Operations Bridge Manager

For Windows® and Linux operating systems

Software Version: 2020.10

Customized output from:

Operations Bridge Manager 2020.10 Interactive Guide

Document Release Date: August 2020

Software Release Date: October 2020

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Java is a registered trademark of Oracle and/or its affiliates.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, Lync®, Windows NT®, Windows® XP, and Windows Vista® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Check your selections

Done: ☐

The following steps are customized according to your selections. Check that your selections are correct.

- Enterprise setup
- Install and configure OBM
- Distributed/Distributed HA
- Microsoft SQL Server (remote DBMS)
- Microsoft Windows

If any selections are not correct, click **Change**. If you are using a printed copy of the interactive document, refer Online Interactive document for the latest updates.

« Change Print »

Check the hardware requirements

Done: ☐

- **Processor.** The following table lists the CPU requirements. We recommend using 2.4 GHz CPU cores or faster.

  In a virtual environment, make sure the number of virtual CPUs is equivalent to the number of physical CPU cores used.

Deployment		Single Server	Data Processing Server	Gateway Server
Small (up to 2,000 nodes)	Minimum	4	3	2
	Recommended	5	4	3
Medium (up to 5,000 nodes)	Minimum	7	5	3
	Recommended	8	6	4
Large (more than 5,000 nodes)	Minimum	11	8	4
	Recommended	12	9	5

  Tip

  Because OBM performance is dependent upon processor speed, we recommend getting the fastest possible processor to ensure adequate performance.

- **Memory.** The following table lists the physical memory requirements (in GB).

Deployment		Single Server	Data Processing Server	Gateway Server
Small (up to 2,000 nodes)	Minimum	14	12	6
	Recommended	16	14	8
Medium (up to 5,000 nodes)	Minimum	16	14	8
	Recommended	20	18	10
Large (more than 5,000 nodes)	Minimum	32	30	10
	Recommended	44	42	12

In addition, some memory is required for temporary data.

Note

The required memory shown in the Configuration Wizard is calculated dynamically based on the memory that is given to all the processes which make up the OBM server. It also takes into account the overrides which a customer might do in the Advanced section. However, it does not include any other consumers of memory on the system, like the basic OS processes/services or CLIs which also need a considerable amount of the available memory. The memory requirement values provided in the table take these into consideration and are therefore higher.

- **Free storage space.** Before performing installation of OBM , make sure the following amount of free storage space (in GB) is available:

Default Folder	Minimum	Recommended
`C:\HPBSM`	31	50
`C:\ProgramFiles\HP\HP BTO Software`	8	12
`C:\ProgramData\HP\HP BTO Software`	1	2
%TEMP% *	12	20

* This is a user environment variable

- **Additional requirements:**
  - Uploading Operations Agent deployment packages to the OBM server requires up to 20 GB of additional free storage space.
  - OBM server must not be installed on a drive that is actually a mapped network folder.

    When using Remote Desktop Protocol (RDP) and device redirection, make sure that you do not install OBM server on a local disk of the client system.
  - For the hardware requirements for remote database servers (database management systems), see the Prepare Database environment.

Check the software requirements

Done: ☐

-

- **Windows patch requirement.** If you are using Windows systems older than Windows Server 2016, you must install Windows Patch KB2999226 and reboot the system.
- **TCP setting.** We highly recommend that you increase the TCP time delay above its default setting.

  For the Windows registry key entry `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`, create a new `DWORD (32-bit) (REG_DWORD)` value named `TcpTimedWaitDelay`, and enter `60` (decimal) for its value data.

  If this change is omitted, a long time delay (configured by default) might result in a problem with exhausting the available TCP resources.

  Caution

  We recommend that you back up Windows Registry before making any changes to it.

- **User Account Control (UAC).** UAC must be disabled before installing OBM 2020.10.

  To turn off UAC via registry, change the DWORD "EnableLUA" from 1 to 0 in "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system".

  After the installation, you can reenable UAC.
- **Fully qualified domain names (FQDNs).** Each OBM server must have a resolvable FQDN. To verify it, run the `hostname` and `nslookup` commands. If either command returns an FQDN, your domain name is supported.

  FQDNs of the server systems must consist only of the following characters: a-z, A-Z, 0-9, hyphen (-), and period (.)
- **Hostname resolution.** OBM servers must be able to resolve names of the systems they communicate with. These include all OBM servers, database servers, and data collectors.
- **Application coexistence.** OBM servers must be installed on dedicated host systems which must not run other applications.

  Installing OBM servers together with most other Micro Focus products on the same host system may result in port conflicts, performance issues, or other unexpected behavior. Coexistence of OBM servers with Operations Agent and Data Flow Probe (DFP) is supported. For details on the coexistence support, select **Operations Bridge Manager** from the product list in the following document:

  Operations Bridge Manager Integration portal

  For more information on the supported versions for OBM, see SUMA link below:

  Support Matrices for Operations Center products
- **Ports.** The installation checks whether the following ports are available: 80, 383, 443, 1098, 1099, 4447, 5445, 8009, 8080, and 29000.

  If the installation checks indicate that these ports are in use, the installation does not fail, but we recommend that you free the necessary ports before configuring OBM.

  For a complete list of ports used by OBM, see Port Usage .
- **Reserved ports.** The operating system reserves a range of ports for the use of applications that require outgoing connections to external systems.

  The installation checks if ports up to 30999 are available. We recommend to ensure that the dynamic port range reserved by the operating system starts at 31000 or above.

a. Check the dynamic port range by running the following command:

```
netsh int ipv4 show dynamicport tcp
```

b. If the reserved ports do not start at 31000 or above, run the following command to change this setting:

```
netsh int ipv4 set dynamicport tcp start=31000 num=16384
```

- **Time settings.** Host systems of all OBM servers and the database management system must have the same settings for the following parameters:
  - Date and time
  - Time zone
  - Daylight saving time configuration
- **L-Core.** OBM installs the L-Core agent packages. If an earlier version of these packages is already installed. Otherwise, the currently installed version is left intact.
- **Web server:**

  OBM deployment requires a web server. The OBM uses its own web server (Apache httpd) and installs it as part of the installation process

  Note

  There must be only one running web server on a system, and it must use the same port as OBM. For example, during the installation of OBM, if you are installing on a system where Microsoft IIS is already running, make sure to stop the IIS services and set their startup type to Manual before initiating the installation process.

  OBM uses a customized version of Apache HTTP Server.

  By default, the Apache HTTP Server is enabled for TLS use. For additional information on configuring the web server to use TLS, see the Apache SSL/TLS Encryption web page.

  OBM runs its Apache HTTP Server that by default uses port 443. The installation wizard checks whether port 443 is available, and generates a warning if it is already in use. You can change the port in the Connection Settings page of the configuration wizard.
- **Access to the OBM installation files.** The unpacked OBM 2020.10 installation files must be available on all systems that will host OBM.

  The installation package is named `OBM_<version>_for_Windows.zip` where version is 2020.10. Download the archive file to the system where you plan to install OBM, and extract all files from the archive.

Optional. Obtain certificates for OBM

Done: ☐

If your company uses a certificate authority (CA) that can generate certificates for OBM, request certificates that include the OBM server.

Check the OBM client system requirements

Done: ☐

- **Web browser configuration:**

  - The browser must be set to accept third-party cookies and allow session cookies.
  - The browser must be set to enable JavaScript execution.
  - The browser must allow pop-ups from the OBM application.
  - Internet Explorer users must:
    - Configure the caching mechanism to automatically check for newer versions of stored web pages (**Internet options > General > Browsing history > Settings > Temporary Internet Files > Check for newer versions of stored pages: Automatically**).
    - Enable the use of TLS 1.2 or later (**Internet Options > Advanced > Security**)
    - Turn off Compatibility View (in Internet Explorer 11 only)
- **Java Runtime Environment (JRE) configuration.** JRE must be configured to use TLS 1.2 or later (**Java Control Panel > Advanced > Advanced Security Settings**).
- **Fonts.** The following fonts must be installed:
  - Arial
  - Meiryo (for Japanese locales)
  - Malgun Gothic or Arial (for Korean locales)
  - SimHei or SimSun (for Simplified Chinese locales)
- **Screen resolution.** 1600x900 or higher (recommended); 1280x1024 (supported).

