



Microsoft®

# System Center Operations Manager

## **Guide to Microsoft System Center Management Pack for Azure SQL Database – Managed Instance**

---

Microsoft Corporation

Published: February 2018

The Operations Manager team encourages you to provide any feedbacks on the management pack by sending them to [sqlmpsfeedback@microsoft.com](mailto:sqlmpsfeedback@microsoft.com).

# Copyright

---

This document is provided "as is". Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

© 2018 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Windows, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

# Contents

---

Guide to Microsoft System Center Management Pack for Azure SQL DB Managed Instance.....	4
Changes History .....	4
Get Started .....	4
Basic Provisions .....	4
Management Pack Scope .....	5
Supported Configurations .....	5
Files in This Management Pack.....	5
Mandatory Configuration .....	5
Management Pack Purpose .....	21
Monitoring Scenarios.....	22
How Health Rolls Up.....	22
Configure the Management Pack .....	23
Best Practice: Create a Management Pack for Customizations .....	23
How to Import a Management Pack .....	24
Security Configuration .....	24
View Information in the Operations Manager Console.....	24
Version-Independent (Generic) Views and Dashboards .....	24
Azure SQL DB Managed Instance Views.....	25
Appendix: Known Issues and Troubleshooting.....	26

# Guide to Microsoft System Center Management Pack for Azure SQL Database – Managed Instance

---

This guide is based on version 1.0.0.0 of the Management Pack for Microsoft Azure SQL DB Managed Instance.

## Changes History

Release Date	Changes
February 2018 (version 1.0.0.0)	Original release of this management pack

## Get Started

In this section:

- [Basic Provisions](#)
- [Management Pack Scope](#)
- [Supported Configurations](#)
- [Files in This Management Pack](#)
- [Mandatory Configuration](#)

### Basic Provisions

Microsoft Azure SQL DB Managed Instance management pack is designed to monitor Azure SQL Database Managed Instance and the corresponding entities by means of T-SQL queries. Azure SQL DB Managed Instance is an automatically managed cloud instance running within Azure SQL Database cloud service.

## Management Pack Scope

Management Pack for Microsoft Azure SQL DB Managed Instance enables the monitoring of the following features:

- Azure SQL DB Managed Instance Database Engine
- Azure SQL DB Managed Instance Database
- Azure SQL DB Managed Instance Memory-Optimized Data
- Azure SQL DB Managed Instance Resource Pool

Please refer to “[Monitoring Scenarios](#)” section for a full list of monitoring scenarios supported by this management pack.

For more information and detailed instructions on setup and configuration, see “[Configure the Management Pack](#)” section of this guide.

## Supported Configurations

This management pack is tested on the following versions of System Center Operations Manager:

- System Center Operations Manager 2012 R2
- System Center Operations Manager 2016

## Files in This Management Pack

The Management Pack for Microsoft Azure SQL DB Managed Instance includes the following files:

- Microsoft.Azure.ManagedInstance.Discovery.mbp
- Microsoft.Azure.ManagedInstance.Library.mbp
- Microsoft.Azure.ManagedInstance.Views.mpb
- Microsoft.Azure.ManagedInstance.Monitoring.mbp
- Microsoft.SqlServer.Visualization.Library.mpb

## Mandatory Configuration

To configure Management Pack for Microsoft Azure SQL DB Managed Instance complete following steps:

- Review the “[Configure the Management Pack](#)” section of this guide.

- Grant the required permissions as described in “[Security Configuration](#)” section of this guide.
- Import the management pack.
- Associate Azure SQL DB Managed Instance Run As profiles with accounts that have appropriate permissions. For more information about configuring Run As profiles see “[How to Configure Run As Profiles](#)” section of this guide.

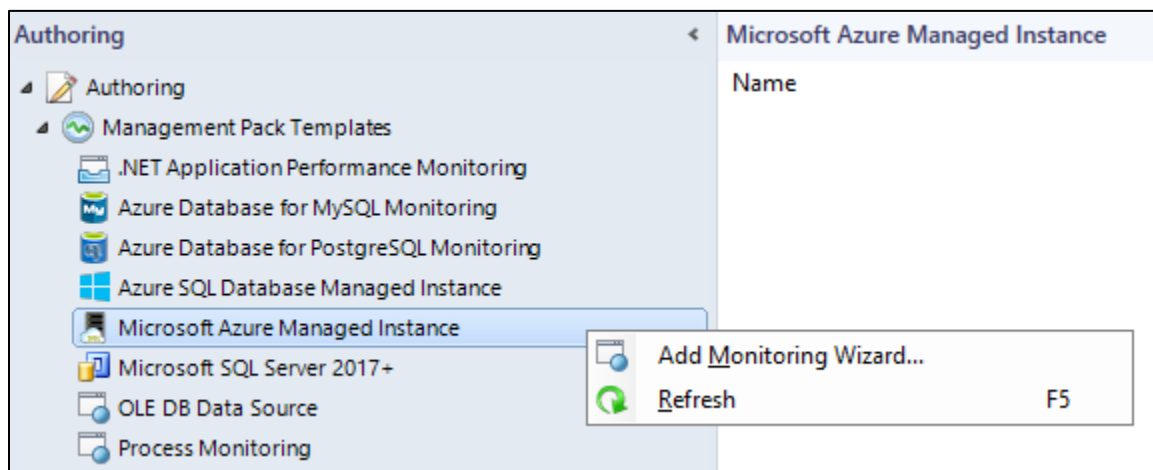
 **Important**

- A dedicated Operations Manager management group is not required for this management pack.
- Installation of .NET Framework 4.5 and newer is required.
- The management pack provides agentless monitoring only.
- Low-Privilege security configuration is not supported in this preview version.

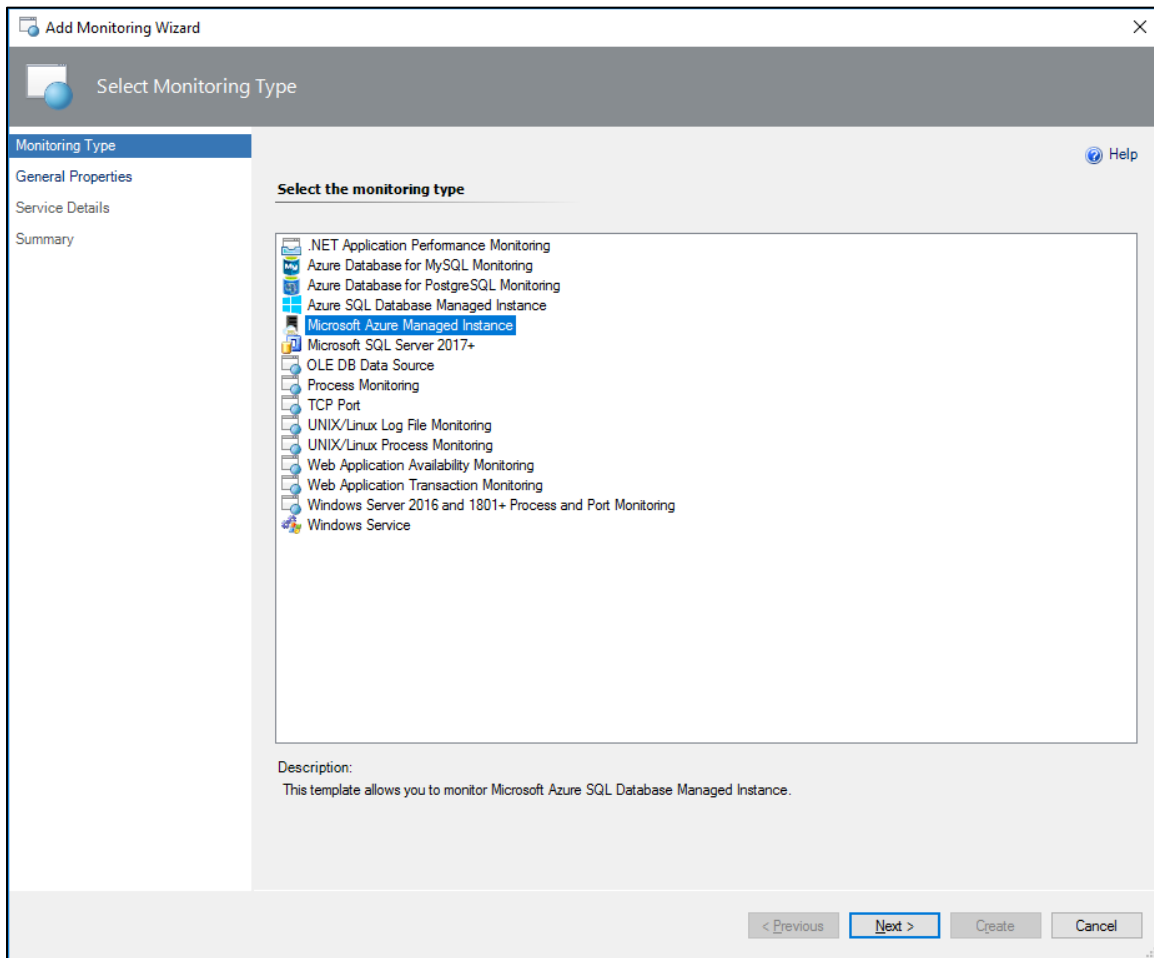
### Configure Monitoring by Add Monitoring Wizard

