opentext ™

OpenText™ Web Site Management
Server

Installation Guide

This documentation describes how to install Management
Server. It also contains information about using Oracle
databases, about the Management Server cluster, and about
Management Server updates, service packs, and hotfixes. The
documentation also describes how to remove Management
Server.

OpenText™ Web Site Management Server
Installation Guide
WSMS160003-IGD-EN-1
Rev.: 2018-June-06

Table of Contents

Chapter 1

About OpenText Web Site Management Server

An Internet presence, or the use of an internal intranet, has become an integral part of daily life for almost all businesses. The Web server forms the information hub for both customers and staff. However, as the numbers of documents and HTML pages increase, so do the associated problems: the effort required for administering data and links increases exponentially with the expansion of the document base.

A content management system can help resolve these challenges.

OpenText Web Site Management Server is a Web-based content management and publishing system. It provides optimal coordination and cooperation of users actions. Management Server simplifies all workflows and provides an intuitive interface for Web site designers. It automates the publication of documents, ensuring that your online publications are always up-to-date.

Management Server offers the following additional benefits:

- Decentralized content administration
- Strict adherence to a predefined design
- Continual design and content control through page preview
- Automatic link consistency
- Quality control by means of release procedures
- Authorization maintenance
- Separation of content and layout
- Ongoing usability of content

Users create and administer content effortlessly with the intuitive technology that Management Server provides.

Management Server assists you in the administration of professional Web sites by integrating numerous functions that support the automated creation, control, and organization of content.

1.1   About this document

This documentation describes how to install Management Server. It also contains information about using Oracle databases, about the Management Server cluster, and about Management Server updates, service packs, and hotfixes. The documentation also describes how to remove Management Server.

Target readership

This documentation is aimed at administrators who have thorough experience with Windows operating systems as well as with connecting external databases and external directory services.

Chapter 2

Installing Management Server

2.1 System requirements

> 💡 **Tip:** For detailed system requirements refer to the Release Notes of your Management Server version.

2.1.1 Hardware

Hardware (recommended minimal configuration)

The hardware configuration for installing Management Server is recommended for project scenarios of average size and workload (stand-alone without other applications). Depending on project structure, size, and usage, the hardware requirements might differ at a wide range. For detailed advice, contact OpenText Support or Global Services. When using virtual environments, the recommended hardware configuration should be considered for each virtual instance.

The recommended minimal hardware configuration to install the Management Server has the following key data:

For servers:

- Intel QuadCore > 3 GHz (or comparable)
- 8 GB of RAM

For clients:

- Intel Core i3 (or comparable)
- 2 GB of RAM

Depending on the size of your projects and user numbers, you may need more RAM and processors. It may be even necessary to setup a cluster with more than one instance of the Management Server.

Hard disk recommendations

Based on the project size, the database server requires a corresponding amount of free disk space. We recommend that you have at least 100 GB of free disk space on all volumes. Note that hard disk access is very slow when using virtual drives. When you use virtual environments, map the physical drives to each virtual instance.

! Important

For production environments, OpenText recommends that you run
Management Server and database server on different physical systems.

2.1.2 Network and internet connections

The speed of the Web-based interface depends on your network or Internet
connection to Management Server.

Firewalls

In up-to-date Microsoft Windows Server versions, firewalls are active by default.
For communication with cluster servers and for internal and external
communication, Management Server uses the ports:

- 10066 – ServerService
- 10077 – ClientService
- 10082 – ObjectProcessService
- 10084 – ServerService
- 2880 – Spell check (Spellchecker.net)
- 139 – MS SQL FILESTREAM
- 445 – MS SQL FILESTREAM

If you have active firewalls, make sure that these permit Management Server to
communicate through the required ports.

Tip: You can restrict the communication within the firewall to the other cluster
nodes. It is sufficient to keep the ports open only for enabling the
communication within the cluster.

Proxies

It is not recommended accessing Management Server through a proxy. Management
Server functionality may suffer depending on type and configuration of the proxy.

It is supported to run Management Server behind a load balancer. The load balancer
must support sticky sessions. It is required that the same session will always be
routed to the same server, because there is no sharing of sessions between
Management Server instances.

2.2 Language support

Management Server provides the following interface languages: English, German, French, Chinese, Czech, Dutch, Greek, Hungarian, Italian, Japanese, Polish, Portuguese, Russian, Spanish, and Swedish.

The documentation and online help are available for download on OpenText My Support in the following languages: English, German, and French.

2.3 Sample project

When you sign in to Management Server for the first time, your first step is to select a project to which you have access. You usually select a project through the **Project** menu item in the module menu. For more information about selecting projects, see section 3.4 "Module menu" in *OpenText Web Site Management Server - Overview Guide (WSMS-UGD)*.

For demonstration purposes, OpenText provides the *Xample* project as a fixed component. This project can be installed when you install Management Server for the first time. With update installations, you will need to import this project manually. For more information about installing, updating, or importing this project, see "Install sample project (optional)" on page 26.

The *Xample* project provides you with many concepts, structures, and building blocks. You can apply these concepts when creating your own projects. Read this documentation to check whether the functionality provided is applicable to your requirements. Note that some of the concepts are designed to ensure sustained quality rather than the quick implementation of a certain feature.

The following goals have been defined for the *Xample* project:

- Easy maintainability is the prerequisite for a website project to have sustainable quality and extensibility. Each Site Builder must be capable of working quickly and intuitively with the project, even after months.

- High adaptability ensures that the project can grow with the requirements over time. With regard to layout, this project provides adaptability by using Twitter Bootstrap, one of the most common HTML5/CSS frameworks. Customization is then simple for the website projects based on it.

- Reusability ensures that individual building blocks from this project can be used in other website projects.

- Suitability as a reference means that the existing functionality can also serve as a reference for certain scenarios so that these functions can be implemented more quickly and reliably.

When you import the *Xample* project, the following users are automatically imported and assigned. All users have the default password demo123 assigned. Make sure that you change the passwords to a new value.

- User name: kate / Full name: Kate Miller / Role: Site builder

- User name: kristen / Full name: Kristen Reed / Role: Author (English)

- User name: sandra / Full name: Sandra Schiller / Role: Author (German)

- User name: jacques / Full name: Jacques Dupont / Role: Author (French)

- User name: sakura / Full name: Sakura Watanabe / Role: Author (Japanese)

- User name: akilah / Full name: Akilah Chaled / Role: Author (Arabic)

- User name: amy / Full name: Amy Redler / Role: Editor in Chief (English)

- User name: bernd / Full name: Bernd Freilich / Role: Editor in Chief (German)

- User name: camille / Full name: Camille Lablanc / Role: Editor in Chief (French)

- User name: haruki / Full name: Haruki Osaka / Role: Editor in Chief (Japanese)

- User name: halim / Full name: Halim Ibrahim/ Role: Editor in Chief (Arabic)

- User name: dora / Full name: Dora Tradlinger / Role: Translator (English to German)

- User name: clair / Full name: Clair Dubois / Role: Translator (English to French)

- User name: honola / Full name: Honola Moriwaki / Role: Translator (English to Japanese)

- User name: yasmin / Full name: Yasmin Dawud / Role: Translator (English to Arabic)

Design and structure have been carefully chosen to keep the sample project simple and at the same time make sure that it can serve as an example of good practice. The structure is uncomplicated but comprehensive so that the project can run out of the box in a basic way.

It should also be taken into account that every project has its own individual requirements. Every project needs its own approaches that may differ from those taken in the *Xample* project. Use this project particularly in the initial phase of your website project to create a solid foundation with clear concepts, conventions, and a clean template code.

Sample project updates

For updates of the sample project, OpenText recommends that you delete your existing sample project and then import the new version.

With update installations, the sample project is not available for automatic import. The import package is available on OpenText My Support (https://knowledge.opentext.com/) and can be imported manually. OpenText recommends that you import the sample project as a test project including archive and administration settings.

2.4 Installation notes

The Management Server installation has been extensively automated. However, be sure to pay attention to certain installation requirements that are described in the next section.

2.4.1 Creating technical Windows users

The following Windows users are required for the Management Server installation:

- **apppooluser** - This user

  - runs the IIS Application Pools used by Management Server

  - does not need to have administrator rights

  - is assigned the logon as service policy during installation

  - should have selected the account attributes *User cannot change password* and *Password never expires*.

- **serviceuser** - This user

  - runs the Management Server Windows services

  - must have a password

  - is assigned the logon as service policy during installation

  - must be created in MS-SQL Server if windows authentication is used

  - should have selected the account attributes *User cannot change password* and *Password never expires*.

> **Notes**
>
> - Optionally, you can also create only one user to perform the tasks of the *serviceuser* and *apppooluser*.
>
> - The users can be regular Windows users and do not need to belong to a group. It is recommended to disable login for these users.
>
> - If the user password has been changed, the changed password must be configured in Management Server by executing the Configuration Utility with the updated password.

2.4.2   Creating website for Device Preview option

If you want to install the **Device Preview** option, you must create a separate website for device preview in IIS. This website must not be the same as the one used for Management Server.

The website must have an HTTPS binding on an arbitrary port. The website is then offered in the Configuration Utility.

2.4.3   Installation checklist

The following requirements must be met regardless of which operating system you use:

- The latest service pack.

- Server logon with local administrator rights (*installingAdministrator* user).

    > **installingAdministrator user**
    >
    > This user
    >
    > - is needed only during installation and update installation.
    > - must have administrator rights
    > - must be created in MS-SQL Server if windows authentication is used.

- Permanent *IP address* for the server.

- Management Server license key.

- Installed Internet Information Services (IIS) [*1]

    > **Important**
    >
    > If the WebDav feature is installed: in the **Internet Information Services (IIS) Manager**, you must uninstall or disable the WebDav feature for the Site hosting your Management Server.
    > The usage of external WebDav folders is still supported.

- Installed Microsoft .NET Framework. For the required .NET Framework version, see the latest release notes. [*1]

    - ASP .NET State Service must be enabled.

- Installed HTTP activation feature. In *MS Windows Server Manager*, navigate to *Add Roles and Features Wizard > Select Features > Features > .NET Framework 4.5 Features > WCF Services* and select **HTTP Activation**.

*1) The installation files should be available for these components.

Supported Windows systems

You must install the *Web Server (IIS)* in Microsoft Windows Server Manager and select the following additional Role Services:

- ASP.NET
- ASP
- CGI

> **Note:** You must install Microsoft .NET Framework before activating ASP.NET. For the required .NET Framework version, see the latest release notes.

> **MS SQL Server collation settings**
>
> If you use MS SQL Server as the database, check the collation name settings in the database properties prior to installation. The sorting must be set to *case insensitive*, which means differences in upper and lower case are ignored. This is the default setting in the standard installation of MS SQL Server. If the sorting is set to **case sensitive**, the installation will fail.

All dependencies shown here must also be applied.

2.4.4 Preparing the installation

Before installing Management Server, pay attention to the following points:

- The setup package contains a release notes file. Open the file and read the *Installation and Upgrade Notes* section carefully.

- Note that day-to-day work on a project (not including image and media objects) can more than double the amount of information stored in the database. Versioning can result in a database that is by far larger than the actual project database.

- Every restriction placed on the operating system or on the administration accounts can have a negative effect on Management Server functionality. You should therefore install Management Server without restrictions first. Then implement the necessary restrictions incrementally and check Management Server functionality after each step.

- If you use Oracle databases for data storage, read the "Oracle as Management Server database" on page 73 section before you install Management Server. Keep the TNS name of the database connection as well as the names and passwords for the defined schemas at hand when you install Management Server.

- Make sure that there are no hardware or software problems with the Windows operating system before installing. Install the operating system in compliance with the Microsoft hardware compatibility list.

- Make sure that the server has a fixed IP address. You will need it to create the license.

- We recommend that you run Management Server and database server on different physical systems.

- We recommend that you install additional software on the server only after you have installed the database server and Management Server. Check the Management Server functionality before installing additional software.

- It is not possible to install Management Server on virtual or connected network drives.

📄 **Check collation name settings**

If you use MS SQL Server as the database, be sure to check the *collation name* settings in the database properties prior to installation. The sorting must be *case-insensitive*, which means differences in upper case and lower case are ignored. This is the case in the standard installation of MS SQL Server. If the sorting is *case-sensitive*, the installation will fail and you will not be able to use the system.

2.4.5   Requirements for Microsoft SQL Server with Windows authentication

To establish a database connection in Management Server by the **MSSQL WinAuth** database access mode, you must prepare the system before you install Management Server.

Notes on installation

To use MS SQL Server with Windows authentication, create the following user accounts in the Windows operating system of the database server and in MS SQL Server:

- user *installingAdministrator*.

- user *serviceuser* for internal Management Server access to the database through services, specified in the installation as SERVICE_USERNAME, for example, *WSMUser*.

See also and .

To create the user for the Management Server installation:

1. Create a Windows user account on the database server that corresponds to the user *installingAdministrator* (with matching user name and password) who will perform the Management Server installation.

2. Add the Windows user that you have created for MS SQL Server as a new user. If the user has not received the necessary permissions through membership in the *PREDEFINED\administrators* group, the user must be assigned the **server role: system administrators** setting.

Example: The *Administrator* Windows user is used for installing Management Server (*installingAdministrator* user). On the database server, the existing administrator is assigned the same password as on the application server. Through the membership in the

PREDEFINED\Administrators group on MS SQL Server, the user has sufficient rights (*system administrators*) if the *PREDEFINED\Administrators* group has been created as predefined.

To create the user for internal access to the database:

Management Server internally uses the *serviceuser* for Windows authentication and to access the databases. See also "Creating technical Windows users" on page 13.

Create the user also on MS SQL Server. Proceed as follows:

1. On the database server, create a Windows user account that corresponds to the *serviceuser* (with matching user name and password) that will be set up during the Management Server installation process. Membership in the *Users* group is sufficient. See also "Creating technical Windows users" on page 13.

2. Add the user that you have created to MS SQL Server. The user must have the Server Role setting **Database Creators + Process Administrators**.

3. After performing the configuration steps as described below, running the Configuration Utility, and creating the administrative database, map the user that you created in step 2 into the administrative database and allow him at least read and write access.

To edit the configuration file and perform the configuration:

1. Perform the Management Server installation either in the command shell or use the graphical user interface. Note that after the installation is completed, you must edit the configuration file manually and perform the configuration part in the command shell.

   > **Note:** Alternatively, you can perform steps 2 and 3 by using the *Configuration Utility* assistant. Run `ConfigurationUtitityGUI.exe` to open the assistant.

2. Edit the `ConfigurationUtility.exe.config` file, as described in "Editing the configuration file" on page 67.

3. Start `ConfigurationUtility.exe`.

   > **Note - User**
   >
   > The *serviceuser* must remain activated on MS SQL Server with the described permissions even after the Management Server installation.
   >
   > The *installingAdministrator* user who is used for the installation can be deactivated for the operation of Management Server after the Management Server installation. This should only occur when a new user account was created on the database server. As opposed to the example, the existing local administrator was not used.

   > **Important - Deactivating groups**
   >
   > Deactivating groups (for example, *PREDEFINED\Administrators*) on MS SQL Server can create a situation in which users no longer have access, which

means that MS SQL Server is no longer available. You must, therefore, be extremely cautious when deactivating users or groups on MS SQL Server.

2.4.5.1   Converting an existing Management Server

An existing Management Server can be converted to Windows authentication. The following steps are necessary:

- "Step 1: Set up a new server connection in Management Server" on page 18

- "Step 2: Create a user on the database server" on page 18

- "Step 3: Modify the RDServer.ini file" on page 19

- "Step 4: Export Management Server projects with administration data" on page 19

- "Step 5: Import Management Server projects with administration data" on page 20

- "Step 6: Assign the user as the database owner" on page 20

- "Step 7: Restart the application server" on page 20

Step 1: Set up a new server connection in Management Server

1.   Open **Server Manager** in Management Server.

2.   Click **Create Server Connection** in the *Action Menu* under *Start > Administer Database Servers > Server Connections*.

      The *Create Server Connection* dialog box opens.

3.   Select **MSSQL WinAuth** from the **Select access mode** drop-down list.

4.   Click **OK**.

      The next dialog window opens.

5.   Specify a **connection name**.

6.   Enter your MS SQL Server data in the **Server** and **Database** boxes.

7.   Click **OK**.

Step 2: Create a user on the database server

Management Server uses the *serviceuser* that was created during Management Server installation to access the database. This user must also be available in the Windows system of the database server and in MS SQL Server. Configure these settings as described in "Notes on installation" on page 16. See also "Creating technical Windows users" on page 13.

Step 3: Modify the RDServer.ini file

1. To enable access to the Management Server administration and language database, you need to change the entries in the `RDServer.ini` file (`<Installation directory>/MS/ASP/RDServer.ini`) as in the following example.
   Example entries before modification:

   ```
   [Administration]
   cs=Provider="SQLOLEDB";Data Source="SQLSERVERNAME";Initial
   Catalog="ioAdministration";
   User Id="sa";Password="<%password%>"; password=86QORHltSqE=
   connectionguid=35AG97F5BFD1489A87CEEA3A23365288
   ```

   Example entries after modification:

   ```
   [Administration]
   cs=Provider="SQLOLEDB";Data Source="SQLSERVERNAME";Initial
   Catalog="ioAdministration";
   Trusted_Connection=yes;
   ```

   The entries for `User Id`, `password`, and `connectionguid` are omitted. The `Data Source` attribute must contain the name of the database server used (in the example: `SQLSERVERNAME`).

2. Save the changes in the `RDServer.ini` file.

Step 4: Export Management Server projects with administration data

Export the projects of the application server for which you want to use Windows authentication. To do so, proceed as follows:

1. Open **Server Manager** in Management Server.

2. Select the desired project under **Start > Administer Projects**.

3. Select the **Export Project** menu item in the Action Menu.

   The *Export Project* dialog window opens.

4. Select an **Export target** using the **Search** function.

5. Make sure that the **Include administration settings** check box is selected (default setting).

6. Click **OK**.

   The project is exported. Depending on the project size, this process may take some time. You can choose to be notified by email when the export process has been completed. For more information, see section 5.1.10 "Exporting projects" in *OpenText Web Site Management Server - Server Manager Guide (WSMSSM-AGD)*.

7. Check the `Project` component in the `wsms.log` file under **Start > Administer Application Servers > Application Servers > Log Files** to make sure that no errors occurred during export.

8. Repeat this procedure for each project for which you want to use Windows authentication.

9. Once the projects have been exported without errors, you can delete them in Server Manager under **Start > Administer Projects** by selecting the desired project and then the **Delete Project** action in the Action Menu.

Step 5: Import Management Server projects with administration data

Import the exported projects back into Management Server using the server connection that you set up in the first step. To do so, proceed as follows:

1. Open **Server Manager** in Management Server.

2. Go to **Start > Administer Projects** and click **Import Project** in the Action Menu.

   The **Import Project** dialog box opens.

3. Enter the name of the project you intend to import in the **Project name** box.

4. In the **Database server** drop-down list, select the database server connection that you set up in the first step.

5. Use the **Search** function to select the **Source** of the project to be imported.

6. Select the **Include administration settings** check box.

7. Click **OK**.

   The project is imported. Depending on the project size, this process may take some time. You can choose to be notified by email when the importing process has been completed. For more information about importing projects, see section 5.1.3 "Importing projects" in *OpenText Web Site Management Server - Server Manager Guide (WSMSSM-AGD)*.

Step 6: Assign the user as the database owner

Execute the stored procedure, sp_changedbowner, on MS SQL Server (for example, using the SQL Server Management Studio) for the Management Server database *ioAdministration*.

The user is now the database owner (dbo).

Example:

```
use ioAdministration
exec sp_changedbowner 'SQLSERVERNAME\CMSUser'
```

SQLSERVERNAME denotes the database server that is used.

Step 7: Restart the application server

Restart the application server so that the new server connection takes effect. This can be achieved either by rebooting the Windows operating system or by restarting the Management Server Windows services:

- To stop the application server, stop the Windows server
  `OTWSMNavigationService`.

- To start the application server, start the Windows server `OTWSMClientService`.

2.5 Performing the installation and configuration

The following sections guide you through the installation process step by step.

The installation consists of two main parts: installation and configuration:

1. **Installation** - The installation part is done by a Windows Installer (*msi* file). This *msi* copies the required files. It also configures the IIS and takes care of installing necessary dependencies like Visual C++ Runtime.

2. **Configuration** - The *configuration* part is done by a normal windows application. It configures the IIS and Application Pool. It also sets up databases and inserts basic data as license key, host name, Management Server administrative user and other settings. Inputs like database connections will be validated. It also configures the Windows Services and starts them after successful configuration. This might take some time.

After finishing the configuration part, the Management Server installation is complete and you can log on to the system.

2.5.1 Start the installer package

1. Unpack the ZIP file `ManagementServer_16_<build>` in a directory on your server.

2. Double-click the `setup.exe` file to start the installation.

   > **Note:** If you do not have the necessary rights, a **Windows User Access Control** dialog shows up and asks for administrator credentials.