Check the network configuration requirements

Done: ☐

- **Network segments.** We recommend that all OBM servers, including the database server, are installed on hosts in the same network segment.

  If OBM servers are installed in multiple network segments, we highly recommend that the number of hops and the latency between the servers are minimal. Network-induced latency may cause adverse effects to the OBM application and can result in performance and stability issues. The network latency should remain below 5 milliseconds, regardless of the number of hops.
- **IPv6 and dual IP stack support.** You can install OBM on host systems that have either the IPv4 or the IPv6 protocol stack or both of them configured.

  Where both IP protocol stacks are configured, OBM uses IPv4 by default.

  To enable OBM operation on a host system that has only the IPv6 protocol stack configured, or to configure OBM to use IPv6 on a host system that has both IP protocol stacks configured, you must modify an appropriate OBM configuration file after OBM is installed. For information, see Enable OBM to use IPv6.
- **Firewalls.** Because OBM uses Java Remote Method Invocation (Java RMI) calls between servers, placing firewalls between OBM servers is not supported.

  If an operating system firewall is active on any OBM server (gateway or data processing server), a channel must be left open to allow all traffic between all OBM gateway or data processing servers.

  Additionally, to enable OBM users and data collectors to communicate with the OBM gateway servers, you must leave open the relevant ports depending on your OBM configuration. The required ports are typically 443 or 80, and 383. For details, see Port Usage.

Check the database requirements

Done: ☐

- **Remote instance configuration.** If you use a remote database instance, OBM can configure it for you or you can configure it directly in the database management system (for example, if your organization does not allow the usage of administrator credentials during setup).

  For detailed database requirements and instructions on creating database instances manually, see Workflow for Microsoft SQL Server deployment.

Check the installing user account requirements

Done: ☐

- **System-wide privileges.** The user account that is used for OBM installation must have administrative privileges on the host systems.

Plan the installation process

Done: ☐

Considerations

Before you begin to install OBM, consider the following:

- You can install and configure OBM in one of the following ways:
  - **Parallel installation and serial configuration.** You can run the installation for all servers (on all host systems) in parallel. The configuration wizard, however, must be run for a data processing server (DPS) first. This server becomes the primary DPS in OBM. It creates the certificates required for secure communication and stores them in the database. After you configure the primary DPS, continue with the configuration of the secondary data processing server (optional), and finally configure the gateway servers.

    For parallel installation and serial configuration, select the **Quit** option in the last page of the post-installation wizard. Such selection enables you to finish installing all OBM servers first and to configure them at a later time.
  - **Serial installation and configuration.** You can install and configure the OBM servers in a sequence. In this case, install and configure an OBM data processing server (DPS) first. This server becomes the primary DPS. Then install and configure OBM on the secondary data processign server (optional). Finally complete the deployment by installing and configuring the gateway servers. The wizard will direct you as to when to begin the installation on the gateway server.

    For serial installation and configuration, select the **Configure OBM** option in the last page of the post-installation wizard. Such selection automatically invokes the configuration wizard after the installation of each server.
- Installing OBM in the console mode (by using the `-console` command line option) is not supported on Microsoft Windows.
- If the anti-virus software is running locally, you can leave it running also during the installation. While you might receive an anti-virus warning, you can safely ignore it and proceed with the installation without taking any action.

- Modifying or repairing the installed OBM is not supported, therefore the Modify and Repair options are unavailable if the OBM installation wizard is invoked when OBM is already installed.

Prerequisites

Before you initiate the installation process, check the following:

- Ensure that no other installations or processes that require Windows Installer are running. If there are, OBM installation cannot complete and you must terminate it by clicking **Cancel** in the OBM installation wizard.

Install and configuration sequence

Depending on the preferred OBM installation and configuration sequence, proceed as follows:

- To install all OBM servers first and configure them afterward, do the following:
  a. On each system that will host either an OBM data processing server (DPS) or an OBM gateway server (GS), **start the installation wizard and install OBM 2020.10**.

     Do *not* proceed to perform a post-installation action at this point.

  b. On the system that will host the OBM *primary* DPS, **start the configuration wizard and configure OBM**.

  c. On each system that will host either the OBM *secondary* DPS or an OBM GS, **start the configuration wizard and configure OBM**.

     You can configure the secondary DPS and the gateway servers in parallel.
- To install and configure all OBM servers one by one, **start the installation wizard and install OBM 2020.10**, then manually **start the configuration wizard and configure OBM** once the installation is complete. Perform these actions in the following systems in sequence:
  a. Each system that will host an OBM data processing server (DPS)

     The DPS that is configured first becomes the *primary* DPS of your OBM deployment.

  b. Each system that will host an OBM gateway server (GS)

Start the OBM installation

Done: ☐

Invocation of the OBM installation is the same for data processing and gateway server in distributed deployment types. You can select the server type (and implicitly choose the deployment) in a dedicated page of the OBM installation wizard.

To start the installation, follow the steps on the staging host systems:

1. Open a Command Prompt window as an administrator.
2. Change the current directory as follows:

   ```
   cd <OBMInstallationFilesDirectory>
   ```

   Note

   You should not have any whitespaces when you enter the path.

3. To start the installation in the GUI mode (invoke the installation wizard), run the following command:

```
install
```

Choose the preferred language

Done: ☐

Your installer may offer additional languages. The language that you choose in the initial installer window is used for the installation wizard.

From the available drop-down list, select the preferred language for the installation wizard, and then click **OK**.

Note

Your selection does not affect the following:

- The language of the configuration wizard (it is determined automatically based on the operating system settings)
- The language used in the OBM console

Attend initialization of OBM installation

Done: ☐

During the initial phase the installation wizard checks the host system for the following:

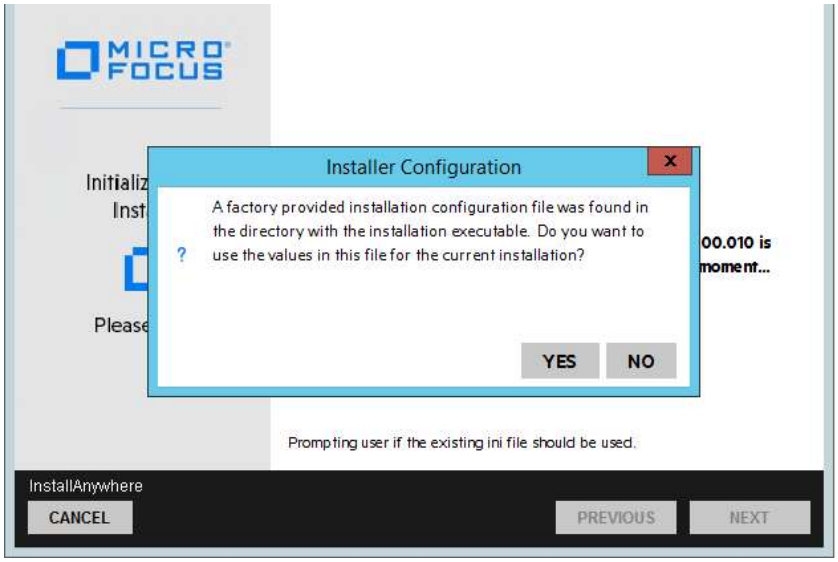
- Supported operating system
- Sufficient physical memory
- Sufficient free storage space at the location defined by the *%TEMP%* user environment variable

Installer Configuration

Done: ☐

During the OBM 2020.10 install initialization phase, installer configuration window displays if any settings from the previous installer are detected. Click **Yes** to proceed with the previous values. You can modify the previous values.