To begin monitoring of Managed Instances, perform the following steps:

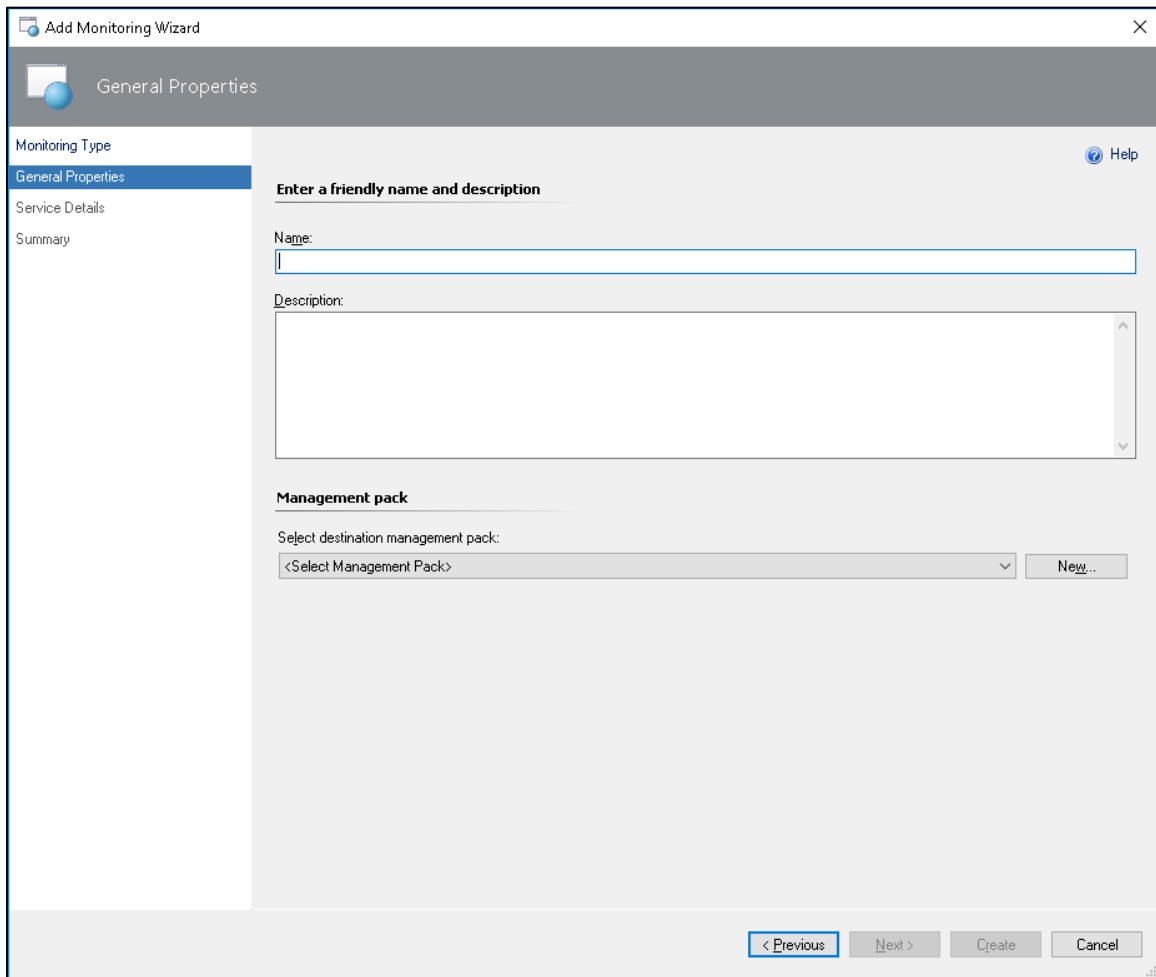
In the Operations Manager, navigate to **Authoring | Management Pack Templates**, right-click **Microsoft Azure Managed Instance** and select **Add Monitoring Wizard...**



In **Monitoring Type** window, select **Microsoft Azure Managed Instance** and click the **Next** button.

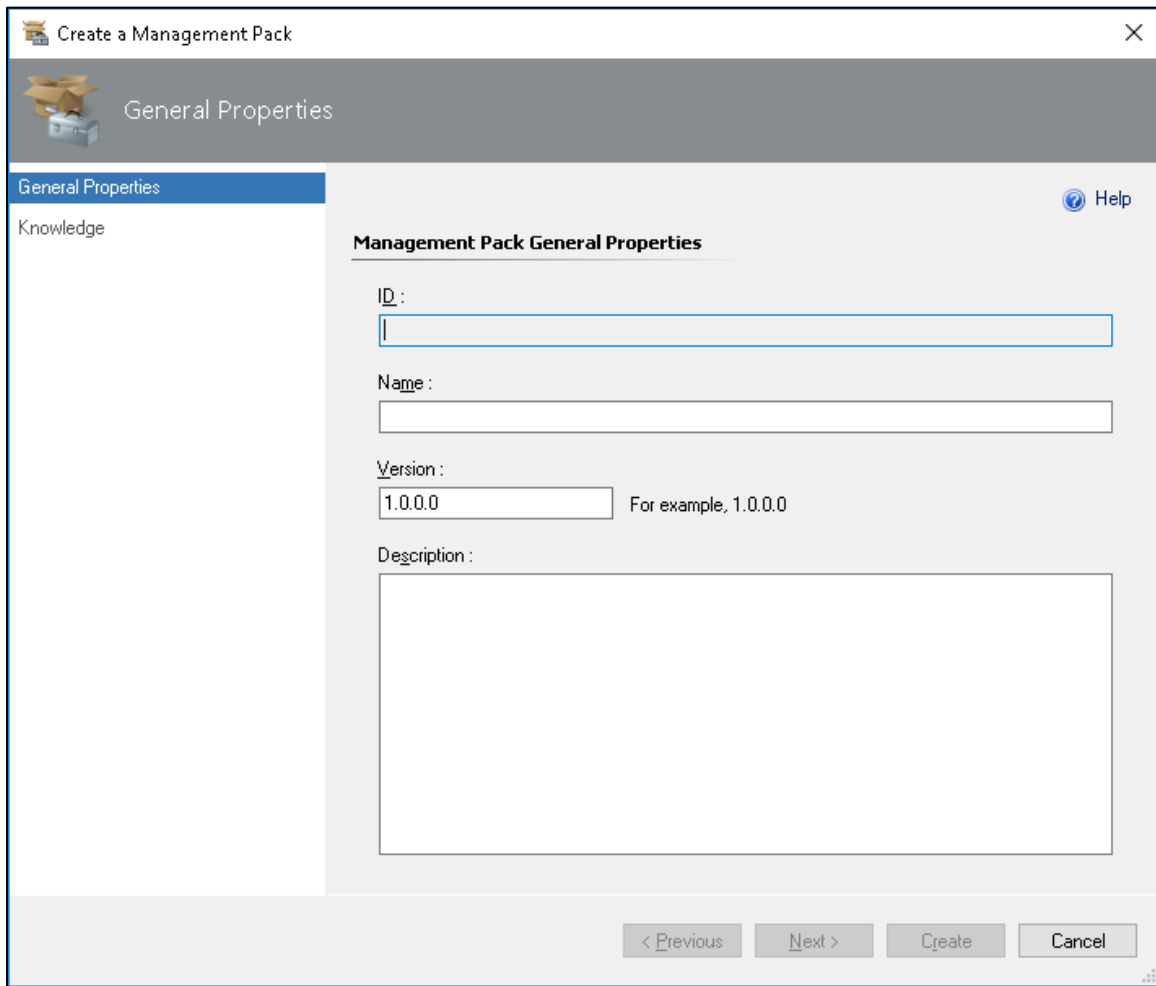


In the **General Properties** window, provide a **Name** and **Description** for your template, as well as **Select destination management pack** where the template will be stored.