   The **Welcome** dialog opens.
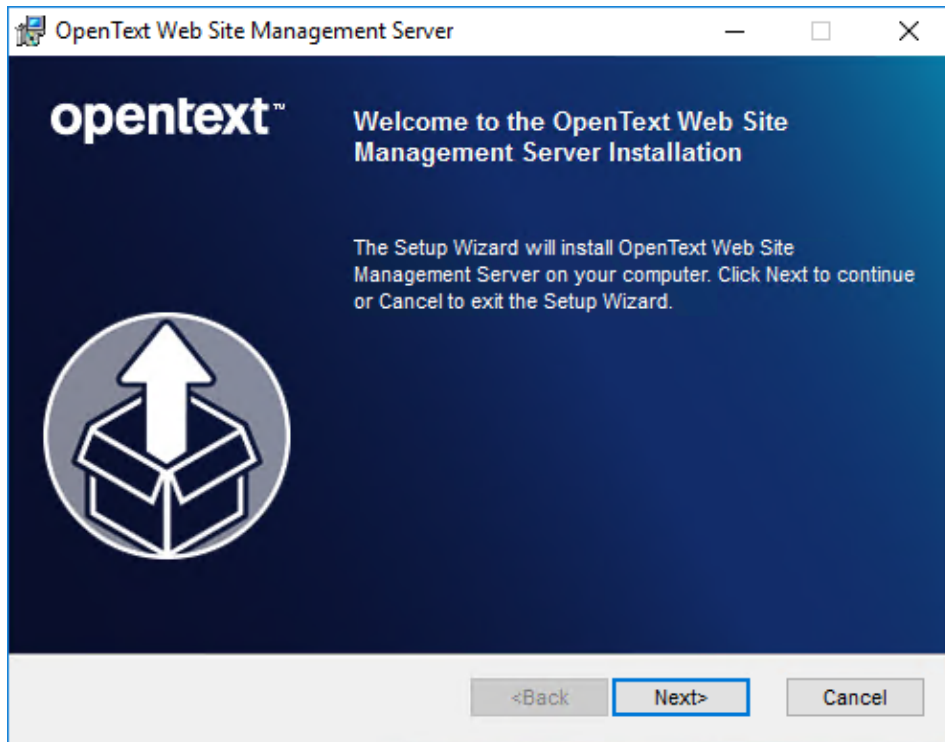
3.   Click **Next**.

The system checks the installation requirements. If any of the installation requirements have not been met, you will receive a corresponding message.

📄 **Creating installation log files**

Per default, no log file is created during installation. If you want to create a log file, you must start the installation in a command shell. Enter the following command:

```
msiexec /l*v <LogfileName> /i <MSIName>.msi
```
For example:
*msiexec /l*v install.log /i OpenText.WS.MS.Installation.msi*

2.5.2   **Read the license agreement**

The **License Agreement** dialog box opens.
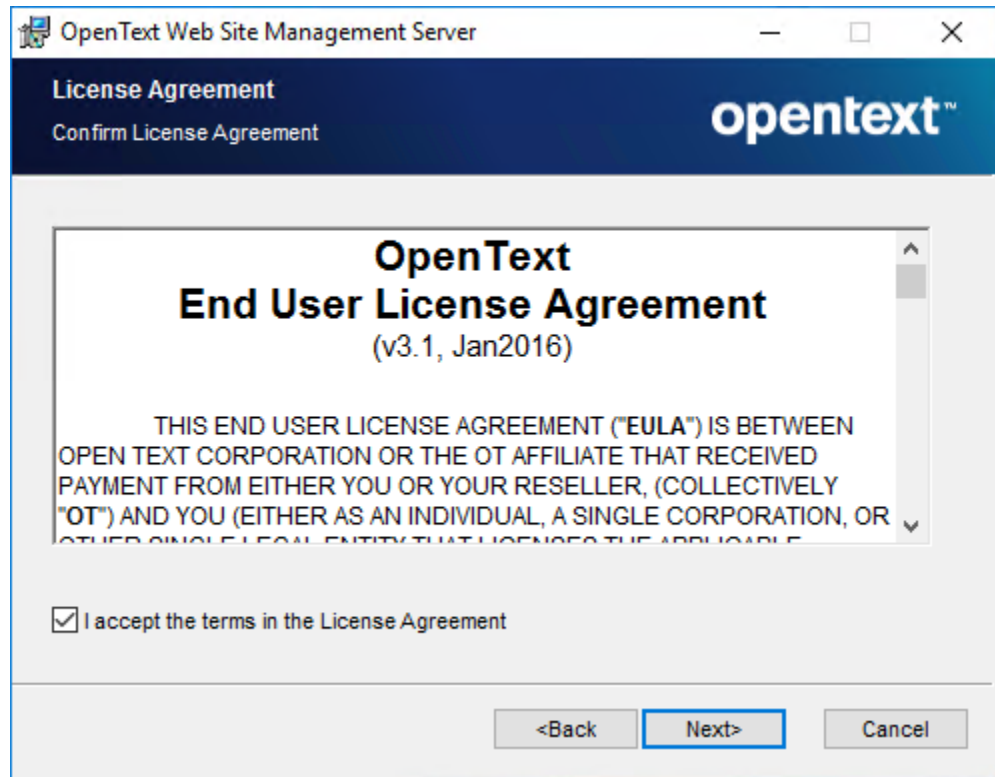
1. Read the license agreement carefully. Confirm the license agreement by selecting the **I accept the terms in the License Agreement** check box.

2. Click **Next**.

2.5.3 Specify the destination folder

The **Destination Folder** dialog box opens.
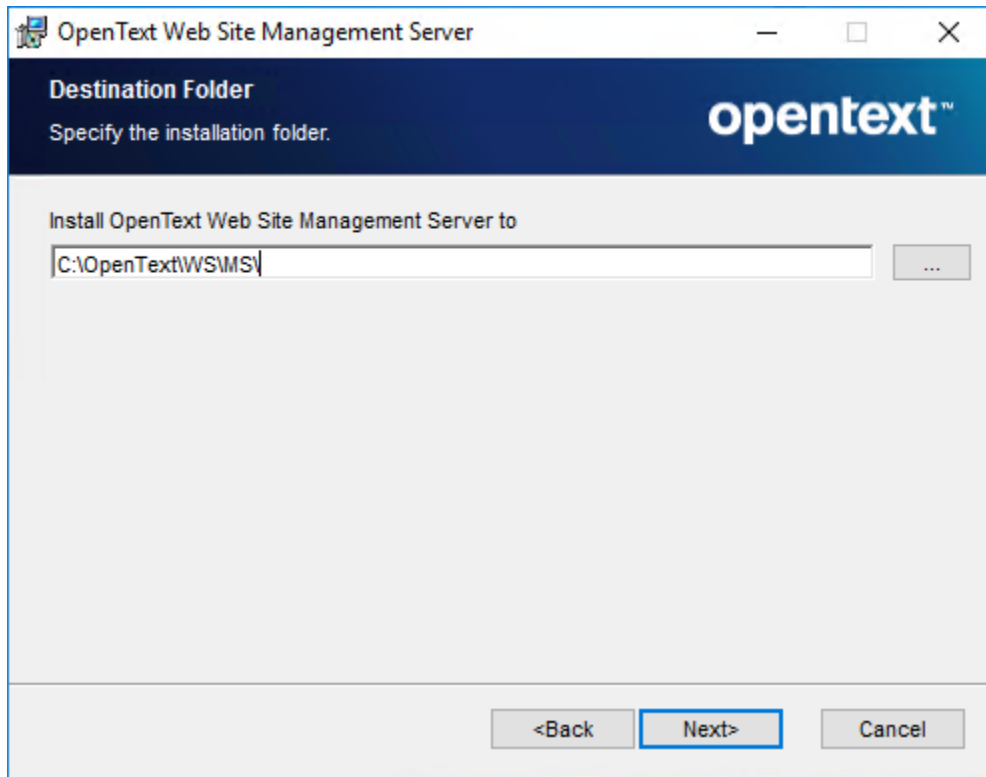
1. Specify the folder to which you want to install Web Site Management Server.

    You can change the installation path by clicking **...**. Always install the software on the hard disk of the local computer.

2. Click **Next**.

2.5.4   Install Mobile Client (optional)

The **Custom Setup** dialog box opens.

> **Note:** The **Custom Setup** dialog is only displayed during first time installation or change installation in **Programs and Features** > **Change** > **Add/Remove Features**. It is not shown during update installations.
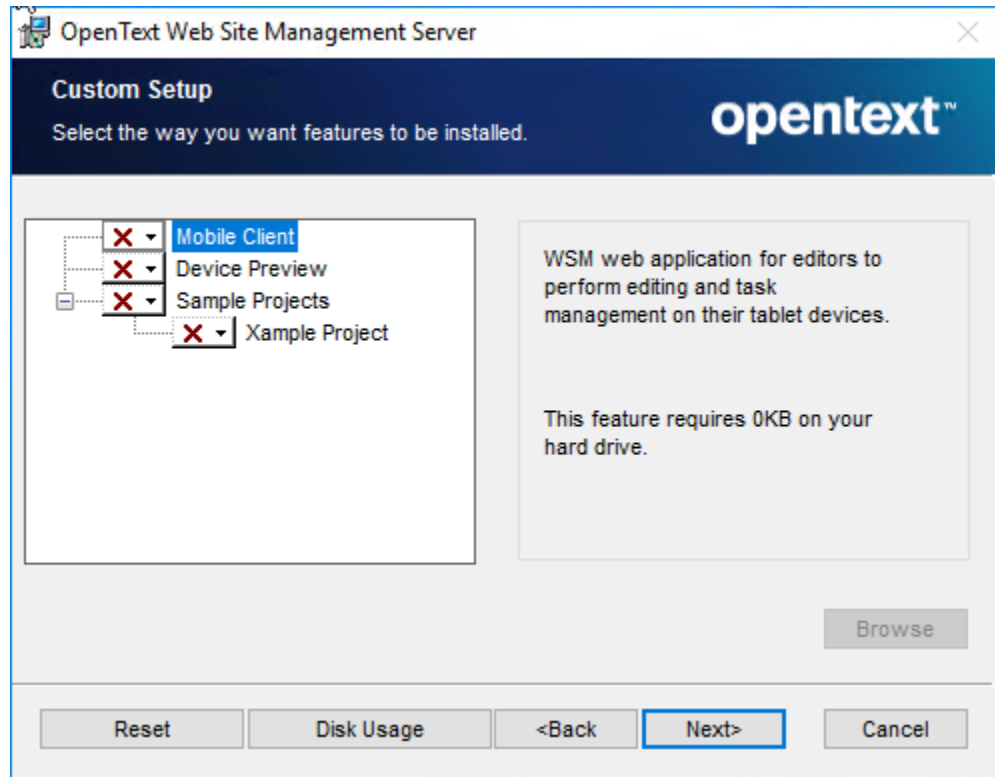
1. Select the **Mobile Client** item.

2. Click ❌▾ to select the way you want to install the Mobile Client. By default, the **Mobile Client** option is set to `This feature will not be available`.

3. Install the next item or click **Next** to leave the **Custom Setup** dialog box.

2.5.5 Install device preview (optional)

> 📄 **Note:** The **Custom Setup** dialog is only displayed during first time installation or change installation in **Programs and Features** > **Change** > **Add/Remove Features**. It is not shown during update installations.

1. In the **Custom Setup** dialog box, select the **Device Preview** item.
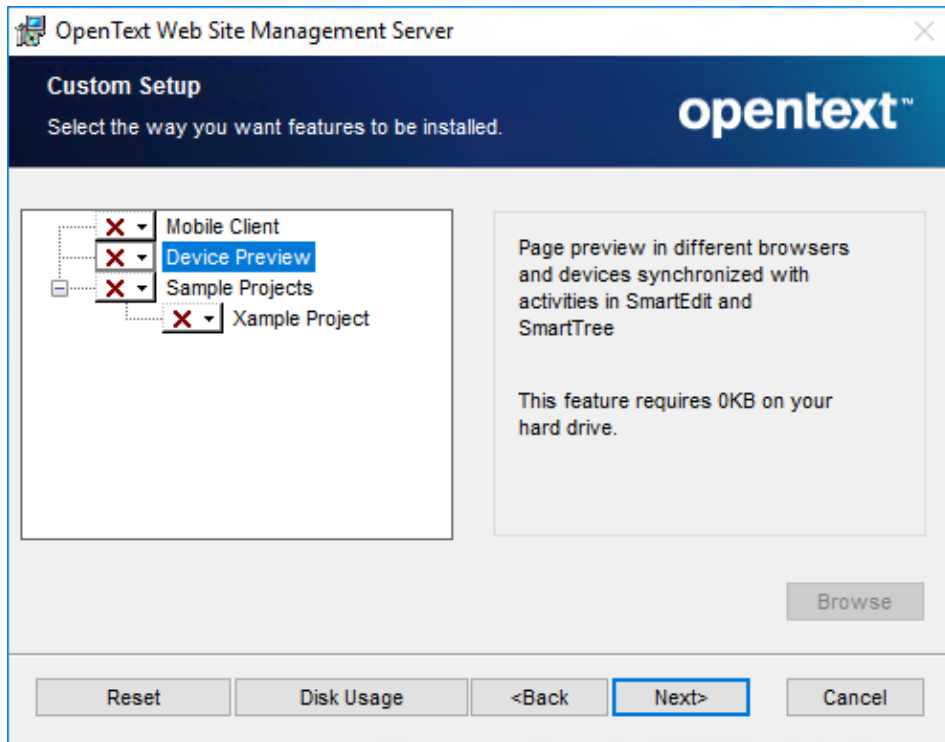
2. Click to select the way you want to install the device preview. By default, the **Device Preview** option is set to `This feature will not be available`.

3. Install the next item or click **Next** to leave the **Custom Setup** dialog box.

2.5.6   Install sample project (optional)

> **Note:** The **Custom Setup** dialog is only displayed during first time installation or change installation in **Programs and Features** > **Change** > **Add/Remove Features**. It is not shown during update installations.

1. In the **Custom Setup** dialog box, select the **Xample Project** item.
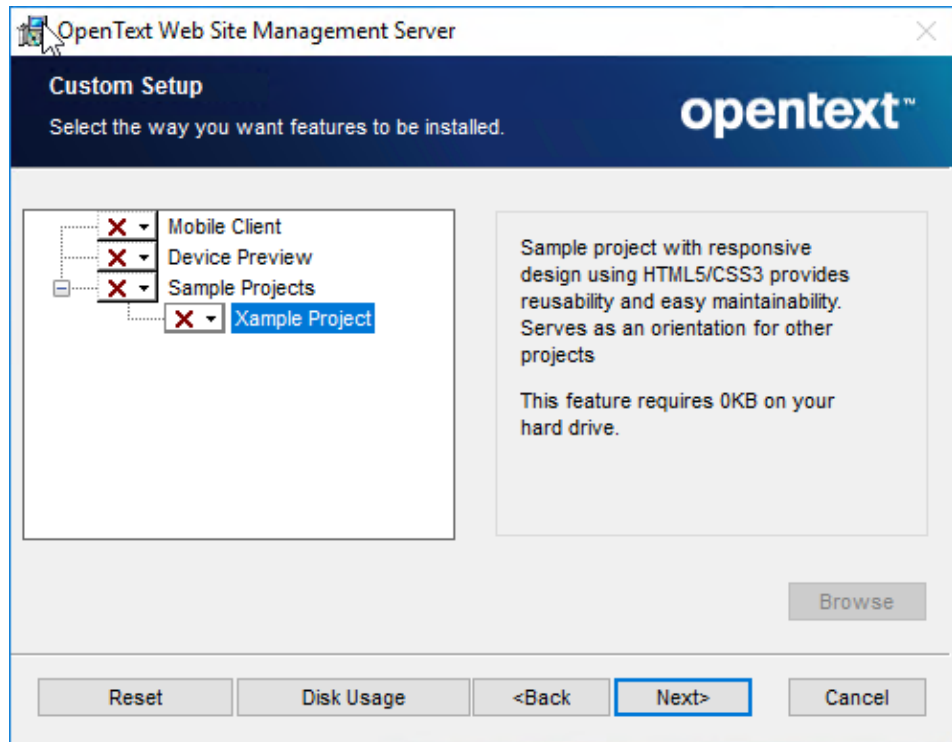
2. Click [X ▾] to select the way you want to install the sample project. By default, the sample project option is set to `This feature will not be available.`

3. Click **Next** to leave the **Custom Setup** dialog box.

> **Sample project**
>
> The installation contains the *Xample* project. It can be imported during installation by adding appropriate entries to the configuration file and running the silent mode configuration. For more information, see "Sample project" on page 11 and "Editing the configuration file" on page 67.
>
> You can also import the project by project import in the installed Management Server. Sample projects are available for download on My Support (https://knowledge.opentext.com/knowledge/cs.dll/Open/19169639).
>
> - The sample project contains default users. For security reasons, the project is set to *not available* in the **Custom Setup** dialog by default. You must select the project explicitly for installation.
>
> - Only during a first time installation, the sample project can be imported using the configuration assistant. There is no graphical configuration during updates or changes.

2.5.7   Finish the installation

The **Ready to Install** dialog box opens.

1.   You have the following options:

   - To start the installation of Management Server, click **Install**.

   - To review or change any of your installation settings, click **Back**.

   - To cancel the installation, click **Cancel**.

2.   If you click **Install**, the **Installing the product...** dialog box opens. Wait until the installation is completed.

3.   When the installation is complete, click **Finish** in the **Completing the Web Site Management Server installation** dialog box.

2.5.8   Start the configuration

After the installation phase is completed, the Configuration Utility for the Management Server initial configuration opens.
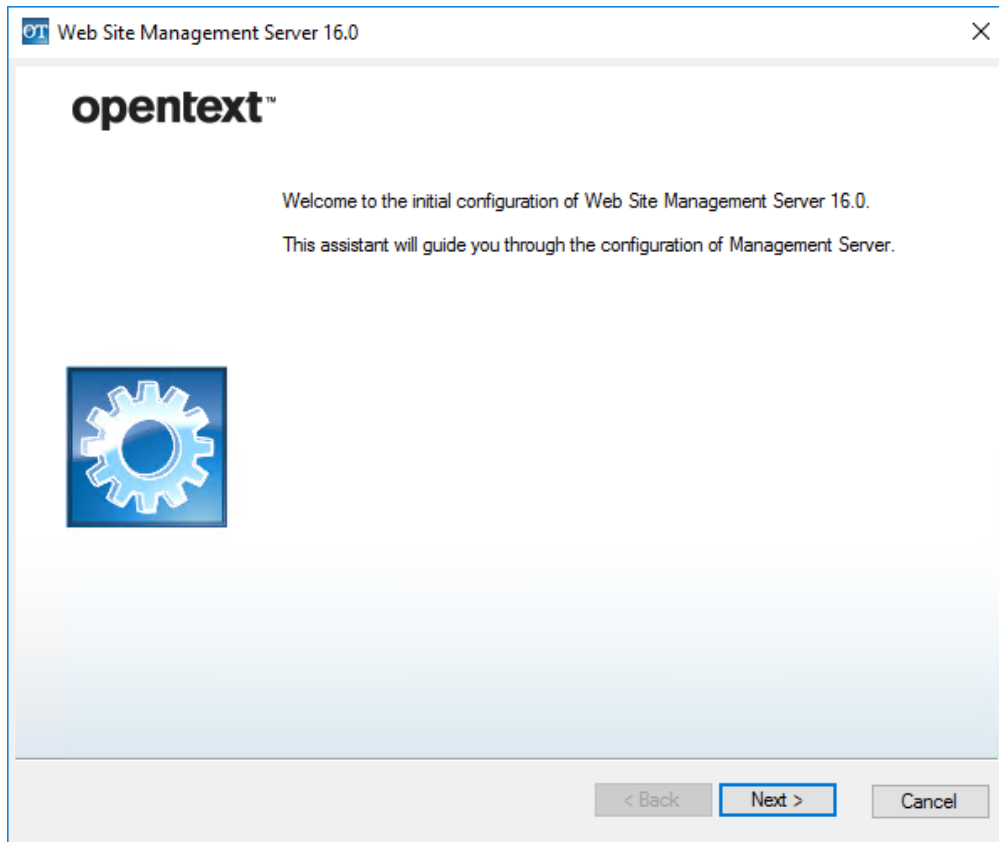
❗ Important

If the Configuration Utility does not open or closes again and you receive an error message, check the following:

- **Environment variable is not set** - Check if the environment variable *RDMS* was set during the installation process. Open a command shell and enter `set rdcms`. If the variable has been set, you should receive as a result the following path:
  `RDCMS = c:\OpenText\WS\MS\ASP`.
  This variable must be set to enable the start of the configuration assistant.

- **Configuration file could not be found** - During the call of the configuration assistant, the `ConfigurationUtility.exe.config` file is created. If this has failed, the configuration assistant cannot proceed.

📄 **Note:** The Configuration Utility uses values that are already configured in an existing configuration file of a previous version. Values that are only stored in the Management Server database or special configuration files cannot be used and might be overwritten. For example, when migrating from version 10.x to version 11.1 or later, the already stored value for `Host URL` will not be taken from an already existing administration database. Instead, it will be overwritten by the one defined in the **Host URL** field in .

- Click **Next**.