If you want to provide new values, click **No** and enter new values.



Read the introduction

Done: ☐

The **Introduction (Install)** page describes the installation wizard in general. Familiarize yourself with the information provided and then click **Next.**

Review the license agreement

Done: ☐

In the **Product Agreement (License Agreement)** page, accept the license agreement and click **Next** to continue with the installation. If you decline, the installation cannot proceed.

Choose the server type

Done: ☐

In the **Product Customization** page, select the OBM server type you want to install on the local system:

- **Gateway Server.** Installs the OBM gateway server.
- **Data Processing Server.** Installs the OBM data processing server.

Click **Next** to continue.

Specify the installation folders

Done: ☐

Select the following folders for the installation:

- Installation folder and data folder for the shared content.

  The following components are included in the shared content:

  - Certificate Management Client
  - Certificate Management Server
  - Cross Platform Component
  - Cross Platform Component Java
  - Graphing Component
  - HTTP Communication
  - HTTP Communication Java
  - Performance Access Java
  - Process Control
  - Security Core
  - Security Core Java

  Note

  - There is additional shared data in the *%ALLUSERSPROFILE%*\HP\BSM directory.

- Installation folder for the product-specific (OBM) content.

  The installation folder for OBM content must not exist yet, and the directory name that you specify must:

  - Be shorter than 16 characters
  - Contain only the following characters: a-z, A-Z, 0-9, underscore (_), hyphen (-), period (.), backslash (\), slash (/), and colon (:)
  - End with the HPBSM string

  If the requirements are not met, the installation wizard prompts you to give the folder a different name in the next step.

Note

If you are installing OBM onto a system running Windows Server 2008 R2, the following message may appear:

```
The installation folder for shared content
is not valid.
```

This may occur because you do not have administrative privileges on the system, which are necessary to install OBM. Check with your system administrator.

Click **Next**.

Review the product requirements

Done: ☐

While the **Product Requirements** page is visible, the installation wizard performs various checks if the system meets the requirements for installing OBM.

In the **Product Requirements** page, click **Next**.

Note

If a requirement check fails, review the warning message and revise the product requirements listed in this guide. After updating the problematic resource, click **Previous** and then **Next** to continue with the installation.

Initiate OBM installation

Done: ☐

In the **Pre-Install Summary** page, review the information and then click **Install** to start the installation.

Attend OBM installation

Done: ☐

While the **Installing** page is visible, attend the installation of OBM. The configuration starts running in the background silently. Wait until the configuration is complete.

Note

If some required VC libraries are used by another process, your system might be rebooted during the installation. Restart the installation wizard after the reboot to continue with the installation.

Complete the installation wizard

Done: ☐

In GUI mode, the configuration continues silently in the background. This process happens in the Post install phase. Wait until the configuration is complete.

When OBM is successfully installed, the installation wizard displays the **Install Complete (Installation Complete)** page with a summary of the installation process. After the configuration is complete, click **Done** to complete the installation.

If the configuration fails to complete silently, you can run the configuration wizard manually. For instructions, see *Start the configuration wizard manually*.

Choose the next step

Done: ☐

When the **Post-Install Configuration** page of the post-installation wizard appears, the installation is complete. In the subsequent **Next Steps** page, you can choose to upgrade or configure OBM, or quit to postpone the upgrade or configuration.

Select **Configure OBM** to configure OBM on this host system immediately. Select **Quit** to postpone the configuration of OBM to a later time.

After making a selection, click **Next**.

Start the configuration wizard manually

Done: ☐

You must specify the same database and connection parameters for each OBM server, regardless of whether the servers are at the same location or they are geographically separated.

You can modify any configuration settings at a later time. To change a setting, start the configuration wizard again.

Run the configuration wizard on primary DPS.

To start the configuration wizard manually, follow the steps:

1. If this is *not* the first time you are starting the wizard, disable OBM. Follow the steps below:

   For Windows Server 2008:

   Select **Start > Programs > Operations Bridge Manager > Administration > Disable Operations Bridge Manager**

   For Windows Server 2012:

   In Windows Search, start typing **Disable Operations Bridge Manager**, and then click **Disable Operations Bridge Manager** in the search results.

   Caution

   Modifying connection parameters for the Management, RTSM, and Event databases while OBM is enabled may cause data loss or severe integrity problems.

2. Do one of the following:
   - Start the wizard from the operating system desktop:

     In Windows Search, start typing **Configure Operations Bridge Manager**. Then click **Configure Operations Bridge Manager** in the search results.
   - Start the wizard from the command line:
     i. Open a Command Prompt window as an administrator.
     ii. Change the current directory as follows:

     ```
     cd <OBM_HOME>\bin
     ```

     iii. Run the following command:

     ```
     config-server-wizard.bat
     ```

Optional. Generate the database creation scripts

Done: ☐

During the configuration, OBM can do one of the following:

- Automatically set up new databases for you
- Connect to the existing databases that were created manually in advance.

  If you not have the required permissions in the remote database management system, you might want to ask the database administrator for assistance with database creation.

OBM requires the following databases:

- **Management.** For storage of system-wide and management-related metadata.
- **RTSM (Run-time Service Model).** For storage of configuration information that is gathered from various Micro Focus and third-party applications and tools.
- **Event.** For storage of events and related data, such as annotations, as well as for storage of configuration data, such as event correlation rules.

After the OBM installation, but *before* the configuration, generate the scripts on the gateway server to create the required objects for populating these databases. You (or the database administrator) must create the databases and then run the scripts in the database management system to create the required objects.

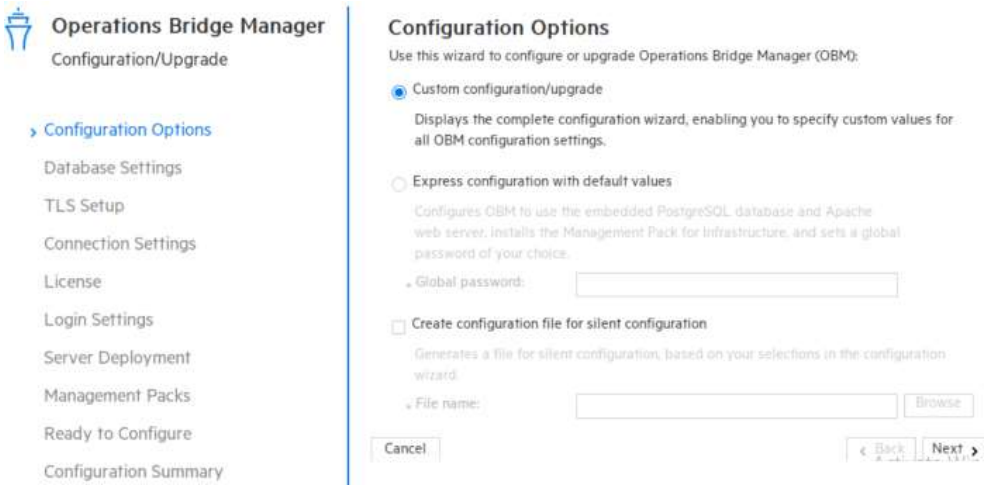
For details on how to install and configure a database management system, and to populate the databases with the required objects, follow the steps described in the *OBM Database Guide*.

Choose general configuration options

Done: ☐

This section is applicable for data processing server and gateway server.

After the configuration wizard starts, the **Configuration Options** page is displayed.



In the **Configuration Options** page, click **Custom configuration**. This option displays all wizard pages, enabling you to specify custom values for all OBM configuration settings. Then click **Next** to continue.