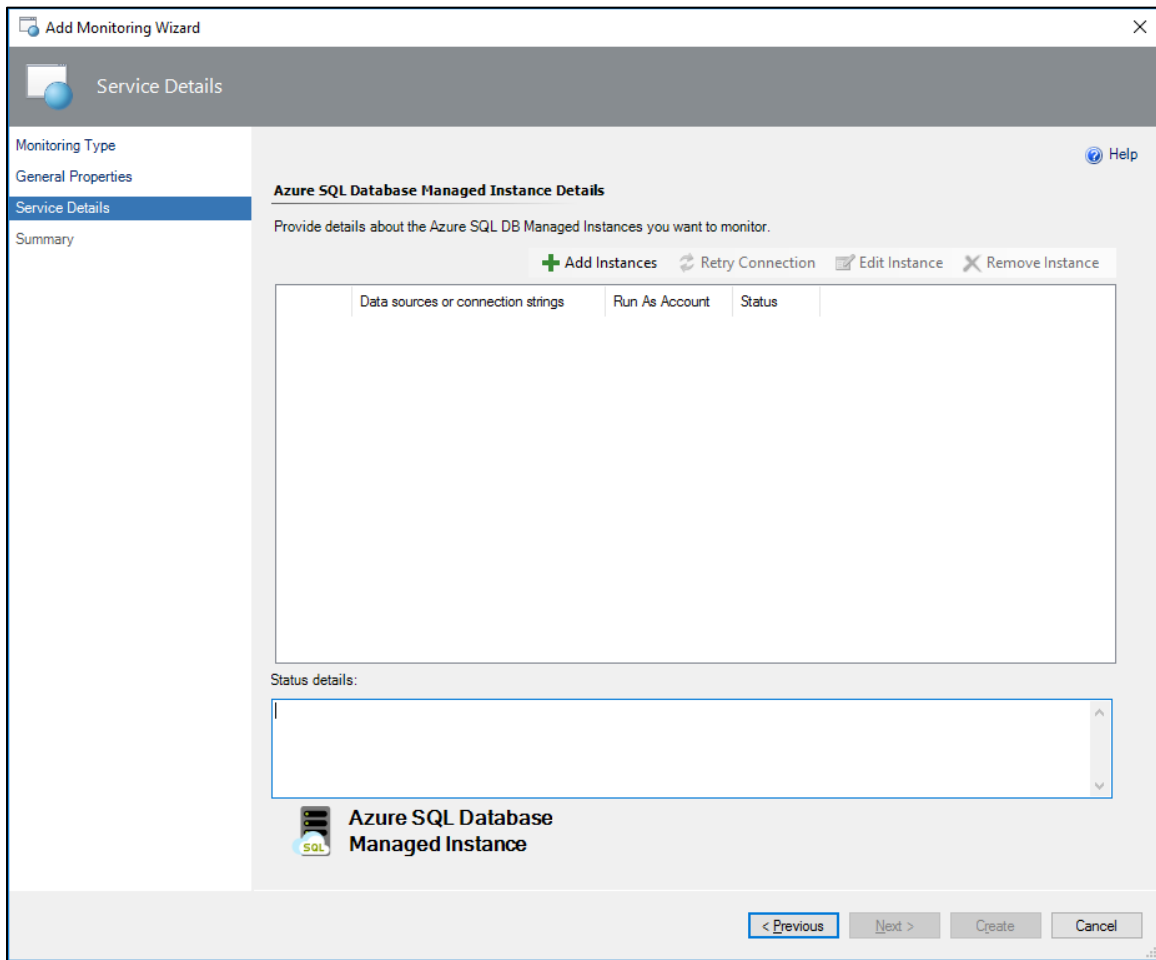


You can also create a new destination management pack by clicking the corresponding button.

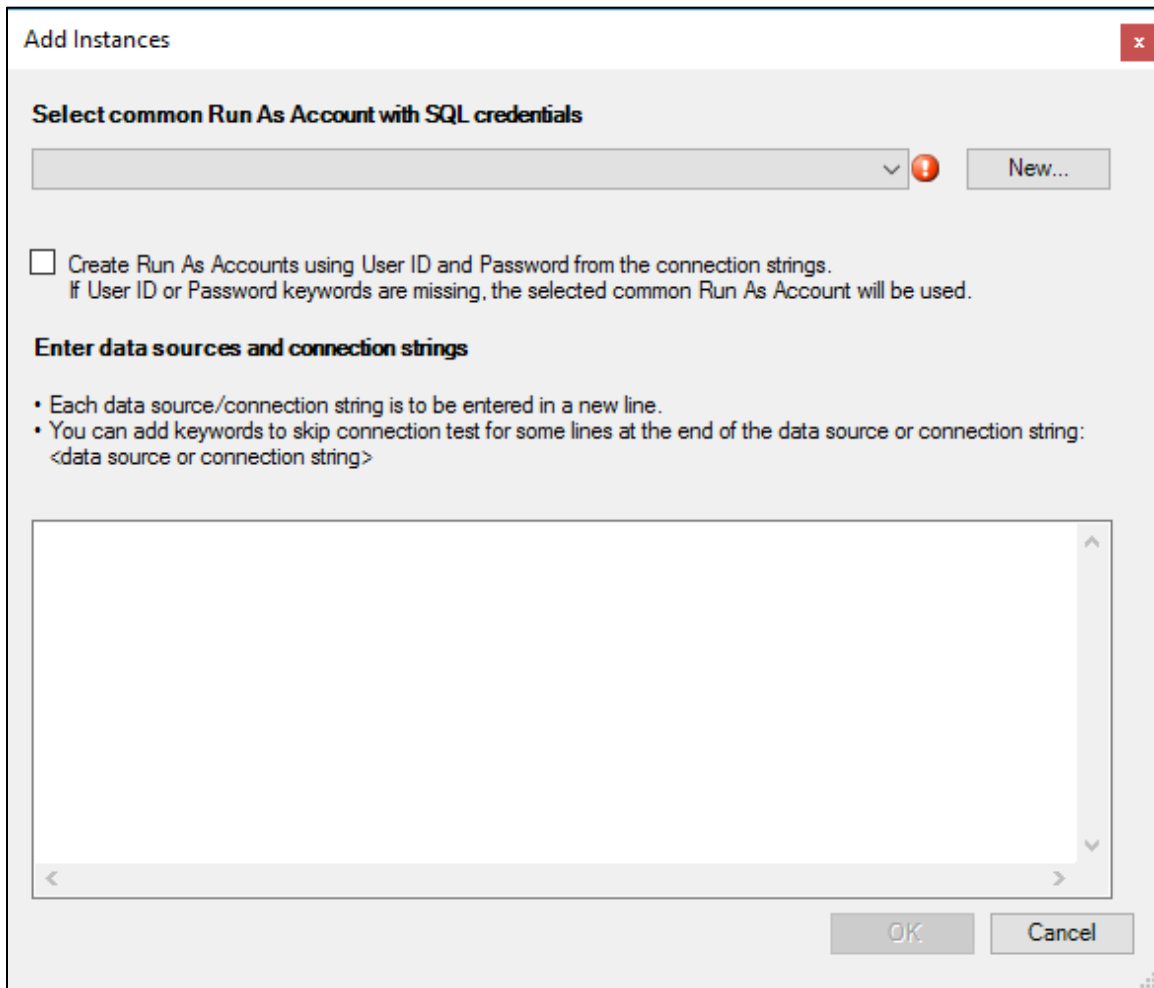




In the **Service Details** window, you should provide the corresponding details about the instances you want to monitor.