2.5.9   Enter the license key

The **License key** dialog box opens.
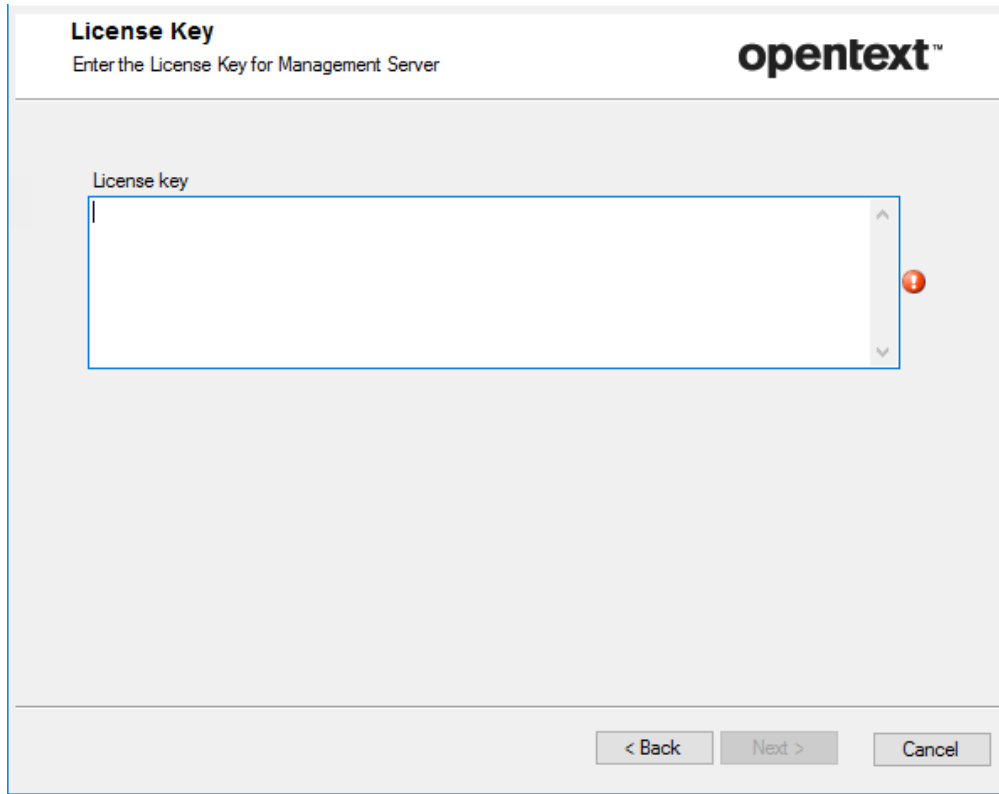
1. In the **License key** box, enter your license key.

2. Click **Next** to continue the configuration.

   The license key is verified when you click **Next**.

   Note: Note that the license key determines some of the following configuration dialog boxes. For example, creating an administration database is only possible with a full license, not with a cluster license.

2.5.10   Specify the Services user

The **Services User** dialog box opens.

1. In the **User name** box, enter the name of the *serviceuser*. Enter .\ or the server name in front of the user name if the user is a local user, or enter the domain name for a domain user.

    Note that the user must already exist. To create the required technical Windows users, see "Creating technical Windows users" on page 13.

2. In the **Password** box, enter the password of the user.

3. Click **Next**.

    📄 **Notes**

    • When clicking **Next**, the credentials are validated. If the user name has been specified without account information, the user name is checked first against the local machine. In case this validation fails, it is then checked against the domain.

    • **Validation of domain user fails** - If the validation of a domain user fails repeatedly, even though you have ensured that the provided credentials are correct, enter the port number in the `ConfigurationUtility.exe.config` file into the `DomainPort` attribute. For more information, see "Editing the configuration file" on page 67.

2.5.11   Specify the Application pool user

The **Application Pools** dialog box opens.

1.   In the **User name** box, enter the name of the *apppooluser*.

   Note that the user must already exist. To create the required technical Windows users, see "Creating technical Windows users" on page 13.

2.   In the **Password** box, enter the password of the user.

3.   Click **Next**.

   📄   **Notes**

   *   When clicking **Next**, the credentials are validated. If the user has been specified without account information, the user name is checked first against the local machine. In case this validation fails, it is then checked against the domain.

   *   **Validation of domain user fails**

      If the validation of a domain user fails repeatedly, even though you have ensured that the provided credentials are correct, enter the port number in the ConfigurationUtility.exe.config file into the DomainPort attribute. For more information, see "Editing the configuration file" on page 67.

2.5.12 Specify the website for Management Server in IIS

The **Management Server IIS configuration** dialog box opens.

1. Select a website for Management Server web client and mobile client. You must have set up this web site before starting the Configuration Utility.

2. Enter the name for the **Application alias (web client)** under which you want to access the Management Server web client after the installation.

3. Enter the name for the **Application alias (mobile client)** under which you want to access the Mobile Client after the installation. This option is only available if the Mobile Client feature is installed. By default, the value is WSM. The name must be unique within the selected IIS website. For the name string, only characters a-z and 0–9 are allowed.

    > **Note:** The Mobile Client will be installed into the same website as Management Server. The entry in the **Website** box cannot be edited.
    >
    > The Mobile Client will be installed in the following folders:
    >
    > - *<Installation folder>*\Web\MobileClient
    >
    > - *<Installation folder>*\Web\WebService\MobileServices

4. Click **Next**.

When clicking **Next**, the alias name is checked for the correct use of characters.

2.5.13   Specify the website for device preview in IIS (only if selected)

The **Device Preview IIS Configuration** dialog box is only shown if the Device Preview feature is installed.
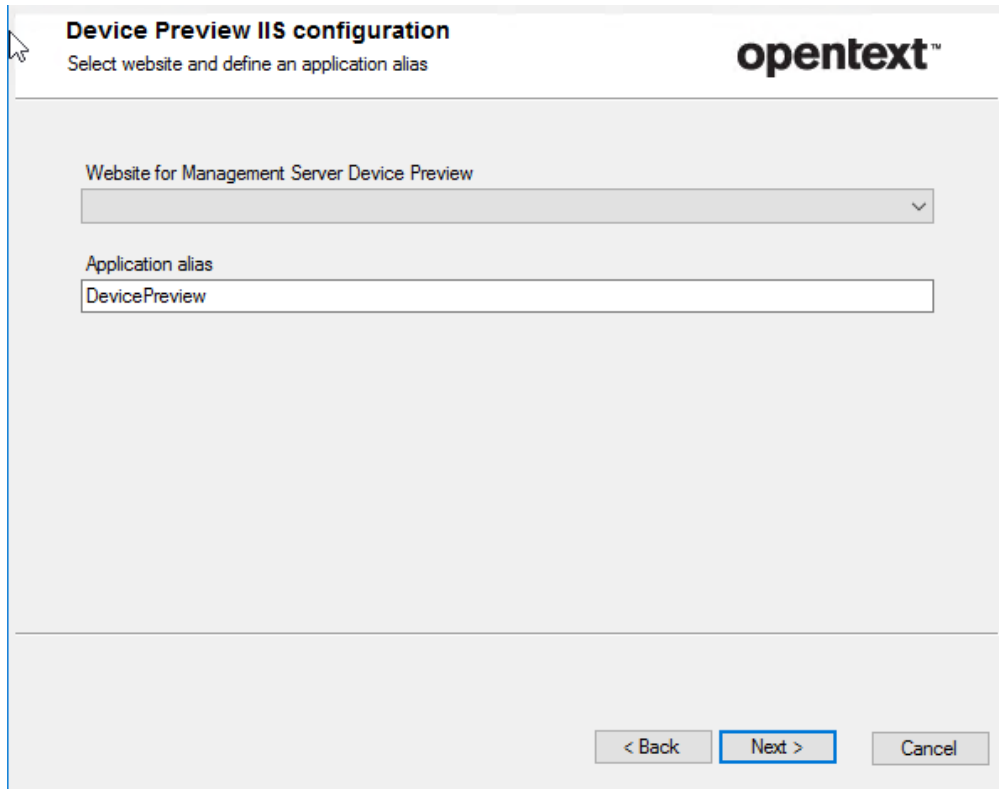
1.   Select a separate **Website** for the device preview installation. Only websites that have an HTTPS binding on an arbitrary port and have not been selected for Management Server in the previous step are offered for selection. You must have set up this web site before starting the Configuration Utility. Do not leave the **Website** box empty.

2.   Enter the name for the **Application alias** under which you want to access the device preview after the installation. By default, the value is `DevicePreview`. The name must be unique within the selected IIS website. For the name string, only the characters `a-z` and `0–9` are allowed. The device preview will be installed in the following folders:

   - *<Installation folder>*\Web\DevicePreview

   - *<Installation folder>*\Web\DevicePreviewService

3.   Click **Next**.

When clicking **Next**, the alias name is checked for the correct use of characters. It is also checked if the selected website has been configured for HTTPS on port 8443.

2.5.14   Select the database

The **Database Type** dialog box opens.

1. Select one of the following options:

   - **MS SQL**

     For the next dialog, see "Configuring the MS SQL database" on page 36.

   - **Oracle**

     This option is only available if you have followed the steps in "Installing the Oracle client software" on page 78. From the **Drivers** list, you can select one of the Oracle database drivers that are installed on the system. For details how to add drivers to the list, see "Installing the Oracle client software" on page 78.

     ! Limitation for listed drivers

     Generally, there are two types of drivers that can be listed here:

     - drivers that are found on disk

- drivers that are installed in the Global Assembly Cache (GAC) and also registered as an ADO.NET Data Provider in `%WINDIR% \Microsoft.NET\Framework64\v4.0.30319\Config\ machine.config` under `<configuration><system.data><DbProviderFactories>.`
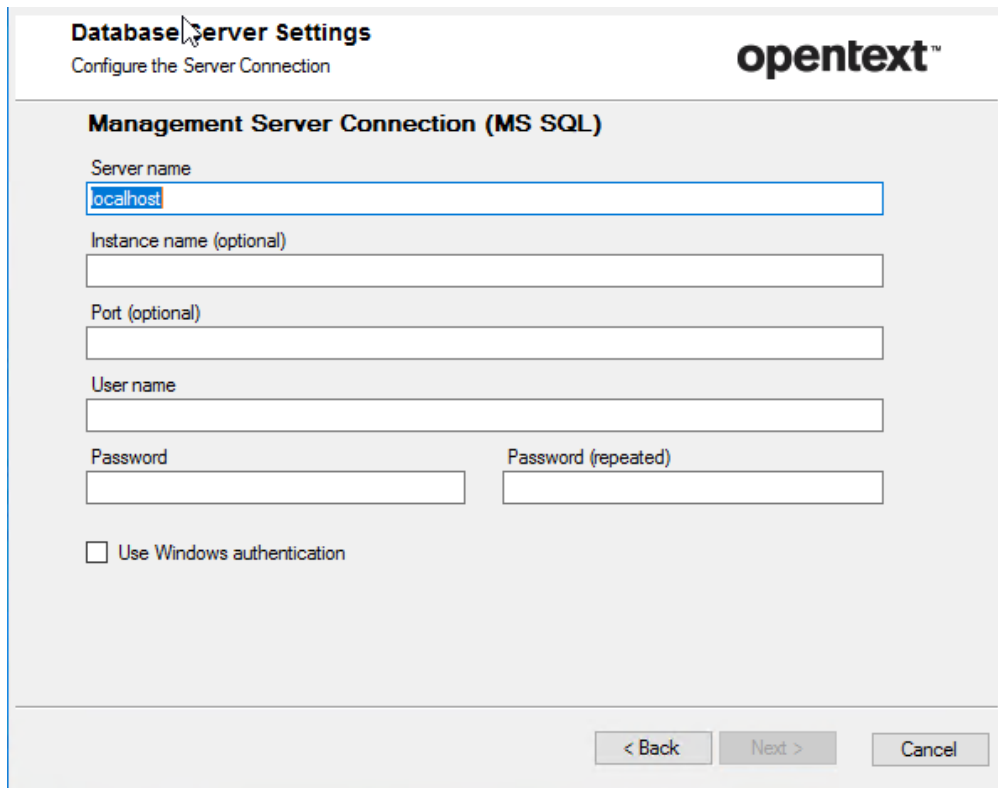
Because of a technical limitation, drivers that are installed in the GAC can mask drivers that are found on disk and make the latter unavailable for selection. If you want to use a driver from disk and cannot find it, uninstall drivers from the GAC. You can uninstall by using the `OraProvCfg.exe` tool that is provided by Oracle as part of the ODAC distribution package.

For the next dialog, see .

2.   Click **Next**.

2.5.14.1   Configuring the MS SQL database
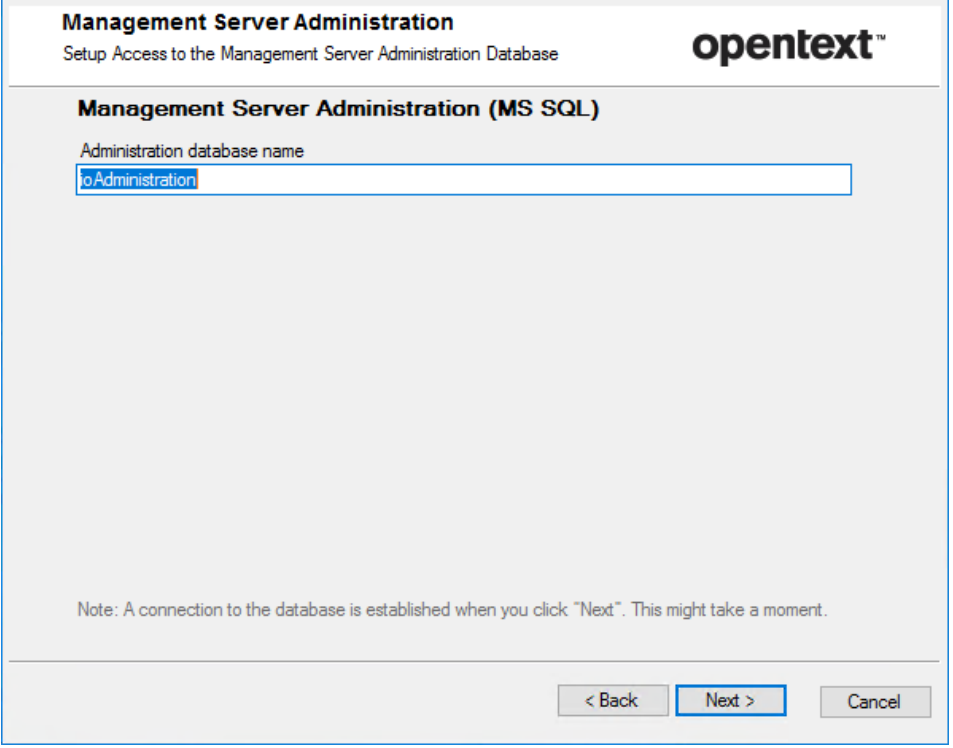
The **Server settings** dialog box opens.

1.   Edit the following settings:

- **Server name** - Enter the name of the database server.

- **Instance name (optional)** - Enter the name of a named instance of the database server, if you do not use the standard port *1433* or if you run more than one database server on your computer.

- **Port (optional)** - Enter the port number for accessing the database server. When you use the standard port *1433*, you can leave the box empty.

- **User name** - Enter the name of your database user.

- **Password** - Enter the password of your database user.

- **Password (repeated)** - Repeat the password of your database user.

- **Use Windows authentication** - Select the check box if you want to use Windows authentication. If the check box is selected, the *User name* and *Password* boxes are greyed out and cannot be edited. For more information about Windows authentication, see "Requirements for Microsoft SQL Server with Windows authentication" on page 16.

2. Click **Next**.

3. The **Management Server Administration** dialog box opens.

In the **Administration database name** box, enter a name for your Management Server administration database. The database is set up if it does not exist yet.

4. Click **Next**.

2.5.14.2   Configuring the Oracle database

The **Management Server Connection (Oracle)** dialog box opens.
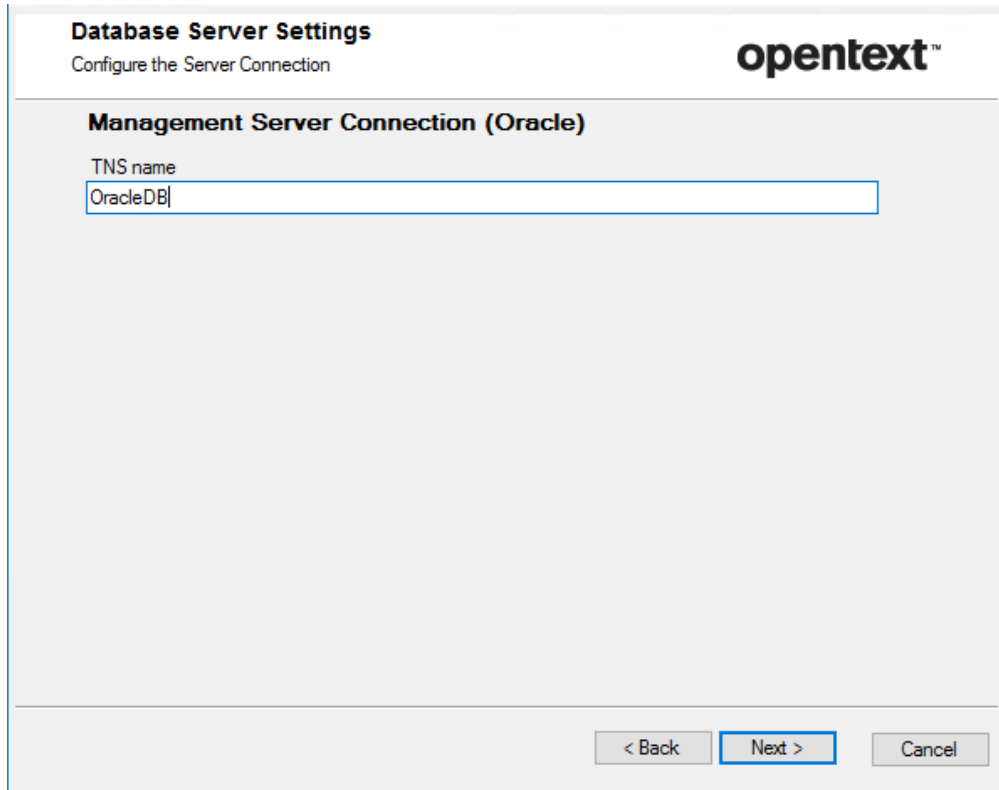
1.   Enter the **TNS name** for your Oracle connection and click **Next**.

The **Management Server Administration (Oracle)** dialog box opens.

2. Enter your prepared schema name in the **Management Server administration schema name** box. For details, see "Creating Oracle database schemas for Management Server" on page 76. Enter your **Schema password** and repeat it in the **Schema password (repeated)** box. Establishing the database connection might take some time.

3. Click **Next**.

2.5.15 Configure Server Settings and SSL

The **Server Settings** dialog box opens:

> **Important**
>
> Some system configuration settings in Management Server have been moved to the Configuration Utility. These settings are no longer editable in Server Manager. To change the settings after installation, you must run the Configuration Utility again. This affects the connection name, host name, host header, which have been renamed to *Host URL (PreExecute and RDExecute)*, cluster URL, port, and the SSL option.

1. Edit the following settings:

   - **Use secure connection (SSL)** - Per default, the check box is selected. If you do not want to use SSL, clear the check box. If the binding in IIS _corresponding to this option is not available, a warning 🔴 is shown.

   - **Host description** - Enter your connection name. The connection is displayed in the tree under this name.

   - **Host Name** - Select your host name from the drop-down list. Available values are host name and all IPV4 addresses of the server.

2. To edit more settings, click the **Advanced** button.

   > **Important**
   >
   > Note that if you click the **Simple** button to change back to Simple mode after editing settings in Advanced mode, the settings will switch back to

the default values. If you want to keep your changed values in the Advanced settings, do not click **Simple**.

In *Advanced* mode, you can edit the following settings:

- **Host URL (Preexecute and RDE execute)** - Enter your Host URL. The Host URL (for example, `https://<server name>:<port>/cms`) addresses the virtual Web site under which Management Server is available. It is used for internal IIS calls with RDExecute and PreExecute constructions. You enter it, for example, if you want to use a Web site other than the default Web site as the virtual Web site, or if a different server name has to be used for internal calls due to the network configuration.

- **Cluster URL** - Enter the name of the DNS cluster in this box. This name

  - is used for the email in which a link is provided to the page preview. In this way, the preview link calls the page via the official cluster URL and not via the application server from which the email was sent.

  - can be used as DNS name for Delivery Server preview if the corresponding option has been selected in the settings of the Delivery Server publishing target used for Delivery Server page preview. For more information, see section 3.6.5 "New Delivery Server publishing targets" in *OpenText Web Site Management Server - SmartTree Guide (WSMSST-AGD)*.

  📄 **Note:** If you want to use the HTTPS protocol for the preview links, you must enter the server name with the protocol in this box (for example, `https://<server name>:<port>/<web directory>`) .

- **Port** - Enter the port number.

3. Click **Next**.

2.5.16   Configure other settings

The **Other Settings** dialog box opens.

1. Edit the following settings:

    •   **User name of Management Server administrator** - Enter the user name of the initial administrator.

    •   **Administrator password** - Enter a password for the initial administrator.

    •   **Administrator password (repeated)** - Repeat the password for the initial administrator.

    •   **Spell checker URL (optional)** - Enter the URL of your spell checker server. For requirements, see "Network and internet connections" on page 10.

    •   **Overwrite configuration files** - If you select this check box, all configuration files are reset to their initial state, except for configuration files that explicitly define to ignore this setting. In addition, the Management Server's Windows services and IIS Web applications are removed and recreated.
        If the Configuration Utility registers that a configuration change requires a resetting to defaults, the check box is automatically selected and appears dimmed.
        After the configuration change has been applied, the check box is cleared to prevent that each running of the Configuration Utility configures the defaults again. For a list of configuration files affected by selecting the check box, see section 7.2.1 "Management Server" in *OpenText Web Site Management - System Overview Guide (WS-GGD)*.

