on how EOS was installed:

- The website can only be accessed from the server itself using the **localhost** URL, but cannot be accessed from the outside using the **hostname** URL.
- The website can be accessed from the outside using the **hostname** URL, but not from the server using the **localhost** URL. The website can, however, be accessed from the server using the **hostname** URL.

Solution

This is because of the default bindings in IIS. These will match the hostname URL(s) configured during installation. By default, these are **localhost**, but they should actually be set to use the hostname of the server as seen from the outside. This is important because the hostname URL will be used in emails sent to users and customers. We also recommend accessing EOS using the **hostname** URL, even if that access is being performed from the server itself.

To change the hostname for either of the websites, just re-run the installer and set the correct hostname for each of the websites: **Enterprise Home**, **System Administration**, **Customer Portal**.

You can also set up access to each website from any machine, regardless of the hostname, by setting the appropriate bindings in IIS. However, the recommendation is that the IIS bindings always match the hostname set during installation, for consistency.

Follow these steps for each of the EOS websites that you want to be accessible remotely:

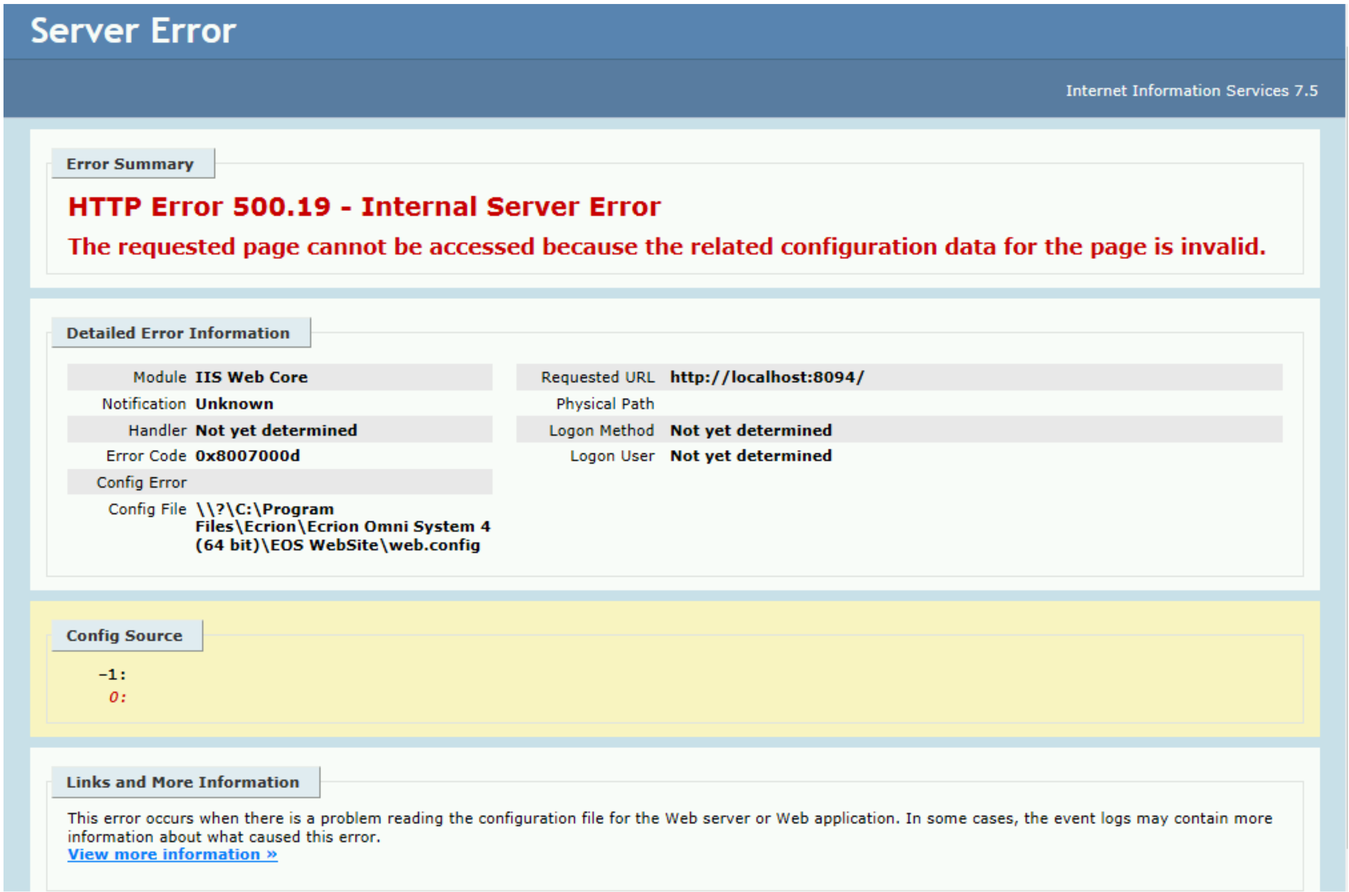
- Open **IIS Manager**.
- Navigate to the website exhibiting the problem.
- On the right-side panel, click **Bindings**.
- Edit the existing binding and change **localhost** to *.
- Click **OK**.

Note: If you do this, the website will be accessible from the intranet if the firewall allows it. Make sure that this is the intended functionality and that website access (especially for System Administration) is properly secured before making the change.

500 Internal Server Error (500.19)

Symptoms

After installation, you receive a **500 Internal Server Error** when trying to access EOS pages from a remote computer. On the server, the detailed error is **500.19 - Internal Server Error. The requested page cannot be accessed because the related configuration data for the page is invalid**, like in the screenshot below:



Server Error

Internet Information Services 7.5

Error Summary

HTTP Error 500.19 - Internal Server Error

The requested page cannot be accessed because the related configuration data for the page is invalid.