Click the corresponding button to **Add Instances** for monitoring.



In this window, select a common Run As Account with appropriate SQL credentials. Then, enter the data sources and (or) connection strings. Please, follow the instructions provided in this window to avoid errors.

The data is to be entered in the Standard Security connection string format:

```
Server=<ServerAddress>;Database=<DatabaseName>;
```

*For instance: Server=testServer.database.windows.net;Database=master;*

If you would like to create a Run As account from the connection string, then use the following format:

```
Server=<ServerAddress>;Database=<DatabaseName>;User Id=<UserName>;Password=<Password>;
```

**Note**

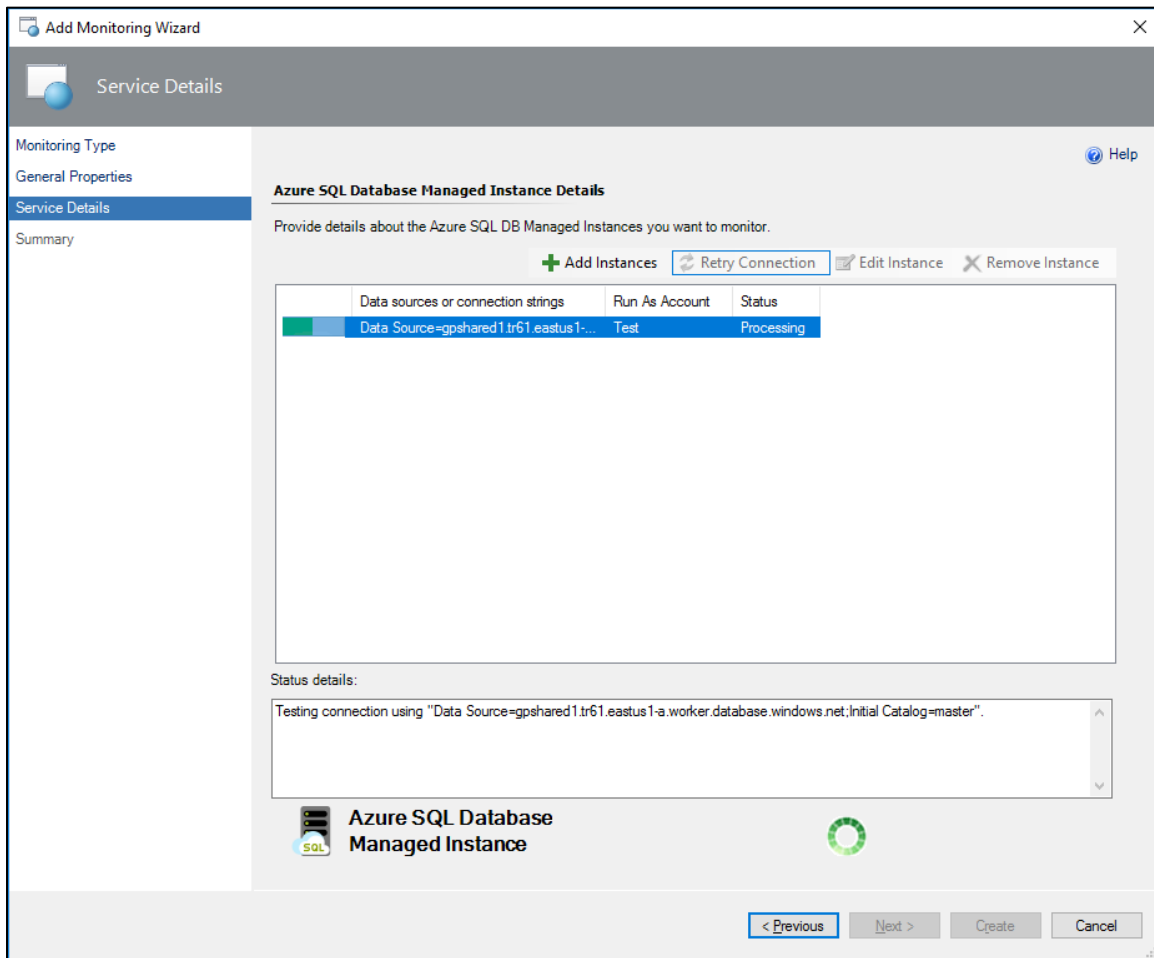
Low-Privilege security configuration is not supported in this preview version. You should grant the Run As account with SA permissions.

You can also create a new Run As account by clicking the **New...** button.

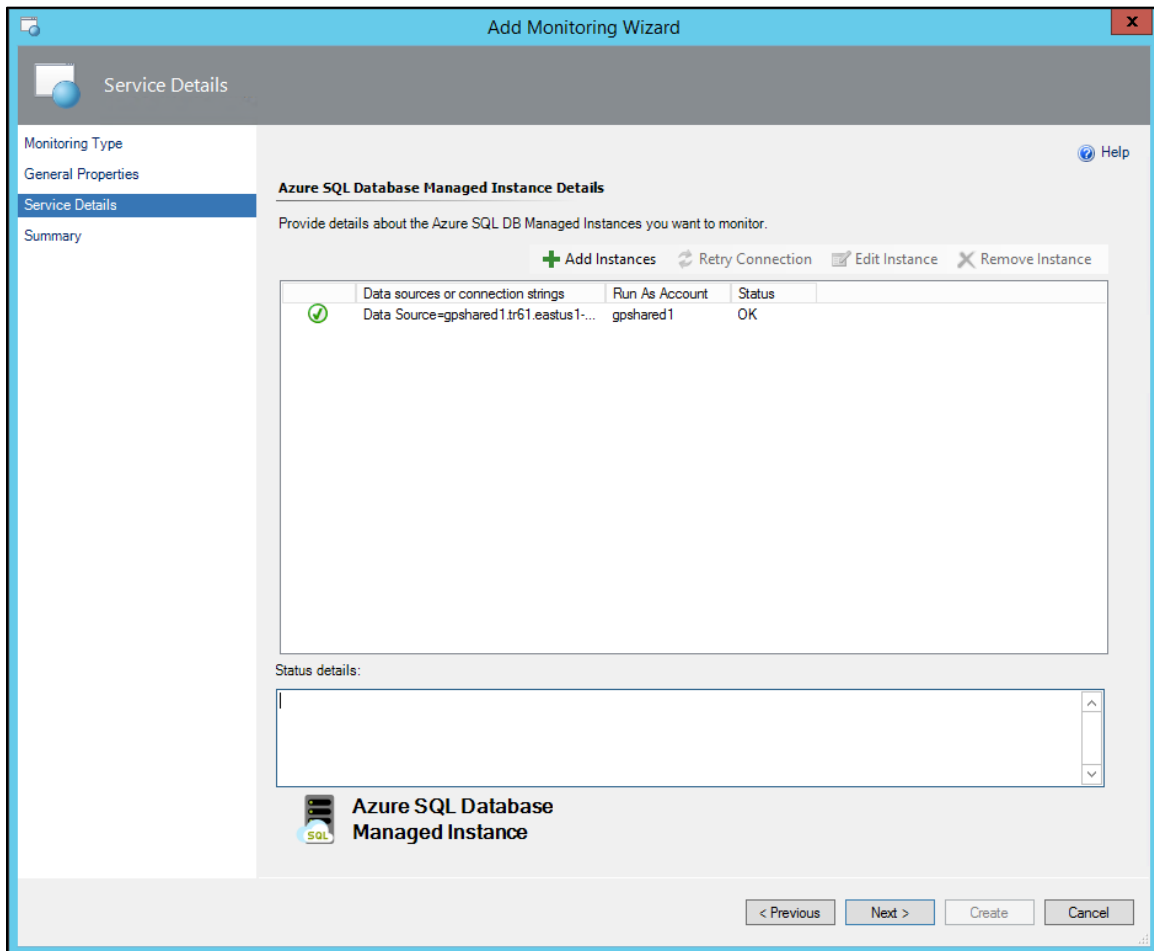
The screenshot shows a dialog box titled "Create new Run As Account". It features a close button (X) in the top right corner. The dialog contains four text input fields: "Account name:", "Login:", "Password:", and "Confirm password:". A red warning icon is positioned to the right of the "Account name:" field. At the bottom of the dialog are "OK" and "Cancel" buttons.