> **When to overwrite configuration files**
>
> Overwrite the configuration files in the following situations:
>
> - You changed the database, for example, when migrating to a new database.
> - You changed SSL settings.
> - You changed spell check settings.
> - Management Server does not work anymore after manually changing of a configuration file, Windows service, or the IIS configuration.

2. Click **Next**.

2.5.17 Import the sample project (optional)

The **Project import** dialog box opens if you selected the Sample Projects item for installation in .

1. If you want to import the sample project, select the **Import "Xample Project"** check box.

2. In the **Name of project in Management Server** box, enter the name under which you want the sample project to display in Management Server.

3. Click **Next**.

4. In the **Project Import** dialog box, do the following:

   - If you use an MS SQL database, enter the name of the sample project database in the **Database name** box.
   - if you use an Oracle database, enter the **Schema name** and the **Password**/ **Password (repeated)**.

5. Click **Next**.

2.5.18 Finish the configuration

The **Summary** dialog box opens.

1. Verify your configuration settings.
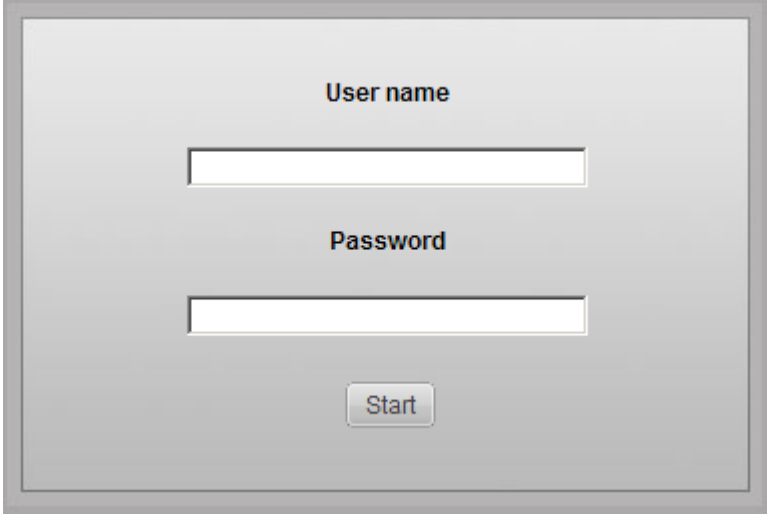
   ⚠ **Important**
   All existing configuration files will be saved as backup files and then overwritten. The only exception is the `validate.xml` file, which will not be overwritten, to keep changes done by integrations. Note that certain backup configuration files contain encrypted passwords. Therefore, we recommend deleting the backup files after checking.

   To change settings, click **Back**.

2. Click **Configure** to apply the configuration settings to your installation.

   The configuration scripts are run. When the configuration is complete, the confirmation dialog box opens.

3. Click **Finish** to complete the configuration.

2.5.19   Sign in to Management Server

1. Open your browser and call Management Server with the following URL:
    `https://<server name>.<domain name>/<application alias>/`
    For example: `https://wsms.yourcompany.local/cms`

    For installations not using *https*, you can also call the URL `http://localhost/cms/`

2. The sign in dialog box opens.

3. Enter the **User name** and **Password** specified during the installation.

2.5.20   Troubleshooting

Permanent reboot cycle on defective configuration file

If you use an invalid `%RDCMS%\processserver.main.config` file and reboot the machine, it might occur that the server enters a permanent reboot cycle.

To resolve this issue, proceed as follows:

1. During the server startup sequence, press **F8** to enter the Windows boot menu. Select **Safe Mode**.

2. Log on to the server.

3. Under **Administrative Tools**, open the **Services** dialog. Scroll down to the **OpenText** services.
    Change the startup type to **Automatic (Delayed Start)** for each of the following services:

    *   OpenText Data Service

    *   OpenText Navigation Service

- OpenText Server Service

- OpenText WebClient Service

This procedure will stop the reboot cycle. The Windows Event Log will show entries like "*Service cannot be started. System.TypeInitializationException: The type initializer for 'OpenText.WS.MS.XMLServer.MainService' threw an exception.
---> System.Exception: Error initializing Worker Assemblies at OpenText.WS.MS.ProcessServer.ProcessServer.InitializeAssemblies() at OpenText.WS.MS.ProcessServer.ProcessServer..ctor() at OpenText.WS.MS.XMLServer.MainService..cctor()*".

To fix the `processserver.main.config` configuration file, you have the following options:

1. Fix the `processserver.main.config` file manually.

2. Run `ConfigurationUtility.exe` again and select the **Reset all Configuration Files** option. This regenerates all (!) of Management Server's configuration files, so you must re-apply all individual changes you have made earlier.

3. Regenerate the `processerver.main.config` file manually:

   1. Delete the existing `processerver.main.config` file.

   2. Copy the `processerver.main.config.sample` file and rename the copy to `processerver.main.config`.

   3. Open the new `processerver.main.config` file in an editor and replace `<%cmspath%>` with the installation path of Management Server. The default installation path is `c:\OpenText\WS\MS`.

Call for Management Server fails

.NET not configured correctly - If .NET was not configured correctly, you receive the following IIS error when browsing to `http://.../cms`:
Error 500.21 - Internal Server Error Handler "ScriptHandlerFactory" has a bad module "ManagedPipelineHandler" in its module list.
Run `aspnet_regiis.exe -i` from the .NET framework to configure it properly. For the required .NET Framework version, see the latest Management Server release notes.

Sign in to Management Server fails

- **Cluster Installation**

  If you install an additional server to your existing cluster, it should have the same build as those in the cluster or it will not be possible to sign in to the server. In this case, you will receive a warning message. For more information, see "Management Server clusters" on page 85.

- **Internet Explorer Security Settings for the Server**

If the increased security settings in Internet Explorer are activated on the server, they will prevent you from logging on to Management Server. Adjust the security settings if you want to call Management Server locally.

Project import fails

The project import or any other asynchronous task, for example publication or export, fails. A possible cause can be an outdated `processserver.main.config` file. To fix this problem, proceed as follows:

1. Stop the `OpenText.WSM.NavigationService` service.

2. Rerun the `ConfigurationUtility.exe` with the option **Reset all configuration files** selected.

Session loss problems in Template Editor

If you experience session loss problems in the Template Editor, check the following:

- The ASP.NET State Service should have been started.

- The following code line should be present in the `\MS\ASP\web.config` file:

```
<configuration>
<system.web>
<sessionState mode="StateServer"
stateConnectionString="tcpip=127.0.0.1:42424" timeout="70" />
<httpRuntime requestValidationMode="2.0" />
 (…)
```

If this is not the case, proceed as follows:

1. In the `\MS\ASP\web.config` file, enter the above stated code line at the beginning of the

   ```
   <system.web>
   ```

   section.

   > **!** **Important**
   > The timeout that is set for ASP.NET State Service in the `web.config` files on every Management Server should have the same value as the **Session timeout** value in the application server settings.

2. Set the **Startup type** of the ASP.NET State Service to `Automatic` and start the service.

2.6   Upgrading to Management Server 16 from Management Server 10.1 SP2

You can only upgrade to Management Server 16 from Management Server 10.1 SP2. For older versions of Management Server, you must perform an upgrade to Management Server 10.1 SP2 first, before you can further upgrade to Management Server 16. For more information, see the Management Server 10.1 SP2 installation guide.

The upgrade procedure to Management Server 16 consists of an installation of Management Server 16 with an existing Management Server 10.1 SP2 administration database.

> **Notes**
>
> - Before exchanging a server, back up project relevant data like file folders or local databases if they exist on the server.
>
> - Note that after performing the upgrade to Management Server 16, you can delete the old language database *ioapplication*.

To upgrade a single server:

1.   Uninstall Management Server 10.1 SP2 or replace the server.

2.   In the IIS Manager, remove the CMS web application.

3.   Start the Management Server 16 installer and connect to the existing databases.

4.   Reboot the server.

5.   Perform the configuration and run the *Configuration Utility*.

6.   After you have finished the previous steps, open a browser and start Management Server 16.

To upgrade a Management Server cluster from version 10.1 SP2 to version 16:

1.   Perform the following steps consecutively with all servers:

   a.   Disable the connection to the administration database temporarily, for example by taking the administration database offline or by stopping the database server. In this way, the Management Server cluster server is not removed from the administration database when uninstalling Management Server 10.1 SP2.

   b.   Uninstall Management Server 10.1 SP2 or replace the server.

   c.   In the **IIS Manager**, remove the CMS web application.

   d.   Enable the database connection.

2.   Install Management Server 16 on the central server and connect to the existing databases. Reboot the server after finishing the installation.

3. Consecutively install Management Server 16 on all cluster nodes and connect to the existing databases.

You can follow either the standard installation procedure or perform a unattended console installation.

2.6.1 Following the standard installation procedure

2.6.1.1 Removing Management Server 10.1 SP2

Before you remove the existing installation, retain the following information:

- User name and password of initial Management Server administrator.

- User name and password of the Windows user running web services in Management Server.

- Database connection for the administration database. You can find the required information in the `%rdcms%\rdserver.ini` file in the `Administration` section:

  - When using a *MSSQL* database: Host name, port, instance name, database/ initial catalog, user name and password.

  - When using an *Oracle* database: TNS name, schema, password.

To remove Management Server 10.1 SP2:

1. Go to **Start** > **Control Panel** > **Add or Remove Programs**.

2. Proceed as described in "Removing Management Server" on page 103 for Management Server 10.1 SP2.

3. After the removal process has finished, perform the following steps:

   - Remove the environment variable `%rdcms%`.

   - Before deleting the folders below, save your configuration files to keep the old settings for later reference.

   - Delete the parent directory of `%rdcms%` and all subitems.

   - In the IIS Manager, remove the *CMS* web application.

2.6.1.2   Starting the Management Server 16 installer

Proceed as follows:

- Start the installer as described in "Start the installer package" on page 21.

2.6.1.3   Performing the configuration

Proceed as follows:

1. Perform the configuration as described in "Start the configuration" on page 28.

   Note the following:

   - Enter your license key. Note that you need a special cluster license if you upgrade a cluster node.

   - Configure your MSSQL or Oracle connection according to your existing system settings.

   - Configure the administration database settings to reference the correct database connection and connect to the correct database/scheme.

   - During an upgrade, you cannot import projects. To import projects, use the **Server Manager** dialog boxes in Management Server.

2.6.2   Performing the unattended console installation

2.6.2.1   Removing Management Server 10.1 SP2

Proceed as described in "Removing Management Server 10.1 SP2" on page 49.

2.6.2.2   Starting Management Server 16 installer

Proceed as follows:

1. Perform the unattended console installation principally as described in "Unattended console installation" on page 67.

2.6.2.3   Performing the configuration

Principally, perform the configuration as described in "Editing the configuration file" on page 67 and "Running the unattended console installation" on page 71.

When you edit the configuration file, note the following:

- In the `<ManagementServer>` element, remove the `Username` and `Password` attributes. For an upgrade, the login data of the Management Server administrator are not required. Enter your license key in the `LicenseKey` attribute. Note that you need a special cluster license if you upgrade a cluster node.

- In the `<MSSQL_Connections>` or `<Oracle_Connections>` section, respectively, configure your database connection according to your existing system settings.

- In the `<AdministrationDatabase>` element, set the `SetupType` to the following:

  - *UpdateAdministration* - if you want to reconnect and update the administration database of an old version.

  - *ClusterNode* - if you want to upgrade a cluster node.

- Configure the administration database settings in the`<MSSQL_Data Connection>` or `<Oracle_Data Connection>` element respectively, to reference the correct database connection and connect to the correct database/scheme.

- During an upgrade, project import is not supported.

2.7 Configuring Management Server after the installation

After completing the installation, there are a number of mandatory configurations that you must perform. You may also perform some optional configurations. The following sections provide an overview of what you can configure before you start working with Management Server as well as options to improve Management Server performance.

2.7.1 Protecting Management Server installations from search engines

OpenText strongly recommends that you ensure your Management Server installation cannot be found by search engines. To achieve this, you can configure the web server using a `robots.txt` file that prevents Web Spiders from indexing the Management Server pages. This `robots.txt` file is a text file that is always located in your web server's root directory. You can create a new `robots.txt` file or enhance the existing file content with the following entries that may be used for a default installation:

```
# Disallow all robots to spider OpenText Web Site Management Server
User-agent: *
Disallow:/cms
```

> **Note:** If you have chosen to install the optional modules **Mobile Client** and **Device Preview**, OpenText recommends to protect their directories as well.

You can find more detailed information on the following Web page: http://support.microsoft.com/?scid=kb%3Ben-us%3B217103&x=&y17=12%29

2.7.2   Defining ASP and ASP.NET settings

2.7.2.1   ASP.NET settings

Changing the Request Timeout Values

File uploads in Management Server use, by default, the request timeout (*executionTimeout*) and maximum request length (*maxRequestLength*) parameters that are configured for ASPX in the `web.config` file in `<Management Server installation directory>\Web\WebClient`. During the Management Server installation, the following section is added to the `web.config` file:

```
<location path="UploadHandler.ashx" allowOverride="false">

<system.web>
<httpRuntime executionTimeout="600" maxRequestLength="2097151" />

 </system.web>
 </location>
```

You can change these values manually in the `web.config` file.

The following list shows the parameters and the default values that are set during the installation:

executionTimeout
Maximum number of seconds that a request is allowed to run before being automatically shut down by ASP.NET. Default value after installation: 600 seconds.

maxRequestLength
Limit for the input stream buffering threshold in KB, to be used to prevent denial-of-service attacks. Default value after installation: 2097151 KB.

For more information about these parameters, see http://msdn.microsoft.com/en-us/library/e1f13641.aspx.

IIS restrictions when uploading large files

By default, Internet Information Services (IIS) prohibits uploading files that are larger than 28.6 MB. If you need to upload larger files, you can add the following to the existing `system.webServer` section in the `web.config` file in the *<Management Server install_dir>*\WebClient\Web folder:

```
<system.webServer>
  <security>
    <requestFiltering>
      <requestLimits maxAllowedContentLength="2000000000"/>
    </requestFiltering>
  </security>
</system.webServer>
```

> **Note:** The value of the *maxAllowedContentLength* parameter is set in Bytes. The default value is 30000000 (28.6 MB). Setting the value to 2000000000 allows file sizes up to 1.86265 GB.

2.7.2.2 ASP settings

The length of the request that a web browser can send to the IIS is limited in the IIS ASP settings. The default parameter might lead to problems saving large texts or templates. If problems occur, change the parameter **`Maximum Requesting Entity Body Limit`** in **ASP/Limits Properties** manually. Note that this parameter will be set back to default with every Management Server update.

> **Note:** The Management Server installation sets the parameter `Response Buffering Limit` in the IIS ASP settings (**ASP/Limits Properties**) to its maximum value = 2 GB.

2.7.3 Activating repository integrations

For security reasons, repository integrations need to be activated in the configuration file `%RDCMS%\..\Configuration\validate.xml`. For current integrations, the configuration file will be updated when installing the integration.

Depending on the setting of the option for overwriting configuration files, the Management Server setup process overwrites existing `validate.xml` files. In these cases, the software installation of the integration needs to be repaired.

2.7.4 Using the preconfigured PreExecute Application pool

When Management Server is installed, a separate application pool and an application for PreExecute are created to prevent Management Server from stopping when script errors that are based on scripts defined in Active Templates occur. To use this preconfigured application, change the settings for **Physical path** and **IIS Application** in the general settings of your Management Server projectas follows:

- **Physical path**: *`<Management Server install_dir>`*`\Web\PreExecute`
- **IIS Application**: `/PreExecute`

If you want to use your own settings for the application pool and application, OpenText recommends that you create a new application pool and application instead of editing the preconfigured ones.

2.7.5 Configuring database connection pooling

Depending on your configurations, changing the database connection pool settings can increase the performance of Management Server.
Connection pooling can be configured by adapting the database connection string. During the installation, the connection string can be adapted in the `ConfigurationUtility.exe.config` file before running the Configuration Utility. For existing configurations, you find the connection string for the administration database in the configuration `rdserver.ini` file.

The connection string template that is used for new database connections is stored in the administration database in the `IO_PRD` table with each database connection type

in the `PRD3` field. The connection string for each project connection is stored in the administration database in the `IO_PRJ` table in the `PRJ19` field in each project's row.

To adjust database connections, you can adapt the respective database connection string for Management Server and Management Server projects as follows:

RDServer.ini

For existing configurations of Management Server, change the `[Administration]` section for the respective database in the `RDServer.ini` file in *<Management Server_installdir>*\ASP.

Example: The following sample data creates an SQL database connection pool with a minimum number of 10 and a maximum of 400 connections, and a connection timeout of 60 seconds:

```
Provider="sqloledb";Data Source="%datasource%";Initial
Catalog="%databasename%";User Id="%username%";Password="%password
%";Min Pool Size="10";Max Pool Size="400";Connection
Lifetime="60";Pooling="true";
```

Configuration utility

During the installation, adapt the connection string by editing the `ConnectionStringTemplate` attribute in the `ConfigurationUtility.exe.config` file before you run the Configuration Utility. See "Editing the configuration file" on page 67 for more information.

Example: The following sample data creates an SQL database connection pool with a minimum number of 10 and a maximum of 400 connections, and a connection timeout of 60 seconds:

```
Provider=&quot;sqloledb&quot;;Data Source=&quot;%datasource
%&quot;;Initial Catalog=&quot;%databasename%&quot;;User Id=&quot;
%username%&quot;;Password=&quot;%password%&quot;;Min Pool Size=&quot;
10&quot;;Max Pool Size=&quot;400&quot;;Connection Lifetime=&quot;
60&quot;;Pooling=&quot;true&quot;;
```

Project databases

For the project databases, you must add a new database access mode that you must use when you define a new database server. For more information about database access modes, see section 6.2 "Administering database access modes" in *OpenText Web Site Management Server - Server Manager Guide (WSMSSM-AGD)*. The connection string can be edited and the necessary settings can be added.

Example: The following entries show sample data for a Provider Template that you can use to adapt an SQL Server connection string:

```
Provder="SQLOLEDB";
Data Source="<%Server|text%>";
Initial Catalog="<%Database|database%>";
User Id="<%Username|text%>";
```

```
Password="<%Password|password%>";
Min Pool Size="<%Minimum number of connections in connection pool|
text%>";
Max Pool Size="<%Maximum number of connections in connection pool|
text%>";
Connection Lifetime="<%Connection lifetime(s)|text%>";
Pooling="true";
```

2.7.6 Editing the default services settings

Management Server runs with a set of the following services:

- OpenText WebClient Service: Provides the functionalities for the ASP.NET client and runs the OpenText.WS.MS.ClientService.exe process. The configuration file is `OpenText.WS.MS.ClientService.exe.config`.

- OpenText Navigation Service: Responsible for processing render tags for the navigation and cluster communications. Transmits the Data for the Object Process Service and runs the OpenText.WS.MS.DataService.exe process. The service runs the OpenText.WS.MS.ObjectProcessService.exe and OpenText.WS.MS.ObjectService.exe processes. The Object Process Service process performs the tasks, and the Object Service process checks the status of the Object Process Service process. The configuration files are `OpenText.WS.MS. ObjectProcessService.exe.config` and `OpenText.WS.MS. ObjectService.exe.config`.

- OpenText Server Service: Responsible for Management Server-oriented functionalities, such as page building and Process Server and runs the OpenText.WS.MS.ServerService.exe process. The configuration file is `OpenText. WS.MS.ServerService.exe.config`.

The following sections describe the default settings that you can change in specific configuration files, for example, to improve Management Server performance.

Cleaning the page cache

The `<Management Server_installdir>`\ASP\main.config file contains by default a trigger for a page cache cleaning operation. The operation is triggered when the amount of memory used by the OpenText Server Service reaches the specified value. The amount of memory used is calculated based on more than just the page cache. Therefore, be aware that when you change the memory limit you are setting the amount of memory used for the page cache and for other processes that also use this memory. However, when the page cleaning operation is triggered, only the memory used by the page cache will be cleaned.

To adjust the memory limit according to your needs, change the default value for `<PageCacheMemoryThreshold>` in the `<PageBuilder>` element. The default memory setting is 2500 MB. In production environments, you must adjust this default setting based on the available physical memory and the caching behavior of projects that use this memory.

Changing thread settings

The `OpenText.WS.MS.ObjectProcessService.exe.config` file contains an `<appSettings>` element in which you can adjust the following key values that can influence the performance of Navigation Manager:

*   *RenderThreads*: Number of threads that are used to render `<next level />` in navigation templates. The default value is 25.

*   *ClusterThreads*: Number of threads that are used to work on cluster updates. The default value is 10. OpenText recommends that you have at least one cluster thread per node in the cluster. For example, a cluster of 12 nodes should at least have 12 cluster threads.

*   *CacheMemory*: Defines how much space is used for items held in cache. The default memory size is 2500 MB. As soon as the specified limit is reached, items are deleted from the cache. The percentage of items that are deleted is defined in *CacheRelease*.

*   *CacheRelease*: Specifies the percentage of items that are deleted from the cache as soon as the cache memory specified in *CacheMemory* is exceeded. The default value is 30.

2.7.7   Configuring cross-site request forgery protection

Management Server provides a mechanism to prevent cross-site request forgery (XSRF).

For plug-ins or external applications that use hyperlinks to the Management Server user interface, you can selectively disable the XSRF protection.

