Configure Remote Management in Server Manager

Updated: August 21, 2012

Applies To: Windows Server 2012

In Windows Server® 2012, you can use Server Manager to perform management tasks on remote servers. Remote management is enabled by default on servers that are running Windows Server 2012. To manage a server remotely by using Server Manager, you add the server to the Server Manager server pool.

You can use Server Manager to manage remote servers that are running Windows Server 2008 and Windows Server 2008 R2, but the following updates are required to fully manage these older operating systems.

- **Windows Management Framework 3.0** To use this release of Server Manager to access and manage remote servers that are running Windows Server 2008 or Windows Server 2008 R2, you must first install .NET Framework 4.0, and then install Windows Management Framework 3.0 on those servers. Server Manager in Windows Server 2012 or Windows 8 cannot fully manage other Windows operating systems until updated Windows Management Instrumentation (WMI) providers are installed on those systems. The updated WMI providers let Server Manager collect information about roles and features that are installed on the managed servers. Until the update is applied, servers that are running Windows Server 2008 or Windows Server 2008 R2 have a manageability status of **Not accessible – Verify that earlier versions of Windows run the Windows Management Framework 3.0 package**.

- **Performance Updates** You cannot get performance data for computers that run Windows Server 2008 or Windows Server 2008 R2 until the performance update that is associated with KB 2682011 is installed on those operating systems. Install KB 2682011 or a superseding update on servers that are running those operating systems, and then turn on performance counters for those servers in Server Manager.

For detailed information about how to add servers that are in workgroups to manage, or manage remote servers from a workgroup computer that is running Server Manager, see Add Servers on the Windows Server TechCenter.

Enabling or disabling remote management

In Windows Server 2012, remote management is enabled by default. Before administrators can connect to a computer that is running Windows Server 2012 remotely by using Server Manager, Server Manager remote management must be enabled on the destination computer if it has been

disabled. The procedures in this section describe how to disable remote management, and how to re-enable remote management if it has been disabled. In the Server Manager console, the remote management status for the local server is displayed in the **Properties** area of the **Local Server** page.

Local administrator accounts other than the built-in Administrator account may not have rights to manage a server remotely, even if remote management is enabled. The Remote User Account Control (UAC) **LocalAccountTokenFilterPolicy** registry setting must be configured to allow local accounts of the Administrators group other than the built-in administrator account to remotely manage the server.

In Windows Server 2012, Server Manager relies on WinRM and the Distributed Component Object Model (DCOM) for remote communications. The settings that are controlled by the **Configure Remote Management** dialog box only affect parts of Server Manager and Windows PowerShell that use WinRM for remote communications. They do not affect parts of Server Manager that use DCOM for remote communications. For example, Server Manager uses WinRM to communicate with remote servers that are running Windows Server 2012, but uses DCOM to communicate with servers that are running Windows Server 2008 and Windows Server 2008 R2, but do not have the Windows Management Framework 3.0 update applied. Microsoft Management Console (MMC) and other legacy management tools use DCOM. For more information about how to change these settings, see To configure MMC or other tool remote management over DCOM in this topic.

Note

Procedures in this section can be completed only on computers that are running Windows Server. You cannot enable or disable remote management on a computer that is running the Windows 8 client operating system by using these procedures, because the client operating system cannot be managed by using Server Manager.

- To configure WinRM remote management, select one of the following procedures.
    - To configure Server Manager remote management by using the Windows interface
    - To enable Server Manager remote management by using Windows PowerShell
    - To configure Server Manager remote management by using the command line
    - To enable Server Manager and Windows PowerShell remote management on earlier releases of Windows Server
- To disable WinRM and Server Manager remote management, select one of the following procedures.
    - To disable remote management by using Group Policy

    - To disable remote management by using an answer file during unattended installation

- To configure DCOM remote management, see To configure MMC or other tool remote management over DCOM.

To configure Server Manager remote management by using the Windows interface

---

1.

   Note

   The settings that are controlled by the **Configure Remote Management** dialog box do not affect parts of Server Manager that use DCOM for remote communications.

2. On the computer that you want to manage remotely, open Server Manager, if it is not already open. On the Windows taskbar, click **Server Manager**. On the **Start** screen, click the **Server Manager** tile.
3. In the **Properties** area of the **Local Servers** page, click the hyperlinked value for the **Remote management** property.
4. Do one of the following, and then click **OK**.
    - To prevent this computer from being managed remotely by using Server Manager (or Windows PowerShell if it is installed), clear the **Enable remote management of this server from other computers** check box.

    - To let this computer be managed remotely by using Server Manager or Windows PowerShell, select **Enable remote management of this server from other computers**.

To enable Server Manager remote management by using Windows PowerShell

---

1. On the computer that you want to manage remotely, do one of the following to open a Windows PowerShell session with elevated user rights.
    - On the Windows desktop, right-click **Windows PowerShell** on the taskbar, and then click **Run as Administrator**.

    - On the Windows **Start** screen, right-click **Windows PowerShell**, and then on the app bar, click **Run as Administrator**.