In the corresponding window, enter an account name and connection credentials for your Managed Instance.

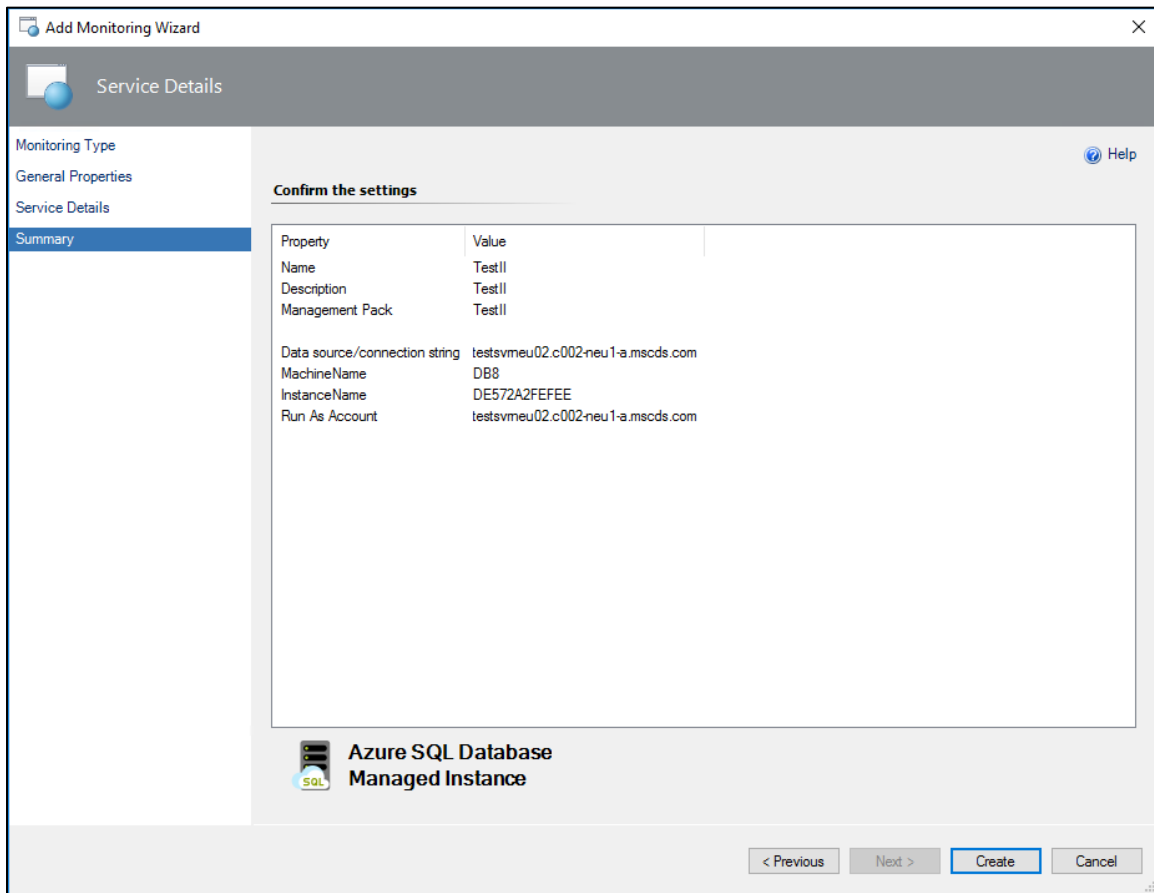
After clicking the **OK** button in **Add Instances** window, testing of the connection to the selected instance will be performed.



When the connection testing is completed, you can view and edit properties of the added instance. To do that, select the instance and click the **Edit Instance** button.



In **Summary** window, you can view you monitoring settings and confirm them by clicking the **Create** button.



After that, your monitoring template will be successfully created.

### Configure Azure SQL DB Managed Instance Monitoring Pool

The monitoring pool is available for configuration in the Operations Manager. To configure the monitoring pool, navigate to **Administration | Resource Pools**, right-click **Azure SQL DB Managed Instance Monitoring Pool** in the list of Resource Pools and check **Manual Membership** option. Then, select **Properties** action. As a result, **Azure SQL DB Managed Instance: Monitoring Pool Properties** window will be displayed.

Azure SQL DB Managed Instance: Monitoring Pool Properties

Enter the Name and Description for the Resource Pool

General Properties

Pool Membership

Summary

Completion

**Enter a friendly name and description**

Name:

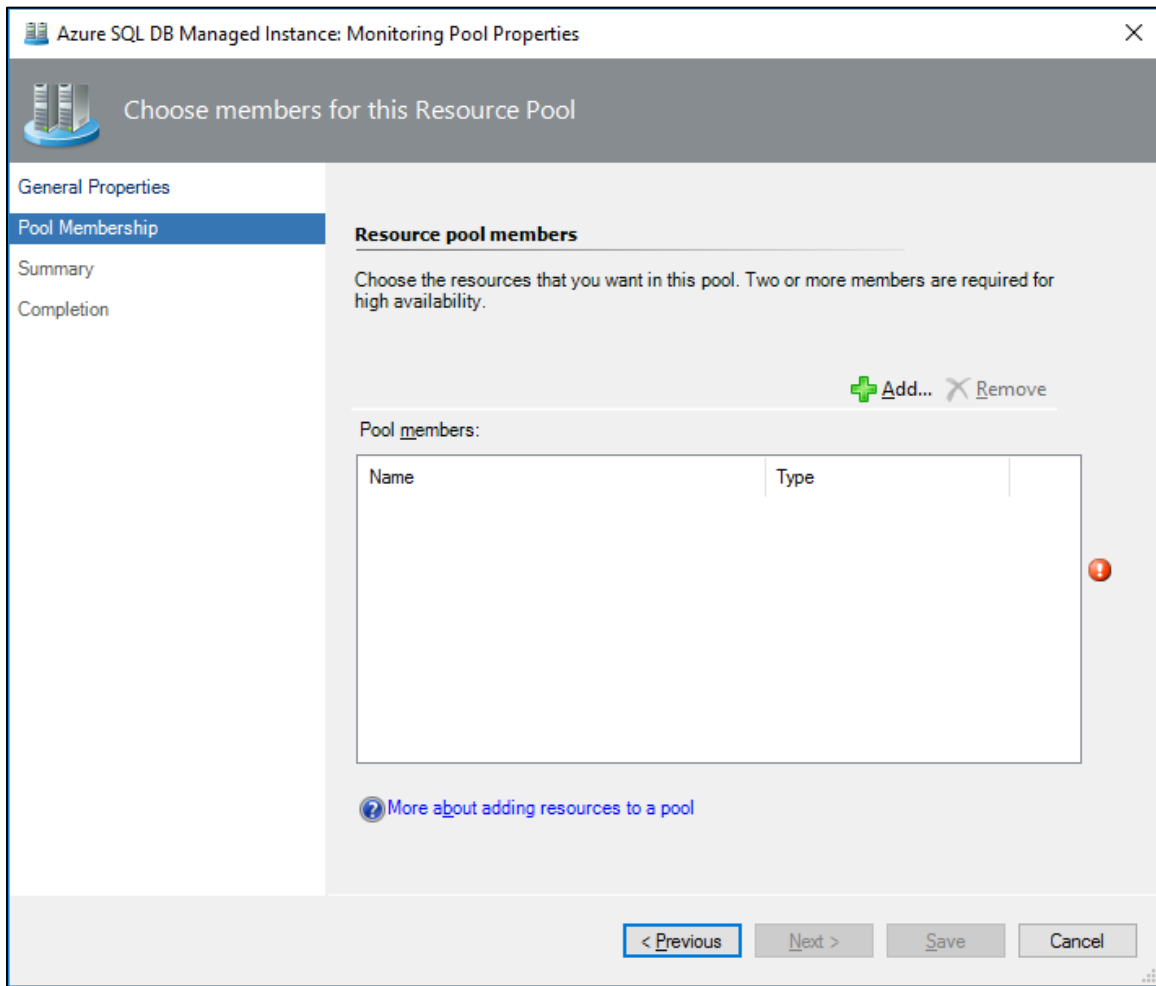
Azure SQL DB Managed Instance: Monitoring Pool