Protection

The protection verifies that each HTTP request that reaches the web server, except for requests for the logon dialog box, originates from within the Management Server user interface.

If the protection detects a malicious request, it responds with an HTTP "403 Forbidden" status code. Any such event is also written to the log file, with:

*   Component: Network

*   Category: System/Security

*   Severity: Error

The log message contains the request URL and the origin of the request that triggered the protection mechanism. You can use this information to disable the protection for similar requests by adding them to a whitelist.

Configuration

The `<Management Server_installdir>`\ASP\main.config file contains a configuration section for disabling XSRF protection for specified requests. The root element for the configuration is:

`<Configuration> / <Security> / <AntiCsrfModule> / <Whitelist>`

Requests can be whitelisted based on their request URL or based on their origin (HTTP referrer). Make sure that an attacker is in no way able to place hyperlinks to Management Server or even arbitrary HTML code on any of the web server's pages.

Whitelisting request URLs

To whitelist a URL:

- Add a `<PathAndQuery>` element as a child to the `<Whitelist>` `<Request>` element.

The element's inner text should be a `.NET` style regular expression that, when applied to the path and query string part of the request URL, matches requests that should be whitelisted.

A specific placeholder `%BASE_VDIR%` represents the name of the virtual directory of Management Server in IIS (usually *cms*). Documentation for the `.NET` regular expression syntax can be found here: http://msdn.microsoft.com/library/az24scfc(v=vs.110).aspx

For sample whitelist items, see the default `main.config` file.

Whitelisting request origins

To whitelist a server:

1. Add a `<TrustedReferrer>` element as a child to the `<Whitelist>` `<Referrer>` element.

2. In this element, use one or both of the following elements:

   <Authority>
   Contains, as inner text, a `.NET` style regular expression that must match the host name and port section of the HTTP referrer URL, for example, the URL of the page from which the request came.

   <PathAndQuery>
   Contains, as inner text, a `.NET` style regular expression that must match the path and query part of the URL, similar to the `<PathAndQuery>` element for whitelisting request URLs.

   Each element that is used must match for the origin to be whitelisted. For sample whitelist items, see the default `main.config` file.

Whitelisting assets in a PDF file and working links produced by a PDF variant

To support displaying assets in a PDF file and working links to following pages produced by a PDF project variant, you must add the following <PathAndQuery> elements to the `main.config` file.

To whitelist working assets in a PDF file:

• Add the following <PathAndQuery> element as a child to the <Whitelist> element:

    <PathAndQuery>^/%BASE_VDIR%/ImageCache/.*</PathAndQuery>

To whitelist working links produced by a PDF variant:

• Add the following <PathAndQuery> element as a child to the <Whitelist> element:

    <PathAndQuery>^/%BASE_VDIR%/WebClient/PreviewHandler\.ashx\?
    Action=Preview</PathAndQuery>

📋   **Adding regular expressions**

When adding regular expressions to the configuration file, keep in mind that the file is in XML. If you want to use characters such as "&" in your expression, you must write it as an XML entity in order not to break the well-formedness of the file.

2.7.8   Configuring redirect validation

Management Server provides a mechanism to validate redirects.

Protection

The protection verifies that redirects to external resources are validated against a configurable whitelist.

If the protection detects an invalid redirect, the operation will be aborted. Any such event is also written to the log file, with:

• Component: Network

• Category: System/Security

• Severity: Error

The log message contains the request URL.

Configuration

The *<Management Server_installdir>*\ASP\main.config file contains a configuration section to control the mechanism. The root element for the configuration is:

```
<Configuration> / <Security> / <OpenRedirect> / <Whitelist>
```

Redirects can be whitelisted based on their request URL.

Whitelisting redirect URLs

To whitelist a URL:

1. Add a `<Request>` element as a child to the `<Whitelist>` element.

2. In this element, use one or both of the following elements:

    <Authority>
    Contains, as inner text, a `.NET` style regular expression that must match the host name and port section of the redirect URL.

    <PathAndQuery>
    Contains, as inner text, a `.NET` style regular expression that must match the path and query part of the URL. A specific placeholder `%BASE_VDIR%` represents the name of the virtual directory of Management Server in IIS (usually *cms*). Documentation for the `.NET` regular expression syntax can be found here:http://msdn.microsoft.com/library/az24scfc(v=vs.110).aspx

Example 2-1: Whitelist for redirect URL

```
<Url>
   <Authority>^cmstest.opentext.net</Authority>
   <PathAndQuery>^/%BASE_VDIR%.*</PathAndQuery>
 </Url>
 <Url>
   <Authority>^cmstest.opentext.net</Authority>
   <PathAndQuery>^/%MOBILECLIENT_VDIR%.*</PathAndQuery>
 </Url>
 <Url>
   <Authority>^cmstest.opentext.net</Authority>
   <PathAndQuery>^/%DEVICEPREVIEW_VDIR%.*</PathAndQuery>
 </Url>
```

2.7.9   Configuring path manipulation protection

Management Server provides a mechanism to prevent unauthorized access to the local file system.

Protection

The protection verifies that each access to the local file system is validated against a configurable whitelist.

If the protection detects an invalid file access, the related operation will be aborted. Any such event is also written to the log file, with:

- Component: Core
- Category: System/Security
- Severity: Error

The log message contains the requested file system path and the type that describes what kind of data should be accessed by the operation.

Configuration

The *`<Management Server_installdir>`*`\ASP\main.config` file contains a configuration section to control the mechanism. The root element for the configuration is:

`<Configuration> / <Security> / <PathManipulation> / <Whitelist>`

By default, the protection mechanism is disabled. The whitelist contains a single entry that will match each requested path. The access to the local file system can be whitelisted based on the requested file path and type.

Whitelisting

To whitelist a file system path:

- Add a `<Path>` element as a child to the `<Whitelist>` element.

  The element's inner text should be a `.NET` style regular expression that, when applied to the file path, matches requests that should be whitelisted. Documentation for the `.NET` regular expression syntax can be found here: http://msdn.microsoft.com/library/az24scfc(v=vs.110).aspx

Each module must be able to access only the information and resources necessary to its legitimate purpose. Therefore, each whitelist entry must provide information about the type of data that should be accessed. Management Server provides the following set of configurable types:

Default
   Used to whitelist all kind of file access.

Assets
Used to access asset relevant data, for example a file in a file system folder.

Archive
Used to control file access to archive relevant data.

Browse
Used to control file access for the file browse dialog.

Integrations
Used to control access for dynamically loaded integration assemblies.

MSWordDataTemp
Used to access temporary WordEditor WebDAV files.

Navigation
Used to access navigation relevant data.

PageExport
Used to access export relevant data.

PageImport
Used to access import relevant data.

PdfConversion
Used to access pdf conversion relevant data.

ProjectExport
Used to access export relevant data.

ProjectImport
Used to access import relevant data.

Publishing
Used to access publishing relevant data.

PublishingLog
Used to access log data in the context of the Publisher module.

RdExecute
Used to access Rd-/PreExecute relevant data.

Staging
Used to control file access to staging relevant data.

Tidy
Used to to access Tidy relevant data.

TidyConfig
Used to control file access to the Tidy configuration files.

Workflow
Used to control worklow relevant data, for example, when a workflow reaction writes an XML file to the local file system.

Internally, Management Server also uses some system relevant types that usually do not need to be configured.

To whitelist file access to assets:

- Add the following `<Path>` element as a child to the `<Whitelist>` element:
  `<Path type="Assets">^C:\\data\\myassets</Path>`

When Management Server tries to access an asset that is stored in the local file system, the requested path will be validated by evaluating each whitelist entry with `Default` or `Assets` type.

2.7.10 Configuring HTTPOnly cookies

By default, Management Server adds an *HTTPOnly* flag in the HTTP response header of all cookies. With the flag included, a cookie cannot be accessed through client-side script.

If applications that run from inside the `/cms` folder, such as plug-ins and custom integrations, require access to cookies from script code, you must exclude them from the mechanism that sets the HTTPOnly flag.

To disable the HTTPOnly cookie configuration selectively for subfolders of the `/cms` folder, edit the existing `web.config` file or add a new `web.config` file to the subfolder.

To disable the HTTPOnly cookie configuration for certain subfolders:

- Add the following element to the `web.config` file:

```
<configuration>

  <system.webServer>

    <modules>

      <remove name="CookieModule"/>

    </modules>

  </system.webServer>

</configuration>
```

You can also disable the HTTPOnly cookie configuration for certain cookies. You add a section to the `main.config` file and list the names of the cookies you want to exclude from the setting of the HTTPOnly flag.

To disable the HTTPOnly cookie configuration for certain cookies:

1. Open the *`<Management Server_installdir>`*`\ASP\main.config` file in an editor.

2. Add the following section to the file:

```
<AvailableToScript>
  <Cookie>NAME OF COOKIE #1</Cookie>
  <Cookie>NAME OF COOKIE #2</Cookie>
  <!-- etc. -->
</AvailableToScript>
```

3. Enter the name of your cookie in the `<Cookie>` section. Note that cookie names are case sensitive.
   List all cookies you want to include in the `<AvailableToScript>` section.

4. You must restart the IIS web server for this setting to take effect.

2.7.11 Configuring Asset processing for Asset folder

The Asset folder uses the Imagenation library, an Open Text technology, to extract metadata from document-type assets like PDF or MS Word.

Process

The process to host and execute the Imagenation library is `OpenText.WS.MS. Imagenation.Sandbox.exe`. Some notes on its lifecycle:

- The process is spawned on-demand, for example, with the first user upload after a restart and will then run permanently.

- If it terminates, for example, due to a bug in the Imagenation library, it is restarted automatically by Management Server.

- It will terminate as soon as the Management Server core process (`ServerService.exe`) has shut down.

Configuration

The `main.config` configuration file contains the following elements below the `<AssetProcessing>` element:

- `<SandboxPort>`: This is a TCP port, bound to localhost only, that is used for interprocess communication between the core Management Server process (`ServerService.exe`) and the Imagenation sandbox process. The default value is 5556.

- `<SandboxMaxThreads>`: Maximum number of threads spawned within the sandbox process to support parallel metadata extraction. Parallel metadata extraction improves performance especially in scenarios with a lot of metadata extraction requests, for example, when converting an Asset Manager folder with a lot of contained assets. The default value is 5.

- `<Timeout>`: Time limit in milliseconds for the maximal waiting period for reading metadata or creating a thumbnail for an asset file. The default value is 10000.

2.7.12   Configuring the OpenText™ Global Help Server connection

By default, Management Server calls the online help on the Global Help Server using the HTTPS protocol. You can use the HTTP protocol instead.

To configure Management Server to use HTTP to connect to the Global Help Server:

1.   In Management Server, go to the `<Management Server_installdir>`\ASP\ `main.config` file.

2.   Go to the `<HostedHelp>` element, and in the `<UrlAddress>` element change the protocol to `http`:

```
<HostedHelp>
   <!-- Hosted help authority and path 'https://
docsapiqa.opentext.com/mapperpi' -->
   <UrlAddress>http://docsapi.opentext.com/mapperpi</UrlAddress>
</HostedHelp>
```

📑   **Note:** Do not change the following additional online help parameters:

- `<Tenant>`: A special online help system identifier supplied by OpenText. Do not specify or change a value unless directed by OpenText.

- `<Type>`: Identifies the OpenText online help type. Do not specify or change a value unless directed by OpenText. If you supply an unsupported value, you can cause the online help system to stop working.

2.8   Accessing RQL web services

The Management Server RQL web services are based on Microsoft Windows Communication Foundation and do no longer use the Microsoft SOAP Toolkit 3.0. Note the following:

- To access the web service through the old URL, you must install the IIS Rewrite Module, see http://www.iis.net/download/URLRewrite. The installation inserts an out-commented entry in the `%RDCMS%\..\Web\WebService\web.config` file. Uncomment the section to make the web service available through the old URL.

- For new implementations, or if you can easily change the access URL in your plug ins, integrations, or products, use the following URL: *http://localhost/CMS/WebService/RqlWebService.svc*.

You have two possibilities to create a client for the RQL Web Service:

- Add a service reference to your Visual Studio 2010 project.

- Create a Web Services client by utilizing the *svcutil*.

To create a web service client, see the *MSDN* or *Solution Exchange* (http://www.solutionexchange.info) for more information.

Chapter 3

Unattended console installation

For Management Server installations you can perform an unattended console installation. An unattended console installation requires practically no user interaction and does not display any indication of its progress.

You must be able to provide the following to meet the requirements:

- *installingAdministrator* user: server logon with local administrator rights.

- Permanent IP address for the server.

- Management Server license key.

As with the standard installation, the unattended console installation consists of the *installation* and the *configuration* part. For the installation part, you need to add the required installation settings as parameters to the `msiexec` command, see "Installation parameters" on page 67. For the configuration part, you must edit the configuration file beforehand, see "Editing the configuration file" on page 67. This configuration file can be stored and reused, for example, for multiple installations.

3.1 Installation parameters

You can add the following parameter to the `msiexec` command:

TARGETDIR
   Installation directory. Default value: `C:\OpenText\WS\MS`.

3.2 Editing the configuration file

Before you can start the Configuration Utility, you must edit the necessary configuration settings in the configuration file. The Configuration Utility uses this file to perform the configuration. Principally, the settings are the same ones that you enter in the GUI during the standard installation and configuration, see "Start the configuration" on page 28.

   Tip: Remove the respective attribute from the XML file to use the default value for a setting.

Proceed as follows:

1. In the `<installation directory>:\OpenText\WS\MS\ ConfigurationUtility` folder, copy the `ConfigurationUtility. exe.config.sample` file and rename the copy to `ConfigurationUtility. exe.config`.

2. Open `ConfigurationUtility.exe.config` in an editor and edit the following settings:

    - `<ManagementServer Username="admin" Password="" ConnectionName=""` `HostHeader="" ClusterUrl="" IsSecureInstallation="true"` `LicenseKey="" SpellcheckingHost="spell.reddot.de"` `ServiceUserName="" ServiceUserPassword="" AppPoolUserName=""` `AppPoolUserPassword="" DomainPort="">`

      If you do not want to use the default name, edit the user name of the initial Management Server administrator and insert a password.

      Insert the values for the connection name, host header and cluster URL. Note that these settings are not editable anymore in Server Manager. To change them, you must run the Configuration Utility again. For more details, see "Configure Server Settings and SSL" on page 39.

      If you do not want to use secure connection, change the value for `IsSecureInstallation` to `false`. Per default, the value is set to `true`.

      Insert your license key and the host name of the spell checker server. The entries for license key and password are mandatory. The passwords will be encrypted by the Configuration Utility.

      Insert service user name, service user password, application pool user name, and application pool user password.

      The `DomainPort` attribute is used to validate the domain user credentials against the domain controller. In most cases the internal evaluated port should work, so that it should not be necessary to configure a value. For more information, see "Specify the Services user" on page 30.

    - `<MSSQL_Connections>` `<add Name="My_MSSQL_Connection" Datasource="localhost"` `AuthenticationMode="Windows">` `<WindowsAuthentication` `ConnectionStringTemplate="Provider="sqloledb";Data` `Source="%datasource%";Initial Catalog="%databasename%";` `Trusted_Connection=yes;"/>` `<ServerAuthentication Username="sa" Password="sa"` `ConnectionStringTemplate="Provider="sqloledb";Data` `Source="%datasource%";Initial Catalog="%databasename%";User` `Id="%username%";Password="%password%";"/>` `</add>`

      If you want to use Management Server with an MSSQL database, edit the necessary settings in this section. You can select either Windows or server authentication by setting the corresponding value `Windows` or `Server` for the attribute `AuthenticationMode`.
      The `Name` must be unique for your database connection list, including the list of Oracle databases. In the attribute `ConnectionStringTemplate`, you can edit the settings for the connection pool.

> **!** **For Windows authentication**
>
> Ensure that the `<WindowsAuthentication ConnectionStringTemplate>` attribute value contains the expression `"Trusted_Connection=yes"` exactly as stated. Do not change the attribute or its value.

- `<Oracle_Connections>`
  `<add Name="My_Oracle_Connection" TNSName=""`
  `ConnectionStringTemplate="Provider=ORAOLEDB.ORACLE;Data Source=`
  `%tnsname%;User Id=%schema%;Password=%password%;prompt=noprompt;`
  `"/>`

  If you want to use Management Server with an Oracle database, edit the necessary settings in this section. The `Name` must be unique for your database connection list, including the list of MSSQL databases. The entry for the `TNSName` is mandatory. In the attribute `ConnectionStringTemplate`, you can edit settings for the connection pool. Note that editing of this attribute should be performed only by experts.

- `<IisSettings Hostname="localhost" WebSiteName="Default Web Site"`
  `VirtualDirectory="CMS" Port="443"/>`

  This section contains the IIS settings for Management Server. The attribute `Hostname` defines the NetBIOS name (15 characters) or the IPv4 address of the current host.

  > **!** **Important**
  >
  > Do not change the attributes `Port`, `WebSiteName` and `VirtualDirectory`. These attributes are auto-generated by the installer.

- `<AdministrationDatabase SetupType="CreateAdministration"`
  `DatabaseType="MSSQL">`

  In this element, edit the settings for the Administration Database of your Management Server. You can set the `DatabaseType` either to *MSSQL* (default) or *Oracle*. Set the appropriate `SetupType` according to the task that you want to perform:

  - *CreateAdministration* – if you want to create a new Administration Database, for example, to set up a database server for a new main cluster server or a new standalone installation.

  - *UpdateAdministration* – if you want to reconnect and update the Administration Database of an old version.

  - *ClusterNode* – if you want to update a cluster node or connect a new computer to an existing cluster.

- `<MSSQL_Data Connection="My_MSSQL_Connection"`
  `Databasename="ioAdministration"/>`

  In this element, insert the settings for your Administration database, if you choose to use a MSSQL database.

`MSSQL_Data Connection` references the MSSQL connection that you have defined earlier. Insert the same value that you have already provided in the `<MSSQL_Connections>` element as `Name`, see above.
`Databasename` defines the name for the administrative database that will be created by Management Server. You can change the default value and choose a name for the database, if you want to create a new database. If you want to update an existing Administration database, we recommend that you keep the existing database name.

- `<Oracle_Data Connection="My_Oracle_Connection" Schema="ioAdministration" Password=""/>`

In this element, insert the settings for your Administration database if you chose to use an Oracle database.
`Oracle_Data Connection` references the Oracle connection that you have defined earlier. Insert the same value that you have already provided in the `<Oracle_Connections>` element as `Name`, see above.
`Databasename` defines the name for the administrative database that will be created by Management Server. You can change the default value and choose a name for the database, if you want to create a new database. If you want to update an existing Administration database, we recommend that you keep the existing database name. The entry of a password is mandatory.

- `<ImportProjects><MSSQL><add Connection="My_MSSQL_Connection" SourcePath="Xample" Name="Xample Project" Databasename="XampleProject"/>`

In this section, you can list the projects that you want to import in Management Server using a MSSQL database.
To import a project, insert for `Connection` the same value that you have already provided in the `<MSSQL_Connections>` element as `Name`, see above. As `SourcePath` enter the path to the project that you want to import. You can find projects exported by Management Server in the *`<install_dir>`* `\OpenText\WS\MS\share\projects` folder. You can enter the project name as value for `SourcePath` if the project exists in this folder.
Choose a `Name` and `Databasename` for your project.
When you install a new cluster node and chose the *ClusterNode* `SetupType`, the Xample project is not imported. If you do not want to import any project at all, leave all attributes empty.

- `<ImportProjects><Oracle><add Connection="My_Oracle_Connection" SourcePath="Xample" Name="Xample Project" Schema="XampleProject" Password=""/>`

In this section, you can list the projects that you want to import in Management Server using an Oracle database. You can add as many entries as you want.

To import a project, insert for `Connection` the same value that you have already provided in the `<Oracle_Connections>` element as `Name`, see above. As `SourcePath` enter the path to the project that you want to import. You can find projects exported by Management Server in the `<install_dir>` `\OpenText\WS\MS\share\projects` folder. You can enter the project name as value `SourcePath` if the project exists in this folder.

Choose a `Name` and `Databasename` for your project.

For `Schema`, insert the name of the project administrative database. This schema must already exist beforehand.

`Name` defines the project name shown in the Management Server UI.

Insert a `Password` for authentication against the schema.

When you install a new cluster node and chose the *ClusterNode* `SetupType`, the Xample project is not imported.

If you do not want to import a project at all, leave all attributes empty.

- `<log4net>`
  In this section, the logging for the configuration part is configured. You can set the `level value` to ERROR or DEBUG during configuration.

For more information, see the commented sections in the configuration file.

> **! Important**
> After installation, store the configuration file in a safe place to protect your data.

3.3 Running the unattended console installation

The unattended console installation consists of an installation and a configuration part.

> **Notes**
>
> - **Creating installation log files**
>
>   Per default, no log files are created during installation. If you want to create a log file, add the following parameters to the `msiexec` command:
>   `msiexec /l*v <LogfileName> /i <MSIName>.msi`
>   For example:
>   *msiexec /l*v install.log /i OpenText.WS.MS.Installation.msi*
>
> - Do not abort the configuration. Some configuration settings, as for example newly created databases, will not be reset automatically.

To run the unattended console installation:

1. Open a command prompt with administrative rights.

2. Change to the directory where you have deployed the installer package.

3. Enter `msiexec` and add the necessary parameters. For the unattended console installation, you must add the parameter `/qn`.