Configure the database settings

Done: ☐

This section is applicable for data processing server and gateway server.

In the **Database Settings** page, you can select the relational database management system you want to use with OBM, create new databases, or connect to existing ones.

Note

When entering database parameters, use only alphanumeric characters.

1. Choose whether you want to connect OBM to an already existing database or if you want OBM to

create a new database for you:

- **Connect to an existing database or user schema.** You generally use this option in the following scenarios:
  - When connecting to a database you manually created directly on the Microsoft SQL Server system.
  - When installing OBM in a distributed environment and running the utility on servers subsequent to the first server. In this case, you should have run the wizard on the data processing server first and on the gateway servers later.
- **Create a new database or user schema.** Use this option when you want OBM to create new databases for you on the Microsoft SQL Server system.
- **Upgrade database from a previous version of OBM.** Use this option when you want to upgrade OBM from previous version to the newer version.

2. Select **SQL Server**.
3. In the **Host** field, type the FQDN of the system where Microsoft SQL Server is installed. If you are connecting to a non-default Microsoft SQL Server instance in the dynamic mode, enter the following: *<FQDN>\<InstanceName>*.

   If you use a Microsoft SQL Server AlwaysOn Availability Group, enter the FQDN of the Availability Group Listener.

   If you use a Failover Cluster, enter the cluster server name.

   Caution

   There is a 26-character limit for the **Host** field while running the configuration wizard. If using a hostname without a domain name is not appropriate in your environment, perform one of these workarounds:

   - Use the IP address instead of the hostname in the **Host** field.
   - Map the hostname to the IP address in the `hosts` file. Use the hostname you mapped in the **Host** field.

4. The **Port** field automatically displays the Microsoft SQL Server's TCP/IP default port **1433**. Change the port number if one of the following applies:
   - If you connect to a named instance in the static mode, enter the port number.
   - If you connect to a named instance in the dynamic mode, change the port number to **1434**. This port can dynamically listen to the correct database port.

5. Choose the **Authentication** type you want to use for connecting to the Microsoft SQL Server database:

   - **Windows.** (on Microsoft Windows systems only) You can create and connect to a database using Windows operating system authentication instead of Microsoft SQL Server authentication. To do so, first ensure that the Windows user account running the OBM service has the necessary permissions to access the Microsoft SQL Server database. For information on adding a Windows user account to Microsoft SQL Server, see "Using Windows Authentication to Access Microsoft SQL Server Databases" in the OBM Database Guide.
   - **SQL Server.** The user name and password of a user with administrative rights on Microsoft SQL Server. A password must be supplied.

     For security reasons, we recommend not to use the default **sa** user.

6. *Optional.* Click **Use TLS** to encrypt the communication with Microsoft SQL Server.

   The Microsoft SQL Server must be running with TLS communication enabled and it must provide a certificate for use by OBM.

7. If you selected the option Use TLS, import the certificate of the database server or of the certificate authority that issued the database server certificates. Select one of the two options:

   - **Connect and import from server**

     Click **Retrieve Certificate** to import the certificate from the server.

   - **Import from file**

     Specify the path or click **Browse** to browse for the certificate file.

   Click **Test Connection** to test the connection using the imported certificate.

   Click **Next**.

8. OBM requires the following databases:

   - **Management.** For storage of system-wide and management-related metadata.
   - **RTSM (Run-time Service Model).** For storage of configuration information that is gathered from various Micro Focus and third-party applications and tools.
   - **Event.** For storage of events and related data, such as annotations, as well as for storage of configuration data, such as event correlation rules.

   Type a name for each database schema. The names must be unique even when the databases reside on different servers.

Distributed deployment: You connect to the databases that you created during the installation of the first data processing server. After you have connected to the Management database, by specifying the same connection parameters that you set during the installation of the first server, the connection parameters for the other databases appear by default. Not all databases appear when running on the gateway server.

9. Click **Next**.

Configure the TLS setup

Done: ☐

This section is applicable for data processing server and gateway server.

The **TLS Setup** page enables you to configure OBM to accept only secure connections to its web server and the JMX consoles.

If you do not want to use HTTPS (not recommended), clear the **Enable HTTPS** option.

Note

Your TLS setup should be consistent for every server.

If your company uses a certification authority (CA) that can generate certificates for OBM, click the **Upload certificates** option. Alternatively, click **OBM-generated certificates** to make OBM generate the certificates required for the configuration.

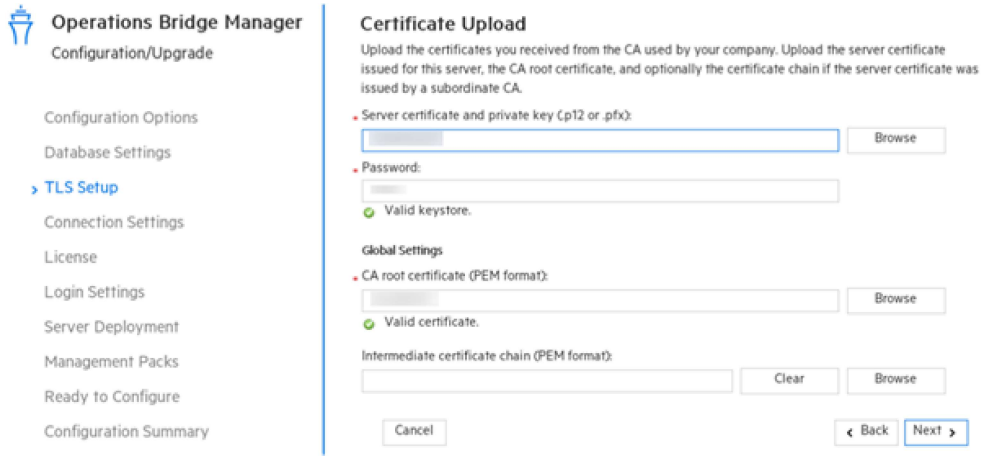
Note

For maximum security, we recommend to use certificates that were issued by the certification authority of your company.

If you choose to use OBM-generated certificates, the CA will be retained. Make sure to establish trust in the web browser from which you will log on to OBM. For

instructions on how to do that, see the Establish Trust in the Browser.

Recommended. Upload custom certificates



Proceed as follows:

1. Obtain server certificates from your CA.

   Generally, server certificates must be issued to the name of the external access point (FQDN) of OBM. This is the name that users and data collectors use to access OBM.

2. Make sure **Enable HTTPS** is selected.
3. Click **Upload certificates** and then click **Next**.
4. In the **Certificate Upload** page, specify the certificates you received from the CA used by your company:

   a. Specify the server certificate issued for the server you are currently configuring. The uploaded file must include both the certificate and private key and must be in .p12 or .pfx format.

   Enter the password for the `.p12` or `.pfx` file.

   b. Specify the CA root certificate (PEM format).

   c. *Optional.* Specify the certificate chain without the root CA if the server certificate was issued by a subordinate CA. The certificate file must be PEM-encoded. Click **Clear** to remove the selected file.

5. Click **Next** to continue.

Use certificates generated by OBM

Proceed as follows:

1. Make sure **Enable HTTPS** is selected.
2. Make sure **OBM-generated certificates** is selected and click **Next**.

3. *Optional.* In the **OBM Certificate Generation** page, you can customize the key options and contents of the certificates generated by the OBM CA. You can define certificate settings for the OBM root CA and for the OBM server for which the certificate is issued:
   - **Key length**: Size of the RSA key.
   - **Certificate validity (days)**: Time period after which the issued certificates will expire.
   - **Organization**: Legal name of your business or organization.
   - **Country**: Country where your business is registered with the government.
   - **Common name**: Name of the OBM CA that issues the certificates.
4. Click **Next** to continue.