Description (optional):

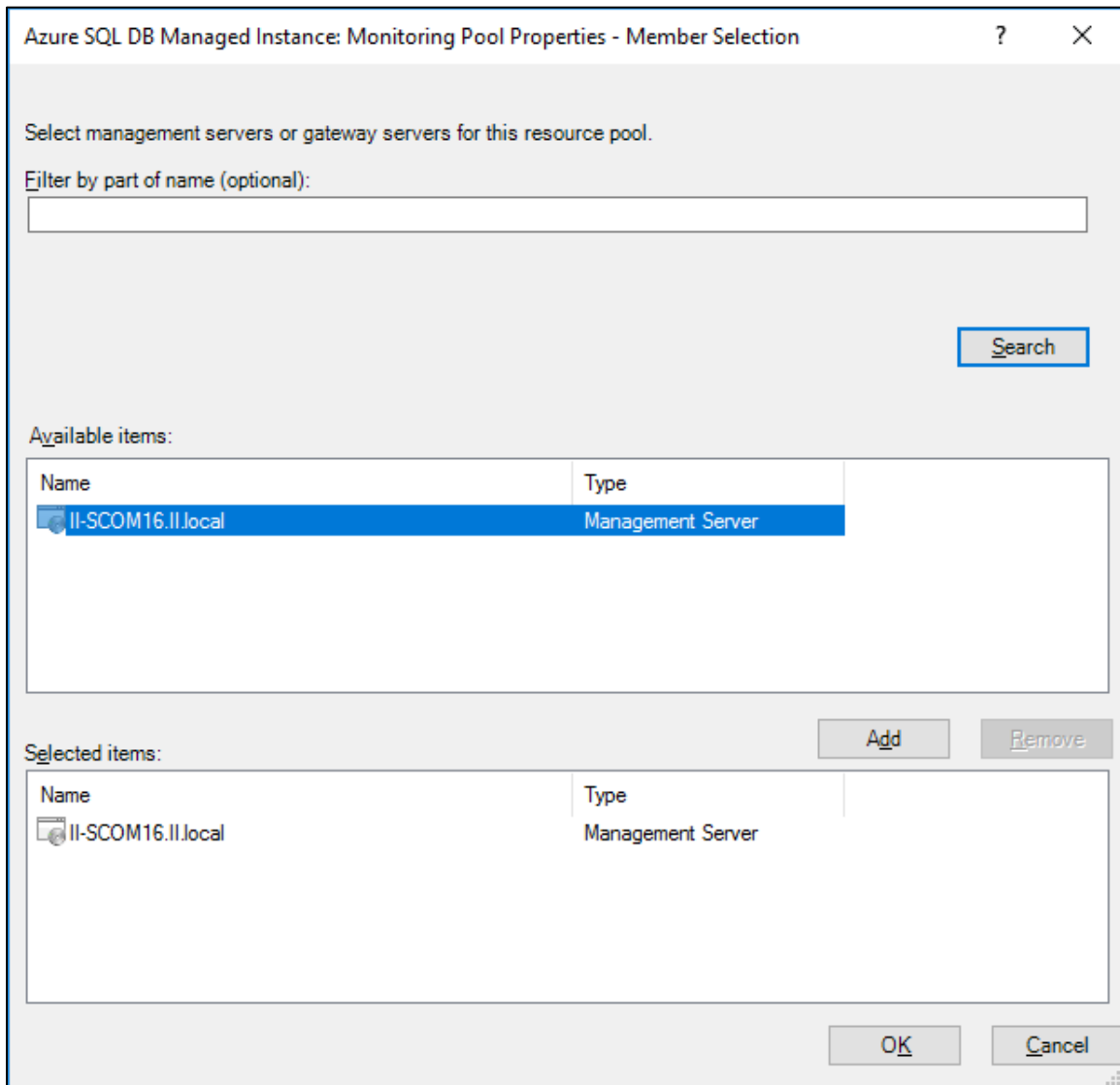
< Previous   **Next >**   Save   Cancel

In this window, enter a name and description for the Resource Pool and click the **Next** button. As a result, the **Pool Membership** window will appear.



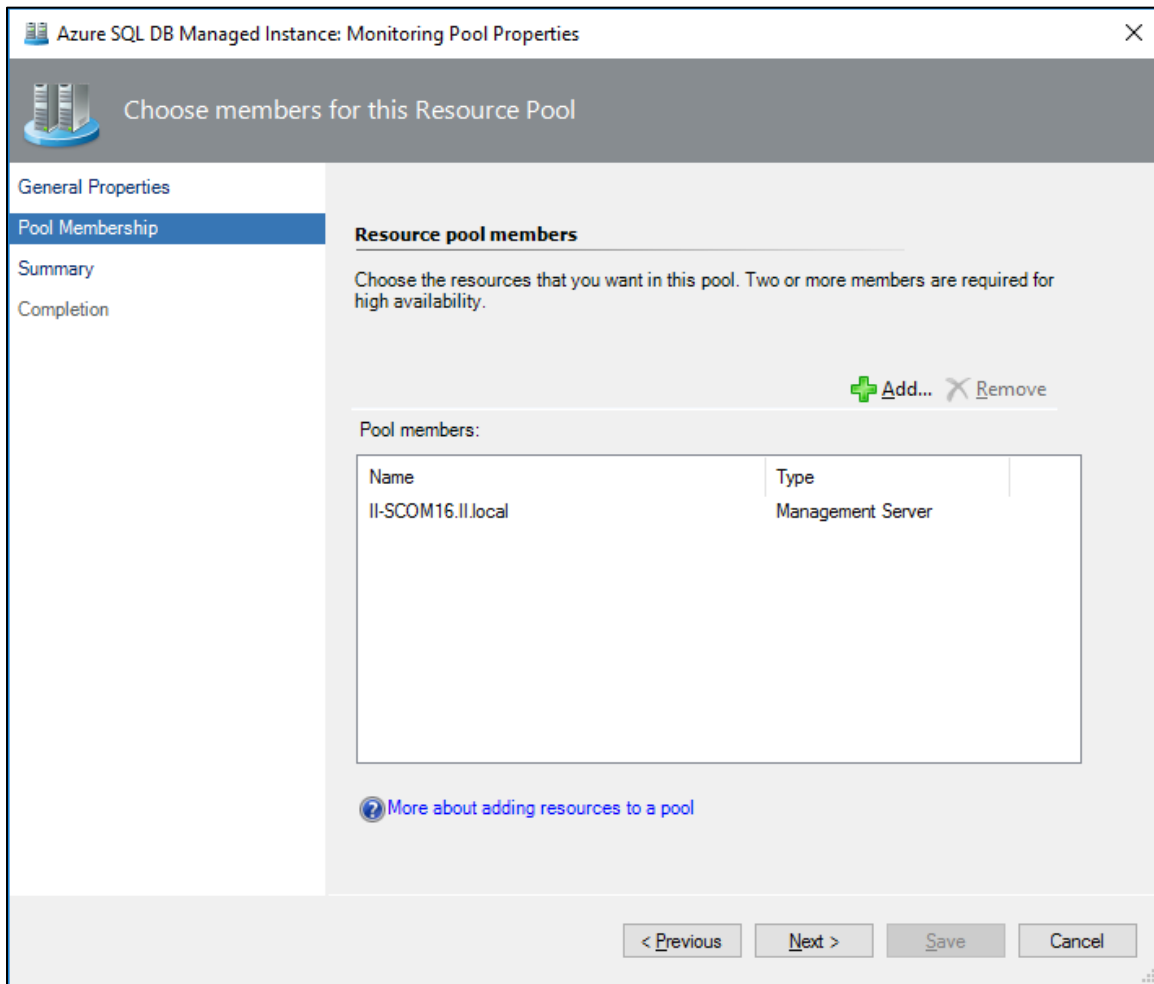


In this window, click the **Add...** button to populate the monitoring pool.

