Email Experience Manager 3.4.2
Sitecore EXM Installation Guide

Installation guide for administrators and developers

sitecore®
Own the experience™

Prerequisites

Prerequisites for the Email Experience Manager 3.4 Update 2:

- Sitecore XP 8.2 Update 3 (rev. 170713) or Sitecore XP 8.2 Update 4 (rev. 170614).
- In the `/App_Config/ConnectionStrings.config` file:
  - Add two empty connection strings with the names *exm.master* and *exm.web*. For example:

```
<add name="exm.master" connectionString="" />
<add name="exm.web" connectionString="" />
```

  - Add the two connection strings `EXM.CryptographicKey` and `EXM.AuthenticationKey`. The keys must be represented in hexadecimal format by 64 characters, where you can use the symbols 0-9 and A-F. For example:

```
<add name="EXM.CryptographicKey" connectionString=
"E040C938FC9E4EBC3E93330B0F7837F284207B8180DB64CB5B6ABEB1AFBF6F5B" />
<add name="EXM.AuthenticationKey" connectionString=
"9D80B4E56AEE694058567BD89C936FB88F2DB1272A4E88F419B6501919E0BB25" />
```

Note
For security reasons, do not use the example key provided above.

- On all CM servers and dedicated dispatch servers, install Visual C++ Redistributable for Visual Studio 2012.

The installation process

To install Email Experience Manager 3.4 Update 2:

1. Download the Email Experience Manager package from the Sitecore Developer Portal.

   The EXM installation package that you download from dev.sitecore.net includes five zip packages – the *Email Experience Manager* and four zip files that match specific server roles.

   Note
   The *Email Experience Manager* is a Sitecore package. You can only use it for the primary content management server. Do not use the files intended for other servers on the content management server.

2. Use the Installation Wizard to install the EXM module. You can open the Installation Wizard from the:
   - Launchpad – click **Control Panel**, **Administration**, and **Install a Package**.
   - Desktop – click the **Sitecore Start** button, **Development Tools**, and then **Installation Wizard**.
3. Before you close the wizard, select **Restart the Sitecore client**.

To complete the installation process:

1. Move the following database files to the */Databases* folder.
   - `Sitecore.Exm.ldf`
   - `Sitecore.Exm.mdf`
   - `Sitecore.Exm_Web.ldf`
   - `Sitecore.Exm_Web.mdf`

   Note
   You can find the files in the *Data* folder or in the *Website\temp\ECM* folder.

2. Attach the `Sitecore_Exm` dispatch database and the `Sitecore.Exm_Web` database to the SQL server.
3. In the `App_Config/ConnectionStrings.config` file of your Sitecore solution, update the `exm.master` and the `exm.web` SQL server connection strings. For example:

```
<add name="exm.master" connectionString="user id=user;password=password;Data
Source=(server);Database=Sitecore_EXM" />
<add name="exm.web" connectionString="user id=user;password=password;Data
Source=(server);Database=Sitecore_EXM.WEB"/>
```

4. In the `/App_Config/Include/Sitecore.Analytics.Tracking.config` file, ensure the value of the *Analytics.ClusterName* setting is set to your instance host name.
5. Set up the message transfer agent that you want to use.
6. Use the Smart Publish option to publish your website.

Note
EXM does not support CMS live mode.

To configure EXM in a scaled environment, see this document.

To configure a dedicated server, see this document.

On the first launch of EXM:

1. Configure the EXM default settings to create a manager root.

   Note
   If you are using the Sitecore MTA provider, you must first add the relevant domain before you can configure the default settings.

2. If you are using the Sitecore MTA provider, in the App Center, configure the `Email Delivery` service.
3. In the App Center, sign up for the `Email Preview` and `Spam Detect` services. This is optional.

Increase security by encrypting connection string information

To increase the security of your EXM installation, Sitecore recommends that you encrypt the connection string information that is stored in the `ConnectionStrings.config` file.

To encrypt the connection string information:

1. In the `%systemroot%/Microsoft.NET/Framework/versionNumber` folder, locate the ASP.NET IIS registration tool – `aspnet_regiis.exe` –.
2. In the Windows command line, run the `aspnet_regiis.exe` utility with the `-pef` option. Pass the string `"connectionStrings"` to encrypt the `ConnectionStrings.config` file and the file location, for example:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet regiis -pef "connectionStrings"
"c:\inetpub\wwwroot\SitecoreCM\Website"
```

When the command is finished, in the `ConnectionStrings.config` file, the `connectionStrings` string contains encrypted information instead of plain text.

Note
To decrypt the encrypted file, use the `aspnet_regiis.exe` utility with the `-pdf` option and the same syntax: `C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis -pdf "connectionStrings" "c:\inetpub\wwwroot\SitecoreCM\Website"`