Configure client certificate authentication

Done: ☐

This section is applicable on each gateway server.

The **Client Certificate Authentication** page enables you to configure OBM to require a client certificate when users log on to OBM or when web services connect to OBM. Depending on the deployment type, you can configure OBM to authenticate the client on the OBM web server or, if available, on the load balancer.

Caution

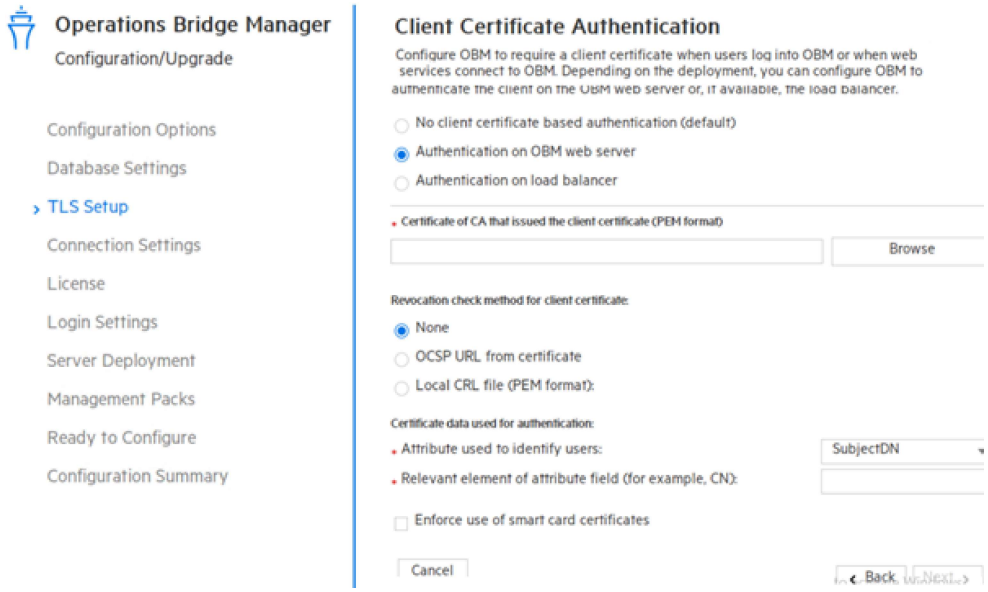
Do not enable client certificate authentication if you are configuring OBM for the first time. Before enabling client-certificate authentication, OBM must be already configured and the superuser must exist.

No client certificate based authentication (default)

Make sure the **No client certificate based authentication** option is selected if this type of security

is not required in your environment or if you want to configure client authentication later.

Authentication on OBM web server

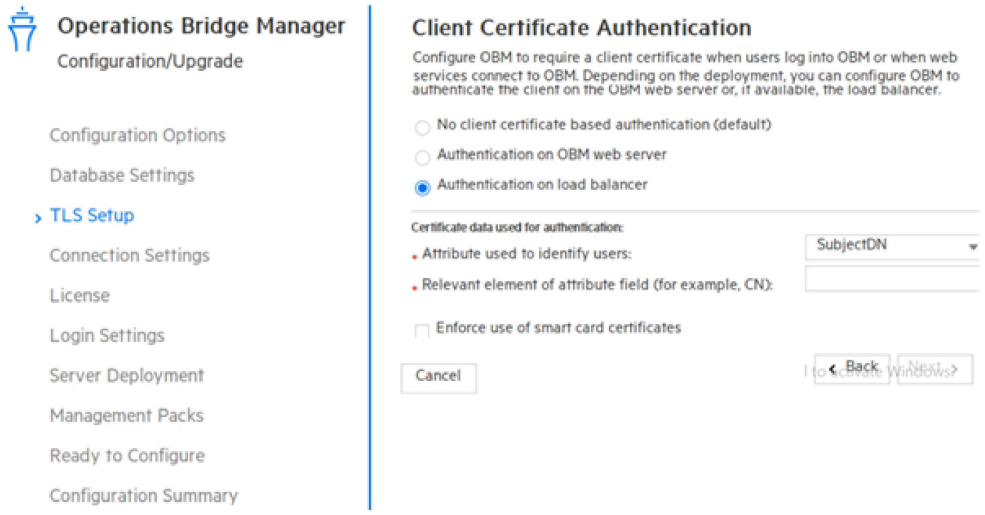


1. Click **Authentication on OBM web server**.
2. Select the certificate of the CA that issued the client certificate. The certificate file must be PEM-encoded.
3. Choose how OBM checks whether the client certificate has been revoked:
   - **None**: OBM does not check the revocation status.
   - **OCSP URL from certificate**: OBM sends an OCSP request to the URL provided in the client certificate and evaluates the OCSP response to determine the revocation status of the certificate.
   - **Local CRL file (PEM format)**: OBM checks the revocation status in a CRL file local to the gateway server. Make sure the CRL file on the gateway server is the latest one available from your CA.
4. Specify the certificate data that is used for authentication:
   - **Attribute used to identify users**: Use the drop-down list to select the attribute that OBM uses to identify users, for example **SubjectDN** or **SubjectAlternativeName**.
   - **Relevant element of attribute field (for example, CN)**: Specify the element of the attribute that OBM uses to identify users, for example **CN**.
5. *Optional.* Click **Enforce use of smart card certificates** to configure OBM to always require a

smart card when a user logs on.

6. Click **Next** to continue.

Authentication on load balancer



1. Click **Authentication on load balancer**.
2. Specify the certificate data that is used for authentication:
   - **Attribute used to identify users**: Use the drop-down list to select the attribute that OBM uses to identify users, for example **SubjectDN** or **SubjectAlternativeName**.
   - **Relevant element of attribute field (for example, CN)**: Specify the element of the attribute that OBM uses to identify users, for example **CN**.
3. *Optional.* Click **Enforce use of smart card certificates** to configure OBM to always require a smart card when a user logs on.
4. Click **Next** to continue.

Configure general OBM connection settings

Done: ☐

In the **Connection Settings** page, you can configure the URL that users use to access OBM.

Note

This section is applicable to each gateway server only. The configuration wizard displays the **Connection Settings** page only during configuration of a single-server or gateway server. The page is not shown during configuration of a data processing server.

Do the following:

1. Under **Web server**, enter the port for the web server that you want to use with your OBM deployment.

   OBM installs **Apache HTTP Server** on all gateway servers during the installation. By default, OBM runs Apache HTTP Server so that it listens on port 443 (HTTPS). Click **Check Port** to verify the connection to the web server. If the default port is already in use, specify a different port.

2. Under **OBM URL**, update the port number in the OBM URL text box if the default web server port is changed. An example of the updated URL is `https://obmweb.company.com:8000`.

   Note

   You cannot change the OBM URL in the configuration wizard after the initial configuration. Instead, change the setting **Default Virtual Gateway Server for Data Collectors URL** in **Infrastructure Settings > Foundations > Platform Administration**.

3. Click **Next**.

Configure the license

Done: ☐

This section is applicable for data processing server and gateway server.

In the **License** page, you can configure the license that OBM uses.

Depending on your recent actions, you have different options:

- If the wizard is running *for the first time*, you can choose to use the evaluation license or to upload your new license to the server.
- If this is *not the first time* the wizard is running, you can select to skip this step or upload additional licenses.

Note

The license file has the `.dat` file name extension and must reside at a local or network location accessible to the host system where the wizard is running.

Click **Next**.

Configure the login settings

Done: ☐

This section is applicable only for OBM data processing server.

In the **Login Settings** page, you can set the passwords for the OBM users.

OBM supports central user management and corporate password policies, it can communicate with the directory services by using LDAP. We recommend such configuration to enforce compliance of OBM user passwords with the respective security policy in your company. To configure the LDAP integration, navigate to **Administration > Users > Authentication Management** in the OBM user interface.