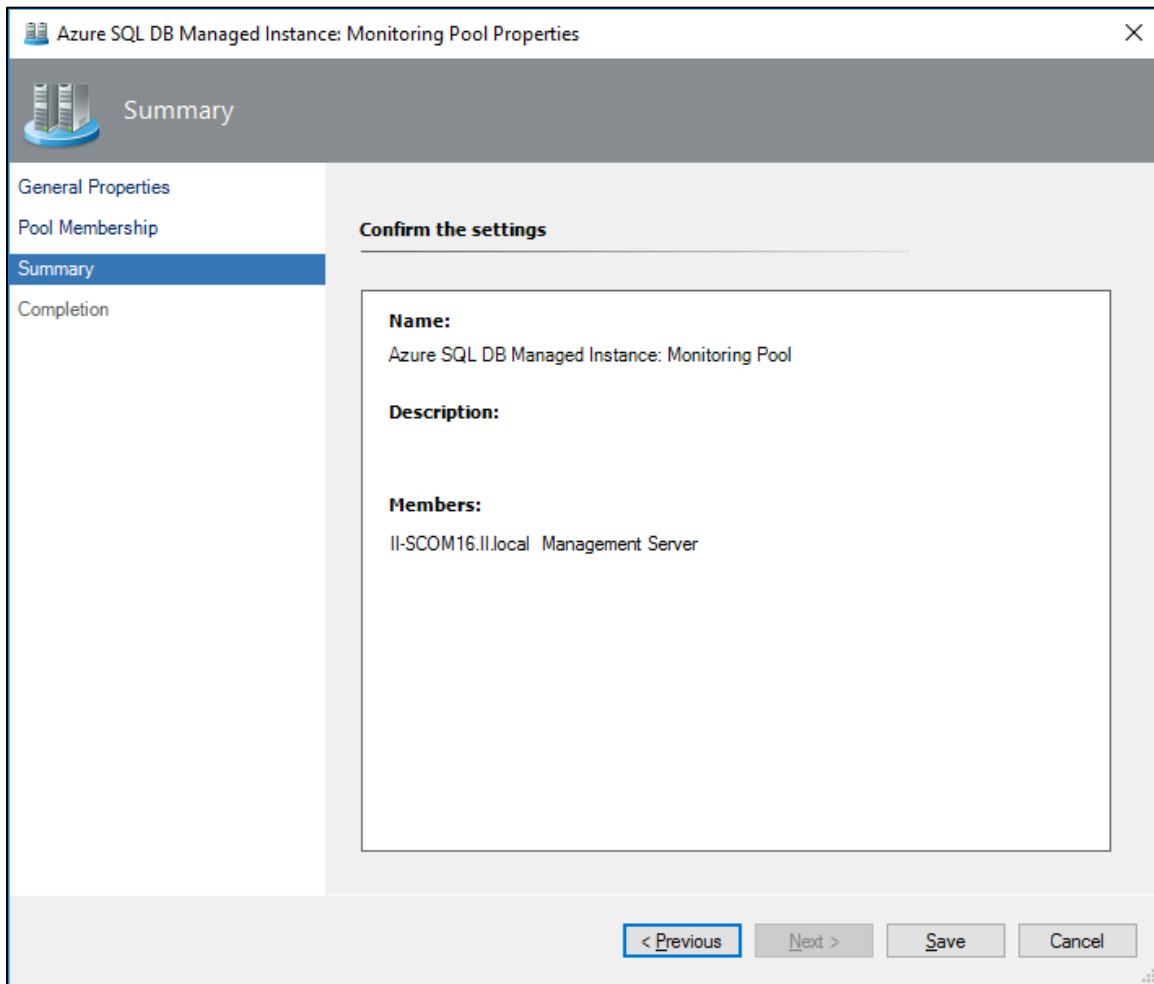


Click the **OK** button to complete the procedure.

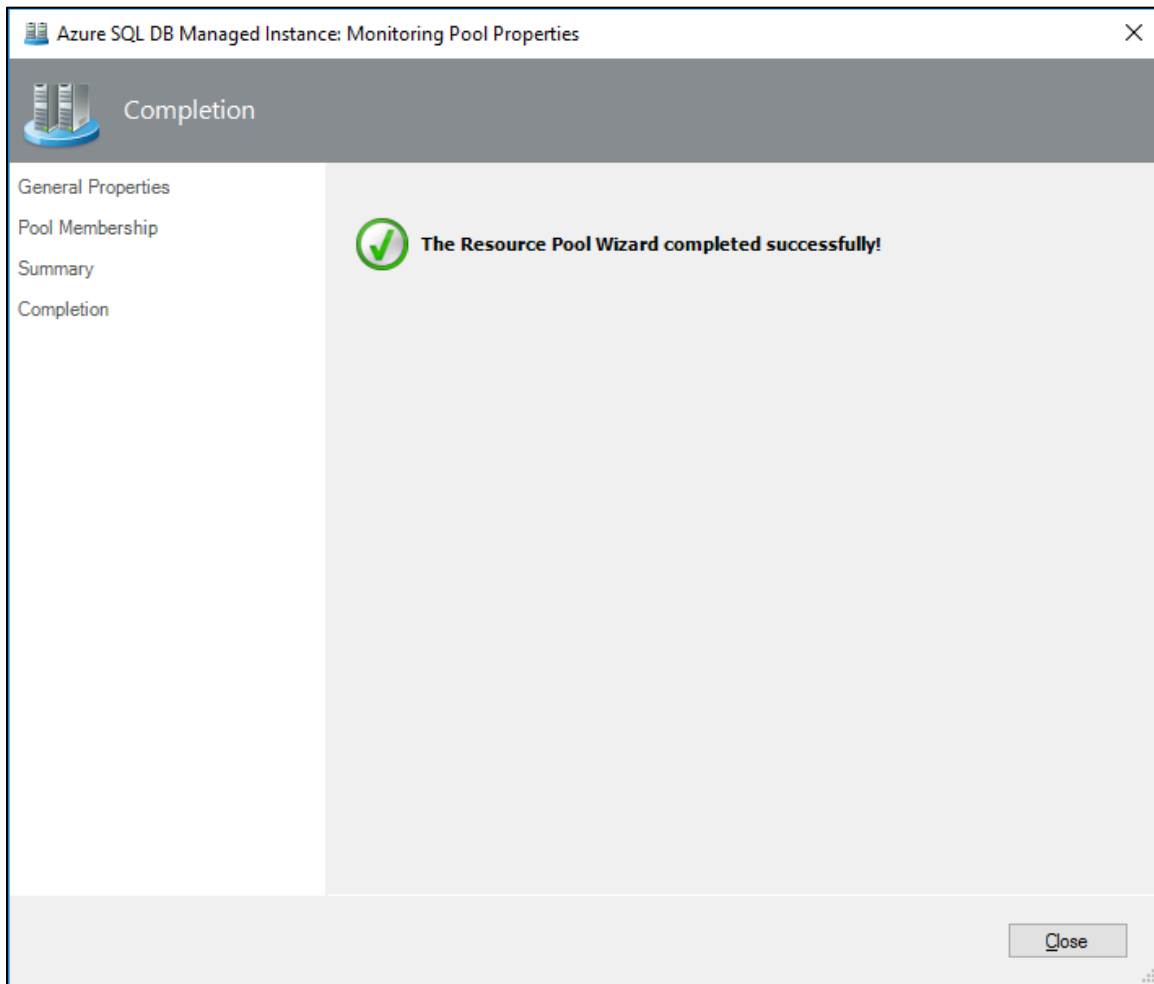
**Note:** If the pool remains empty, it mirrors the contents of All Management Servers pool. The pool can be populated with either Gateways or Management Servers, but they should not be added to the pool together.



Click the **Next** button to view the **Summary** window.



In this window, check the applied settings and click the **Save** button if they are correct. Otherwise, click the **Previous** button and make necessary corrections.



Close the final **Completion** window by clicking the corresponding button.

## Management Pack Purpose

In this section:

- [Monitoring Scenarios](#)
- [How Health Rolls Up](#)



### Note

For details on the discoveries, rules, and monitors contained in this management pack, see the following section of this guide:

- [Appendix: Management Pack objects and workflows](#)

## Monitoring Scenarios

### Database Discovery and State Monitoring

For each Managed Instance, its databases are discovered and monitored using a number of rules and monitors. Please refer to “[Appendix: Management Pack objects and workflows](#)” section for the full list of rules and monitors targeted to databases.