    For example:

    ```
    msiexec /qn /i OpenText.WS.MS.Installation.msi /l*v install.log
    TARGETDIR="C:\TP"
    ```

4. When the installation process is finished, open a new command prompt with administrative rights and enter `cd %rdcms%\..\ConfigurationUtility` to change to the *Configuration Utility* folder in the installation directory. Copy the configuration file to this folder.

5. Edit the configuration file as described in "Editing the configuration file" on page 67.

6. Run `ConfigurationUtility.exe`.

7. After the configuration process has been finished, open a browser and enter `https://<server name>.<domain name>/cms` to start Management Server.

Chapter 4

Oracle as Management Server database

4.1 About this chapter

This section describes the activities you have to perform if you plan to use an Oracle database for storing Management Server data. It is therefore intended primarily for Oracle and Windows administrators.

You will first learn about the preparatory activities that you have to perform before you install Management Server. This is followed by an overview of the activities you perform during Management Server operation.

Precise knowledge of Oracle administration is required to configure and use an Oracle database. In particular, this involves installing the Oracle server and client, preparing database instances, and establishing a database connection between Management Server and the Oracle database.

For more information, see the Oracle documentation.

4.2 Data storage with Oracle

If you use Oracle, Management Server accesses different schemas of a single Oracle database rather than multiple databases. Database schemas are defined in Oracle by creating users. Accordingly, the schema name and user name are identical.

Data storage for Management Server is based on two schemas for system data and one schema for a first project. You create another schema (or user) for each additional project.

The archive data from a Management Server project is saved in the schema for the respective project. As such, only one schema is necessary for each project. A different user accesses each schema.

The Oracle administrator does not have to perform any activities on the database during Management Server operation. Management Server administers the schema objects itself. Where necessary, you can create schema objects yourself by running the appropriate script.

4.3   System requirements

Note the system requirements described below for using Oracle databases with Management Server.

4.3.1   Client software

When using Oracle databases with Management Server, note the sections, "Before installing Management Server" on page 75 and "During operation..." on page 80.

Update   When you update a client software version, be sure to remove the previous client software completely and delete all the files. You then need to restart the server where the Oracle client is installed. We recommend running the *RegClean* program afterwards. The `tnsnames.ora` file can be reused after an update; you should back it up before removing.

4.3.2   Main memory

To ensure good performance, you must allocate sufficient main memory to the active Oracle database. The system does not allocate the memory automatically. Oracle reserves this memory when the database is set up. You cannot increase it at runtime.

Be sure to always use the latest initialization parameters for allocating the memory. Use the following initialization parameters:

- `sga_target`

- `pga_aggregate_target`

- `sort_area_size`
  Allocate at least 5 MB for this parameter.

Oracle docu-
mentation   For more information, see the Oracle documentation at http://www.oracle.com/technetwork/indexes/documentation/index.html.

4.3.3   Hard disk space

Due to the wide variety of different structures used in assorted Management Server projects, it is not possible to say how quickly the amount of required disk space will grow, nor in which places (tables).

Therefore, when you set up a Management Server project, make sure that enough disk space is available for the database files and that this space can actually be used. We recommend setting the growth forecast of the Oracle objects, Tablespace, Table, and LOB Segment, to *Unlimited growth*. If this is not possible, you will have to monitor the objects and issue an alert when the fill level reaches 90%. Data might be lost if the allocated memory space of an object is exceeded.

We recommend using locally managed tablespace with automatic growth. This passes the storage options on to the objects in the tablespace. Tables, indexes, and

LOB segments can then grow without limit in the tablespace. In this case, you only have to monitor the tablespace, not the objects themselves.

Use data storage in the file system for the folders in Management Server. Avoid saving binary files to prevent unnecessary growth and database load. In many projects with binary data storage in the database, the share of binary data can amount to 75% or more of total database space. Convert the folders for such projects to data storage in the file system.

4.4 Before installing Management Server

You have to perform the following preparatory tasks before you install Management Server:

- If it has not yet been installed: Install the Oracle server

- Create a suitable Oracle database or check the configuration of an existing database

- Create Oracle database schemas for Management Server

- Install the Oracle client software on the application server

- Configure the database connection between the Oracle client and the Oracle server

You can then begin installing Management Server. For more information, see "Installing Management Server" on page 9.

4.4.1 Installing the Oracle server

You install the Oracle server using the Oracle Universal Installer.

Note that the sample database created during the installation is not a suitable basis for a schema intended to record Management Server data. For more information, see "Creating the Oracle database" on page 75 and "Creating Oracle database schemas for Management Server" on page 76.

4.4.2 Creating the Oracle database

You can either use an existing Oracle database or use the Database Configuration Wizard to create a new one. In any case, the database must have the following settings for it to be used with Management Server:

- Application type: Online Transaction Processing (OLTP)

- Mode: Dedicated server mode

- Default database component: Oracle Text (for full-text search)

- Character sets: Must support Unicode (see details below)

- Tablespace (User): Automatic extension

4.4.3 Character sets for Unicode support

Select a Unicode-compliant character set for the database character set (NLS_CHARACTERSET) and the country-specific character set (NLS_NCHAR_CHARACTERSET) of the Oracle database.

- Database character set: AL32UTF8, AL16UTF16, UTF8, or UTFE

- Regional character set: AL16UTF16 or UTF8

For More Information: Oracle Database Globalization Support Guide/Supporting Multilingual Databases with Unicode

4.4.4 Creating Oracle database schemas for Management Server

You create three schemas (or users) in the Oracle database for Management Server data. Management Server data is saved in these user schemas. To do this, you have to assign a tablespace to these users. In addition, these users need specific roles and the associated permissions.

Schemas

The application server carries out numerous read/write operations on the schema depending on the number of users.

The **RDADMINISTRATION** schema contains all data pertaining to application servers, projects, users, groups, and other data. Read/write access is required during Management Server operation; the files are small (around 2-10 MB).

The **RDPROJEKT001** is used to set up the sample project. A project schema contains all information pertaining to a Management Server project. The size of a Management Server project can easily exceed 2 GB, however. The application server carries out numerous read/write operations on the schema depending on the number of users.

> 📄 **Note - Schema names**
>
> The names used here are only suggestions. You can assign other names if desired.
>
> You will need the names of the schemas and the corresponding passwords when you install Management Server.

Tablespace

The tablespace assigned to users should be sufficiently generous and also take potentially rapid data growth into account. For more information, see the notes in "Hard disk space" on page 74.

User roles

The necessary user roles are CONNECT, RESOURCE, and CTXAPP.

As an alternative to the RESOURCE role, you can also create a user-defined role under a different name. This role merely has to contain the following rights, which the RESOURCE role also possesses:

```
CREATE ROLE "REDDOTROLE" NOT IDENTIFIED;
GRANT CREATE CLUSTER TO "REDDOTROLE"
GRANT CREATE INDEXTYPE TO "REDDOTROLE"
GRANT CREATE OPERATOR TO "REDDOTROLE"
GRANT CREATE PROCEDURE TO "REDDOTROLE"
GRANT CREATE SEQUENCE TO "REDDOTROLE"
GRANT CREATE TABLE TO "REDDOTROLE"
GRANT CREATE TRIGGER TO "REDDOTROLE"
GRANT CREATE TYPE TO "REDDOTROLE"
```

If you cannot assign the RESOURCE role with the associated rights because, for example, of internal security guidelines, you need to set up various Management Server processes as the Oracle administrator. This includes installing, creating projects, copying projects, importing projects, and creating language variants.

The CTXAPP role is required for full-text searches and is only needed in the project schema.

Otherwise, Management Server administers all schema objects from the application, and the Oracle database administrator is not involved.

Example 4-1: How to create a schema/user

```
CREATE USER RDPROJECT001
IDENTIFIED BY password

DEFAULT TABLESPACE users
TEMPORARY TABLESPACE temp;

GRANT UNLIMITED TABLESPACE TO RDPROJECT001;
GRANT connect TO RDPROJECT001;
GRANT resource TO RDPROJECT001;
GRANT ctxapp TO RDPROJECT001;
```

Important - Creating new schemas for new projects

When you create or import a new project, you have to create a new schema or new user for each project in the Oracle database. Clearing an existing schema to reuse it for another project is not sufficient; instead, it results in an error message in Management Server and the process of creating or importing the project is canceled.

For more information: Oracle Documentation/Oracle9i Database Administrator's Guide/25 Managing User Privileges and Roles

4.4.5   Installing the Oracle client software

Management Server is delivered with an ODP.NET Managed Oracle Driver. It is neither required nor recommended to install the ODP.NET Oracle Client software manually. To proceed with the configuration, follow the steps in "Preparing database connections" on page 79.

Using an alternative ODP.NET Oracle Driver

If you want to use a different ODP.NET Oracle Driver, you can install other versions of the managed or unmanaged ODP.NET 64-bit driver. They are usually provided by Oracle as part of their Oracle Data Access Components (ODAC) software package. You must install the driver manually.

If you have obtained your driver from ODAC, you have the following options to make it available for use with Management Server:

- The environment variable `%ORACLE_HOME%` must be defined on the system. Install the driver in one of the following locations:

  - `%ORACLE_HOME%\ODP.NET\managed\common\Oracle.ManagedDataAccess.dll`

  - `%ORACLE_HOME%\ODP.NET\bin\4\Oracle.DataAccess.dll`

- Register the driver as an ADO.NET Data Provider.
  Usually, the necessary steps are executed automatically by the ODP.NET installer program:

  - the driver must be installed in the Global Assembly Cache

  - the driver must be referenced in `%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config` under `<configuration><system.data><DbProviderFactories>`.

Ensure that the Management Server Service User has at least `read` access to the Oracle driver.

Upgrading an alternative ODP.NET Oracle Driver

To upgrade the alternative ODP.NET Oracle Driver that you use, proceed as follows. Otherwise, Management Server will refuse to use the upgraded driver and will not start

To upgrade an ODP.NET Oracle Driver:

1. Run the configuration utility again.

2. In the **Database Type** dialog box, select the new driver.

3. In the **Other Settings** dialog box, select the **Overwrite configuration files** check box.

4.4.6 Preparing database connections

Management Server connects to the Oracle Database Server using TNS Names, which are defined in the `tnsnames.ora` configuration file. Management Server uses the system wide environment variables `Oracle_Home` and `TNS_ADMIN` to locate the `tnsnames.ora` configuration file in the file system. Ensure that at least one of them is set.

The expected location for `tnsnames.ora` is either the `%Oracle_Home%\network\admin` directory or alternatively `%TNS_ADMIN%`. Ensure that the Management Server Service User has at least `read` access to the `tnsnames.ora` configuration file.

Example: Assuming `Oracle_Home` is set to `C:\Oracle`. The `tnsnames.ora` configuration file is then expected in the file system at `C:\Oracle\network\admin\tnsnames.ora`.

Creating or editing the `tnsnames.ora` configuration file

We recommend to create or edit the configuration file using a text editor.

Example: The entry defines the TNS Name `MyTnsName` connecting to the Oracle Database Server on host `MyOracleDbHost` via Port `1521` using the server name `MyOracleDbServiceName`. This enables you to use `MyTnsName` as **TNS name** in the Configuration Utility in the **Management Server Connection (Oracle)** dialog.

```
MyTnsName =

  (DESCRIPTION =

    (ADDRESS = (PROTOCOL = TCP)(HOST = MyOracleDbHost)(PORT = 1521))

    (CONNECT_DATA =

      (SERVICE_NAME = MyOracleDbServiceName)

    )

  )
```

The `tnsnames.ora` configuration file can contain more than one TNS Name entry. Refer to your Oracle documentation or contact your Oracle administrator if you need more details.

4.4.7   Installing Management Server

Once you have completed all the preparatory tasks described in this section, you can begin installing Management Server on the application server. For more information, see "Installing Management Server" on page 9.

4.5   During operation...

This section describes the tasks you have to perform as the Oracle administrator while running Management Server.

4.5.1   Configuring the sort mode

The sort sequence used in both the Management Server user interface and the published pages depends on the language settings of the Oracle database.

If you do not set the *NLS_SORT* and *NLS_LANGUAGE* parameters for the database, binary sorting is applied by default, which we do not recommend in this context. Therefore, set the *NLS_SORT* or *NLS_LANGUAGE* parameter (to AMERICAN or ENGLISH, for example) to ensure that country-specific sorting is applied.

You can currently only apply one sort order setting. It is therefore not possible to select a separate sort order setting for each language variant in a Management Server project.

If you cannot set the *NLS_LANGUAGE* or *NLS_SORT* parameter in the database– because other applications also use the database, for example– you can set the *oracle_nls_sort* parameter for the appropriate value (for example, *oracle_nls_sort=AMERICAN*) in the Management Server *rdserver.ini* file.

For More Information: Oracle Database Globalization Support Guide/Setting Up a Globalization Support Environment

4.5.2   Updating statistics

The Oracle Optimizer uses the database object statistics for its optimization activities. We therefore recommend you update the statistics at regular intervals (automated).

To generate statistics, choose **Analyze** in Oracle Enterprise Manager and analyze all schemas (Management Server projects). We recommend calculating the statistics completely for smaller schemas. When larger schemas are involved, you can estimate the statistics based on 10% of the data volume.

You can also use the following PLSQL command to update the statistics:

```
Begin
dbms_stats.gather_schema_stats(ownname=> '<%SCHEMANAME%>' ,
cascade=> TRUE);
end;
```

> 📄 **Note:** If no statistics are available, you should set the *optimizer_mode = rule* parameter in the database to improve Management Server system performance.

For more information:

Oracle Database Performance Tuning Guide/Managing Optimizer Statistics

4.5.3 Updating full-text indexes

Management Server uses a full-text index (index type CTX CONTEXT) to search for specific content. This index type is only available if Oracle Text (for Oracle 9/10) has been installed on the database. The full text is saved in column *VAL5* of the language variant-dependent table *IO_VAL_<LGV>*, which means that a full-text index is created for each language variant. In Management Server, this full-text index is case insensitive.

You need to regularly update the full-text indexes for content searches in language tables as this is not performed automatically. You have the following options for updating indexes:

- **Use the SQL command**

  - For Enterprise Edition:
    ```
    ALTER INDEX IX_IO_VAL_XYZ5 REBUILD ONLINE PARAMETERS ('sync memory 10M')
    ```

  - For Standard Edition:
    ```
    ALTER INDEX IX_IO_VAL_XYZ5 REBUILD PARAMETERS ('sync memory 10M')
    ```

- **Use the PLSQL command (recommended by Oracle)**

  ```
  EXEC CTX_DDL.Sync_Index ('IX_IO_VAL_XYZ5')
  ```

- **Use the RQL command**

  ```
  <IODATA loginguid="loginguid">

  <DATABASE action="rebuildfulltextindex"

   guid="projectguid" />

  </IODATA>
  ```

  This RQL command executes the above-mentioned PLSQL command. You can configure the RQL command as a scheduled job in Server Manager.

- **Use the CTXSRV program**

  This program updates the index after each DML command. This option places a heavy load on system performance. Oracle no longer provides or supports this program in version 10 of the Oracle server software, nor is its use recommended for earlier versions.

  > 📄 **Note - Updating**
  >
  > Note that the Standard Edition of the Oracle server software does not have the *Index Online Build* feature. As a result, the index is not available during the

update. Accordingly, run the update at a time when no page searches are being performed in the Management Server user interface.

You should call the SQL, RQL, or PLSQL regularly (between hourly and daily).

Oracle users need the role CTXAPP to create the case insensitive full-text index.

For more information: Oracle Text Reference

4.5.4   Deleting projects

If you delete a project in Server Manager, the schema and its objects remain on the Oracle server. If you delete the user on the Oracle server, all schema objects related to this user are deleted automatically. If you want to retain the user or schema for a new project, you have to first delete the schema completely and then create it again under the same name. It is not sufficient to delete the tables and objects of the old schema only.

4.6   Special notes for Oracle support

4.6.1   Modifying connection string when updating Management Server

The connection string for the administration database is located in the configuration file MS\ASP\rdserver.ini. The database connection strings for project databases are stored in the administration database. They cannot be edited in the Management Server user interface but have to be edited directly in the database.

For additional information, see the Oracle documentation (http://docs.oracle.com/html/E10927_01/featConnecting.htm).

4.6.2   Using Oracle database on on Unix/Linux operation systems

If you use an Oracle database server on a Unix/Linux operating system, it can be necessary to modify the database scripts for Oracle databases. Proceed as follows:

1.   During the Installation, stop at the **Welcome to the initial configuration of Web Site Management Server** screen in the Configuration Utility GUI.

2.   Exchange \r\n with \n in all .SQL files stored in the folders

   • (...)\ASP\Schema\Current\Oracle

   • (...)\ASP\Schema\SQLScripts\Oracle

   • (...)\ASP\Schema\Update\Oracle

and in all subfolders.

3. Continue the Configuration Utility to finish the installation.

4.6.3 Using SecureFiles feature with Asset folders

While Asset Manager folders have an option for storing assets on the file system, Asset folders always stores assets in the database. Database technology has matured to a point where this is possible without performance loss.

Note the following:

- Under Oracle, Asset folders prefer using the SecureFiles feature. For more information about the SecureFiles feature, see the respective Oracle documentation (http://www.oracle.com/technetwork/database/features/secure-files/securefiles-160920.html).

- Asset folders also run without the SecureFiles feature but with decreased performance.

- For databases created with Oracle 12c or later, SecureFiles is already configured as the default. Databases created with Oracle versions less than 12c or created with Oracle 12c without the SecureFiles feature have to be migrated to SecureFiles manually. Migrating can be done online while the database is running. For the required steps, see Using SecureFiles to Improve Performance, Maximize Storage, and Enhance Security (http://www.oracle.com/technetwork/testcontent/securefile-095630.html).

Chapter 5

Management Server clusters

5.1 Definitions

Management Server clusters

A Management Server cluster is a combination of several application servers that make use of the same administration database (*IOAdministration*) that is installed on a database server.

Build numbers

Management Server has an official version number, for example, version 16, as well as a build number that represents the current status of the software.

When you log on to Management Server, you can see the current version and build number of the software in the upper left corner of your browser. If you are already logged on, you can display the same information by clicking the Web Solutions symbol in the upper left corner of your screen.

Load balancing (network load balancing software)

Servers can only accommodate a certain number of user requests. If there are a large number of user requests, we recommend distributing them to additional servers. You can do this using load balancing software. For example, Microsoft Server incorporates network load balancing. The load balancing software administers the various IP addresses under a common DNS name. When users log on to the DNS name, the load balancing software searches among the application servers to find the one with the least traffic and transfers the user request to this server.

Asynchronous processes

Management Server is a Web-based application. With normal client applications you can expect to wait for server response, but this is hardly possible with a browser-based client. For this reason, time-consuming program functions, like page publication, are initiated without requiring the client to wait for execution. The client merely receives confirmation that a function has been started. These special independent program functions, known as asynchronous processes, can be executed concurrently on a server. When an asynchronous process is complete, Management Server records this in the general `wsms.log` file and notifies the user via email.

Not all asynchronous processes can be managed in clusters. You can use a cluster to manage the following processes with Management Server:

- Automatic and manual publishing jobs

- Escalation procedures for the workflow

5.2   Cluster applications

OpenText recommends that you use a cluster if one of the following constraints applies to your system:

- A large number of user requests
- A high processor load

5.2.1   Optimizing user requests - web load balancing (web clusters)

When the number of Management Server users increases, so too does the strain on the Windows operating system Internet Information Services (IIS) as well as the dependent processes of the application server.

The right time to add an additional application server to handle user requests depends on your project size, structure, the available hardware, and user behavior.

If Management Server performance suffers due to an increase in the number of users, we recommend you add an additional application server.

Implement Web load balancing for this type of clustering. Web load balancing is not a component of Management Server. Web load balancing or a Web cluster unites several Windows servers under a common DNS or IP address, which, depending on load or a predefined number, then distributes the user requests to the appropriate application servers automatically via HTTP.

5.2.2   Optimizing processor load

Management Server handles a large number of requests within the system as asynchronous processes.

The main task of Management Server is the production of static pages through publishing jobs. These publishing jobs belong to asynchronous processes, which can be distributed to the various application servers via the integrated cluster function.

If publishing jobs are usually executed at night when user activity is low, adding another application server for these asynchronous processes will not reduce processor load. If, however, one or more publishing jobs is always running, it is highly recommended that you implement a dedicated application server for them.

5.2.3 Optimization options for application servers

You can enhance the performance of every application server regardless of whether it is a standalone server or a part of a cluster.

- Increase the number of processors on the application server

- Increase the size of the application server's RAM

- Increase the throughput of the network connection between the application servers or between application servers and client PCs.