Detailed Error Information

Module	IIS Web Core	Requested URL	http://localhost:8094/
Notification	Unknown	Physical Path	
Handler	Not yet determined	Logon Method	Not yet determined
Error Code	0x8007000d	Logon User	Not yet determined
Config Error			
Config File	\\?\C:\Program Files\Ecrion\Ecrion Omni System 4 (64 bit)\EOS WebSite\web.config		

Config Source

```
   -1:
    0:
```

Links and More Information

This error occurs when there is a problem reading the configuration file for the Web server or Web application. In some cases, the event logs may contain more information about what caused this error.

View more information »

Solution

Install the URL Rewrite module for IIS 7 or later: https://www.iis.net/downloads/microsoft/url-rewrite

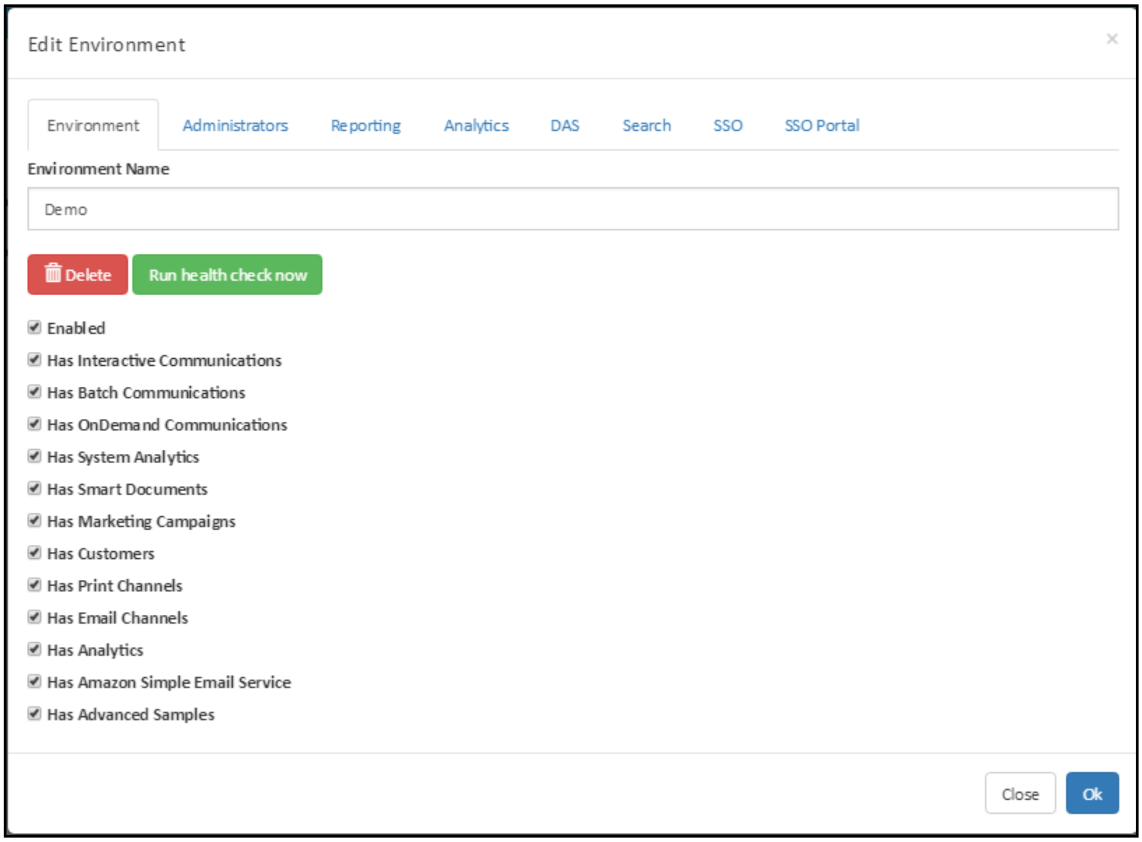
Missing Modules on Home Page

Symptoms

After creating a new environment, most of the modules on the home page are missing.

Solution

Enable this functionality in the System Administration website by clicking on the corresponding environment. New environments are automatically created with a minimal set of modules enabled. The sysadmin must then enable the functionality they need from the **Edit Environment** dialog:



Edit Environment

Environment Name

Demo

☑ Enabled
☑ Has Interactive Communications
☑ Has Batch Communications
☑ Has OnDemand Communications
☑ Has System Analytics
☑ Has Smart Documents
☑ Has Marketing Campaigns
☑ Has Customers
☑ Has Print Channels
☑ Has Email Channels
☑ Has Analytics
☑ Has Amazon Simple Email Service
☑ Has Advanced Samples

License Not Found

Symptoms

License Not Found error when accessing one of the EOS websites, or missing functionality.

Solution

Common license errors are:

- Missing suitable license for specific product or feature
- Suitable license found but doesn’t support the number of cores

Make sure you have the appropriate licenses installed and activated on the machine. **You need a total of 8 distinct licenses for a fully functional setup**, one for each of the components. Some components are optional, e.g. the Customer Portal website or the Analytics Engine.

If you are not sure whether you have the correct license(s) installed, please reach out to support@ecrion.com.

Enabling Logging

Logging can be enabled by setting the following value in the main configuration, then restarting the EOS service and websites (e.g. via **iisreset**):

```
LogLevel=Normal
```

For the Publishing, Data and Analytics services, the value must be added to their respective configuration files. The services must also be restarted after this operation.

Valid values for **LogLevel**, from most verbose to least verbose, are: **Debug**, **Normal**, **None**. The default is **None**. For production, the recommendation is **Normal**.