LDAP authentication of all users is possible only when the mixed mode authentication is disabled in the OBM LDAP infrastructure settings. For instructions on how to adjust this setting, see the "LDAP Authentication" section in Authentication Management.

To configure OBM passwords, specify the following options:

- **Administrator password, Confirm.** Type the password of the OBM administrator (user name: `admin`) for the OBM user interface. This password is required to log on to OBM, and can be changed in the OBM user interface at a later time.
- **JMX password, Confirm.** Type the password to be used by the OBM administrator for all OBM JMX consoles (user name: `admin`) and for the RTSM JMX console (user name: `sysadmin`). If there is a default password already present, re-enter the new password.

  Note

  The JMX password is valid on all host systems that constitute your OBM environment.

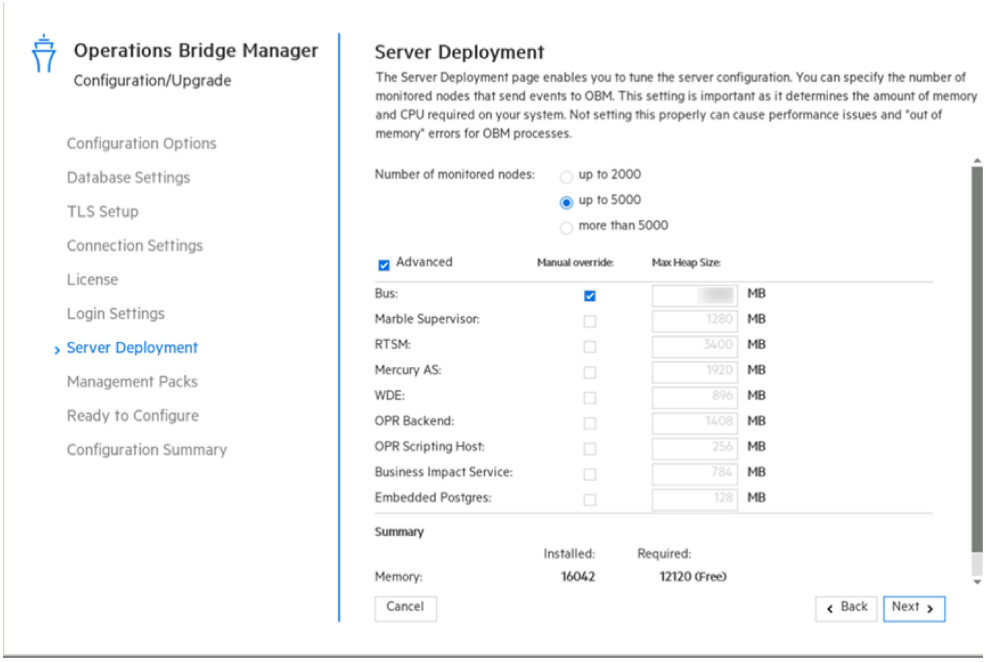
Click **Next**.

Configure the server deployment

Done: ☐

This section is applicable for data processing server and gateway sever.

In the **Server Deployment** page, you can define the size of your OBM deployment.



Note

When configuring a gateway server, modules and nodes cannot be configured because the selections are taken from the data processing server.

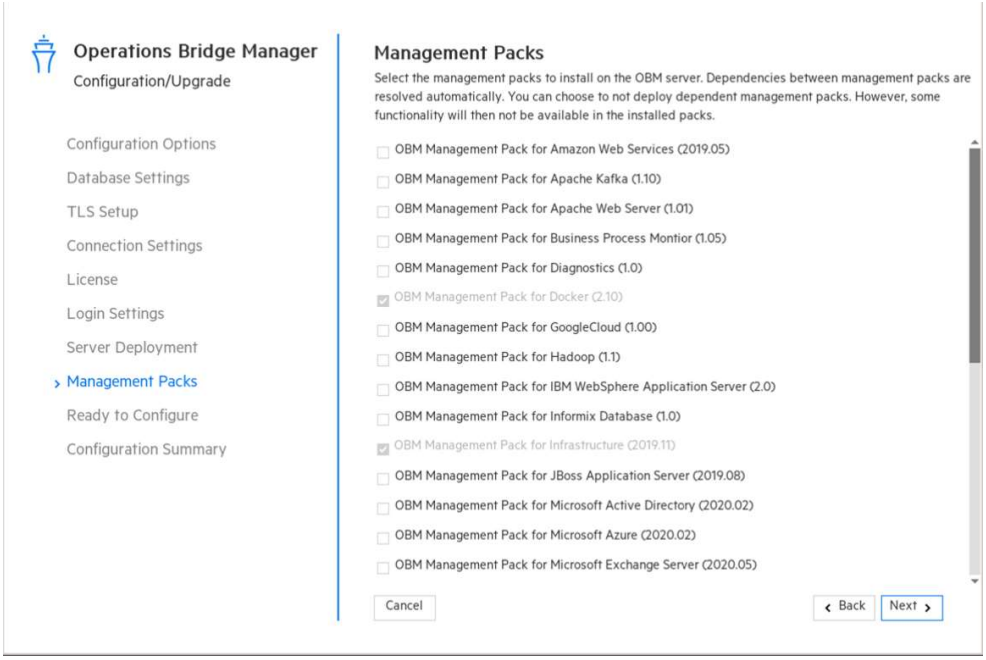
1. Select the **Number of monitored nodes** that send events to OBM. This includes all nodes that are present as CIs and that send events to OBM (for example, nodes connected to HP Operations Manager (OM), nodes sending events via other domain managers (For example: NNMi, SCOM, etc)
2. *Optional.* Click **Advanced** to adjust the maximum memory that the Java Virtual Machine (JVM) allocates to the OBM processes. To change the allocated memory, click **Manual override** and type the new values in the text boxes.
3. Click **Next**.

The required memory shown in the Configuration Wizard is calculated dynamically based on the memory that is given to all the processes which make up the OBM server. It also takes into account the overrides which a customer might do in the Advanced section. However, it does not include any other consumers of memory on the system, like the basic OS processes/services or CLIs which also need a considerable amount of the available memory. The memory requirements specified in *Check the hardware requirements* section take these into consideration and are therefore higher.

Deploy management packs

Done: ☐

In the **Management Packs** page, you can select additional OBM Management Packs to install in your OBM environment. Default Management Packs will be selected automatically. Dependencies between them are resolved automatically. You can choose not to install dependent management packs. However, if you do so, the functional scope of the selected management packs might reduce.



Management packs provide add-on content on top of OBM. They deliver automatic and end-to-end monitoring solutions of infrastructure and applications. Management packs enable users to monitor, detect, troubleshoot, and remediate issues in the IT domain. They increase the productivity of users by optimizing and automating various tasks, and reduce the mean time to resolve (MTTR) incidents.

Management packs discover application domains and proactively monitor the domains for availability and performance issues. They include, for example, management templates, aspects, policy templates, performances graphs, troubleshooting tools, auto remediation flows, and topology-based event correlation (TBEC) rules.

To install management packs after the first configuration, start the configuration wizard again and select the management packs you want to install. The list of management packs already installed are automatically selected and cannot be de-selected. With a distributed deployment, start the configuration wizard first on the data processing servers and subsequently on all gateway servers. Note though that the Management Packs page does not appear during the gateway server configuration.

Tip

We recommend to disable OBM before starting the configuration wizard, and to enable it after the configuration:

- Windows Server 2008:

  Select **Start > Programs > Operations Bridge Manager > Administration > Disable Operations Bridge Manager**.

- Windows Server 2012:

  In Windows Search, start typing **Disable Operations Bridge Manager**, and then click **Disable Operations Bridge Manager** in the search results.