5.3 Architecture

The following graphic is an example of a cluster architecture:
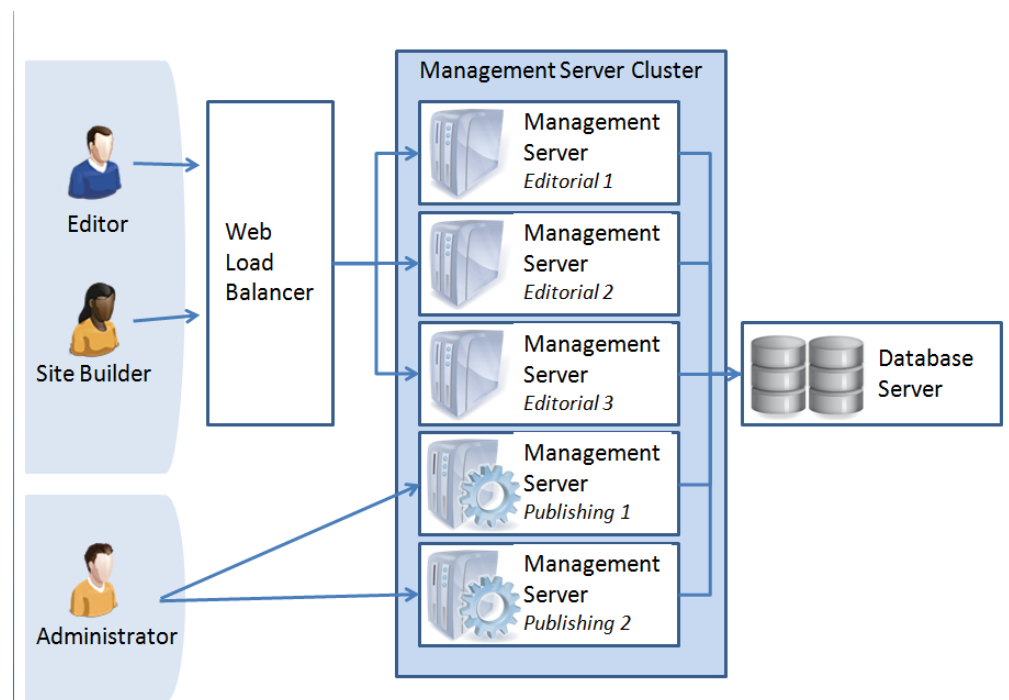
To set up clustering, you should implement a high speed standard network connection between the individual application servers as well as between them and the database server.

The application server clocks must all be synchronized. Deviations larger than two minutes causes the cluster to generate a warning message, which is sent to all users that have the *Server Manager* module.

5.3.1   Distributing user requests – web load balancing

In general, each application server has a unique IP and is accessible through HTTP. In this example, you have provided Management Server users with the unique IP or server name.

To facilitate a large number of users and automatically distribute the generated load, you need to add additional application servers and implement Web load balancing.

Web load balancing is not a component of Management Server. You therefore need to implement appropriate third party tools. These tools assimilate all application servers that are used for user requests under a common DNS name. This means that users are transferred automatically using the common name to the application server with the least load. Refer to the respective handbook of your installed software for the relevant information on installing and using Web load balancing.

The load balancer must support sticky sessions. It is required that the same session will always be routed to the same server, because there is no sharing of sessions between Management Server instances.

For information on how to install additional application servers designed to distribute user requests, see the relevant sections.

We recommend that you reduce the number of asynchronous processes running on these servers and that you distribute them to dedicated servers located outside the Web load balancing.

5.3.2   Distributing processes – clusters

Management Server executes a large number of asynchronous activities, such as publishing, parallel to other functions or processes. To distribute these processes, you need to install additional application servers.

For large projects, we recommend that you set aside separate application servers for the processing of asynchronous processes.

Application servers outside of a Web load balancing environment are generally used by administrators only. This is because editors do not usually have access to their IPs (use of the Web load balancing DNS name). In this way, the servers are not overloaded and can carry out more asynchronous processes.

Later sections contain information about how to install additional application servers and their settings.

5.3.3   Increasing failsafe reliability

If you want to increase your failover, thus increasing security for your editing environment, we recommend that you add additional application servers. If an application server fails, the affected user can make use of other available application servers by simply logging on to a different server and continuing his or her work.

If an application server fails, the cluster recognizes this and informs administrators (with the Server Manager role) via email.

Content that has been edited already will remain intact—however, content currently on the client itself will be lost. The editors simply log on to a different application server. The current session information is not shared among the different application servers, so when a server fails, this information is no longer available.

5.3.4   Scaling the database server

Many database products let you set your own scaling, such as the Microsoft SQL server products. This enables high availability and/or performance gains. This form of scaling is not a component of Management Server. Refer to the selected database product documentation and note its outlined functionality.

To use a cluster, you need to install a dedicated database server.

5.4   Before using Management Server clusters

If you plan to implement Web load balancing, install it and then check its functionality without using the application server. IIS must retain the client session information and the assigned Web server must remain assigned during a session.

All application servers must be in the same LAN and be able to access one another. Ideally they should all be connected via a common switch.

All Management Server installations must have the same software build. Servers that have different software builds than the rest of the servers in the cluster are automatically deactivated.

> **Notes**

- **Projects in Management Server clusters**

  Paths defined in the project settings (for instance, folders) that refer to system folders instead of database folders must be changed to conform to UNC path guidelines or mapped network drives. Make sure these requirements are met for all paths (for example, when publishing files and pages) of all projects contained in the cluster.

  If you use network drives, you need to be sure that at least one user has been set up on the application server whose operating system contains this drive assignment.

Access via the application server to directories is based on the identity of the user. Access authorization to network drives should be made accordingly.

- **Reference directories for publishing targets in clusters**

Management Server creates a reference directory for each publishing target except targets on the file system. All files are published to the reference directory first, and then, if changed, transferred to the configured target for this directory. The reference directory is, by default, created under the ...\ASP \RedDotTemp directory. You can configure the path for the reference directory of a publishing target.

In a Management Server cluster, all nodes performing publishing for a target must be configured to a common reference directory, for example, using an UNC path (go to: *SmartTree > Start > Administer Publication > Project > Edit General Settings*). For details, see section 3.6 "Working with publishing targets" in *OpenText Web Site Management Server - SmartTree Guide (WSMSST-AGD)*.

5.5 Installation

5.5.1 Installing Management Server in a cluster

5.5.1.1 Performing the standard installation

If you install the main cluster server, follow the standard installation procedure as described in "Performing the installation and configuration" on page 21. To install an additional cluster server for an existing cluster, you need a special cluster license. Proceed as follows:

To install an additional application server for a cluster:

1. Follow the hints described in "Before using Management Server clusters" on page 89.

2. Start the Management Server installation on the new computer and follow the steps as described in "Performing the installation and configuration" on page 21.

3. In the **Enter license key** step of the configuration, enter your cluster license key.

4. In the **Select database** step of the configuration, enter the connection data for your existing cluster database server.

5. In the **Database connection** dialog box, enter the name of your existing cluster Administration Database.

6. Proceed with the configuration as usual.

7. After the installation has been completed, log on to this cluster server.

If a message appears informing you that the server is inactive because it has an earlier software build, see the "Updating cluster servers" on page 92 section.

5.5.1.2 Performing the unattended console installation

To install a main cluster server or an additional cluster node, principally perform the installation as described in "Unattended console installation" on page 67. When you edit the configuration file for an additional cluster server, note the following:

- Follow the hints described in "Before using Management Server clusters" on page 89.

- First, you must have installed the main cluster server before you can install an additional cluster server.

- To install the new cluster server, you need a special cluster license.

- In the database sections of the configuration file, enter the connection data for your existing cluster database server.

- In the `<AdministrationDatabase>` element, set `SetupType="`*`ClusterNode`*`"`.

- Enter the name of your existing cluster Administration database as `Databasename` if you use an MSSQL database or as `Schema` if you use an Oracle database.

- No project will be imported, when you have set the `SetupType="`*`ClusterNode`*`"`.

5.5.1.3 Configuring Management Server with IPv6

To run a Management Server cluster with IPv6, you must add the server's IPv6 address to the configuration files for each cluster server.

To add the ipv6 address:

1. Open the following file: `OpenText.WS.MS.ObjectProcessService.exe. config`

2. Locate the port configuration:

   `<channel name="ServiceProcessTcpChannel" ref="tcp" port="10082">`

3. Add your server's IPv6 address as **bindTo** parameter, for example:

   `<channel name="ServiceProcessTcpChannel" ref="tcp" port="10082" `**`bindTo="[fe80::5c2a:648f:1281:1635]"`**`>`

5.5.2   Installing separate application servers

In this case, you want to install an additional server on the same database server but do not want to integrate it in a cluster.

To install a separate application server:

1. Perform the Management Server installation on the new computer and follow the steps as described in "Performing the installation and configuration" on page 21.

2. Start the configuration assistant.

   In the **Select database** step of the configuration, enter the connection data for your database server.

3. In the **Database connection** dialog window enter a name for your new Administration Database.

4. You can now proceed with the installation as usual. After the installation has been completed, log on to this application server.

5.6   Updating cluster servers

To work effectively and maintain data integrity, all application servers in the cluster must have the same Management Server software build. During the update application servers will be deactivated automatically when a mismatch of installed software builds is detected.

To understand the cluster update procedure, it is necessary to distinguish between **central server** and **cluster nodes**. A central server is an application server that has a license with users and modules. A cluster node is an application server that has a cluster license (without users and modules).

During the update procedure only those nodes will be active that have the same software build installed as the central server. Major database updates will only be performed when the central server is updated.

📄 **Note:** The update from version 10.1 to version 16 is a special migration. For details, see "To upgrade a Management Server cluster from version 10.1 SP2 to version 16:" on page 48

5.6.1 Preparing the update

Before updates of application servers, perform the following actions:

- If the respective application server is administered by external load balancing software, deactivate it before beginning the update to block the server to user requests.

- Before updating, notify all active users who are logged on to the affected application server through Server Manager. This gives them time to end their work on the current server and log on to a different application server to continue their work. If you are not using a load balancing system, give users the URL of a different application server so that they can continue working.

5.6.2 Updating the cluster nodes

If there are multiple cluster nodes in the cluster, we recommend to update half of the cluster nodes before the central server is updated. That way it can be made sure that during the update procedure half the cluster performance can be maintained.

Note: In a cluster with only two servers, any of the servers may be updated first.

Proceed as follows:

1. Start the update of a cluster node. Note the following:

   - Once the update procedure has been initiated, the cluster node will be deactivated and not available in the cluster.

   - Users currently logged on to this cluster node will be logged off automatically.

   - Active publishing jobs are stopped but can be restarted by other available servers in the cluster.

2. Once the update of the cluster node is complete, the server will remain deactivated as its software version is different from the software version of the central server. Once the central server is updated with the same software version, the cluster node will be reactivated automatically.

5.6.3   Updating the central server

After you have updated half of the cluster nodes, we recommend to update the central server before the remaining cluster nodes.

1.   Start the update of the central server. Note the following:

   • Once the update procedure has been initiated, the central server will be deactivated.

   • Users currently logged on to this central server will be logged off automatically.

   • During the update of the central server, the whole cluster is deactivated as it might be required to update the database system and no access to the database is allowed during that time.

   • When the update process of the central server has been completed, the central server will become active in the cluster again and activates all cluster nodes that have the same software version installed as the central server.

Example 5-1: Updating three application servers as a cluster

   1.   Before the update, all application servers (A, B, and C) have the same installed version.

   2.   Server A has a license with users and modules and is the central server. Servers B and C have cluster licenses and are the cluster nodes.

   3.   Update cluster node C first. After the update it will be deactivated. A and B remain active during that time.

   4.   Update the central server A now. Once the central server A has been updated, the updated cluster node C is automatically reactivated and the cluster node B is deactivated as it is running with a different software version than the central server.

   5.   Update the cluster node B. Once B has been updated all servers are up-to-date and active again.

5.7   Administering application servers

You administer application servers in the **Administer Application Servers** area of Server Manager.

Every administrator with the *Server Manager* role can administer the cluster using Server Manager.

5.7.1 Adding a new application server to a cluster

Install a new application server as described in "Installing Management Server in a cluster" on page 90.

5.7.2 Management Server cluster display in Server Manager

Application servers that are part of a cluster are displayed in the tree as shown in the example below:

Administer Application Servers

Application Servers

SERVER_1 Active - 0/10 Async. processes

SERVER_2 Inactive - No asynchronous processes

SERVER_3 Inactive, replacement release later version -10/10 Async. processes

SERVER_4 Inactive, replacement release earlier version -2/Unlimited async. processes
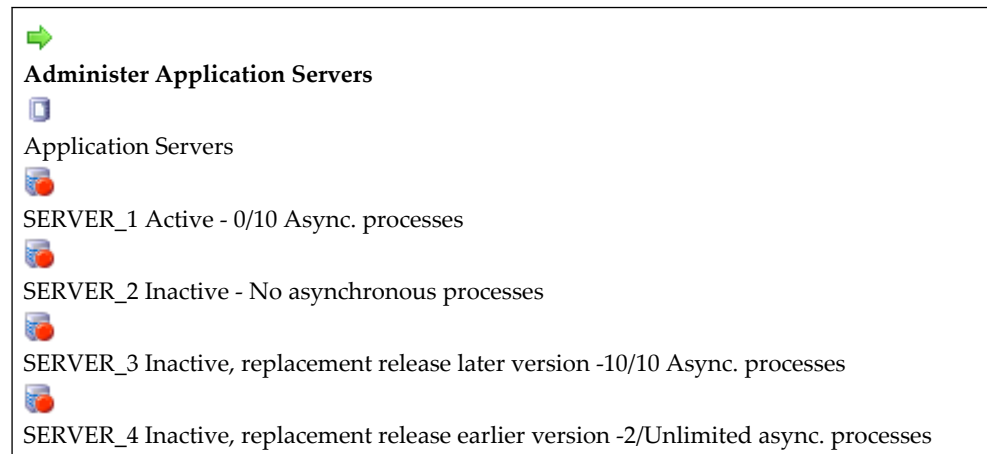
This list shows four application servers in various conditions. The comments next to the application server name indicate the status and process information. The server status is shown first.

The following status values have been defined:

Active	Application server is available for processes and user requests.
Inactive	Application server has been deactivated and is not available. Only an Administrator with the *Server Manager* role can access this application server. Application servers like this can be reactivated by any other application server in the cluster.
Inactive, replacement release later version	This application server has a later (higher) build and is therefore not available. An Administrator with the *Server Manager* role can log on to the server and activate this build. All application servers with earlier (lower) builds are then deactivated.
Inactive, replacement release earlier version	This application server has been deactivated because it has an earlier (lower) build than the current build. You need to update this application server to the latest build before you can activate it.

The status information is followed by an overview of how processes have been distributed among the application servers. Here are some examples:

1/10 Asynchronous processes
Ten processes can be carried out on this application server simultaneously. One is currently running.

No asynchronous processes
> This application server has been set to accept no processes.

2/Unlimited asynchronous processes
> This application server has been set to accept an unlimited number of processes. Two are currently running.

5.7.3   Asynchronous processes

Navigation path

> Server Manager **>** Administer Application Servers **>** (Select application server)
> Action: Edit Settings

You can define the number of simultaneous processes that each application content server within the cluster can accept in a dialog window.

You can configure two settings in the *Asynchronous Processes* area of the **Edit Application Server Settings** dialog window:

Query interval   Here you can define (in seconds) how often the application server should search the database server for new asynchronous processes waiting to be completed. The default setting is 60 seconds.

Number of simultaneous processes   Here you can define how many simultaneous asynchronous processes this application server should accept. The following settings are possible:

-1	The application server is allowed to start any number of processes.
0	The application server is not allowed to start any processes.
1– 500	Number of processes that the application server can process concurrently.

5.7.4   Dialog box - Asynchronous processes

Navigation path

> Server Manager **>** Administer Application Servers **>** Application Servers
> Action: Edit Asynchronous Processes   *or*

> SmartTree **>** Administer Project Structure **>** Project
> Action: Show Asynchronous Processes

You can view and edit all of the asynchronous processes assigned to the application server in a dialog window (see Asynchronous Processes).

You can utilize this process list for the following:

- To see which processes and how many are currently running or waiting to be run on the selected application server

- To distribute, stop, delete, or deactivate processes.

The process list is sorted according to when a process is scheduled to begin on a specific application server. The active process is listed first, followed by the next scheduled process, while the lowest priority processes and those scheduled to run last are listed at the bottom.

For more information on the editing options in the *Edit Asynchronous Processes* and *Show Asynchronous Processes* dialog windows, see *OpenText Web Site Management Server - Server Manager Guide (WSMSSM-AGD)*.

5.7.5 Error messages using email notification

When problems occur, administrators with the *Server Manager* role receive the email notification described below.

Email notification is an automatic server function. The email text cannot be edited and always appears in English.

Server (name) with IP (IP) has wrong timestamp, please correct the time settings

Administrators with the Sever Manager role receive this notification if the timestamp of any application server deviates more than two minutes from any other application server.

Synchronization is important because it helps to coordinate the various application servers and to detect server failure.

If you receive this notification, you should correct the computer clock of the affected application server. We recommend setting up automatic synchronization of the various server clocks.

Server (name) with IP (IP) is not responding, error

Administrators with the Sever Manager role receive this notification if any application server fails to react to user requests for several minutes.

If the server downtime is not due to scheduled maintenance, you need to take the following measures:

- Check to see if the affected application server is still functioning properly. The failure could have the following causes:

  - A technical defect has disabled the application server.

  - The network connection to the application server has been lost.

  - The operating system has ceased to function due to irregularities in the software/hardware.

- If the affected application server is part of a load balancing environment, you need to deactivate the application server as soon as possible to prevent users from being redirected to it.

Chapter 6

Management Server updates, service packs, and hotfixes

6.1 Additional information for updates, service packs, and hotfixes

6.1.1 General

In Management Server 16, you can principally downgrade to an earlier build of the same version.

Service Packs

A service pack is a compendium of solutions for Management Server. You install a service pack in the same way as you would an update. Make sure that you read the supplied Release Notes.

Hotfixes

If you have received a hotfix for an urgent problem, pay attention to the following points:

- A hotfix does not meet the strict quality controls that a release or an update does. So if you implement a hotfix, you do so at your own risk. Otherwise, wait for the solution contained in a release, update, or service pack.

- Make sure that you read the supplied Release Notes.

> **License keys**
>
> You do not need a new license key for an upgrade of Management Server; licenses are independent from versions. You need a new license key in the following situations:
>
> - Changing IP address
> - Moving from IPv4 to IPv6
> - Adding additional modules

6.1.2   Checklist for updates

- Updates, hotfixes, and service packs can contain dialogs or changes that have not been covered in this handbook. **It is very important that you read the accompanying Release Notes before you start**.

- Log on to the server as `installingAdministrator` user. See also installingAdministrator user on page 14.

- Ensure that all users have logged off from Management Server and no publishing jobs are active.

- Open Text recommends that you restart your system before implementing the update, service pack, or hotfix.

6.2   Updating Management Server

6.2.1   Installing hotfix/service pack

You can install the hotfix/service pack either from the UI or from command line.

For more information about the required users, see "Creating technical Windows users" on page 13 and installingAdministrator user on page 14.

To install a hotfix/service pack from the UI:

1. Double-click `setup.exe` to start the installer. If you are not logged in as `installingAdministrator` user, a *User Account Control* dialog opens to ask for the appropriate credentials.

    The installation path will be set automatically.

    The user names for the `serviceuser` and `apppooluser` are preset with the values from the previous configuration.

2. When required, edit the user names. Enter the passwords.

3. After the installation is complete, the Configuration Utility GUI starts automatically. Follow the configuration steps and enter the required data.

To install a hotfix/service pack from the command line:

Note that you must use an elevated command prompt.

1. Run the installer using the following command line:

    `msiexec /qn /i OpenText.WS.MS.Installation.msi`.
    The installation path will be set automatically.

2. Edit the `ConfigurationUtility.exe.config` file. You have two options:

    - adapt the existing `ConfigurationUtility.exe.config`. In the `<ManagementServer>` element, remove the `Username` and `Password` attributes completely.

- redeploy the configuration file using the `ConfigurationUtility.exe.config.sample` file. Edit the file and enter all required data.

3. Run `ConfigurationUtiliy.exe`.

> **Note:** When updating Management Server, a **Files In Use** dialog may show up listing an **IIS Worker Process**.

You have the following options:

- **Restart IIS** - Restart the Internet Information Services (IIS). Ensure that no user logs on to the current machine. Click **Retry** to continue the installation.

- **IIS cannot be restarted** - If the Internet Information Services (IIS) cannot be restarted, open the IIS Manager and click **Recycle...** for the following application pools:

  - OpenTextWsmAppPool64

  - OpenTextWsmPreExecuteAppPool

  Ensure that no user logs on to the current machine. Click **Retry** to continue the installation.

Do not click Ignore Do not click **Ignore** because this can result in files that are not correctly updated.

6.2.2 Rolling back hotfixes

Management Server supports rolling back hotfixes. You can go back to a previous hotfix version of Management Server by revoking the installation of the current hotfix.

You can roll back the installation of software components but not content changes.

Proceed as follows:

To roll back the installation on a single server:

1. Uninstall the current Management Server version.

2. Install the older Management Server version. The `Configuration Utility` maintains the existing version's configuration information and sets down the version number.

To roll back the installation on a cluster node in a cluster scenario:

1. Uninstall the current Management Server version.

2. Install the older Management Server version. The `Configuration Utility` maintains the existing version's configuration information. The server will be deactivated. The version number of the cluster will not be changed.

To roll back the installation on a central server in a cluster scenario:

1. Uninstall the current Management Server version.

2. Install the older Management Server version. The `Configuration Utility` maintains the existing version's configuration information and sets down the version number in the cluster.

Cluster nodes that still have the previous Management Server version installed will be automatically deactivated when downgrading the central server and thus the cluster version.

6.2.3   Important information regarding use after updates

- After an update, clear the browser cache for all browsers on all computers. We recommend setting the value of the browser cache size as low as possible.