2. Type the following, and then press **Enter** to enable all required firewall rule exceptions.

   Configure-SMRemoting.exe -enable

To configure Server Manager remote management by using the command line

---

1. On the computer that you want to manage remotely, open a command prompt session with elevated user rights. To do this, on the **Start** screen, type **cmd**, right-click the **Command Prompt** tile when it is displayed in the **Apps** results, and then on the app bar, click **Run as Administrator**.
2. Run the following executable file.

   %windir%\system32\Configure-SMRemoting.exe

3. Do one of the following:
   - To disable remote management, type **Configure-SMRemoting.exe -disable**, and then press **Enter**.
   - To enable remote management, type **Configure-SMRemoting.exe -enable**, and then press **Enter**.
   - To view the current remote management setting, type **Configure-SMRemoting.exe -get**, and then press ENTER.

[To enable Server Manager and Windows PowerShell remote management on earlier releases of Windows Server]

- Do one of the following:
  - To enable remote management on servers that are running Windows Server 2008 R2, see [Remote Management with Server Manager] in the Windows Server 2008 R2 Help.
  - To enable remote management on servers that are running Windows Server 2008, see [Enable and Use Remote Commands in Windows PowerShell].
  - To enable remote management on servers that are running Windows Server 2003, see [How to Install Windows PowerShell on Windows Server 2003 and Enable Remote Management] to enable remote management by using Windows PowerShell, or [Installation and Configuration for Windows Remote Management] to enable remote management by using **winrm**.

[To configure MMC or other tool remote management over DCOM]

---

1. Do one of the following to open the Windows Firewall with Advanced Security snap-in.
   - In the **Properties** area of the **Local Server** page in Server Manager, click the hypertext value for the **Windows Firewall** property, and then click **Advanced settings**.
   - On the **Start** screen, type **WF.msc**, and then click the snap-in tile when it is displayed in the **Apps** results.

2. In the tree pane, select **Inbound Rules**.
3. Verify that exceptions to the following firewall rules are enabled, and have not been disabled by Group Policy settings. If any are not enabled, go on to the next step.
    - COM+ Network Access (DCOM-In)
    - Remote Event Log Management (NP-In)
    - Remote Event Log Management (RPC)
    - Remote Event Log Management (RPC-EPMAP)
4. Right-click the rules that are not enabled, and then click **Enable Rule** on the context menu.
5. Close the Windows Firewall with Advanced Security snap-in.

To disable remote management by using Group Policy

---

1. Do one of the following to open Local Group Policy Editor.
    - On a server that is running Windows Server 2012, on the **Start** screen, type **gpedit.msc**, and then click the **gpedit** tile when it is displayed.
    - On a server that is running Windows Server 2008 R2 or Windows Server 2008, in the **Run** dialog box, type **gpedit.msc**, and then press **Enter**.
2. Open **Computer Configuration\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service**.
3. In the content pane, double-click **Allow remote server management through WinRM**.
4. In the dialog box for the **Allow remote server management through WinRM** policy setting, select **Disabled** to disable remote management. Click **OK** to save your changes and close the policy setting dialog box.

To disable remote management by using an answer file during unattended installation

---

1. Create an unattended installation answer file for Windows Server 2012 installations by using Windows System Image Manager (Windows SIM). For more information about how to create an answer file and use Windows SIM, see What is Windows System Image Manager? and Step-by-Step: Basic Windows Deployment for IT Professionals.
2. In your answer file, locate the setting **Microsoft-Windows-Web-Services-for-Management-Core\EnableServerRemoteManagement**.
3. To disable Server Manager remote management by default on all servers to which you want to apply the answer file, set **Microsoft-Windows-Web-Services-for-Management-Core \EnableServerRemoteManagement** to **False**.

    Note

    This setting disables remote management as part of the operating system setup process.

Configuring this setting does not prevent an administrator from enabling Server Manager remote management on a server after operating system setup is complete. Administrators can enable Server Manager remote management again by using steps in To configure Server Manager remote management by using the Windows interface or To enable Server Manager remote management by using Windows PowerShell in this topic.
If you disable remote management by default as part of an unattended installation, and do not enable remote management on the server again after installation, servers to which this answer file is applied cannot be fully managed by using Server Manager. Servers that are running Windows Server 2012—and that have remote management disabled by default—generate manageability status errors in the Server Manager console after they are added to the Server Manager server pool.

Windows Remote Management (WinRM) listener settings

Server Manager relies on default WinRM listener settings on the remote servers that you want to manage. If the default authentication mechanism or the WinRM listener port number on a remote server has been changed from default settings, Server Manager cannot communicate with the remote server.

The following list shows default WinRM listener settings for managing by using Server Manager.

- The WinRM service is running.
- A WinRM listener is created to accept HTTP requests through port number 5985.
- Port number 5985 is enabled in Windows Firewall settings to allow requests through WinRM.
- Both **Kerberos** and **Negotiate** authentication types are enabled.

The default port number is 5985 for WinRM to communicate with a remote computer.

For more information about how to configure WinRM listener settings, at a command prompt, type **winrm help config**, and then press ENTER.