Alternatively, use the `opr-mp-installer` command-line utility to install management packs without having to disable OBM. For more information, see `opr-mp-installer`.

The pre-selected management packs are selected on the source version of OBM. Once installed, management packs cannot be removed, even though their entries appear in the **Management Packs** page.

To verify the installed management packs on the production server, run the following command:

```
<OBM_HOME>/bin/opr-mp-installer -le
```

Note

To update a management pack to a later version than the one included with OBM, download its installation package from the ITOM Marketplace and install the management pack manually. You can also install additional management packs that are not bundled with OBM. However, such additions are not reflected in the OBM configuration wizard.

For more information about the management packs, see the management pack documentation.

Select the management packs that you want to install in your OBM environment and then click **Next**.

Ready to Configure

Done: ☐

This section is applicable on data processing server and gateway server.

The **Ready to Configure** page displays the current settings. Check whether your selections are correct. To change a setting, click **Edit**.

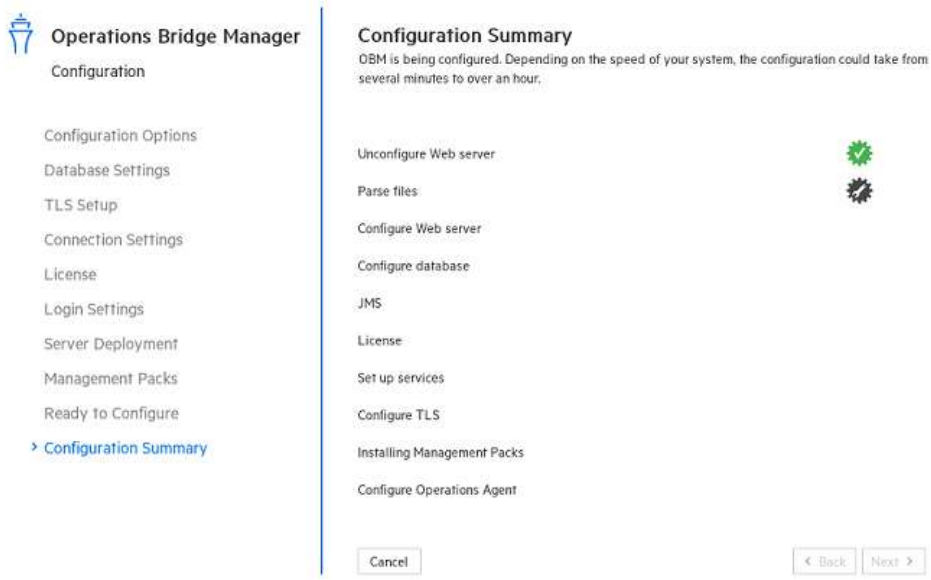
When you are ready, click **Next** to initiate the configuration actions.

Complete the configuration wizard

Done: ☐

This section is applicable for data processing server and gateway server.

After the configuration has been successfully applied, the configuration wizard displays a summary of the configuration changes. Click **Finish** to conclude the configuration.



Note

After running configuration wizard on the primary DPS, configure each gateway server and secondary DPS (if applicable). Enable the primary DPS, the gateways server(s) and the secondary DPS (if applicable).

You can use the following command to run the configuration wizard:

```
<TOPAZ_HOME>\bin\config-server-wizard.bat
```

Enable OBM

Done: ☐

Note

Instructions vary based on your deployment. Make sure to follow the procedure carefully before you start the services.

In a distributed environment, run the start command on the DPS first. Wait until the process is complete. After the DPS is fully up, enable the gateway server(s).

In an HA environment, run the start command on the primary DPS. Wait until the process is complete. After the primary DPS is fully up, enable the gateway servers and secondary DPS.

To enable OBM, do the following:

In Windows, select **Start > Applications >Enable Operations Bridge Manager**.

Note

You can also monitor the below log files:

```
<TOPAZ_HOME>\log\supervisor\nanny_all.log
```

```
<TOPAZ_HOME>\ucmdb\runtime\log\startup.log
```

The UCMDB pre-initializer takes a considerable amount of time when you start OBM services after installing for the first time. In BSM status page, the pre-initializer description is periodically updated to show the background task. The last modified time stamp is also shown on the DPS.

To check the BSM status, go to **Start > Programs > Operations Bridge Manager > Operations Bridge Manager Status.**

Note

Depending on what you used the configuration wizard for, perform the appropriate post-configuration action after the wizard completes:

- If you added a new gateway server or modified the previously defined database types or connection parameters:

  Restart all OBM servers and data collectors.

  Keep in mind that the My Workspace and Service Health pages are emptied and the OBM perspectives are removed.

- To restore the pages' contents and the perspectives, do the following:

  a. Navigate to the following directory:

  <GatewayServerRootDirectory>`/conf/uimashup/import`

  It contains two subdirectories: `/loaded` and `/toload`.

  b. Copy the contents of the `/loaded` directory into the `/toload` directory.

  c. Restart OBM services.

Log on to OBM

Done: ☐

You can log on to OBM from a supported web browser on a client system by using the Login page.

To access the OBM Login page and log on for the first time:

1. Import the CA certificate to the browser's trusted root certificate store:

   a. Make sure the web browser is configured to support TLS.

   b. Export the CA certificate from the OBM certificate inventory:

   ```
   <OBM_HOME>\bin\opr-cert-mgmt.bat -export "OBM Webserver CA Certificate" PEM
   "C:\ca_certificate.crt"
   ```

   If applicable, export the intermediate CA certificate:

   ```
   <OBM_HOME>\bin\opr-cert-mgmt.bat -export "OBM Webserver Intermediate CA
   Certificate 0" PEM "C:\ca_intermediate_certificate.crt"
   ```

   c. Import the CA certificate to the browser's certificate store:

   - Internet Explorer:

     Double-click the CA certificate file (`C:\ca_certificate.crt`, for example) and click **Install Certificate**. Make sure to select the **Trusted Root Certification Authorities** certificate store.

- Mozilla Firefox:

  Navigate to **Options > Privacy & Security > Certificates**. Click **View Certificates**. In **Authorities** tab, click **Import**. In the **Edit Certificate**, select the **This Certificate can identify websites** check box. Click **OK**.

d. Import the CA certificate to the truststore of the browser's JRE:

   i. Open the **Java Control Panel**. Open the **Security** tab and click **Manage Certificates**.

   ii. In the **Certificates** dialog box, select the certificate type **Secure Site CA** and click **Import**.

e. *Optional.* Disable TLS certificate revocation checks in the Java Control Panel.

   The Java console displays the following warning for OBM-generated certificates when the certificate revocation check cannot be performed:

   ```
   security: Failing over to CRLs: Certificate does not specify OCSP responder
   security: Revocation Status Unknown
   ```

   To avoid the warning, generate OBM self-signed certificates with an OCSP responder URL or disable the TLS certificate revocation checks in the Java Control panel:

   i. Open the **Java Control Panel** and then open the **Advanced** tab.

   ii. In **Perform TLS certificate revocation checks on**, click **Do not check (not recommended)**.

   Caution

   This will disable the revocation check for *all* TLS connections that are established by Java-based applications on this system.

2. In the web browser's address bar, enter the following URL:

   `http(s)://<FullyQualifiedDomainName>/obm`

   <FullyQualifiedDomainName> is the FQDN of the OBM server. If there are multiple servers, or if OBM is deployed in a distributed architecture, specify the gateway server URL.

3. Enter the default administrator user name (`admin`) and the password specified in the configuration wizard, and then click **Log In**. After logging in, the user name appears at the top right.

Note

- For the logon troubleshooting information, see Troubleshooting and Limitations.
- By default, single sign-on (SSO) logon is disabled. We recommend to use the default setting if no integrations are required for your installation. For details on this as well as other logon authentication strategies, see Authentication Management .