- After updating Management Server, you may have to update the project databases before you can select projects for editing. For more information, see section 5.1.12 "Updating project databases" in *OpenText Web Site Management Server - Server Manager Guide (WSMSSM-AGD).*

- After an update, asynchronous processes may not start automatically. In this case, use the Server Manager to start the asynchronous processes.

Chapter 7

Removing Management Server

This section guides you through the removal process.

> **❗ Important - Starting the removal process**
>
> Log on to the server as administrator with local administrator rights.

7.1 Removing Management Server

1. Open the **Start** menu and click **Control Panel** > **Programs and Features**.

2. In the **Programs and Features** list, right-click **OpenText Web Site Management Server** and click **Change** to start the installation.

3. In the **Welcome to the Web Site Management Server Installation** dialog, click **Next** or press **Enter**.
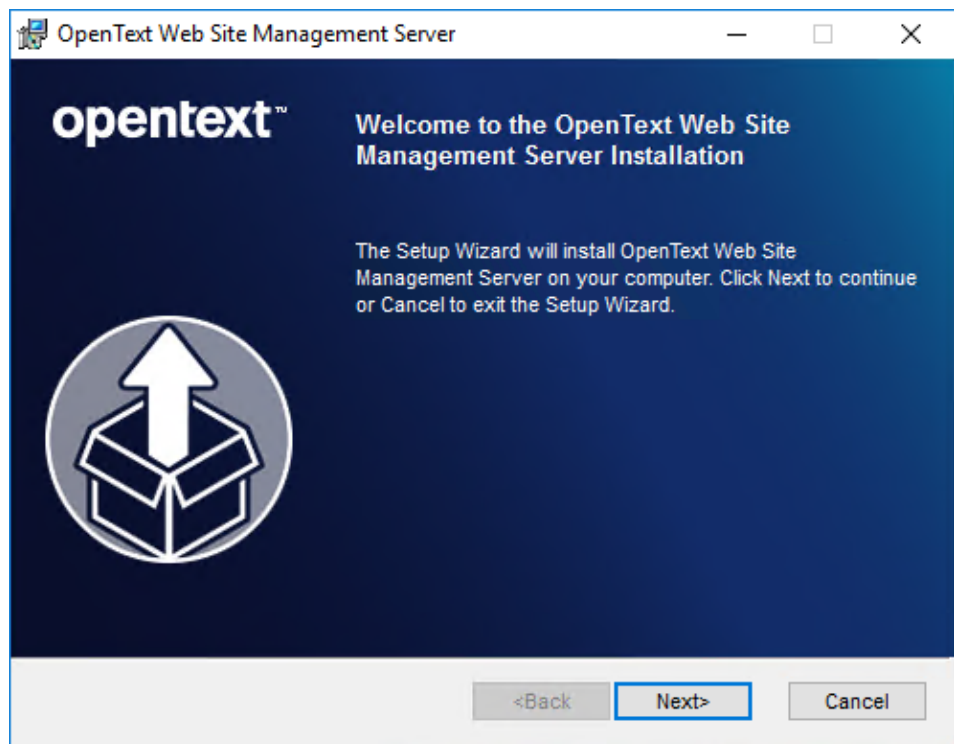
4. In the **Change, Repair or Remove Installation** dialog, click **Uninstall**.
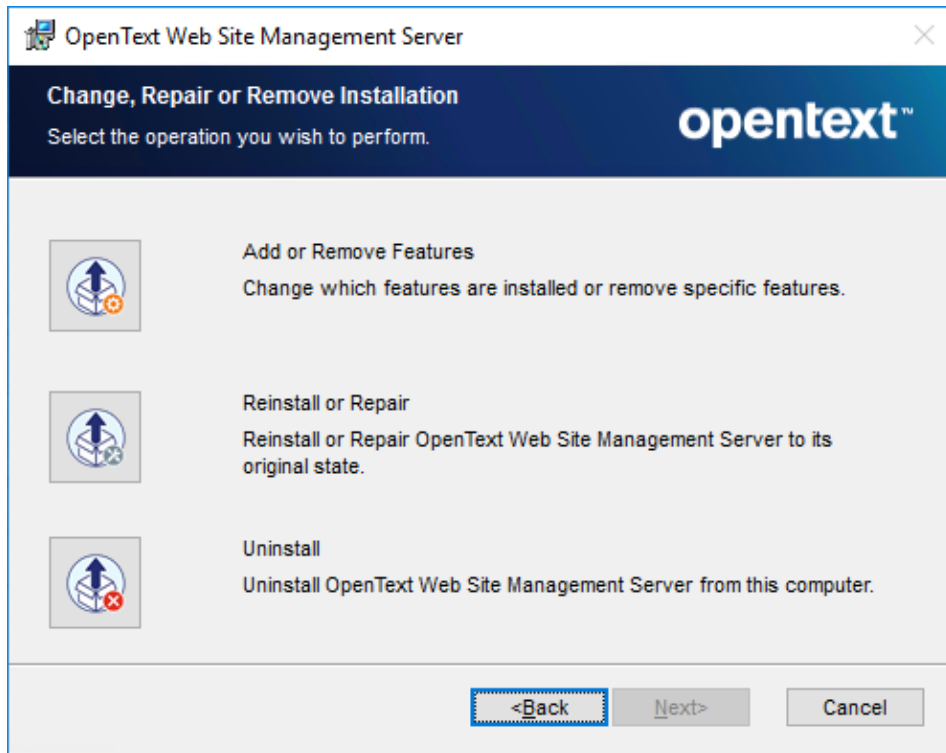
5.   In the **Ready to Remove** dialog, click **Remove** or press **Enter**.

6.   When the removal process is complete, click **Finish**. Click **Refresh** to reload the **Programs and Features** list, if necessary.
     OpenText Web Site Management Server is removed from the list.

7.2   Removing folders

After the removal, several folders remain on the server.

MS

This folder (for standard installations) is stored in the `Open Text\WS\` folder. You can delete this folder and all its subfolders. Do not delete the higher-level **Open Text\WS** folder if it contains other applications.

> **!   Important**
>
> Note that the `MS` folder contains configurations and log files that you might want to keep. Check the following files:
>
> * `MS\ASP\Log\*`
>
> * `MS\ASP\*.config`
>
> * `MS\ASP\rdserver.ini`
>
> * `MS\Configuration\*`

- `MS\ConfigurationUtility\ConfigurationUtility.exe.config`

Chapter 8

Appendix

This chapter contains additional information.

8.1 Implementing the OpenText Private Help Server for Management Server

The Management Server online help is delivered using the OpenText Global Help Server system, which provides users with live access to the latest version of the online help. If you do not want to use the OpenText Global Help Server system, you can choose to download a copy of the online help files and host them on a local server by deploying OpenText Private Help Server.

📄 **Note:** The Private Help Server can support multiple OpenText products. If the Private Help Server has already been installed within your organization to support another OpenText product, you can add the Management Server online help to that installation.

Setting up the Private Help Server requires you to complete the following general tasks:

1. Prepare a server with the following:

   - Apache Tomcat 7 or 8 application server.

   - Java 1.6 or later.
2. Download and extract a copy of the product help files from OpenText My Support.
3. Deploy the Private Help Server, which includes a web application that can locate and return the locally deployed help files.
4. Configure the product to direct help requests to the Private Help Server.

8.1.1   Downloading the OpenText Private Help Server Kit and product online help files

The first step in setting up the OpenText Private Help Server Kit is gathering the required files. These include the following:

- The OpenText Private Help Server Kit is available on OpenText My Support: https://knowledge.opentext.com/go/62360624

- A copy of the product online help files that the Private Help Server will host. The Online Help files are available on the OpenText My Support as a subfolder of the Management Server documentation.

8.1.2   Deploying the Private Help Server

You can install the Private Help Server application by completing the tasks described below.

Extracting the files

Extract the Private Help Server Kit to a temporary directory. You will modify the files in this working directory and then deploy them to your site in later steps.

> **Notes**
>
> - The Private Help Server Kit contains two similarly named files, one compatible with Apache Tomcat 7.x and the other with Apache Tomcat 8.x. During the setup process, you will need to rename these files by removing the version information for the file that is compatible with your version of Apache Tomcat.
>
> - The Private Help Server Kit supports two help file branches, `help` and `pi_hosted`, and contains support files for each branch. Management Server uses the `pi_hosted` branch.

After you extract the files, you should see an `Private Help Server Kit` directory that includes the following:

- `application` directory: Contains `docsapimapper.war`, the Private Help Server Web application file.

- `help_support` directory: Contains support files for the `help` branch:

  - `docsapimapper.xml.tomcat`*`<version>`*: The Web application descriptor file.

  - `docsapimapper.properties`: The configuration properties file declaring the installed product help under the `help` branch and the installation path.

- `pi_hosted_support` directory: Contains support files for the `pi_hosted` branch:

  - `docsapimapper.xml.tomcat`*`<version>`*: The Web application descriptor file.

- pidocsapimapper.properties: The configuration properties file declaring the installed product help under the pi_hosted branch and the installation path.

- Sample directory: Contains sample descriptor and configuration files taken from a working sample deployment for each branch. Do not use these files in your deployment.

- _readme.txt: A summary description of the files intended for users without access to the information in this guide.

- docs.zip: Sample help files used to verify your Private Help Server deployment.

- Test Help Page - OT Private Help Server.zip: A sample page you can use to connect to your Private Help Server deployment.

Creating the local help directory

You must create the *<help_root>* directory, which is the directory where you will deploy the help files you want to make available through the Private Help Server and then add the test files used to verify your deployment.

To create the <help_root> directory:

1. Create the directory where you will extract the online help files, for example C:\ot_docs.

   The *<help_root>* directory can exist on any local drive, but its path must not contain any names with spaces.

2. Extract the sample help files in the docs.zip file into the *<help_root>* directory.

   📄 **Note:** Always use the **Extract all** option when you extract OpenText online help files.

3. After you extract the files, open the *<help_root>*/docs/pi_hosted/test/v160200/test-h-ugd/en/ofh directory and verify that the following files were extracted:

   - context.properties

   - index.html

Creating a help folder alias

You need to define an alias that the Private Help Server application can use to locate the online help files.

To create the help folder alias:

1. In the pi_hosted_support folder where you extracted the zip file, rename the docsmapperapi.xml.tomcat*<version>* file for your version of Tomcat to docsmapperapi.xml.

2. Open the `docsmapperapi.xml` file in a text editor, and then locate the `<Context>` element.

3. Replace the *<help_root>* with the full path to the help file directory you created in "To create the <help_root> directory:".

For example, using the folder created above, the setting for Apache Tomcat 7.x on Windows is:

```
<?xml version="1.0" encoding="UTF-8"?>
<Context aliases="/docs/pi_hosted=C:\ot_docs\docs
\pi_hosted
</Context>
```

> **Note:** On non-Windows operating systems, use appropriate slashes, double quotes, and brackets, for example:
>
> ```
> <Context aliases="/docs/pi_hosted=C:/ot_docs/docs/pi_hosted">
> ```

The same example for Apache Tomcat 8.x is:

```
<?xml version="1.0" encoding="UTF-8"?>
<Context>
    <Resources
className="org.apache.catalina.webresources.StandardRoot" >
        <PreResources webAppMount="/docs/pi_hosted" base="C:/
ot_docs"
className="org.apache.catalina.webresources.DirResourceSet" />
    </Resources>
</Context>
```

Creating a configuration properties directory

You must create a properties file that contains the setting required to locate your help files.

To create a configuration properties directory and file:

1. Create a folder where the configuration properties file will be stored, known as the *properties root* directory. For example `C:\ot_docsconfig\properties\docsmapper`.

   > **Note:** You can create the properties root directory on any local drive, but the directory path must:
   >
   > • Not contain any spaces or special characters.
   >
   > • Contain the subdirectories `\properties\docsmapper`. For example, if the properties root directory is `C:\ot_docsconfig`, the full path is `C:\ot_docsconfig\properties\docsmapper`.

2. In the `pi_hosted_support` folder, copy the `pidocsapimapper.properties` file from the extracted files to the *<properties_root>*`\properties\docsmapper` directory.

3. Open the `pidocsapimapper.properties` file in a text editor and define the `webserverHelpRoot` and `techDocs Root` settings as follows:

webserverHelpRoot
> The Tomcat root URL for the local help. The URL contains the following information:
>
> `http://`*`<host>`*`:`*`<port>`*`/docsapimapper/docs/pi_hosted`
>
> where *<host>* is the server where Tomcat is deployed and *<port>* is the port on which Tomcat listens. For example, on a server named `host.mycompany.com` listening on port `8080`, the setting is:
>
> `http://host.mycompany.com:8080/docsapimapper/docs/pi_hosted`
>
> 📄 **Note:** Specify the full server name or IP address as the *<host>* value. Do not use `localhost`. Also, the value you use must be used in all *<host>* settings, including URLs. IP address will not resolve to host names and host names will not resolve to IP address.

techDocs Root
> The path to the directory where the help files are stored. For example `C:/ot_docs/docs/pi_hosted`.

<product_code>
> Each OpenText product online help is identified by a specific product code. In the **<PRODUCT CODE>** section of the file, create a new line and specify your product code as *<product_code>=<product_code>*.
>
> The product code setting for Management Server is: wsms=wsms
> wsmsam=wsmsam
> wsmsnm=wsmsnm
> wsmsse=wsmsse
> wsmssm=wsmssm
> wsmsst=wsmsst

➡️ **Example 8-1: Sample pidocsapimapper.properties file**

```
# All values marked by < > must be updated.
# This file should be on the app server class path.

# URL and directory mappings
# helproot server MUST match JS setting
webserverHelpRoot=http://host.mycompany.com:8080/
docsapimapper/docs/pi_hosted

#Path to the help folder root
techDocsRoot=C:/ot_docs/docs/pi_hosted

# <PRODUCT CODE>
# Product directory mapping - will be the same as the
OpenText product name setting in the live Private Help Server
```

```
implementation.
# See your product documentation for the specific value for
your product.
# Some OpenText product codes are:
# Media Management: medmgt=medmgt
# InfoFusion: inf=inf
# Web Experience Management: wcmgt=wcmgt
# NOTE: test=test is required to verify the initial set up.
test=test
wsms=wsms

wsmsam=wsmsam

wsmsnm=wsmsnm

wsmsse=wsmsse

wsmssm=wsmssm

wsmsst=wsmsst

# Default locale to use
defaultLocale=en

# Parameter names - DO NOT MODIFY UNLESS INSTRUCTED
product=product
version=version
locale=locale
context=context
module=module
type=type
securityKey=security
```

Installing the descriptor and application files

The final step before testing the Private Help Server is deploying the application files.

To install the files and start the application:

> **!** **Important**
> Verify that Tomcat services are **not** running when you complete these tasks.

1. Copy the docsapimapper.war file into the *<Tomcat_home>*\webapps directory. If there is an existing docsapimapper directory or docsapimapper.war file in the folder, delete them.

2. Copy the docsapimapper.xml file from the working directory into the *<Tomcat_home>*\conf\Catalina\localhost directory. If the Catalina\localhost directory does not exist, create it.

3. Add the *<properties_root>* you created in "To create a configuration properties directory and file:" on page 110 (for example C:\ot_docsconfig) to the Tomcat Java classpath.

   For example, on Windows run the tomcat*<x>*w.exe file in the *<Tomcat_home>*\bin folder, click the **Java** tab, and then append the properties root path to the **Java Classpath** field. On non-Windows, set the path using the setenv.sh command.

4. Start Tomcat.

Testing the Private Help Server

After Tomcat starts, you can test the deployment by submitting URL requests to it through the Private Help Server Test Page. The Test Page contains a simple JavaScript function that simulates an online help button that can call the test help pages that are included with the Private Help Server.

> **Note:** The Test Page is intended to verify that your Private Help Server is installed and configured correctly. The page uses a simple method to request the help files that may not work with all online help formats. Do not attempt to modify the page to access other online help files or beyond the tasks described in the procedure below.

To test the Private Help Server:

1. Extract the Test Help Page - Private Help Server.zip file to a working directory.

   > **Note:** Always use the **Extract all** option when you extract OpenText online help files.

2. In the extracted Test Help Page - OT Private Help Server folder, locate the pi_hosted\TestPage.html file, and then open it in a text editor.

3. Locate the urlRoot: setting, and then replace the *<host>* and *<port>* values with your Tomcat server name and the port on which it listens.

4. Save the file and then open it in a browser.

   > **Note:** We recommend that you use a recent release of the Firefox or Chrome browsers.

5. Click **Test Your Local Server** to test your deployment.

   The page displays the URL it will attempt to open based on the settings you made to the HTML file.

   If the Private Help Server is deployed correctly, the URL will be processed and return a help page that confirms that the deployment is working.

Deploying additional help files

Once you have successfully set up the Private Help Server, you can deploy other product help files in addition to the test file.

To deploy additional help files:

1. Stop Tomcat.

2. Extract the additional help files to the help root folder you created in "To create the <help_root> directory:".

   📄 **Note:** Always use the **Extract all** option when you extract OpenText online help files.

3. Update the Private Help Server help registry by executing the following command at a command line prompt:

   ```
   java -jar <tomcat_home>\webapps\OTHelpServer\WEB-INF\lib
   \HelpServer-<version>.jar -d <help_dir> -s
   ```

   where *<tomcat_home>* is the path to your Tomcat installation, *<version>* is an optional version number in the `jar` file name and *<help_dir>* is the help root folder. For example, the following command updates the help registry for a help root folder `C:\ot_docs\docs\pi_hosted`:

   ```
   java -jar C:\PROGRA~1\APACHE~1\TOMCAT~1.0\webapps\OTHelpServer
   \WEB-INF\lib\HelpServer-16.0.0.jar -d C:\ot_docs\docs\pi_hosted -s
   ```

4. Edit the `pidocsapimapper.properties` file and add the product code for your help on the line below the test setting `test=test`. For more information, see "Creating a configuration properties directory" on page 110.

5. Restart Tomcat.

To access the help files, you can use the `TestPage.html` file as long as you modify the settings to reflect the values for your help. You can gather these settings from the file path after you extract the help files to the help folder.

The help file path uses the following convention:

```
<helproot>/docs/pi_hosted/<product>/<version>/<module>/<language>/
<type>
```

For example, the *OpenText Web Experience Management - Content Workspaces Help Collection (WCMGT-UGD)* version 16.4 online help extracts to the following path:

```
<helproot>/docs/pi_hosted/wcmgt/v160400/wcmgt-h-ugd/en/ofh
```

So, to use the `TestPage.html` file, the JavaScript settings must be updated as follows:

```
product: 'wcmgt',
version: 'v160400',
```

```
type: 'ofh',
module: 'wcmgt-h-ugd'
```

Modify your installed product to use the Private Help Server

After you have successfully deployed and tested the Private Help Server and added your copy of the product online help to it, you are ready to modify your installation of Management Server to redirect help requests from the OpenText Global Help Server to your Private Help Server. For more information, see .

8.1.2.1 Troubleshooting the Private Help Server

If you get an error when you attempt to set up the Private Help Server, check the following common issues:

- Verify that you are using the correct slashes in any folder paths you must specify in settings. The direction of slashes in folder paths can matter for some operating systems.

- Verify that the Tomcat classpath is set correctly. The path you specify should *not* include the `properties\docsmapper` folders; it should specify the path to the folder where you created those subfolders. For more information about setting the Tomcat classpath, see .

- Analyze the log files in the `<Tomcat_home>\logs` folder, including the `hosteddocslog.<date>` file for more information.

8.1.3 Configuring Management Server to use the Private Help Server

To configure Management Server to redirect to the Global Help Server Private Help Server:

1. In Management Server, go to the `<Management Server_installdir>\ASP\main.config` file.

2. Go to the `<HostedHelp>` element, and then change the value of the `<UrlAddress>` element to point to the Global Help Server Private Help Server:

   ```
   <HostedHelp>
      <!-- Hosted help authority and path 'https://
   docsapiqa.opentext.com/mapperpi' -->
      <UrlAddress>https://<Private Help Server>/mapperpi</
   UrlAddress>
   </HostedHelp>
   ```

   📄 **Note:** Do not change the following additional online help parameters:

   - `<Tenant>`: A special online help system identifier supplied by OpenText. Do not specify or change a value unless directed by OpenText.

- `<Type>`: Identifies the OpenText online help type. Do not specify or change a value unless directed by OpenText. If you supply an unsupported value, you can cause the online help system to stop working.

8.2   Third-party software components

Management Server uses third-party software components. These components have been carefully selected and their functionality with Management Server has been tested. Nonetheless, some third-party software components require OpenText to include acknowledgements or disclaimers within Management Server documentation.

The document *3rd Party Licenses Management Server*, which is part of the software documentation, lists the licenses of all third party products used in this component and any components it directly or indirectly depends on. Listed Open Source components are licensed from the copyright holder without warranties of any kind, either express or implied warranties, including without limitation the implied warranty of merchantability and fitness for a particular purpose. Copyright holders mentioned herein shall not be responsible for any damages, general, special, incidental or consequential, arising out of the use or inability to use this component/ software. Check the respective license agreement for more details. This does not limit the liability and warranty as provided under your license agreement with OpenText for the OpenText products as a whole.

OpenText shall not be liable and does not provide any warranties in the event that the Customer makes any changes to the delivered objects, modules, parts thereof or the like, re-links, converts, connects or in particular combines such modules or parts thereof with any Open Source Software. In regard to any existing, i.e. not modified modules, the liability and warranty provisions of the License Agreement shall apply and shall remain unaffected unless interfaces between changed and unchanged parts are affected.