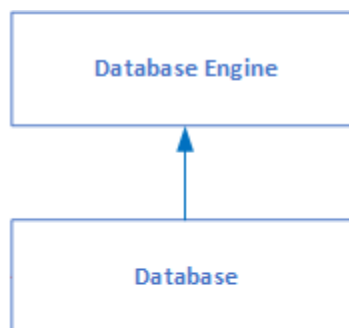
### Blocked Sessions

The management pack defines the “**Blocking Sessions**” monitor, which is designed to query each database for sessions, which are blocked during a significant period. If blocking is detected and it exceeds the given threshold, then the state is changed and an alert is raised.


You can apply an override to change the **WaitMinutes** parameter, which is used to determine if the blocked session should be considered as long-running or not. The default value for this parameter is **one minute**.

### How Health Rolls Up

The following diagram shows how the health states of objects roll up in this management pack.



#### Legend:

WorstOf Algorithm 

## Configure the Management Pack

This section provides guidance on configuring and tuning this management pack.

In this section:

- [Best Practice: Create a Management Pack for Customizations](#)
- [How to Import a Management Pack](#)
- [Security Configuration](#)
  - [Run As Profiles](#)
  - [Low-Privilege Environments](#)

### Best Practice: Create a Management Pack for Customizations

The Management Pack for Microsoft Azure SQL DB Managed Instance is sealed so that you cannot change any of the original settings in the management pack file. However, you can create customizations, such as overrides or new monitoring objects, and save them to a different management pack. By default, the Operations Manager saves all customizations to the default management pack. As a best practice, you should instead create a separate management pack for each sealed management pack you want to customize.

Creating a new management pack for storing overrides has the following advantages:

- When you create a management pack for storing customized settings for a sealed management pack, it is helpful to base the name of the new management pack on the name of the management pack that it is customizing, such as “Microsoft Azure SQL DB Managed Instance Overrides”.
- Creating a new management pack for storing customizations of each sealed management pack makes it easier to export the customizations from a test environment to a production environment. It also makes it easier to delete a management pack, because you must delete any dependencies before you can delete a management pack. If customizations for all management packs are saved in the Default Management Pack and you need to delete a single management pack, you must first delete the Default Management Pack, which also deletes customizations to other management packs.

For more information about sealed and unsealed management packs, see [Management Pack Formats](#) article. For more information about management pack customizations and the default management pack, see [About Management Packs](#) article.

## How to Create a New Management Pack for Customizations

1. Open the Operations console, and then click the **Administration** button.
2. Right-click **Management Packs**, and then click **Create New Management Pack**.
3. Enter a name (for example, “Azure SQL MI MP Customizations”), and then click **Next**.
4. Click **Create**.

## How to Import a Management Pack

For the detailed information about importing a management pack, see [How to Import a Management Pack](#) article.

## Security Configuration

This section provides guidance on configuring the security for this management pack.

In this section:

- [Run As Profiles](#)



### Note

Low-Privilege security configuration is not supported in this preview version. You should grant your monitoring accounts with SA permissions.

## Run As Profiles

The Management Pack contains a single Run As Profile, which is used by all discoveries, monitors, and tasks defined in the management pack:

- Microsoft Azure SQL Database Managed Instance SQL Credentials Run As Profile















## View Information in the Operations Manager Console

### Views and Dashboards

This management pack introduces common folder structure, which will be used by future releases of management packs for different components of Azure SQL DB Managed Instance.



The following views and dashboards are version-independent and show information about all versions of Azure SQL DB Managed Instance:

-  **Microsoft Azure SQL DB Managed Instance**
  -  **Active Alerts**
  -  **All Performance Data**
  -  **Summary**
  -  **Task Status**
  -  **Managed Instances**
    -  **Databases**
    -  **Managed Instances**
  -  **Memory-Optimized Data**
    -  **Active Alerts**
    -  **All Performance Data**
    -  **Memory-Optimized Data Filegroup Containers**
    -  **Memory-Optimized Data Filegroups**
    -  **Resource Pools**

## Azure SQL DB Managed Instance Views

The Management Pack for Microsoft Azure SQL DB Managed Instance introduces the comprehensive set of state, performance and alert views, which can be found in the dedicated folder:

-  **Monitoring**
  -  **Microsoft Azure SQL DB Managed Instance**

### **Note**

Some views may contain a very long list of objects or metrics. To find a specific object or group of objects, you can use the **Scope**, **Search**, and **Find** buttons on the Operations Manager toolbar. For more information, see “[Finding Data and Objects in the Operations Manager consoles](#)” article in the Operations Manager Help.

## Appendix: Known Issues and Troubleshooting

### **Rules and monitors may provide incorrect data if default interval override values are changed**

**Issue:** If the value of Interval (seconds) overridable parameter is set lower than the default value, rules and monitors may provide incorrect data.

**Resolution:** Make sure that Interval (seconds) overridable parameter is set no lower than the default value.

### **Seed discovery of a deleted platform pack may be still working on the pool nodes**

**Issue:** An error may occur when a platform pack was deleted, but its seed discovery is still working on the pool nodes.

**Resolution:** Upon deletion of a platform pack, delete the corresponding seed discovery manually.

### **“Database Status” monitor is constantly changing its status**

**Issue:** If “Auto Close” parameter for the database is set to “True”, “Database Status” monitor is constantly changing its status from “Healthy” to “Recovering/Restoring” and vice versa according to the timeout set in the override parameters.

**Resolution:** In view of the monitoring operation specifics, no resolution is required.

### **Enabling of “Auto Close” database parameter blocks collection of the performance metrics**

**Issue:** If “Auto Close” parameter for the database is set to “True”, all performance rules return empty values.

**Resolution:** Set “Auto Close” database parameter back to “False”.

### **If a Managed Instance is not available, multiple errors occur in the watcher node event log**

**Issue:** If a Managed Instance is not available, multiple errors appear in the watcher node event log. The errors will keep coming until the Managed Instance is available.

**Resolution:** No resolution available.

### **Double quotes in a database name may cause database console tasks failures**

**Issue:** Database console tasks take database names enclosed in double quotes as one of their arguments. A database name may contain any symbol including double quotes. If it does, the console tasks for this database will not work.

**Resolution:** No resolution.

**When an instance is not available,**

**Module.Monitoring.Performance.SqlOsPerfCounterReaderHelper exception is received in the event log**

**Issue:** When an instance is not available, Module.Monitoring.Performance.SqlOsPerfCounterReaderHelper exception is received in the event log. This exception will keep coming until the instance is available. The interval of this exception coming is equal to the lowest interval set for the performance rules.

**Resolution:** No resolution.

**Odd behavior of the monitors' operational states**

**Issue:** If the resource pool contains more than one management server, the operational states of all the monitors will be changing according to the failover settings of the resource pool.

**Resolution:** No resolution.

**Monitoring errors 40 and 121 may occur**

**Issue:** Monitoring errors 40 and 121 may sporadically occur in the event log.

**Resolution:** No resolution.

**Extended discovery intervals**

**Issue:** In case of using a resource pool with several watcher nodes, the discovery intervals may be significantly extended.

**Resolution:** No resolution.

**Some error messages may appear in the Operations Manager events after adding a new database to already monitored MI**

**Issue:** Some error messages may appear in the Operations Manager events after adding a new database to already monitored MI during the discovery process:

- Skipping the default startup of the database because the database belongs to an availability group.
- The database cannot be opened due to inaccessible files, insufficient memory or lack of disk space.

**Resolution:** No resolution.

**Error messages may appear in the event log after monitoring template creation**

**Issue:** "Windows logins are not supported in this version of SQL Server" and "Object reference not set to an instance of an object" error messages may appear in the Operations Manager event log after the creation of a monitoring template.

**Resolution:** No resolution.

**Memory-Optimized Data Stale Checkpoint File Pairs Ratio monitor may not change its state**

**Issue:** Memory-Optimized Data Stale Checkpoint File Pairs Ratio monitor may not change its state from Warning to Success.

**Resolution:** Reset health state of the monitor.