When you complete your session, we recommend that you log off from the website to prevent unauthorized entry. To log off from OBM, select **Logout** from the user menu ( ).

Optional. Review the log files, enable IPv6, Done: ☐

and configure Automatic Failover

Check the installation log files

The main installation log file and the additional installation log files for individual packages are created in the following directory on each OBM server:

`%TEMP%\..\MicroFocusOvInstaller\HPOMi_<BuildVersion>`

In the above instance, *%TEMP%* is a user environment variable.

File names are as follows:

- Main installation log file:

  `HPOMi_<BuildVersion>_<DateTime>_ MicroFocusOvInstallerLog.[html|txt]`

  (for example, `HPOMi_xx.xxx_MicroFocusOvInstallerLog.txt`).

- Installation log files for individual packages:

  `Package_<PackageType>_<PackageName>_install.log`

  (for example, `Package_msi_HPOMiDoc_install.log`).

The log files in /tmp are deleted as per configuration defined in /usr/lib/tmpfiles.d/tmp.conf, which is by default 10 days. You can modify the file to retain the log files for a required period of time. For example, to retain the log files for 30 days, modify the below entry in the file as follows:

```
v /tmp 1777 root root 30d
```

Check the startup log files

You can find the startup log file on all the servers at the following location:

`<OBM_HOME>\log\supervisor\nanny_all.log`

`<OBM_HOME>\ucmdb\runtime\log\startup.log`

Check the post-installation log file

You can find the post-installation log file on all the servers at the following location:

`<OBM_HOME>\log\configserver\postinstall_all.log`

Check the configuration log file

You can find the configuration log file on all the servers at the following location:

`<OBM_HOME>\log\configserver\configserver_all.log`

Check the certificates

During the configuration of OBM, the gateway server sends a certificate request to the data processing server to be granted after startup. To check whether the gateway and data processing servers trust each other, run the following command on each server:

`%ovinstalldir%/bin/win64/bbcutil -ping https://<GatewayOrDataProcessingServer>`

Configure Automatic Failover

To make sure that OBM functions properly in the event of a primary data processing server failure, the backup data processing server can take over.

To ensure that services are automatically reassigned to the backup DPS, you must define the backup DPS in the JMX console and enable automatic failover in the Infrastructure Settings. For details, see High Availability for the Data Processing Server.

Enable OBM to use IPv6

Note

Completing the procedure in this section is *mandatory* on host systems with only the IPv6 protocol stack and *optional* on host systems with both IPv4 and IPv6 protocol stacks configured.

To enable OBM operation on a host system that has only the IPv6 protocol stack configured, or to configure OBM to use IPv6 on a host system that has both IP protocol stacks configured, enable the use of IPv6 manually as follows:

1. Make sure the local `hosts` file contains the following line:

   ```
   127.0.0.1 localhost
   ```

2. Run the following commands in sequence:

   ```
   %ovdatadir%\bin\ovconfchg -ns sec.cm.server -set IsIPV6Enabled TRUE
   ```

   ```
   %ovdatadir%\bin\ovc -kill
   ```

   ```
   %ovdatadir%\bin\ovc –start
   ```

3. If OBM uses IPv6 on a host system that has only the IPv6 protocol stack configured, to enable its communication with non-OBM host systems that have both IP protocol stacks configured, configure your DNS server so that it resolves host names only to IPv6 addresses.

Recommended. Connect data providers

Done: ☐

For more information on the integrations, see the Integrations section in Operations Bridge Manager (OBM) community pages of the ITOM Marketplace website.

For details on supported integration versions, see the following document:

Support Matrices for Operations Center products

Connect Operations Agents

To connect an agent-monitored system to OBM, first ensure that the Operations Agent is installed on that system, then connect the agent to OBM, and finally grant the required certificates in OBM. For more information on connecting Operations Agents, see Connect Operations Agent to OBM.

Connect an Operations Manager server

Operations Manager (OM) can be integrated into your OBM environment to become a data provider for OBM.

After you have installed both OBM and OM, follow the procedures documented for the OBM / OM integration in the *OBM Integrations Guide* to connect OBM and OM. This connection enables bi-directional synchronization of events between the two systems, tool execution, and instruction text retrieval. The connection configuration requires you to configure a connected server for OM in OBM, to establish a trust relationship between OBM and the OM systems, and to configure a message forwarding policy.

Connect a SiteScope server

SiteScope is an agentless monitoring solution that enables you to remotely monitor the availability and performance of your IT infrastructure (for example, servers, operating systems, network devices, network services, applications, and application components). For more information on connecting SiteScope servers to OBM, see "Integrations" in the OBM Integrations Interactive documentation.

Connect an Network Node Manager i server

The NNMi-OBM integration forwards NNMi management event incidents as SNMPv2c traps to the Operations Connector on the NNMi management server. The Operations Connector filters the NNMi traps and forwards them to OBM.

The NNMi-OBM integration can also forward the SNMP traps that NNMi receives to the Operations Connector.

In addition, the NNMi-OBM integration provides the NNMi console for access from within the OBM event browser.

For information on configuring the NNMi-OBM integration, see "Integration" in the OBM Integrations Interactive documentation.

Connect a third-party management tool through Operations Connector

Operations Connector (OpsCx) is a component of Operations Bridge Manager that enables you to collect data from third-party and Micro Focus management tools (typically enterprise management systems) into OBM. You can integrate events, metrics, and topology data.

Third-party management tools are not provided by Micro Focus (for example, Microsoft System Center Operations Manager, Nagios, and Zenoss). Operations Connector also works with some Micro Focus applications (for example, ArcSight Logger, Network Node Manager i, and Systems Insight Manager).

For information on configuring the OBM-Operations Connector integration, see the Operations Connector documentation.

You can download Operations Connector implementations for third-party management tools from the Operations Bridge Manager community pages of the ITOM Marketplace website.

Connect Application Performance Management

For information on integrating Application Performance Management (APM) with OBM, see the OBM Integrations Interactive documentation.

Optional. Connect trouble ticket, automation, and reporting tools

Done: ☐

For more information on the integrations, see the Operations Bridge Manager (OBM) community pages of the ITOM Marketplace website.

For details on supported integration versions, select **Operations Bridge Manager** from the product list in the following document:

Support Matrices for Operations Center products

Connect Service Manager or other trouble ticket tools

The Service Manager integration enables you to forward events from OBM to Service Manager. Forwarded events and subsequent event changes are synchronized back from Service Manager to OBM. You can also drill down from OBM events to Service Manager incidents.

For information on configuring the OBM-Service Manager integration, see the OBM / SM integration in the OBM Integrations Interactive documentation.

OBM also supports integrations with third-party trouble ticket systems, for example BMC Remedy Action Request System or ServiceNow.

Connect Operations Orchestration or other automation tools

Operations Orchestration (OO) provides a simple way for users to run scripts for automatic actions. The integration with OBM uses the OO capabilities for building investigation tools or service remediation scripts, providing the operators with a simple way to validate a problem, investigate it, or automatically correct it. A run book can be executed manually. OO run books can be launched from the Service Health and Event Browser applications.

For information on configuring the OBM-Operations Orchestration integration, see "Integration" in the OBM Integrations Interactive documentation.

OBM also supports integrations with third-party automation tools, for example xMatters.

Connect Operations Bridge Reporter

Operations Bridge Reporter is business service-driven IT reporting software that provides resource and response time reporting across server and application environments. It consolidates resource metrics, response time data, and business service topology data to enable a unique understanding and perspective on the behavior of dynamic virtualized IT infrastructure and the way it impacts end users. With patterns illustrated across applications, you can plan activities to optimize the performance of your business services to meet or exceed requirements.

For information on configuring the OBM-Operations Bridge Reporter integration, see the Operations Bridge Reporter Integrations Guide.